DCA: Delayed Charging Attack on the Electric Shared Mobility System

Shuocheng Guo, Hanlin Chen, Mizanur Rahman, *Member, IEEE*, and Xinwu Qian

***Abstract*— An efficient operation of the electric shared mobility system (ESMS) relies heavily on seamless interconnections among shared electric vehicles (SEV), electric vehicle supply equipment (EVSE), and the grid. Nevertheless, this interconnectivity also makes the ESMS vulnerable to cyberattacks that may cause short-term breakdowns or long-term degradation of the ESMS. This study focuses on one such attack with long-lasting effects, the Delayed Charge Attack (DCA), that stealthily delays the charging service by exploiting the physical and communication vulnerabilities. To begin, we present the ESMS threat model by highlighting the assets, information flow, and access points. We next identify a linked sequence of vulnerabilities as a viable attack vector for launching DCA. Then, we detail the implementation of DCA, which can effectively bypass the detection in the SEV's battery management system and the cross-verification in the cloud environment. We test the DCA model against various Anomaly Detection (AD) algorithms by simulating the DCA dynamics in a Susceptible-Infectious-Removed-Susceptible process, where the EVSE can be compromised by the DCA or detected for repair. Using real-world taxi trip data and EVSE locations in New York City, the DCA model allows us to explore the long-term impacts and validate the system consequences. The results show that a 10-min delay results in 12-min longer queuing times and 8% more unfulfilled requests, leading to a 10.7% ($311.7) weekly revenue loss per driver. With the AD algorithms, the weekly revenue loss remains at least 3.8% ($111.8) with increased repair costs of $36,000, suggesting the DCA's robustness against the AD.**

***Index Terms*— Delayed charging attack, false data injection attack, electric shared mobility system, shared electric vehicle, cybersecurity.**

NOMENCLATURE

AD	Anomaly Detection.
BMS	Battery Management System.
CAN	Control Area Network.
CC-CV	Constant-Current-Constant-Voltage.
CCS	Combined Charging System.
CSMS	Charging Station Management System.
Ctrl&Comm.	Control&Communication.
DCA	Delayed Charging Attack.
DCFC	DC Fast Charging.
DDoS	Distributed Denial of Service.
DSO	Distribution System Operators.
ECU	Electronic Control Units.
EM	Expectation-Maximization.
EMS	Energy Management System.
ESMS	Electric Shared Mobility System.
EVSE	Electric Vehicle Supply Equipment.
FDIA	False Data Injection Attack.
GMM	Gaussian Mixture Model.
HMI	Human Machine Interface.
IF	Isolation Forest.
KLD	Kullback-Leibler Divergence.
KMeans	K-Means Clustering.
MitM	Man-in-the-Middle.
MTTR	Mean-Time-To-Repair.
NYC	New York City.
OCPI	Open Charge Point Interface.
OCPP	Open Charge Point Protocol.
PCC	Principal Component Classifier.
PLC	Power Line Communication.
SEV	Shared Electric Vehicle.
SIRS	Susceptible-Infectious-Removed-Susceptible.
SoC	State-of-Charge.

Manuscript received 2 February 2023; revised 31 March 2023; accepted 12 June 2023. Date of publication 28 June 2023; date of current version 1 November 2023. This work was supported in part by the National Science Foundation under Grant 2104999. The Associate Editor for this article was M. Bilal. *(Corresponding author: Xinwu Qian.)*

Shuocheng Guo, Mizanur Rahman, and Xinwu Qian are with the Department of Civil, Construction and Environmental Engineering, The University of Alabama, Tuscaloosa, AL 35487 USA (e-mail: sguo18@ua.edu; mizan.rahman@ua.edu; xinwu.qian@ua.edu).

Hanlin Chen is with the Lyles School of Civil Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: chen1368@purdue.edu).

Digital Object Identifier 10.1109/TITS.2023.3287792

I. INTRODUCTION

ELECTRIFYING the fleet for shared mobility service is a promising direction to lower operation costs and reduce greenhouse gas emissions [1], [2]. As an example, Shenzhen, China has a fully-electrified taxi fleet by the end of 2019 [3]. Moreover, New York City (NYC) will embrace 100% electrification of its for-hire vehicles fleet by 2030 [4], which further requires the deployment of over 1,750 DC-Fast charging ports [5]. For large-scale electric shared mobility systems (ESMSs), the essence of the efficient operation is the optimal scheduling of charging and mobility services, which requires seamless interconnections among the major assets in the ESMS (see Fig. 1), including the shared electric vehicles (SEVs), EV supply equipment (EVSE), charging station management system (CSMS), and EVSE and SEV operators, facilitated by multiple communication protocols, e.g., Open Charge Point Protocol (OCPP) [6] and Open Charge Point Interface (OCPI) [7]. However, these communication pathways also present vulnerabilities that can be exploited to compromise the SEVs and EVSE [8], [9], [10], resulting in

1558-0016 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

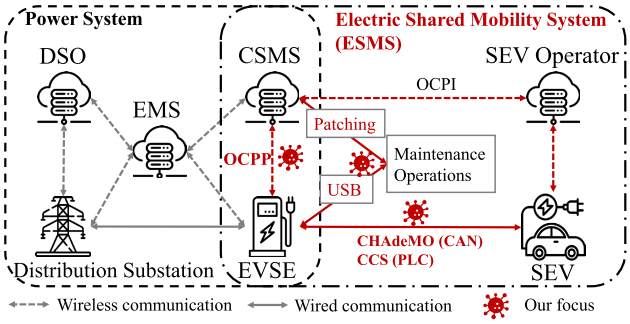


Fig. 1. Communication framework in the ESMS (DSO: Distribution System Operators; EMS: Energy Management System).

the battery charging controller malfunctions and inconsistent changing outcomes for SEVs, thus disrupting the coordination of charging schedules across the entire fleet. This will translate into local congestion at EVSEs, excessive downtime for vehicle supply, and degradation of system performances or even catastrophic failure of the entire mobility system. Considering the vulnerabilities and significant consequences above, this study will take the first step to investigate an attack model that can disrupt ESMS and understand its long-term impacts on operational dynamics.

The cybersecurity issues have been extensively studied in the fields of smart grid [11], [12], [13], Internet-of-Things [14], mobility-as-a-service systems [15], traffic signal control systems [16], cyber-physical systems [17], [18], [19], intelligent transportation systems [20], and more recently, the ESMS [21], [22], [23], [24], [25]. While the ESMS offers improved efficiency with coordinated charging and dispatching, it also inherits the cyber threats from its assets, including SEVs, EVSE, and the communication interfaces with the CSMS and SEV operator. As such, the ESMS can be subject to new forms of cyberattacks due to the increased system dependencies.

As depicted in Fig. 1, we showcase a potential attack vector represented by red lines for a distinct type of False Data Injection Attack (FDIA), known as the Delayed Charging Attack (DCA). The DCA aims to stealthily delay the charging process of the SEV fleet while maintaining the safety requirements of the SEV (e.g., avoiding excessive current). This attack can be accomplished by compromising the EVSE via a physical access point (i.e., USB port) or intercepting the communication between the SEV and EVSE by patching via the OCPP during the maintenance operations. The compromised EVSE then injects falsified State-of-Charge (SoC) data into the SEV via the CHAdeMO or CCS physical connections. As a result, the SEV is spoofed to accept a reduced charging rate (e.g. lower current or voltage), which extends the charging time to reach the target SoC. The compromised EVSE and SEV operator bypass cross-verification achieved by the OCPI by uploading constant charging log information to the cloud environment (i.e., CSMS and SEV operator). For full steps of implementation, see Section III-A.

Unlike other types of attacks (e.g., denial-of-service) which cause an entire breakdown in one shot, the DCA is designed as a stealthy cyberattack with long-term consequences. In this regard, the DCA is likely to be overlooked for two reasons: (1) the DCA will not lead to an immediate collapse of the ESMS, but instead a gradual degradation over time, and (2) the anomalies resulting from the DCA are challenging to detect, particularly in the ESMS, where outliers (e.g., extended charging duration) can be indistinguishable due to the large variation in charging duration (which can range from several minutes to 1-2 hours) across all charging activities.

To the best of our knowledge, no prior studies have investigated the DCA on the large-scale ESMS. This study aims to address this gap by exploring the system-level consequences of the DCA and evaluating the DCA's efficacy and robustness under different length of delayed charging service and various Anomaly Detection (AD) techniques. Specifically, we define the robustness of DCA as its ability to maintain the performance even in the presence of AD algorithms, which highlights the DCA's effectiveness and stealthiness. This study will begin by presenting the ESMS threat model and identifying a linked sequence of potential vulnerabilities, which forms a viable attack vector for launching DCA. Then, we model the DCA dynamics based on the Susceptible-Infectious-Removed-Susceptible (SIRS) process. Detection strategies are incorporated by comparing widely adopted AD techniques, which can detect the malfunctioning EVSE based on the deviation of the normal system performance. Those malfunctioning EVSE will revert to susceptible state upon repair.

Our major contributions are summarized as follows:

- We present a threat model for ESMS with detailed assets, information flow, and access points. Through our analysis, we identify various vulnerabilities that can be exploited as access points for launching DCA, including physical entry points (e.g., USB ports) and communication interfaces (e.g., signal exchanges between EVSE and SEV, software updates).
- We develop a novel DCA model that encompasses attack vectors, potential consequences for the ESMS, and implementation details. We employ different anomaly detection strategies to demonstrate the robustness of the DCA.
- We develop a high-fidelity simulation platform that uses real-world data to assess the long-term effects of the DCA on a large-scale ESMS and validate the system consequences of this attack.

