2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) | 979-8-3503-4793-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/DSN58367.2023.00042

Detection of e-Mobility-based Attacks on the Power Grid

Dustin Kern
Darmstadt University of Applied Sciences
Darmstadt, Germany
dustin.kern@h-da.de

Christoph Krauß
Darmstadt University of Applied Sciences
Darmstadt, Germany
christoph.krauss@h-da.de

***Abstract*—The increasing use of information and communication technology in power grids and connected e-mobility infrastructures enables cyber attacks. E-mobility infrastructure components such as Charge Points (CPs) or Electric Vehicles (EVs) could be used as attack vector on power grids via False Data Injection (FDI) or Manipulation of demand (Mad) attacks. To detect such attacks, Intrusion Detection Systems (IDSs) which are adapted to the specifics of e-mobility are required. In this paper, we propose a novel hybrid IDS for detecting e-mobility-based attacks on the power grid consisting of a rule-based IDS and an anomaly detection component using regression-based forecasting. The IDS is distributed among different e-mobility-related backend systems, namely Charge Point Operators (CPOs) and grid operators. We implemented our IDS and evaluate it on several data sets while simulating realistic attack scenarios to show the effectiveness of our approach. Our evaluation compares different IDS design choices and regression models. Especially, decision tree regression proved to be an effective base for detection at CPOs. By combining the distributed IDS reports of individual CPOs at the grid operator, the overall detection performance is further improved. The distributed nature of the system allows it to identify large-scale attacks effectively and thus robustly detect realistic threats to power grid operation.**

***Index Terms*—E-Mobility, Smart Grid, Intrusion Detection System, False Data Injection, Manipulation of Demand**

I. Introduction

Power grids are critical infrastructures whose disruption would have significant consequences such as blackouts. Since information and communication technology is used for intelligent grid control, e.g., to adapt grid load to the fluctuating generation from renewable energies, cyber attacks are a serious threat [1], [2]. Connecting the e-mobility infrastructure to the power grid creates new and realistic attack vectors as can be seen in the assessments from science [3]–[6] and industry [7]. These attack vectors can be classified as False Data Injection (FDI) and Manipulation of demand (Mad) attacks. FDI attacks target the state estimation of the grid and can thus lead to instabilities. Mad attacks directly alter the load on the grid and can thus cause overload scenarios.

An attacker who controls a large number of Charge Points (CPs) and/or Electric Vehicles (EVs) can, for instance, attempt to disrupt the power grid with synchronized charging loads. Notably, control over a large enough number of CPs and/or EVs could be gained via a remotely exploitable vulnerability and the existence of such vulnerabilities is not uncommon due to the high complexity of these systems (cf., e.g., [8], [9]). Afterwards, different attack strategies are possible, such as, a direct manipulation of the charging load profile (by CPs) or a shift of charging load into peak times (by CPs and/or EVs).

Ensuring cyber resiliency of power grids under attacks via e-mobility is a major challenge. Cyber resiliency is defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" [10]. A general approach for cyber resiliency is the detection of attacks by means of Intrusion Detection Systems (IDSs). An IDS generally serves as a second line of defense, i.e., to provide some kind of security even if an attack has successfully breached prior protections. With regard to the mentioned attack vectors, intrusion detection is especially relevant since an adversary with control over CPs and/or EVs could repeatedly attack the grid to counteract any recovery activities and thus cause even greater harm to the resilience of this critical infrastructure.

In this paper, we propose an approach for detecting e-mobility-based attacks on the power grid, with the following main contributions: *(i)* We analyze representative EV charging protocols for the potential influence of different actors on the scheduling of charge sessions (regarding charge speed, -amount, -time etc.). *(ii)* We provide a detailed analysis of attack vectors via e-mobility on the power grid under consideration of existing protocols, processes, and security measures. *(iii)* We propose a novel hybrid IDS for detecting attacks on the power grid via e-mobility. The hybrid approach consists of a rule-based IDS for detecting simple attacks and an anomaly detection component for detecting advanced attacks. The IDS is distributed across different e-mobility-relevant backend systems allowing for an efficient detection of large-scale attacks. *(iv)* We implement our IDS, compare different design choices, and simulate different attacks to evaluate detection rates. The simulation of attacks is based on our analysis of realistic attack vectors and uses different base data sets, including multiple public data sets of real CP charge sessions. *(v)* We release our simulated attack data sets (cf. Footnote 1 in Section VI).

The paper is structured as follows: we distinguish our work from related work in Section II. In Section III we derive our system model and in Section IV we motivate the adversary model. We introduce our concept of an IDS for e-mobility in Section V and describe the implementation and evaluation in Section VI. Finally, we conclude the paper in Section VII.

2158-3927/23/$31.00 ©2023 IEEE
DOI 10.1109/DSN58367.2023.00042

II. Related Work

In this section, we discuss related work on cyber attacks and IDS approaches in the context of power grids and e-mobility. Additionally, we identify work on e-mobility machine learning with relevance to IDS. Finally, we discuss open issues in the applicability of smart grid IDS work or e-mobility machine learning to the context of an e-mobility-specific IDS.

A. Cyber Attacks on the Grid

The successful cyber attacks on the Ukrainian power grid in 2015 and 2016 [11], [12] have shown that security is important for any communication or control mechanisms related to the power grid. The effect of cyber attacks to grid stability is analyzed in several papers (e.g., [13]–[15]). For instance, [15] shows that a botnet of high wattage Internet of Things (IoT) devices can be used to manipulate the power demand and disrupt normal grid operation by the use of so-called Manipulation of demand via IoT (MadIoT) attacks.

Several papers investigate the potential of e-mobility-based attacks on the power grid. The general possibility of such attacks is discussed in [16], [17]. In [3]–[6] different simulation-based studies are performed to analyze the specific effects of an e-mobility demand-side attack on the grid. All studies show that attacks can lead to negative consequences (frequency instability, line outages, etc.) assuming a high enough penetration of EVs and a large scale adversarial compromise.

B. Intrusion Detection in Power Grids

Intrusion detection is commonly identified as an important component in securing critical infrastructures such as power grids. Applications include IDSs for the grid's control systems, substations, and metering infrastructure [18], [19]. Several papers propose IDSs for the detection of generic network attacks (Denial of Service (DoS), unauthorized access, probing, etc.; e.g., using the KDD99 data set [20]) in the grid context. For example, [21], [22] propose an IDS for different grid layers, [23] evaluates several data stream classifiers for metering data, and [24] proposes a rule-based IDS for the DNP3 protocol.

However, since grids are cyber-physical systems, a consideration of generic network attacks alone is not sufficient. Instead, it is also important to consider attacks related to the physical state of the system. Several papers propose IDS for respective attacks (FDI and Mad attacks). For example, regarding FDI attacks, in [25] a distributed collaborative IDS for smart meters is presented, [26] proposes an IDS for anomaly detection in grid state estimations based on cyber-state correlation patterns, and [27] proposes a deep learning-based framework for detection of FDI attacks in smart grids.

Regarding MadIoT attacks, some recent work investigates respective IDS approaches. The authors of [28] present a simulation testbed for the analysis of MadIoT attacks, including a co-simulation of power grid and communication network. In [29], the authors propose the detection of MadIoT attacks via dynamic thresholding in combination with time series prediction and evaluate their approach based on public energy consumption data with self-generated attacks.

C. Intrusion Detection in e-Mobility

Research that specifically focuses on IDSs in the e-Mobility sector is currently very limited. For instance, [30] proposes a method for detection of cyber-attacks against EV batteries, such as denial-of-charge attacks or overcharging of the battery, and [31] investigates the detection of message flooding attacks on the Controller Area Network (CAN) bus in EVs. In [32] a simple centralized detection approach of FDIs attacks from EVs to the grid is proposed and evaluated based on simulated data. In [33], a project report is presented that mentions an anomaly detection system for predicting next measurements and detecting anomalies based on simulated data and a regression model. However, details regarding the approach, such as specifics of the IDS design or a comprehensive evaluation, are missing. Furthermore, the report mentions a second anomaly detection system against sensor data spoofing at CPs, using data from a point of common coupling (the point where multiple CPs connect to the grid) and predictions from different neural networks to identify misbehaving CPs. Finally, the authors of [34] propose a collaborative anomaly detection system for charging stations. Collaborative detection uses a voting process, whereby individual operators are asked by a central coordinator to provide their anomaly predictions for a charge session report. Individual predictions use supervised classification based on pre-labeled data sets containing a mix of normal sessions and anomalies. The pre-labeled data sets are generated by randomly inserting generic anomalies into publicly available charge session summary data sets (listing total energy, total duration, average power, etc.).

