Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication

Maria Zhdanova
maria.zhdanova@mailbox.org
Fraunhofer SIT | ATHENE
Darmstadt, Germany

Julian Urbansky
julian.urbansky@umsicht.fraunhofer.de
Fraunhofer UMSICHT
Oberhausen, Germany

Anne Hagemeier
anne.hagemeier@umsicht.fraunhofer.de
Fraunhofer UMSICHT
Oberhausen, Germany

Daniel Zelle
daniel.zelle@sit.fraunhofer.de
Fraunhofer SIT | ATHENE
Darmstadt, Germany

Isabelle Herrmann
Fraunhofer UMSICHT
Oberhausen, Germany

Dorian Höffner
Fraunhofer UMSICHT
Oberhausen, Germany

ABSTRACT

With Electric Vehicles (EVs) becoming more prevalent, their battery recharge creates significant loads on power grids. Especially in local grids with a high share of households that own an EV, this additional energy demand can stress existing power distribution systems that were not designed for this kind of loads. The unexpected peak consumption may reduce service quality, damage sensitive equipment, cause power failures and even local blackouts. To mitigate this risk, grid components must be either significantly upgraded to match the increased demand, or the demand must be managed to avoid critical situations. Vehicle-to-Grid (V2G) technology is a major emerging trend for enabling load management in connection with EV charging. A key component of V2G is the ISO 15118 protocol allowing to set grid-friendly charging schedules for EVs. This standard is further supported by backend protocols like OCPP to permit corrective actions by a network operator.

In this paper, we analyze conditions under which V2G insecurity can lead to grid collapse. We use quantitative analysis and dynamic simulations of a typical European suburban grid to determine the scope and impact of EV charging manipulation. We then review shortcomings of existing V2G protocols, analyze attack strategies able to cause overloads and validate known attacks based on experiments with off-the-shelf products. While load management is vital to future cost-effective grid operation, we show that it is also critical to consider the impact of known and unknown attacks, and consider possible mitigations and fallback positions.

CCS CONCEPTS

• **Security and privacy** → *Distributed systems security*; *Security protocols.*

ACSAC '22, December 5–9, 2022, Austin, TX, USA

ACM ISBN 978-1-4503-9759-9/22/12.
https://doi.org/10.1145/3564625.3568136

KEYWORDS

grid simulation, vehicle-to-grid, security, attacks, ISO 15118, OCPP

ACM Reference Format:
Maria Zhdanova, Julian Urbansky, Anne Hagemeier, Daniel Zelle, Isabelle Herrmann, and Dorian Höffner. 2022. Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication. In *Annual Computer Security Applications Conference (ACSAC '22), December 5–9, 2022, Austin, TX, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564625.3568136

1 INTRODUCTION

There are already over 10 million fully battery-powered or plug-in hybrid Electric Vehicles (EVs) worldwide [3], and their penetration in suburban and rural areas is expected in the near future [74]. To recharge EV batteries at home, many private households install charge points. As the capabilities of European low voltage (LV) grid installations vary, studies suggest that some can manage large EV fleets, while others require immediate improvements to avoid a collapse [1, 11, 12]. Regions where EVs are starting to outsell gasoline-powered cars provide first examples of grid impacts: due to a heat wave forecast, California advised to avoid EV charging to save energy [63], while Norway restricted EV charging times to avoid peak-hour charging [16, 76]. Operators can cope with the growing demand and imminent overload situations by means of grid expansion or load management. But since grid expansion requires enormous local investments, digital load management solutions are economically attractive and an integral part of present discussions on improving LV grid capacity [1, 11, 12, 29, 32].

V2G technology provides a communication interface between EVs, charge points and backend systems of various stakeholders such as Distribution System Operators (DSOs), Charge Point Operators (CPOs), and E-Mobility Service Providers (eMSPs). This way, energy availability forecasts, charging schedules and overload signals can be timely forwarded to all concerned parties in the local grid to ensure stable energy supply and prevent overloads.

Contributions. We analyze the security implications of deliberate attacks on EV charging and load management processes in a typical European LV grid. In particular, we explore grid-wide effects caused by the integration of EVs using dynamic simulations based on realistic load profiles for households, and determine under

which conditions the grid will collapse. We then review the security of V2G protocols and attack vectors for V2G systems and describe attack strategies that can trigger such conditions.

While we identify several (partly known) shortcomings in the specifications, which we could also confirm in widely available charging products, our focus is not on the detailed exploitation of a particular security issue. Rather, we use the very concrete threat of V2G attacks to model, simulate, and study the risk of local blackouts in future load-managed power grids. As such, the focus of our simulation is not on the mechanics of a local grid failure but to find situations that would lead to a collapse.

In detail, we provide the following contributions:

(1) We estimate the power levels reachable via targeted manipulation of EV charging using a quantitative analysis of a typical LV grid. We discuss the implications for different grids, which will become highly relevant for DSOs as more and more EVs are connected in the near future. As grid capacity is limited, managing this load helps stable power supply.
(2) We define the threat model and attack strategies that would allow an adversary to control a significant number of charging facilities using known attack methods and newly found weaknesses in the V2G protocols ISO 15118 and OCPP.
(3) We develop a test setup and evaluate several open-source tools to validate the key steps of our V2G attack strategies.
(4) We discuss limitations of our attacks and resulting mitigation strategies.

2 RELATED WORK

Attacks on Power Grids. In [22], attacks affecting grid frequency by means of the coordinated modulation of the power consumption in a botnet of zombie computers were designed. Unstable states in the grid could be triggered with 2.5 to 9.8 million infections. The simulation used a Matlab/Simulink model and focused on the grid's response to a production-consumption imbalance considering self-regulation and primary control. In [70], a botnet attack of high wattage IoT devices was investigated. The authors analyzed frequency instability, line failures resulting in cascading failures and increasing operating costs. The simulation used Power-World software and the Matlab library MATPOWER. The focus lay on dynamic simulation of power flows in the transmission network.

In contrast to these works, we analyze manipulations on the lowest grid level in our simulations. At this level, grid frequencies are not affected and the threat lies in overload situations that an attack can cause. So our simulations are fundamentally different: no dynamic consumer and producer models are needed, instead, we focus on modeling an LV grid with a realistic structure and new technologies like PV, heat pumps and EVs, and on integrating consistent time series of household consumption and production.

The vulnerability of smart grids to attacks against IT-based control systems were analyzed, e.g., in [10, 47, 82]. However, neither local grids nor recent V2G communication protocols were considered. A real-world attack on a DSO is known [84]. In [80], the control over a power plant was lost due to an attack on the communication link. Further reported attacks targeting corporate networks are the Sony hack [83], DigiNotar and Comodo breaches [31, 48].

Attacks on V2G Components. With regard to the real-world security of cyber-physical systems in V2G, practical attacks on chargers and EVs from multiple manufacturers have been demonstrated. In [23], the installation of manipulated firmware on the charger via an USB port and masquerading a high-wattage device (a waffle iron) as a charging vehicle were shown. In [20], the authors used reverse-engineering to manipulate the firmware update provided online by a CPO and to gain remote control of its charge points. The results of penetration tests for charge points of various brands reported in [73] revealed further vulnerabilities allowing full adversarial control. Attack vectors for connected cars have also been analyzed and validated in practice [19, 43]. Miller and Valasek first demonstrated the remote exploitation and control of a car in their famous "Jeep hack" [34, 50]. More recently, remote attacks on EVs from Tesla [56, 57, 79], BMW [2], and Kia [21] were shown. A communication gateway connecting a manufacturer's backend to the vehicle's E/E system was used as an entry point. Only the Kia hack required a compromised application being installed in the car's telematics in advance. The work [45] exploited connected car apps to remotely control EVs, install updates and manage charging sessions. In [46], a Denial-of-Service (DoS) attack on powerline communication (PLC) that can stop EV charging remotely was reported. The possibility to eavesdrop plaintext ISO 15118 messages via PLC was shown in [14, 28] whereby the testbed [28] allows attackers to read and modify the complete stack, e.g., inject crafted V2G messages. These works are complementary to our research.

3 BACKGROUND

3.1 Distribution Grids

Electrical energy is transferred from power plants to different regions and then delivered to local consumers via distribution grids. European distribution grids comprise multiple power levels. Households are usually connected to LVs grids, which have nominal phase voltage of 400 V and supply 30 to 500 residential units with power.

Today's LV grids were built, modified and extended to meet changes in demand over decades. The determining factors are the population density, new technologies like photovoltaics (PV), heat pumps and e-mobility, additional consumers, migration in urban areas, and other local developments. Since the power requirements evolved regionally in different ways, European LV grids differ profoundly with respect to their size, structure and load capacities.

In recent years, additional electricity consumers have been integrated into the grids. For example, new buildings are often heated using heat pumps [58]. Due to the increasing adoption of EVs, the number of charge points in LV grids is also rising. The standard charging power of EV chargers in Europe is 11 kW or 22 kW, which is the limit for 16 A or 32 A AC charge points (three-phase). They are comparable to American Level-2-chargers (usu. 9.6 to 19.2 kW). This is a considerable additional load compared to other loads in typical households. During simultaneous charging of several EVs in one LV grid the total power can add up significantly. If the load exceeds critical limits, grid components such as transformers and cables will be overloaded. Overload situations in LV grids lead to accelerated aging of technical equipment and can cause damage to the grid components. Therefore, various physical safety devices are deployed

to protect the grid like NH fuses (from German "Niederspannungs-Hochleistungs-Sicherung") [67] and thermal overload relays with switch disconnectors. Notably, critical voltage fluctuations due to rapid load changes in weak grids can cause disconnection of electric devices like PCs and malfunction of electrically operated processes.

