Analysis of E-Mobility-based Threats to Power Grid Resilience

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

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

ABSTRACT

The increasing complexity of the e-mobility infrastructure leads to an increasing risk of security threats, which may negatively affect any connected infrastructures such as the power grid. The grid is one of the most important critical infrastructures, making it a valuable target for cyber attacks. This situation gives rise to the potential of e-mobility-based attacks to the grid, e.g., causing large-scale black outs based on a sudden increase in charging demand. In this paper, we propose a framework for simulating and analyzing the impact of e-mobility-based attacks on grid resilience. We derive e-mobility-specific attacks, based on an analysis of adversaries and threats, and combine these attacks in our framework with models for grid and e-mobility as well as simulation-based outage analysis. In different case studies, the effects of e-mobility-based attacks on grid resilience are evaluated. The results show, e.g., the scope of increased vulnerability during peak load hours, enabling attacks even at low levels of e-mobility compromise, the increased impact of combined attack strategies, and the time from attack to outage, which may decrease to sub-second ranges for high levels of e-mobility growth and compromise. We further discuss potential protection mechanisms for different resilience objectives including approaches for detection, prevention, and response. This work thus provides the basis for comprehensive resilience research regarding the interconnection of e-mobility and grid.

CCS CONCEPTS

• **Security and privacy → Systems security**; *Distributed systems security*; *Denial-of-service attacks*; *Vulnerability management*.

KEYWORDS

Electric Vehicles, E-Mobility, Manipulation of Demand Attacks, False Data Injection Attacks, Power Grid, Resilience

ACM Reference Format:
Dustin Kern and Christoph Krauß. 2021. Analysis of E-Mobility-based Threats to Power Grid Resilience. In *Computer Science in Cars Symposium (CSCS '21), November 30, 2021, Ingolstadt, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3488904.3493385

1 INTRODUCTION

As a critical infrastructure, power grids must maintain their functionality under any circumstances since a large-scale power outage could negatively affect the lives of millions of people. Of paramount importance is the protection against cyber attacks, since the grid is an attractive target for sophisticated attacks [Hollick and Katzenbeisser 2019] with an increasing risk of cyber attacks by nation-states [Geers 2010]. Perimeter-based security fails to protect against today's threats, making alternative approaches such as cyber resiliency necessary. 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" [Ross et al. 2019].

A major challenge is the secure integration of e-mobility. Due to the close link between e-mobility infrastructure and power grid, any disturbances or changes in behavior of one can have grave effects on the other. For instance, it is commonly predicted that, due to the steady growth of the Electric Vehicle (EV) market, an uncontrolled charging of EVs will have negative effects on the power grid ranging from lower power quality, over a decline in transformer life span, to increased line loss [Xiao et al. 2014]. This issue can be addressed via controlled charging (e.g., by shifting the bulk of EV load to night hours) [Verzijlbergh et al. 2012] and moreover, the use of Vehicle to Grid (V2G) power transfer could even be used to increase grid stability [Tan et al. 2016]. Both of these methods, however, generally require a trustworthy e-mobility infrastructure that faithfully implements the grid-friendly charging schedules (defining consumption over time) and V2G strategies. Thus, when considering an active attacker with (partial) control over the e-mobility infrastructure, traditional methods for grid stability fail and the threat of targeted demand-side attacks arises. For example, an attacker controlling a botnet of compromised EVs or Charge Points (CPs) can manipulate the charging schedules in order to perform demand-side attacks causing line failures and power outages. For the development of resiliency solutions, it is necessary to know the behavior of the power grid under attack and what impact the attacker can cause.

In this paper, we propose a framework for simulating and analyzing the impact of e-mobility-based attacks on the resilience of the power grid against these kinds of attacks. The framework combines models for e-mobility and power grid with different types of identified attacks to simulate and analyze possible grid outages. It shows at what times of a day attacks are most easily carried out, how many compromised CPs and EVs are needed for successful attacks, and how much time is available to respond to attacks before a power outage occurs. With our implementation of the framework, we analyze several case studies showing the impact of the different attacks. In addition, we propose and discuss possible protection mechanisms to increase the resilience of the power grid against e-mobility-based attacks.

The remainder of this paper is structured as follows: we distinguish our work from related work in Section 2. Section 3 describes

CSCS '21, November 30, 2021, Ingolstadt, Germany

ACM ISBN 978-1-4503-9139-9/21/11.
https://doi.org/10.1145/3488904.3493385

our assumed system model and in Section 4 the assumed adversary model. We introduce our framework in Section 5 and describe the implementation and evaluation of the case studies in Section 6. Possible protection methods to increase resiliency are discussed in Section 7. Finally, we conclude the paper in Section 8.

2 RELATED WORK

The successful cyber attacks on the Ukrainian power grid in 2015 and 2016 [Case 2016; Kshetri and Voas 2017] have shown that security is of paramount importance with regard to any communication or control mechanisms related to the power grid. Dynamic load altering attacks against power grid stability are discussed in [Amini et al. 2016] where the attacker controls the changes in the victim load based on a feedback from the power system frequency. They also discuss a possible protection scheme. Dvorkin and Garg propose a modeling framework to analyze the impact of distributed cyber attacks via Internet of Things (IoT)-controlled loads on power grids [Dvorkin and Garg 2017]. The framework can model an attacker that has hacked several IoT-controlled loads to alternate their net power injections into the electrical grid to disrupt normal grid operations. Soltan et al. discuss the use of an IoT botnet of high wattage devices to disrupt the power grid by the use of so called Manipulation of demand via IoT (MadIoT) attacks [Soltan et al. 2018]. Based on simulations, Soltan et al. demonstrate that a botnet of compromised high wattage devices such as air conditioners can be used to manipulate the power demand in the grid and disrupt normal operation.

With the integration of e-mobility into the power grid, the security of the e-mobility infrastructure is becoming increasingly important. Security issues of the e-mobility charging infrastructure are discussed in [Pratt and Carroll 2019] and of CPs in [Gottumukkala et al. 2019]. An overview of security issues of EVs connected to other vehicles, road infrastructure systems, Internet systems etc. is given in [Fraiji et al. 2018]. The security of ISO/IEC 15118 (a protocol for the communication between EVs and CPs) is analyzed in [Bao et al. 2018] showing several scenarios for successful attacks. Baker and Martinovic show that electromagnetic side-channel attacks on the Power Line Communication (PLC) of ISO/IEC 15118 are possible to eavesdrop on the communication [Baker and Martinovic 2019]. They also identified security issues in real systems, e.g., the widespread absence of TLS in public locations or the leakage of private information such as long-term unique identifiers. Security threats of Open Charge Point Protocol (OCPP) (a protocol for the communication between CPs and their operator) are discussed in [Alcaraz et al. 2017].

Several works address security and privacy for e-mobility. For example, the integration of Hardware Security Modules (HSMs) into ISO/IEC 15118 to protect critical data such as credentials is proposed in [Fuchs et al. 2020a,b,c,d]. A protection mechanism against man-in-the-middle attacks on OCPP is proposed in [Rubio et al. 2018]. In [Zelle et al. 2018], the authors propose a mechanism for privacy-preserving charging and billing. However, none of these works addresses the impact on the power grid.

The general potential of e-mobility based attacks on the grid is discussed in [Ahmed and Dow 2016; Pratt and Carroll 2019]. In [Mousavian et al. 2015], a probabilistic model for the worm propagation between EVs and CPs is proposed. The model is used to evaluate threat levels and afterwards isolate infected nodes in order to minimize the potential of attacks to the power grid. The work presented in [ElHussini et al. 2021] and [Acharya et al. 2020] is closest to ours by analyzing EV-based attacks on the power grid. The authors of [ElHussini et al. 2021] propose three attack variations (sudden surge in power demand, sudden surge in power supply, and a switching attack) to cause disturbances to the grid frequency and perform a simulation-based study to show the possible effects of successful attacks. The authors of [Acharya et al. 2020] evaluate how a demand-side attack can cause frequency instability in the power grid and show the potential of attack optimization via publicly available data. They also perform simulations to evaluate the impact of this attack on the power grid of Manhattan, NY, USA.

In contrast to related work, our work considers the full range of attack vectors that result from the complex e-mobility infrastructure. Additionally, our work aims for a more comprehensive consideration of the possible e-mobility effects on grid resiliency, which is important due to the high criticality of the power grid infrastructure.

