IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 22, 2022, accepted May 20, 2022, date of publication May 25, 2022, date of current version May 31, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3177842

Electric Vehicle User Data-Induced Cyber Attack on Electric Vehicle Charging Station

SEONG ILE JEONG, (Student Member, IEEE), AND DAE-HYUN CHOI, (Member, IEEE)
School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 156-756, South Korea

Corresponding author: Dae-Hyun Choi (dhchoi@cau.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF), Ministry of Education, under Grant 2020R1F1A1049314; and in part by the Chung-Ang University Research Scholarship Grants, in 2021.

ABSTRACT Electric vehicle (EV) user data (e.g., arrival/departure times and initial/desired state of energy (SOE) of the EV at EV charging stations (EVCSs)) are crucial data based on which the energy management system (EMS) of EVCS calculates the economic charging schedules of EVs according to their preferred charging conditions. In this paper, we present a novel cyber attack via the manipulation of EV user data against the EMS of an EVCS that may result in incorrect electricity costs incurred by the EVCS through distorted charging schedules of EVs. The proposed attack method is formulated as a mixed-integer linear-programming-based bi-level optimization problem that comprises upper- and lower-level optimization problems. At the upper level, malicious EV user data injected into the communication network between the EVs and the EMS of the EVCS are calculated, while a normal operation of the EV charging optimization algorithm in the EMS is ensured at the lower level even if malicious data are delivered from the upper level. The formulated bi-level optimization problem is converted into a single-level optimization problem by replacing the lower-level problem with its corresponding Karush–Kuhn–Tucker conditions. The feasibility of the proposed cyber attack against EVCSs is demonstrated via a simulated scenario in which 40 EVs arrive at an EVCS, which has six charging poles with different charging speeds. The economic impact of such an attack is quantified in terms of the total electricity cost incurred by the EVCS, charging schedule, initial/desired SOE of EVs, and attack effort.

INDEX TERMS Cyber attack, electric vehicle, electric vehicle charging station, energy management system, bi-level optimization method.

I. INTRODUCTION

Transportation electrification through which fossil-fuel vehicles are replaced by electric vehicles (EVs) is becoming feasible owing to the environmental and economic advantages of EVs [1]. Compared to fossil-fuel vehicles, EVs can reduce carbon pollution, greenhouse gas emissions, and the consumption of fossil resources. Furthermore, EVs are utilized as flexible loads to conduct peak shaving and voltage regulation by controlling their charging and discharging capabilities through the vehicle-to-grid technology, thereby maintaining a stable operation of the power distribution grid [2]. For transportation electrification, EV charging stations (EVCSs) constitute a crucial equipment through which EVs charge their desired power from the power distribution grid. To achieve transportation electrification along with the aforementioned advantages of EVs, it is necessary to develop a system for EVCS operators to manage the charging schedules of EVs to minimize their electricity charging costs while maintaining the charging preferences of EV users [3].

Energy management systems (EMSs) for EVCS constitute a core technology for EVCS operators to conduct optimal charging scheduling of EVs that charge their power via charging poles at the EVCS. In general, an optimization algorithm is implemented in the EMS to calculate the optimal charging schedules of EVs by minimizing the costs incurred by the EVCS while purchasing electricity from power utilities according to the charging preferences of EV users [4]. To this end, two types of data need to be embedded into the optimization algorithm of EMSs prior to its execution. The first type corresponds to static data, which include the number and type of charging poles of the EVCS (these poles can have different

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Abdur Razzaque.

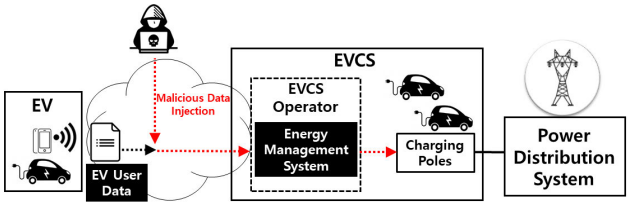

FIGURE 1. EV user data-induced cyber attack on the EMS of an EVCS.

charging speeds) as well as the time-of-use (TOU) pricing tariff. The second type represents dynamically varying data of heterogeneous EV users, which are transmitted through the communication network from EV users to the EMS of an EVCS via their mobile phones. These dynamically varying data for each EV user include i) the predicted arrival time and initial state of energy (SOE) of the EV when the EV arrives at the EVCS, and ii) the preferred departure time and desired SOE of the EV when the EV departs from the EVCS.

The mobile communication network employed for communication between EVs and the EMSs of EVCSs may be vulnerable to potential cyber attacks that compromise the mobile phones of EV users, as illustrated in Fig. 1. The adversary can penetrate the communication channels in cellular or Wi-Fi wireless networks and inject malicious data into the aforementioned second type of EV user data. Consequently, the manipulated EV user data may lead to the malfunction of the optimization algorithm in the EMS of an EVCS, thereby increasing the total electricity cost incurred by the EVCS by distorting the EV charging schedules. The primary goal of this study is to propose a novel cyber attack strategy in which the adversary increases the electricity cost incurred by the EVCS by manipulating EV user data and investigate the economic impact of the operation of EVCS subject to such an attack.

Given that EVCSs and EVs are tightly coupled through an advanced information and communication technology (ICT) for efficient EV charging and stable operation of the power distribution grid, numerous previous studies have explored various types of cyber threat models, which exploit the vulnerability of ICT networks, and developed methods for detecting and mitigating such threats. In [5]–[7], three types of confidentiality-integrity-availability cyber attacks on EVCSs, namely eavesdropping attack (confidentiality attack), man-in-the-middle attack (integrity attack), and denial-of-service attack (availability attack), were introduced, and the risk assessment of EVCSs subject to these attacks was conducted. In [8], a risk assessment framework for large-scale EVCSs was developed to evaluate the vulnerability of EVCSs to cyber attacks on the communication between EVCSs and electric utilities. Various cyber attacks on EVs and EVCSs were presented in [9]; herein, cyber attacks were classified according to the type of exchanged data among the EVs, EV aggregators, and EVCS control centers. A novel data-driven cyber attack strategy was proposed in [10] in which the adversary manipulates EVs and the EVCS loads to yield frequency instability in the electric power grid using available data from power grid, EVCSs, and EVs. In [11], a cyber attack for manipulation of the SOE of EVs was presented, and a method for estimating the manipulated SOE was developed using a back-propagation neural network based on experimental data. In [12], the impact of cyber attacks on the transportation system, electric power grid, and EVCSs was discussed, and some guidelines to protect the EV charging network from cyber attacks were introduced. The vulnerability of the onboard charger hardware of an EV to data integrity attacks was investigated in [13] wherein the adversary disrupts the main charger controller logic and battery management system by performing fake communication between the charging controller and electronic control units. In [14], [15], new attack strategies to distort the communication protocol, in particular the open charge point protocol, between the EMS of an EVCS and the EVCS control center were introduced. Here, the adversary following the attack strategy misleads the EVCS operator, causing incorrect authentication of new EV users and dispatching incorrect charging commands to EVs. More recently, a cyber attack based on the manipulation of EV charging and discharging against a power grid was investigated in [16]. It was verified that because of the high reactive power demand of EVs, the manipulation of EV load has a greater detrimental impact on the power grid operation than that of the residential load. A concise review of various cyber attacks on EVs and EVCSs and the risk assessment of power grid operation subject to such attacks is provided in [17]. In contrast with attack models and corresponding attack impact analysis, various defending algorithms that detect cyber attacks on EVs and EVCSs and mitigate the impact of such attacks have been developed. Data-driven approaches were adopted for the detection of cyber attack against i) EVs using a machine learning method based on the transient physical characteristics of EVs [18], and ii) EVCSs using deep neural networks and long-short-term memory methods [19]. In [20], a mixed-integer linear programming (MILP)-based optimization model was presented to minimize the risk of attack propagation by isolating a group of compromised EVCSs. A new attack mitigation approach using cyber insurance was proposed in [21] in which the risk of EVs to cyber attack is transferred by cyber insurance to a third party so that the EVs are always assigned the best charging/discharging price. In [22], a cyber attack that targets the inter-area stability of the power grid through the malfunction of EVCSs was considered, and a two-stage defending method for EVCSs was developed for attack detection using a back-propagation neural network scheme. Attack mitigation through the deletion of adversarial requests from EVCSs was also proposed.