The rest of the paper is organized as follows. Section II describes ESMS threat model and examines the viability of the DCA model. Section III proposes the SIRS-based DCA model and AD algorithms, and Section IV introduces the key components in our high-fidelity simulation platform. Section V presents the scenario design and parameter assumption, followed by numerical experiments in Section VI. Section VII concludes our paper.

II. Threat Model for the ESMS

In this section, we present the threat model of the ESMS by highlighting the major assets, information flows, and access points. We make a significant contribution by streamlining a generic SEV-EVSE threat model [26] to only include the

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

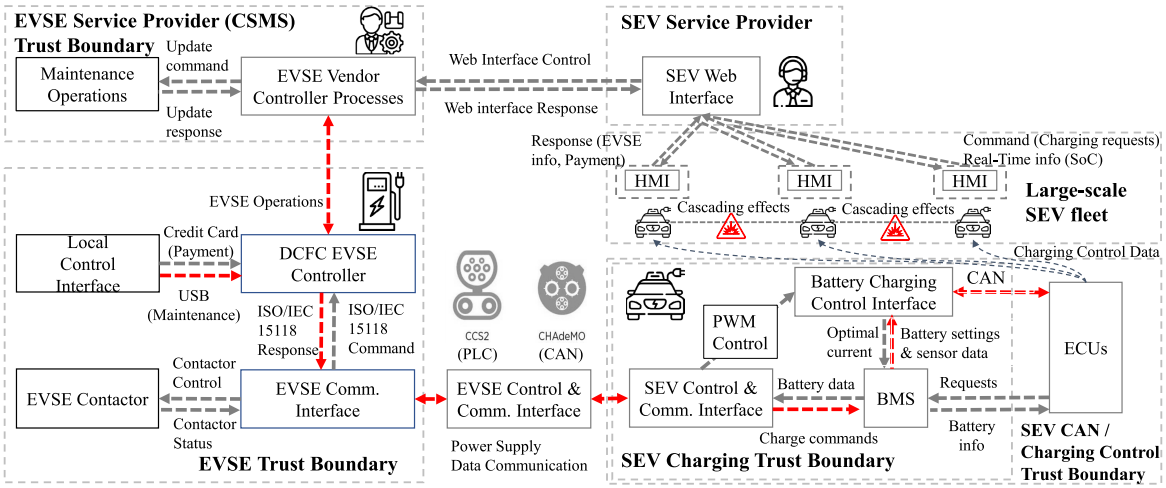


Fig. 2. A minimal implementation of ESMS, adapted from the STRIDE threat model proposed by the Sandia National Laboratories [26]. (The red arrows indicate the communication channels that carry falsified data, and the grey arrows represent other communication channels).

essential components for a minimal implementation of the large-scale ESMS while preserving the same properties as in the original model. By extending the framework to the system level, we demonstrate the communications between a large-scale SEV fleet and the SEV service provider and the potential cascading effects among the SEVs, which is a novel contribution compared to the single-vehicle version threat model. Moreover, we focus on specific cyber-physical threats that occur in the real-world, rather than providing a generic description of possible attack approaches, which allows us to better understand the uniqueness of the ESMS and provides prerequisites for the development of the DCA.

Our threat model, shown in Fig. 2, provides a minimal implementation of the electric shared mobility service operated by a single EVSE and SEV service provider. It includes four types of trust boundaries, the SEV fleet, and the SEV service provider. Information flows are detailed between the major assets and interfaces, including EVSE or SEV control & communication interfaces, connectors, battery management system in the SEV, and the external entities (e.g., SEV and EVSE service providers).

A. Major Assets

We summarize the major assets in the ESMS threat model as follows:

- **CSMS**: The CSMS enables SEV drivers and EVSE operators to control and monitor the EVSE remotely, including charging record-keeping, scheduling, and user authentication [27].
- **EVSE**: The EVSE consists of four major components: DC Fast Charging (DCFC) EVSE controller, EVSE communication interface, EVSE Contactor, and local control interface. The main function of the EVSE is to transport the electric power from the power grid to the SEV battery.
- **DCFC EVSE controller**: The DCFC EVSE controller processes the exchanged data from the local control interface (e.g., payment information) and EVSE communication interface (e.g., SEV battery data). It processes the real-time information between the EVSE and the EVSE vendor controller in the CSMS, e.g., availability status. In addition, the EVSE controller also supports the maintenance service, which can be conducted by either physical access (e.g., USB) or over-the-air service via OCPP from the CSMS (e.g., patch and software update).
- **EVSE communication interface**: The EVSE communication interface communicates with the EVSE Contactor for power supply, obtains charging requirements from the EVSE control & communication interface, and sends it to the DCFC EVSE controller [28].
- **EVSE control&communication interface**: The EVSE control&communication interface is typically the only physical link between the EVSE and SEV, which is embedded in the charging connector. The most popular types of DC Fast charging connectors in the U.S. include the CHAdeMo, Combined Charging System (CCS), and Tesla charger [29]. The connector consists of power lines, control lines, control pilots (i.e., power line communication (PLC) in CCS, or CAN buses in CHAdeMO), enabling power supply, analog control, and data communication, respectively [30].
- **Battery Management System (BMS)**: BMS controls the status of the SEV battery within the specified safe operating conditions [31]. For instance, it monitors the real-time voltage, current, and battery temperature to avoid excessive current or overheating [30].
- **SEV control & communication interface**: SEV battery charging interface collects the battery data information from the BMS and sends the EVSE's configuration to the BMS for a compatibility check [30].

B. Information Flows in SEV Charging Process

The ESMS relies heavily on seamless communication for an efficient coordination of dispatching and charging needs. In particular, a full cycle of charging service, from charging reservations to completion, requires various communication exchanges between the SEV driver, EVSE, and CSMS.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

TABLE I
SUMMARY OF POSSIBLE ATTACKS ON THE ESMS

Type of attacks	Targeted assets	Impacts	Ref.
EV-EVSE interface tampering	EV-EVSE communication	Terminate charging unless manually reconnecting	[8]
Distributed Denial-of-Service	CSMS and its communication with EVSE	Unavailability of EVSE, delayed response from CSMS	[38]
Electronic control manipulation	EVSE Human Machine Interface (HMI) or SEV	Modify the HMI front panel display (SoC, time remaining), disrupt controls coordination between power modules	[37]
Man-in-the-Middle attack	Communication between EVSE, EV, and EV driver	Track issues, payment fraud, spoofing for a free service	[39]

For instance, the SEV driver must initiate a charging request with the desired SoC or charging duration, which can be accomplished through the charging app (e.g., EVgo [32] and EVmatch [33]) or human-machine interface (HMI). Before the charging starts, several rounds of confirmation will proceed via the analog control lines for a compatibility check (e.g., SEV battery and charger parameters) [30]. During the charging process, numerous communication exchanges take place between the EVSE and SEV regarding power supply and battery conditions [30] (e.g., maximum voltage to stop charging, target voltage, battery capacity, and maximum admissible current of the EVSE and SEV). Furthermore, the BMS continuously calculates the optimal charging current based on the current SoC, battery condition, and temperature. Upon reaching the target SoC or charging duration, the BMS sends a signal to the EVSE to end the charging process.

C. Access Points

The wireless communication and physical entries in the ESMS open a wide attack surface, which can be exploited as access points to disrupt the charging process. We briefly summarize three types of access points in the ESMS as follows (for a comprehensive review, see Johnson et al. [24]).

- **Control Area Network (CAN)**: The initial design purpose of CAN was to ensure communication performance under a complex electromagnetic environment, which does not include consideration for cybersecurity [34]. The communication mechanism within CAN utilizes a broadcasting mechanism, enabling eavesdropping attacks. As seen in Fig. 2, the CAN buses cover the major components in the EVSE and SEV through the EVSE control & communication interface, where the transmitted messages can be modified and broadcast to all covered electronic control units (ECUs) without discretion. [34].
- **OCPP**: Nasr et al. [27] reported 13 types of vulnerabilities (e.g., missing authentication, hard-coded credentials, and missing rate limit) in 16 real-world CSMSs. Those vulnerabilities can be further exploited to compromise the lower-level EVSE by embedding malware into patches, thus disrupting the charging process and manipulating the default setting of the EVSE.
- **USB port on EVSE**: Although potential vulnerabilities of USB ports were demonstrated in several studies [22], [35], the first attack via the external interface, e.g., USB or serial interfaces, was reported by the Idaho National Laboratory [36], [37]. After obtaining physical and remote access to the EVSE, researchers successfully manipulated the modular power electronics modules in EVSE ports equipped with J1772 CCS and CHAdeMO protocols, thus disrupting the charging process.

D. Possible Attacks on ESMS

In the ESMS, the vulnerabilities identified during the charging process create a *linked sequence* from the external USB port in the maintenance interface, via the connector, and to the BMS and ECUs in the SEV. These vulnerabilities provide various attack surfaces for different malicious attacks, including an EV-EVSE tampering attack, Distributed Denial-of-Service (DDoS) attack, Man-in-the-Middle (MitM) attack, and electronic control manipulation. We summarize these attack vectors and their corresponding impacts on the charging service in Table I. Specifically, the EV-EVSE interface tampering is only possible by physically deploying the off-the-shelf radio near the EVSE, which will significantly suffer from high attacking costs for large-scale impacts. Moreover, the charging process will completely terminate unless manually reconnecting to the connector, making the attack easily detectable through manual reporting of malfunctions. Similarly, the consequences of DDoS and electronic control manipulation are mainly explicit and easier to detect, e.g., delayed server response and web service disruption for hours [40], which have little impact on the ESMS in the long run. As for the MitM attack, the primary target is the data privacy issue, yet few impacts have been reported on the system performance of ESMS. In summary, we note that the above attacks target either one-time breakdowns or data privacy issues, which do not align with our research goal. On the other hand, our proposed DCA serves as a special type of the FDIA that stealthily falsifies the SEV to accept a lower charging rate, leading to a delayed charging service and long-term degradation of the ESMS. In the following sections, we will present the stage-by-stage DCA development and the AD techniques for the DCA detection.