3 E-MOBILITY SYSTEM MODEL

In this section, we briefly describe our assumed e-mobility system model and the connection between e-mobility infrastructure and power grid.

From a power grid perspective, an EV is a new mobile power consumer with relatively large power and high difficulty to plan energy demand, high storage capacity, and optional time flexibility of power demand. E-mobility must be integrated into the power grid in a way that serves the grid in order to keep power generation and power consumption in balance. This requires (bidirectional) communication between EV 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 required in order to adapt the charging power to the available electricity.

EVs can be charged at CPs in private, semi-public, or public locations. Typical charging powers at private locations range from 3.7 kW to 11 kW, in some cases even up to 22 kW. The EVs are often charged overnight at home at a wallbox and can thus be very well integrated into a load management system. At semi-public locations, CPs with 11 or 22 kW charging power are usually found. Here, too, the EVs can be well integrated into a load management, e.g., as long as the EV is charged during the day in the parking lot at work. CPs with 11 or 22 kW for so-called normal charging can also be found at public locations. However, there are also more and more fast CPs with up to 150 kW, e.g., at highway rest stops where EVs have to be charged as quickly as possible. Charging capacities of up to 450 kW are also being standardized. At public locations, load management is more difficult to implement. At highway rest stops, time-based load management is hardly feasible. Nevertheless, the charging power can be adapted to the available electricity. For public charging with longer standing times, e.g., at CPs integrated in streetlights, load management could be implemented.

Figure 1 shows our assumed system model with the close connection of e-mobility infrastructure and power grid.

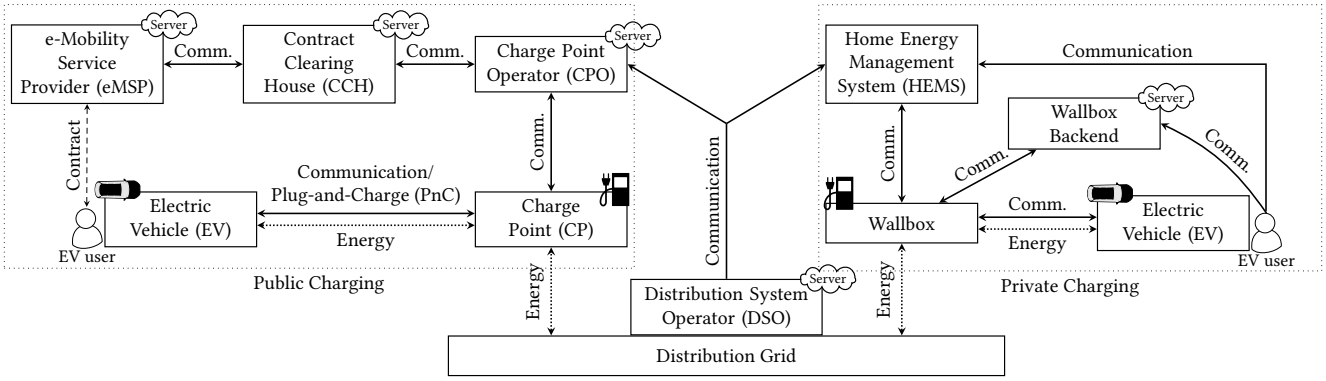

Figure 1: E-Mobility System Model

The right part shows private charging where the EV is charged at a CP for example at home at a wallbox. The charging event can be influenced regarding the charging power and can be shifted in time remotely by the Distribution System Operator (DSO) via the EV user's Home Energy Management System (HEMS). In addition, the charging event can be influenced by the EV user, either by accessing a wallbox backend system which communicates via OCPP with the wallbox or via the HEMS. Additionally, the EV itself could influence the charging schedule. However, the DSO has always the highest priority in performing load management to ensure grid stability.

The left part shows charging at public CPs. The EV user has a contract with an e-Mobility Service Provider (eMSP) and either receives External Identification Means (EIM) credentials, e.g., an RFID card which is presented at the CP for authorization (not shown), or contract credentials which are installed in the EV enabling Plug-and-Charge (PnC) according to ISO/IEC 15118 [ISO/IEC 2014]. In the latter case, the EV user then only needs to connect the charging cable and authentication, negotiation of charging parameters, etc. is done automatically via PLC over the charging cable and no further user interaction is required. The CP is operated by a Charge Point Operator (CPO) and communication is done via OCPP or IEC 63110. The CPO communicates with the eMSP, e.g., via Open Charge Point Interface (OCPI) (cf. [ElaadNL 2017]), for authentication and billing processes. In case of roaming, i.e., the EV is charged at a CP where the user has no contract, a Contract Clearing House (CCH) can serve as intermediary between the different parties. The DSO provides energy to the CPs of the CPO and communicates via Open Smart Charging Protocol (OSCP) with the CPO to provide information such as capacity forecasts. Load management can be performed by the DSO directly, especially in critical cases to ensure grid stability, the CPO by sending load profiles to the charging EVs, or the eMSP by sending variable price tariffs which are negotiated via ISO/IEC 15118. Charging at semi-public CPs can either be the same as the private or public scenario or a combination of both.

The e-mobility system model is currently still being further developed. In the near future, bidirectional charging enables application such as vehicle to home (V2H) for energy transfer between EVs and the home system and V2G for feeding energy from the EV back into the power grid.

4 ADVERSARY MODEL

A successful attack to the power grid could negatively affect the lives of millions of people, with consequences ranging from significant economic damages to severe harm of human health [Anderson and Bell 2012; Joo et al. 2007]. The grid thus represents a high value target with an increased risk of sophisticated attacks by potent adversaries. Due to the general potential of high-wattage devices to disrupt the grid [Soltan et al. 2018] in combination with the close link between e-mobility and grid, we thus consider the following strong but realistic e-mobility-based adversaries to grid resilience:

E-Mobility Backend Hacker: The e-mobility infrastructure (cf. Section 3) includes a variety of backend systems that can all have an effect on the charging behavior of EVs/CPs. If an adversary is able to spoof or take control of one or more of these systems, an attack to the power grid (e.g., by altering the charging behavior of a large amount EVs/CPs) may be possible. That the successful hack of e-mobility backend systems is a realistic threat to consider is demonstrated by the many successful attacks on corporate/industrial systems of the past such as the 2013 Yahoo hack in which over 1bn accounts were compromised [Thielman 2016], the 2014 Sony hack, which resulted in the first attribution of a cyber attack to a nation-state by a US president [Haggard and Lindsay 2015], or Stuxnet, which affected approximately 100,000 hosts while targeting industrial control systems primarily in Iran [Falliere et al. 2011]. Moreover, the potential of a cyber attack to a corporate/industrial system being used to attack the power grid is exemplified by the successful attacks to the Ukrainian grid in 2015 and 2016, which led to significant blackouts based on compromises to the grid operators' computer systems [Case 2016; Kshetri and Voas 2017]. The threat of similar cyber attacks to power grids around the world is often considered to be realistic [Sullivan and Kamensky 2017]. Thus, the potential of attacks to the grid based on compromised e-mobility backend systems should not be neglected.

Botnet of EVs/CPs: Similar to the high wattage IoT device-based attacks [Soltan et al. 2018], a botnet of EVs/CPs may be used to adversely affect the grid. That the successful establishment of a large scale botnet is a realistic threat to consider is demonstrated by the variety of real-world botnet-based attacks in

the past [Kolias et al. 2017], most famously the Mirai botnet with an estimated peak of 600,000 infected devices, which was used to conduct over 15,000 attacks including high-profile targets such as the Domain Name System (DNS) provider Dyn [Antonakakis et al. 2017]. Additionally, it is not uncommon that locally/remotely exploitable vulnerabilities in vehicles are exposed (cf., e.g., [Checkoway et al. 2011]), which may enable the establishment of a botnet. The most prominent example is the 2015 Jeep hack [Miller and Valasek 2015], which could be exploited via a vehicle's cellular interface and enabled an adversary to remotely take (partial) control of the vehicle's internal systems leading to a recall of 1.4m vehicles. Similarly, vulnerabilities in CPs are not uncommon. For instance, in [Dalheimer 2017] a CP could be compromised through the installation of a custom firmware via physical access to a local interface (allowing full control of the CP), in [Dmitry Sklya 2018] a CP could be compromised through its wireless interfaces due to insecure input processing (allowing full control of the CP), and in [ElHussini et al. 2021] CPs could be compromised remotely due to the insecure configuration of their web interfaces with default username/password (allowing access to the CPs' web interface-controlled functions, including charge schedules). Thus, the potential of attacks to the grid based on a botnet of EVs/CPs should not be neglected.