To the best of our knowledge, there is currently no approach, which *(i)* models realistic attacks in real data sets, *(ii)* includes charge session details that reflect a varying load over time, *(iii)* considers large-scale coordinated attacks, and *(iv)* does not require data sets with pre-labeled anomalies for training to better handle previously unseen anomalies. We address these open issues by proposing a regression-based forecasting method for anomaly detection, which works semi-supervised (i.e., training only requires data sets of the normal operation and not pre-labeled attacks) and considers charge session details within their temporal context. Additionally, we focus on coordinated attacks and model specific attack vectors that we derive from our analysis of existing protocols.

D. Machine Learning in e-Mobility and its IDS Applicability

The research on e-mobility-specific IDSs is currently limited, especially with regards to FDI and Mad attacks. However, the previously discussed related work for IDSs in the general smart grid context show that machine learning-based state predictions are commonly used as basis for anomaly detection of these kinds of attacks. Hence, related works on state predictions for e-mobility (most commonly based on regression models) are also of importance to the IDS context.

Due to a growing interest in data-driven modeling of EV charging, several papers investigate respective machine learning-based approaches [35]. For instance, [36] investigates the use of regression models for predicting EV departure

times. The authors consider a variety of features (including car type, weekday, and mean arrival/departure/duration) and different regression models. In [37], the authors compare different regression algorithms to predict the daily charging consumption at individual CPs. The authors of [38] propose a regression-based method for CP (individual and group) charge capacity prediction with 15-minute intervals.

While related work in the general smart grid context identifies regression-based forecasting is a viable method for anomaly detection (cf. Section II-B), a detailed analysis of its applicability to the e-mobility context is still missing. Since the e-mobility context involves a specific infrastructure, protocols, data, and load profiles, important questions with regards to an e-mobility IDS are still open, such as, on which system(s) to run the IDS, which features to use for the regression model, which algorithms to use, and so on. Furthermore, related work which analyses the use of regression-based forecasting in the e-mobility context does not consider anomaly detection under adversarial conditions. Additionally, an open issue is to define at which point a divergence between forecast and actual value should be classified as an anomaly. In this work, we propose a concept to address these open research issues (cf. Section V).

III. System Model

Due to the potentially very high load that EVs incur on the grid, a grid-friendly strategy for the integration of the e-mobility infrastructure into the power grid is important. This requires (bidirectional) communication between EVs and the e-mobility infrastructure as well as between the e-mobility infrastructure and the power grid to control the charging processes, i.e., intelligent load management is needed in order to adapt the charging load to the available electricity generation.

Figure 1 shows our system model with the close connection of e-mobility infrastructure and power grid. The named actors/protocols are representative and widely adopted on an international level [7]. EVs can be charged at CPs in private, semi-public, or public locations, with charging speeds of 3.7 kW (slow AC charging), 11–22 kW (faster AC charging), or over 150 kW (fast DC charging). For (semi-)public charging, a Charge Point Operator (CPO) is responsible for managing CPs, which includes the distribution of grid-friendly charging profiles. Charging profiles can implement load balancing by directly limiting the allowed consumption over time. Alternatively, price incentives can be defined in order to steer consumption (e.g., cheaper prices during off-peak hours) [39]–[41]. For private charging a flexibility provider may be responsible for grid-friendly charging of EVs by communicating with CPs directly or indirectly via a Home Energy Management System. In the following, we refer to flexibility providers as CPOs for simplicity since (for our purposes) they serve similar roles. The Distribution System Operator (DSO) makes sure that the grid load stays within acceptable bounds, which includes sending forecasts of the available capacity to CPOs.

Communication between a DSO and CPOs uses the Open Smart Charging Protocol (OSCP) [42], CPOs communicate with their CPs using the Open Charge Point Protocol (OCPP) [43], and CPs communicate with EVs using ISO 15118 [44]. All communication channels use Transport Layer Security (TLS). The respective processes are detailed in the following:

DSO Forecasts and CPO Charge Profiles: Periodically, a DSO sends *UpdateGroupCapacityForecast* messages to CPOs (Step 1 in Figure 1), which are used to indicate the maximum allowed (or optimal) energy consumption (or generation) for an area over time. This forecast can be based on current measurements and/or consumption statistics.
The CPO can distribute the received forecast over its CPs in the indicated area using *SetChargingProfileRequest* messages (Step 2), which define charging rate limits over time and can optionally include an associated tariff (e.g., to implement load balancing via price incentives).

Charge Parameter Negotiation: After an EV is authorized to start charging at a CP, the two parties exchange charging parameters. The EV starts by sending an estimate of the required energy, its supported current/voltage limits, and an optional planned departure time in a *ChargeParameterDiscoveryReq* message (Step 3). At this point, the CP may request a more specific charging profile (taking into account the EV's needs) from its CPO by sending a *NotifyEVChargingNeedsRequest* (Step 4), which contains the previously received data from the EV. The CPO can respond by sending a *SetChargingProfileRequest* with a session specific profile (Step 5). The CP responds to the EV with a charging profile (indicating the maximum allowed energy consumption over time along with associated tariffs) and its current and voltage limits in a *ChargeParameterDiscoveryRes* message (Step 6). The EV indicates its selected charging profile and optionally its planned energy consumption over time (e.g., if the planned consumption is less than the allowed maximum) in a *PowerDeliveryReq* message (Step 7). The CP can optionally inform the CPO of the EV's selected profile via a *NotifyEVChargingScheduleRequest* message (Step 8). Afterwards, the transfer of energy can start.

Charge Session: During a charge session, both parties can initiate a re-negotiation of charge parameters. The CP can periodically send meter values to the EV in *ChargingStatusRes* messages (Step 9). The CP's meter values are usually signed by its energy meter. Additionally, the EV can send a signature over the meter values in a *MeteringReceiptReq* message (Step 10) if requested by the CP.
During a charge session, a CP also sends the current (signed) meter values to its CPO using *TransactionEventRequest* messages (Step 11). This message may indicate further charge-related values like the maximum offered power or the EV's State of Charge (SoC). Furthermore, a CPO may receive additional meter values from different locations. For example, if multiple CPs are connected to the grid via the same transfer point, a separate meter may be installed at this point, measuring the combined consumption of all CPs.

Periodic Meter Aggregates: A CPO periodically send aggregated meter values of its CPs (grouped into different areas) to the DSO using *UpdateGroupMeasurements* mes-

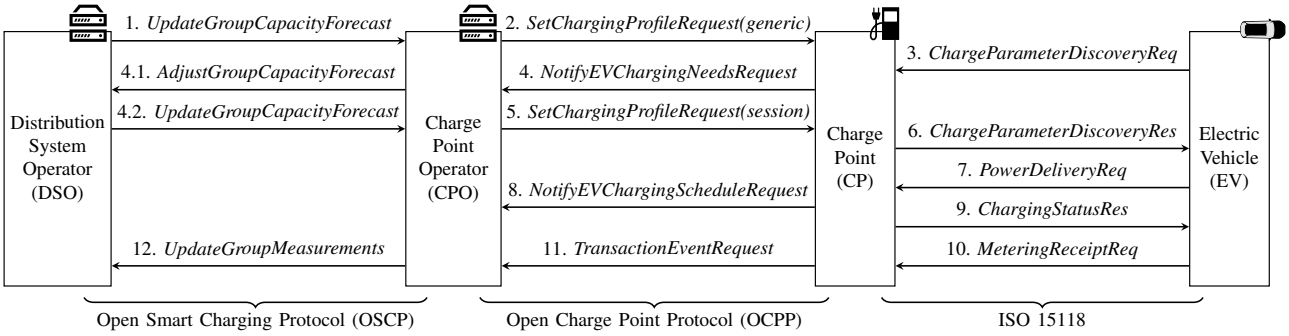


Fig. 1: e-Mobility System Model

sages (Step 12). The DSO may use this data as input for the generation of future capacity forecasts. If a CPO needs more energy than was provided in the DSO's forecast, it can request additional capacities using a *AdjustGroupCapacityForecast* message (Step 4.1; e.g., in response to Step 4). The DSO may grant additional capacities using the *UpdateGroupCapacityForecast* message (Step 4.2).

IV. Adversary Model

In this section, we briefly describe the assumed adversary model and analyze the resulting attack vectors on grid stability under consideration of the processes form Section III.

A. Adversary with a Botnet of CPs/EVs

A successful attack on the power grid can negatively affect the lives of millions of people, with consequences ranging from significant economic damages [45] to severe harm of human health [46]. The grid thus represents a high value target with an increased risk of sophisticated attacks by potent adversaries. Moreover, the potential of cyber attack-based blackouts is exemplified by the successful attacks on the Ukrainian grid in 2015/16 [11], [12]. Thus, it is important and realistic to consider the threat of cyber attacks on the grid by a strong adversary. As outlined in Section II-A, such attacks may be possible via vulnerabilities in e-mobility systems.