However, previous studies have neither formulated a mathematical attack strategy via the manipulation of EV user data to cause malfunction of the EMS of an EVCS nor conducted attack impact analysis. To the best of our knowledge, the present study is the first of its kind aiming to develop a man-in-the-middle attack method based on a bi-level optimization

problem in which the adversary stealthily injects malicious data into the EV user data and causes a malfunction of the EMS, thereby increasing the total electricity cost incurred by the EVCS owing to the manipulated EV charging schedule. The main contributions of this study can be summarized as follows:

1) We propose a cyber attack on the EV charging optimization algorithm deployed in the EMS of an EVCS. The adversary distorts the charging schedules of EVs at the EVCS by stealthily manipulating the EV user data (arrival/departure times and initial/desired SOE of EVs at the EVCS), which are transmitted from EVs to the EVCS, thereby increasing the total electricity cost incurred by the EVCS.
2) We address the proposed attack method using a bilevel optimization problem that comprises upper- and lower-level optimization problems. In the former, malicious data injected into the EV user data are calculated to distort the EV charging schedule with minimum attack effort. In the latter, the EV charging optimization algorithm is ensured to be executed normally even if malicious data are calculated from the former. We then reformulate the bi-level optimization problem into a single-level optimization problem by replacing the lower-level problem with its Karush–Kuhn–Tucker (KKT) conditions.
3) We validate the feasibility and performance of the proposed attack method through a simulation scenario in which 40 EVs charge power via charging poles with different charging speeds at an EVCS during one day. Numerical examples confirm that the proposed attack method has a detrimental economic impact on the EVCS operation by manipulating the EV charging schedule in terms of the total electricity cost incurred by the EVCS and charging energy of EVs.

The remainder of this paper is organized as follows. Section II introduces a system model for the charging of multiple EVs at an EVCS and an EV charging optimization problem with an attack model. Section III presents a mathematical formulation of the proposed attack strategy using both bi-level and single-level optimization problems. Section IV presents numerical examples that demonstrate the performance of the proposed attack method. Finally, conclusions and future research directions are drawn in Section V.

II. PROBLEM DESCRIPTION

A. SYSTEM MODEL

Let us consider a situation in which multiple EVs with different charging conditions and EV user preferences are charged at a single EVCS having three different charging power levels (i.e., Levels 1, 2, and 3). The EVCS is connected to power distribution system, which is managed by distribution system operator (DSO). In this study, DSO provides the EVCS with the TOU pricing signal, using which the EVCS purchases power from the distribution grid and supplies it to EVs connected to the EVCS. The EV charging scenario comprises the following two steps:

Step 1) Before the EVs arrive at their targeted EVCS, EV users send their private charging information using their mobile phones through a communication network to the EVCS.
Step 2) Using the information received from the EV users in Step 1), the EMS in the EVCS schedules optimal charging powers for EVs that arrive at the EVCS and assigns optimal charging poles.

In Step 1), vector $\mathbf{D}_j$ encoding the private charging information delivered by the EV user $j \in \mathcal{J}$ contains four types of data:

$$\mathbf{D}_j = \left[a_j, d_j, SOE_j^{\mathrm{I}}, SOE_j^{\mathrm{D}}\right]. \tag{1}$$

In (1), a_j and d_j represent the predicted arrival and desired departure times of EV j at the EVCS, respectively; SOE_j^{I} is the predicted initial SOE of EV j when it arrives at the EVCS; SOE_j^{D} is the minimum threshold for the desired SOE level of EV j when it departs from the EVCS. In this study, we assume that the predicted and desired data of EV users are quite accurate.

In Step 2), we assume that the EVCS has multiple charging poles $i \in \mathcal{I} = \mathcal{I}^{(1)} \bigcup \mathcal{I}^{(2)} \bigcup \mathcal{I}^{(3)}$ that are categorized into three types of charging poles with different maximum charging limits: $i \in \mathcal{I}^{(1)}$ for Level-1 charging (50 kW), $i \in \mathcal{I}^{(2)}$ for Level-2 charging (100 kW), and $i \in \mathcal{I}^{(3)}$ for Level-3 charging (200 kW). The EVCS is assumed to be equipped with an optimization-based EMS to achieve economic operation. Under TOU pricing tariff, the EMS assists the EVCS operator to minimize the total charging cost of EVs (i.e., the total cost suffered by the EVCS while purchasing electricity from power utilities) through the optimal charging scheduling and charging pole assignment for EVs according to the predicted EV charging condition and desired comfort level of the EV user. Note that the EMS requires various types of input data to economically operate the EVCS and completely satisfy EV user preferences. These input data include the maximum SOE ($SOE_j^{\max}$) of each EV j and the maximum charging power ($P_i^{\max}$) at charging pole i for the EVCS along with the private user data of EV j ($\mathbf{D}_j$) defined in Step 1). The EMS includes an EV charging optimization module based on the aforementioned input data. The mathematical model is detailed in the next subsection.

B. EV CHARGING OPTIMIZATION MODEL

For each EV j, at a scheduling time $k \in \mathcal{K} := \{t, t+1, \ldots, t+h-1\}$ with a scheduling unit time Δt and prediction horizon h, the EV charging algorithm is formulated in terms of the following MILP optimization problem:

$$\min J = \sum_{k\in\mathcal{K}} \left(C_k \sum_{j\in\mathcal{J}} P_{j,k} \right) \Delta t \tag{2}$$

$$\text{s.t. } \boldsymbol{\alpha} : SOE_{j,k+1} = SOE_{j,k} + P_{j,k}\Delta t \tag{3}$$

$$\boldsymbol{\beta} : SOE_j^{\mathrm{I}} \le SOE_{j,k} \le SOE_j^{\max} \tag{4}$$

$$\boldsymbol{\gamma} : SOE_j^{\mathrm{D}} \leq SOE_{j,t+h} \tag{5}$$

$$\boldsymbol{\chi} : 0 \leq P_{j,k} \leq \sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} P_i^{\max} \tag{6}$$

$$\boldsymbol{\lambda} : \frac{SOE_j^{\mathrm{D}} - SOE_{j,k}}{SOE_j^{\max}} \leq b_{j,k}^{\mathrm{nf}} \leq \left(\frac{SOE_j^{\mathrm{D}} - SOE_{j,k} - \epsilon}{SOE_j^{\max}} \right) + 1 \tag{7}$$

$$\boldsymbol{\theta} : \sum_{j \in \mathcal{J}} b_{i,j,k}^{\mathrm{ch}} \leq 1 \tag{8}$$

$$\boldsymbol{\zeta} : \sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} \leq b_{j,k}^{\mathrm{s}} \tag{9}$$

$$\boldsymbol{\rho} : b_{i,j,k-1}^{\mathrm{ch}} + b_{j,k}^{\mathrm{nf}} - 1 \leq b_{i,j,k}^{\mathrm{ch}} \leq b_{i,j,k-1}^{\mathrm{ch}} + b_{j,k}^{\mathrm{nf}} \tag{10}$$

$$b_{i,j,k}^{\mathrm{ch}}, b_{j,k}^{\mathrm{nf}} \in \{0, 1\}. \tag{11}$$

This MILP optimization problem aims to minimize the objective function in (2), which is the total electricity charging cost calculated using the TOU price C_k and charging power $P_{j,k}$ for all EVs during the prediction horizon h. Equation (3) represents the dynamics of the SOE for EV j at a future time $k+1$ in terms of the SOE at current time k and charging power $P_{j,k}$ with scheduling unit time Δt. Equations (4) and (5) describe the constraints on the SOE with an initial SOE (SOE_j^{I}) when EV j arrives at the EVCS at time k along with the maximum SOE ($SOE_j^{\max}$) and with a desired SOE (SOE_j^{D}) when EV j completes its charging at the end of the prediction horizon, respectively. The EV charging power is limited by the maximum charging power $P_i^{\max}$ at charging pole i with the three different charging levels defined in (6), where $b_{i,j,k}^{\mathrm{ch}}$ represents the binary decision variable that determines the charging status of EV j at charging pole i (''1'' for charging; ''0'' otherwise). Equation (7) states that EV j is not fully charged at time k (i.e., $b_{j,k}^{\mathrm{nf}} = 1$) if $SOE_{j,k}$ is smaller than SOE_j^{D}; otherwise, EV j is fully charged at time k (i.e., $b_{j,k}^{\mathrm{nf}} = 0$). Here, ϵ is a sufficiently small positive number. Equation (8) guarantees that each charging pole i is at most connected to one EV at time k. According to (9), the charging process of EV j at charging pole i can be allowed only when the EV stays at the EVCS (i.e., $b_{j,k}^{\mathrm{s}} = 1$). Equation (10) allows for consecutive or no consecutive charging of the EV at times $k-1$ and k depending on the non-fully charging status $b_{j,k}^{\mathrm{nf}}$, corresponding to i) $b_{i,j,k-1}^{\mathrm{ch}} = b_{i,j,k}^{\mathrm{ch}} = 1$ when $b_{j,k}^{\mathrm{nf}} = 1$ and ii) $b_{i,j,k-1}^{\mathrm{ch}} = b_{i,j,k}^{\mathrm{ch}} = 0$ when $b_{j,k}^{\mathrm{nf}} = 0$, respectively. The binary decision variables are defined in (11).