Based on these adversaries, we identify the following e-mobility-based attack vectors to grid resilience:

(1) *Manipulation of charge schedules:* An adversary who has compromised a grid operator[1] or can spoof a grid operator to a CPO (e.g., due to a security flaw in the used communication protocol or a leaked private key) can send manipulated grid capacity forecasts leading the CPO to generate charge schedules that may exceed the actual grid capacity. Similarly, an adversary who has compromised a CPO or can spoof a CPO to CPs can directly instruct any affected CP to change its charge schedule to exceed grid capacity.
An adversary with a botnet of compromised CPs can directly change their charge schedules in order to conduct demand-side attacks to the grid. Furthermore, an adversary with a botnet of compromised EVs can alter their charge schedule selection (within the bound of offered schedules) with potentially harmful effects to the grid.

(2) *Manipulation of charge prices:* The designs of load balancing mechanism are commonly based on price incentives in order to couple the goals of grid operators and customers (e.g., cheaper prices during off-peak hours) [Eid et al. 2016; Gan et al. 2012; Maigha and Crow 2016]. Thus, an adversary that can manipulate the reported electricity prices can indirectly influence the charge schedule selection of EV users (or EVs if they are pre-programmed to charge based on user preferences) and with that the adversary can affect the electricity demand at select times. An adversary who has compromised an eMSP or can spoof an eMSP to the CCH or CPOs can define manipulated price data. Similarly, if price data is not end-to-end authenticated, then a compromised/spoofed CCH, CPO, or CP may also manipulate price data. In case of private charging, the respective target would usually be the electricity provider or DSO. If an adversary can incentivize enough EVs/users to charge at inopportune times, they may be able to cause grid overload scenarios.

(3) *Manipulation of reported data:* The possibility of false data injection attacks against state estimation in the power grid is a general issue [Liu et al. 2011] and a similar threat arises in the context of e-mobility integration. In order to accurately predict and plan for the available/required grid capacity in an area, the grid operator is informed about the e-mobility demand. The respective e-mobility data includes current measurements of CPs, the EVs' selected charge schedules, and CP reservations (allowing the derivation of the future energy demand at CPs). While a compromised/spoofed eMSP or CCH could only manipulate the reported CP reservations, a compromised/spoofed CPO could manipulate any of these values. Additionally, a botnet of compromised CPs could be used to report manipulated measurements and charge schedule selections. The malicious manipulation of these values may lead to an underestimation of demand, i.e., to an overestimation of available grid capacity and thus cause grid overload scenarios.

[1] Assuming the grid operator compromise does not allow the adversary to directly influence the grid, e.g., if the compromise only affects the grid operator's system that is used for communication with CPOs.

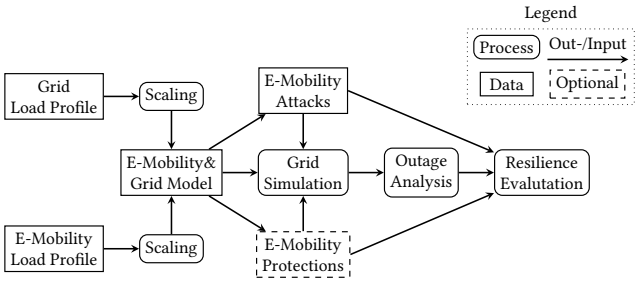

Figure 2: Overview of Analysis Framework

5 FRAMEWORK FOR E-MOBILITY-BASED GRID ATTACK ANALYSIS

The general idea for e-mobility-based grid attack analysis is to use a combined e-mobility/grid model with simulation-based grid outage analysis while applying the attacks from Section 4 (cf. Fig. 2). Grid and e-mobility load profiles are scaled to the desired scenario (e.g., reflecting a certain penetration of EVs) such that the resulting e-mobility/grid models allow for the analysis of different realistic use cases. The model is used as basis for the implementation of e-mobility-base attack scenarios, possibly considering additional protection methods, which serves as input for the simulation based grid outage analysis. The results, under consideration of attacks and protections, can then be used for resilience-related evaluations.

5.1 E-Mobility and Grid Model

As the grid attack analysis is based on a model of e-mobility and grid, it is important for a meaningful analysis that this model reflects a realistic scenario. For power grids, fine-grained load profiles are commonly available for larger scale networks. For smaller scale distribution networks, privacy-protection often hinders the availability

of detailed profiles, making synthetic datasets the more promising solution [Zhang et al. 2018]; especially, considering that energy consumers usually exhibit distinct and predictable load profiles [Kim et al. 2011], which allows synthetic datasets to be reasonably representative of realistic scenarios.

Similarly, an e-mobility model may be derived from public data (cf., e.g., [Acharya et al. 2020]). Public e-mobility data, however, usually can only represent the load profiles of public CPs and thus does not reflect charging at home or at work. Considering that the (large scale) charging behavior of EV users too is predictable [Gaete-Morales et al. 2021; Qian et al. 2010], synthetic models for e-mobility load are a promising alternative, capable of reflecting relevant parameters (current load, grid availability, State of Charge (SoC), etc.) at fine-grained time intervals. Furthermore, synthetic models may be used to represent different load balancing strategies (e.g., instant charging or shifting charges to off-peak hours) and their effect on the discussed e-mobility attacks.

By scaling both kinds of input data, a combined e-mobility and grid model can be built. The data could, for instance, be scaled to represent the same scenario if the data comes from different sources or be scaled to represent the desired situation such as peak load times or the future growth of the e-mobility sector. The combined model is thus suited for a detailed analysis of the interdependence between the two infrastructures in any given scenario.

5.2 Grid Simulation and Outage Analysis

For the analysis of failures in a power system, it is common practice to use simulation models, most importantly, *(i)* models using transient analysis with detailed system dynamics and *(ii)* models using AC power flow-based steady-state analysis [Huang et al. 2019]. Transient analysis can model detailed voltage and frequency control properties of generators [Ma and Chowdhury 2006]. Steady-state analysis can model cascading outages due to line overloads and/or unacceptable voltage conditions [Henneaux et al. 2018]. With regard to cascading outages, several grid protection mechanisms are relevant [Huang et al. 2019]: *(i)* over-/underfrequency protections, which may initiate controlled load shedding if the grid frequency is too low or may disconnect generators to prevent hardware damage if the frequency is too high/low, *(ii)* overcurrent protections, which may disconnect power lines if their current is too high, and *(iii)* over-/undervoltage protection, which may initiate generator disconnects or load shedding if the voltage is too high/low. Overcurrent and over-/undervoltage protections are commonly based on inverse-time relays [Mirko 2008; Siemens 2005; Wang and Baldick 2013], initiating protective actions after a time that is calculated based on the following equations:

$$\text{Overcurrent: } t = \frac{0.14}{(I/I_S)^{0.02} - 1}\text{TMS}[s] \tag{1}$$

$$\text{Overvoltage: } t = \frac{\text{TMS}}{(V/V_S) - 1}[s] \tag{2}$$

$$\text{Undervoltage: } t = \frac{\text{TMS}}{1 - (V/V_S)}[s] \tag{3}$$

Where t is the tripping time in seconds, TMS is the time multiplier setting, I is the measured current, I_S is the relay setting current, V is the measured voltage, and V_S is the relay setting voltage.

By using the combined e-mobility and grid model as the basis for simulation, the detailed effects of e-mobility-based attacks on grid resilience can be evaluated during outage analysis. The e-mobility-based attacks discussed in Section 4 can initiate cascading outages in different ways. An increase in demand either through a manipulation of charge schedules, prices, or reported data would increase currents and decrease frequencies/voltages, thus, potentially triggering the respective protections. Similarly, a decrease in demand or increase in V2G power transfer through any of the mentioned manipulations would increase frequencies/voltages and thus potentially triggering the respective protections. Additionally, combinations of the different adversaries and attacks are possible, e.g., a botnet of CPs could be used to increase the demand of affected charging sessions via manipulated charge schedules while a compromised eMSP backend system simultaneously indicates reduced charge prices in order to increase the demand at charging sessions that are not directly affected by the botnet. While e-mobility (or general smart grid) protection measures are not investigated in detail in this paper, their influence on grid resilience can be analyzed similarly during simulation. In addition, this approach is suitable for analyzing the interdependence between the initial conditions, attacks, and protections (e.g., with regard to EV penetration, method of compromise, and response timings).

