

基于用户数据的电动汽车充电桩网络攻击模型

叶超[†], 曹宁

(重庆应用技术职业学院, 重庆 401520)

摘 要: 电动汽车(electrical vehicle, EV)的用户数据是优化 EV 充电成本的关键数据, 对用户数据的操纵可能导致错误的充电成本, 使充电桩运营商蒙受经济损失。针对 EV 充电桩, 提出了一种基于用户数据的网络攻击模型, 该模型通过篡改接入 EV 充电桩的用户数据生成虚假的充电计划, 从而提高充电桩的充电成本。所提出的攻击模型为一种基于混合整数线性规划的两层优化模型, 在上层生成注入 EV 充电桩的恶意用户数据, 下层为 EV 充电计划优化算法, 通过应用 KKT 条件使两层优化模型转化为单层优化攻击模型。仿真以一个虚拟充电站场景为例, 相较于无攻击情况, 该攻击模型通过提高 EV 的充电能量或移动 EV 的充电时段增加了充电站的总充电成本, 验证了该攻击模型的可行性和危害性。

关键词: 电动汽车; 充电桩; 网络攻击; 用户数据; 两层优化模型

中图分类号: TM93

文献标识码: A

Cyber Attack Model of EV Charging Pile Based on User Data

YE Chao[†], CAO Ning

(Chongqing Vocational College of Applied Technology, Chongqing 401520, China)

Abstract: The user data of electric vehicle (EV) is the key data to optimize the EV charging cost. Manipulation with the user data may lead to incorrect charging costs and cause economic losses to the charging pile operator. For EV charging pile, a cyber attack model based on user data is proposed. This model generates a incorrect charging plan by tampering with the user data connected to EV charging pile, thus increasing the charging cost. The proposed attack model is a two-stage optimization model based on mixed integer linear programming, which generates malicious user data injected into EV charging piles on the upper level and EV charging plan optimization algorithm on the lower level. By applying KKT conditions, the two-stage optimization model is transformed into a single-level optimization attack model. The simulation takes a virtual charging station scenario as an example. Compared with the non attack scenario, the attack model increases the total charging cost of the charging station by increasing the charging energy of the EV or the charging period of the mobile EV, which verifies the feasibility and harmfulness of the attack model.

Key words: electric vehicle; charging pile; cyber attack; user data; two-stage optimization

对于 EV 充电桩的运营商来说, EV 的充电时段和充电时长关乎自身的运营收益。为了将自身的收益最大化, 需要对 EV 的充电计划进行管理, 以最大限度降低 EV 的充电成本, 同时最大限度满足用户的充电习惯^[1-2]。能源管理系统 (energy management system, EMS) 是运营商实现 EV 充电桩与 EV 间最优充电规划的调度系统。通常来说, EMS 以 EV 用户的充电习惯为基础, 通过采用优化算法, 将从电网购买电能时产生的成本最小化, 从而计算得到 EV 的最优充电计划。

EV 与充电桩的 EMS 之间的通信网络可能容易受到潜在的网络攻击, 攻击者可以穿透无线网络将恶意数据注入 EV 用户数据中。因此, 被篡改的 EV 用户数据可能导致 EMS 中充电计划优化错误, 从而导致 EV 充电的总电力成本提高。

许多文献已经研究了各种类型的网络攻击模型, 并提出了检测和防范相应攻击的方法。文献[3-5]分别建立了对 EV 充电桩的窃听攻击、中间人攻击和拒绝服务攻击的网络攻击模型, 并针对这些攻击进行了风险评估; 文献[6]针对大型 EV 充电桩开发了一个评估框架, 以评估充电桩与电网间通信安全的脆弱性; 文献[7]对操纵 EV 充放电的网络攻击进行了研究, 证实了对 EV 攻击的不利影响大于对居民用电的攻击。文献[8]提出了一种基于混合整数线性规划的优化模型, 通过隔离已经被侵入的充电桩, 将攻击传播的风险降至最低; 文献[9]提出了一种基于网络安全保险的攻击防范方法, 其将 EV 充电桩收到的网络攻击通过网络保险的方式转移到第三方, 从而保证 EMS 优化算法的正确性。