Finally, the decision variables for the EV charging optimization problem in (2)–(11) are expressed as $[P_{j,k}, SOE_{j,k}, b_{i,j,k}^{\mathrm{ch}}, b_{j,k}^{\mathrm{nf}}]$. Note that $b_{j,k}^{\mathrm{s}}$ is a parameter with a binary value defined as

$$b_{j,k}^{\mathrm{s}} = \begin{cases} 1, & a_j \leq k < d_j \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

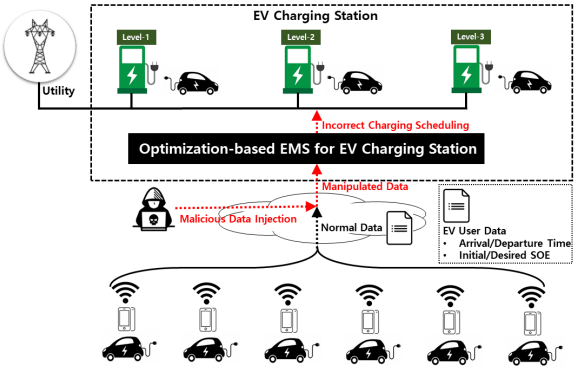

FIGURE 2. Conceptual diagram illustrating a cyber attack on the EMS of an EVCS.

where a_j and d_j denote the arrival and departure times of EV j at the EVCS, respectively. In this study, the charging window T_j^{w} of EV j at the EVCS is defined as $d_j - a_j$ and includes its charging time T_j^{c} (i.e., $T_j^{\mathrm{c}} \subset T_j^{\mathrm{w}}$).

In general, bi-level optimization problems are hard to be solved by the commercial optimization solvers. To resolve this issue, as described in Section III, the proposed bi-level optimization-based attack strategy needs to be transformed into a single-level optimization problem by replacing the lower-level optimization problem (i.e., EV charging optimization problem defined by (2)–(11)) with its KKT conditions. Evidently, the optimal solution of the single-level optimization problem is readily calculated by many available optimization solvers. However, no KKT conditions for the MILP optimization problem exist because the MILP optimization problem is convex no longer. Therefore, the MILP-optimization-based EV charging problem should be converted into a convex linear-programming-based optimization problem by relaxing the binary decision variables in (11) with continuous variables as follows:

$$\boldsymbol{\xi} : 0 \leq b_{i,j,k}^{\mathrm{ch}} \leq 1, \quad \boldsymbol{\nu} : 0 \leq b_{j,k}^{\mathrm{nf}} \leq 1. \tag{13}$$

In the relaxed EV charging optimization problem, all variable vectors ($\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\chi}$, $\boldsymbol{\lambda}$, $\boldsymbol{\theta}$, $\boldsymbol{\zeta}$, $\boldsymbol{\rho}$, $\boldsymbol{\xi}$, and $\boldsymbol{\nu}$) associated with the equality and inequality constraints represent Lagrangian multipliers with non-negative values. The Lagrangian multiplier vector of the inequality constraint having both the upper and lower limits is expressed as the corresponding Lagrangian multiplier subvectors. For example, vector $\boldsymbol{\beta}$ in constraint (4) is decomposed into two subvectors, i.e., $\boldsymbol{\beta} = [\boldsymbol{\beta}^+, \boldsymbol{\beta}^-]$, where $\boldsymbol{\beta}^+$ and $\boldsymbol{\beta}^-$ correspond to the upper and lower limits of the inequality constraint, respectively.

C. PROPOSED ATTACK MODEL AND ASSUMPTIONS

As illustrated in Fig. 2, we consider a scenario in which an adversary stealthily injects malicious data into the EV data (i.e., arrival/depareture times and initial/desired SOE) that are transmitted via a communication network from the EV users' mobile phones to the EMS of the EVCS. In this attack scenario, the EV data manipulated by the adversary are fed

into the EV charging optimization algorithm of the EMS described in Section II-B as input data, thereby leading to changes in its optimal solution (e.g., an increase in the total electricity cost incurred by the EVCS through a distorted EV charging schedule). The primary goal of the proposed attack is to have a detrimental impact on the operation cost of the EVCS.

For a successful attack based on the proposed attack strategy, the adversary needs to satisfy the following assumptions:

- The adversary is capable of breaching a mobile communication network and compromising mobile phones of EV users by monitoring and manipulating their data. As more EV users communicate with the EVCS using their mobile phones via a wireless network, it is evident that the possibility of the attack on such communication will increase.
- The adversary can formulate an EV charging optimization problem and calculate its optimal solution with the knowledge of the EVCS operating conditions, including the number and type of charging poles with different charging speeds and the TOU pricing tariff.

III. MATHEMATICAL FORMULATION OF CYBER ATTACK ON EVCS

In this section, we present an optimization problem that describes an EV user data-induced cyber attack on an EVCS. Section III-A introduces a bi-level optimization attack formulation that comprises upper- and lower-level optimization problems. In the bi-level optimization problem, the upper- and lower-level problems correspond to the adversary and EVCS operator, respectively. In Section III-B, the bi-level optimization attack problem formulated in Section III-A is transformed into an equivalent single-level optimization problem using the KKT conditions of the lower-level optimization problem.

A. BILEVEL OPTIMIZATION MODEL FOR THE PROPOSED EVCS ATTACK

The proposed attack strategy is formulated as the following bi-level MILP optimization problem with multi-objective function and constraints:

■ Upper level

$$\max J^{\mathrm{U}} = \sum_{k\in\mathcal{K}} \left(C_k \sum_{j\in\mathcal{J}} P_{j,k} \right) \Delta t - \omega \sum_{j\in\mathcal{J}} b_j^{\mathrm{a}} \tag{14}$$

$$\text{s.t.} \ -\tau SOE_j^{\mathrm{I}} b_j^{\mathrm{a}} \le \Delta SOE_j^{\mathrm{I}} \le \tau SOE_j^{\mathrm{I}} b_j^{\mathrm{a}} \tag{15}$$

$$-\tau SOE_j^{\mathrm{D}} b_j^{\mathrm{a}} \le \Delta SOE_j^{\mathrm{D}} \le \tau SOE_j^{\mathrm{D}} b_j^{\mathrm{a}} \tag{16}$$

$$\Delta SOE_j^{\mathrm{I}} \le \Delta SOE_j^{\mathrm{D}} \le \min(SOE_j^{\max} - SOE_j^{\mathrm{D}} + \Delta SOE_j^{\mathrm{I}}, SOE_j^{\max} - SOE_j^{\mathrm{D}}) \tag{17}$$

$$0 \le \Delta a_j \le \kappa b_j^{\mathrm{a}} \tag{18}$$

$$-\kappa b_j^{\mathrm{a}} \le \Delta d_j \le 0 \tag{19}$$

$$b_{j,k}^{\mathrm{s,a}} = \begin{cases} 1, & a_j + \Delta a_j \le k < d_j + \Delta d_j \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

■ Lower level

$$\min J^{\mathrm{L}} = \sum_{k\in\mathcal{K}} \left(C_k \sum_{j\in\mathcal{J}} P_{j,k} \right) \Delta t \tag{21}$$

$$\text{s.t.} \ \widetilde{\boldsymbol{\beta}} : SOE_j^{\mathrm{I}} + \Delta SOE_j^{\mathrm{I}} \le SOE_{j,k} \le SOE_j^{\max} \tag{22}$$

$$\widetilde{\boldsymbol{\gamma}} : SOE_j^{\mathrm{D}} + \Delta SOE_j^{\mathrm{D}} \le SOE_{j,t+h} \tag{23}$$

$$\widetilde{\boldsymbol{\lambda}} : \frac{SOE_j^{\mathrm{D}} + \Delta SOE_j^{\mathrm{D}} - SOE_{j,k}}{SOE_j^{\max}} \le b_{j,k}^{\mathrm{nf}} \le \left(\frac{SOE_j^{\mathrm{D}} + \Delta SOE_j^{\mathrm{D}} - SOE_{j,k} - \epsilon}{SOE_j^{\max}} \right) + 1 \tag{24}$$

$$\widetilde{\boldsymbol{\xi}} : \sum_{i\in\mathcal{I}} b_{i,j,k}^{\mathrm{ch}} \le b_{j,k}^{\mathrm{s,a}} \tag{25}$$

$$\text{Eqn. (3), (6), (8), (10), (13).} \tag{26}$$

1) UPPER LEVEL

In the upper level (14)–(20), the adversary calculates four types of malicious data ($\Delta SOE_j^{\mathrm{I}}$, $\Delta SOE_j^{\mathrm{D}}$, Δa_j, and Δd_j) that are injected into the user data of EV j. The malicious data calculated at the upper level are fed into the EV charging optimization problem at the lower level to simultaneously maximize the total electricity cost incurred by the EVCS and minimize the attack effort while maintaining undetectable conditions along with limited attack capability. The first term in the multi-objective function (14) for the proposed attack represents the total electricity charging cost for all EVs, whereas the second term represents the total number of injected malicious data, where b_j^{a} is equal to one when the data for EV j are manipulated; otherwise, b_j^{a} is equal to zero. In the second term of the multi-objective function, ω denotes a penalty for the attack effort. A smaller ω leads to a larger number of $b_j^{\mathrm{a}} = 1$, thereby wasting more attack effort; however, it allows the adversary to further increase the total electricity charging cost.