5.3 Resilience Evaluations

As previously mentioned, the close relation between e-mobility and power grid motivates considerations from a resilience perspective. That is, it is important to, under consideration of the interdependence of grid and e-mobility, evaluate the combined system's ability to anticipate, withstand, recover from, and adapt to adversarial and non-adversarial disruptions/threats (cf. [Ross et al. 2019]).

For the evaluation of resilience, corresponding metrics are generally based on an assessment of the system's performance level before, during, and after a disruption in order to capture the negative effects of the disruption throughout its entire lifespan as well as positive effects of potential prevention-, detection-, response-, adaption-, and recovery-related measures [Bodeau et al. 2018]. Within the context of the power grid, resilience-related performance levels can cover a wide variety of aspects, including the timely delivery of meter data, the timely curtailment of demand for load balancing, the timely identification of and recovery from outages, or the timely detection of and response to security threats before other operations are effected [AlMajali et al. 2012].

Within the context of simulation-based outage analysis, we focus on the continued delivery of electricity as main performance indicator. Thus, with regard to the analysis of e-mobility-based threats to grid resilience, i.e., from an adversary's perspective, we are primarily concerned with the amount of outage over time while considering adversarial threats (cf. Section 4) as well as non-adversarial threats (e.g., peak loads or a naturally increasing e-mobility electricity demand). For a more thorough evaluation of resilience in this context, respective protection measures may be included in order to represent important functions like prevention, response, or recovery (cf. Section 7).

6 IMPLEMENTATION AND CASE STUDIES

The framework for e-mobility-based grid attack analysis was implemented in Python using pandapower [Thurner et al. 2018] for grid simulation, specifically, AC steady-state analysis. Thus, outage analysis assumes that the attacks do not cause frequency instabilities. Considering that in [Soltan et al. 2018] frequency instabilities required much larger attacks than line outages, we consider this assumption reasonable. The implementation of the outage analysis process is based on the general AC cascading failure model described in [Cetinay et al. 2018], using the more detailed grid protections as discussed in Section 5.2.

Regarding grid protections, the value I_S of Equation 1 is set to 1.5 × the rated current (I_N) of the line (cf. [Siemens 2005]) and to 2 × I_N in case of initially overloaded lines (cf. [Cetinay et al. 2018]), using the values of the pandapower models for I_N. The overvoltage value V_S of Equation 2 is set to 1.3 pu and the undervoltage value V_S of Equation 3 is set to 0.8 pu (cf. [Huang et al. 2019]). The TMS values are set to 0.05 for Equation 1 and 0.5 for Equations 2 and 3 [Huang et al. 2019]. For undervoltage load shedding at a bus, a default value of 25% is used [Song et al. 2015].

EVs are modeled as electricity storages in pandapower and the corresponding e-mobility load profile is based on the synthetic dataset with hourly precision generated with the tool *emobpy* described in [Gaete-Morales et al. 2021]. This data describes the vehicle mobility, driving consumption, grid availability, grid demand, and SoC of 200 representative EV profiles over the year (cf. [Gaete-Morales et al. 2021]). Notably, grid availability indicates whether and with which power rating an EV is connected to the grid, including level 1 (3.6 kW), 2 (11 or 22 kW), and 3 (75 or 150 kW) charging (0 kW if not connected). Additionally, grid demand and SoC are each calculated for different charging/load balancing strategies, namely *immediate full capacity* (no load balancing), *immediate balanced* (immediate charging but at a reduced rate, such that a full SoC is reached just in time before departure), *at home balanced* (similar to the previous one but only at home), and *at home night-time balanced* (similar to the previous one but only at night).

The e-mobility load profile is scaled to the desired scenario from the 200 EV profiles for a specific point in time by means of weighted random sampling, whereby the weights are based on the distributions of level 1, 2, and 3 charging demand as reported/estimated in [Engel et al. 2018] for the European Union in the years 2020 and 2030, i.e., 36%, 58%, 6% and 7%, 61%, 32% respectively. The grid load profile data and scaling are discussed in the following subsections.

6.1 Case Study 1: MV Oberrhein

For the first case study, we use the synthetic Medium Voltage (MV) distribution system MV Oberrhein as provided in pandapower. In order to represent changes in load over time, we use public load profile data from an MV system [EWE Netz 2020] (specifically MS I; using the mean load per hour as the data is provided with 15 min precision). The load profile is scaled to fit the peak within the capacity of the MV Oberrhein system.

We consider two EV penetration scenarios for Germany (cf. [Federal Ministry of Transport and Digital Infrastructur 2021]), namely *(i)* the current (2020 in the following) scenario with 1,000,000 EVs and *(ii)* a 2030 scenario with 14,000,000 EVs; assuming the previously mentioned distributions of level 1, 2, and 3 charging from [Engel et al. 2018]. Additionally, we assume a steady population of 83,000,000 in Germany [Federal Statistical Office (Destatis) 2019] and a population of 36,413 for the area that the MV Oberrhein system is designed to cover [Statistisches Landesamt Baden-Württemberg 2021], resulting in 439 EVs for the 2020 scenario and 6,142 EVs for 2030.

The respective amounts of EVs for the 2020 and 2030 cases are sampled from the EV charging data [Gaete-Morales et al. 2021] per hour as previously described. The resulting hourly EV loads are added to the default grid load and the resulting cumulative load is again scaled to fit the peak within the capacity of the MV Oberrhein system. The load profiles of this combined e-mobility and grid model for the 2030 scenario with the four different load balancing strategies as well as without EV loads are shown in Fig. 3. Specifically, the more pale-colored lines in Fig. 3 show the mean power consumption per hour of day, group by business days, Saturdays, and Sundays, over the four seasons.

Based on this model, we evaluate the attack potential of an e-mobility-based adversary to the grid. Hereby, we focus on the *outage* as the loss in demand as a result of the attack [Soltan et al. 2018]. The attack consists of increasing the active charging power of any adversary controlled charging process with a not full SoC to the respective grid availability (based on the data from [Gaete-Morales et al. 2021]). For this, the adversary controlled charging processes are picked randomly and the scope of adversary control is reported as *compromise* (e.g., a compromise of 50% may reflect a compromised backend system that controls 50% of the CPs or a botnet that incorporates 50% of CPs in the area). This attack reflects the manipulation of charge schedules or charge prices (assuming a change of charge price enables an increase to grid availability) as described in Section 4.

In order to evaluate an adversaries attack potential over the year, we simulated this attack for the different models and at different levels of compromise (in 25% steps) for every hour of the year. In the 2020 scenario, no attack lead to an outage. In the 2030 scenario, attacks lead to outage starting at 50% compromise. Notably, an exception was the immediate full capacity load balancing strategy, which never resulted in any outage. This is a result of the EVs mostly sitting at full SoC such that even a 100% compromise did not result in enough demand for a successful attack. While this could be interpreted as a positive, it is worth noting that every (considered) adversary who is able to increase demand is also able to lower it (e.g., directly via the charge schedule or indirectly by increasing the charging price; cf. Section 4). Hence, in the following, we consider an adversary who prepares their demand increase attack by first stopping or lowering the speed of any controlled charging process and is thus always able to increase the active charging power to the respective grid availability.