然而, 上述文献还未有对基于操纵 EV 用户数据的 EV 充电桩网络攻击模型进行研究, 也未对其攻击的影响进行评估和分析。鉴于此, 本文提出了一种基于用户数据的 EV 充电桩网络攻击模型, 通过篡改 EV 的用户数据形成虚假的 EV 充电桩的充电计划, 从而使 EV 充电桩的总充电成本增加。该攻击模型可描述为一个两层优化问题, 在上层对注入 EV 充电桩的恶意用户数据进行计算, 形成虚假的充电计划; 在下层为 EV 充电桩的 EMS 的正常充电计划优化算法, 之后将两层优化问题转化为单层优化攻击模型。仿真通过一个 EV 充电站的典型场景验证了所提出攻击方法的可行性并评估了其攻击的性能和影响。

1 EV 充电桩充电计划优化模型

1.1 EV 充电场景描述

假设单个 EV 充电站配置有三种充电功率等级的充电桩, 同时包含多个具有不同充电条件和用户习惯的 EV。其中, EV 充电桩接入配电网, 配网运营商向充电桩提供分时电价, 充电桩按照分时电价对输入 EV 的电能进行计费。在此基础上, EV 充电场景可分为以下两个步骤:

(1) 在 EV 到达充电站前, EV 用户通过通信网络向充电桩发送个人充电信息。

(2) 充电桩中的 EMS 接收到用户充电信息后, 通过优化算法为用户分配最佳的充电桩, 并计算最优充电功率。

在步骤(1)中, 个人充电信息可由向量 $\mathbf{D}_j$ 表示, 如式(1)所示。

$$\mathbf{D}_j = [a_j \quad d_j \quad SOE_j^1 \quad SOE_j^D] \quad (1)$$

式(1)中, a_j , d_j 分别为第 j 辆 EV 的预计到达时间和期望离开时间; SOE_j^1 为第 j 辆 EV 到达充电站的预计初始 SOE, SOE_j^D 为第 j 辆 EV 离开充电站时的期望 SOE 的最小值。

在步骤(2)中, 假设充电站包含三种功率等级的充电桩: A 级、B 级和 C 级充电桩, 额定功率分别为 50 kW, 100 kW, 200 kW, 且均配置有 EMS。根据分时电价, EMS 可通过优化 EV 充电计划和充电桩分配方案协助充电桩运营商最小化 EV 的充电成本, 优化所需要的数据除了步骤(1)中个人充电信息 $\mathbf{D}_j$, 还包含第 j 辆 EV 的最大 SOE 和第 i 个充电桩的最大充电功率, 分别由 $SOE_j^{\max}$ 和 $P_i^{\max}$ 表示。

1.2 EV 充电计划优化模型

对于第 j 辆 EV 来说, 假设存在充电时刻 k 属于 $\{t, t+1, \dots, t+h-1\}$, 单位充电时长为 Δt , h 为预计充电时间范围, 则 EV 充电计划的确定可以表述为混合整数线性规划问题, 如式(2) - (11) 所示。

$$\min J = \sum_{k=t}^{t+h-1} (C_k \sum_{j=1}^M P_{j,k}) \Delta t \quad (2)$$

$$\text{s. t. } SOE_{j,k+1} = SOE_{j,k} + P_{j,k} \Delta t \quad (3)$$

$$SOE_j^1 \leq SOE_{j,k} \leq SOE_j^{\max} \quad (4)$$

$$SOE_j^D \leq SOE_{j,t+h} \quad (5)$$

$$0 \leq P_{j,k} \leq \sum_{i=1}^N b_{i,j,k}^{\text{ch}} P_i^{\text{max}} \quad (6)$$

$$\frac{SOE_j^{\text{D}} - SOE_{j,k}}{SOE_j^{\text{max}}} \leq b_{j,k}^{\text{nf}} \leq \left(\frac{SOE_j^{\text{D}} - SOE_{j,k} - \epsilon}{SOE_j^{\text{max}}} \right) + 1 \quad (7)$$

$$\sum_{j=1}^M b_{i,j,k}^{\text{ch}} \leq 1 \quad (8)$$

$$\sum_{j=1}^M b_{i,j,k}^{\text{ch}} \leq b_{j,k}^{\text{s}} \quad (9)$$

$$b_{i,j,k-1}^{\text{ch}} + b_{j,k}^{\text{nf}} - 1 \leq b_{i,j,k}^{\text{ch}} \leq b_{i,j,k-1}^{\text{ch}} + b_{j,k}^{\text{nf}} \quad (10)$$

$$b_{i,j,k-1}^{\text{ch}}, b_{i,j,k}^{\text{ch}}, b_{j,k}^{\text{nf}} \in \{0, 1\} \quad (11)$$