III. DCA DEVELOPMENT AND ANOMALY DETECTION

In this section, we focus on the development of the DCA model and its evaluation against AD techniques. Specifically, we contribute to a novel DCA model that includes the attack vector, potential consequences for the ESMS, and implementation details. To evaluate the efficacy and robustness of the proposed DCA, we introduce five different AD techniques and incorporate them into a SIRS process, enabling the modeling of DCA dynamics in a more realistic and practical manner.

A. DCA Modeling

The DCA is a distinct form of FDIA that aims to disrupt the charging service for the SEV fleet by injecting falsified SoC

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

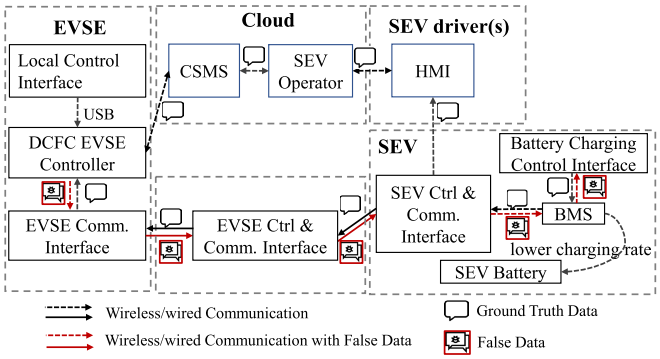


Fig. 3. A block diagram of DCA.

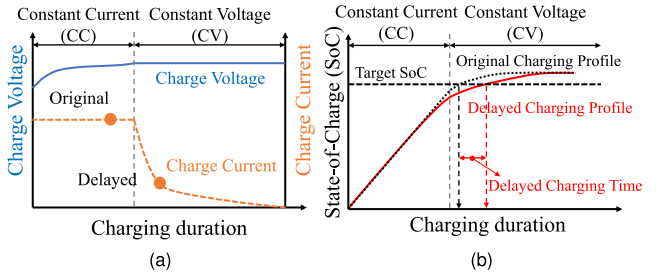


Fig. 4. Charging profiles under normal operation and DCA: (a) CC-CV charging process and (b) SoC profile.

information into the SEV. The attacker exploits vulnerabilities in physical entries (e.g., USB ports) and communication interfaces and protocols (e.g., CAN bus and OCPP) to manipulate the SEV into accepting a reduced charging rate while still ensuring SEV battery's safety (e.g., avoiding excessive current or voltage). The DCA first compromises a set of EVSE via the USB port and targets the delay of charging services for the SEV fleet. This deviation from the normal operation can hardly be detected by SEV drivers and standard AD techniques due to the wide range of charging duration, from several minutes to 1-2 hours [3]. These minor delays in individual charging activities will result in local congestion at EVSEs and the unavailability of SEVs, eventually leading to a cascading failure in ESMS.

It is worth noting that a straightforward DCA can be executed by directly charging the SEV at a lower rate. However, the BMS in SEV continuously monitors the input current via the CAN bus and ECUs. The BMS will raise the alarm if the deviation from the optimal charging current surpasses a set threshold. Therefore, special care is required to devise a DCA model that can stealthily slow down the charging process. We next outline the full steps of the DCA implementation as below (also illustrated in Fig. 3, where the falsified data are highlighted as red arrows):

1) Compromise the EVSE via the USB port.
2) Before the charging starts, the compromised EVSE sends true configuration data to the SEV for the compatibility check.
3) During the charging process:
   a) The DCFC EVSE controller collects the ground-truth information of the SEV battery via CAN and reports it to the CSMS via OCPP.
   b) The DCFC EVSE controller sends falsified SoC information to the BMS in SEV through the EVSE control&communication interface (CAN bus in CHAdeMO and PLC in CCS protocol).

Step 3(b) serves as the core of our DCA for delaying the charging service. It ensures that the battery safety requirement, e.g., maximum current and voltage, are met while bypassing the BMS's monitoring for the optimal charging current. Furthermore, our DCA guarantees that the charging log information uploaded to the cloud (e.g., CSMS and SEV Operator) remains unchanged, allowing for successful cross-verification in the cloud.

To better understand the SEV battery's recharging and monitoring mechanisms, we present the charging profiles of the normal operation and the DCA in Fig. 4. We assume that the BMS adopts the constant-current-constant-voltage (CC-CV) recharging scheme that is widely used for Lithium-ion batteries. Under the proper design of falsified SoC information, the charging service can be delayed within safe limits.

The CC-CV recharging scheme, shown in Fig.4a, maps the charging duration (or SoC information) and charging rate (i.e., charge voltage and current) in a one-to-one relationship. During the constant current (CC) phase, the charge voltage increases gradually to reach its maximum. At a certain SoC tipping point (e.g., 80%), the charge current begins to decrease gradually to zero in the constant voltage (CV) phase. This relationship allows the BMS to detect a change in the charging rate if the SoC information and charge voltage (or current) do not match. In light of this, our DCA leverages this characteristic to manipulate the SoC reported to the BMS, leading to a reduction in the optimal charging current. The difference between the original and delayed charging currents are shown in Fig. 4a, indicating that the optimal charging current under DCA will be less than or equal to the original charging rate. As illustrated in Fig. 4b, the lower charging rate will produce a smoother charging profile and lead to a longer charging duration to reach the target SoC, while still respecting the safety limits of charge voltage and current.

B. DCA Dynamics in SIRS Process

To model the DCA dynamics, we consider an SIRS process. First, the DCA is launched at a set of infectious EVSE ports. As discussed in Sec. III-A, the infected EVSE controller will send falsified SoC information to the SEV's BMS, resulting in a lower optimal charging current and an extended time to reach the same target SoC. As shown in Fig. 5, the DCA model comprises three states of EVSE: **S** (Susceptible), **I** (Infectious), and **R** (Removed), as well as parameters β and γ that denote the transmission rate and recovery rate, respectively. In addition, we denote by τ the repair rate, where $1/\tau$ represents the repair time, indicating the time required for an EVSE to return to the susceptible state. The implementation is outlined in Algorithm 1.

1) S-I Transmission: In the S-I transmission process, an EVSE is compromised by either a wireless communication

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

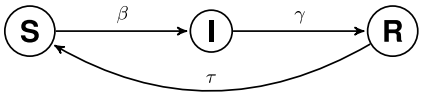


Fig. 5. SIRS model under DCA.

Algorithm 1 SIRS Model in the ESMS

Input: At time step t, set of SEVs $\mathcal{V}^t$, set of EVSE $\mathcal{S}^t = \mathcal{S}_S^t \bigcup \mathcal{S}_I^t \bigcup \mathcal{S}_R^t$
Output: Set of EVSE $\mathcal{S}^{t+1}$ with updated status.

for $i \in \mathcal{S}^t$ **do** {*/loop all EVSE*/}
  if i is susceptible **then**
    Calculate $x_i^{S\to I} \leftarrow B(1,\beta)$ {*/B is Binomial distribution*/}
    if $x_i^{S\to I} == 1$ **then**
      Update the status to infectious
      $\mathcal{S}_I^{t+1} \leftarrow \mathcal{S}_I^t \bigcup \{i\}$; $\mathcal{S}_S^{t+1} \leftarrow \mathcal{S}_S^t \setminus \{i\}$
      Record the time stamp $t_i^I \leftarrow t$
    end if
  else if i is removed **and** $t - t_i^R \geq 1/\tau$ **then** {*/Repair is finished*/}
    Update the status back to susceptible
    $\mathcal{S}_S^{t+1} \leftarrow \mathcal{S}_S^t \bigcup \{i\}$; $\mathcal{S}_R^{t+1} \leftarrow \mathcal{S}_R^t \setminus \{i\}$
  end if
end for
for $i \in \mathcal{S}_I^t$ **do** {*/loop all infectious EVSE*/}
  Proceed $\delta_i^{I\to R} \leftarrow$ AnomalyDetection(d_i, t_i, c_i)
  if $\delta_i^{I\to R} == 1$ **then** {*/EVSE is identified to be an anomaly*/}
    Conduct alarm validation
    if alarm is true positive **then**
      Update the status to removed.
      Record the time stamp $t_i^R \leftarrow t$
      $\mathcal{S}_R^{t+1} \leftarrow \mathcal{S}_R^t \bigcup \{i\}$; $\mathcal{S}_I^{t+1} \leftarrow \mathcal{S}_I^I \setminus \{i\}$
    end if
  end if
end for

interface (e.g., between CSMS and EVSE under OCPP) or an external physical entry (e.g., USB port). For this study, we make a conservative assumption such that the *EVSE is only infected by the physical access via the USB port*, as this approach has been validated to disrupt the SEV's charging service by the Idaho National Laboratory [36], [37]. We also note that the malware may also spread through the EVSE communication network and SEV-EVSE connection [21]. These stronger assumptions may contribute to a higher transmission rate β. However, there is currently a lack of real-world evidence within the ESMS to support such assumptions. As such, these types of malware infection will be the focus of future research as more vulnerabilities in the ESMS are identified.