In this paper, we consider an adversary with control over a botnet of EVs and/or CPs. Note that, since we investigate the possibility of attack detection by the backend systems, the respective backend systems are assumed to be secure. A botnet of EVs and/or CPs could be established by means of locally/remotely exploitable vulnerabilities in a number vehicles (cf., e.g., [9], [47]) or CPs (cf., e.g., [6], [8]). Specific examples of real-world vulnerabilities include: *(i)* the prominent 2015 Jeep hack [48], which could be exploited via a vehicle's cellular interface and enabled an adversary to remotely control internal systems of vehicles or *(ii)* the remote compromised of CPs due to the insecure configuration of their web interfaces [5]. The adversary tries to use this botnet to negatively affect the power grid and cause small- or large-scale power outages, for instance, in the context of inter-state conflicts, terrorism, or extortion. For this, the adversary can try to directly modify the charging behavior of controlled systems or manipulate the data that the controlled systems generate/send. Forwarded data can only be modified if it is not cryptographically protected. More specifically, the adversary uses any of the potential attack vectors identified in the following sub-section (IV-B).

B. Attack Vectors

Broadly speaking, there are two types of attacks in the context of e-mobility-based attacks on the power grid: First, False Data Injection (FDI) attacks, [49] meaning that the data used for state estimation in the power grid is manipulated. Second, Manipulation of demand (Mad) attacks [15], where the energy consumption of devices is directly manipulated. These attacks can cause overload scenarios or a significant imbalance in power demand and generation and thus harm the grid (cf. [15]). Namely, a significant increase in demand could overload lines and potentially cause cascading line failures leading to large scale blackouts. Additionally, a significant imbalance in demand and generation could cause the system's frequency to go outside of the safe operating limits resulting in generator tripping and potentially blackouts.

Considering the system model from Section III in combination with an adversary controlling a large enough number of EVs and/or CPs, we identify the following e-mobility-based attack vectors (AV) to grid resilience:

EV Botnet: An adversary with control over a botnet of EVs could conduct FDI and/or Mad attacks as follows:

AV_1 Sending manipulated *ChargeParameterDiscoveryReq* to CPs: The adversary can maliciously affect charging speeds by sending manipulated current or voltage limits. Additionally, the combination of estimated energy needs and expected departure time could be used to affect load balancing algorithms, e.g., by indicating that a large amount of energy is needed within a short period of time, which could even lead to CPOs requesting additional capacities from the DSO and could be problematic if the indicated energy is not actually consumed by the EVs.

AV_2 Sending manipulated *PowerDeliveryReq* to CPs: The adversary can maliciously affect charging speeds based on their charge profile selection, with the limitation that only offered profiles can be selected, i.e., it does not

allow for arbitrary definitions by the EV. However, the EV can indicate planned energy consumption over time (within the bounds of the chosen profile), e.g., to indicate a lower/higher consumption than what it actually plans to charge, which may affect load balancing algorithms. Additionally, an EV could choose sub-optimal tariffs to affect charging speeds, i.e., to counteract price incentive-based load balancing and charge at high speed/cost during peak or low speed/cost during off-peak hours.

CP Botnet: An adversary with control over a botnet of CPs could conduct FDI and/or Mad attacks as follows:

AV_3 Sending manipulated *NotifyEVChargingNeedsRequest* to the CPO: The adversary can affect charging speed by forwarding manipulated EV charge parameters (current/voltage limits) to the CPO, which could result in sub-optimal charge profile generation by the CPO. Additionally, CPs can maliciously affect load balancing by forwarding altered EV charge parameters (estimated energy needs and expected departure time) to the CPO.

AV_4 Sending manipulated *ChargeParameterDiscoveryRes* to EVs: The adversary can reduce charging speeds by sending manipulated max power over time, current or voltage limits. Similarly, sending manipulated sales tariffs could be used to reduce or increase charging speeds. Notably, while sales tariffs are signed by the respective backend actor for validation by EVs, the standard does not prevent replay attacks. Hence, manipulated CPs can, without spoofing the signature, send malicious tariffs to an EV, e.g., by replaying an off-peak tariff during peak hours.

AV_5 Sending manipulated *NotifyEVChargingScheduleRequest* to the CPO: The adversary can maliciously affect the grid state estimation/load balancing by reporting an altered charge profile selection to the CPO, indicating that EVs are planning to charge more/less than they actually do.

AV_6 Sending manipulated *TransactionEventRequest* to the CPO: The adversary can maliciously affect the grid state estimation/load balancing algorithm by sending manipulated meter values to CPOs, e.g., indicating lower consumptions, which could lead to an increased consumption at non-compromised CPs or indicating higher consumptions, which could lead to increased generation or lowered consumption at other controllable consumers, causing an imbalance in power generation/consumption.

EV&CP Botnet: AV_7 An adversary with control over a botnet of compromised EVs and CPs can generally conduct the same attacks as the previous adversaries (AV_1-AV_6). The main difference is, that an adversary with control over both parties of a charging session is not bound to the standard protocols/processes. For instance, if the adversary only compromised the CP of a charging session, the non-compromised EV would still expect the usual ISO 15118 protocol steps (authentication, profile negotiation, etc.) before the charge can start. If, however, both parties are compromised the adversary can directly define the charging behavior and is only bound by physical limits.

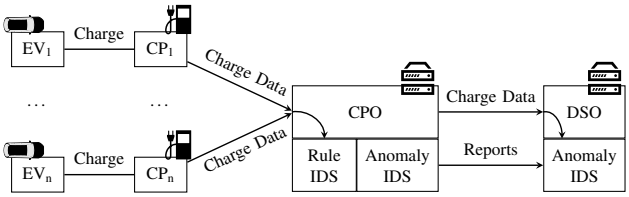


Fig. 2: Concept of an IDS for e-Mobility Systems

V. E-Mobility-based IDS Concept

In this section, we present our IDS concept for detecting e-mobility-based attacks on the power grid. The IDS is a hybrid solution and distributed across the different backend actors and aims to identify the existence of FDI and/or Mad attacks in received data. More specifically, it is a hybrid of rule-based and anomaly-based detection and runs with differing capabilities on CPOs and DSOs. The next paragraphs provide an overview (cf. Fig. 2) and Sections V-A and V-B provide details.

The rule-based detection approach serves as a first layer of detection in order to filter for more simple kinds of attacks that, e.g., violate set limits or cause inconsistencies. For this, we analyze the processes of existing communication protocols (cf. Section III) for included data with relevance to FDI and/or Mad attacks. We discuss the potential use of this data in rule-based detection under consideration of existing security measures as well as the adversary's potential to tamper with this data. If the existing security measures are not sufficient, we further propose fixes that enable the use of this data for intrusion detection under the considered adversary model.

For more advanced attacks that can be executed within the bounds of the defined rules, we present an anomaly-based detection approach. The basic idea is to use regression model-based forecasting in order to predict the expected charging load and later compare these predictions to the received values. A sufficiently high divergence between prediction and received values is marked as potential anomaly. We perform feature engineering in order to identify information that could be used as features for training of the regression model. Hereby, we again consider the adversary's potential to affect this data. The anomaly detection is split among the backend actors (CPOs and DSOs) using different kinds of available data for detection at multiple levels (whole grid and CP groups). The additional IDS step on the DSOs enables better detection of large-scale coordinated attacks, while taking the distributed CPO IDSs reports as extra input. The results are further post-processed for optimized detection and the reduction of false positives.

A. Rule-based IDS

Rule-based IDSs provide a relatively low overhead method to detect potential attacks. For this, rules are defined that describe the allowed behavior/states of a system and any deviation from these rules can be interpreted as an anomaly. Under consideration of the defined adversary model, we analyzed the e-mobility system for the potential for rule-based detection on the CPO. We only consider CPOs and not DSOs, since

DSOs only receive summarized consumption data, rather than detailed session information, which does not lend itself well to rule-based detection. Results are discussed in the following:

Physical limits: A CPO can check received charge session data for consistency with the physical limitations of the involved CP and EV. Notably, a CPO should already be aware of the limits of CPs that they manage, meaning that the considered adversary (who cannot alter backend data) cannot manipulate this data. Relevant CP limits include current/voltage limits as well as number of connectors and thus limit the potential charging speed as well as the maximum amount of concurrent charging sessions. Hence, simple rule-based detection could be applied against FDI attacks that violate these limits (cf. AV_6 in Section IV-B).
Security Considerations: Notably, a botnet of CP's could still max out the previously mentioned concurrent charging sessions in the context of FDI attacks even without any actual EVs being present. This is because an EV's authentication (as basis for charge authorization) is only assured towards the CP (via signature over a nonce) and not securely verifiable by the CPO as replay attacks are possible. In order to prevent this, a change of the nonce generation by CPs would be required that allows the CPO to verify the freshness of an EV's authentication (e.g., via the inclusion of a timestamp or of a nonce from the CPO).
Furthermore, the EV's current/voltage limits are sent from the EV over the CP to the CPO (cf. AV_1 and AV_3). Since this data is not end-to-end protected, it could be altered by a manipulated EV as well as a manipulated CP. While tampering from the CP could be prevented via a change of the standard that allows an EV to sign this data (assuming freshness is ensured), this change would not prevent tampering by the EV. Thus, the better alternative would be to include this data in the EV's public key certificate (used by the EV during charge authorization), which would prevent tampering from both considered adversaries. However, with the current state of the standard, the reliability of this data for attack detection is limited.