While, with the modified attack, no outages occurred in the 2020 scenario, in the 2030 scenario, outages started at 50% compromise for all load balancing strategies. The resulting mean outages over the year are shown in Fig. 3. With the modified attack, the immediate full capacity load balancing strategy generally results in the highest outages due to the overall increased demand and also results in the highest peak of 12.28% mean outage during winter business

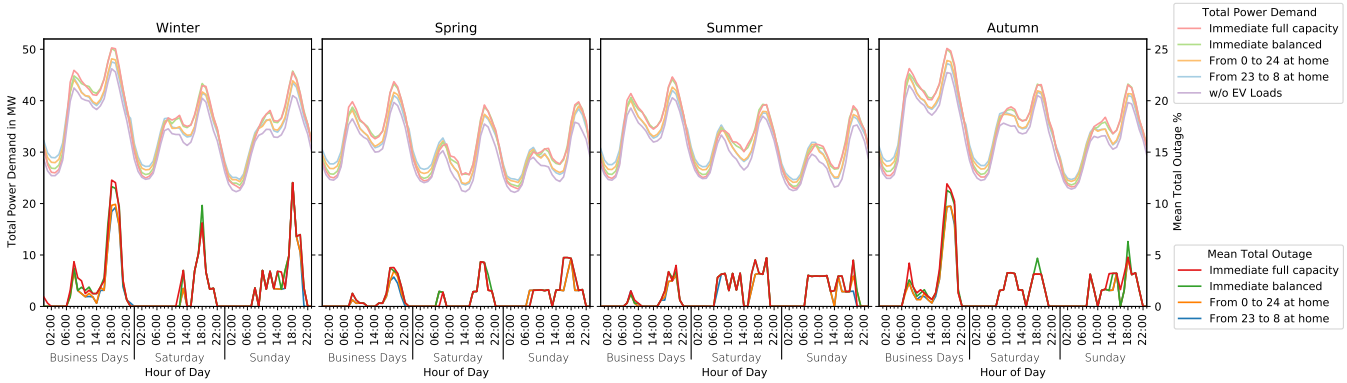

Figure 3: Base Grid Load Compared to Outage % in MV Oberrhein Scenario 2030 at 50% Compromise

days at 18:00. The other load balancing strategies only show minor differences. Further results are that the difference between load balancing strategies becomes smaller with increasing compromise percentage since the demand of non-compromised charge sessions becomes less important and that at 75% compromise attacks resulted in outages even during off-peak hours.

Since grid load profiles as well as e-mobility load profiles commonly exhibit similar trends, it is a reasonable assumption that the demonstrated times with high attack potential are valid for most scenarios. Additionally, considering that the load profiles are fairly predictable and information on them is widely available, it is also a reasonable assumption that an adversary would attempt an attack during peak load times. For this reason, we investigate the attack potential at different levels of compromise during peak load times in more detail. Based on the previous experiment, we can identify winter business days at 18:00 as one of the times with the highest attack potential. We hence simulate the modified attack at different levels of compromise (in 1% steps) during every winter business days at 18:00 for the immediate full capacity load balancing strategy as a worst-case scenario. The simulations were run 10 times each and results are summarized in Fig. 4 and Table 1. Specifically, Fig. 4 shows a scatter plot of the outage over time, i.e., showing the up to four different outage stages representing the up to four line failures, for the different levels of compromise. The data points are grouped based on proximity and the sizes of the marks in Fig. 4 represent the respective group sizes.

Table 1: Outage over Time at Different Compromise %

Compro-	Fastest Outage		Highest Outage		Avg. Line	Mean Total
mise %	Time in s	Outage %	Time in s	Outage %	Failures	Outage %
100.0	0.455	27.621	2.324	81.459	3.774	73.245
90.0	0.473	22.773	5.002	80.958	3.452	66.835
80.0	0.476	24.156	5.618	80.766	2.955	57.650
70.0	0.646	21.442	7.506	80.257	2.061	40.798
60.0	0.888	21.321	7.374	77.849	1.089	22.057
50.0	1.376	21.426	112.068	54.346	0.579	11.934
40.0	3.020	20.946	25.955	34.409	0.114	2.362
30.0	165.644	20.799	165.644	20.799	0.002	0.032

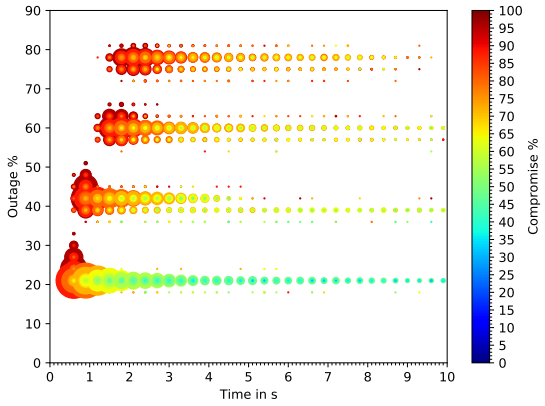

Figure 4: Outage over Time at Different Compromise %

The results show that outages not only become larger with increasing level of compromise but also faster. For example, the mean times of the first line failure for 100%, 80%, and 60% compromise are 0.66s, 1.4s, and 8.1s respectively. The mean total outages for 100%, 80%, and 60% compromise are 73.25%, 57.65%, and 22.06% respectively. The results also show that outages start becoming possible at 30% compromise and rather likely at 50% compromise with an average 0.58 line failures per attack. Fig. 5 shows the average times and probabilities of line failures for the 100% compromise case. Note that line failures (2) and (3) as well as (4) and (6) were mutually exclusive resulting in up to four line failures.

In order to investigate the potential of combined attacks, we again start with the immediate full capacity load balancing scenario during winter business days at 18:00. In this scenario, we evaluate an attack that combines the previously described demand increase attack at adversary controlled charging processes (including the SoC preparation modification) with the malicious modification of reported data as discussed in Section 4. For this, the adversarial effect of the modified data is modeled as a percentage increase in

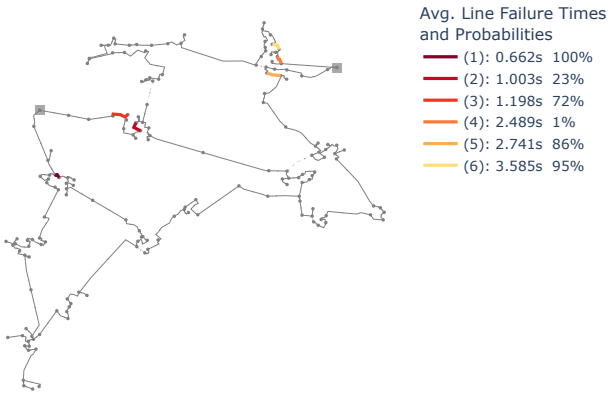

Figure 5: Line Failures at 100% Compromise

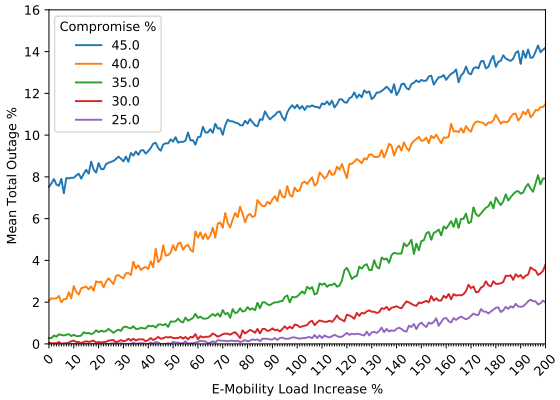

Figure 6: Mean Outage of Combined Attack

overall e-mobility demand. Thus, this attack represents the potential of an adversary to, e.g., use a botnet of CPs or a spoofed CPO to report a low demand, leading to the overestimation of available capacity and thus to the generation of charging schedules with increased demand that affect any charging sessions in the area (in addition to the direct demand increase at adversary controlled sessions).

The simulations were run 10 times per winter business day at 18:00 for different levels of compromise percentage (with 5% steps from 25% to 45%) and different levels overall e-mobility load increase (with 1% steps up to 200%). Notably, an increase in overall e-mobility load of 200% based on the manipulation of load balancing-relevant data can be considered possible since the highest difference in peak e-mobility load between the different load balancing strategies for the case study is 207.6% (cf. Fig. 3). Additionally, manipulated e-mobility data may also affect the load balancing of other non-e-mobility energy consumers, resulting in similar demand increases.

Fig. 6 shows the mean total outage percentage at the end of an attack for the different levels of compromise in relation to the e-mobility load increase percentage. As shown in Fig. 6, the combined attack can significantly increase the attack potential of an adversary. For instance, an increase in 1%, 5%, and 10% of e-mobility load leads to an average increase in outage percentage of 0.03, 0.15, and 0.3 respectively. Additionally, the results demonstrate that attacks start to become successful at even lower levels of compromise. Specifically, with a 25% compromise, attacks start resulting in outages at an 8% e-mobility load increase and the mean outage percentage surpasses that of the default 30% and 35% compromise cases at 34% and 91% e-mobility load increase respectively.