2) I-R Transmission: The I-R transmission relies on the AD algorithm based on the charging log information. Upon a positive alarm, the EVSE operator will first verify it through the EVSE communication network (assumed within one minute) and send out technician for repair service. If the alarm is confirmed to be a true positive (the EVSE is infectious), the EVSE will be isolated and the technicians will inspect and repair. Therefore, the recovery rate (γ) strongly depends on the effectiveness of the AD algorithm, which will be introduced in Section III-C.

3) R-S Transmission: The R-S transmission occurs after the completion of the repair process for the infected EVSE. The duration of this process is determined based on the mean-time-to-repair (MTTR), denoted by τ. During this period, the EVSE is out of service, and the queued SEV will relocate to other available EVSE ports.

C. Anomaly Detection for DCA

To examine the robustness of the DCA model, we incorporate the AD algorithms in the ESMS that proactively monitor the system charging performances and protect against potential threats. The core purpose of the AD algorithms is to prevent the SEV fleet from experiencing delays in charging service, thereby mitigating the potential for cascading failures in the entire system due to the local congestion and excessive downtime of SEV supply, especially during the peak hour. In particular, we will focus on five AD techniques considering (1) the features of anomalies and (2) the ESMS operation. For the former, the anomalies in our study are assumed to be contextual [41]. For instance, a short charging duration (e.g., 20 min) may be considered anomalous during the nighttime but acceptable during the peak hours [3]. For the latter, we treat the historical charging performance as the baseline (e.g., training set), assuming that it only includes data instances collected during the normal operation before the DCA launched. We next introduce five AD techniques as follows:

1) Isolation Forest (IF): The IF algorithm was first proposed by Liu et al. [42] for the purpose of AD and was later used for the purpose of cyberattack detection [43]. The IF-based detection algorithm proceeds as follows. We first train the IF model using the benign historical charging log data to understand the properties of the normal operation. The charging log data consists of the charging duration, time of day, and the initial SoC, denoted by (d_i, t_i, c_i). With a predefined false alarm rate α_I and the number of estimators n, we are able to train an IF model consisting of n proper binary trees, where α_I of the samples are considered as the anomaly. Next, we collect batches of charging log data online as testing data. We denote the anomaly score of sample i in the testing set by $s_i \in [0, 1]$, which takes the form:

$$s_i = 2^{-\frac{\bar{h}_i}{\bar{h}}} \tag{1}$$

where $\bar{h}_i$ denotes the average path length of a sample i from a collection of isolation trees, and $\bar{h}$ is the average path length of an unsuccessful search, which is adapted to normalize the $\bar{h}_i$. Thus the anomaly score can be understood as the efforts to find a path in the isolated tree, where the anomalies can be identified at the early stage of exploration. By further incorporating with a false alarm rate α_I, the anomaly is defined by a binary indicator y_i, where $y_i = 1$ if $s_i < \alpha_I$ (the sample i is identified to be an anomaly) and 0 otherwise.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

2) Kullback-Leibler Divergence (KLD): The KLD [44] measures the differences between two probability distributions $p(x)$ and $q(x)$ regarding the event $x \in \mathcal{X}$, denoted by $D(p||q)$, which can be expressed as:

$$D(p||q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)} \tag{2}$$

where the $p(x)$ and $q(x)$ are assumed to represent the historical distributions of one EVSE under normal operation and DCA, respectively. Specifically, $p(x)$ is obtained based on the historical charging log data, and $q(x)$ represents the real-time charging logs. For the charging log sample x, each log can be expressed as a triple (d_i, t_i, c_i). And the anomaly is identified if the samples are associated with the KLD $D(p||q)$ larger than a pre-defined threshold α_{KLD}.

3) K-Means Clustering (KMeans): The KMeans clustering method [45] is a cluster-based algorithm that groups the input samples into K disjoint clusters based on the sample features. Specifically, we first obtain K clusters based on the historical charging log data (d_i, t_i, c_i). Next, we measure the distance between the online charging logs (d_j, t_j, c_j) and the nearest centroid of the K clusters. Given a sensitivity level of α_{KM}, we report the EVSE $i \in \mathcal{S}$ as an anomaly if more than $\alpha_{KM}\%$ of the real-time samples are associated with a distance larger than the pre-defined threshold D_{KM}.

4) Gaussian Mixture Model (GMM): The GMM is a model consisting of K separate multivariate normal distributions $\mathcal{N}(\cdot)$, known as mixture components. Each mixture component is parameterized by $\theta_k := \{\mu_k, \Sigma_k\}$, where μ_k and Σ_k represent the mean value vector and covariance matrix of the k-th mixture component. Let $\pi_k \geq 0$ be the associated weight for the k-th mixture component, where $\sum_{k=1}^{K} \pi_k = 1$. We consider the probability density function for the GMM as a weighted sum of the mixture components:

$$p(\mathbf{x}|\theta) = \sum_{k=1}^{K} \pi_k \mathcal{N}(\mathbf{x}|\mu_k, \Sigma_k) \tag{3}$$

where $\mathbf{x}$ is a collection of tuple (d_i, t_i, c_i) with the dimension $K = 3$. For the GMM-based AD technique, we define the anomaly as the samples x_i with $p(x_i|\theta) < c_G$, where c_G denotes the significance level of the GMM. An anomaly is detected if more than $\alpha_G\%$ samples for an EVSE are identified as an outlier. Note that there is no analytical solution for the parameters $\theta := \{\theta_k : k = 1, \cdots, K\}$. Instead, we can estimate the parameters θ using the Expectation-Maximization (EM) algorithm [46]. The EM algorithm proceeds by initiating a random set of parameters $\hat{\theta}$ and iteratively estimating the optimal set $\hat{\theta}^{\star}$ that can maximize the average log-likelihood given the training set $\mathbf{x}$. For the detailed implementation of the EM algorithm, we refer interested readers to Reynolds [47].

5) Principal Component Classifier (PCC): The PCC [48] first obtains the principal components from the covariance matrix of the training data (assumed as the historical charging log data under normal operation). Next, an anomaly score is assigned to each online charging event based on its deviation from the principal components. The anomaly score incorporates the *major* and *minor* components. Specifically, the former detects extreme observations (charging events with large variances). The minor components help to detect the values that are not outliers but inconsistent with the correlation structure as the normal operation. For each EVSE $i \in \mathcal{S}$, we define the EVSE i as an anomaly if over $\alpha_P\%$ of the batch of real-time charging events are associated with a significant level of c_P for either the major or minor components.

IV. Agent-Based Simulation Platform

We develop an agent-based simulator[1] to characterize the interactions between agents (SEVs) and the environment (passenger demand and EVSE ports). Our simulator has five components: matching, dispatching, repositioning, charging, and DCA unit. Specifically, the DCA unit includes the SIRS-based DCA model and AD techniques to demonstrate the robustness of DCA. In addition, we also design utility-based heuristic algorithms that guide unoccupied SEVs to the under-supply areas and match the SEVs to available EVSE. Key features in our simulator are listed below (for more detailed settings, see Qian et al. [49]).

A. DCA Unit

1) SIRS-Based DCA Model: We first assume all EVSEs are infectious after the warm-up period. The SEVs using the infectious EVSE ports will encounter a delayed charging service following the Gaussian noise $\Delta d \sim \mathcal{N}(\mu_d, \sigma_d)$ such that the charging duration is $d_i \leftarrow d_i + \Delta d$. If the infectious EVSE is detected, it will undergo the Infectious-Removed-Susceptible process, such that the EVSE can be infected again after being repaired.

2) AD Techniques for DCA Detection: The infectious EVSE can be identified as an anomaly by comparing the real-time and historical charging log information (e.g., charging duration, time of day, and initial SoC), see details in Section III-C and Algorithm 1.

B. Charging

1) Matching With EVSE Ports: We consider a utility-based heuristic such that each SEV is assigned to the EVSE with the highest utility scaled by a soft-max function. For each EVSE port $j \in \mathcal{S}$, a shorter queuing time q_j and travel time $t_{\cdot j}$ will lead to a higher utility. Specifically, for an SEV i, the probability of selecting EVSE j, $P^c(j|i)$, is shown below:

$$P^c(j|i) = \frac{\exp\left(-q_j t_{ij}\right)}{\sum_{j \in \mathcal{S}} \exp\left(-q_j t_{ij}\right)} \tag{4}$$

where $\sum_{j \in \mathcal{S}} P^c(j|i) = 1$ and $P^c(j|i) > 0$ for each location i.

2) Charging Service and Queuing: The charging service follows the first-come-first-serve rule.

3) SIRS Process: Only the EVSE in susceptible and infectious statuses can serve SEVs. If an infectious EVSE is detected for repair, the SEV in the queue will relocate to a nearby EVSE with the highest utility following Eq. (4).

[1] https://github.com/sguo28/DCA_Simulator

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

C. Repositioning

To better describe the status-quo scenario [50], we assume that the idled SEVs will reposition to an under-supplying area. Specifically, we conduct a utility-based heuristic analogous to the EVSE matching (see Eq. (4)). The utility score is calculated based on the supply-demand gap and travel time. At location j, the supply-demand gap is defined by the gap between the number of fulfilled orders (N_j^{order}) and idled SEVs (N_j^{idle}) in the past 15 min. For an empty SEV at location i, the probability of selecting location $j \in \mathcal{Z}$, $P^r(j|i)$, takes the form of a soft-max function, shown as follows.

$$P^r(j|i) = \frac{\exp\left(\frac{N_j^{\text{order}} - N_j^{\text{idle}}}{t_{ij}}\right)}{\sum_{j \in \mathcal{Z}} \exp\left(\frac{N_j^{\text{order}} - N_j^{\text{idle}}}{t_{ij}}\right)} \tag{5}$$

where $\mathcal{Z}$ denotes the set of hexagonal zones, and t_{ij} is the travel time between locations i and j.