Charge profile/schedule: CPOs can check received charge session data for consistency with a session's charge profiles/schedules. First, the charge profile (maximum allowed consumption over time) is defined by the CPO and thus gives robust limits that should never be violated during a charging session (cf. AV_3-AV_6). While a manipulated EV (or CP since the data is not end-to-end protected) can have a limited effect on a session specific charge profile (cf. AV_1 and AV_3), by sending altered charge parameters (required energy and planned departure time), the resulting profile should nonetheless represent a reasonable maximum.
Second, the charge schedule (EV's planned consumption over time) is defined by the EV and could be used by a rule-based IDS at the CPO by verifying that the schedule fits within the relevant charging profile and that the schedule is not violated during the charging session without prior rescheduling (cf. AV_2, AV_4, AV_5, and AV_6).
Security Consideration: The EV's charge parameters could be protected from a manipulated CP via a signature from the EV (assuming freshness is ensured). However, protection from a manipulated EV is difficult (compared to the static physical limits) since this data is dynamically generated by the EV. Additionally, the EV's charge schedule is not end-to-end secured with similar security implications as previously discussed for the EV's charge parameters.

Redundant metering: A CPO can verify the consistency of the redundant/related data of a charging session. Specifically, a CPO can receive metering data at different points of the CP (energy import and -export) as well as the vehicles SoC. A rule-based IDS could be used to verify the consistency of this data, allowing some minor divergences due to loss or metering inaccuracies (cf. AV_6 and AV_7).
Furthermore, a source of redundant metering information could be a separate electricity meter at the grid connection point (e.g., with multiple CPs connected via the same point of common coupling as considered in [33]). This scenario is especially useful if the connection point's meter values are more trustworthy than the CP's (e.g., if secured via a Smart Meter Gateway (SMGW) [50]). This data could again be used in a rule-based IDS to detect any inconsistencies with the data received from the CP or EV (cf. AV_6 and AV_7).
Security Considerations: While again, the EV's data (SoC) is not end-to-end protected, it could be secured via a signature (assuming freshness is ensured). Notably, if the CPO receives both secure EV and CP data, a verification of the consistency of this redundant/related data would be able to detect any attack that is exclusively executed by either EV or CP. However, undetected attacks would still be possible if both EV and CP are manipulated and sending consistently altered data (cf. AV_7).
Additionally, a requirement for valid EV metering receipts (signatures over the CP's meter values) could be used by the rule-based IDS as a redundant confirmation of the CP's data and achieve a similar effect of requiring adversaries to control both EV and CP. However, the ISO 15118 standard defines that metering receipts only serve as a confirmation that the CP's meter values were received and not that these values were accurate. Hence, to use metering receipts in the IDS context, the standard would have to be changed to require a validation of these values by the EV.

B. Anomaly-based IDS

While the previously discussed rule-based IDS approach can already provide a level of simple attack detection, it fails to detect more advanced attacks that work in the given limits and produce consistent data. For this reason, we propose an anomaly detection system, as a second step in attack detection.

Our proposed concept for an anomaly-based IDS is centered around the idea of regression-based forecasting of EV charging loads. That is, a regression model is trained on previous, non-adversarial, meter values and afterwards used to predict the expected future values. The predicted values are compared to the actually received meter values and anomalies are detected

based on the difference in prediction and received values. Specifically, this task requires the definition of where to implement the IDS, which algorithms to use, which features to include in the regression model, and at what point to classify a difference in prediction and received values as an anomaly. We discuss these aspects in the following sub-sections.

1) Distributed Anomaly Detection Architecture: We propose a distributed IDS architecture. Namely, anomaly detection is distributed among the different CPOs and the DSO. At CPOs, the rule-based detection approach serves as an initial filter that provides simple attack detection for more obvious cases as discussed in Section V-A. If the rule-based system did not identify any anomalies, the CPO employs the forecasting-based system as a second step of detection. Hereby, the CPO's forecasting can be directly based on the detailed information it receives from its CPs, which also allows for a more fine-grained application of anomaly detection for the different kinds of CPs (e.g., splitting CPs based on their physical limits into type 1 with 3.7 kW, type 2 with 11 to 22 kW, or type 3 with 150+ kW). However, the scope of detection by a CPO is also limited to its managed CPs. Hence, we propose a further forecasting-based detection step at the DSO, which aims to detect large-scale (i.e., grid-wide) attacks. For this, the DSO can generate own forecasts based on the (aggregated) data as received from CPOs. Additionally, the DSO can incorporate the individual CPOs' detection results as input in a weighted voting process, whereby weights can be adjusted to further optimize detection results.

2) Regression-based Forecasting: As mentioned previously, forecasting is based on a regression model. In general, a regression algorithm is trained on a time series of data points, whereby a set of *lag* values, i.e., previous values in the time series, is used as input to the regression algorithm when trying to predict the next data point [51]. For our purpose, the regression model receives a set of charging values $CV_{i-n} \dots CV_i$ as lag with the goal of predicting the anticipated next value CV_{i+1}. Further, an arbitrary set of additional features, i.e., exogenous variables EX_x, can be defined for the values of the time series such that EX_{i+1} will be considered in the prediction of CV_{i+1}. Additionally, this approach can be extended to the forecasting of intervals (instead of single data points) by recursively shifting predicted values into the lag for further forecasting. That is, in order to forecast CV_r with CV_i being the last known value and $r > i$, one first has to predict the value of CV_{r-1} until $r = i$.

The choice of lag window as well as forecasting of interval size are important design factors. While a larger lag window provides the regression model with more information when it comes to the prediction of future values, further removed charging values also show less relation to the future data points. Larger interval sizes on the other hand have the issue that predictions become further removed from the last known value, which can increase biases and prediction error, while smaller interval sizes are more prone to be affected by adversarial changes in the data. Hence, we consider different values for both of these variables and evaluate their effect on anomaly detection later in this paper.

3) Regression Models: Another important design factor is the choice of algorithm to build the regression model. Several regression algorithms exist but based on what was successfully used in related work, we consider decision tree regression, linear regression, gradient boosting, support vector regression, and artificial neural networks. Decision trees combine a sequence of logical rules, which compare an attribute against some threshold or a set of possible values, resulting in models that are relatively easy to comprehend/interpret by humans [52]. Similarly, linear regression models are a widely used technique due to their simplicity and high degree of interpretability [53]. Support vector regression is effective for real-value function estimation with the main advantage that its computational complexity is independent of the input space dimensionality [54]. Gradient boosting combines a set of *weak learners* in an ensemble and approximates results as a weighted sum, whereby it can achieve accurate results in a variety of use cases [55]. Similarly, artificial neural networks receive great popularity in a variety of use cases. They present an interconnection of *neurons* that individually compute values based on received input and forward this data further through the network [56].

4) Feature Engineering: The selection of appropriate features (exogenous variables) as input to the regression model also represents an important design factor. The charging values for lags and prediction, represent the accumulated current load of all CPs or groups of CPs (e.g., for the type-specific detection as mentioned in Section V-B1). Based on our analysis of related work and the e-mobility system model, we further consider the following types of data for use as exogenous variables by CPOs: (i) Date/time information, since aggregated EV load exhibits certain time-dependent patterns (e.g., high--levels of at-home charging load in the evening as people are coming home from work), (ii) Overall connection/session data, including current session count, connected capacity, and load balancing profile, and (iii) CP specific session data, including per CP the current session state, absolute/relative load, energy sum, available capacity, and SoC. Notably, all CP specific session data could be manipulated by an adversary with control over the respective CPs (cf. AV_3-AV_6 in Section IV-B).

As the DSO receives different data during normal operation than CPOs (cf. Section III), different considerations apply with regard to feature definition. For one, DSO only receives accumulated reports from CPOs over the overall energy consumption rather than session-specific information. Thus, the use of this data as charging values for lags and prediction is still possible. However, without a change to the respective protocol, the use of the previously discussed exogenous variables by the DSO is limited to the general date/time information. Additionally, the load balancing profile information could be used to some extent as the DSO can influence these with their *UpdateGroupCapacityForecast* messages (e.g., giving guidelines for slower charging during peak hours) even if the specific load balancing profiles (as sent from CPOs to CPs) are not known to the DSO. While, with changes to the

respective protocol, the DSO would be able to use the same exogenous variables as the CPOs, this might be undesirable, e.g., due to the large overhead or for data protection reasons as specific charging data is privacy-sensitive [57]. Similarly, with changes to the respective protocol, the DSO would be able to incorporate the CPOs' IDS results in their own detection process and thus indirectly the CPOs' specific data with only minor overhead and without the potential privacy issues.