3.2 Protocols for Electric Vehicle Charging

Out of a large variety of communication protocols proposed for EV charging [35, 55, 62], only few are internationally recognized and deployed in real products. The two main standards are ISO 15118 [38] and Open Charge Point Protocol (OCPP) [5, 59] by the Open Charge Alliance that enable the communication between EV, charger, and service backend systems in major V2G use cases.

ISO 15118 specifies two authentication methods: certificate-based Plug-and-Charge (PnC) and generic External Identification Means (EIM) comprising RFID cards, smartphone apps, etc. The charge point can offer both methods during charging setup. ISO 15118 supports PnC natively, with the challenge-response protocol being part of the message sequence. In EIM, the charger authenticates the EV user out-of-band before negotiating services via ISO 15118. The term "Plug-and-Charge" is sometimes used to refer to less secure methods such as Autocharge that simply checks EV's ID or MAC address against a whitelist, which is highly contentious in the community. For PnC, a valid charging contract is linked to the EV and used to issue vehicle's access credentials in form of a X.509v3 certificate. When the EV is plugged to charge, it can be identified, authorized and billed for the consumed energy automatically.

Once the EV and the charger are connected with a charging cable and in a ready state (cf. IEC 61851), the vehicle establishes the communication link via the control pilot wire by means of PLC using a custom flavor of the HomePlug Green PHY (HPGP) standard, e.g., omitting security [40]. Then, the EV performs the IPv6 address discovery and initiates a TCP connection [39]. The EV can request a unilateral TLS channel from the charger, before the application protocol V2GTP starts [39]. V2GTP is a request-response protocol with strict XML/EXI-based message format and sequence requirements. During session setup, the services, authentication method, charge parameters (duration, battery status, etc.), tariffs and schedules are negotiated. During energy transfer, status data are exchanged. The EV can pause and resume charging at any time. The charger can renegotiate, if the grid situation has changed. Once the battery is charged, the session ends.

The new edition of the network and application layer specification ISO 15118-20 [41] adds support of bidirectional power transfer and wireless charging. The security concept has also been reworked, e.g., to make TLS mandatory and to integrate the TPM 2.0 [85].

Using OCPP, the charger receives energy tariffs and data needed to define charging schedules from the CPO and other stakeholders like DSO and eMSP. The OCPP's smart charging allows the CPO/DSO to set the maximum power available at a given time for EV charging. This way, the desired consumption behavior over time depending on the forecast grid capacity or energy price can be achieved. OCPP is an application request-response protocol, where operations can be initiated by charge points or backend systems. In contrast to ISO 15118, it allows "wild card" messages to transfer arbitrary data. The smart charging is supported starting OCPP 1.6 [59],

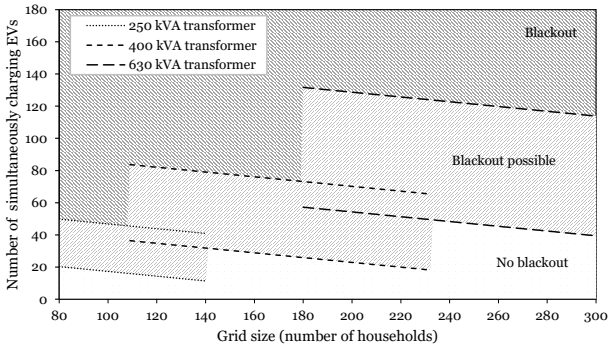


Figure 1: Quantitative analysis: Number of simultaneously charging EVs to trigger a local blackout depending on grid size for commonly used transformers

while the latest issue OCPP 2.0.1 [5] also supports ISO 15118-2 and extended load management. Moreover, this is the first version with basic communication security [6].

4 GRID SIMULATION

First, we estimate in a quantitative analysis how many EVs have to be charged simultaneously to trigger a local blackout when the grid is already stressed due to the daily peak load in the early afternoon. With the number of households n_h and $\cos\varphi = 0.9$, the daily peak load can be calculated as follows [36]:

$$S_\mathrm{max} = n_\mathrm{h}(0.07 + 0.93\frac{1}{n_\mathrm{h}}) \cdot \frac{1}{\cos\varphi} \cdot 21\ \mathrm{kW} \quad (1)$$

Depending on the grid size, various transformers and fuses are used. These safety devices cut the power supply depending on the duration and power of the overload. Typical characteristic curves of standard fuses show that grids work stably at 1.5x nominal power of the transformer for at least 90 minutes (no blackout). On the contrary, these fuses will surely trip after 3 to 5 minutes at 2.8x nominal power (blackout). Based on this consideration, the minimum number of simultaneously charging EVs for a local blackout depending on the size of the grid and transformer is shown in Figure 1.

The quantitative analysis indicates that typical grid configurations can supply only few EVs at the same time. If an external action can effect the simultaneity, a local blackout due to an attack is possible. In addition to the grid configuration, the actual grid load and availability of rechargeable EVs depend on the weather and people's behavior. Thus, a detailed simulation is needed to make sound statements about the vulnerability of common grids.

We focus on a typical LV grid in Europe with reasonable sizing of the components. These grids were not designed to support large EV fleets. Therefore, the DSOs has to use smart load management systems to prevent overload situations due to an excessive amount of simultaneous charging processes. There are many grids which are badly equipped and where a blackout might happen even with fewer EVs or with a shorter attack span. Still, we were able to identify conditions, under which an attack could lead to a local blackout even in a typical grid.

4.1 Modeling Language

For the grid simulation, the modeling language Modelica was chosen [52]. Modelica is an object-oriented programming language for the dynamic modeling of physical systems. Problems can be expressed in terms of differential-algebraic equations (DAE). Due to its flexibility, it is not limited to one physical domain but can represent a wide range of engineering domains [75]. It has therefore been used to model automotive, building, control, chemical, hydraulic or thermal systems and is also being used for the simulation of power systems (see, e.g., [33, 78, 81]). Basic models for modeling of different systems are published in the Modelica Standard Library by the Modelica Association. Various other libraries are commercially or freely available. For the simulations in this paper, we used the TransiEnt Library for the simulation of complex integrated systems that contains models for integrated simulation of gas, heat and electrical systems [68].

4.2 Model Definition

LV grids are structured similarly throughout Europe. Therefore, we rely on a benchmark grid model that represents a great amount of real grids [24]. A model representing a suburban district with mostly one family houses (OFH) and a few two family houses (TFH) was selected [42], as a high share of electric vehicles could be expected for this consumer structure in the near future. Figure 2 shows the chosen reference model. The district is assumed to date from the mid-90s, thus, having a grid structure that was not designed to integrate the loads due to the usage of heat pumps and EVs.

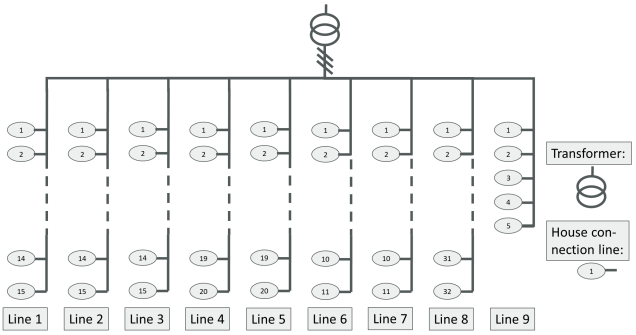


Figure 2: Local grid reference model adopted from [42]

The grid serves 170 households. The heat demand of each of them was modeled using a simple one-zone building simulation model in Modelica. Typical meteorological year weather data for the city of Miesbach were used for the simulations [44]. The heat profiles were randomized by using different ventilation, heating setpoint and inner loads profiles. Annual heating demand of the houses ranges between 19 MWh for houses built in the mid 90s and 12 MWh for houses built in 2001-2008 or refurbished houses [17].

Consistent demand profiles for electricity and hot water as well as driving and location profiles for the EVs are generated using the LoadProfileGenerator, which creates individual and stochastic electricity demand profiles based on a psychological needs model [61]. The household composition, e.g., singles, couples, families is based on the data on the composition of households in the German city of Cologne [71]. 25% of the consumers are assumed to use heat pumps as their heating technology. All other consumers use non-electric technologies, e.g., gas boilers, which are not modeled explicitly. To take renewable energies into account, 25% of the consumers are additionally implemented with photovoltaic plants. The dimensioning of the installed PV capacity is done individually for each consumer, based on their electricity demand profile. The heat pumps are dimensioned for the respective building type [25, 26].

Table 1: Parameters of the simulated consumer structure

Total number of households	170
Number of households with PV	43
Number of households with heat pump	43
Number of households with charge point	85
Heating demand per household (space heating plus domestic hot water)	14 to 21 MWh (depending on building age)
Electricity demand per household	2 - 8 MWh (depending on household type)
Proportion of single/two-person/family households	9% / 23% / 68%
Charging power per wallbox	11 kW
Weather data	Test reference year for Miesbach, Germany

Based on an electrification scenario in [8], 50% of the households are assumed to have an EV. Every home that uses an EV is equipped with its own charge point with a charging power of 11 kW for one EV. The maximum electrical load of the households ranges between 6 and 16 kW, therefore, the EV charging adds a significant load to each consumer. Driving and location profiles from the LoadProfileGenerator determine the state of charge of the battery and the time span when the EV is at home. Battery charging will start immediately when the car is present. Every charge point can be accessed by the network operator in case of an overload at the transformer. This will happen before the power at the transformer exceeds 400 kVA. In this case, maximum charging power of each charge point will be reduced gradually, leading to longer charging times but preventing the overload. The parameters of the grid and the consumers are summarized in Table 1.

Grid safety devices, e.g., the fuses at the transformer and the power lines were not modeled explicitly. However, the situations in which a local blackout would occur can be deduced from the load situations in the simulation results.