D. Matching With Requests

We conduct a greedy matching strategy, which sequentially assigns idle vehicles to the open orders to achieve the shortest travel time within the permissible waiting time threshold. These include the idling and cruising SEVs that are traveling to the relocation destination. For the cruising SEVs, it is considered available for matching at its real-time location. After being matched, it will stop cruising and move to the assigned pick-up location.

E. Dispatching

The SEVs with assigned requests will be dispatched to the pick-up location. The idled SEV will, on the other hand, be guided to the target location with the highest utility considering the supply-demand pattern and travel time. The route is generated and processed from the Open Source Routing Machine (OSRM) engine [51], which provides the detailed real-time location for each simulation tick.

V. Numerical Experiments

A. Case Study Area

We conduct a real-world case study in NYC to demonstrate the effectiveness of the DCA model on the ESMS. In particular, we develop a high-fidelity simulation platform extended from our previous study [49]. The simulation environment is updated every minute and covers 1,347 hexagon cells (each covering an area of 0.14 square miles). We use NYC taxi data in May 2016 as the input [52], and all trips are assumed to originate and head to the centroid of the hexagon cells. In addition, we obtain the real-world locations of EVSE ports from the Alternative Fuels Data Center [53]. Note that we only consider the DCFC ports considering the system efficiency and poor accessibility for taxi drivers to home charging in NYC [5]. The travel time between each pair of centroids is obtained by overlaying with the actual road network and then querying from the OSRM engine.

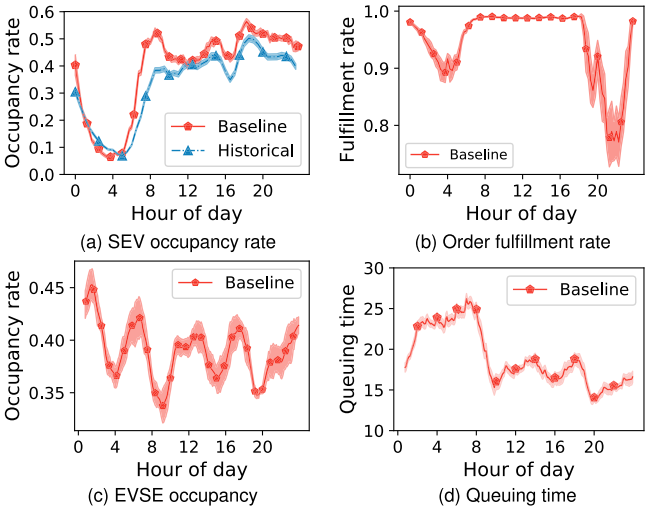


Fig. 6. Major metrics in the baseline scenario.

We perform a downscaled status-quo experiment of the taxi system by randomly sampling 25% of the historical trip record (around 130,000 trips). As existing EVSE facilities can hardly support the charging demand of the 100% electrified SEV fleet [5], we also consider enlarging the number of charging piles of the real-world charging stations [53]. To find the best combination of the SEV fleet size, demand, and the number of EVSE ports, we conduct a cross-validation procedure by first fixing 25% of the taxi trip demand and tuning the fleet size from 1,300 to 1,500, incremented by 50 and increasing the number of EVSE by 1.5 to 3.0 times stepped by 0.5. The best combination consists of 1,400 SEVs and 215 DC Fast EVSE ports to serve 25% of real-world daily taxi trips. The baseline scenario is justified by real-world evidence (see Figs. 6a-6c) Unless otherwise specified, available SEVs will be dispatched to passengers that can be reached within 20 min, and the maximum waiting time for passengers is 10 min. Finally, we consider a 4-week simulation using three random seeds, where the first week is regarded as a warm-up, and the other three weeks are the validation period. The DCA is launched at the end of the warm-up.

B. Parameter Setting

We summarize in Table II the parameter setting in this study, including SEV, mobility service, and the SIRS process.

Specifically, we adopt the prototype of the Tesla Model 3 for the electric mobility service [60], which is supported by both Tesla Supercharging and CCS EVSE ports. Based on the field experiment by Moloughney [56], it took 32 min for a Tesla Model 3 to reach 80% SoC and another 31 min for a full charge, where the charging rate for the first 80% is observed to be approximately linear. Such a linear charging profile is also validated by the in-vehicular database [57], which reports an average charging rate of 3.3 %SoC/min (5.13 miles/min) for our prototype. For the DCA model, a higher sensitivity level ($\alpha_{(\cdot)}$) results in a more sensitive AD, which may effectively identify the anomaly but incur a higher repair cost (e.g., sending out technician labor to inspect and repair).

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

TABLE II
PARAMETER ASSUMPTION

Item	Assumptions	Ref.
SEV		
SEV prototype	2019 Tesla Model 3 Standard Range	[54]
Charging profile	Constant charging rate under an SoC below 80%	[55], [56]
Target SoC	$\mathcal{N}(0.78, 0.02)$ bounded by 0.80	-
Charging rate	5.13 mile/min	[57]
Battery capacity	50 kWh for 220 miles	[57], [54]
Mobility service		
Payment	$\$0.631 \times \Delta\text{dist} + \$0.287 \times \Delta\text{time}$	[49], [58]
SIRS process		
Transmission rate β	0.1	-
Recovery rate γ	Related to AD techniques	Sec. III-C
Repair rate τ	1/3 hours	[59]

TABLE III
CROSS-VALIDATION FOR AD TECHNIQUES

AD	Range of $\alpha_{(\cdot)}$	Hyperparameters
IF (α_I)	0.05 to 0.15 by 0.025	-
KLD (α_{KLD})	1 to 5 step by 1	-
KMeans (α_{KM})	0.2 to 0.6 step by 0.1	$D_{KM} = 2.5$
GMM (α_G)	0.05 to 0.55 step by 0.1	$c_G = 0.01$
PCC (α_P)	0.3 to 0.8 step by 0.1	$c_P = 0.005$

To compromise the EVSE, we make a conservative assumption based on real-world evidence [36]. The susceptible EVSE is infected by manually inserting a USB drive every 30 min with a transmission rate of $\beta = 0.1$. The AD algorithm is conducted every 30 min, and the technicians for repair service are sent out for on-site assistance every 30 min. The whole repair process for an EVSE port is set as $\tau = 3$ hours. According to the Avista EVSE pilot report [59], we assume that the MTTR is 15 days to address the issue completely and the average cost to repair is \$214 (including the warranty and non-warranty labor and material costs). We note that multiple times of on-site assistance (e.g., power cycling, inspection, repair, or replacement) are required to fully resolve the issue [59]. Therefore, the repair cost is estimated to be \$1.78 per time.

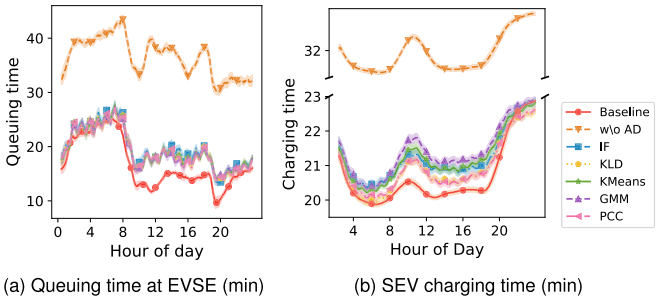
C. Simulation Scenarios

We present the detailed scenario design considering the different time delays for the charging service from 5 min to 15 min and the sensitivity levels of the AD algorithms ($\alpha_{(\cdot)}$). We will consider three types of experiments: (1) baseline, (2) DCA without AD, and (3) DCA with AD. The attack-free baseline scenario is to justify the downscaled status quo under normal operation. We also compare the scenarios under DCA with and without the AD to explore the trade-off between repair cost and improvement of the system performance. Finally, we conduct sensitivity analyses on the AD techniques. The range of $\alpha_{(\cdot)}$ is determined by a cross-validation procedure, where the parameter settings are shown in Table III.

VI. RESULTS

A. Baseline Scenario

This subsection presents the dynamics in the baseline scenario using real-world data. As seen in Figs. 6a-6d, we show four primary metrics to justify the status quo simulation experiment, including (1) SEV occupancy rate, (2) order fulfillment rate, (3) EVSE occupancy rate, and (4) SEV queuing time at EVSE. Fig. 6a compares the SEV's occupancy rate with the historical NYC taxi fleet [61]. The simulation results are observed to agree with the historical records, where the overall occupancy rate varies from less than 0.1 during 3 - 6 AM to nearly 50% during the evening peak. The slightly higher occupancy rates in the simulation may result from the undersupply of the SEV fleet. In addition, we report an admissible fulfillment rate of nearly 100% during the daytime and over 75% during the evening peak (6 - 11 PM). Moreover, the validity of the EVSE occupancy rate and the SEV queuing time is confirmed by the real-world practice of the fully electrified taxi fleet in Shenzhen, China. In this case, an EVSE occupancy rate from 10% to 80% [62] and a queuing time of 10 min to 40 min [63] are considered to be plausible. Despite the different taxi market settings between NYC and Shenzhen, we believe that the charging dynamics in our simulation platform are permissible in the real-world ESMS, which can sufficiently justify our baseline scenario.