5) Anomaly Classification: Finally, after a regression model is trained with a certain feature set and lag size, it can be used to predict certain forecasting interval sizes. In order to use these forecasts for anomaly detection, the basic idea is that the results of an accurate regression model are going to be close to the actually measured/received values and any sufficiently large attack (using any of AV_1-AV_7 from Section IV-B) would cause the measured/received values to be noticeably different to the predicted values. Thus, an anomaly could be detected based on this noticeable difference. Specifically, however, there are different methods for interpreting this difference, which may have an effect on detection accuracy. We consider the following classification methods CM:

- CM_1 Relative threshold: if the difference between prediction and received measurement exceeds a relative threshold, the measurement is marked as an anomaly. The threshold is defined in relation to the predicted value, e.g., if the received measurement is 50% greater than the predicted value it is interpreted as an anomaly.
- CM_2 Static threshold: if the difference between prediction and received measurement exceeds a static threshold, the measurement is marked as an anomaly. In order to define a threshold that is applicable to different use-cases, the threshold is defined in relation to the average load observed in the training data.
- CM_3 Hour-specific threshold: if the difference between prediction and received measurement exceeds a threshold that is defined for the current hour-of-day, the measurement is marked as an anomaly. The value for hour-specific threshold could be defined either in relation to the mean or the standard deviation of the hour-specific load as observed in the training data.
- CM_4 Prediction intervals: if the received measurement lies outside of the forecaster's prediction interval, the measurement is marked as an anomaly. The interval is estimated based on the expected errors of the forecaster, which assuming future errors are related to past errors, e.g., based on bootstrapping [58].

VI. Implementation and Evaluation

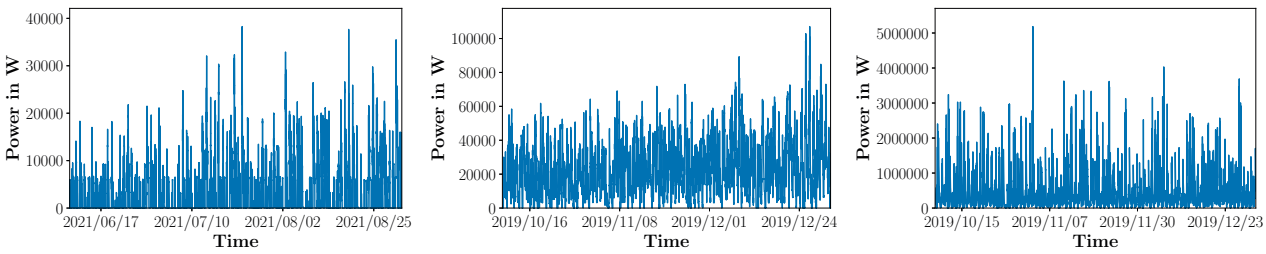
In order to evaluate the proposed IDS concept, it is first important to attain appropriate data sets with and without attacks present. Similarly to related work (cf. Section. II-B), we start with data sets without attacks and insert simulated attacks as no other option exists. For the base data sets without attacks, we include five different options in our evaluation, namely, the three Adaptive Charging Network (ACN) data sets [59], the ElaadNL data set [60], and a simulated data set based on emobpy [61]. Figure 3 shows the summed charging load for the last three months of select data sets.

The ACN data sets are: *(i)* ACN Caltech, which contains data of 54 semi-public CPs in a university garage, *(ii)* ACN JPL, which contains data of 52 workplace CPs from a national research lab, and *(iii)* ACN Office 1, which contains data of 8 workplace CPs from an office building. The data sets contain detailed charge session metering data at mostly 4 second intervals over a time period of roughly 2.5 to 3.5 years (depending on the data set). For our purposes, we only use one year of each data set and aggregate data over 15 minute intervals. The ElaadNL data set contains data from 850 public charging stations, which are operated by EVnetNL in the Netherlands, and contains detailed charge session metering data at 15 minute intervals over a time period of one year. However, since, to the best of our knowledge, no openly available data set can reflect the entire CP charging dynamics (including public-, workplace-, and home charging with different CP types implementing slow/faster AC charging as well as fast DC charging) in a local grid, we additionally consider a simulated charge session data set.

We generate the simulated data set using emobpy [61] in Python for 1320 CPs at 15 minute intervals over a time period of one year. Charge events are generated such that they reflect the distributions between at-home, work, and public charging as reported in [62], i.e., roughly 75%, 20%, and 5% respectively. Movement profiles and vehicle types are randomly sampled from the values provided in emobpy. Load balancing strategies are defined based on the time of day, whereby charging during typical off-peak hours uses no load balancing and charging during peak hours uses the strategy of lowering the charging speed to the minimum amount that is required to achieve the defined charging goal before departure.

Based on the mentioned data sets, we generate the corresponding per-CP OCPP 2.0 traffic using ns-3 [63] for network simulation, i.e., to generate realistic traffic as it would be received by CPOs. Charge session data is reported at 15 minute intervals, assuming one CPO per data set. The generation of OCPP messages is based on *cereal-ocpp2* [64]. For each data set, we generate OCPP traffic out of the first 11 months of charge session data without attacks for training and validation of the regression models and several data sets with different attacks out of the last month for testing purposes.

More specifically, we consider FDI and Mad attacks with different magnitudes and different amounts of corrupted EVs and/or CPs. Based on related work (cf. Section II-A) and our analysis of attack vectors (cf. Section IV), we consider different types of attack patterns, namely: *(i)* synchronized alterations at a specific point in time, *(ii)* preparation of a demand increasing attack with a prior load reduction to increase the attack capacity, and *(iii)* slowly increasing alterations over time. For detection at the DSO large-scale attacks are defined to be coordinated across CPs of different CPOs, i.e., across (comparable) data sets. Attacks can either change existing charge session data or create new data/sessions. The adversary can control 20%–100% of the relevant systems (EVs



(a) ACN Caltech Data Set (b) ElaadNL Data Set (c) Emobpy Data Set

Fig. 3: Last Three Months of Select Data Sets

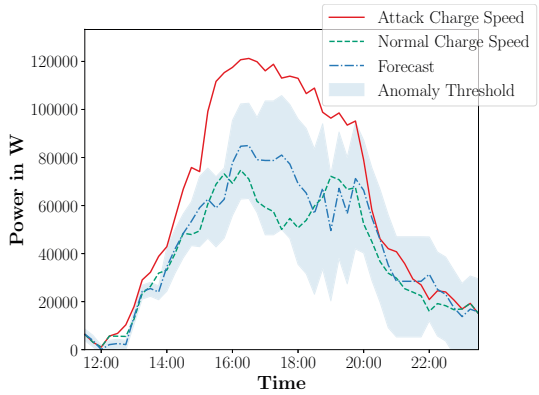


Fig. 4: Example of an Attack and Anomaly Prediction

and/or CPs). All attacks are similarly inserted into the data sets, i.e., an attack-type is selected, the adversary controlled systems are randomly chosen, and an attack time is defined (using a high-stress time at which power grids are typically more susceptible to attacks, cf. [3]). Afterwards, all adversary controlled systems execute the attack if possible (e.g., a Mad attack by a manipulated CP still requires that an EV is present at the time of attack and ready to charge). All attacks can last for varying amounts of time (affecting 1 to 20 successive messages to the backend) and may be executed multiple times in a row (same time on 1 to 10 successive days). However, all attacks are restricted to the bounds of the rule-based IDS (cf. Section V-A) as any violation of a rule would lead to a trivial detection. In total, we generated 108 attack data sets (half Mad, half FDI) per base data set, each containing an average of 20 attacks at different points in time (not overlapping). The the synthetic normal and attack datasets are provided online.[1]

An example of an attack is shown in Fig. 4. The shown attack is part of one of the ACN JPL attack data sets and represents a synchronized charge load increase (i.e., Mad attack) during typical grid peak hours. For the attack, the adversary is assumed to control 26 CPs. However, for a Mad attack, any adversary controlled CP can only participate in the attack if an EV is connected. The figure also shows the normal summed charge speed, i.e., what the curve should look like without an attack, as well as a regression forecast using a decision tree model and the corresponding anomaly classification threshold using method CM_3 (hour-specific thresholds).

Feature extraction and anomaly detection are implemented in Python. The generated charge session traffic is parsed with scapy [65] and interpreted with the mobilityhouse OCPP framework [66]. The features as discussed in Section V-B4 are extracted from the OCPP traffic.

Regarding anomaly detection, we mainly focus our evaluation on the forecasting-based part of the IDS (unless specified otherwise), since, as previously mentioned, rule-based detection is trivial in the sense that any violation of a rule would be correctly identified as an anomaly. However, the rule-based detection concept still influences the evaluation by limiting potential attacks to the rule-defined bounds.