6.2 Case Study 2: Polish Grid 2008

For the second case study, we use the model of the polish grid during the 2008 summer morning peak as provided in pandapower. This scenario is used to evaluate the potential of large-scale attacks during peak demand times. Specifically, we evaluate the attack potential at different levels of compromise (at 10% steps) and with different levels of EV penetration. EV penetration is represented as the average amount of EVs per person (with steps of 0.0125), assuming a population of 38,354,000 in the grid area [Statistics Poland 2020] (i.e., each step corresponds to an addition of 479,425 EVs). For comparison, in the previous case study, the German 2020 scenario was equal to an EV penetration of 0.012 EVs per person and the German 2030 scenario was equal to 0.169 EVs per person.

The different amounts of EVs are randomly sampled, using the 2020 distribution of level 1, 2, and 3 charging, from the e-mobility data set for every summer business day at 08:00, representing the summer morning peak. The EV loads are added to the pandapower grid model and afterwards, all demand is scaled down such that the resulting load is equal to the load before EV addition. The attack is again modeled as the increase of demand at adversary controlled charging sessions including the SoC preparation modification as discussed in Section 6.1. We assume that the compensation for the increased demand is distributed among all generators with an amount that is proportional to their capacity [Soltan et al. 2018].

Fig. 7 shows the mean total outages after the attacks at the different levels of compromise and EV penetration (marks with a mean total outage of 0% are omitted for better visibility). The results show, for instance, that attacks with 100%, 50%, 40%, 30%, and 20% compromise start to result in outages at 0.025, 0.5, 0.0625, 0.0750, and 0.1250 EVs per person respectively. It also shows a strong rise in outage sizes as either compromise percentage or EV penetration increases. Fig. 8 shows the average times and probabilities of line failures for the 100% compromise case with 0.1 EVs per person. It shows, e.g., sub-second times for most line failures and that many lines had a 100% failure probability during this attack scenario.

In order to investigate the effect of the changing distributions in level 1, 2, and 3 charging demand, we simulate the same attack during the same times on the example of a 50% compromise with 0.075 EVs per person. EVs are randomly sampled, using the previously mentioned 2020 and 2030 distributions. The simulations were run 10 times for every included day and the resulting outages over time are shown in Fig. 9. Specifically, results are grouped based on the order of line failures and Fig. 9 shows the mean values for every line failure sequence that occurred more than once. Line thickness represents the amount of simulations with the same order of line failures and Xs show individual line failures. The results show a

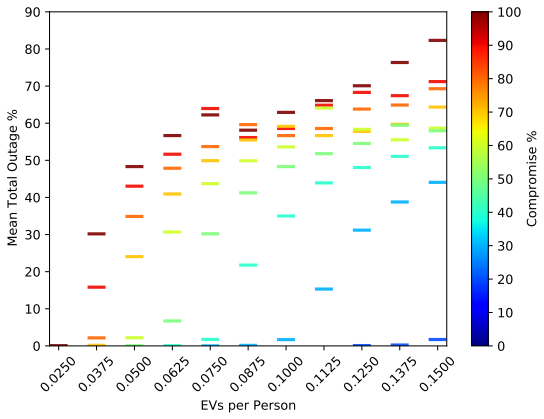

Figure 7: Outage over EV Penetration and Compromise %

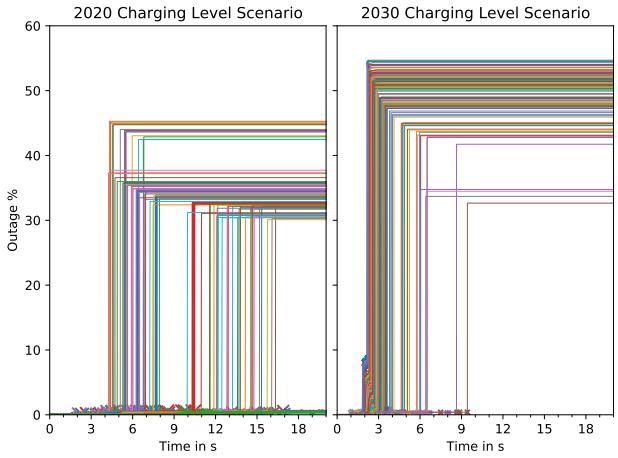

Figure 9: Outage Trend (50% Compromise, 0.075 EV/Person)

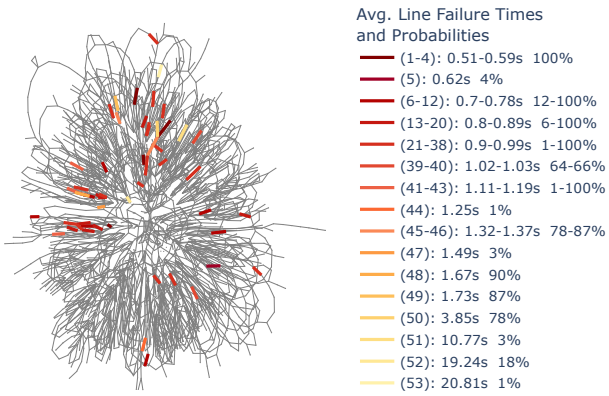

Figure 8: Line Failures (100% Compromise, 0.1 EV/Person)

strong tendency for faster and larger outages with the 2030 distribution. With the 2020 distribution, the average time for the first line failure was 2.5s and for the first resulting outage 4.6s, whereas with the 2030 distribution, the times were 1.1s and 2.2s respectively. Additionally, with the 2020 distribution, the mean final outage was 33.9% and with the 2030 distribution, it was 51.6% (notably higher than the 49.9% outage of the 70% compromise case at 0.075 EVs per person with 2020 charge level distribution; cf. Fig. 7).

7 E-MOBILITY-BASED PROTECTIONS

Compared to the regular MadIoT attacks, the e-mobility sector introduces new attack vectors to grid resilience due to its complex infrastructure and variety of protocols. However, the e-mobility infrastructure also opens up possibilities for unique protection measures (e.g., due to its intrinsic support for metering or load balancing with the possibility of V2G), which can serve to address different aspects of resilience:

Detection: A timely and accurate attack detection is important in order to adequately respond to potential threats. In the general smart grid context, several attack detection approaches have been proposed including Intrusion Detection Systems (IDSs) [Radoglou-Grammatikis and Sarigiannidis 2019] and machine learning-based mechanisms [Ozay et al. 2015]. The use of similar/new techniques in the context of e-mobility should consider its distinct challenges (e.g., the mobility of EVs raises increased privacy concerns, which may affect the possibility to use fine-grained data) and opportunities (e.g., the infrastructure involves communication and sensor readings from disparate sources, which may serve to increase resilience if used appropriately). Thus, the investigation of specialized detection approaches for the different e-mobility-based attacks (cf. Section 4) is relevant, considering privacy needs, the existing infrastructure, and timing-/accuracy-constraints (e.g., to guarantee attack detection before any outage).

Prevention: The two distinct types of adversaries (cf. Section 4) mostly require different types of preventive measures (besides the application of common security best practices). The threats from backend hackers could be addressed via more decentralized approaches. Blockchain-based approaches have already been proposed in the general smart grid context with the possibility of increasing resilience [Musleh et al. 2019]. In the e-mobility context, however, decentralized approaches usually only focus on secure authentication (e.g., [Huang et al. 2018]) and further investigations of their potential resiliency benefits are warranted.

The threat of a botnet based attack could, for instance, be addressed via the use of trusted computing methods such as a secure boot (i.e., a device can only boot after a validation of its local software) or remote attestation (i.e., a device can attest the integrity of its software state to a remote verifier). The use of trusted computing methods for additional security in the smart grid context is generally advisable [Metke and Ekl 2010] and approaches that integrate trusted computing into

existing e-mobility protocols with a focus on secure authentication already exist [Fuchs et al. 2020a,b,c,d]. However, further investigations of the potential to increase resilience based on trusted computing methods is still required.