4.3 Simulation

To show the effect of the load management, we first did a whole-year simulation of the grid without EV charging, the grid with EV charging but without load management (with both a 50% and 70% EV penetration) and the grid with EV charging and load management of the charge points in case of imminent overload with a 50% EV penetration. The resulting annual power duration curves for the four cases, showing the amount of time per year that the apparent power at the transformer exceeds a certain value, are displayed in the left part of Figure 3. The right part of Figure 3 depicts the first 10% of the annual power duration curve to enable a closer look at the high power values that are of interest for this analysis. Without EV charging, the annual maximum power remains below 400 kVA,

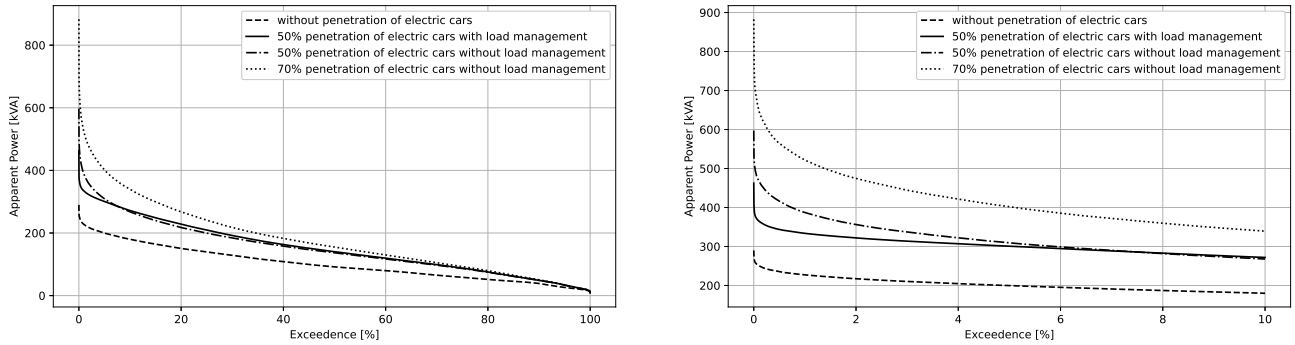


Figure 3: Sorted annual power duration curve of the power at the transformer, left: whole year, right: zoom at highest power values that occur during 10% of the year

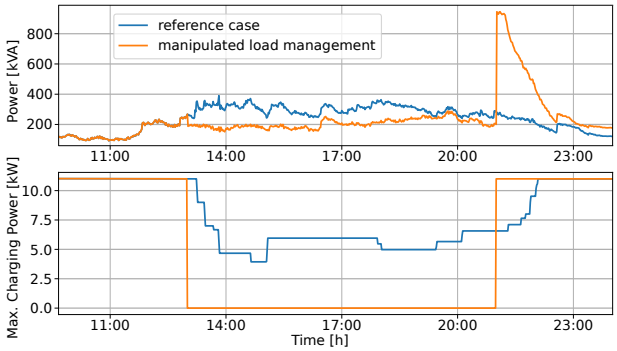


Figure 4: Power at the transformer and maximum charging power over all charge points during the course of Jan 18th

thus, not exceeding the maximum power of the transformer. With an increasing number of EVs, the grid load increases. When the transformer is charged with loads over 400 kVA, the grid components are strained, leading to accelerated aging. As can be seen from the curve, this happens on about 3 days in total with the 50% EV penetration and on about 18 days in the case of the 70% EV penetration. The effect of the load management is also clearly visible: the occurrence of peak powers over 400 kVA is largely reduced, leading to more charging at lower powers.

Next, we manipulated the load management in the grid with the 50% EV penetration to show the effect this would have on the grid. We chose a day with the high load due to cold temperatures so that the power consumption would be already high because of the usage of heat pumps. On this day (Jan 18th), we blocked EV charging for a certain amount of time to increase the number of simultaneously charging EVs. Then, at the time of the high grid load due to the electric heating power used by the heat pumps, charging of all EVs present at the charge points was enabled. The resulting load on the transformer can be seen in the upper graph in Figure 4 (orange curve). The lower graph shows the maximum charging power over all the charge points in the grid. The blue curve shows the reference case without the manipulation of the load management. At 1 p.m. the charge points received a signal blocking EV charging until 9 p.m. and leading to the charging power of 0 W. In the reference case, charging power of the charge points was reduced gradually to ensure the maximum power of the transformer did not exceed 400 kVA. At 9 p.m. charging was enabled again but the load management was blocked. In the examined threat scenario, 68 EVs started their charging processes at the same time. This lead to a sudden increase of the grid power to well above 900 kVA.

4.4 Results

The simulation results show that the V2G technology is suitable to avoid overloads in a suburban LV grid that would otherwise experience overload situations due to EV battery recharge. However, there are only a few days per year with imminent overload situations in the examined grid. This overload situations could reach about 140% of the nominal power, therefore, failures of components and ultimately of the electrical power supply are not to be expected. If the load management system were to fail, for example, as a result of a communication failure, this grid would age prematurely but probably operate stably.

However, the simulation results show that a local blackout caused by communication attacks is principally possible in a typical LV grid with EV charging and load management. By blocking EV charging for a certain amount of time and then suddenly enabling charging, the high number of simultaneous charging processes leads to substantially higher loads that could cause a local blackout in the LV grid. Whether the power supply actually fails depends on the behavior of safety devices. There are fuses both at the transformer and at the cables to protect them from overload situations. If overcurrents occur for a certain amount of time, the fuses will trip and thus lead to the blackout in parts or even the whole LV grid.

The chosen grid transformer (400 kVA) is generally protected with an NH gTr fuse (577 A) [67]. This fuse trips at currents 1.5 times higher than the nominal current after max. 2 hours. At higher currents, the tripping will happen after a shorter time span. During the simulated communication attack, the current peak is shorter than 2 hours, but with 1300 A more than 2.2 times higher than the nominal current. Typical characteristic curves show that a fuse tripping in this case is probable. Moreover, if a thermal overload relay as an additional protection for the transformer is used, the

switch disconnector will probably trip in this case, too. The detailed simulation showed that a local blackout could be caused by 68 EVs. This result is consistent with our initial analysis, where we estimated that 27 to 75 EVs must be charged simultaneously to trigger a blackout in the examined grid (cf. Figure 1).

Furthermore, partial power failures in single power lines as a result of the attack are also possible. Whether one of the power line NH fuses would trip in the existing grid depends highly on the grid structure and chosen NH fuse. Therefore, it is difficult to predict whether the electricity will fail due to a tripped power line fuse or not. However, power lines are generally equipped with smaller fuses than transformers. Especially in streets with a high concentration of EVs, limit exceedances are expected. The power line with most connected EVs is line 8 (cf. Figure 2). This line would typically be protected with a 100 A or 160 A NH fuse. The smaller one (100 A) would trip with certainty in this investigation, the larger one (160 A) possibly too. From an attacker's point of view, to cause a blackout in only one power line, a reduced number of charge points has to be manipulated due to the smaller fuses. In the model, there are 16 EVs affected by the communication attack on line 8.

Another result of a high grid load could be a voltage drop that may affect connected equipment. The strongest effect would be at the furthest point from the transformer. Therefore, we also investigated the voltage drop at the end of the longest power line (line 8). During the attack, the voltage drops to a minimum of 375 V at this point. This is less than a 10% reduction compared to the nominal voltage (400 V). Hence, we expect no negative effects for the grid or for connected electric devices due to voltage fluctuations in the regarded suburban grid.

To sum up, the effect of the manipulation depends on the installed equipment. With typically used fuses, the technical limits would be exceeded in the examined threat scenario. These results lead us to the conclusion that a local blackout or at least a partial power failure caused by the communication attack is possible.

It should be noted that a cold day with an already high load due to the electric heat pumps and a high number of EVs to charge was investigated. On an average day, the threat of a local blackout based on communication manipulations or failures is lower.

For this study, an average mid-90s suburban grid was chosen in order to analyze whether it is vulnerable to such power failures. However, several LV grids in Europe are less developed or more stressed due to the expansion [24]. This could mean that the grid load is already close to the transformer limit, even without EV charging. Especially in those weak grids, it must be assumed that the risk of power failures in the examined threat scenario is unavoidable. Also, less charge points would have to be attacked or it would suffice to block the charging for a shorter amount of time. Additionally, an attack would lead to negative consequences on more days of the year. The simulation results also show that the number of EVs affected by the attack has a major effect on the grid stability. The risk of power failures caused by such communication attacks increases with the EV penetration. Moreover, the penetration of EVs could locally exceed 50% of households in the near future due to concentration effects, especially in suburb areas. As a consequence, the threat of a local blackout would grow.

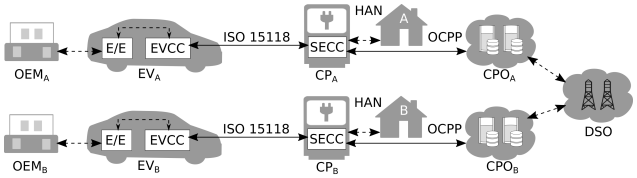


Figure 5: A V2G communication system for exemplary households A and B in the local grid's neighborhood

Those European LV grids that are already enhanced with more powerful transformers and cables [24] are sufficiently protected against the regarded threat scenarios.