该规划问题目标在于最小化式(2)所示的目标函数,该目标函数为预计充电时间范围内考虑分时电价 C_k 和 EV 充电功率 $P_{j,k}$ 的总充电成本。式(3)~(11)为约束条件,其中式(3)表示当前 k 时刻与未来 $k+1$ 时刻各 EV 的 SOE 的动态变化;式(4)~(5)分别表示 EV 到达和离开充电桩时 SOE 的上下限;EV 的充电功率受到充电桩最大功率 P_i^{max} 的限制,如式(6)所示,其中 $b_{i,j,k}^{\text{ch}}$ 为二元决策变量,表示 k 时刻第 j 辆 EV 在第 i 个充电桩的充电状态,“1”代表充电,“0”代表不充电;式(7)表示第 j 辆 EV 在 k 时刻是否充满,如果未充满,则 $SOE_{j,k} < SOE_j^{\text{D}}$,此时非满电状态标志 $b_{j,k}^{\text{nf}} = 1$,如果充满则 $SOE_{j,k} = SOE_j^{\text{D}}$,此时 $b_{j,k}^{\text{nf}} = 0$, ϵ 为足够小的正数;式(8)保证在每一时刻第 i 个充电桩最多只能给一辆 EV 充电;式(9)表示当第 j 辆 EV 到达充电桩后第 i 个充电桩才能允许给其充电;式(10)根据 $b_{j,k}^{\text{nf}}$ 判断在 k 时刻和 $k-1$ 时刻是否允许 EV 连续充电,例如当 $b_{j,k}^{\text{nf}} = 1$ 时, $b_{i,j,k-1}^{\text{ch}} = b_{i,j,k}^{\text{ch}} = 1$,当 $b_{j,k}^{\text{nf}} = 0$ 时, $b_{i,j,k-1}^{\text{ch}} = b_{i,j,k}^{\text{ch}} = 0$;式(11)表示 $b_{i,j,k-1}^{\text{ch}}, b_{i,j,k}^{\text{ch}}, b_{j,k}^{\text{nf}}$ 为二元决策变量。

综上, EV 充电计划优化问题的决策变量可表示为 $[P_{j,k}, SOE_{j,k}, b_{i,j,k}^{\text{ch}}, b_{j,k}^{\text{nf}}]$ 。通常来说,两层优化问题难以使用目前的商用求解器求解,为了解决这个问题,需要将该攻击的双层优化模型转化为单层优化模型,此转化过程需要得到式(2)~(11)的库恩-塔克(KKT)条件^[10]。然而,混合整数线性规划问题由于不是凸函数优化问题而不存在 KKT 条件,因此需要将式(2)~(11)转化为凸线性函数优化问题,以获取其 KKT 条件。通过将式(11)所示二元决策变量 $b_{i,j,k}^{\text{ch}}, b_{j,k}^{\text{nf}}$ 转化为连续变量可将问题转化为凸松弛优化问题,如式(12)所示。

$$\begin{cases} 0 \leq b_{i,j,k}^{\text{ch}} \leq 1 \\ 0 \leq b_{j,k}^{\text{nf}} \leq 1 \end{cases} \quad (12)$$

综上,式(2)~(10),(11)就构成了 EV 充电计划的凸松弛优化问题,通过应用拉格朗日乘数法即可得到该优化问题的 KKT 条件。

2 基于用户数据的 EV 充电桩攻击模型

假设在 EV 充电过程中攻击者将恶意数据暗中注入 EV 用户数据,通过 EV 用户的终端连接到充电桩的 EMS,如图 1 所示。在此攻击场景中,攻击者篡改的 EV 用户数据作为输入变量输入至第 1 节中的 EV 充电计划优化模型中,从而导致充电成本最优解的变化,攻击的主要目的在于提高 EV 充电桩的运营成本,获取不法利益。