Forecasting utilizes the regression algorithms as implemented in sklearn [67]. Specifically, we use `DecisionTreeRegressor` as an implementation of decision trees, `ElasticNet` and `HuberRegressor` as implementations of linear regression, `GradientBoostingRegressor` as an implementation of gradient boosting, `LinearSVR` as an implementation of a support vector regression, and `MLPRegressor` as an implementation of a multi-layer perceptron type of artificial neural network. The regression algorithms are applied to the forecasting domain based on the skforecast [68] framework. Furthermore, the specific hyperparameters of the different regression algorithms as well as the lag size and forecasting interval are optimized based on a grid search. Optimization is based on the mean squared error performance metric, using the data sets for training and validation. This preliminary analysis showed one day to be a good guideline for lag window and forecasting interval across the different data sets and regression algorithms, which we use in the following evaluations unless specified otherwise.

Optimized regression models are trained on the combined training and validation data sets and used to predict the values of the test sets. The predictions are compared to the actually received values and anomalies are classified using the four methods mentioned in Section V-B5, whereby different threshold values were tested in order to identify optimal parameters for the methods. Notably, since we are concerned with e-mobility-based attacks to the power grid, we consider two attack scopes AS for the IDS evaluation based on the

[1] https://code.fbi.h-da.de/seacop/e-mobility-ids-data-sets

TABLE I: CPO Detection Results for Classification Method CM_3 and Attack Scope AS_1

	DecisionTreeRegressor		ElasticNet		GradientBoostingRegressor		HuberRegressor		LinearSVR		MLPRegressor		mean	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
ACN Caltech	0.925	0.078	0.585	**0.038**	**0.930**	0.096	0.632	0.050	0.860	0.186	0.665	0.044	0.766	0.082
ACN JPL	**0.941**	0.050	0.774	**0.016**	0.917	0.085	0.912	0.140	0.906	0.276	0.699	0.027	0.858	0.099
ACN Office1	**0.999**	**0.019**	0.566	0.368	0.993	0.424	0.910	0.362	0.953	0.529	0.910	0.362	0.888	0.344
ElaadNL	0.972	0.029	0.918	0.011	0.995	0.008	0.995	0.008	**0.995**	0.011	0.993	**0.006**	0.978	0.012
Emobpy	0.996	**0.014**	0.989	0.028	0.992	0.047	**1.000**	0.036	0.993	0.060	0.997	0.059	0.994	0.041
mean	**0.967**	**0.038**	0.766	0.092	0.965	0.132	0.890	0.119	0.941	0.212	0.853	0.100	0.897	0.116

results of [3], namely: AS_1 an attack scope with at least 20% malicious charge sessions resulting in at least a 2-fold increase in overall EV charging load and AS_2 an attack scope with at least 70% malicious charge sessions resulting in at least a 9-fold increase in overall EV charging load. With the expected growth of the e-mobility sector over the next few years, these attack scopes were shown in [3] to be able to respectively cause minor- or major outages during peak load times.

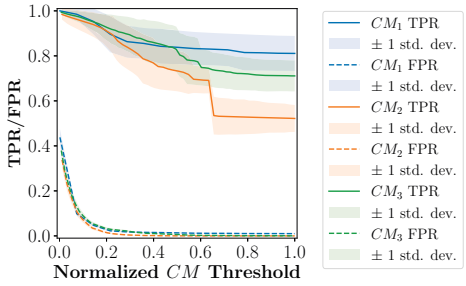
Results for detection by CPOs, i.e., with the full feature set of detailed CP data, for attack scope AS_1, and classification method CM_3 (hour-specific thresholds) are shown in Table I. We report the detection rate, i.e., the True Positive Rate (TPR), and the false alert rate, i.e., the False Positive Rate (FPR), as core performance metrics for all combinations of base data set and regressor. Per base data set, the TPR and FPR are reported as the mean over all corresponding attack data sets for simplicity. Additionally, we highlight the best TPR and FPR, i.e., the highest TPR and lowest FPR, for each base data set in bold font. The CM thresholds are optimized assuming equal importance of TPR and FPR. Later in this section, threshold optimization is discussed in more detail (cf. Fig. 5). For Table I, same optimization allows for better comparability across algorithms. Comparability across data sets is limited as, e.g., a data set may be too small for a given prediction task.

The results show good performance across most regression algorithms. Notably, the `DecisionTreeRegressor` provides the best overall TPR and FPR, which indicates that it is a good choice for the use case. Additionally, `ElasticNet` provides the worst overall TPR and `LinearSVR` the worst overall FPR. The results also show that the regression models provided the overall worst TPR for the ACN Caltech data set and the overall worst FPR for the ACN Office data set. Notably, only the `DecisionTreeRegressor` provides good TPR and FPR for both of these data sets.

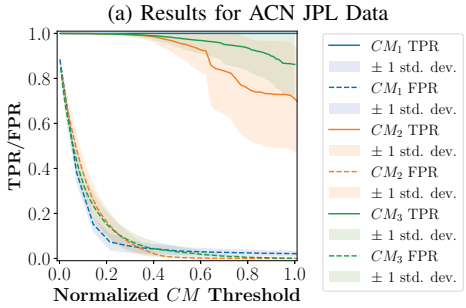
Regarding different classification methods, our results show that CM_3 provides the overall best results when averaged across regression algorithms and data sets (assuming equal importance of TPR and FPR). Compared to this method, CM_1 performed on average 8.98% worse, CM_2 performed 4.29% worse, and CM_4 performed 14.26% worse (not shown in Table I). However, the ranking of classification methods varies between algorithms and data sets.

In order to exemplify this fact, Fig. 5 shows further evaluations for the `DecisionTreeRegressor` with the ACNs JPL and ElaadNL data sets, representing semi-public and public charging respectively. Specifically, we show the TPR/FPR trade-off for different tuning of the respective CM threshold values for CM_1, CM_2, and CM_3 (the chosen regression algorithm does not provide prediction intervals for CM_4). The shown CM threshold value ranges are as follows: *(i)* for CM_1 a sample is classified as an anomaly if the absolute difference between prediction and received measurement is greater than $[0.01, ..., 5.6]$ times the predicted value, *(ii)* for CM_2 the difference has to be greater than $[1000, ..., 93{,}000]$ W, and *(iii)* for CM_3 the difference has to be greater than $[0.01, ..., 0.79]$ times the hour-specific standard deviation of the training data. Additionally, the threshold values are normalized to the range of $[0, ..., 1]$ for comparability. The results show that for the considered public charging cases, CM_1 provides the best detection performance and for the considered semi-public charging cases, CM_1 and CM_3 provide the best performance, assuming equal importance of TPR and FPR. Notably, if the CM threshold value is optimized towards low FPR, CM_1 for semi-public charging cases tends to have the problem that the FPR curve flattens out relatively early, while the TPR curve steadily decreases. In Fig. 5a, for instance, an FPR of less than 0.01 is reached by CM_1 with a TPR of 0.80 and by CM_3 with a 0.85 TPR. The better performance of CM_3 in semi-public/workplace charging cases can be explained by the observation that these charging cases exhibit a closer relation between time and charging behavior (e.g., related to working hours) than the public charging case. In practice, an operator could optimize the thresholds either for an acceptable FPR value using only the training data with normal behavior or for the most desirable TPR/FPR trade-off using real/simulated attack data (if available; cf. Fig. 5). For example, our evaluations of the different classification methods for ACN JPL with AS_1 show good threshold values around: 0.81 for CM_1 (equal to 0.145 in Fig. 5), 13,000 for CM_2 (equal to 0.139 in Fig. 5 or 0.84 times the mean load of the test data set), and 0.21 for CM_3 (equal to 0.265 in Fig. 5), always assuming equal importance of TPR and FPR.

Regarding attack scope AS_2 (not shown in Table I), our results show that overall performance is significantly better, with an overall mean TPR of 0.976 and FPR of 0.102 as well as a mean `DecisionTreeRegressor` TPR of 0.995 and FPR of 0.013 (using CM_3). While a better performance for attack scope AS_2 was to be expected as a larger attack should



(a) Results for ACN JPL Data



(b) Results for ElaadNL Data

Fig. 5: Evaluation of CM Threshold Values for AS_1

result in a bigger anomaly, these results still show that the IDS is very good at detecting attacks that could cause major outage scenarios. Fig. 6 shows a more detailed evaluation of the detection performance for different levels of minimum adversarial manipulations using `DecisionTreeRegressor` with CM_1–CM_3 for the ACN Caltech data set (i.e., the worst case for the chosen regressor in Table I). An adversarial manipulation of 100% (a 2-fold increase) is equal to AS_1 and 800% is equal to AS_2. All classification methods are optimized towards a FPR of less than 0.02 (e.g., with a threshold value of 0.53 for CM_3 in Fig. 6) to allow for an easier comparability based on only TPR. The results show a steep increase of TPR to above 0.8 (using CM_3) with an adversarial manipulation in load of at least 90%. For comparison, the same TPR level, also at a 0.02 FPR, can be reached for the ACN JPL data set at a minimum manipulation of 30% and for the ElaadNL data set at 20%. The results also identify a relatively poor detection rate at small levels of compromise as a limitation of the presented approach. While smaller-scale attacks can still have undesirable consequences, e.g., cause financial damage to operators [34] or physical damage to an EV's battery [69], we argue that this limitation is acceptable in our context as we focus on attacks to power grid stability.