5 SYSTEM AND THREAT MODEL

System Model. Figure 5 is a detailed view of our grid model from Section 4 showing all entities involved in EV charging and load management processes. We consider a heterogeneous system consisting of EVs (EV_A and EV_B) and charge points (CP_A and CP_B) from different manufacturers connected to the suburban grid of the DSO. Charge points can be managed by the same or distinct CPOs (CPO_A and CPO_B) using OCPP over wired or wireless connections. CPOs receive energy forecasts and overload signals from the DSO and forward this information to their charge points. A charge point can also be connected to the user's Home Area Network (HAN) to allow the user to check the charging status or adjust the preferences. A charger and an EV communicate via ISO 15118, whereby native authentication modes, i.e., PnC and external means can be used. A Supply Equipment Communication Controller (SECC) and an Electric Vehicle Communication Controller (EVCC) implement OCPP and ISO 15118 functions for the charger and the EV, respectively. The EVCC is connected to the electrical and electronic (E/E) system to exchange data with other internal components like telematics or battery management system and to receive updates from the EV's Original Equipment Manufacturer (OEM) (OEM_A or OEM_B). The dotted lines in Figure 5 depict the respective proprietary links.

We expect a certain mix of popular brands and models of EVs and chargers connected to the grid, due to regional offers and neighbors influence limiting consumer choice [72]. But unlike in public charging, where charge points at the same location are often served by one CPO, freely accessible and seldom under surveillance, the control over a single CPO would be insufficient to affect our grid, and the window of opportunity for local attacks is limited.

Attacker Model. The goal of our adversary is to undermine charging and load management processes in the local power grid. While we are especially interested in malicious actions that can trigger local blackouts, we also consider an attack successful, if it can hinder charging, impersonate an EV or its user, or masquerade devices that cannot flexibly adjust their energy demand as such.

In order to achieve the above goals, the adversary observes the situation on the grid and tampers with EV charging and/or load management in such a way that the conditions identified in our simulation (cf. Section 4) occur. To recap, the adversary wants to determine the moment when the energy consumption is already high and simultaneously activate additional loads on the grid, until the transformer's capacity is exceeded and overload protection trips.

In our exemplary grid, the adversary may need to control charging processes for multiple vehicles. Thereby, depending on the grid structure, blackouts in power lines along one street are likely to occur before the energy supply of the district fails. For this purpose, the adversary (or a group) can observe, intercept, inject, delete, or tamper with any messages transferred in the V2G system, except for encrypted communications unless the cryptographic keys are leaked [27]. Since EVs and charge points are often accessible from the street or in the common parking garage, the adversary can use physical access to tamper with the physical components, extract secrets, or inject crafted (configuration) data.

Attack Vectors. The adversary can use the following main attack vectors to gain the unauthorized control over the V2G system:

- Communications: ISO 15118 stack over PLC (charging cable), E/E communications (CAN, CAN-FD or Ethernet), HAN (WiFi), Wide Area Network (WAN) including OCPP-based and proprietary connections (usually via cellular networks);
- Local systems: EV (EVCC, E/E system), charge point (SECC), and, optionally, IoT devices in home WiFi;
- Backend systems: DSO and CPO (remote access to a set of charge points), OEM (remote access to a set of EVs);
- EV charging processes: EV authentication, charging authorization, session handling, parameter (re)negotiation, target setting, system management.

We assume that the DSO can monitor the situation on the grid (at least, with regard to EV charging), and as soon as the load critically rises, a signal to reduce the consumption is distributed down the chain of command: CPO→Charger→EV for a selected subset of CPOs. Notably, this response cannot take effect instantaneously due to communication delays. For the attack to succeed, the adversary should either be faster to produce the overload before charging is throttled, or be able to counteract this action as part of the attack strategy. For example, first forcing charging EVs to pause helps the adversary prevent the early intervention by the DSO.

6 SECURITY ISSUES OF V2G PROTOCOLS

ISO 15118 provides security controls such as TLS, XML Security, PKI-based authentication, and private key protection [39, 41]. In contrast, OCPP 1.6 [59] is inherently insecure. The security concept enabling optional secure connection setup using TLS 1.2 and secure remote firmware updates was first introduced with OCPP 2.0 in 2018 and then adapted for OCPP 1.6 [4]. Legacy systems are still allowed to use insecure TLS 1.0 and 1.1. OCPP 1.6 was found vulnerable to Man-in-the-Middle (MitM) attacks as well as DoS and data tampering attacks with the potential to disrupt energy services and create overloads [13, 64]. In ISO 15118-2, problems with time synchronization, certificate validation and optional TLS encryption were reported [15, 30].

We confirm these findings and also expect vulnerabilities in the real-world products due to high specification complexity, optional security features and unclear security assumptions. Below we summarize our security analysis of ISO 15118-20 [41] and OCPP 2.0.1 [6], which has not been reported before.

(1) *Insecure channels:* To protect data exchange on the application layer in ISO 15118-2/20, the underlying TLS channel can be used. However, ISO 15118-2 requires TLS only for PnC; with external identification and in private environments like private households the communication is in plaintext [39]. While ISO 15118-20 always applies mTLS, in private environments certificate validation can be skipped and installation of own (root) certificates is permitted [41]. Moreover, it allows a fallback to -2 for legacy support (cf. (2)). Security profiles in OCPP 2.0.1 still use optional TLS [6].

(2) *Version downgrade:* While ISO 15118-20 supports mandatory mTLS with future-proof cipher suits and key lengths, during session setup, a less secure ISO 15118-2 can be negotiated, which allows unencrypted communication in case of EIM and in private environments. The implementation of optional security is up to the vendors and thus TLS is often omitted [14]. The adversary can trick the systems into the downgrade and eavesdrop on all exchanged data.

(3) *Insecure PLC:* The integration of HPGP into ISO 15118 [40] does not support encryption and is subject to eavesdropping and MitM attacks. Thus, an attacker can easily obtain the Network Membership Key used for authentication and join the network as we show in Annex A.

(4) *Session hijacking:* During ISO 15118 session resumption, it is sufficient to send `SessionID` of the previously authenticated session. Since TLS is optional, this data can be eavesdropped by the adversary and used as a bearer token to impersonate the original EV and pause/resume charging, renegotiate charging profiles, or charge on the victim's account. ISO 15118-20 recommends to bind `SessionID` to the mTLS certificates. Yet, these certificates are not part of the application layer authentication, and respective entries on the endpoints can be falsified. While V2GTP protocol is tunneled via TLS, session handling occurs on application layer, and lack of channel binding may also lead to session hijacking.

(5) *No end-to-end guarantees:* While ISO 15118's scope is limited to the communication between an EV and a charge point, most charging processes involve backend systems. Since the data are protected only until they reach the charge point, and there is no end-to-end integrity and confidentiality protection between the EV and the recipient, the charger can easily manipulate the backend communication.

(6) *Cryptographic key reuse:* Neither of the standards properly defines key and certificate management; issues related to, e.g., revocation and deletion of certificates and keys are not discussed at all. ISO 15118 allows reusing authentication keys for signing and encryption purposes.

(7) *Non-existent PKI services:* ISO 15118 and OCPP rely on the V2G PKI to establish trust. Currently, such global trusted party does not exist, and in practice identities cannot be verified with high assurance. The certificate profiles are not detailed enough for full syntactic and semantic validation.

7 V2G ATTACK STRATEGIES

Several parameters handled both in ISO 15118 and OCPP communication can influence the EV charging behavior and thus are of special interest to the adversary:

- Charging profile/schedule: defines (future) time periods when EV or charge point actively consume or transfer energy;

- Tariffs: EVs can be set to charge when energy price is low using tariff updates from one of the backend systems;
- State-of-charge: charging cycles effect battery longevity, and EV avoids overheat, over- or fully discharging the battery;
- User preferences: set target (departure time, state-of-charge) when EV should be charged and ready to go;
- Control signals from DSO/CPO: reduce or increase energy consumption by EVs depending on the grid situation.

Being able to manipulate these parameters is sufficient to control EV charging and the related grid load. The main challenge is reaching the attack scope needed to trigger a blackout (cf. Section 4), which requires a carefully planned attack strategy.

7.1 Attacks on EVs and Charge Points

7.1.1 Car-bot Attack. The adversary gains (remote) access to the EVCC or the E/E system of a vehicle, e.g., using one of the exploits described in Section 2 and is able to inject commands to start/stop or pause/resume charging. In case of paused charging, the resumed session uses the previously negotiated charging schedule and parameters, which may not fit to the current grid situation and directly lead to a peak consumption. If not, the adversary injects a new charging schedule pausing and activating the load at a chosen time to facilitate the planned attack. Since many OEMs offer connected car apps allowing users to manage the battery recharge, the adversary can also use compromised apps or stolen user credentials to create such schedule, e.g., by changing the departure time. In addition, the adversary can connect own prepared EVs to the local grid using the charge points in the neighborhood open for public charging to amplify the effect caused by the botnet.

7.1.2 Charger-bot Attack. The adversary manages to install malicious firmware on a charge point, e.g., via an USB port or manipulated update image (cf. Section 2), potentially with help of social engineering to get physical access to the device. This gives the adversary persistent remote access that allows eavesdropping on the charger's communication with the CPO and the vehicle and modify messages to induce the desired behavior. This way, the adversary can suppress load reduction commands received from the backend, tailor the charging schedule to the planned attack schedule, spoof tariff information, or simply start and stop charging at will (in ISO 15118, only vehicle can pause/resume a charging session). The adversary can also use the physical access to start/stop charging of the connected vehicle, e.g., by pushing the button on the user interface featured by many private chargers. Since AC chargers for private use are much less expensive than EVs, security features are often limited, which can facilitate attacks.

7.1.3 Masquerading as Flexibility Resource. The adversary can connect a vehicle simulator such as EVSim [23] that can be recognized as a controllable load by the charger but provides false data about power consumption and ignores any overload signals.

7.2 Attacks on Charging Communications

7.2.1 DoS Attack. To stop charging in a desired area at once, the adversary sends a jamming signal like one described in the Broken-wire attack [46]. If the charging system recovers automatically, the attack is repeated. The connection to the backend over a cellular network is subject to DoS or fake base station attacks that can block load management processes in the targeted area in a similar way.