Reaction: Another important aspect of resilience are appropriate reactive measures in order to, e.g., constrain the attack, restore the system into its pre-attacked state, or transform the system into a new working state. A commonly suggested reactive measure in the smart grid context is islanding, i.e., splitting the system into stable self-sufficient islands in order to isolate failures and prevent a cascade [Panteli et al. 2016]. Additionally, the e-mobility sector is commonly envisioned to support islanding mechanism via V2G technology [Mohsen et al. 2014]. However, the secure integration of e-mobility-based islanding support into existing protocols and/or under consideration of sophisticated adversaries (e.g., consideration the potential of compromised CPs/EVs) still provides room for more research. Similarly, load balancing mechanisms are a general measure to increase smart grid resilience with high relevance to the e-mobility use case (e.g., [Khalid et al. 2020]). However, the secure integration of these mechanisms into existing protocols under consideration of sophisticated e-mobility-based adversaries, the potential of load balancing as a reactive protection measure under consideration of the potentially very strict requirements for reaction times, as well as the need for privacy considerations still provides room for more research.

One should note that, due to the power grid's high level of criticality, no single solution can provide an adequate level of resilience. Instead, it is important to implement a comprehensive defense-in-depth approach, including a multitude of protective measures at different levels, such that even the failure of a single (or multiple) protective measure(s) does not enable the disruption of operations.

8 CONCLUSION

Due to the close relation between e-mobility sector and power grid, the potential of e-mobility-based attacks to the grid is feasible. Moreover, the threat of such an attack is especially relevant due to the complexity of the e-mobility infrastructure and the risk of these attacks is steadily increasing with the ever-rising EV market share. In this work, we define e-mobility-specific adversaries and attacks with the potential to negatively affect the grid. Moreover, we propose a framework to evaluate the impact of these attacks on the grid from a resilience-perspective that uses a combined e-mobility and grid model in conjunction with simulation-based outage analysis.

The framework is implemented using AC steady-state outage analysis and examples for grid and e-mobility models, reflecting different case studies and scenarios. The implementation is used to demonstrate the attack potential at different times of day, levels of e-mobility growth, and levels of compromise as well as the attacks' impact on the grid over time, which, e.g., may serve to indicate the required response time of protective measures. Evaluations show the high significance of the overall grid load in enabling a successful attack at lower levels of compromise and in increasing the impact at higher levels of compromise. It is further shown that, while, general EV-related load balancing approaches only have a relatively small impact on attack potential, if security is not guaranteed, an adversary may abuse load balancing mechanisms to further increase the impact of attacks to the grid by reporting manipulated data in a combined attack. The results further indicate that, while, successful attacks at current levels of EV penetration are unlikely, the growing e-mobility sector steadily raises the risk, making attacks at high level of compromise feasible in the near-term future.

These observations highlight the importance of security- and moreover resilience-related research in the area. In this context, we propose and discuss possible protection methods including mechanisms for detection, prevention, and reaction that may serve to increase resilience. This paper can thus be used as a starting point for further research on resiliency mechanisms for the power grid against e-mobility-based attacks.

ACKNOWLEDGMENTS

This research work has been 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.

REFERENCES

Samrat Acharya, Yury Dvorkin, and Ramesh Karri. 2020. Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable? *IEEE Transactions on Smart Grid* 11, 6 (2020), 5099–5113.

S Ahmed and Fouad M Dow. 2016. 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, 1–5.

Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. 2017. OCPP protocol: Security threats and challenges. *IEEE Transactions on Smart Grid* 8, 5 (2017), 2452–2459.

Anas AlMajali, Arun Viswanathan, and Clifford Neuman. 2012. Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack.. In *CSET*.

Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. 2016. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Transactions on Smart Grid* 9, 4 (2016), 2862–2872.

G Brooke Anderson and Michelle L Bell. 2012. Lights out: impact of the August 2003 power outage on mortality in New York, NY. *Epidemiology (Cambridge, Mass.)* 23, 2 (2012), 189.

Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*. 1093–1110.

Richard Baker and Ivan Martinovic. 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 407–424.

Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. 2018. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science-Research and Development* 33, 1-2 (2018), 3–12.

Deborah J Bodeau, Richard D Graubart, Rosalie M McQuaid, and John Woodill. 2018. *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods*. MITRE Technical Report.

Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

Hale Cetinay, Saleh Soltan, Fernando A Kuipers, Gil Zussman, and Piet Van Mieghem. 2018. Analyzing cascading failures in power grids under the AC and DC power flow models. *ACM SIGMETRICS Performance Evaluation Review* 45, 3 (2018), 198–203.

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. 2011. Comprehensive experimental analyses of automotive attack surfaces.. In *USENIX Security Symposium*, Vol. 4. San Francisco, 2021.

Mathias Dalheimer. 2017. Chaos Computer Club hacks e-motor charging stations. https://www.ccc.de/en/updates/2017/e-motor

Kaspersky Lab Security Services Dmitry Sklya. 2018. ChargePoint Home security research. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/13084354/ChargePoint-Home-security-research_final.pdf accessed 2021-08-30.

Yury Dvorkin and Siddharth Garg. 2017. IoT-enabled distributed cyber-attacks on transmission and distribution grids. In *2017 North American Power Symposium (NAPS)*. IEEE, 1–6.

Cherrelle Eid, Elta Koliou, Mercedes Valles, Javier Reneses, and Rudi Hakvoort. 2016. Time-based pricing and electricity demand response: Existing barriers and next steps. *Utilities Policy* 40 (2016), 15–25.

ElaadNL. 2017. EV Related Protocol Study. https://www.elaad.nl/research/ev-related-protocol-study/ Arnhem, The Netherlands.

Hossam ElHussini, Chadi Assi, Bassam Moussa, Ribal Atallah, and Ali Ghrayeb. 2021. A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid. *ACM Transactions on Internet of Things* 2, 2 (2021), 1–21.

Hauke Engel, Russell Hensley, Stefan Knupfer, and Shivika Sahdev. 2018. Charging ahead: Electric-vehicle infrastructure demand. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/charging-ahead-electric-vehicle-infrastructure-demand. accessed 2021-08-28.

EWE Netz. 2020. Grid Load Data. http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/. accessed 2021-08-28.

Nicolas Falliere, Liam O Murchu, and Eric Chien. 2011. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response* 5, 6 (2011), 29.

Federal Ministry of Transport and Digital Infrastructur. 2021. Erstmals rollen eine Million Elektrofahrzeuge auf deutschen Straßen. https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2021/080-scheuer-altmaier-schulze-1-mio-elektrofahrzeuge.html accessed 2021-08-30.

Federal Statistical Office (Destatis). 2019. A changing population - Assumptions and results of the 14th coordinated population projection. https://www.destatis.de/EN/Themes/Society-Environment/Population/Population-Projection/_node.html. accessed 2021-08-30.

Yosra Fraiji, Lamia Ben Azzouz, Wassim Trojet, and Leila Azouz Saidane. 2018. Cyber security issues of Internet of electric vehicles. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6.

Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. 2020a. HIP: HSM-Based Identities for Plug-and-Charge. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (Virtual Event, Ireland) *(ARES '20)*. Association for Computing Machinery, New York, NY, USA, Article 33, 6 pages. https://doi.org/10.1145/3407023.3407066

Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. 2020b. Securing Electric Vehicle Charging Systems through Component Binding. In *39th International Conference on Computer Safety, Reliability and Security, SAFECOMP*. Springer. https://doi.org/10.1007/978-3-030-54549-9_26

Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. 2020c. TrustEV: Trustworthy Electric Vehicle Charging and Billing. In *Proceedings of the 35th ACM/SIGAPP Symposium on Applied Computing SAC 2020*. ACM. https://doi.org/10.1145/3341105.3373879

Andreas Fuchs, Dustin Kern, Christoph Krauß, Maria Zhdanova, and Ronald Heddergott. 2020d. HIP-20: Integration of Vehicle-HSM-Generated Credentials into Plug-and-Charge Infrastructure. In *Computer Science in Cars Symposium* (Feldkirchen, Germany) *(CSCS '20)*. Association for Computing Machinery, New York, NY, USA, Article 12, 10 pages. https://doi.org/10.1145/3385958.3430483

Carlos Gaete-Morales, Hendrik Kramer, Wolf-Peter Schill, and Alexander Zerrahn. 2021. An open tool for creating battery-electric vehicle time series from empirical data, emobpy. *Scientific data* 8, 1 (2021), 1–18.