如果想实施一次成功的攻击,则攻击者需要满足以下条件:一是攻击者有能力入侵通信网络从而监控和操纵 EV 用户数据;二是攻击者可以根据分时电价和充电桩的数量和充电功率求解 EV 充电计划优化问题。

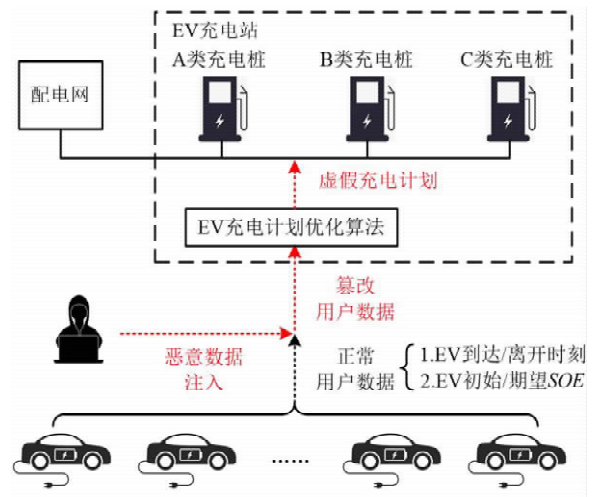


图 1 基于用户数据的充电桩攻击场景

2.1 上层优化模型

本文所提出的攻击模型可表示为两层多目标混合整数线性优化模型,在上层,优化问题可表示为式(13)~(19)。

$$\max J^U = \sum_{k=t}^{t+h-1} (C_k \sum_{j=1}^M P_{j,k}) \Delta t - \omega \sum_{j=1}^M b_j^a \quad (13)$$

$$\text{s. t. } -\tau SOE_j^{\text{D}} b_j^a \leq \Delta SOE_j^{\text{I}} \leq \tau SOE_j^{\text{I}} b_j^a \quad (14)$$

$$-\tau SOE_j^{\text{D}} b_j^a \leq \Delta SOE_j^{\text{D}} \leq \tau SOE_j^{\text{D}} b_j^a \quad (15)$$

$$\Delta SOE_j^l \leq \Delta SOE_j^D \leq \min (SOE_j^{\max} - SOE_j^D + \Delta SOE_j^l, SOE_j^{\max} - SOE_j^D) \quad (16)$$

$$0 \leq \Delta a_j \leq \kappa b_j^a \quad (17)$$

$$-\kappa b_j^a \leq \Delta d_j \leq 0 \quad (18)$$

$$b_{j,k}^{s,a} = \begin{cases} 1, & a_j + \Delta a_j \leq k \leq d_j + \Delta d_j \\ 0, & k < a_j + \Delta a_j \text{ or } k > d_j + \Delta d_j \end{cases} \quad (19)$$

在上层优化模型中,攻击者的目标为计算四种类型的恶意数据,即式(1)所示个人充电信息的扰动量,表示为 $\Delta \mathbf{D}_j = [\Delta a_j, \Delta d_j, \Delta SOE_j^l, \Delta SOE_j^D]$,上层计算的恶意数据输入下层的 EV 充电计划优化模型,以同时满足 EV 充电桩的总充电成本最大化和攻击成本的最小化。式(13)所示目标函数多项式中的第一项代表所有 EV 的总充电成本,第二项代表注入的恶意数据,其中 b_j^a 为篡改标志,当第 j 辆 EV 用户数据遭到篡改时, $b_j^a = 1$,否则 $b_j^a = 0$, ω 表示攻击成本的惩罚因子。对于约束条件,式(14)~(15)表示注入的 SOE 扰动量幅值大小分别受到攻击限制因子 τ 的限制;式(16)的约束是为了确保恶意数据不会被 EV 用户或运营商检测到;式(17)~(18)表示扰动量 Δa_j , Δd_j 幅值大小分别受到攻击限制因子 κ 的限制,需要注意的是 Δa_j 应不小于零, Δd_j 应不大于零,否则可能会导致下层充电计划的优化结果超出 EV 在充电站的停留时段,造成异常而被运营商检测到。式(19)表示 EV 在被篡改后的到达和离开时间段内停留的状态, $b_{j,k}^{s,a}$ 为变量,其随着 Δa_j , Δd_j 的变化而变化。