7.2.2 PLC Injection Attack. Since the link layer in ISO 15118 is not protected against eavesdropping and manipulation, the adversary can use a commercial, e.g., CCS Listener [77] or a custom-made PLC device [28] connected to the same grid via, e.g., an earthed socket on the charger or at the parking lot to capture, inject and modify V2G messages. Since TLS in ISO 15118-2 is optional, all communication can be available to the eavesdropper. The adversary can extract such information as EVCCID (vehicle's MAC), `sessionID` of the current charging session, charging schedules and tariffs, which can help preparing the attack. Using the captured `sessionID`, the adversary can craft and inject arbitrary messages that meet the specified ISO 15118 format to control the charging session to suit the selected attack strategy. Moreover, the adversary can disturb the UDP based pairing via HPGP between the EVCC and SECC, thus, causing the disconnect and charge stop, or even make the vehicle to connect to a decoy.

7.2.3 MitM Attack. The communication between a charge point and the CPO backend is usually unencrypted, which makes it possible to intercept it. Also, the lack of authentication between these systems allows the adversary to impersonate any of the parties and spoof communications. Even if TLS is used, OCPP 2.0.1 does not require from the charger to validate the certificate provided by the backend. Therefore, if the adversary manages to tap into the communication link, e.g., by using a fake base station, the backend system can be easily spoofed. This allows remotely sending OCPP commands to start/stop charging or initiating a complex attack using charging schedules and tariffs. Spoofing the charge point is also possible in ISO 15118-2/20, as in private environment certificate validation is relaxed. In some cases, the leaked private root may be needed to succeed in ISO 15118-20.

7.3 Attacks on V2G Processes

7.3.1 PnC Authorization Attack. Using an in-cable adapter and weaknesses in the channel binding and PnC authentication (cf. Section 6), the adversary can impersonate a benign EV to join the grid. As charging schedules are often reputation-based, i.e., relying on the known behavior of the authorized consumer, the adversary can exploit priority charging options this way.

7.3.2 Resumption Attack. Once authenticated, the vehicle can pause and resume ISO 15118 sessions by simply presenting the identifier `sessionID`. In EIM mode, the V2GTP communication is not encrypted and thus all parameters can be extracted by the attacker. Other ways to obtain this value are a compromised EV or charger or by bruteforce. Some chargers use simple counters for `sessionID`, which can be predicted. The length also depends on the implementation, e.g., RISE-V2G uses only 8 bytes. The adversary then can control the session, inject messages, or spoof the EV.

7.4 Malicious Backend Attack

CPO and DSO backend systems are part of the load management, as they provide charging schedules suited to the LV grid situation in the first place. Thus, backend attacks have the potential to cause critical conditions and cannot be ruled out. If an adversary gains

control over the management processes in the backend, they can observe the load fluctuations on the grid and change the charging behavior of the managed chargers. The adversary can craft a charging schedule to facilitate the overload and distribute it via OCPP to charge points. Each charge point will start renegotiating the ongoing charging session via ISO 15118. If the EV and the charger negotiated the dynamic control mode (vs scheduled mode, where EVCC takes into user's needs), the charge point simply adapts the charging behavior per backend's request. Also, the adversary can inject a tariff update (since authenticating signature is optional) to encourage or discourage EVs from charging by using the energy price. Such backend systems will require ISO 27000 certification in Europe and would be harder to compromise than private charging facilities, which are the focus of our study.

8 EXPERIMENTAL SECURITY ANALYSIS OF V2G COMMUNICATION

In Section 6, we defined the risk of attacks on local power grids serving EV charging. In this section, we show these attacks are possible against real charge points through practical evaluation of the main communication links: Charger↔CPO and Charger↔EV.

8.1 Evaluation of Charger Communication

Our evaluation environment comprises three charge points from different manufacturers: two 22 kW Alternating Current (AC) wallboxes and one Direct Current (DC) high power charger (HPC). All charge points implemented OCPP 1.6 and TLS to interface with the CPO (cf. Table 2). Our tests used default security settings.

Table 2: Charger configurations observed in experiments

Wallbox A	OCPP 1.5, 1.6	TLS 1.0, 1.1, 1.2	TLS active
Wallbox B	OCPP 1.6, 2.0	TLS 1.0, 1.1, 1.2; SSL 3.0	TLS active
HPC	OCPP 1.5, 1.6	TLS 1.0, 1.1, 1.2; SSL 3.0	TLS active

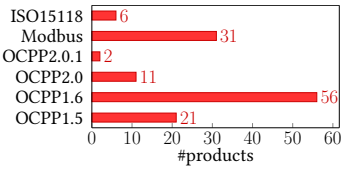
8.1.1 Evaluation Summary. We intercepted messages between the chargers and the CPO to analyze the security of this connection. Thereby we checked the TLS version, the supported ciphers, the certificate validation, and the possibility to inject OCPP messages. All chargers accepted arbitrary self-signed certificates and thus even with activated TLS encryption were vulnerable to MitM attacks. Only for Wallbox B, with help from the manufacturer, we could configure the firmware to validate certificates correctly. All chargers featured insecure TLS versions. Especially the usage of SSL and ciphers containing RC4 pose a serious threat for downgrade attacks.

8.1.2 Practical Attack. Using SteVe [66] for OCPP and own self-signed certificates, we could read and modify the communication of all three products to cause the desired behavior: alter a charging schedule by injecting carefully crafted messages and interrupt the charging process at will. Figure 6a shows Wallbox A disabled by a remote attack on the OCPP connection, which is indicated by the red status light. Annex A describes the attack's details.

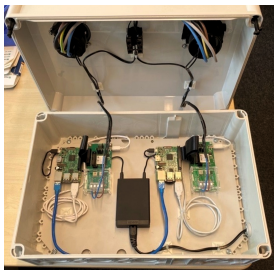
8.2 Evaluation of ISO 15118 Communication

In the second practical evaluation, we analyzed the security of data exchange between the charger and the EV via ISO 15118. To be able to intercept and manipulate the low-level communication using HPGP/PLC, we designed and built an evaluation setup based on a PLC development board with a Qualcomm QCA7000 controller shown in Figure 6c. In our experiments, we used RISE V2G [54] as the reference implementation for ISO 15118-2.

(a) Wallbox disabled by OCPP attack



(b) Protocols supported in modern chargers



(c) Test setup for ISO 15118 communication

Figure 6: Experimental analysis of OCPP and ISO 15118

In a simple DoS attack, we were able to interrupt the active communication session and stop the charging process by using V2GInjector [28, 60] to send a `SessionStop` message from a rogue PLC device. Due to the strict timeouts and message format requirements in ISO 15118, delaying or injecting unexpected or malformed messages also led to charging failures.

Since the performance of Python-based V2GInjector was insufficient for more complex attacks, we developed a native C implementation for further tests. This way, we realized a MitM attack on ISO 15118 communication described in Annex A and were able to eavesdrop on charging sessions and collect data like private payment details or service information. These data help predict charging behavior and plan offensive actions. We could also inject own charging schedules and tariffs to activate loads at a selected time as well as pause and restart charging sessions at will.

8.3 Relevance of the Evaluation Results

Both practical evaluations show that it takes little effort for an adversary to control charging sessions. The relevance of this result for the security of power supply in the local grid partly depends on the real-world adoption of the protocols at hand. Therefore, we analyzed products from the German market overview [7] including wallboxes with 11 kW and 22 kW, AC and DC chargers (cf. Annex B). As shown in Figure 6b, 90 models support OCPP but only two offer the newest version protecting against MitM attacks. The vast majority supports OCPP 1.6 or lower with known specification weaknesses. ISO 15118 is implemented only in 6 products. Considering this analysis and our practical evaluation, we argue that most charging products should add measures against the V2G attacks.

8.4 Ethic Considerations and Disclosure

We run our practical experiments in the controlled environment of a private car park, with a certified electrician present to ensure safety. Grid-wide effects were only studied in simulation.

We disclosed our findings on charge point security to the respective manufacturers. Since we did not receive any feedback, we must assume that products will remain vulnerable and do not plan to publish implementations of our attacks at this time.

9 LIMITATIONS AND MITIGATION

Practicality of the Attack. According to our simulation and analysis, damaging the equipment or causing a blackout in the LV grid is possible but takes a significant load accumulated over time. If limits are exceeded, intervention by the DSO is required to prevent impact to equipment, blackouts and possible harm to consumers. Our attack assumes detailed knowledge of local EV models and installed chargers, but the currently fragmented market may soon consolidate. Adequate detection by DSO or CPO may prevent an attacker from experimenting for a long time to find the correct timing. But practical experience with fire drills or power outages tells that this is unlikely to work unless the event is regularly exercised.

Larger-scale attacks and generalizations must also be considered. Future attackers could devise a *blackout botnet* comprising several components to reach the required load $L_{total} = L_{basic} + L_{delayed} + L_{scheduled} + L_{controlled} + L_{blackiot}$. Here, L_{basic} is normal energy consumption in the neighborhood driven by personal needs of the residents. $L_{delayed}$ are consumers whose charging was shifted by a DoS attack like Brokenwire [46], which can interrupt multiple charging sessions in the radius of up to 40 m. $L_{scheduled}$ are charging facilities following a predictable or attacker-manipulated schedule. This can be achieved by manipulating the communication of charge points as described in Sections 7.2, 8 and Annex A, or by hijacking their cellular connections using one of the proven methods [9, 18, 37, 49, 51, 53, 65, 69]. $L_{controlled}$ are consumers that either belong to the adversary or are under his/her direct control, e.g., due to compromised software update [20, 34]. Finally, $L_{blackiot}$ reflects the possibility to boost the attack using a botnet of regular (non-managed) but high-wattage devices, e.g. as in [70]. Inconspicuous devices such as wallboxes, air conditioners, heat pumps and other systems may remain compromised for a long time as they are rarely updated or replaced.