Lingwen Gan, Ufuk Topcu, and Steven H Low. 2012. Optimal decentralized protocol for electric vehicle charging. *IEEE Transactions on Power Systems* 28, 2 (2012), 940–951.

Kenneth Geers. 2010. The challenge of cyber attack deterrence. *Computer Law & Security Review* 26, 3 (2010), 298–303.

Raju Gottumukkala, Rizwan Merchant, Adam Tauzin, Kaleb Leon, Andrew Roche, and Paul Darby. 2019. Cyber-physical system security of vehicle charging stations. In *2019 IEEE Green Technologies Conference (GreenTech)*. IEEE, 1–5.

Stephan Haggard and Jon R Lindsay. 2015. North Korea and the Sony hack: Exporting instability through cyberspace. (2015).

Pierre Henneaux, Emanuele Ciapessoni, Diego Cirio, Eduardo Cotilla-Sanchez, Ruisheng Diao, Ian Dobson, Anish Gaikwad, Stephen Miller, Milorad Papic, Andrea Pitto, et al. 2018. Benchmarking quasi-steady state cascading outage analysis methodologies. In *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. IEEE, 1–6.

Matthias Hollick and Stefan Katzenbeisser. 2019. Resilient Critical Infrastructures. In *Information Technology for Peace and Security*, Christian Reuter (Ed.). Springer, 305–318.

Bing Huang, Alvaro A Cardenas, and Ross Baldick. 2019. Not everything is dark and gloomy: Power grid protections against IoT demand attacks. In *28th USENIX Security Symposium (USENIX Security 19)*. 1115–1132.

Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu. 2018. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* 6 (2018), 13565–13574.

ISO/IEC. 2014. *Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements*. ISO Standard 15118-2:2014. ISO, Geneva, Switzerland.

Sung-Kwan Joo, Jang-Chul Kim, and Chen-Ching Liu. 2007. Empirical analysis of the impact of 2003 blackout on security values of US utilities and electrical equipment manufacturing firms. *IEEE Transactions on Power Systems* 22, 3 (2007), 1012–1018.

Rabiya Khalid, Nadeem Javaid, Ahmad Almogren, Muhammad Umar Javed, Sakeena Javaid, and Mansour Zuair. 2020. A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid. *IEEE Access* 8 (2020), 47047–47062.

Young-Il Kim, Jong-Min Ko, and Seung-Hwan Choi. 2011. Methods for generating TLPs (typical load profiles) for smart grid-based energy programs. In *2011 IEEE Symposium on Computational Intelligence Applications In Smart Grid (CIASG)*. IEEE, 1–6.

Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.

Nir Kshetri and Jeffrey Voas. 2017. Hacking power grids: A current problem. *Computer* 50, 12 (2017), 91–95.

Yao Liu, Peng Ning, and Michael K Reiter. 2011. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)* 14, 1 (2011), 1–33.

Hong Tao Ma and Badrul H Chowdhury. 2006. Dynamic simulations of cascading failures. In *2006 38th North American Power Symposium*. IEEE, 619–623.

Maigha and M. L. Crow. 2016. Cost-constrained dynamic optimal electric vehicle charging. *IEEE Transactions on Sustainable Energy* 8, 2 (2016), 716–724.

Anthony R Metke and Randy L Ekl. 2010. Security technology for smart grid networks. *IEEE Transactions on Smart Grid* 1, 1 (2010), 99–107.

Charlie Miller and Chris Valasek. 2015. Remote Exploitation of an Unaltered Passenger Vehicle.

Mirko. 2008. *MU2300 voltage protection relay - User's Manual*. Selangor, Malaysia.

Seyed Mohsen, Mohammadi Hoseini Nezhad, Alireza Fereidunian, Hamid Lesani, and Mirjavad Hashemi Gavgani. 2014. Enhancement of self-healing property of smart grid in islanding mode using electric vehicles and direct load control. In *2014 Smart Grid Conference (SGC)*. IEEE, 1–6.

Seyedamirabbas Mousavian, Melike Erol-Kantarci, and Thomas Ortmeyer. 2015. Cyber attack protection for a resilient electric vehicle infrastructure. In *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 1–6.

Ahmed S Musleh, Gang Yao, and SM Muyeen. 2019. Blockchain applications in smart grid–review and frameworks. *Ieee Access* 7 (2019), 86746–86757.

Mete Ozay, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R Kulkarni, and H Vincent Poor. 2015. Machine learning methods for attack detection in the smart grid. *IEEE transactions on neural networks and learning systems* 27, 8 (2015), 1773–1786.

Mathaios Panteli, Dimitris N Trakas, Pierluigi Mancarella, and Nikos D Hatziargyriou. 2016. Boosting the power grid resilience to extreme weather events using defensive islanding. *IEEE Transactions on Smart Grid* 7, 6 (2016), 2913–2922.

Richard M Pratt and Thomas E Carroll. 2019. Vehicle charging infrastructure security. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 1–5.

Kejun Qian, Chengke Zhou, Malcolm Allan, and Yue Yuan. 2010. Load model for prediction of electric vehicle charging demand. In *2010 International Conference on Power System Technology*. IEEE, 1–6.

Panagiotis I Radoglou-Grammatikis and Panagiotis G Sarigiannidis. 2019. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* 7 (2019), 46595–46620.

Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. 2019. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Volume 2.

Juan E Rubio, Cristina Alcaraz, and Javier Lopez. 2018. Addressing security in OCPP: Protection against man-in-the-middle attacks. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 1–5.

Siemens. 2005. *Applications for SIPROTEC Protection Relays*. Nuernberg, Germany.

Saleh Soltan, Prateek Mittal, and H Vincent Poor. 2018. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In *27th USENIX Security Symposium (USENIX Security 18)*. 15–32.

Jiajia Song, Eduardo Cotilla-Sanchez, Goodarz Ghanavati, and Paul DH Hines. 2015. Dynamic modeling of cascading failure in power systems. *IEEE Transactions on Power Systems* 31, 3 (2015), 2085–2095.

Statistics Poland. 2020. Population. Size and structure and vital statistics in Poland by territorial division in 2020. As of 30th June. https://stat.gov.pl/files/gfx/portalinformacyjny/en/defaultaktualnosci/3286/3/28/1/population_size_and_structure_and_vital_statistics_in_poland_by_territorial_division_in_30.06.2020.pdf. accessed 2021-08-30.

Statistisches Landesamt Baden-Württemberg. 2021. Bevölkerung nach Nationalität und Geschlecht – vierteljährlich. https://www.statistik-bw.de/BevoelkGebiet/Bevoelk_I_D_A_vj.csv. accessed 2021-08-30.

Julia E Sullivan and Dmitriy Kamensky. 2017. How cyber-attacks in Ukraine show the vulnerability of the US power grid. *The Electricity Journal* 30, 3 (2017), 30–35.

Kang Miao Tan, Vigna K Ramachandaramurthy, and Jia Ying Yong. 2016. Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques. *Renewable and Sustainable Energy Reviews* 53 (2016), 720–732.

Sam Thielman. 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian* (12 2016).

L. Thurner, A. Scheidler, F. Schäfer, J. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun. 2018. pandapower — An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems. *IEEE Transactions on Power Systems* 33, 6 (Nov 2018), 6510–6521. https://doi.org/10.1109/TPWRS.2018.2829021

Remco A Verzijlbergh, Marinus OW Grond, Zofia Lukszo, Johannes G Slootweg, and Marija D Ilic. 2012. Network impacts and cost savings of controlled EV charging. *IEEE transactions on Smart Grid* 3, 3 (2012), 1203–1212.

Yezhou Wang and Ross Baldick. 2013. Case study of an improved cascading outage analysis model using outage checkers. In *2013 IEEE Power & Energy Society General Meeting*. IEEE, 1–5.

Han Xiao, Yuan Huimei, Wei Chen, and Li Hongjun. 2014. A survey of influence of electrics vehicle charging on power grid. In *2014 9th IEEE Conference on Industrial Electronics and Applications*. IEEE, 121–126.

Daniel Zelle, Markus Springer, Maria Zhdanova, and Christoph Krauß. 2018. Anonymous charging and billing of electric vehicles. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 1–10.

Chi Zhang, Sanmukh R Kuppannagari, Rajgopal Kannan, and Viktor K Prasanna. 2018. Generative adversarial network for synthetic time series data generation in smart grids. In *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 1–6.