Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure

Erdem Gumrukcu
Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
erdem.guemruekcue@eonerc.rwth-aachen.de

Ali Arsalan
Automotive Engineering Department
Clemson University
Clemson, South Carolina
USA
aarsala@clemson.edu

Grace Muriithi
Automotive Engineering Department
Clemson University
Clemson, South Carolina,
USA
gmuriit@clemson.edu

Charukeshi Joglekar[1,2]
[1]Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
[2]Department of Digital Energy,
Fraunhofer Institute for Applied Information Technology, 52074
Aachen, Germany
charukeshi.joglekar@eonerc.rwth-aachen.de

Ahmed Aboulebdeh
Electrical and Electronics Engineering
Marmara University
Istanbul, Turkey
a_d_2999@hotmail.com

Mustafa Alparslan Zehir
Electrical and Electronics Engineering
Marmara University
Istanbul, Turkey
alparslan.zehir@marmara.edu.tr

Behnaz Papari
Automotive Engineering and Holcombe Department of Electrical and Computer Engineering
Clemson University
South Carolina, USA
bpapari@clemson.edu

Antonello Monti[1,2]
[1]Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
[2]Department of Digital Energy,
Fraunhofer Institute for Applied Information Technology, 52074
Aachen, Germany
amonti@eonerc.rwth-aachen.de

2022 4th Global Power, Energy and Communication Conference (GPECOM) | 978-1-6654-6925-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/GPECOM55404.2022.9815727

***Abstract*—Expanding adoption of electric vehicles (EVs) and broad deployment of charging stations push the limits of distribution grid infrastructure and increase the importance of effective charging coordination. Smart EV chargers with several functionalities and charging coordination solutions that can manage the charging sessions of hundreds of EVs are becoming common, with the increasing risk of triggering significant operational problems in case of cyberattacks. The information exchange between the charging coordinator, distribution network operator, and users is essential in the scheduling of a large number of charging sessions, relying on customer preferences, without violating operational grid constraints. Both the user mobile apps used for charging session reservations and DSO-charging coordinator interfaces are vulnerable to cyberattacks which may cause considerable technical and economic consequences. An important concern is the potential impacts of attacks when a single node or communication link is compromised. This study investigates the impacts of false data injection (FDI) and hijacking attacks on EV charging coordination in case of a single point of failure. Hijacking of one user's mobile app and FDI attack on the DSO-charging coordinator interface are investigated by simulating a 24-hour scenario with 12 chargers, 34 realistic charging sessions, and an EV charging coordination approach based on each session's tolerance to delays. The study highlighted considerable negative impacts that could be encountered in case of a single point of failure in EV charging coordination.**

Keywords—cybersecurity, electric vehicle charging, energy management, false data injection, hijacking.

I. INTRODUCTION

In order to reduce carbon emissions, the automobile industry is beginning to shift away from internal combustion engine vehicles (ICEVs) to electric vehicles (EVs). In 2020, despite pandemic challenges, the market has grown by 41% with record-breaking annual sales, exceeding 3 million. In 2021 with arising supply challenges in the industry, annual electric car sales more than doubled to 6.6 million, reaching around 9% of the global car market and more than tripling market share compared to 2019 [1]- [2]. Until 2030, 130 to 250 million EVs are expected to be on roads. As of March 2022, there are 188 available models on the road and 36 announced models upcoming in the near future [3]. Battery capacities of the available EVs range from 16.7 to over 100 kWh providing a driving range from 95 to 640 km [3]. By ever increasing demand for the EV infrastructure, an appropriate secure control and management system is required to fulfill the goals for resilient smart cities.

EV chargers are being equipped with smart functionalities, ranging from individual charging power level adjustment to overall charging power-sharing among a group of chargers, bidirectional power exchange for V2G services to distributed generation from renewables-following charging, tariff-based charging, and many other [4]. Moreover, the user mobile apps have several availabilities such as charging management, scheduling, monitoring, and real-time statistics to provide more flexibility to EV users [5]. Furthermore, there are emerging charging coordination solutions that can manage the charging sessions of up to 1000 EVs on-premise [6].