Mitigation Strategies. Our simulations show that an adversary can make an LV grid collapse by manipulating V2G communication used for load management. The detailed conditions for a successful attack, as well as the required effort and possible impact should be considered by the individual grid operators and policy makers. Possible countermeasures can be undertaken in terms of improving overall grid capacity, improving the security of load management, and possibly also in form of safety and fallback mechanisms.

In terms of securing the load management infrastructure, identified weaknesses in deployed protocols and implementations should be fixed. Strong mutual authentication and mandatory use of secure channels on all communication layers between EV and charger, as well as charger and backend would mitigate the identified MitM attacks. Additionally, management data and commands transferred via intermediaries should be authenticated end-to-end, to prevent adversaries from manipulating charging schedules or tariffs.

In our experiments with OCPP, it sufficed to join the network connecting the charger to its backend to gain control of the charger due to flawed implementation of the certificate validation. As it is often not possible to update insecure protocol versions in legacy systems like private wallboxes, we believe that adequate protection of the underlying communication networks and separation of network segments used for load management from other types of traffic is an important measure for private environments.

Where possible, countermeasures should also be put against known and widely applicable attacks such as Brokenwire [46], to prevent attackers from combining multiple vectors. In our simulated attack, DoS attacks on V2G communication are instrumental in reaching the required consumption level.

Finally, it should be mandatory for participants in this critical infrastructure to have a security process in place to ensure a minimum level of configuration and security management. Automotive ISO 21434 requires this for car manufacturers, but not for other participants in the V2G infrastructure.

10 CONCLUSION

The need to integrate a continuously growing fleet of EVs in local power grids puts their operators before a dilemma: should they invest into equipment upgrades or can they rely on load management and V2G technology to cope with the increased demand? In this work, we show that the ability to manage grid load can be impacted by targeted manipulation of large consumers such as EVs. To assess the risks, we model and analyze the conditions under which local grids can collapse and review a range of possible attack vectors that could be exploited to this end.

Our simulation shows that blackouts are possible if the grid's capacity is close to its limit, or if unchecked vulnerabilities create a potential for large-scale attacks. We hope that our analysis will be useful for operators and policy makers to better understand the future risks and provide adequate mitigation.

ACKNOWLEDGMENTS

This work was partly funded by the German Federal Ministry of Education and Research (BMBF) and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. Further funding was provided by the German Federal Ministry for Economic Affairs and Climate Action (BMWK) within the projects IntegraNet II (FKZ 03EI1008A), unIT-e^2 (FKZ 01MV21UN12) and LamA-connect (FKZ 01MZ18009A). We thank Steffen Schulz, our shepherd Mu Zhang, and our anonymous reviewers for their valuable suggestions.

REFERENCES

[1] 2015. Green eMotion: Development and demonstrations of a unique and user-friendly framework for green electromobility in Europe.
[2] 2018. *Experimental Security Assessment of BMW Cars: A Summary Report.* Technical Report. Tencent Keen Security Lab.
[3] 2020. Global EV Outlook 2021. https://www.iea.org/reports/global-ev-outlook-2021/trends-and-developments-in-electric-vehicle-markets
[4] 2020. *Improved security for OCPP 1.6-J.* Technical Report. Open Charge Alliance.

[5] 2020. *Open Charge Point Protocol 2.0.1 – Part 0 – Introduction.* Open Standard. Open Charge Alliance.

[6] 2020. *Open Charge Point Protocol 2.0.1 - Part 2 - Specification.* Open Standard. Open Charge Alliance, Arnhem, Netherlands.

[7] 2022. Ministry of Economics, Innovation, Digitalization and Energy of Nordrhein-Westfalen. Charge Point Market Overview. https://www.elektromobilitaet.nrw/unser-service/marktuebersicht-ladestationen/

[8] 50Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, and TransnetBW GmbH. 2021. *Netzentwicklungsplan Strom 2035.* Technical Report.

[9] Dare Abodunrin, Yoan Miche, and Silke Holtmanns. 2015. Some dangers from 2G networks legacy support and a possible mitigation. In *2015 IEEE Conference on Communications and Network Security (CNS)*. 585–593. https://doi.org/10.1109/CNS.2015.7346872

[10] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. 2020. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access* 8 (2020), 214434–214453. https://doi.org/10.1109/ACCESS.2020.3041074

[11] RWE Deutschland AG. 2011. Grid for Vehicles – Analysis of the impact and possibilities of a mass introduction of electric and plug-in hybrid vehicles on the electricity networks in Europe: Final Publishable Summary Report.

[12] RWE Deutschland AG. 2016. PlanGridEV: Distribution grid planning and operational principles for electric vehicle mass roll-out while enabling integration of renewable distributed energy resources.

[13] C. Alcaraz, J. Lopez, and S. Wolthusen. 2017. OCPP Protocol: Security Threats and Challenges. *IEEE Transactions on Smart Grid* 8, 5 (Sept 2017), 2452–2459. https://doi.org/10.1109/TSG.2017.2669647

[14] 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, 407–424.

[15] K. Bao, H. Valev, M. Wagner, and H. Schmeck. 2017. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science - Research and Development* (01 Sep 2017).

[16] Jesper Berggreen. 2017. Norwegian Grid Struggling To Keep Up With Growing EV Fleet. https://evobsession.com/norwegian-grid-struggling-keep-growing-ev-fleet

[17] Uwe Bigalke, Aline Armbruster, Franziska Lukas, Oliver Krieger, Oliver Schuch, and Jan Kunde. 2016. *dena Gebäudereport: Statistiken und Analysen zur Energieeffizienz im Gebäudebestand.* Technical Report. Deutsche Energie-Agentur GmbH.

[18] Evangelos Bitsikas and Christina Pöpper. 2021. Don't Hand It Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications. In *Annual Computer Security Applications Conference (ACSAC '21)*. Association for Computing Machinery, 900–915. https://doi.org/10.1145/3485832.3485914

[19] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security (SEC'11)*. USENIX Association.

[20] Huajiang Chen and Wu Ming. 2021. Remotely Rooting Charging Station For Fun And Maybe Profit. http://chv.link/kevin2600

[21] Gianpiero Costantino and Ilaria Matteucci. 2020. *KOFFEE - Kia OFFensivE Exploit.* Technical Report. National Research Council CNR.

[22] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 2017. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC '17)*. ACM, 303–314. https://doi.org/10.1145/3134600.3134639

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

[24] CIGRÉ Des électriques, Conseil international grands réseaux. 2014. *Benchmark systems for network integration of renewable and distributed energy resources.* CIGRÉ.

[25] DIN Deutsches Institut für Normung e. V. 2017. DIN EN 12831-1:2017 Energetische Bewertung von Gebäuden – Verfahren zur Berechnung der Norm-Heizlast – Teil 1: Raumheizlast, Modul M3-3.

[26] DIN Deutsches Institut für Normung e. V. 2017. DIN EN 15316-4-3:2017-09: Energetische Bewertung von Gebäuden.

[27] D. Dolev and A. Yao. 1983. On the security of public key protocols. *IEEE Transactions on Information Theory* 29, 2 (Mar 1983), 198–208. https://doi.org/10.1109/TIT.1983.1056650

[28] Sébastien Dudek, Jean-Christophe Delaunay, and Vincent Fargues. 2019. *V2G Injector: Whispering to cars and charging units through the Power-Line.* Technical Report. SSTIC 2019. https://www.sstic.org/media/SSTIC2019/SSTIC-actes/v2g_injector_playing_with_electric_cars_and_chargi/SSTIC2019-Article-v2g_injector_playing_with_electric_cars_and_charging_stations_via_powerline-dudek.pdf

[29] ENTSO-E. 2021. Electric Vehicle Integration into Power Grids: Position Paper.

[30] R. Falk and S. Fries. 2012. Electric vehicle charging infrastructure security considerations and approaches. *INTERNET 2012: The Fourth International Conference on Evolving Internet* (2012), 58–64.

[31] Dennis Fisher. 2011. DigiNotar Says Its CA Infrastructure Was Compromised. https://threatpost.com/diginotar-says-its-ca-infrastructure-was-compromised-083011/75594/

[32] ForskEl. 2012. Electric vehicles in a Distributed and Integrated market using Sustainable energy and Open Networks (E.D.I.S.O.N.) – EV portfolio management and grid impact study.

[33] Yangyang Fu, Sen Huang, Draguna Vrabie, and Wangda Zuo. 2011. Coupling Power System Dynamics and Building Dynamics to Enabling Building-to-Grid Integration. In *Proceedings of the 13th International Modelica Conference*, Modelica Association (Ed.). Regensburg, Germany, 561–566.

[34] Andy Greenberg. 2015. Hackers Remotely Kill A Jeep On The Highway – with Me In It.

[35] Simon Haverkamp and Martin Simons. 2022. *Cybersecurity in the charging ecosystem. Status quo and stakeholder ambitions.* Technical Report. umlaut energy GmbH on behalf of Mercedes-Benz AG.

[36] Klaus Heuck, Klaus-Dieter Dettmann, and Detlef Schulz. 2013. *Elektrische Energieversorgung: Erzeugung, Übertragung und Verteilung elektrischer Energie für Studium und Praxis* (9. ed.). Springer Vieweg, Wiesbaden.

[37] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *25th Annual Network and Distributed System Security Symposium NDSS*. The Internet Society.