The magnitudes of the injected malicious SOE data, i.e., $\Delta SOE_j^{\mathrm{I}}$ and $\Delta SOE_j^{\mathrm{D}}$, are limited by the attack limit factor τ in (15) and (16), respectively. Equation (17) ensures that these malicious data are undetected by both the EV user and EVCS operator; it can be derived from the following inequality constraints (27), (28):

$$SOE_j^{\mathrm{D}} \le SOE_j^{\mathrm{D,a}} - SOE_j^{\mathrm{I,a}} + SOE_j^{\mathrm{I}} \tag{27}$$

$$SOE_j^{\mathrm{D,a}} - SOE_j^{\mathrm{I,a}} + SOE_j^{\mathrm{I}} \le SOE_j^{\max} \tag{28}$$

where the manipulated initial and desired SOE data are respectively defined as

$$SOE_j^{\mathrm{I,a}} = SOE_j^{\mathrm{I}} + \Delta SOE_j^{\mathrm{I}} \tag{29}$$

$$SOE_j^{\mathrm{D,a}} = SOE_j^{\mathrm{D}} + \Delta SOE_j^{\mathrm{D}}. \tag{30}$$

Equation (27) guarantees that the manipulation of the SOE data is undetected by the EV user. This is because the sum

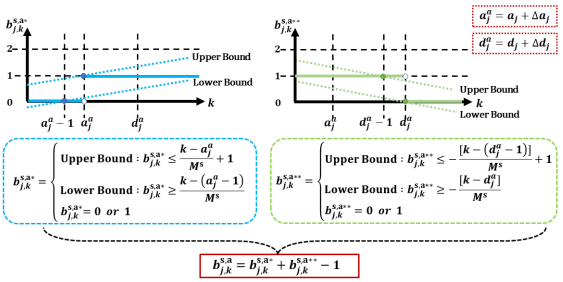

FIGURE 3. Illustration of the derivation of the upper and lower bounds for auxiliary binary variables $b_{j,k}^{\mathrm{s,a}^*}$ and $b_{j,k}^{\mathrm{s,a}^{**}}$.

of the attack-related charging energy ($SOE_j^{\mathrm{D,a}} - SOE_j^{\mathrm{I,a}}$) and the attack-free initial SOE (SOE_j^{I}) is still larger than or equal to the desired SOE level. In addition, the right-hand side of (27) should be limited by $SOE_j^{\max}$, as expressed in (28). This inequality constraint makes the EVCS operator believe that the EV charging optimization algorithm is carried out correctly. Finally, the constraints (27) and (28) along with the additional inequality constraint $SOE_j^{\mathrm{D,a}} \leq SOE_j^{\max}$ become equivalent to the constraint (17).

The magnitudes of the injected malicious data, i.e., Δa_j and Δd_j, are limited by the attack limit factor κ in (18) and (19), respectively, when the attack is initiated with $b_j^{\mathrm{a}} = 1$. Note that Δa_j and Δd_j should be set as non-negative ($\Delta a_j \geq 0$) and non-positive ($\Delta d_j \leq 0$) integers, respectively. This is because, under an attack with $\Delta a_j < 0$ or $\Delta d_j > 0$, the EV charging optimization problem may calculate the charging schedule earlier than a_j or later than d_j; however, the EV actually arrives or departs at a_j or d_j. As a result, this phenomenon allows the EVCS operator to readily detect such abnormal situations. Equation (20) represents the binary status of an EV that stays at the EVCS (i.e., $b_{j,k}^{\mathrm{s,a}} = 1$) between the manipulated arrival ($a_j + \Delta a_j$) and departure ($d_j + \Delta d_j$) times. In contrast to the fact that $b_{j,k}^{\mathrm{s}}$ in (12) without attack is a fixed parameter, $b_{j,k}^{\mathrm{s,a}}$ is a variable that changes with Δa_j and Δd_j. Equation (20) can be relaxed using the following linear equality and two linear inequality constraints with a large positive number M^{s}:

$$b_{j,k}^{\mathrm{s,a}} = b_{j,k}^{\mathrm{s,a}^*} + b_{j,k}^{\mathrm{s,a}^{**}} - 1 \tag{31}$$

$$\frac{k - (a_j + \Delta a_j) + 1}{M^{\mathrm{s}}} \leq b_{j,k}^{\mathrm{s,a}^*} \leq \frac{k - (a_j + \Delta a_j)}{M^{\mathrm{s}}} + 1 \tag{32}$$

$$\frac{d_j + \Delta d_j - k}{M^{\mathrm{s}}} \leq b_{j,k}^{\mathrm{s,a}^{**}} \leq \frac{d_j + \Delta d_j - k - 1}{M^{\mathrm{s}}} + 1. \tag{33}$$

In (31), $b_{j,k}^{\mathrm{s,a}}$ is expressed in terms of two auxiliary binary variables, i.e., $b_{j,k}^{\mathrm{s,a}^*}$ and $b_{j,k}^{\mathrm{s,a}^{**}}$, and they are limited by the manipulated arrival and departure times, respectively, as described in (32) and (33). Fig. 3 illustrates a conceptual diagram that explains how to derive the upper and lower bounds of two auxiliary binary variables.

2) LOWER LEVEL

The lower level (21)–(26) corresponds to the EV charging optimization problem that is introduced in Section II-B. In the lower-level problem, four constraints of the EV charging optimization problem are modified according to (22)–(25), including four types of malicious data ($\Delta SOE_j^{\mathrm{I}}$, $\Delta SOE_j^{\mathrm{D}}$, Δa_j, Δd_j) that are transferred from the upper level.

B. SINGLE-LEVEL OPTIMIZATION MODEL FOR THE PROPOSED EVCS ATTACK

This subsection presents the transformation of the bilevel-MILP-optimization-based attack method, described in the previous subsection, into a single-level optimization problem. A key part of this transformation is that the KKT conditions of the lower-level optimization problem are derived and merged into the upper-level optimization problem as its constraints.

Given the vectors for decision variables $\mathbf{x}$ and data $\mathbf{d}$, an optimization problem with linear equality constraints ($\mathbf{Ax} = \mathbf{d}$) and linear inequality constraints ($\mathbf{Bx} \leq \mathbf{d}$) is expressed as

$$\min_{\mathbf{x}} J(\mathbf{x}, \mathbf{d}) \tag{34}$$

$$\text{s.t. } \boldsymbol{\pi} : \mathbf{Ax} = \mathbf{d}, \tag{35}$$

$$\boldsymbol{\eta} : \mathbf{Bx} \leq \mathbf{d}. \tag{36}$$

Let us denote the Lagrangian function as $\mathcal{L}(\mathbf{x}, \mathbf{d}) = J(\mathbf{x}, \mathbf{d}) - \boldsymbol{\pi}(\mathbf{Ax} - \mathbf{d}) + \boldsymbol{\eta}(\mathbf{Bx} - \mathbf{d})$. Subsequently, the following KKT conditions are derived:

1) First-order optimality conditions: $\nabla_{\mathbf{x}}\mathcal{L}(\mathbf{x}, \mathbf{d}) = \mathbf{0} \Rightarrow \nabla_{\mathbf{x}} J(\mathbf{x}, \mathbf{d}) - \boldsymbol{\pi}\nabla_{\mathbf{x}}(\mathbf{Ax} - \mathbf{d}) + \boldsymbol{\eta}\nabla_{\mathbf{x}}(\mathbf{Bx} - \mathbf{d}) = \mathbf{0}$,
2) Primal feasibility conditions: $\mathbf{Ax} = \mathbf{d}$, $\mathbf{Bx} \leq \mathbf{d}$,
3) Complementary slackness and dual feasibility conditions: $\boldsymbol{\eta}(\mathbf{Bx} - \mathbf{d}) = \mathbf{0}$, $\boldsymbol{\eta} \geq \mathbf{0}$.

Detailed expressions for the KKT conditions of the lower level in the proposed bi-level optimization attack problem are presented in the subsequent subsections.