978-1-6654-6925-8/22/$31.00 ©2022 IEEE

Thus, the nexus of EVs, electric vehicle supply equipment (EVSE) flexibility, smart meters, and the power grid creates complex cyber-physical interdependencies [7]. This increasing penetration of IoT-based Electric Vehicle (EV) infrastructure in a smart grid network makes it more vulnerable to cyber-related threats as compared to traditional vehicles. As these systems get more complex and interconnected, malicious intruders develop increasingly sophisticated techniques of breaking into the cyber-physical system. False data injection attacks (FDIAs) [8], denial of service (DoS) [9], controller hijacking [10], replay attacks, stealthy attacks [11], and other methods of circumventing cyber-physical system (CPS) security mechanisms are among the most common types. Such attacks are capable of wreaking havoc on network stability and control architecture. Several cyber-physical attacks have been documented in the past, posing a serious threat to the control centers. Without requiring a physical attack, an attack on energy systems monitored and controlled by an external entity can severely impact the system's processes by gaining targeted access through the supervisory control and data acquisition (SCADA) system [12].

An EV under cyber/physical attack can pose a significant risk to the driver, (EVSE), other EVs, the utility grid, and specially in-vehicle electronic systems. Even a single compromised vehicle can cause widespread cyber-attack propagation in an IoT-enabled EV network as demonstrated in [13]. IoT layers of intelligent transport systems are described in details, ranging from live traffic to driving information, membership service to traffic information, parking service to vehicle insurance and service violations in [14]. In [15] a remote hijacking attack via a cybersecurity breach in critical system controls due to software deficiencies on a Cherokee Jeep being driven on the highway is demonstrated. A similar attack on a Tesla vehicle was reported in [16], where the vehicle was hacked by researchers through a cellular connection and Wi-Fi. Therefore, to improve the robustness and dependability of the cyber-physical system (CPS), it is critical to conduct a holistic analysis of its security. The North American Electric Reliability Corporation (NERC) established the Critical Infrastructure Protection (CIP) 002-009 standard, to assure the safe and dependable operation of the power grid [17]. Similarly, the IEC 62351 standard for the cybersecurity of industrial communication protocols was produced by the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 [18]. Network (cyber) security measures alone cannot ensure the secure operation of the entire system, which leads to cyber-physical security. The protection of the distribution grid with extensive penetration can only be ensured by detecting and mitigating cyber-attacks.

Ref [19] conducted a systematic evaluation of long-term complex attacks in hybrid electric vehicles (HEVs). A probability-based detection model was developed to improve the cybersecurity of the HEVs. Authors in [20] studied a cyber-threat evaluation for a Level 2 AC-powered EVSE. Due to the bidirectional connectivity between electric car chargers and external devices, the stations meant for public usage are intrinsically vulnerable to cyber threats [21]. Furthermore, one of the conceivable attack scenarios is the infection of the electric vehicle supply equipment (EVSE) controller and the central management system via the data connection buses with unwanted malware or viruses. Both the software and hardware can potentially be harmed because of malware assaults, and the EVSE can be easily disrupted by assessing the station through the communication network or physically by using the universal serial bus (USB) to inject malware.

Considering the vulnerability of EV power electronic systems with a specific focus on lateral stability control system (LSCS) and motor drives, a coordinated detection approach and performance degradation evaluation metrics has been presented in [22]. A distributed control system is utilized in [23] as a viable solution to counter cyber-attacks as compared to a centralized approach and a distributed blockchain for sensitive data integrity and safety. For secure energy trading between smart grid and EV infrastructure, a software-defined networking (SDN) model along with distributed ledger-based BC is utilized in [24]. In [25] a backpropagation-based artificial neural network is proposed to predict the SoC (state of charge) of EV in the normal or compromised scenarios to detect an FDI attack on the battery management system (BMS). Authors in [26], have investigated the security of the EVSEs and smart card payment processes to verify users; nonetheless, smart credit cards could be used by unauthorized persons if they are lost. In [27], Joseph et al. examined the impact of EV charging station risks on grid operations and classified cyber-attacks connected to the charging system for mitigating those attacks. Authors in [28] proposed a hidden Markov model for formulating cyber-attacks in extreme fast-charging stations to further understand and deploy the appropriate mechanism against such attack vectors. The results achieved indicate that the proposed method improved the overall charging efficiency and cyber-physical security.