[38] ISO/IEC. 2013. *Road vehicles – Vehicle to grid communication interface – Part 1: General information and use-case definition.*

[39] ISO/IEC. 2014. *Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements.*

[40] ISO/IEC. 2015. *Road vehicles – Vehicle to grid communication interface – Part 3: Physical and data link layer requirements.*

[41] ISO/IEC. 2022. *Road vehicles – Vehicle-to-Grid Communication Interface – Part 20: Network and application protocol requirements.* Geneva, Switzerland.

[42] Georg Kerber. 2011. *Aufnahmefähigkeit von Niederspannungsverteilnetzen für die Einspeisung aus Photovoltaikkleinanlagen.* Ph.D. Dissertation. TU Munich.

[43] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. 2010. Experimental Security Analysis of a Modern Automobile. In *2010 IEEE Symposium on Security and Privacy*. 447–462. https://doi.org/10.1109/SP.2010.34

[44] S. Krähenmann, A. Walter, S. Brienen, F. Imbery, and A. Matzaraki. 2018. High-resolution grids of hourly meteorological variables for Germany. *Theoretical and Applied Climatology* 131 (2018), 899––926. Issue 2018. https://link.springer.com/content/pdf/10.1007/s00704-016-2003-7.pdf

[45] Mikhail Kuzin and Victor Chebyshev. 2017. Mobile apps and stealing a connected car. https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/

[46] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. 2022. Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging. arXiv:2202.02104 [cs.CR]

[47] Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu. 2012. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine* 50, 8 (2012), 38–45. https://doi.org/10.1109/MCOM.2012.6257525

[48] Robert McMillan. 2011. Comodo Hacker Claims Another Certificate Authority. https://www.pcworld.com/article/223760/article.html

[49] Ulrike Meyer and Susanne Wetzel. 2004. A Man-in-the-Middle Attack on UMTS. In *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04)*. Association for Computing Machinery, 90–97. https://doi.org/10.1145/1023646.1023662

[50] Charlie Miller and Chris Valasek. 2015. *Remote Exploitation of an Unaltered Passenger Vehicle.* Technical Report. Illmatics.

[51] Stig F. Mjølsnes and Ruxandra F. Olimid. 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. In *Computer Network Security*. Springer International Publishing, 235–246.

[52] Modelica Association. 2017. *Modelica - A Unified Object-Oriented Language for Systems Modeling. Language Specification. Version 3.4.* Technical Report. Linköping, Sweden.

[53] T. Moore, T. Kosloff, J. Keller, G. Manes, and S. Shenoi. 2002. Signaling system 7 (SS7) network security. In *The 2002 45th Midwest Symposium on Circuits and Systems MWSCAS*, Vol. 3.

[54] Marc Mueltin. 2022. RISE V2G: the Reference Implementation Supporting the Evolution of the Vehicle-2-Grid. https://github.com/SwitchEV/RISE-V2G

[55] Myriam Neaimeh and Peter Andersen. 2020. Mind the gap – open communication protocols for vehicle grid integration. *Energy Informatics* 3 (02 2020).

[56] Sen Nie, Ling Liu, and Yuefeng Du. 2017. *Free-Fall: Hacking Tesla From Wireless To CAN Bus.* Technical Report. Keen Security Lab of Tencent.

[57] Sen Nie, Ling Liu, Yuefeng Du, and Wenkai Zhang. 2019. *Over-The-Air: How We Remotely Compromised The Gateway, BCM, and Autopilot ECUs Of Tesla Cars.* Technical Report. Keen Security Lab of Tencent.

[58] Thomas Nowak. 2021. European heat pump market. *REHVA Journal* August 2021 (02 2021), 40–43.

[59] Open Charge Alliance (OCA) 2017. *Open Charge Point Protocol (OCPP) 1.6* (edition 2 ed.). Open Charge Alliance (OCA). http://www.openchargealliance.org/protocols/ocpp/ocpp-16/
[60] Penthertz. 2022. V2GInjector. https://github.com/FlUxIuS/V2GInjector
[61] N. Pflugradt and B. Platzer. 2012. Behavior based load profile generator for domestic hot water and electricity use. In *Innostock 12th International Conference on Energy Storage, Lleida (Spanien)*.
[62] P. Rademakers and P. Klapwijk. 2017. EV Related Protocol Study.
[63] Khaleda Rahman. 2022. Californians Told Not to Charge Electric Cars Days After Gas Car Sales Ban. https://www.newsweek.com/californians-told-not-charge-electric-cars-gas-car-sales-ban-1738398
[64] J. E. Rubio, C. Alcaraz, and J. 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)*. 1–5. https://doi.org/10.1109/NTMS.2018.8328675
[65] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on Layer Two. In *2019 IEEE Symposium on Security and Privacy (SP)*. 1121–1136. https://doi.org/10.1109/SP.2019.00006
[66] RWTH Aachen University. 2022. SteVe. https://github.com/RWTH-i5-IDSG/steve
[67] Schneider Electric. 2022. *Electrical Installation Wiki.* https://www.electrical-installation.org/enwiki/Main_Page
[68] Anne Senkel, Carsten Bode, Jan-Peter Heckel, Oliver Schölting, Gerhard Schmitz, Christian Becker, and Alfons Kather. 2021. Status of the TransiEnt Library: Transient Simulation of Complex Integrated Energy Systems. In *Proceedings of the 14th International Modelica Conference*, Modelica Association (Ed.). https://doi.org/10.3384/ecp21181187
[69] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 221–231. https://doi.org/10.1145/3317549.3319728
[70] 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)*. USENIX Association, 15–32.
[71] Stadt Köln - Amt für Stadtentwicklung und Statistik. 2021. Generationenwechsel in älteren Ein- und Zweifamilienhausgebieten: Untersuchung im Rahmen des Stadtentwicklungskonzeptes Wohnen. (2021). https://www.stadt-koeln.de/mediaasset/content/pdf15/statistik-bauen-und-wohnen/generationenwechsel_in_aelteren_ein-_und_zweifamilienhausgebieten_bw_ksn_2012_2.pdf
[72] Carolin Stockkamp, Juliane Schäfer, Jan A. Millemann, and Sven Heidenreich. 2021. Identifying Factors Associated with Consumers' Adoption of e-Mobility – A Systematic Literature Review. *Sustainability* 13, 19 (2021). https://doi.org/10.3390/su131910975
[73] Vangelis Stykas. 2021. Smart car chargers. Plug-n-Play for hackers? https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/
[74] Bernd Thormann, René Braunstein, Johannes Wisiak, Franz Strempfl, and Thomas Kienberger. 2019. Evaluation of Grid Relieving Measures for Integrating Electric Vehicles in a Suburban Low-Voltage Grid.
[75] Michael Tiller. 2001. *Introduction to physical modeling with Modelica.* The Kluwer international series in engineering and computer science, Vol. SECS 615. Kluwer Academic Publishers, Boston.
[76] Ultra Lithium Inc. 2019. Peak-Hour Charging a Norwegian Problem. https://ultralithium.com/peak-hour-charging-norwegian-problem
[77] Vector. 2022. CCS Listener. https://www.vector.com/int/en/products/products-a-z/hardware/vh5110/
[78] Bart Verbruggen, Juan Van Roy, Roel De Coninck, Ruben Batens, Lieve Helsen, and Johan Driesen. 2011. Object-Oriented Electrical Grid and Photovoltaic system modelling in Modelica. In *Proceedings of the 8th International Modelica Conference*, Modelica Association (Ed.). 730–738.
[79] Ralf-Philipp Weinmann and Benedikt Schmotzle. 2021. *TBONE – A zero-click exploit for Tesla MCUs.* Technical Report. Comsecuris UG.
[80] Marian Willuhn. 2022. Satellite cyber attack paralyzes 11GW of German wind turbines. https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/
[81] Dietmar Winkler. 2017. Electrical Power System Modelling in Modelica – Comparing Open-source Library Options. In *Proceedings of the 58th SIMS*. Reykjavik, Iceland, 263–270. https://doi.org/10.3384/ecp15118695
[82] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. 2012. A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys and Tutorials* 14, 4 (2012), 998–1010. https://doi.org/10.1109/SURV.2012.010912.00035
[83] Kim Zetter. 2014. Sony Got Hacked Hard: What We Know and Don't Know So Far. https://www.wired.com/2014/12/sony-hack-what-we-know/
[84] Kim Zetter. 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/
[85] Maria Zhdanova. 2022. *Security and Trust in Safety Critical Infrastructures.* Ph.D. Dissertation. Technical University Darmstadt. https://doi.org/doi.org/10.26083/tuprints-00021505

A DETAILS OF EXPERIMENTAL ATTACKS

A.1 OCPP Attack

It is possible for an attacker to compromise the OCPP communication between the charge point and the backend system of its operator and even become MitM. This attack requires solving several problems in order to gain access to the network and the communication. As a first step, the attacker needs to obtain access to the network used for the charging communication. Charge points are either physically connected to the home or company network or remotely connected via a cellular network. In our tests, we maintained access to the company network serving 8 AC and 1 DC chargers via a physical LAN connection. Alternatively, a WiFi access could be used. Moreover, a cellular connection by itself would not hold the attacker back due to the known security issues of the existing mobile communication standards like GSM [9], SS7 [53], UMTS [49], and LTE [37, 65]. So lack of authentication and integrity protection allow the attacker to eavesdrop or redirect mobile traffic of charge points in the area via a false base station [18, 51, 69]. In contrast, the usage of VPN would impede the attack but we did not see this technique in operation during our tests. Using ARP spoofing, we were able to redirect traffic to our attack device.

On the application level, the attacker needs to overcome the TLS protection. It should be noted that TLS is often optional or not active in private environments and less expensive wallboxes. In our setup, the TLS was active but certificate validation was not performed, so presenting a self-signed certificate during the key exchange was sufficient to achieve the MitM position.