To evaluate the difference between for the CP type independent (as reported in Table I) and CP type-specific detection methods we could only use the emobpy data set, since, as previously mentioned, it is the only data set which includes a mix of public-, workplace-, and home charging with different CP types. The difference for CP type-specific detection is that individual models have to be trained for the grouped consumption of each CP type (slow/faster AC charging as

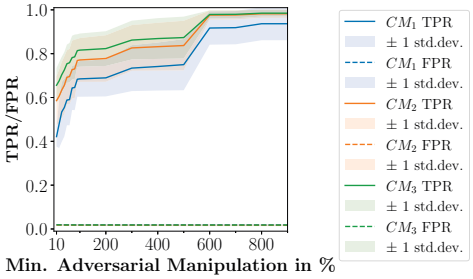


Fig. 6: Evaluation wrt. Level of Manipulation for ACN Caltech

TABLE II: TPR over Lag Windows and Forecasting Intervals

ElaadNL with CM_1 and AS_1		Lag Window in hours 12	24	36	48
Forecasting Interval in hours	1	0.969	0.996	0.998	0.975
	6	0.954	0.986	0.982	0.962
	12	0.911	1.000	0.957	0.938
	24	0.913	1.000	0.955	0.932
	48	0.901	0.999	0.947	0.993

well as fast DC charging). The results show no significant overall performance increase (e.g., only 0.24% better TPR for the `DecisionTreeRegressor`). This does not indicate that the added overhead of training separate models for CP type-specific detection is justified. However, more evaluations, especially with real data sets, are needed to confirm this result.

As previously mentioned, our preliminary analysis indicates a lag window and forecasting interval of one day as a good guideline based on regression accuracy on the training/validation data. In Table II we show a more detailed evaluation of these parameters wrt. to detection performance, using `DecisionTreeRegressor` with CM_1 and considering AS_1 for the ElaadNL data set. The CM threshold is optimized towards a FPR of less than 0.01 to allow for a comparison based on only TPR. The results show an optimum at a lag window of 24 hours with a forecasting interval of 12 or 24 hours, which supports the results of the preliminary analysis. Comparable evaluations with different data sets show different optimum values with, e.g., a TPR of 0.883 for ACN JPL at a lag of 48 and a forecasting interval of 48 compared to 0.876 at one day for both or a TPR of 0.781 for ACN Caltech at a lag of 24 and a forecasting interval of 6 compared to 0.774 at one day for both. However, as the difference in TPRs is relatively low, using one day for both can still be seen as a good guideline. Results for AS_2 are comparable (with higher TPRs) and generally show even less difference between the different parameter value choices.

As previously mentioned, the main effect of the rule-based detection concept on previous evaluations was that it limits potential attacks to the rule-defined bounds. In order to explicitly show the potential effect of the rule-based system, we perform an additional evaluation, whereby a portion of the previously described attack data set anomalies are changed to violate a rule. Specifically, we increase the reported charging load above the respective CP's possible capacity (FDI attack)

TABLE III: Effect of Rule-based IDS on TPR for ACN Caltech

	Portion of Attacks with Rule Violation					
	0.0	0.2	0.4	0.6	0.8	1.0
Rules	0.000	0.200	0.400	0.600	0.800	1.000
CM_3	0.816	0.825	0.836	0.846	0.845	0.859
CM_3+Rules	0.816	0.879	0.927	0.960	0.983	1.000

TABLE IV: DSO Detection Results for Attack Scope AS_1

	Without Distributed CPO Reports		With Distributed CPO Reports (Weighted Voting)	
	TPR	FPR	TPR	FPR
ACN	0.938	0.205	0.991	0.021
Emobpy	0.995	0.026	0.991	0.009
mean	0.967	0.116	0.991	0.015

for some adversary-controlled sessions. The TPR results for the ACN Caltech data set with AS_1 and CM_3, optimized for less than 0.02 FPR, are shown in Table III. The results show, as expected, that the TPR of the rule-based system is always equal to the portion of anomalies that violate the rule (FPR is always 0.0; not shown). Additionally, the TPR of the regression-based detection (CM_3) slightly increases with increasing rule violation since these violations are implemented by further increasing the adversarial load. Furthermore, the results show that the combination of rule- and regression-based detection further enhances the detection results since each system can detect attacks which are missed by the other.

Table IV show the results for detection on the DSO, i.e., with a more limited feature set and with or without the addition of distributed IDS reports from individual CPOs, for attack scope AS_1. For DSO detection we only consider the `DecisionTreeRegressor` and CM_3 based on the previously discussed results. We only consider the ACN and emobpy data sets since they allow a straight forward way of splitting them into individual CPO data sets (Caltech, JPL, and Office for ACN; home and public for emobpy). The combination of CPO and DSO detection is implemented by a simple weighted voting ensemble, whereby one DSO collects the individual predictions of CPOs and combines them with the own predictions based on a weighted average. The results for attack scope AS_1 show worse performance for detection by the DSO with only the limited feature set in comparison to detection by the CPO (cf. Table I). Especially the high FPR for the ACN data sets is problematic. With inclusion of the distributed CPO IDS however, the DSO's detection can reach performance levels that surpass individual CPO detection. This shows the viability of large-scale distributed detection without requiring detailed charge session info on the DSO, which results in less overhead and arguably no privacy risks. The results for attack scope AS_2 (not shown) demonstrate slightly better performance of 3.75% in the basic DSO detection case and 0.76% in the case of distributed detection.

VII. Conclusion

The power grid is a critical infrastructure and its continuous operation is of upmost importance. Due to the close relationship between e-mobility and the grid, the grid's operation can be threatened by adversarial behavior in the e-mobility sector. This opens up the possibility of orchestrating attacks on the grid based on cyber attacks against e-mobility systems. These attacks on the grid are especially problematic if they are persistent and can be executed repeatedly causing great harm to power grid resilience. For this reason, concepts for the detection of e-mobility-based attacks on the grid are important.

In this paper, we provide a detailed analysis of related IDS work and of the potential attack vectors that exist in the current e-mobility system. Based on our analysis we present a novel IDS approach for the detection of e-mobility-based attacks on the grid. The IDS is a hybrid system consisting of rule- and anomaly-based IDSs and it is distributed across relevant e-mobility backend actors (CPOs and DSOs). The rule-based system aims to filter out basic attacks based on the observation that the e-mobility system contains several kinds of related/redundant data. Afterwards, the anomaly-based system detects more advanced attacks by using regression-based forecasting and comparing predicted values to received measurements to detect anomalies. Several different design choices for the anomaly-based system are discussed and evaluated.

The evaluation shows that most of the considered regression models can provide good detection performance for the considered attacks. Notably, the `DecisionTreeRegressor` model provided the overall best detection to false positive ratio. Regarding the classification of received measurements that diverge from predictions, the evaluation shows that the hour-specific threshold method performed generally the best. Additionally, the evaluation shows that efficient large-scale detection on the DSO is possible even without detailed session info, by using the distributed IDS predictions of individual CPOs as inputs. These results indicate that the proposed IDS could provide a meaningful increase in power grid resilience.

However, since the IDS is designed for larger attacks with the potential to harm grid stability, the detection smaller (e.g., session-specific) attacks is out-of-scope. Our evaluation also confirms this to be a limitation of the approach. The detection of small-scale attacks could be enhanced via the use of a session-level IDS to identify anomalies in individual charge sessions. A session-level IDS could, for instance, be implemented via regression-based forecasting for individual sessions. The effectiveness of this IDS design is currently not investigated by related work and is an option for future work.

Acknowledgment

This research work has been partly funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – project number 503329135.

REFERENCES

[1] M. Hollick and S. Katzenbeisser, "Resilient critical infrastructures," in *Information Technology for Peace and Security*, C. Reuter, Ed. Springer, 2019, pp. 305–318.

[2] K. Geers, "The challenge of cyber attack deterrence," *Computer Law & Security Review*, vol. 26, no. 3, pp. 298–303, 2010.

[3] D. Kern and C. Krauß, "Analysis of e-mobility-based threats to power grid resilience," in *Computer Science in Cars Symposium*, 2021, pp. 1–12.

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

[5] H. ElHussini, C. Assi, B. Moussa, R. Atallah, and A. Ghrayeb, "A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid," *ACM Transactions on Internet of Things*, vol. 2, no. 2, pp. 1–21, 2021.

[6] M. Zhdanova, J. Urbansky, A. Hagemeier, D. Zelle, I. Herrmann, and D. Höffner, "Local power grids at risk–an experimental and simulation-based analysis of attacks on vehicle-to-grid communication," in *Annual Computer Security Applications Conference*, 2022, pp. 42–55.