2.2 下层优化模型

下层优化模型即 1.2 节中描述的 EV 充电计划优化模型,但考虑到攻击者对用户数据的篡改,部分约束可重写为下列各式:

$$\text{s. t. } SOE_j^l + \Delta SOE_j^l \leq SOE_{j,k} \leq SOE_j^{\max} \quad (20)$$

$$SOE_j^D + \Delta SOE_j^D \leq SOE_{j,r+h} \quad (21)$$

$$\frac{SOE_j^D + \Delta SOE_j^D - SOE_{j,k}}{SOE_j^{\max}} \leq b_{j,k}^{nf} \leq \left(\frac{SOE_j^D + \Delta SOE_j^D - SOE_{j,k} - \epsilon}{SOE_j^{\max}} \right) + 1 \quad (22)$$

$$\sum_{j=1}^M b_{i,j,k}^{ch} \leq b_{j,k}^{s,a} \quad (23)$$

其中,式(4)重写为式(20),式(5)重写为式(21),式(7)重写为式(22),式(9)重写为式(23)。

综上,式(2)~(3),(6),(8),(10)~(11),(20)~(23)就构成了下层优化模型。

2.3 单层优化攻击模型的转换

如 1.2 节所述,两层优化模型需要转换为单层优化模型,此转换过程的关键为得到下层优化模型的 KKT 条件,并将其整合到上层优化模型中。

假设优化问题包含决策变量向量 x 和输入变量向量 y ,则带有等式和不等式约束的优化问题可表示为

$$\min J(x, d) \quad (24)$$

$$\text{s. t. } Ax = d \quad (25)$$

$$Bx \leq d \quad (26)$$

定义拉格朗日函数为 $\mathcal{L}(x, d) = J(x, d) - \lambda(Ax - d) + \eta(Bx - d)$,之后 KKT 条件可以通过下列各式得到:

(1)一阶最优性条件:

$$\begin{aligned} \nabla_x \mathcal{L}(x, d) &= 0 \\ \Rightarrow \nabla_x J(x, d) - \lambda(Ax - d) + \eta(Bx - d) &= 0 \end{aligned} \quad (27)$$

(2)原始可行性条件:

$$Ax = d, \quad Bx \leq d \quad (28)$$

(3)互补和松弛条件:

$$\eta(Bx - d) = 0, \quad \eta \geq 0 \quad (29)$$

通过对 2.2 节中的下层优化模型应用式(27)~(29)即可得到相应的 KKT 条件。将得到的 KKT 条件作为新的约束整合至上层优化模型即可得到单层优化攻击模型。

2.4 攻击模型的检测

对于网络攻击模型检测一般通过使用物理机制分析或深度学习的方法来提取充电桩受到攻击时的系统特征,并比较检测到的特征以确定是否发生了网络攻击。针对本文充电桩网络攻击,基于物理机制的检测方法主要是在攻击存在情况下检测充电桩的实际充电过程是否发生异常,例如 ΔD_j 的设置不合理导致的充电时段超出 EV 停留时段、 SOE 已达到最大值仍继续充电等,然而此种检测方法由于上层优化模型的约束导致 ΔD_j 超限的几率很小,因此实际发生充电异常情况的概率也很低,检测效果很差。

考虑到攻击者仅在 EV 传输至充电桩的用户数据进行了篡改,可以考虑在 EMS 接收到用户信息后返回一个充电确认信息,用户在 EV 端对发送和接收到的充电信息进行核对,如果无误再向充电

桩发起充电请求,如此就规避了攻击者的恶意数据。另一种方法是考虑到攻击造成了 EV 充电电量的普遍升高,因此可以在 EV 充电结束后对比预期和实际的充电电量,若实际电量明显超出预期充电电量,则可以判断受到了恶意攻击。