Figure 7: Manipulating OCPP communication

As a next step, the attacker has to send a carefully prepared `SetChargingProfileRequest` message with a new charging profile to the charge point to reduce the charged power to a minimal level (cf. Figure 7). We were also able to reset the limit within this profile at an arbitrary point in time. This way, the adversary can control the charging behavior of the connected EV, and ensure that its battery is not fully charged until the planned start of the blackout attack.

Once network access is established, this attack is very easy to carry out. The described attack steps have been proved effective for all evaluated charge points from Section 8.1.

A.2 ISO 15118 Attack

Since the low-level powerline communication (PLC) in ISO 15118 is unencrypted [40], we use it as an entry point to compromise the load management during EV charging in the setup described in Section 8.2. The attack on HPGP/PLC runs in 3 steps: (1) connecting to the PLC network, (2) intercepting messages to get into a MitM position, and, finally, (3) executing an application level attack.

As a first step, an adversary connects to the HPGP/PLC network of the targeted charger to impersonate this charger for a vehicle. In ISO 15118, the SLAC Protocol (Signal Level Attenuation Characterization) is used to establish pairing between an EV and a charge point [40]. In this process, the charge point is the central coordinator that broadcasts `CM_SLAC_MATCH` messages containing the so-called Network Membership Key. Any device that wishes to connect to this network requires this key.

Once the adversary has access to this HPGP/PLC network on the MAC and IP level, an attack against the service discovery (SDP) [39] of ISO 15118 is possible. Figure 8 illustrates this process, where an EV searches for a charge point using an `SECC_RequestMessage` and both the charge point and the MitM attacker replies with an `SECC_ResponseMessage` containing the target port and IP address.

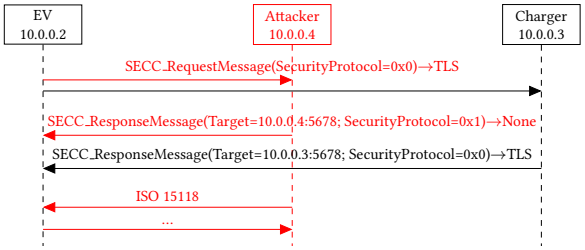


Figure 8: MitM attack on ISO 15118 communication

To be able to send this message faster than the charger, we implemented a small native program in C. This program can also disable the TLS connection for the EV by injecting an SDP message such that the vehicle believes that the charger does not support TLS (and the charger believes that the vehicle did not request TLS). This results in downgrading authentication options to external means (EIM) only and communicating in plaintext. Since management operations in ISO 15118-2 are also possible with EIM, this should suit most adversarial goals.

Now, the attacker can redirect the traffic from the vehicle to own device by sending a specially crafted response with its port and address. In this position, the attacker owns the charging session with the EV and can now change arbitrary parameters of the charging process for this vehicle without further difficulties. For example, the attacker can inject a `SessionStop` request to stop the charging session without risking an error state or can inject a `PowerDelivery` request to initiate the renegotiation of charging parameters and force the desired charging schedule. This way, the attacker can ensure that the EV is available as a load when needed.

Similarly, the attacker can impersonate the vehicle to the charger. It should be noted that all application messages in the ISO 15118's communication flow are encoded using the Efficient XML Interchange (EXI) standard. It is a relatively exotic standard and only few EXI implementations exist.

B CHARGING PRODUCTS ON GERMAN MARKET

Tables 3 and 4 give an overview of the communication protocols supported by modern charging products based on the recent study [7].

Table 4: Chargers and protocols

Manufacturer	Model	Supported Protocol	Year
e.Go	Wallbox Home	OCPP1.6	2022
	eBox smart	OCPP2.0, ISO 15116 ready	2022
ESL E-MOBILITY	WALLI LIGHT PRO	Modbus TCP / RS 485	2022
	WALI LIGHT COMFORT	Modbus TCP / RS 485	2022
	INCH Home	OCPP1.6, Modbus TCP	2022
	INCH Pro	OCPP1.6, OCPP2.0, Modbus TCP	2022
	HomeLine	OCPP1.2, OCPP1.5, OCPP1.6	2021
EVSE-WiFi.de	smartWB	Modbus / TCP	
go-e	go-e Charger HOME+	OCPP1.6	2022
	go-eCharger HOMEfix	OCPP1.6	2022
Entratek	Wallbox Power Dot Eco	OCPP1.6	2022
	Wallbox Power Dot Fix	OCPP1.6, Modbus	2022
	Wallbox Power Dot Pro	OCPP1.6	2022
	Wallbox Power Dot Pro 2	OCPP1.6	2022
Gustav Hensel	witty flow	EEBUS, TCP/IP, ISO15118	2021
Heidelberg	eBox wr30-R/L Smart	eCCP, OCPP1.6, Modbus TCP	2021
	eBox sr10 Smart	eCCP, OCPP1.6, Modbus TCP	2021
Ingeteam	INGEREV GARAGE	OCPP	2022
	eBox smart	OCPP1.6	
	eBox Professional	OCPP1.6, ISO 15118	
	c-series	OCPP, UDP& Modbus TCP	2022
	x-series	OCPP, UDP& Modbus TCP	2022
	Mikro	Modbus	2021
	AMTRON Compact 2.0s	Modbus RTU	2022
	AMTRON Professional	OCPP1.5, OCPP1.6	2022
myenergi	BOXX	OCPP	2022
openWB	e-Wallbox Premium	OCPP	2017
PRACHT	ALPHA XT(+)	Modbus RTU	2022
RTB	Kormo	OCPP	2021
	EVlink Wallbox G4 smart	OCPP1.6	2022
SMA	EV CHARGER 7,4 / 22	digital input	
	Pay-Charge	OCPP1.5, OCPP1.6	2022
SWARCO	evolt EVe mini	OCPP1.5	2018
	evolt EVe Duo	OCPP1.5	2018
	evolt Public PWB	OCPP1.5	
TechniSat Digital GmbH	TECHNIVOLT 100	Modbus RS485	2022
	TECHNIVOLT 101	Modbus RS485	2022
	TECHNIVOLT 1100 SMART	OCPP1.5, OCPP 1.6, ISO 15118 ready	2022
	TECHNIVOLT 2200 SMART	OCPP1.5, OCPP 1.6, ISO 15118 ready	2022
	ID. Charger Connect	OCPP2.0	2022
	ID. Charger Pro	OCPP2.0	2022
	LUX	Modbus RS485	2022
	LUX smart	Modbus RS485	2022
	Pro	Modbus TCP, OCPP 1.6	2022
	Pro Plus	Modbus TCP, OCPP 1.6	2022
	NEO	OCPP1.5, OCPP1.6	2022

Table 3: Chargers and protocols

Manufacturer	Model	Supported Protocol	Year
ABB	EVLunic Pro S	OCPP1.5	2019
	EVLunic Pro M	OCPP1.5	2019
	Terra AC	OCPP1.6	2022
ABL	eMH1	OCPP1.5+	2019
	eMH2	OCPP1.6	2019
	eMH3 (twin)	OCPP1.5, OCPP1.6	2019
Alfen (NL)	Eve Single S-line	OCPP1.6	2022
	Eve Single Pro-line	OCPP1.6, Modbus TCP	2022
	Eve Double Pro-line	OCPP1.5, OCPP1.6, OCPP2.01, TCP	2022
aixACCT charging solutions	elexon A1	OCPP1.6	2020
	elexon A1	OCPP1.6	2020
AoNeng	11 kW Wallbox / Comfort	OCPP1.6	2018
	Comfort-Duo	RS-485	2022
	Comfort-Pro	RS-485	2022
	Comfort-Pro-Duo	RS-485, Optional: RJ45	2022
	CLS2000-A2	Modbus-RTU	2022
cFos eMobility	cFos Power Brain Wallbox	OCPP1.6	2022
		OCPP1.5, OCPP1.6, TCP	2022
ChargePoint	CP4100	OCPP	2022
	CP4100	OCPP	2022
	CP4300	OCPP	2022
	CP4300	OCPP	2022
ChargeX	Aqueduct+	Plug & Play	2022
	Aqueduct+ Pro	Plug & Play	2022
Circontrol	eNext	OCPP 1.6 (2.0 ready)	2022
	eNext	OCPP 1.6 (2.0 ready)	2022
	WB eVolve Smart	OCPP 1.5 (1.6 optional)	2022
	WB eVolve Smart	OCPP 1.5 (1.6 optional)	2022
	WB Smart	OCPP1.2, OCPP1.5	2022
	WB Smart	OCPP1.2, OCPP1.5	2022
Compleo Charging Solutions	Compleo SOLO smart	OCPP 1.6	2022
	Compleo SOLO advanced	OCPP 1.6	2022
	Compleo SOLO premiumline	OCPP 1.6, ISO 15118 ready	2022
Compleo Connect GmbH	Compleo ECO s	Modbus TCP	2022
	Compleo Pro	Modbus TCP, OCPP 1.6	2022
	Compleo PRO erk	Modbus TCP, OCPP 1.6	2022
	Compleo PRO plus	Modbus TCP, OCPP 1.6	2022
Delta Electronics	AC Mini Plus	OCPP1.5, OCPP1.6	2022
	AC MAX	OCPP1.5, OCPP1.6, OCPP2.0, ICO 15118 ready	2022
E3/DC	Wallbox easy connect	Modbus TCP	2022
Easee	Home / Charge	OCPP1.6	2022
eCharge Hardy Barth	cPμ2 Charger	OCPP1.6	2022
	cPH2 Charger	OCPP1.6	2022
ecotap	Homebox	OCPP1.6	2022
	Wandcharger Duo	OCPP1.6	2022
elexon GmbH	elexon A1	OCPP1.6, OCPP2.0	2022
	elexon A1	OCPP1.6, OCPP2.0	2022