(a) Queuing time at EVSE (min) (b) SEV charging time (min)

Fig. 7. Charging dynamics under the baseline scenario and 10 min delay.

B. System Performance of EVSE

We next present the daily-average charging dynamics over the three-week period under the DCA, including queuing time at EVSE and charging duration, shown in Figs. 7a-7b. Specifically, Fig. 7a shows the queuing time of a SEV at an EVSE port. We will consider three cases: baseline, the DCA with and without AD under a fixed delayed charging time of 10 min. For the baseline scenario, we observe two peaks during the early morning period (e.g., 6 - 8 AM) and the late afternoon period (around 4 PM), with the longest queuing time exceeding 22 min compared with the shortest queuing time of about 10 min. After launching DCA with a 10 min delay, an additional queuing time of over 15 min is observed during the noon period and even nearly 20 min during the early morning period (e.g., 7-8 AM). The extended queuing time is due to the cascading effects. For instance, one SEV may relocate to the EVSE with the higher utility (e.g., average queuing time and travel time) after exceeding a queuing time threshold, which accelerates the snowballing of the excessive queuing time. With the AD techniques, the queuing time is greatly reduced by over 10 min. However, there still exists space for improvement during the daytime, especially during the daytime (9 AM - 5 PM). This is because there exists a

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

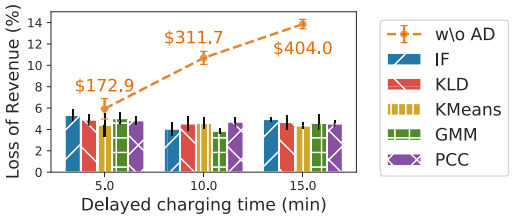


Fig. 8. Comparison of total revenue during the last (4th) week in simulation.

proportion of EVSE that is removed for repair and out-of-service for at least $\tau = 3$hours. In this regard, the SEVs in the queue have to relocate to other EVSE ports, resulting in local congestion at the EVSE ports in S and I statuses. As seen in Fig. 7b, the charging duration can be reduced from over 30 min to relatively the same levels as the baseline under all five AD techniques. Compared with the early morning and evening periods, the average delays in charging service are observed to be longer at around 6 AM and 2 PM, potentially due to a higher proportion of infectious EVSE ports.

C. System Performance for SEV Fleet

This subsection shows the SEV driver's weekly revenue loss under different lengths of charging delay with and without the AD models. To better understand the degradation of the mobility service, we also present two major dynamics, including order fulfillment rate and SEV occupancy rate.

Fig. 8 displays the system revenue loss during the last week in our simulation to capture the long-term impact of the DCA. One immediate observation is the strong linear relationship between delayed charging time and revenue loss. Specifically, without the AD, we report a system revenue loss of at least \$172.9 (5.9%), \$311.7 (10.7%), and up to \$404.0 (13.9%) under the delay of 5, 10, and 15 min, respectively. With a delay of 15 min, the system revenue loss can be reduced to about \$140.1 (4.8%) comparing all five AD techniques. Furthermore, our results show that for both IF and GMM, the revenue losses initially decrease when the delay in charging time is between 5 to 10 minutes, but start to increase as the delay grows from 10 to 15 minutes. This suggests that as the extended charging time increases, it may result in more severe charging delays at the system level, while also making it more susceptible to detection as the charging duration deviates further from the normal operation. This highlights the importance of carefully balancing between DCA's efficacy and robustness. Finally, despite the improvement in a system revenue loss of up to 8.6% (from 13.9% to 5.9%), the underlined repair cost may grow exponentially with longer delay of charging, which will be evidenced in Fig. 11.

Figs. 9a-9b illustrate the order fulfillment and SEV fleet's occupancy rates under the baseline and the DCA with and without AD. For the scenarios under AD, we only show the results of the KLD, which is observed to be one of the most effective AD techniques in Fig 8. In Fig. 9a, distinct differences between the baseline and scenarios without the AD are observed during the morning and evening peaks (e.g., 8 to 10 AM and 6 to 11 PM). In this case, we report a reduction of fulfillment rates of about 20% during the morning

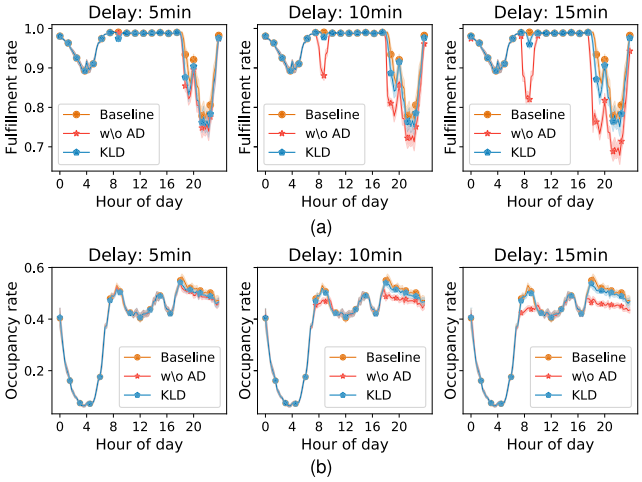


Fig. 9. Dynamics of electric mobility service during the last (4th) week in simulation: (a) order fulfillment rate and (b) SEV fleet's occupancy rate.

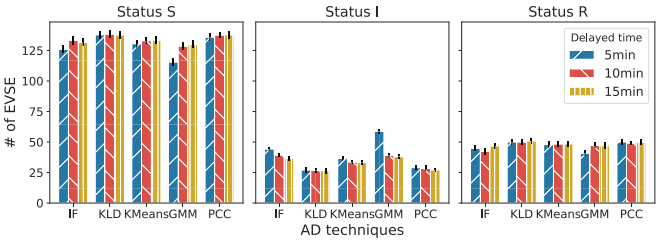


Fig. 10. Proportion of EVSE in statuses S, I, and R under five AD techniques.

peak and 12% during the evening peak, yielding fulfillment rates of 80% and 67%, respectively. Similarly, the reduction of SEV occupancy rates varies from 2% to 6% under the delay of 5 min and 15 min from 6 PM to 11 PM. Under the PCC, we report an improvement in fulfillment rate of up to 8% and a SEV occupancy rate as high as 5% under the delay of 15 min.

D. Impacts of EVSE

We illustrate in Fig. 10 the SIR proportions of EVSE under different delays and AD techniques during the 4th week.

In general, the numbers of susceptible (status S) EVSE under 5 min delay are lower than those under 10 min and 15 min delay. In particular, under a 5 min delay, the IF and GMM are associated with the lowest number of susceptible EVSE, which implies the relatively higher revenue loss in Fig. 8. At the same time, significantly higher proportions of infectious EVSE and lower proportions of removed EVSE are observed under the IF and GMM, especially with the delay of 5 min. This can be explained by the stealthiness of DCA, which can hardly be detected by the AD techniques mentioned above. In addition, the numbers of removed EVSE under 15 min delay are reported to be higher than those under 10 min delay. In this case, the higher proportion of removed EVSE results in a higher revenue loss, as observed in Fig. 8, and lower fulfillment rates and occupancy rates in Fig. 9.

E. Performance of AD Techniques

Table IV reports the performance between the five AD techniques: accuracy, precision, recall, and F1 score.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

TABLE IV
COMPARISON BETWEEN FIVE AD TECHNIQUES

	5 min				10 min				15 min			
AD	Accuracy	Precision	Recall	F1	Accuracy	Precision	Recall	F1	Accuracy	Precision	Recall	F1
IF	0.73(0.01)	0.82(0.01)	0.74(0.01)	0.78(0.01)	0.80(0.01)	0.81(0.01)	0.85(0.01)	0.83(0.01)	0.80(0.01)	0.82(0.01)	0.86(0.01)	0.84(0.01)
KLD	**0.86(0.05)**	0.86(0.05)	**0.99(0.0)**	**0.92(0.03)**	**0.87(0.01)**	**0.88(0.01)**	**0.99(0.0)**	**0.93(0.0)**	0.85(0.01)	0.86(0.01)	**0.99(0.00)**	**0.92(0.01)**
KMeans	0.78(0.01)	0.84(0.00)	0.86(0.01)	0.85(0.00)	0.82(0.00)	0.84(0.00)	0.91(0.00)	0.88(0.00)	0.81(0.00)	0.84(0.00)	0.91(0.00)	0.87(0.00)
GMM	0.64(0.01)	0.81(0.00)	0.57(0.02)	0.67(0.02)	0.77(0.01)	0.79(0.01)	0.78(0.02)	0.78(0.01)	0.79(0.00)	0.79(0.01)	0.80(0.01)	0.79(0.01)
PCC	0.85(0.00)	**0.87(0.00)**	0.98(0.00)	**0.92(0.00)**	0.85(0.00)	0.86(0.00)	0.98(0.00)	0.92(0.00)	**0.86(0.00)**	**0.87(0.00)**	0.98(0.00)	**0.92(0.00)**

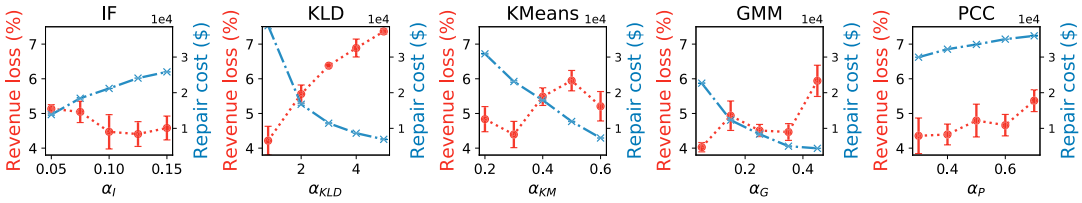


Fig. 11. Trade-off between revenue loss and repair cost under a delay of 10 min over a three-week period.