3 仿真验证

本节以一个虚拟的充电站为例,该充电站包含 40 个具有不同用户数据的 EV,在到达充电站后,充电桩按照 EMS 充电计划的优化结果对 EV 进行充电。每辆 EV 的到达和离开时间服从离散均匀分布。假设虚拟充电站包括 6 个充电桩,其中 A 级、B 级和 C 级充电桩各两个,最大功率等级分别为 50 kW、100 kW、200 kW。配电网提供的分时电价如图 2 所示。

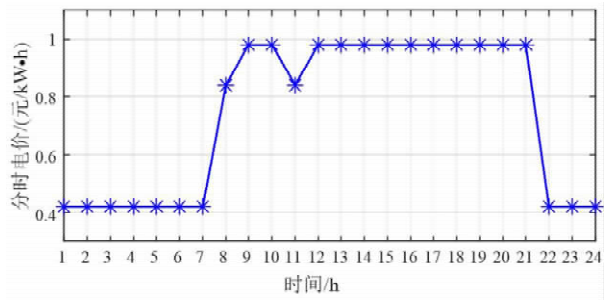


图 2 配电网提供的分时电价

为简化分析,每辆 EV 的充电时段、最大 SOE、初始 SOE 和期望 SOE 设置为相同值, $a_j - d_j = 2.5 \text{ h}$, $SOE_j^{\max} = 72.6 \text{ kW} \cdot \text{h}$, $SOE_j^I = 14.5 \text{ kW} \cdot \text{h}$, $SOE_j^D = 65.3 \text{ kW} \cdot \text{h}$ 。在上层优化模型中,惩罚因子 ω 、SOE 攻击限制因子 τ 、到达\离开时间的攻击限制因子 κ 分别设置为 0.1、0.2 和 0.3。在下层优化模型中,非满电状态标志 ϵ 设置为 10^{-7} 。仿真时长为 24 h,单位充电时长为 $\Delta t = 15 \text{ min}$,预计充电时间范围 $h = 16\Delta t$ 。仿真优化模型基于 MATLAB 2018b 中的 CPLEX 12.8 优化工具包进行求解。

本节对所提出的攻击模型对 EV 充电桩的总充电成本和 SOE 的影响进行量化分析,图 3 显示了在整个充电计划期间 EV 充电站分别在无攻击和有攻击情景下的总充电成本。由图 3 可见,有攻击情况下累计总充电成本在 2:30 之后开始高于无攻击情况,最终在充电计划时长结束时,无攻击和有攻击情况下的总充电成本分别为 1287.85 元和

1377.11 元,可见所提出的攻击模型确实可通过注入恶意用户数据实现增加总充电成本的目标。

图 4 对比了在 7 个分时电价区间下无攻击和有攻击情况的总充电成本,每个充电时段区间有着相同的价格,如图 2 所示。从图 4 中可以看出攻击导致的充电成本增加主要在两个分时电价时段,即 (00:00~08:00)和(16:00~22:00)时段,这是由于攻击者的攻击解除了 SOE 的原始约束,增加了 EV 的初始和期望 SOE 水平,即在约束式(20)~(21)内 $SOE_{j,k}$ 和 $SOE_{j,t+h}$ 不会低至原来的下限;另一方面,攻击者将 EV 充电计划移至分时电价更高的时间段,从而使充电桩产生的充电成本增加。