1) FIRST-ORDER OPTIMALITY CONDITIONS

By differentiating the Lagrangian function of the EV charging optimization problem associated with the lower level, the following first-order optimality conditions are obtained:

$$C_k \Delta t - \alpha_{j,k} \Delta t - \chi_{j,k}^{-} + \chi_{j,k}^{+} = 0, \quad k \in \mathcal{K} \tag{37}$$

$$-\widetilde{\beta}_{j,k}^{-} + \widetilde{\beta}_{j,k}^{+} - \widetilde{\gamma}_j + \alpha_{j,k-1} = 0, \quad k = t + h \tag{38}$$

$$-\widetilde{\beta}_{j,k}^{-} + \widetilde{\beta}_{j,k}^{+} + \alpha_{j,k-1} - \alpha_{j,k} - \widetilde{\lambda}_{j,k}^{-} + \widetilde{\lambda}_{j,k}^{+} = 0, \quad b\, k \in \mathcal{K}\ (k \neq t) \tag{39}$$

$$-\chi_{j,k}^{+} P_i^{\max} + \theta_{i,k} + \widetilde{\xi}_{j,k} - \rho_{i,j,k}^{-} + \rho_{i,j,k}^{+} - \xi_{i,j,k}^{-} + \xi_{i,j,k}^{+}, \quad k = t + h - 1 \tag{40}$$

$$-\chi_{j,k}^{+} P_i^{\max} + \theta_{i,k} + \widetilde{\xi}_{j,k} - \rho_{i,j,k}^{-} + \rho_{i,j,k+1}^{-} + \rho_{i,j,k}^{+} - \rho_{i,j,k+1}^{+} - \xi_{i,j,k}^{-} + \xi_{i,j,k}^{+} = 0, \quad k \in \mathcal{K}\ (k \neq t + h - 1) \tag{41}$$

$$-\widetilde{\lambda}_{j,k}^{-} SOE_j^{\max} + \widetilde{\lambda}_{j,k}^{+} SOE_j^{\max} + \rho_{i,j,k}^{-} - \rho_{i,j,k}^{+} - \nu_{j,k}^{-} + \nu_{j,k}^{+} = 0, \quad k \in \mathcal{K}. \tag{42}$$

2) PRIMAL FEASIBILITY CONDITIONS

The primal feasibility conditions include all equality and inequality constraints of the lower-level problem:

$$\text{Eqn. (22)} - \text{(26)}. \tag{43}$$

3) COMPLEMENTARY SLACKNESS CONDITIONS

The complementary slackness conditions are expressed in the multiplication form of the inequality constraints and their corresponding Lagrangian multipliers.

$$\widetilde{\beta}_{j,k}^{-} \left(-SOE_{j,k} + \Delta SOE_j^{\mathrm{I}} + SOE_j^{\mathrm{I}}\right) + \widetilde{\beta}_{j,k}^{+} \left(SOE_{j,k} - SOE_j^{\max}\right) = 0 \tag{44}$$

$$\widetilde{\gamma}_j \left(\Delta SOE_j^{\mathrm{D}} - SOE_{j,t+h} + SOE_j^{\mathrm{D}}\right) = 0 \tag{45}$$

$$-\chi_{j,k}^{-} P_{j,k} + \chi_{j,k}^{+} \left(P_{j,k} - \sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} P_i^{\max}\right) = 0 \tag{46}$$

$$\widetilde{\lambda}_{j,k}^{-} \left(-b_{j,k}^{\mathrm{nf}} SOE_j^{\max} + \Delta SOE_j^{\mathrm{D}} - SOE_{j,k} + SOE_j^{\mathrm{D}}\right) \widetilde{\lambda}_{j,k}^{+} \left(b_{j,k}^{\mathrm{nf}} SOE_j^{\max} - \Delta SOE_j^{\mathrm{D}} + SOE_{j,k} - SOE_j^{\max} + \epsilon - SOE_j^{\mathrm{D}}\right) = 0 \tag{47}$$

$$\theta_{i,k} \left(\sum_{j \in \mathcal{J}} b_{i,j,k}^{\mathrm{ch}} - 1\right) = 0 \tag{48}$$

$$\widetilde{\zeta}_{j,k} \left(\sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} - b_{j,k}^{\mathrm{s,a}}\right) = 0 \tag{49}$$

$$\rho_{i,j,k}^{-} \left(b_{i,j,k-1}^{\mathrm{ch}} + b_{j,k}^{\mathrm{nf}} - b_{i,j,k}^{\mathrm{ch}} - 1\right) + \rho_{i,j,k}^{+} \left(-b_{i,j,k-1}^{\mathrm{ch}} - b_{j,k}^{\mathrm{nf}} + b_{i,j,k}^{\mathrm{ch}}\right) = 0. \tag{50}$$

In addition, the nonlinear complementary slackness conditions derived above are linearized using the big-M method with additional auxiliary binary decision variables ($\delta_{j,k}^{\widetilde{\beta}^-}$, $\delta_{j,k}^{\widetilde{\beta}^+}$ $\delta_j^{\widetilde{\gamma}}$, $\delta_{j,k}^{\chi^-}$, $\delta_{j,k}^{\chi^+}$, $\delta_{j,k}^{\widetilde{\lambda}^-}$, $\delta_{j,k}^{\widetilde{\lambda}^+}$, $\delta_{j,k}^{\theta}$, $\delta_{j,k}^{\widetilde{\zeta}}$, $\delta_{i,j,k}^{\rho^-}$ and $\delta_{i,j,k}^{\rho^+}$) and a large positive constant M^{c} as follows:

$$\begin{cases} \widetilde{\beta}_{j,k}^{-} - M^{\mathrm{c}} \delta_{j,k}^{\widetilde{\beta}^-} \le 0 \\ SOE_{j,k} - \Delta SOE_j^{\mathrm{I}} - SOE_j^{\mathrm{I}} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\widetilde{\beta}^-}) \\ \widetilde{\beta}_{j,k}^{+} - M^{\mathrm{c}} \delta_{j,k}^{\widetilde{\beta}^+} \le 0 \\ SOE_j^{\max} - SOE_{j,k} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\widetilde{\beta}^+}) \\ \delta_{j,k}^{\widetilde{\beta}^-} + \delta_{j,k}^{\widetilde{\beta}^+} \le 1 \end{cases} \tag{51}$$

$$\begin{cases} \widetilde{\gamma}_j - M^{\mathrm{c}} \delta_j^{\widetilde{\gamma}} \le 0 \\ SOE_{j,t+h} - \Delta SOE_j^{\mathrm{D}} - SOE_j^{\mathrm{D}} \le M^{\mathrm{c}} (1 - \delta_j^{\widetilde{\gamma}}) \end{cases} \tag{52}$$

$$\begin{cases} \chi_{j,k}^{-} - M^{\mathrm{c}} \delta_{j,k}^{\chi^-} \le 0 \\ P_{j,k} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\chi^-}) \\ \chi_{j,k}^{+} - M^{\mathrm{c}} \delta_{j,k}^{\chi^+} \le 0 \\ P_{j,k} - \sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} P_i^{\max} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\chi^+}) \\ \delta_{j,k}^{\chi^-} + \delta_{j,k}^{\chi^+} \le 1 \end{cases} \tag{53}$$

$$\begin{cases} \widetilde{\lambda}_{j,k}^{-} - M^{\mathrm{c}} \delta_{j,k}^{\widetilde{\lambda}^-} \le 0 \\ b_{j,k}^{\mathrm{nf}} SOE_j^{\max} - \Delta SOE_j^{\mathrm{D}} + SOE_{j,k} - SOE_j^{\mathrm{D}} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\widetilde{\lambda}^-}) \\ \widetilde{\lambda}_{j,k}^{+} - M^{\mathrm{c}} \delta_{j,k}^{\widetilde{\lambda}^+} \le 0 \\ -b_{j,k}^{\mathrm{nf}} SOE_j^{\max} + \Delta SOE_j^{\mathrm{D}} - SOE_{j,k} + SOE_j^{\max} - \epsilon + SOE_j^{\mathrm{D}} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\widetilde{\lambda}^+}) \\ \delta_{j,k}^{\widetilde{\lambda}^-} + \delta_{j,k}^{\widetilde{\lambda}^+} \le 1 \end{cases} \tag{54}$$

$$\begin{cases} \theta_{j,k} - M^{\mathrm{c}} \delta_{j,k}^{\theta} \le 0 \\ 1 - \sum_{j \in \mathcal{J}} b_{i,j,k}^{\mathrm{ch}} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\theta}) \end{cases} \tag{55}$$

$$\begin{cases} \widetilde{\zeta}_{j,k} - M^{\mathrm{c}} \delta_{j,k}^{\widetilde{\zeta}} \le 0 \\ b_{j,k}^{\mathrm{s,a}} - \sum_{i \in \mathcal{I}} b_{i,j,k}^{\mathrm{ch}} \le M^{\mathrm{c}} (1 - \delta_{j,k}^{\widetilde{\zeta}}) \end{cases} \tag{56}$$

$$\begin{cases} \rho_{i,j,k}^{-} - M^{\mathrm{c}} \delta_{i,j,k}^{\rho^-} \le 0 \\ -b_{i,j,k-1}^{\mathrm{ch}} - b_{j,k}^{\mathrm{nf}} + b_{i,j,k}^{\mathrm{ch}} + 1 \le M^{\mathrm{c}} (1 - \delta_{i,j,k}^{\rho^-}) \\ \rho_{i,j,k}^{+} - M^{\mathrm{c}} \delta_{i,j,k}^{\rho^+} \le 0 \\ b_{i,j,k-1}^{\mathrm{ch}} + b_{j,k}^{\mathrm{nf}} - b_{i,j,k}^{\mathrm{ch}} \le M^{\mathrm{c}} (1 - \delta_{i,j,k}^{\rho^+}) \\ \delta_{i,j,k}^{\rho^-} + \delta_{i,j,k}^{\rho^+} \le 1. \end{cases} \tag{57}$$