[7] S. Haverkamp and M. Simons, "Cybersecurity in the charging ecosystem – status quo and stakeholder ambitions," Report, 03 2022. [Online]. Available: https://www.charin.global/media/pages/news/charin-task-force-cybersecurity/af8d69da69-1645626738/20220203-charging-ecosystem-stakeholder-landscape-rev_1.3.pdf

[8] 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, 2022.

[9] F. Sommer, J. Dürrwang, and R. Kriesten, "Survey and classification of automotive security attacks," *Information*, vol. 10, no. 4, p. 148, 2019.

[10] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber resilient systems: A systems security engineering approach," NIST Special Publication 800-160, Volume 2, 11 2019.

[11] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[12] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[13] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2016.

[14] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *2017 North American Power Symposium (NAPS)*. IEEE, 2017, pp. 1–6.

[15] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.

[16] S. Ahmed and F. M. Dow, "Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems," in *2016 4th International Conference on Control Engineering & Information Technology (CEIT)*. IEEE, 2016, pp. 1–5.

[17] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019, pp. 1–5.

[18] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[19] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[20] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD cup 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*. Ieee, 2009, pp. 1–6.

[21] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[22] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *2011 IEEE Power and Energy Society General Meeting*. IEEE, 2011, pp. 1–8.

[23] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Systems journal*, vol. 9, no. 1, pp. 31–44, 2014.

[24] S. N. Mohan, G. Ravikumar, and M. Govindarasu, "Distributed intrusion detection system using semantic-based rules for SCADA in smart grid," in *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. IEEE, 2020, pp. 1–5.

[25] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[26] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206–213, 2015.

[27] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2019, pp. 1–6.

[28] G. Chen, Y. Qu, and D. Jin, "Cyber-physical simulation testbed for madiot attack detection and mitigation," in *Proceedings of the 2022 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation*, 2022, pp. 59–60.

[29] S. Madabhushi and R. Dewri, "Detection of demand manipulation attacks on a power grid," in *2021 18th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2021, pp. 1–7.

[30] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 1, pp. 478–487, 2020.

[31] A. Kavousi-Fard, T. Jin, W. Su, and N. Parsa, "An effective anomaly detection model for securing communications in electric vehicles," *IEEE Transactions on Industry Applications*, 2020.

[32] S. Abedi, A. Arvani, and R. Jamalzadeh, "Cyber security of plug-in electric vehicles in smart grids: application of intrusion detection methods," in *Plug In Electric Vehicles in Smart Grids*. Springer, 2015, pp. 129–147.

[33] D. Coats, H. Suryanarayana, Z. Wang, A. Brissette, Y. Zhang, V. Ramanan, D. Scoffield, D. Woodbury, N. Haltmeyer, and A. Benzinger, "Final scientific/technical report-cybersecurity for grid connected extreme fast charging (XFC) station (CyberX)," ABB, Inc., Cary, NC (United States), Tech. Rep., 2021.

[34] J. Cumplido, C. Alcaraz, and J. Lopez, "Collaborative anomaly detection system for charging stations," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 716–736.

[35] S. Shahriar, A.-R. Al-Ali, A. H. Osman, S. Dhou, and M. Nijim, "Machine learning approaches for EV charging behavior: A review," *IEEE Access*, vol. 8, pp. 168 980–168 993, 2020.

[36] O. Frendo, N. Gaertner, and H. Stuckenschmidt, "Improving smart charging prioritization by predicting electric vehicle departure time," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 10, pp. 6646–6653, 2020.

[37] M. Majidpour, C. Qiu, P. Chu, R. Gadh, and H. R. Pota, "A novel forecasting algorithm for electric vehicle charging stations," in *2014 International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2014, pp. 1035–1040.

[38] Y. Lu, Y. Li, D. Xie, E. Wei, X. Bao, H. Chen, and X. Zhong, "The application of improved random forest algorithm on the prediction of electric vehicle charging load," *Energies*, vol. 11, no. 11, p. 3207, 2018.

[39] L. Gan, U. Topcu, and S. H. Low, "Optimal decentralized protocol for electric vehicle charging," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 940–951, 2012.

[40] C. Eid, E. Koliou, M. Valles, J. Reneses, and R. Hakvoort, "Time-based pricing and electricity demand response: Existing barriers and next steps," *Utilities Policy*, vol. 40, pp. 15–25, 2016.

[41] Maigha and M. L. Crow, "Cost-constrained dynamic optimal electric vehicle charging," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 2, pp. 716–724, 2016.

[42] OCA, "Open Smart Charging Protocol 2.0," Open Charge Alliance, Arnhem, Netherlands, Open Standard, 10 2020. [Online]. Available: https://www.openchargealliance.org/protocols/oscp-20/

[43] ——, "Open Charge Point Protocol 2.0.1 - Part 0 - Introduction," Open Charge Alliance, Arnhem, Netherlands, Open Standard, 3 2020. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/

[44] ISO/IEC, "Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements," ISO, Geneva, Switzerland, ISO Standard 15118-2:2014, 4 2014.
[45] S.-K. Joo, J.-C. Kim, and C.-C. Liu, "Empirical analysis of the impact of 2003 blackout on security values of us utilities and electrical equipment manufacturing firms," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1012–1018, 2007.
[46] G. B. Anderson and M. L. Bell, "Lights out: impact of the august 2003 power outage on mortality in new york, ny," *Epidemiology (Cambridge, Mass.)*, vol. 23, no. 2, p. 189, 2012.
[47] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, vol. 4, no. 447-462. San Francisco, 2011, p. 2021.
[48] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," 8 2015.
[49] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.
[50] N. Kroener, K. Förderer, M. Lösch, and H. Schmeck, "State-of-the-art integration of decentralized energy management systems into the german smart meter gateway infrastructure," *Applied Sciences*, vol. 10, no. 11, p. 3665, 2020.
[51] J. Amat Rodrigo and J. Escobar Ortiz, "Skforecast: time series forecasting with python and scikit-learn," Tech. Rep., 8 2022. [Online]. Available: https://www.cienciadedatos.net/documentos/py27-time-series-forecasting-python-scikitlearn.html
[52] S. B. Kotsiantis, "Decision trees: a recent overview," *Artificial Intelligence Review*, vol. 39, no. 4, pp. 261–283, 2013.
[53] G. Ristanoski, W. Liu, and J. Bailey, "Time series forecasting using distribution enhanced linear regression," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 2013, pp. 484–495.
[54] M. Awad and R. Khanna, "Support vector regression," in *Efficient learning machines*. Springer, 2015, pp. 67–80.
[55] C. Bentéjac, A. Csörgő, and G. Martínez-Muñoz, "A comparative analysis of gradient boosting algorithms," *Artificial Intelligence Review*, vol. 54, no. 3, pp. 1937–1967, 2021.
[56] A. R. Khan, A. Mahmood, A. Safdar, Z. A. Khan, and N. A. Khan, "Load forecasting, dynamic pricing and dsm in smart grid: A review," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1311–1322, 2016.
[57] D. Kern, T. Lauser, and C. Krauß, "Integrating privacy into the electric vehicle charging architecture," *Proceedings on Privacy Enhancing Technologies*, vol. 3, pp. 140–158, 2022.
[58] R. J. Hyndman and G. Athanasopoulos, *Forecasting: principles and practice*. OTexts, 2018.
[59] Z. J. Lee, T. Li, and S. H. Low, "ACN-Data: Analysis and Applications of an Open EV Charging Dataset," in *Proceedings of the Tenth International Conference on Future Energy Systems*, ser. e-Energy '19, Jun. 2019.
[60] ElaadNL, "ElaadNL open EV charging transactions," 2019. [Online]. Available: https://platform.elaad.io/download-data/
[61] C. Gaete-Morales, H. Kramer, W.-P. Schill, and A. Zerrahn, "An open tool for creating battery-electric vehicle time series from empirical data, emobpy," *Scientific data*, vol. 8, no. 1, pp. 1–18, 2021.
[62] S. Hardman, A. Jenn, G. Tal, J. Axsen, G. Beard, N. Daina, E. Figenbaum, N. Jakobsson, P. Jochem, N. Kinnear *et al.*, "A review of consumer preferences of and interactions with electric vehicle charging infrastructure," *Transportation Research Part D: Transport and Environment*, vol. 62, pp. 508–523, 2018.
[63] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and tools for network simulation*. Springer, 2010, pp. 15–34.
[64] tritiumdev, "cereal-ocpp2." [Online]. Available: https://github.com/tritiumdev/cereal-ocpp2
[65] P. Biondi, "Scapy." [Online]. Available: https://github.com/secdev/scapy
[66] The Mobility House, "OCPP implementation." [Online]. Available: https://github.com/mobilityhouse/ocpp
[67] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
[68] J. Amat Rodrigo and J. Escobar Ortiz, "skforecast." [Online]. Available: https://github.com/JoaquinAmatRodrigo/skforecast/
[69] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty, "Security challenges in automotive hardware/software architecture design," in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2013, pp. 458–463.