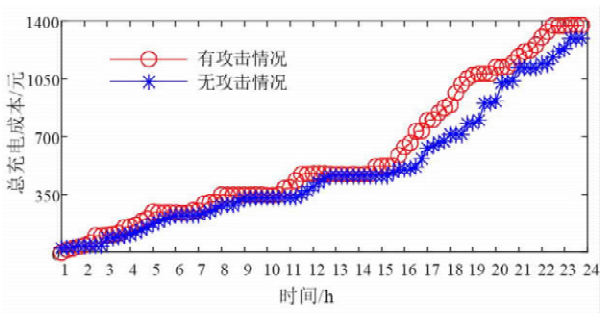


图 3 无攻击和有攻击情景下的总充电成本

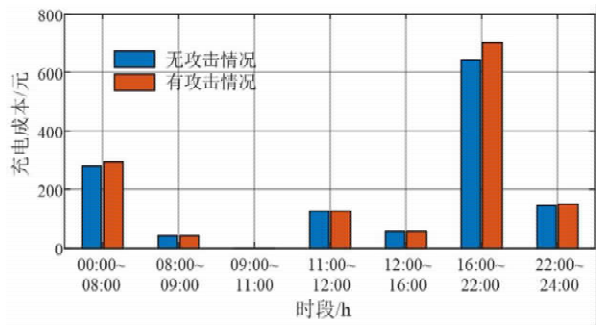


图 4 无攻击和有攻击情景下的分时段充电成本

在(00:00~08:00)时段,充电成本的增加是攻击令初始/期望 SOE 水平的增加导致的,使得 EV 的期望 SOE 从 640.66 kW·h 上升至 698.74 kW·h。在(16:00~22:00)时段,充电成本的增加大于(00:00~08:00)时段,说明此时段充电桩受到了更多的攻击,这是由于此时段攻击者发起的攻击同时提高了 EV 的期望 SOE 水平和移动 EV 的充电计划至分时电价更高的时段,对于 SOE 水平的提高使得 EV 充电总能量由 183.28 kW·h 增加至 206.70 kW·h,对于充电计划的时移使得三辆 EV 的充电时段发生了改变,其中第 20 辆 EV 的充电

时段由(16:00~16:30)移至(15:45~6:15),第 34 辆 EV 的充电时段由(22:00~22:30)移至(21:45~22:15),其中第 37 辆 EV 的充电时段由(22:30~23:00)移至(21:00~21:15)和(22:00~23:00)。

4 结 论

提出了一种基于用户数据的 EV 充电桩网络攻击模型。通过操纵 EV 向充电桩传输的用户数据,使 EMS 中 EV 充电计划优化算法发生异常,导致 EV 充电桩的总充电成本增加。该网络攻击模型为一个包含上层和下层优化模型的两层优化模型,在上层计算注入网络的恶意用户数据,在下层接收恶意数据计算得到虚假的充电计划,以最大化 EV 的总充电成本,之后通过应用 KKT 条件将两层优化模型转化为最终的单层优化攻击模型。仿真以一个虚拟充电场景为例,结果验证了该网络攻击模型的可行性和危害性,相较于无攻击情况,该攻击模型提高了 EV 的初始/期望 SOE,并将部分 EV 的充电时段移至分时电价更高的时段,确实提高了固定时段内 EV 的总充电成本。

参考文献

[1] 吴芳柱,田园. 基于分时电价的电动汽车有序充放电策略研究[J]. 电工电气,2022(04):21-25.

[2] 周毅,袁泉,汤奕,等. 基于路电-耦合网络的电动汽车充电

决策优化方法[J]. 电网技术,2021,45(9):3563-3572.

[3] GOTTUMUKKALA R, MERCHANT R, TAUZIN A, et al. Cyber-physical system security of vehicle charging stations[C]//2019 IEEE Green Technologies Conference (GreenTech). IEEE, 2019: 1-5.

[4] REEH D, TAPIA F C, CHUNG Y W, et al. Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats[C]//2019 IEEE Transportation Electrification Conference and Expo (ITEC). IEEE, 2019:1-6.

[5] BHUSAL N, GAUTAM M, BENIDRIS M. Cybersecurity of electric vehicle smart charging management systems[C]//2020 52nd North American Power Symposium (NAPS). IEEE, 2021: 1-6.

[6] WANG B, DEHGHANIAN P, WANG S, et al. Electrical safety considerations in large-scale electric vehicle charging stations[J]. IEEE Transactions on Industry Applications, 2019, 55(6): 6603-6612.

[7] SAYED M A, ATALLAH R, ASSI C, et al. Electric vehicle attack impact on power grid operation[J]. International Journal of Electrical Power & Energy Systems, 2022, 137: 107784.

[8] MOUSAVIAN S, EROL-KANTARCI M, WU L, et al. A risk-based optimization model for electric vehicle infrastructure response to cyber attacks[J]. IEEE Transactions on Smart Grid, 2017, 9(6): 6160-6169.

[9] HOANG D T, WANG P, NIYATO D, et al. Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model[J]. IEEE Access, 2017, 5: 732-754.

[10] 赖纪东,姚娴,苏建徽,等. 一种基于 KKT 算法的 DAB 回流功率优化方法[J]. 电力电子技术,2022,56(6):103-106.