We note that the KLD and PCC outperform the other AD techniques under different charging delays, where the accuracy and precision are over 0.86 and F1 scores are at least 0.92. In particular, the recall can reach up to 0.99, which suggests a significantly low miss-detection rate (as low as 1%). The superior performance of KLD and PCC can be explained by the non-parametric features, where no prior assumptions are made on the sample distribution. In particular, the low-rank approximation under the PCC exhibits the great potential of identifying the anomaly, especially for large-scale problems. In addition to the PCC, we also report good performances under the KMeans. In this case, all metrics are over 0.80 under the 10 min and 15 min delay. Also, we observe that the precision and recall exceed 0.80 in all cases, indicating a good performance regarding the false-positive and miss-detection rates. As a clustering-based technique, high-quality clusters are obtained based on the historical data under normal operation. The outliers are likely to be associated with high anomaly scores (i.e., long distance to the cluster).

F. Sensitivity Analysis

To better understand the trade-off between repair cost and system revenue loss, we conduct sensitivity analyses on the AD techniques with respect to $\alpha_{(\cdot)}$ (the ranges for the cross-validation procedure were detailed in Table III). We summarize the repair cost and revenue loss under the 10 min delay in Fig. 11. We first observe that the higher sensitivity levels lead to linearly or even exponentially increasing repair costs, ranging from about $6,000 (KMeans) to nearly $40,000 (KLD and PCC). This is because the AD models aim to perform more sensitive DCA detection by grouping more charging events as anomalies, resulting in higher repair costs to send out a technician for repair service. At the same time, the revenue loss (red dotted lines) witnessed an overall reduction with significantly higher repair costs due to more sensitive detection. However, the revenue loss remains at least 4% in all five AD models regardless of the repair cost, which suggests the robustness of the DCA model. Observing the trade-off between repair cost and revenue loss, we note that a slight compromise on the revenue loss can result in a significantly lower repair cost, e.g., $\alpha_I = 0.05, 0.075$, $\alpha_{KLD} = 1, 2$, and $\alpha_P = 0.3, 0.4$. Those trade-off decisions will shed light on the coordinated management of SEV and EVSE for commercial purpose [64]. We highlight that there will always be a proportion of infectious EVSEs serving the SEV fleet, resulting in huge revenue loss regardless of the sensitivity levels of the DCA detection models. Meanwhile, more sensitive detection may not contribute to more successful detection but lead to exponentially increasing repair costs and higher miss-detection rates (proportion of false-positive and false-negative alarms). In this regard, we alert more tailored AD models that can best balance the trade-off between system revenue and repair cost.

VII. CONCLUSION

This study presents a novel DCA model that can surreptitiously impede the ESMS by delaying the charging service of the SEV fleet. By utilizing the NYC taxi trip data and real-world EVSE locations, we evaluated the system impacts of the DCA on the ESMS in NYC using a self-developed high-fidelity simulation platform. Our results demonstrate a long-term degradation of the ESMS caused by the DCA, with a 10 min delay resulting in up to 35% longer queuing times at EVSE during the daytime (11AM - 6PM) and up to 6.8% longer average charging times at around 10AM. Furthermore, such a disruption to the charging service leads to an 8% increase in unfulfilled requests, which results in a 10.7% ($311.7) weekly revenue loss per SEV driver. Even with the AD techniques, our results show that the weekly revenue loss remains at a minimum of 3.8% ($111.8), along with increased repair costs of up to $36,000 per week. Therefore, our DCA model highlights a realistic and stealthy cyberattack approach that can chronically harm the ESMS. In conclusion, this study contributes to the field of cybersecurity by introducing a new cyberattack approach and providing insights into the system-level impacts of the DCA on the ESMS.

Future research should focus on incorporating a more realistic EVSE choice model to better understand the impacts of DCA and its cascading failures. For instance, the SEV

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

may detour to a relatively distant EVSE due to the preference [65]. Additionally, tailored defense strategies should be developed to effectively identify malfunctioned EVSEs, even under minimal disruptions in charging service (e.g., a 2 min delay). This is especially relevant to the increasing prevalence of high-wattage EVSEs (e.g., extreme fast chargers [29]) and heavy-duty electric trucks in the ESMS. Moreover, SEV drivers may have different target SoC levels (e.g., above or below 80%) due to time constraints, which can result in a non-linear CC-CV charging profile. Future studies should incorporate this factor to simulate more realistic charging behaviors. Finally, battery degradation [66] is an important consideration that adds another layer of variability to charging duration beyond human-involved activities. Incorporating battery degradation in our future research will make our proposed DCA approach even more robust and applicable to real-world scenarios.

ACKNOWLEDGMENT

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, and the U.S. Government assumes no liability for the contents or use thereof.

REFERENCES

[1] X. Qian, T. Lei, J. Xue, Z. Lei, and S. V. Ukkusuri, "Impact of transportation network companies on urban congestion: Evidence from large-scale trajectory data," *Sustain. Cities Soc.*, vol. 55, Apr. 2020, Art. no. 102053.

[2] A. Jenn, "Emissions benefits of electric vehicles in Uber and Lyft ride-hailing services," *Nature Energy*, vol. 5, no. 7, pp. 520–525, Jun. 2020.

[3] T. Lei, S. Guo, X. Qian, and L. Gong, "Understanding charging dynamics of fully-electrified taxi services using large-scale trajectory data," *Transp. Res. C, Emerg. Technol.*, vol. 143, Oct. 2022, Art. no. 103822.

[4] THE CITY OF NEW YORK. (2023). *Mayor Adams Outlines 'Working People's Agenda' for NYC in Second State of the City Address*. Accessed: Jan. 2023. [Online]. Available: https://www.nyc.gov/office-of-the-mayor/news/063-23/mayor-adams-outlines-working-people-s-agenda-nyc-second-state-the-city-address

[5] M. Moniot, Y. Ge, and E. Wood, "Estimating fast charging infrastructure requirements to fully electrify ride-hailing fleets across the United States," *IEEE Trans. Transport. Electrific.*, vol. 8, no. 2, pp. 2177–2190, Jun. 2022.

[6] Open Charge Allianc. (2022). *Open Charge Alliance—OCPP*. Accessed: Jul. 2022. [Online]. Available: https://www.openchargealliance.org/

[7] EV Roaming Foundation. (2022). *OCPI Background*. Accessed: Jul. 2022. [Online]. Available: https://evroaming.org/ocpi-background/

[8] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Demo: End-to-end wireless disruption of CCS EV charging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2022, pp. 3515–3517.

[9] CybersecurityHelp. (2021). *Multiple Vulnerabilities in Texas Instruments Simplelink*. Accessed: Jul. 2022. [Online]. Available: https://www.cybersecurity-help.cz/vdb/SB2021050304

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

[11] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[12] Y. Liu, O. Ardakanian, I. Nikolaidis, and H. Liang, "False data injection attacks on smart grid voltage regulation with stochastic communication model," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 7122–7132, May 2023.

[13] J. Su, C. Xie, P. Dehghanian, and S. Mehrani, "Optimal defense strategy against load redistribution attacks under attacker's resource uncertainty: A trilevel optimization approach," in *Proc. IEEE PES Grid Edge Technol. Conf. Expo.*, Apr. 2023, pp. 1–5.

[14] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[15] J. Thai, C. Yuan, and A. M. Bayen, "Resiliency of mobility-as-a-service systems to denial-of-service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 370–382, Mar. 2018.

[16] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "On the cybersecurity of traffic signal control system with connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16267–16279, Sep. 2022.

[17] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.

[18] X. Zhao, S. Zou, and Z. Ma, "Decentralized resilient H_∞ load frequency control for cyber-physical power systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 11, pp. 1737–1751, Nov. 2021.

[19] J. Zhang, L. Pan, Q. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[20] A. R. Javed et al., "Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey," *Sensors*, vol. 22, no. 12, p. 4394, Jun. 2022.

[21] 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.

[22] 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.

[23] E. Gumrukcu et al., "Impact of cyber-attacks on EV charging coordination: The case of single point of failure," in *Proc. 4th Global Power, Energy Commun. Conf. (GPECOM)*, Jun. 2022, pp. 506–511.

[24] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, no. 11, p. 3931, May 2022.

[25] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability," *Energies*, vol. 16, no. 3, p. 1113, Jan. 2023.

[26] J. Johnson. (2019). *Securing Vehicle Charging Infrastructure*. Accessed: Jul. 2022. [Online]. Available: https://www.osti.gov/servlets/purl/1644893

[27] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102511.

[28] Texas Intruments. (2021). *Multiple Vulnerabilities in Texas Instruments Simplelink*. Accessed: Jul. 2022. [Online]. Available: https://www.ti.com/solution/dc-charging-pile-station

[29] ND. (2022). *Developing Infrastructure to Charge Electric Vehicles*. Accessed: Jun. 2022. [Online]. Available: https://afdc.energy.gov/fuels/electricity_infrastructure.html

[30] B. Jar, A. Miller, and N. Watson, "Rapid EV chargers: Implementation of a charger," presented at the EEA Conf. Exhib., Wellington, New Zealand, Jun. 2016. [Online]. Available: https://ir.canterbury.ac.nz/bitstream/handle/10092/15517/2016%20Rapid%20EV%20Chargers%20-%20Jar.pdf and https://www.researchgate.net/publication/319162700_Rapid_EV_Chargers_Implementation_of_a_Charger

[31] K. W. E. Cheng, B. P. Divakar, H. Wu, K. Ding, and H. F. Ho, "Battery-management system (BMS) and SOC development for electrical vehicles," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 76–88, Jan. 2011.