4) DUAL FEASIBILITY CONDITIONS

The dual feasibility conditions represent the following Lagrangian multipliers with non-negative values:

$$\left[\boldsymbol{\alpha}; \widetilde{\boldsymbol{\beta}}; \widetilde{\boldsymbol{\gamma}}; \boldsymbol{\chi}; \widetilde{\boldsymbol{\lambda}}; \boldsymbol{\theta}; \widetilde{\boldsymbol{\zeta}}; \boldsymbol{\rho}; \boldsymbol{\xi}; \boldsymbol{\nu}\right] \ge 0. \tag{58}$$

Finally, using the aforementioned KKT conditions, the proposed bi-level attack optimization problem can be reformulated in terms of the following single-level optimization problem:

■ Single-level attack optimization problem

$$\max J = \sum_{k\in\mathcal{K}} \left(C_k \sum_{j\in\mathcal{J}} P_{j,k} \right) \Delta t - \omega \sum_{j\in\mathcal{J}} b_j^{\mathrm{a}} \quad (59)$$

$$\text{s.t. Eqn. } (15)-(19),\ (31)-(33) \quad (60)$$

$$\text{Eqn. } (37)-(43),$$

$$(51)-(58) \text{ (KKT conditions).} \quad (61)$$

IV. NUMERICAL EXAMPLES

A. SIMULATION SETUP

We set up a simulation environment in which 40 EVs with different charging information and preferences communicate with the EMS of an EVCS before they arrive at the EVCS. Upon arrival, the EVs charge power via the charging poles of the EVCS according to the charging schedule calculated by the EMS. The arrival/departure times of each EV were randomly distributed based on a discrete uniform distribution during one day. The EVCS was assumed to be equipped with six charging poles, three pairs of which correspond to different maximum charging power capacities as follows: $P_i^{\max} = 50$ kW for $i = 1, 2 \in \mathcal{I}^{(1)}$ (Level 1), $P_i^{\max} = 100$ kW for $i = 3, 4 \in \mathcal{I}^{(2)}$ (Level 2), and $P_i^{\max} = 200$ kW for $i = 5, 6 \in \mathcal{I}^{(3)}$ (Level 3). As illustrated in Fig. 4, under TOU tariff, the EV charging optimization algorithm in the EMS calculates the optimal charging schedules of EVs by minimizing their electricity charging cost. For simplicity, the preferred charging window ($T_j^{\mathrm{w}} = d_j - a_j$) and maximum/initial/desired SOE ($SOE_j^{\max}/SOE_j^{\mathrm{I}}/SOE_j^{\mathrm{D}}$) for each EV j were identically set as $T_j^{\mathrm{w}} = 2.5$ h, $SOE_j^{\max} = 72.6$ kWh, $SOE_j^{\mathrm{I}} = 0.2 \times SOE_j^{\max}$ kWh, and $SOE_j^{\mathrm{D}} = 0.9 \times SOE_j^{\max}$ kWh. In the upper level of the bi-level optimization attack problem, the penalty (ω) for the attack effort, the attack limit factor (τ) of the SOE, and the attack limit factor (κ) of arrival/departure times were set to 0.1, 0.2, and 3, respectively. In the lower level of the bi-level optimization attack problem, the value of ϵ associated with a non-fully charging status of the EV was set to 10^{-7}. The values of M^{s} and M^{c} associated with the EV stay and relaxation of the complementary slackness condition were identically set to 10^6. The simulation was conducted for 24 h with a 15-min scheduling resolution (i.e., $\Delta t = 15$ min) and a predicted horizon $h = 16$ (i.e., 4 h). The proposed attack strategy was simulated in a computer (AMD Rygen 7 2700X Eight-Core Processor clocking at 3.7 GHz and 32 GB of RAM) using the IBM ILOG CPLEX Optimization Studio 12.8 solver through MATLAB R2018b.

B. ATTACK RESULTS OF ELECTRICITY COST OF EVCS AND CHARGING ENERGY OF EV

In this subsection, we present a quantification of the impact of the proposed EVCS attack on the total electricity cost and the amount of charging energy scheduled by the EMS of the EVCS. Fig. 5 illustrates two cumulative electricity costs incurred by the EVCS without and with attack over the entire charging scheduling period. Note from this figure that

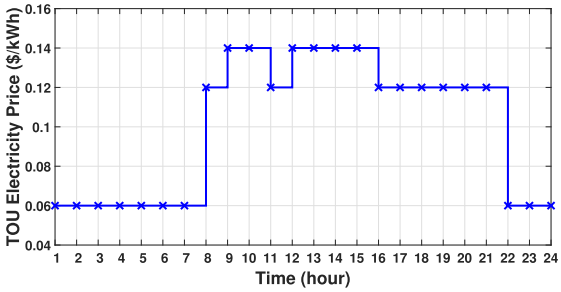

FIGURE 4. Profile of TOU price.

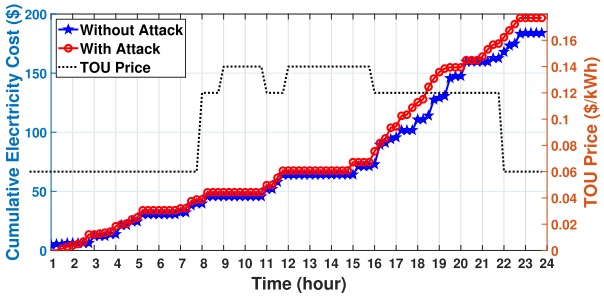

FIGURE 5. Comparison results of the cumulative electricity costs suffered by the EVCS without and with attack during one day.

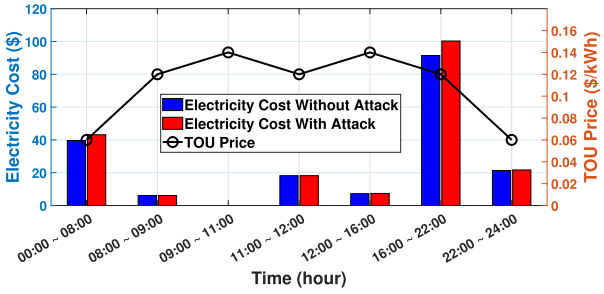

FIGURE 6. Comparison results of the cumulative electricity costs of EVCS in seven different TOU-price time blocks without and with attack.

the cumulative electricity cost with attack becomes higher than that without attack after the scheduling period 02:30. Eventually, the total electricity costs without and with attack reach 183.98 $ and 196.73 $ at the end of the scheduling period, respectively. Thus, we can conclude that the proposed attack method can successfully increase the electricity cost for the EVCS by stealthily injecting malicious data into the EV user data.

Fig. 6 compares the cumulative electricity costs for the EVCS without and with attack in seven different TOU-price time blocks. Each of these time blocks has an identical price, as indicated in Fig. 4. Note from this figure that a significantly increasing electricity cost due to the attack can be identified at two TOU-price time blocks, namely ($00:00 \sim 08:00$) and ($16:00 \sim 22:00$). This result derives from the following two characteristics of the adversary using the proposed attack strategy:

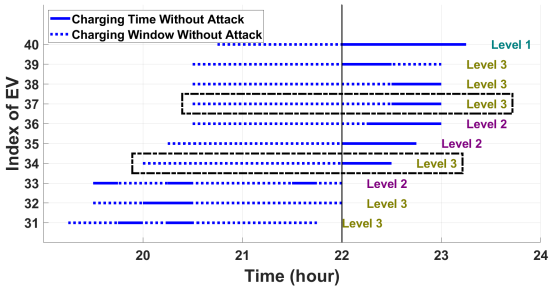

FIGURE 7. Charging windows (T_j^{w}) and charging times (T_j^{c}) from EV31 to EV40 around the scheduling period 22:00 without attack.

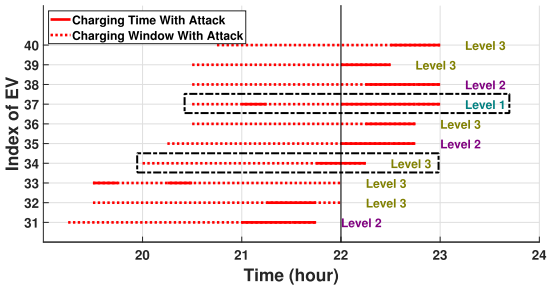

FIGURE 8. Charging windows (T_j^{w}) and charging times (T_j^{c}) from EV31 to EV40 around the scheduling period 22:00 with attack.