The stages of malware-based cyber-attacks are mainly categorized as discovery, propagation, access, control, infection, and trigger, leading to the active attack stage aiming disruption, destruction, theft, extortion, or repurpose. The majority of the studies in the literature focus on the discovery and access stages. The reconnaissance attacks are based on collecting screenshots of controllable assets details, control screens, and monitoring the commands and messages exchanged through the communication channels to prepare for sophisticated actual active attacks in the future. There is alack of studies on analyzing the impacts of active attacks. The studies in the literature have not investigated the possible impacts of attacks on single points in EV charging coordination systems. Single point of failure (SPOF) is a useful concept to find out the critical vulnerabilities of cyber-physical systems. It is not only used in studies on communication and control system operational failures, but also in cybersecurity studies. In communication studies, it is considered as a critical point, if fails that cause the entire system failure. In the scope of this study, from the perspective of cybersecurity of electric vehicle charging coordination, it is used to describe a single user mobile app or a communication link between charging cluster operator and a stakeholder, if compromised will cause the related operational service

(meeting a target SoC level by the end of charging, keeping aggregate power demand below a DSO specified threshold and other) to fail. There are several simplifications and assumptions commonly preferred for EV charging profiles and coordination mechanisms, conflicting with field deployments. So, there is a need to adopt more detailed, realistic, and closer to field modeling and coordination approaches in EV charging cybersecurity studies.

This study contributes to the literature by investigating the impacts of attacks on EV charging coordination in case of a single point of failure (SPOF). In a daily scenario with high resolution, realistic, EV charging profiles, related user preferences, and an EV charging coordination algorithm that prioritize conflicting charging sessions based on shifting availabilities, the impacts of hijacking of a user's mobile app and FDI attack on the communication link between the DSO and charging cluster operator (CCO) are analyzed. Section 2 explains the EV charging modeling and EV charging coordination approaches developed and cyberattack modelling approaches adopted and adapted by the authors. Section 3 presents the case study and provides the results of the analysis. Section 4 concludes the paper by summarizing findings and providing future research directions.

II. METHODOLOGY

The methodology followed in this study consists of stochastic generation of daily charging profiles for a determined number of EVs. Moreover, the charging preferences of EV owners, an aggregated EV charging coordination approach, and cyberattacks are modeled along with the impact analysis of EVs and EV charging infrastructure to demonstrate the superiority of the proposed approach. This section describes each of the three main stages of the followed methodology under dedicated subsections.

A. Stochastic Daily EV Charging Profile Generation and EV Owner Preferences Modelling

In majority of studies, electric vehicle charging behavior is modeled by considerably sacrificing from reality due to oversimplification and very generalized assumptions. In aggregated charging analysis, the individual details of each EV are usually not considered. In field pilots, mostly a limited variety of EV brands and models are used by a specific customer segment for a short time period. New charging methods emerge, and the charging power and energy storage capability of EVs increase; but these changes are not satisfactorily reflected in analyses.

One of the common assumptions in the literature is consideration of EV charging sessions in particular time periods of a day. On the other hand, field pilots proved that EV charging takes place at any time periodhija in a day based on different probabilities [29]. Another wide assumption present in the literature is reaching to full SoC level by the end of every charging session, while in the field demonstration, 30 to 50% of the customers interrupt charging activities and start their trips with 50 to 90% SoC levels. Contrary to studies that consider single charging throughout a day, 20% of the customers is observed to be charging twice daily. Another common assumption is consideration of same or a limited range of initial SoC levels in the beginning of charging events, while in reality EVs start charging with any initial SoC level inside their operational range with 9 to 13% probability. The inconsistencies between the common assumptions in the literature and the field applications require adoption of more detailed approaches in modelling daily EV charging behavior, utilizing realistic statistics and probabilities.

Contrary to the simplifications summarized in the previous paragraph, there are several real measurement data and detailed models about the individual charging behavior of EVs in reliable resources. Moreover, statistics are available in different resources about the technical parameters of EV brands and models, driving times, distances, parking times and charging habits [3]. In this study, a probabilistic charging profile generation methodology, which combines technical characteristics and field demonstration statistics from several resources is preferred. This methodology was formerly introduced in details in [30]. In the first stage, the main technical characteristics of the 23 cars available in the US market in the last ten years are obtained from [3] and [31] . Type-2 charging power (in kW), full charging time (in minutes), battery energy storage capacity (in kWh), and energy consumption per km (in Wh/km) specific for each car model are considered. The charging power of the considered cars range from 3.6 to 16.5 kW, while battery energy storage capacity is from 16 to 95 kWh and full charging time is from 3 to 14 hours. Based on the specified number of EVs in a scenario, a random cluster of cars is assigned to each customer.

In the next step, probabilities for charging session starting time and initial SoC levels from [29] are used to stochastically specify the charging starting time and initial SoC level for each single charging session. After that, final SoC level higher than the assigned initial SoC level is specified per charging session using the probabilities from the same source [29]. Based on the charging starting time, initial SoC and final SoC, charging power and battery energy storage capacity parameters, the charging ending time is derived per charging session. Considering idle waiting, parking times spent after charging available in the literature, additional parking times up to charging duration per charging session are stochastically assigned. This information is used by the EV charging coordination algorithm explained in the next subsection to shift some of the simultaneous charging sessions based on the priorities and urgencies.

B. EV Charging Coordination Approach

Coordinated EV charging is the key enabler for optimized operation under load simultaneity constraints. In various domains, different agents such as charging station operators, microgrid operators, and aggregators can be responsible for charging coordination. For the sake of generality, an agent that is responsible for a cluster of EVSEs is referred to as charger cluster operator (CCO) in this work. This study considers a charging coordination strategy based on least-laxity-first (LLF) concept, which, in essence, sorts the EV(s) with respect to their tolerance for delayed charging completion and prioritizes the ones that have least tolerance (laxity) when the aggregate consumption of a charger cluster must be limited.

The tolerance is determined by the amount of charging demand and minimum time required for transferring this energy to the EV battery. With v representing a particular EV, the tolerance of the EV for delayed charging at a given time t, $m_v(t)$, is calculated in equations (1) and (2).

$$m_v(t) = \frac{D_v - t - \underline{T_v}(t)}{D_v - t} \quad (1)$$

$$\underline{T_v}(t) = \frac{(S_v^* - s_v(t)).E_v}{P_v} \quad (2)$$

In above equations, S_v^* is the target SoC specified by the driver, D_v the estimated departure time –in other words the deadline for charging completion-, and E_v the battery capacity of v. Equation (2) calculates, $\underline{T_v}(t)$, the minimum time required for transferring the remaining charging demand –set forth by the difference between target and actual SoCs, respectively S_v^* and $s_v(t)$. $\underline{T_v}(t)$ depends also on P_v, the power rating of the EVSE that v is connected to. The larger values of $\underline{T_v}(t)$ indicate the need for longer times for completing the charging and thus, the smaller $m_v(t)$, for delayed charging.

The considered algorithm is executed in three steps $k = \{0,1,2\}$. In each step, the aggregate power consumption of the controlled EVSEs, $p^{\Sigma,k}$ is compared with the given real-time power constraint of the CCO, P^{Σ}. If $p^{\Sigma,k}$ occurs to be smaller than or equal to P^{Σ} at any k, i.e. $p^{\Sigma,k} \leq P^{\Sigma}$, this means that no further adjustment is required and thus the execution is stopped. The step-wise structure of the algorithm is designed to use the flexibility from the least possible number of EV and avoid discharging EV batteries as long as possible.

In the initialization step ($k = 0$), all EVs connected to the EVSEs under the control of the CCO are assigned with the maximum power rating such that $p_v^{k=0} = P_v$. When the aggregate consumption calculated in the initial step indicates a violation, i.e. $p^{\Sigma,0} - P^{\Sigma} = \Delta^0 > 0$, then the EVs are sorted with respect to $m_v(t)$ in descending order. Step 1 ($k = 1$) Iterates over EVs –starting from the v with largest m_v- and aims to remove the violation by reducing the (temporary) set point of the corresponding v to zero, i.e. $p_v^{k=1} = 0$. If the aggregate consumption calculated after finishing the loop in the first step of $p^{\Sigma,1} = \sum_v p_v^{k=1}$ is still larger than P^{Σ} i.e. $p^{\Sigma,1} - P^{\Sigma} = \Delta^1 > 0$, the process is repeated in Step 2 but reducing the temporary set points to the negative values such that $p_v^{k=2} = -P_v$ when necessary. It is important to note that the negative flexibility is only available for bidirectional EVSEs.

C. Hijacking and FDI Attacks Modelling

Two types of cyberattacks are considered in the scope of this study: 1) Hijacking (HIJ) and 2) False Data Injection (FDI). The cyberattacks are modelled based on the methods suggested in [10] and [32]. The HIJ attacks are modeled to emulate the scenario in which the user mobile app for reserving charging sessions and providing customer preferences is infected.

The customer provides a target SoC and a departure time which may be relatively longer than the time needed to reach the desired SoC, which may be used for further charging to reach even higher SoC levels or just idle parking. In the scope of this study, due to a HIJ attack, the attacker able to corrupt the departure time communicated by the EV user to the CCO, affecting EV charging coordinator priorities and delaying decisions. The attack is formulated as represented in equation (3).

$$D_{vi}^{'} = (1 - \eta_{vi}).D_{vi} + \eta_{vi}.D_v^C \quad (3)$$

In (3), $D_{vi}^{'}$ stands for the corrupted departure time information for the vehicle v for the charging session i, while D_{vi} is the original uncorrupted data and $\eta_{vi} \in \{0,1\}$ defines if an attack has occurred on the related vehicles' driver mobile app used for providing the charging preferences for the charging session i. FDI is modelled by corrupting the aggregated demand constraint specified by the DSO. The attack is formulated as represented in equation (4).

$$P_j^{'} = P_j + \eta_j.F_j \quad (4)$$

In (4), $P_j^{'}$ is the corrupted aggregate power demand constraint for the time j, communicated between the DSO and the CCO, while P_j is the original uncorrupted data. $\eta_j \in \{0,1\}$ denotes an attack has occurred and F_j is the false data injected in the communication link between the DSO and the CCO in the cyber-physical system.

The diagram of the proposed methodology is depicted in Fig. 1.

III. Case Study

This part investigates the possible impacts of two types of cyberattacks on the consumption profile of an EV charger cluster: (i) hijacking targeting customer mobile app and (ii) FDI targeting the communication link between the DSO and the CCO. The considered scenario was generated by using the methodology explained in Section 2-A and considering the characteristic parameters of the 23 EV models available in the US market in the last ten years. Numerical simulations were performed –with 1-minute resolution in the daily operation- to investigate the charging behaviors under the defined cyber-attack scenarios. For the simulations, the Python-based electro-mobility simulator developed by the RWTH Aachen University was used. The mentioned software is based on the object-oriented modeling approach introduced in [33]. For this paper, additional capabilities were added in the mentioned software to incorporate cyberattack scenarios.

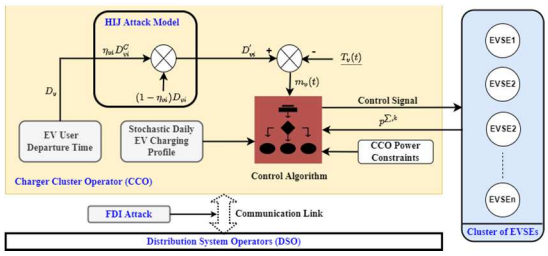

Fig. 1. The proposed diagram of EV charging coordination associated with cyber/physical attcaks

A. *Cyberattack scenario 1: Hijacking customer app*

In this scenario, (upon DSO request) the CCO is obliged to limit its power consumption by 30% of the installed capacity of the 12 available EV chargers throughout the simulated period (i.e., $P^{\Sigma} = 30\% \cdot 11 \cdot 12\ kW$). Due to the pronounced peak power limit, 11 kWh of the overall charging demand remains unfulfilled in the no-attack scenario. This study aims to investigate how a hijacking attack affects the demand fulfillment in the operation. In the considered cyberattack scenario, an attacker hijacks one of the EV user's mobile app and modifies the charging demand specifications of the user. The corrupted departure time information indicates a parking duration that is 50% less of the real estimation of the EV user, being 3 hours 51 minutes instead of 7 hours 42 minutes. In this way, the attacker misleads the CCO about the urgency of the charging demand of this particular EV and consequently, the CCO assigns a higher priority value (m_v) to this EV.

The cumulative energy supply of the CCO in two cases - without versus with hijacking- are plotted in Fig. 3. The graph shows that the energy that the system supplies in identical periods decreases when only one of the EV user's app is hijacked. In practice, assigning higher m_v to an EV affects how the available capacity is allocated to all EVs in the system. Therefore, the CCO postpones some other charging sessions while prioritizing the session of the EV whose departure time estimation is modified by the attacker. The results show that the change in prioritization due to hijacking results in that 9 EVs leaving their charging station with SoC levels lower than their targets and the unfulfilled demand increases by around 100%.

B. *Cyberattack scenario 2: FDI attack on the DSO-CCO interface*

This scenario assumes that the DSO is entitled to assign an aggregate power consumption constraint to the CCO in the range of 40%-60% of the total installed capacity of the EV chargers. This test aims to show how an FDI attack would affect the power consumption profile of the charger cluster. In the tested scenario, the DSO constraint is 60% ($P^{\Sigma} = 66\ kW$) before 18:00. However, due to a congestion in the upstream network, the DSO requests a further reduction to 42% ($P^{\Sigma} = 51.7\ kW$) for 18:00 to 22:00.

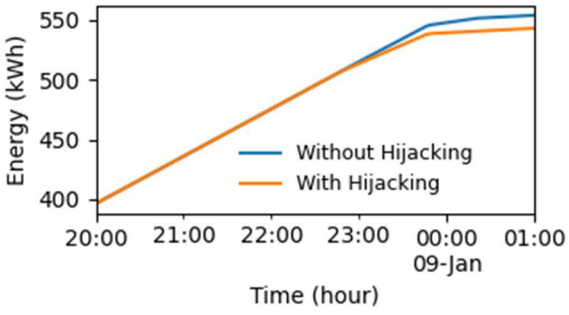

Fig. 2. Cumulative energy supplied by the CCO to the EVs without/with hijacking

In the FDI scenario, the attacker injects false data into the communication channel between the DSO-CCO such that CCO still considers 66 kW as the peak demand constraint. The resulting power consumption profiles of the CCO under scenarios without and with FDI are plotted in Fig 4. The results show that the cluster's power consumption exceeds the DSO constraint by up to 11 kW from time to time. The extra energy consumed by violated peak threshold due to FDI attack in that period is found as 14 kWh. The business model between CCO-DSO and the impact of the altered consumption behavior on the power grid is not within the scope of this paper. However, it is safe to foresee that such a constraint violation obliges the CCOs to pay penalties and more importantly leads to grid congestion. Further research should be conducted to quantify the impact of the FDI attacks in terms of grid congestion and operational costs of the CCOs.

IV. Conclusion

This study analyzes the impacts of hijacking of EV owner mobile app to determine the departure time as well as FDI into the DSO-CCO interface for exchanging peak demand constraints on (SPOF). In the first explored scenario, among the simulated stochastic daily 34 EV charging profiles, compromise of one car owner's mobile app and intentional statement of an earlier departure time than reality caused considerable performance reduction in the charging service performance and led some other cars reaching their departure times with SoC less than the levels desired by their drivers. In the second investigated scenario, FDI into the interface between the DSO and CCO caused the violation of peak demand constraints by the CCO. A CCO that is capable of keeping the aggregate peak demand below the lowered threshold without the FDI attack, has been put into a position that is subject to a financial penalty and a higher possibility of triggering technical problems in the upstream network. They explored scenarios highlighted the vulnerability of EV charging coordination systems to cyberattacks even in the case of SPOF without requiring compromise of several devices and controllers.

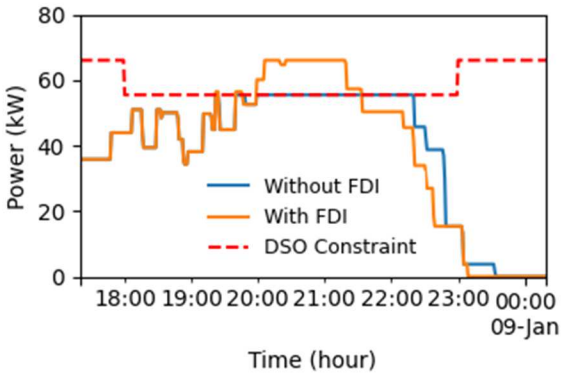

Fig. 3. Aggregate power consumption of the CCO without and with FDI

Future studies will cover different cyberattacks' impacts on EV charging systems, detection of attacks based on KPIs,

and MetaMetrics and prevention mechanisms to minimize the technical and financial losses in real-time.

ACKNOWLEDGMENT

This work was supported by the project ALigN, funded by the Federal Ministry for Economic Affairs and Energy of Germany (Grant Number:01MZ18006G). The authors assume full responsibility for the content of this work

REFERENCES

[1] IEA, "Global EV Outlook 2019: Scaling up the transition to electric mobility," 2019. [Online]. Available: http://webstore.iea.org/global-ev-outlook-2019.

[2] IEA, "Electric cars fend off supply challenges to more than double global sales," 2022. [Online]. Available: https://www.iea.org/commentaries/electric-cars-fend-off-supply-challenges-to-more-than-double-global-sales.

[3] EV-Database, "All electric vehicles," 2022. [Online]. Available: https://ev-database.org/.

[4] Wallbox, "Copper SB," 2022. [Online]. Available: https://wallbox.com/en_catalog/copper.

[5] Wallbox, "MyWallbox," 2022. [Online]. Available: https://wallbox.com/en_catalog/mywallbox.

[6] JET Charge, "Solutions: JET Charge CORE," [Online]. Available: https://jetcharge.com.au/solutions/core/. [Accessed 02 04 2022].

[7] S. Acharya, Y. Dvorkin, H. Pandžić and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access,* vol. 8, pp. 214434-214453, 2020.

[8] L. Guo, J. Ye and B. Yang, "Cyberattack Detection for Electric Vehicles Using Physics-Guided Machine Learning," *IEEE Transactions on Transportation Electrification,* vol. 7, pp. 2010-2022, 2020.

[9] K. Ding, X. Ren, D. E. Quevedo, S. Dey and L. Shi, "DoS attacks on remote state estimation with asymmetric information," *IEEE Transactions on Control of Network Systems,* vol. 6, pp. 653-666, 2018.

[10] S. Sahoo, J. C.-H. Peng, S. Mishra and T. Dragičević, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Transactions on Power Electronics,* vol. 35, pp. 7574-7582, 2019.

[11] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan and W. Song, "Cyber--Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges, and Future Visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics,* vol. 9, pp. 4639-4657, 2020.

[12] C.-W. Ten, C.-C. Liu and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems,* vol. 23, pp. 1836-1846, 2008.

[13] S. Mousavian, M. Erol-Kantarci, L. Wu and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Transactions on Smart Grid,* vol. 9, pp. 6160-6169, 2017.

[14] M. Moazzami, N. Sheini-Shahvand, E. Kabalci, H. Shahinzadeh, Y. Kabalci and G. B. Gharehpetian, "Internet of Things Architecture for Intelligent Transportation Systems in a Smart City," in *2021 3rd Global Power, Energy and Communication Conference (GPECOM)*, 2021.

[15] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it," *Wired,* vol. 7, pp. 21-22, 2015.

[16] P. Panda, *Cyber attacks in connected cars: What tesla did differently to win,* Tech. Rep., Sep. 2017.[Online]. Available: https://www. appknox. com/blog …, 2017.

[17] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves and P. Verissimo, "The CRUTIAL way of critical infrastructure protection," *IEEE Security & Privacy,* vol. 6, pp. 44-51, 2008.

[18] J. Hong, R. Karnati, C.-W. Ten, S. Lee and S. Choi, "Implementation of Secure Sampled Value (SeSV) Messages in Substation Automation System," *IEEE Transactions on Power Delivery,* 2021.

[19] J. Y. a. L. D. L. Guo, "Cyber–Physical Security of Energy-Efficient Powertrain System in Hybrid Electric Vehicles Against Sophisticated Cyberattacks," *IEEE Transactions on Transportation Electrification,* vol. 7, pp. 636-648, 2021.

[20] S. Saadat, S. Maingot and S. Bahizad, "Electric Vehicle Charging Station Security Enhancement Measures," in *2020 5th IEEE Workshop on the Electronic Grid (eGRID)*, 2020.

[21] Y. Park, O. C. Onar and B. Ozpineci, "Potential cybersecurity issues of fast charging stations with quantitative severity analysis," in *2019 IEEE CyberPELS (CyberPELS)*, 2019.

[22] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives," *IEEE Transactions on Power Electronics,* vol. 36, pp. 4463-4477, 2020.

[23] V. Kamuni, U. Asfia, S. Sutavani, A. Sheikh and D. Patel, "Secure energy market against cyber attacks using blockchain," in *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2019.

[24] K. Kaur, G. Kaddoum and S. Zeadally, "Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, pp. 5178-5189, 2021.

[25] S. Rahman, H. Aburub, Y. Mekonnen and A. I. Sarwat, "A study of EV BMS cyber security based on neural network SOC prediction," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2018.

[26] C. Carryl, M. Ilyas, I. Mahgoub and M. Rathod, "The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, 2013.

[27] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah and C. Assi, "A detailed security assessment of the EV charging ecosystem," *IEEE Network,* vol. 34, pp. 200-207, 2020.

[28] M. Girdhar, J. Hong, H. Lee and T.-j. Song, "Hidden Markov Models based Anomaly Correlations for the Cyber-Physical Security of EV Charging Stations," *IEEE Transactions on Smart Grid,* 2021.

[29] J. Quiros-Tortos, L. Ochoa and T. Butler, "How electric vehicles and the grid work together: Lessons learned from one of the largest electric vehicle trials in the world," *IEEE Power and Energy Magazine,* vol. 16, p. 64–76, 2018.

[30] P. H. Hoang, G. Ozkan, P. R. Badr, B. Papari, C. S. Edrington, M. A. Zehir, B. Hayes, L. Mehigan, D. Al Kez and A. M. Foley, "A Dual Distributed Optimal Energy Management Method for Distribution Grids With Electric Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* 2021.

[31] Argonne National Laboratory, "Light Duty Electric Drive Vehicles Monthly Sales Updates," 2022. [Online]. Available: https://www.anl.gov/es/light-duty-electric-drive-vehicles-monthlysales-updates.

[32] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid,* vol. 9, p. 6731–6741, 2017.

[33] A. Yavuzer, E. Gümrükcü, M. A. Zehir and A. Monti, "Modeling for Cross-Domain Electromobility Simulations," in *PESS 2020; IEEE Power and Energy Student Summit*, 2020.