[32] EVgo. (2023). *Reserve a Fast Charging Session—EVgo*. Accessed: Jan. 2023. [Online]. Available: https://www.evgo.com/reservations/

[33] EVmatch. (2023). *Find and Reserve Charging for Your Electric Vehicle—EVmatch*. Accessed: Jan. 2023. [Online]. Available: https://www.evmatch.com/solutions/charging

[34] R. Currie, "Hacking the CAN bus: Basic manipulation of a modern automobile through CAN bus reverse engineering," SANS Reading Room, White Paper, Jun. 2017. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/paper/37825

[35] K. Harnett et al., "DOE/DHS/DOT Volpe technical meeting on electric vehicle and charging station cybersecurity report," John A. Volpe Nat. Transp. Syst. Center, U.S. Dept. Transp., Cambridge, MA, USA, Tech. Rep. DOT-VNTSC-DOE-18-01, 2018.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.

[36] B. Carlson and K. Rohde, "Cyber security of DC fast charging: Potential impacts to the electric grid," Idaho Nat. Lab., Idaho Falls, ID, USA, Tech. Rep. INL/MIS-18-51289, 2018.

[37] K. W. Rohde, "Cyber security of DC fast charging: Potential impacts to the electric grid," Idaho Nat. Lab. (INL), Idaho Falls, ID, USA, Tech. Rep. INL/CON-18-52242-Rev000, Jan. 2019.

[38] 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. 200–207, May 2020.

[39] 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.

[40] M. Antonakakis et al., "Understanding the Mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[41] X. Song, M. Wu, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 631–645, May 2007.

[42] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *Proc. 8th IEEE Int. Conf. Data Mining*, Dec. 2008, pp. 413–422.

[43] M. Elnour, N. Meskin, K. Khan, and R. Jain, "Application of data-driven attack detection framework for secure operation in smart buildings," *Sustain. Cities Soc.*, vol. 69, Jun. 2021, Art. no. 102816.

[44] S. Kullback and R. A. Leibler, "On information and sufficiency," *Ann. Math. Statist.*, vol. 22, no. 1, pp. 79–86, 1951.

[45] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: A K-means clustering algorithm," *J. Roy. Stat. Soc. C*, vol. 28, no. 1, pp. 100–108, 2010.

[46] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm," *J. Roy. Stat. Soc., B*, vol. 39, no. 1, pp. 1–22, 1977.

[47] D. A. Reynolds, "Gaussian mixture models," *Encyclopedia Biometrics*, vol. 741, nos. 659–663, Jul. 2009.

[48] M. L. Shyu, S. C. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," in *Proc. ICDM Found. New Directions Data Mining Workshop*, 2003, pp. 171–179. [Online]. Available: https://www.biostat.wisc.edu/~page/ICDM_Workshops/Foundations-workshop.pdf

[49] X. Qian, S. Guo, and V. Aggarwal, "DROP: Deep relocating option policy for optimal ride-hailing vehicle repositioning," *Transp. Res. C, Emerg. Technol.*, vol. 145, Dec. 2022, Art. no. 103923.

[50] A. Millard-Ball, L. Liu, W. Hansen, D. Cooper, and J. Castiglione, "Where ridehail drivers go between trips: Trading off congestion and curb availability?" Dept. Environ. Stud., UC Santa Cruz, Santa Cruz, CA, USA, Tech. Rep. UC-ITS-2020-15, 2021.

[51] D. Luxen and C. Vetter, "Real-time routing with OpenStreetMap data," in *Proc. 19th ACM SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst.*, New York, NY, USA, Nov. 2011, pp. 513–516.

[52] The New York City Taxi and Limousine Commission. (2021). *2016 NYC Yellow Taxi Trip Record Data*. Accessed: Apr. 2021. [Online]. Available: https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page

[53] ND. (2022). *Alternative Fuels Data Center: Electric Vehicle Charging Station Locations*. Accessed: Jun. 2022. [Online]. Available: https://afdc.energy.gov/fuels/electricity_locations.html#/find/nearest?fuel=ELEC

[54] ND. (2022). *2019 Tesla Model 3 Standard Range*. Accessed: Jun. 2022. [Online]. Available: https://www.fueleconomy.gov/feg/Find.do?action=sbs&id=41415

[55] Y. Zheng, Z. Shao, Y. Zhang, and L. Jian, "A systematic methodology for mid-and-long term electric vehicle charging load forecasting: The case study of Shenzhen, China," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102084.

[56] Moloughney. (2021). *How Fast Does a 2021 Tesla Model 3 Charge? We Find Out*. Accessed: Jul. 2022. [Online]. Available: https://insideevs.com/news/506520/tesla-model-3-supercharger-test/

[57] EV Database. (2022). *Tesla Model 3 Standard Range*. Accessed: Jul. 2022. [Online]. Available: https://ev-database.uk/car/1060/Tesla-Model-3-Standard-Range

[58] The New York City Taxi and Limousine Commission. (2018). *Driver Income Rules*. Accessed: Jul. 2022. [Online]. Available: https://www1.nyc.gov/assets/tlc/downloads/pdf/driver_income_rules_12_04_2018.pdf

[59] R. Farley, M. Vervair, and J. Czerniak, "Electric vehicle supply equipment pilot final report," Washington Utilities Transp. Commission (UTC), Tech. Rep., 2019. [Online]. Available: https://www.myavista.com/-/media/myavista/content-documents/energy-savings/electricvehiclesupplyequipmentpilotfinalreport.pdf

[60] F. Lambert. (2021). *Tesla Model 3 Becomes More Popular as NYC Yellow Cab*. Accessed: Jan. 2023. [Online]. Available: https://electrek.co/2021/04/02/tesla-model-3-becomes-more-popular-nyc-yellow-cab/

[61] The New York City Taxi and Limousine Commission. (2016). *TLC Factbook*. Accessed: Jul. 2022. [Online]. Available: https://www1.nyc.gov/assets/tlc/downloads/pdf/2016_tlc_factbook.pdf

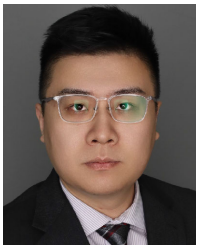
[62] G. Wang et al., "SharedCharging: Data-driven shared charging for large-scale heterogeneous electric vehicle fleets," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 3, no. 3, pp. 1–25, Sep. 2019.

[63] Z. Dong, C. Liu, Y. Li, J. Bao, Y. Gu, and T. He, "REC: Predictable charging scheduling for electric taxi fleets," in *Proc. IEEE Real-Time Syst. Symp. (RTSS)*, Dec. 2017, pp. 287–296.

[64] Blink Charging. (2022). *Electric Fleets: EVS for Businesses*. [Online]. Available: https://blinkcharging.com/electric-fleets-evs-for-businesses/

[65] Y. Guo, X. Qian, T. Lei, S. Guo, and L. Gong, "Modeling the preference of electric shared mobility drivers in choosing charging stations," *Transp. Res. D, Transp. Environ.*, vol. 110, Sep. 2022, Art. no. 103399.

[66] Y. Zhao, Z. Wang, Z.-J.-M. Shen, and F. Sun, "Assessment of battery utilization and energy consumption in the large-scale development of urban electric vehicles," *Proc. Nat. Acad. Sci. USA*, vol. 118, no. 17, Apr. 2021, Art. no. e2017318118.



Shuocheng Guo received the B.E. degree in civil engineering from Central South University, Changsha, China, and the M.S. degree in transportation engineering from the University of Illinois at Urbana–Champaign, Urbana, IL, USA. He is currently pursuing the Ph.D. degree in transportation engineering with The University of Alabama, Tuscaloosa, AL, USA. His research interests include combinatorial optimization, electrified transportation networks, and urban computing.

Hanlin Chen received the B.S. degree in electrical engineering and automation from the Huazhong University of Science and Technology, Wuhan, Hubei, China, and the M.S. degree in mechanical engineering technology and the Ph.D. degree in computer and information technology from Purdue University, West Lafayette, IN, USA. She is currently a Post-Doctoral Research Assistant in civil engineering with Purdue University. Her research interests include cooperative perception, traffic-informed perception, planning on vehicle side, cybersecurity and resilience in CDA systems, and CAV in homeland security.

Mizanur Rahman (Member, IEEE) is currently an Assistant Professor with the Department of Civil, Construction and Environmental Engineering, The University of Alabama, Tuscaloosa, AL, USA. After his graduation in August 2018, he joined as a Post-Doctoral Research Fellow with the Center for Connected Multimodal Mobility (C^2M^2), a U.S. Department of Transportation Tier 1 University Transportation Center (cecas.clenson.edu/c2m2). After that, he has also served as the Assistant Director of C2M2. His research interests include traffic flow theory, and transportation cyber-physical systems for connected and automated vehicles and smart cities.

Xinwu Qian received the B.S. degree in transportation engineering from Tongji University, Shanghai, China, and the M.S. and Ph.D. degrees in transportation engineering from Purdue University, West Lafayette, IN, USA. He is currently an Assistant Professor with the Department of Civil, Construction and Environmental Engineering, The University of Alabama. His research interests include big data analytics, complex network analysis, and network modeling and optimization.

Authorized licensed use limited to: the Leddy Library at the University of Windsor. Downloaded on July 13,2024 at 06:34:01 UTC from IEEE Xplore. Restrictions apply.