(C1) **Unbinding SOE constraint attack:** The adversary increases the amount of EV charging energy to a level greater than its original initial/desired SOE level, thereby generating the unbinding SOE constraint. Here, the unbinding SOE constraint implies that $SOE_{j,k}$ and $SOE_{j,t+h}$ do not hit their original lower limits (SOE_j^{I} and SOE_j^{D}) in the constraints (22) and (23).

(C2) **Time shiftable attack:** The adversary moves the EV charging schedule to a higher TOU-price time block, thereby leading to an increase in the electricity cost incurred by the EVCS.

An increasing electricity cost in the time period (00 : 00 ∼ 08 : 00) due to the attack derives from attack (C1), which increases the amount of EV charging energy from 660.66 kWh to 718.74 kWh. In this time period, the TOU price is identical. Thus, attack (C2) has no impact on the electricity cost incurred by the EVCS. By contrast, the time period (16 : 00 ∼ 22 : 00) includes two different TOU prices: 0.12 $/kWh at (16 : 00 ∼ 21 : 00) and 0.05 $/kWh at 22 : 00. As depicted in Fig. 6, an increase in the electricity cost due to the attack is much higher in the time period (16 : 00 ∼ 22 : 00) than in the time period (00 : 00 ∼ 08 : 00). This is because both attacks (C1) and (C2) occur in the time period (16 : 00 ∼ 22 : 00), whereas only attack (C1) occurs in the time period (00 : 00 ∼ 08 : 00). Specifically, such attack consequence in the time period (16 : 00 ∼ 22 : 00) results from the following two attack characteristics: i) for attack (C1), the amount of charging energy increases from 203.28 kWh to 226.70 kWh, and ii) for attack (C2), the charging schedules for three EVs (EV20, EV34, and EV37) are shifted to higher TOU-price time blocks as follows: from (16 : 00 ∼ 16 : 30) to (15 : 45 ∼ 16 : 15) for EV20, from (22 : 00 ∼ 22 : 30) to (21 : 45 ∼ 22 : 15) for EV34, and from (22 : 30 ∼ 23 : 00) to (21 : 00 ∼ 21 : 15) and (22 : 00 ∼ 23 : 00) for EV37.

Figs. 7 and 8 depict the charging windows (T_j^{w}) and charging times (T_j^{c}) around 22 : 00 along with the assigned charging poles for EV31∼EV40 without and with attack, respectively. Note in these figures that the scheduling time 22 : 00 is a boundary between a high TOU price (before 22 : 00) and a low TOU price (after 22 : 00). We first verify from a comparison of Figs. 7 and 8 that T_{34}^{w} for EV34 shrinks with the reduced departure time of EV34 owing to the attack. In the shrunken charging window, the charging schedule of EV34 is shifted from a low TOU-price time period to a high one without changing the charging pole and charging duration. By contrast, no manipulation of T_{37}^{w} for EV37 is conducted by the adversary as illustrated in Figs. 7 and 8. However, T_{37}^{c} for EV37 becomes longer and includes a high TOU-price time period. This phenomenon stems from the fact that T_{40}^{w} for EV40 shrinks by the adversary, which requires a faster charging pole to maintain the desired SOE level of EV40. Consequently, Level-1 and Level-3 charging poles allocated for EV40 and EV37 prior to the attack are switched with each other by the adversary to provide EV40 with a satisfactory charging service. Evidently, EV37 spends a longer charging time via the slower Level-1 charging pole.

TABLE 1. Results with varying penalties (ω) of the attack effort and attack limit factors (τ) of the initial and desired SOE data.

ω	0.1	0.3	0.5
Total electricity cost ($)	196.73	193.25	183.98
Total charging energy (kWh)	2170.7	2112.7	2032.8
No. of the attacked EVs	40	28	0
τ	0.1	0.2	0.3
Total electricity cost ($)	188.89	196.73	200.73
Total charging energy (kWh)	2076.4	2170.7	2214.3
No. of the attacked EVs	28	40	40

C. IMPACT OF PARAMETERS IN THE UPPER-LEVEL PROBLEM ON THE EVCS ATTACK

In this subsection, we present an assessment of the attack performance subject to the parameters associated with the attack capability of the adversary in the upper-level problem. Table 1 lists the results of the attack performance with different attack effort penalties (ω) and attack limit factors (τ) of the initial and desired SOE data in terms of the total electricity cost/charging energy and the number of attacked EVs. As expected, the results in this table indicate that a smaller ω leads to a larger total electricity cost and charging energy at the expense of the attack effort with an increasing number of attacked EVs. Another observation is that for an attack with $\omega = 0.3$, the adversary manipulates data of 28 EVs out of 40 EVs, whereas no attack occurs on 12 EVs

(EVs1∼12). The reason for this fact can be explained as follows. In the simulation setup, the charging windows of EVs1∼10 belonged to the cheapest TOU-price time block, i.e., (00 : 00 ∼ 08 : 00), prior to the attack. Because their charging windows only shrink within the cheapest price time block due to the attack, no time-shiftable attack (C2), described in Section IV-B, was initiated to increase the total electricity cost for the EVCS. In addition, the charging windows of EV11 and EV12 prior to the attack were identically set to (05 : 45 ∼ 08 : 15), which includes two different TOU prices. Even if the adversary obtains a room (i.e., time interval with higher TOU price) to initiate a time-shiftable attack, the attack room (08 : 00 ∼ 08 : 15) for EV11 and EV12 will be smaller than that for the other EVs (e.g., (20 : 00 ∼ 21 : 45) for EV34 and EV37). Furthermore, given that most of the charging windows for EVs1∼12 correspond to the cheapest TOU-price time block, the impact of the unbinding SOE constraint attack (C1) defined in Section IV-B is not very significant.

Note also from Table 1 that a larger τ results in a larger total electricity cost and charging energy along with an increasing number of attacked EVs. This observation is natural because more manipulation of the initial/desired SOE data owing to larger τ leads to more charging of EVs, thereby increasing the total electricity cost for the EVCS. In addition, Table 1 indicates that the number of attacked EVs with $\tau = 0.1$ is smaller than that with $\tau = 0.2$ and $\tau = 0.3$. Our simulation results demonstrate that the adversary with $\tau = 0.1$ performs no attack on EVs1∼12, which is consistent with the result when $\omega = 0.3$. This observation implies that the adversary with insufficiently manipulated SOE data fails to completely conduct the unbinding SOE constraint attack (C1) and time-shiftable attack (C2).

D. IMPACT OF PARAMETERS IN THE LOWER-LEVEL PROBLEM ON THE EVCS ATTACK

In this subsection, we present an investigation of the attack performance subject to the parameters in the EV charging optimization problem associated with the lower-level problem. Fig. 9 illustrates the results of the total electricity cost and charging energy under different initial and desired SOE conditions without and with attack. In this figure, the x-axis corresponds to five pairs of $(a^{\mathrm{D}}, a^{\mathrm{I}})$ that represent multiplicative coefficients for the calculation of the desired and initial SOEs, respectively. Using these multiplicative coefficients, SOE_j^{D} and SOE_j^{I} are computed as $SOE_j^{\mathrm{D}} = a^{\mathrm{D}} \times SOE_j^{\max}$ and $SOE_j^{\mathrm{I}} = a^{\mathrm{I}} \times SOE_j^{\max}$. According to the gap between SOE_j^{D} and SOE_j^{I}, five labels along the x-axis are categorized into three groups each of which takes an identical value of $a^{\mathrm{D}} - a^{\mathrm{I}}$ as follows: $(a^{\mathrm{D}}, a^{\mathrm{I}}) = (0.9, 0.25), (0.85, 0.2)$ for Group I, $(a^{\mathrm{D}}, a^{\mathrm{I}}) = (0.9, 0.2)$ for Group II, and $(a^{\mathrm{D}}, a^{\mathrm{I}}) = (0.95, 0.2), (0.9, 0.15)$ for Group III.

First, note from Fig. 9 that the total electricity cost and charging energy increase significantly because of the attack for the five different pairs of initial and desired SOEs. Note also that as the gap between SOE_j^{D} and SOE_j^{I} increases, the total electricity cost and charging energy for both scenarios without and with attack increase; the three groups can be ranked in the decreasing order of total electricity cost and charging energy as follows: Group III > Group II > Group I. Additionally, for Groups I and III without attack, no change in the total electricity cost and charging energy occurs even if the values of a^{I} and a^{D} vary. This is because the gap between SOE_j^{D} and SOE_j^{I} for each Group I and III is identical. However, as illustrated in the attack results for Groups I and III in Fig. 9, a change in the total electricity cost and charging energy takes place due to the attack even if the identical gap between SOE_j^{D} and SOE_j^{I} is maintained with varying a^{I} and a^{D}.

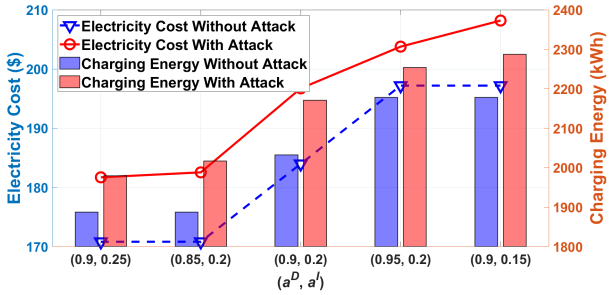

FIGURE 9. Comparison results of the total electricity cost and charging energy under different initial and desired SOE conditions without and with attack.

TABLE 2. Results with varying prediction horizons (h) in the EV charging optimization model.

Prediction horizon (h)	14	16	18
Difference of the total electricity cost between with and without attack ($)	11.96	12.75	14.30
Avg. of computation time of the attack method (min)	3.75	8.15	12.30

Table 2 presents the gap between the total electricity cost for with and without attack scenarios along with the average computation time of the proposed bilevel attack optimization method in terms of prediction horizon h for the EV charging optimization problem. Note from this table that the electricity cost gap due to the attack increases with increasing h. This is because the adversary can obtain more attack room to manipulate the EV user data in a longer prediction horizon. In addition, as expected, Table 2 indicates that the average computation time for the proposed bilevel attack optimization problem during the entire scheduling periods increases as the value of h increases. From the perspective of computational complexity, the proposed attack method is feasible because its computation time presents a scheduling resolution of below 15 min for the EV charging optimization problem.

Lastly, our proposed bi-level attack optimization problem is limited to provide suboptimal solutions due to the following two aspects i) the utilization of the KKT conditions of the

relaxed MILP problem at the lower level and ii) non-optimal selection of the value of M in the big-M method as reported in [23], [24]. An important extension of our work here would be to develop a more optimal attack strategy that addresses the aforementioned limitations, and it is referred to as a future work.

The main observations from the simulation analysis can be summarized as follows:

- The proposed attack successfully increases the total electricity cost for the EVCS while stealthily bypassing the EVCS operator and EV users under undetectable conditions of SOE data manipulation.
- An increase in the total electricity cost for the EVCS due to the proposed attack derives from two types of attack characteristics: i) unbinding SOE constraint attack and ii) time-shiftable attack.
- An unbinding SOE constraint attack increases the amount of EV charging energy, whereas a time-shiftable attack shifts the EV charging time period to a higher TOU-price time period; therefore, both attacks increase the total electricity cost incurred by the EVCS.
- The increase in the attack effort and attack limit factor results in less and more electricity cost suffered by the EVCS, respectively.
- The proposed attack leads to higher electricity costs for the EVCS as the gap between the desired SOE and initial SOE becomes larger prior to the attack.
- The EV charging optimization problem with a larger value of the prediction horizon is more susceptible to the proposed attack and requires more computation time to solve the proposed bilevel attack optimization problem.

V. CONCLUSION

In this study, we considered a situation in which EVCS purchases power from the distribution grid under the TOU pricing tariff sent by DSO and supplies it to EVs connected to the EVCS. In this situation, we proposed a cyber attack on EVCS, which increases the total electricity cost incurred by the EVCS by causing a malfunction in the EV charging optimization algorithm through the manipulation of EV user data (arrival/departure times and initial/desired SOE of EVs at the EVCS) transmitted from the EVs to the EVCS. We formulated such a cyber attack in terms of a bi-level optimization problem comprising upper- and lower-level problems. In the upper-level problem, malicious data injected into the EV user data are calculated to simultaneously maximize the total electricity cost for the EVCS and minimize the attack effort. In the lower-level problem, the EV charging optimization algorithm yields the distorted charging schedules of EVs using manipulated EV user data delivered from the upper level. Subsequently, we transformed the bi-level attack optimization problem into a single-level optimization problem by replacing the lower-level problem with its KKT conditions. Simulation results indicate the feasibility and detrimental impact of the proposed attack strategy on the EVCS operation in terms of the total electricity cost of EVCS, the charging schedule and initial/desired SOE of EVs, attack effort, and computation time of the proposed attack strategy.

In the future, we plan to present a new cyber attack on multiple EVCSs located in a realistic power distribution system. Vulnerability assessment of both EVCS and power distribution system operations for such a cyber attack will be conducted in terms of the real and reactive charging powers of EVs as well as the nodal voltage magnitude along the distribution feeder.

REFERENCES

[1] M. Boucher, "Transportation electrification and managing traffic congestion: The role of intelligent transportation systems," *IEEE Electrific. Mag.*, vol. 7, no. 3, pp. 16–22, Sep. 2019.
[2] H. Farzin, M. Moeini-Aghtaie, and M. Fotuhi-Firuzabad, "Reliability studies of distribution systems integrated with electric vehicles under battery-exchange mode," *IEEE Trans. Power Del.*, vol. 31, no. 6, pp. 2473–2482, Dec. 2016.
[3] Z. Yang, X. Huang, T. Gao, Y. Liu, and S. Gao, "Real-time energy management strategy for parking lot considering maximum penetration of electric vehicles," *IEEE Access*, vol. 10, pp. 5281–5291, 2022.
[4] C. Diaz-Londono, L. Colangelo, F. Ruiz, D. Patino, C. Novara, and G. Chicco, "Optimal strategy to exploit the flexibility of an electric vehicle charging station," *Energies*, vol. 12, no. 3834, pp. 1–29, Oct. 2019.
[5] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *Proc. IEEE Green Technol. Conference(GreenTech)*, Apr. 2019, pp. 1–5.
[6] 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," in *Proc. IEEE Transp. Electrific. Conf. Expo. (ITEC)*, Jun. 2019, pp. 1–4.
[7] N. Bhusal, M. Gautam, and M. Benidris, "Cybersecurity of electric vehicle smart charging management systems," in *Proc. 52nd North Amer. Power Symp. (NAPS)*, Apr. 2021, pp. 1–6.
[8] B. Wang, P. Dehghanian, S. Wang, and M. Mitolo, "Electrical safety considerations in large-scale electric vehicle charging stations," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6603–6612, Nov. 2019.
[9] I. Nedyalkov and D. Arnaudov, "Attacks and security measures of the exchanged information in the charging infrastructure for electromobiles," in *Proc. IEEE 28th Int. Sci. Conf. Electron. (ET)*, Sep. 2019, pp. 1–4.
[10] 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, Nov. 2020.
[11] S. Rahman, H. Aburub, Y. Mekonnen, and A. I. Sarwat, "A study of EV BMS cyber security based on neural network SOC prediction," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Apr. 2018, pp. 1–5.
[12] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–5.
[13] A. Chandwani, S. Dey, and A. Mallik, "Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and countermeasures," *IEEE Access*, vol. 8, pp. 226982–226998, 2020.
[14] S. Saadat, S. Maingot, and S. Bahizad, "Electric vehicle charging station security enhancement measures," in *Proc. 5th IEEE Workshop Electron. Grid (eGRID)*, Nov. 2020, pp. 1–8.
[15] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A detailed security assessment of the EV charging ecosystem," *IEEE Netw.*, vol. 34, no. 3, pp. 27–200, May/Jun. 2020.
[16] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, "Electric vehicle attack impact on power grid operation," *Int. J. Electr. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107784.
[17] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.
[18] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 3, pp. 2010–2022, Sep. 2021.
[19] M. Basnet and M. Hasan Ali, "Deep learning-based intrusion detection system for electric vehicle charging station," in *Proc. 2nd Int. Conf. Smart Power Internet Energy Syst. (SPIES)*, Sep. 2020, pp. 408–413.

[20] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, Nov. 2018.
[21] D. T. Hoang, P. Wang, D. Niyato, and E. Hossain, "Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model," *IEEE Access*, vol. 5, pp. 732–754, 2017.
[22] 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, Sep. 2021.
[23] S. Pineda and J. M. Morales, "Solving linear bilevel problems using big-ms: Not all that glitters is gold," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2469–2471, May 2019.
[24] T. Kleinert, M. Labbé, F. Plein, and M. Schmidt, "Technical note—There's no free lunch: On the hardness of choosing a correct big-M in bilevel optimization," *Oper. Res.*, vol. 68, no. 6, pp. 1716–1721, Nov. 2020.

SEONG ILE JEONG (Student Member, IEEE) received the B.S. degree in electrical and electronics engineering from Chung-Ang University, Seoul, South Korea, in 2021, where he is currently pursuing the M.Sc. degree. His research interests include cyber security of smart grid and optimization methods for electric vehicle charging scheduling.

DAE-HYUN CHOI (Member, IEEE) received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2002, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from Texas A&M University, College Station, TX, USA, in 2008 and 2014, respectively. From 2002 to 2006, he was a Researcher at Korea Telecom (KT), Seoul, where he worked on designing and implementing home network systems. From 2014 to 2015, he was a Senior Researcher at LG Electronics, Seoul, where he developed home energy management systems. He is currently an Assistant Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul. His research interests include power system state estimation, electricity markets, cyber-physical security of smart grids, and theory and application of cyber-physical energy systems. He received the Best Paper Award from the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan.