Proceedings Paper:
Yazdanipour, S., Arani, F.M. and Jahromi, A.A. (2024) Investigating Cyberattacks Against Off-Grid Solar-Powered Electric Vehicle Charging Stations. In: 2024 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). 2024 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 06-09 May 2024, Anaheim, CA, USA. Institute of Electrical and Electronics Engineers (IEEE). ISBN: 979-8-3503-1638-4. ISSN: 2160-8555. EISSN: 2160-8563.

https://doi.org/10.1109/td47997.2024.10556091

Investigating Cyberattacks Against Off-Grid Solar-Powered Electric Vehicle Charging Stations

Samaneh Yazdanipour and Mohammadreza F. M. Arani
Toronto Metropolitan University
Toronto, Canada
samaneh.yazdanipour@torontomu.ca, marani@torontomu.ca

Amir Abiri Jahromi
University of Leeds
Leeds, United Kingdom
a.abirijahromi@leeds.ac.uk

***Abstract*—The rapid installation of charging stations is imperative to facilitate the transition to decarbonization of the transport sector and cope with the booming sales of electric vehicles (EVs) in recent years. Yet, the installation of charging stations requires capital intensive and time-consuming network reinforcement investments. The installation of off-grid EV charging stations can be considered as a viable solution to address this challenge in locations where the electric grid is not nearby, or the required investments to upgrade the grid is expensive. Solar generation, a battery energy storage system (BESS) and an energy management system (EMS) can be incorporated into EV charging stations to realize off-grid solar-powered EV charging stations. The incorporation of solar generation, a BESS and an EMS transforms the EV charging station into a complex cyber-physical system which is prone to various cyberattacks. In this paper, we investigate vulnerability of off-grid solar-powered EV charging stations to cyberattacks. We demonstrate an attacker can compromise the measurements and control commands in an off-grid solar-powered EV charging station to force the charging station out of service.**

***Index Terms*—Cyber-physical security, off-grid EV charging stations, solar power and energy storage, resilience.**

I. Introduction

THE transport sector around the world is on the verge of significant transformation moving from fossil-fuel based transport toward electric transport to address global warming concerns and achieve ambitious decarbonization goals. Many countries have set various policies and regulations to gradually phase out fossil-fuel based vehicles over the next few decades [1], [2]. Yet, the range anxiety created by the scarcity of fast electric vehicle (EV) charging stations is considered as the main barrier in front of quick adoption of electric vehicles by public [3]. Another challenge is the need for capital intensive and time-consuming network reinforcement investments to accommodate fast EV charging stations which can quickly erode the compelling economics and motivations behind transport electrification and decarbonization [4].

Incorporating renewable energy resources and battery energy storage systems (BESS) into fast EV charging stations can be considered as a viable solution to postpone capital intensive and time-consuming network reinforcement investments and achieve decarbonization objectives [5]. In particular, off-grid renewable-powered EV charging stations are essential in remote locations where the electric grid is not nearby. At the same time, the existence of off-grid EV charging stations and EV charging stations with islanded mode of operation can contribute to diversifying EV charging stations and improving the resilience of EV charging infrastructure during blackouts. Nevertheless, cybersecurity can become the weakness of off-grid EV charging stations which requires further investigation.

EV charging stations are cyber-physical systems. The existence of various information and communication technologies, internet of things, and applications in EV charging stations creates various attack surfaces which can be exploited by cyberattackers [6]. For instance, the security weakness in the ChargePoint Home smart phone application of EV charging stations is revealed by Kaspersky Lab [7]. Considerable efforts have been undertaken in recent years by various institutions and government bodies to address the cybersecurity challenges of EV charging stations [8]. Yet, there is still inconsistency among manufacturers in implementing cybersecurity measures. This necessitates the careful examination of the cybersecurity of EV charging stations.

Cybersecurity of EV charging stations has been extensively investigated in the literature. A secure architecture based on defence-in-depth concept has been proposed in [9] for EV ecosystem which participates in demand-side management. A data-driven cyberattack strategy has been designed in [10] to target EV charging stations and cause frequency instability in a power system. In [11], a switching attack has been designed to cause inter-area instability in a power system. A method has also been proposed to detect and mitigate switching attacks against EV charging stations. A threat modelling framework based on STRIDE methodology has been presented in [12] for extreme fast EV charging stations. Furthermore, a detection and mitigation strategy has been proposed based on Hidden Markov Model. False data injection attacks and distributed denial of service attacks against 5G enabled remote Supervisory Control and Data Acquisition (SCADA) system of EV charging stations have been simulated in [13]. A machine learning-based intrusion detection system has also been proposed. The cybersecurity challenges of EV charging stations has been examined thoroughly in [14]. In [15], the effects of cyberattacks against EV charging stations on distribution networks have been investigated. Cyberattacks against residential loads and EV charging stations have been simulated and compared in [16]. In addition, two methods have been proposed to detect attacks against EV charging stations. The vulnerabilities of EV charging stations have been thoroughly investigated in [17] and mitigating countermeasures have been proposed. However, to the best of our knowledge, no prior work has investigated the cybersecurity of off-grid EV charging stations.

In this paper, we examine cyberattacks against measurements and control commands in the energy management system and DC link voltage regulating mechanism of off-grid solar-powered EV charging stations. We demonstrate that false data injection (FDI) attacks and denial of service (DoS) attacks can be used by cyberattackers to force the off-grid solar-powered EV charging station out of service. The main

contributions of this paper are as follows:

- Cybersecurity of off-grid solar-powered EV charging stations is examined for the first time.
- Various cyberattacks are simulated against measurements and control commands in energy management system and DC link voltage regulating mechanism of off-grid solar-powered EV charging station and their impacts are demonstrated.

The remainder of the paper is organized as follows. Section II presents the threat model against off-grid solar-powered charging station. The simulation results are provided in Section III before concluding the paper in Section IV.

II. Threat Model

Availability, integrity and confidentiality form the pillars of cybersecurity in cyber-physical systems like off-grid solar-powered EV charging stations. Availability is concerned with the timely delivery of signals to the legitimate devices. Integrity is focused on the authenticity and accuracy of signals. Confidentiality is about protecting signals from unauthorized access. A breach of confidentiality does not have disruptive consequences for off-grid solar-powered EV charging stations, but it can assist cyberattackers to successfully implement attacks on the availability and integrity of signals. This is while attacks on the availability and integrity of signals can cause disruptive consequences for off-grid solar-powered EV charging stations. As such, we focus on the attacks against the availability and integrity of signals in off-grid solar-powered EV charging stations in this paper.

Figure 1 illustrates the cyber and physical elements in off-grid solar-powered EV charging stations and the associated security reference architecture [18]. The physical elements in an off-grid solar-powered charging station include EV chargers, solar units, BESS, and dump loads. The cyber elements of the station consist of several layers which connect measurement instruments, actuators, protection relays, controllers and an energy management system as illustrated in Fig. 1. It is worth noting that the DC link voltage is regulated using the BESS in this paper. Despite the straightforward nature of this control mechanism, it creates the possibility of considering the BESS and battery management system as the single point of failure for off-grid solar-powered charging stations. It is possible to implement a distributed control mechanism for regulating the DC link voltage by considering the contribution of solar generation. The use of distributed control mechanism for DC link voltage regulation may increase the resilience of off-grid solar-powered charging stations, but this control mechanism is beyond the scope of this paper.

Cyberattacks targeting the communication network between EV chargers and EV charging management system (EV-CMS) have been investigated in the literature [6]–[17]. In this paper, we focus on the attacks targeting the communication network between the energy management system and different elements of the solar-powered EV charging station including solar management system, EV charging management system, BESS and dump load as illustrated in Fig. 2. We also consider the communication network between the battery energy management system and measurement instruments of the DC link. Various employees in off-grid solar-powered charging stations have access to these communication networks and measurement instruments. Therefore, the attacker can recruit a disgruntled employee or use stolen keys and credentials of employees to

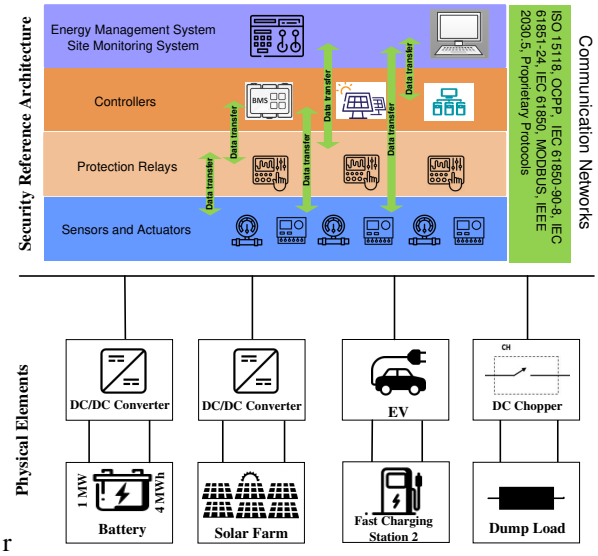

Fig. 1. Cyber-physical elements in off-grid solar-powered EV charging stations.

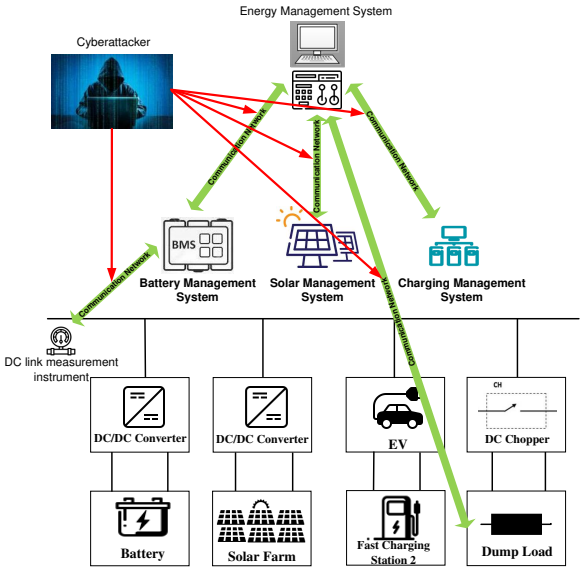

Fig. 2. Attack vectors against off-grid solar-powered EV charging station.

access the communication network of the energy management system and measurement instruments to implement the attack.

Cyberattackers can implement various attacks against the communication networks and measurement instruments of off-grid solar-powered EV charging stations including denial of service attack, and false data injection attack. The objective of the attacker is to force the charging station out of service. This objective can be accomplished by forcing the DC link voltage out of its normal operating limits and triggering the protection of the DC link. The significance of this attack is that it can simultaneously take all the fast EV chargers out of service. This attack can have serious implications for transport sector. In particular, the attack can cause disruptions in electric transportation during blackouts and in remote areas where there is a scarcity of EV charging stations.

III. Simulation Results

Two classes of attacks are conducted in this section using MATLAB/Simulink to demonstrate the vulnerability of off-grid solar-powered EV charging stations to cyberattacks. The

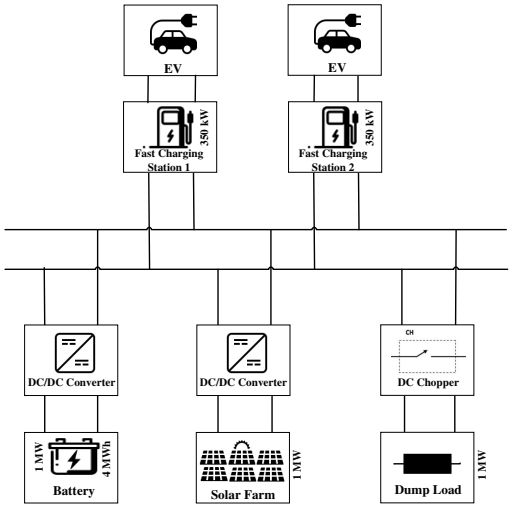

Fig. 3. Study system of the off-grid solar-powered EV charging station

first class of attack employs control commands from the energy management system to different components of the off-grid solar-powered EV charging station. This class of attack is called a control-related attack. The second class of attack targets the measurements in the off-grid solar-powered EV charging station. This class of attack forces the energy management system or local controllers to make incorrect decisions.

The test system considered in this paper for the off-grid solar-powered EV charging station is illustrated in Fig. 3. The charging station includes two 350 kW fast charging stations, a 1-MW solar farm, a 1-MW, 4-MWh battery energy storage system and a 1-MW dump load. The battery energy storage system regulates the DC link voltage. The dump load is a controllable DC chopper used to avoid overcharging of the battery during the abundance of solar power and in the absence of charging EVs.

A. Control-Related Attacks Against off-grid Solar-Powered EV Charging Stations

Three different attack scenarios are conducted here to demonstrate the vulnerability of off-grid solar-powered EV charging stations to control-related attacks.

In the first scenario, we consider an operating state of the off-grid solar-powered EV charging stations where the dump load is activated to consume extra solar power generation. This operating state commonly occurs when the BESS is close to its maximum charging state and there is no EV charging. It is worth noting that the attacker needs to eavesdrop the communication network between energy management system and other components of the off-grid solar-powered EV charging stations to detect this operating state and right time to implement the attack.

The attacker sends a falsified command to phase out the dump load by compromising its communication network to the energy management system. The attack forces the battery management system to disable the DC link voltage regulating function to protect the battery from overcharging. The battery state of charge (SoC), the active power of the battery and the DC link voltage during the attack are illustrated in Fig. 4. As shown in Fig. 4, the voltage deviation of DC link forces the off-grid solar-powered EV charging stations out of service by triggering protection relays.

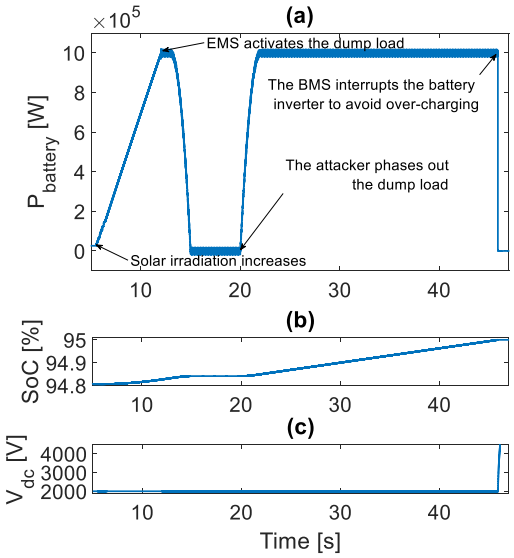

Fig. 4. Scenario 1 of the control-related attacks: a falsified control command is sent to phase out the dump load. (a) Output power of the BESS. (b) SoC of the BESS. (c) Voltage of the DC link.

In the second scenario, we consider an operating state of the off-grid solar-powered EV charging stations where the state of charge of battery energy storage system is low. However, there is enough solar generation to cover the EV charging load and charge the battery energy storage system. This operating state commonly occurs when there is high charging demand during a day. Similar to the first case, the attacker needs to eavesdrop the communication network between the energy management system and other components of the off-grid solar-powered EV charging stations to detect this operating state and right time to implement the attack.

The attacker sends a falsified command to curtail the solar generation. To maintain the health of the battery, the battery energy management system disables the DC link voltage regulating function which results in large DC link voltage deviation. The battery state of charge, the active power of the battery and DC link voltage during the attack are illustrated in Fig. 5. As shown in Fig. 5, the voltage deviation of DC link forces the off-grid solar-powered EV charging stations out of service.

In the third scenario, we consider an operating state of the off-grid solar-powered EV charging stations where there is a shortage of solar generation and a high EV charging demand. However, the battery energy storage system has enough charging to serve the EV charging load. This operating state commonly occurs in mornings, evenings and during nights or cloudy days.

The attacker sends a falsified command to activate the dump load. The rating of the inverter of the battery energy storage system is not enough to simultaneously satisfy the demand of EV chargers and the dump load. As a result, a power imbalance in the DC link occurs which depletes the DC link capacitor. It is worth noting that in the absence of an attack the dump load and EV chargers would never become active simultaneously during the shortage of solar generation. Therefore, the rating of the inverter of the battery energy storage will not be designed for this scenario in practice.

The active power of the battery and DC link voltage during the attack are illustrated in Fig. 6. As illustrated in Fig. 6, the

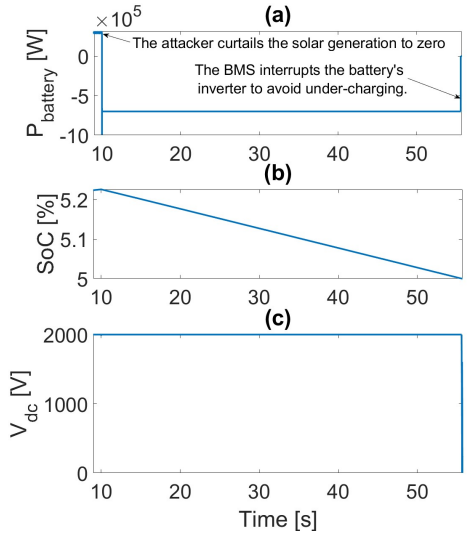

Fig. 5. Scenario 2 of the control-related attacks: a falsified control command is sent to curtail the solar generation. (a) Output power of the BESS. (b) SoC of the BESS. (c) Voltage of the DC link.

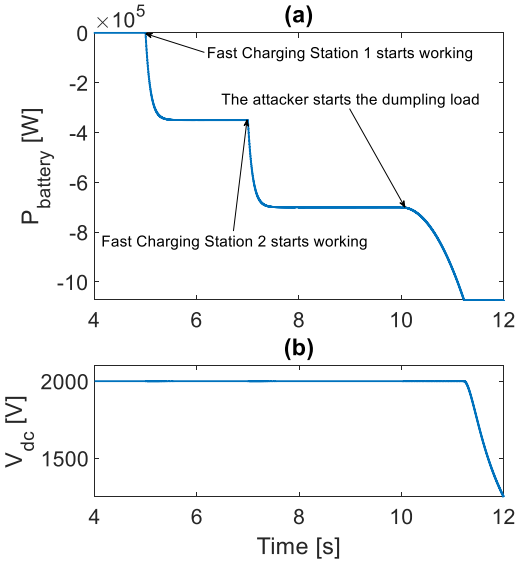

Fig. 6. Scenario 3 of the control-related attacks: a falsified control command is sent to activate the dump load. (a) Output power of the BESS. (b) Voltage of the DC link.

voltage collapse of DC link forces the off-grid solar-powered EV charging stations out of service. In contrast to the first and second scenarios, the success of this attack is not dependent on the state of charge of the battery because the battery has enough energy, but the power rating of the inverter of the battery is not enough to satisfy the demand.

The control-related attacks can be mitigated using various authentication methods. However, in the absence of authentication, a physics aware intrusion detection system is required to detect and mitigate control-related attacks. Nevertheless, this is out of the scope of the present paper and will be investigated in our future research.

B. Attacks Against Measurements in off-grid Solar-Powered EV Charging Stations

Two different attack scenarios are conducted here to demonstrate the vulnerability of off-grid solar-powered EV charging stations to attacks against measurements.

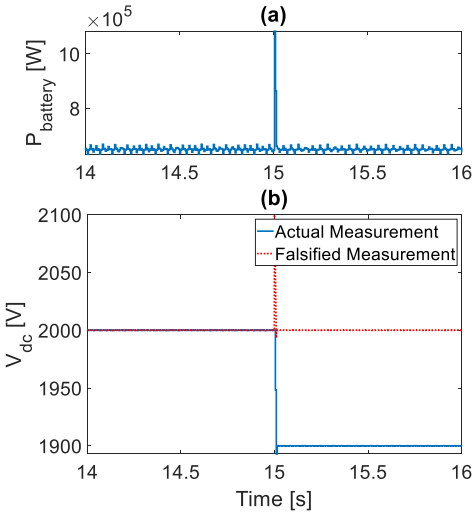

Fig. 7. Scenario 1 of the FDI attacks against measurements: a constant value has been added to the voltage measurements of the DC link. (a) Output power of the BESS. (b) Actual and falsified voltage of the DC link.

In the first scenario, the DC link voltage measurements sent to the battery management system are falsified to manipulate the DC link voltage regulation function. The manipulation of the voltage regulation function results in the DC link voltage deviation from the normal operating range and activation of protection relays.

The DC link voltage measurements can be falsified to indicate higher or lower values with respect to the actual value. We first consider a case where the attack starts at 15 seconds by adding a constant value to the voltage measurement of the DC link. The actual and falsified DC link voltage measurements and the output power of the battery energy storage system are illustrated in Fig. 7. As shown in Fig. 7, the battery management system will reduce the DC link voltage level which triggers the protection relays. Instead of adding a constant value, the attacker can subtract a constant value from the DC link voltage measurement as illustrated in Fig. 8. In this case, the battery management system will increase the DC link voltage level which triggers the protection relays.

In the second scenario, the attacker delays the delivery of the DC link voltage measurements, for example for 2 seconds, by using a denial of service attack. The delay introduced by the denial of service attack destabilizes the control mechanism of the DC link voltage regulation. The DC link voltage and the output power of the battery energy storage system are illustrated in Fig. 9.

It is worth noting that the measurements from different components of the off-grid solar-powered EV charging station can further be manipulated by the attacker to force the energy management system to make incorrect decisions. For instance, an attack can be implemented when the dump load is activated to consume extra solar power generation in the off-grid solar-powered EV charging station. In this case, the attacker falsifies the measurements from the solar unit indicating that solar power generation output has dropped. As such, the energy management system incorrectly phases out the dump load. Consequently, the battery energy storage system may disable the DC link voltage regulating function to protect the battery from overcharging. The outcome of this scenario is similar to the first scenario described in Section III. A. The difference is

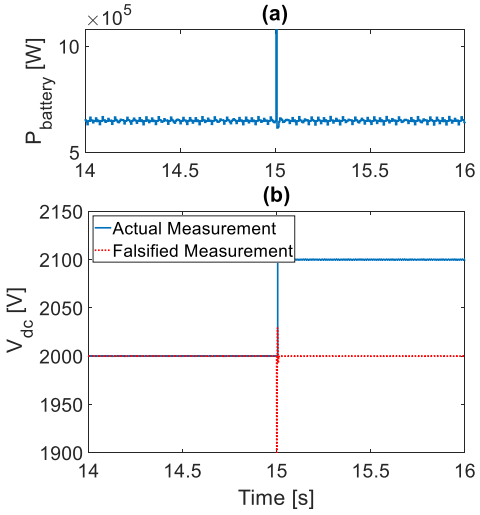

Fig. 8. Scenario 1 of the FDI attacks against measurements: a constant value has been subtracted from the voltage measurements of the DC link. (a) Output power of the BESS. (b) Actual and falsified voltage of the DC link.

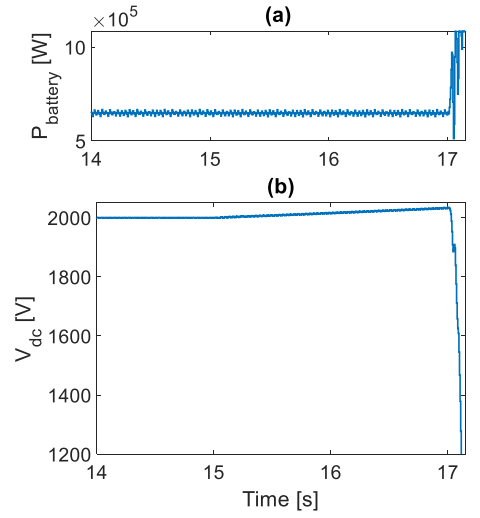

Fig. 9. Scenario 2 of the attacks against measurements: a denial of service attack is implemented against the voltage measurements of the DC link. (a) Output power of the BESS. (b) Voltage of the DC link.

that it is implemented using falsified measurements rather than falsified commands. The second and third scenarios in Section III. A can also be reproduced using the falsified measurements, but we do not explain these scenarios for the sake of brevity.

Although control-related attacks and attacks against measurements may result to similar outcomes, different mitigating methods are required to address these attacks. In contrast to control-related attacks, it is more difficult to use authentication or encryption for measurements due to their higher transmission rates. The observer-based methods are more apt for detection and mitigation of attacks against measurements. Again, this is out of the scope of present paper and the mitigation strategies will be pursued in our future research.

IV. Conclusion

This paper presented various cyberattack scenarios against the energy management system and DC link voltage regulating mechanism of off-grid solar-powered EV charging stations. Two classes of attacks including control related attacks and attacks against measurements are simulated and the results are presented. It is demonstrated that these attacks can force the voltage of the DC link out of its normal operating limits. The abnormal deviation of the DC link voltage forces the off-grid solar-powered EV charging station out of service. The outage of off-grid solar-powered EV charging stations can cause serious consequences for the electric transport, in particular, during blackouts and in remote areas where there is a scarcity of EV charging stations. We will investigate potential strategies for detection and mitigation of the attacks in our future research. The cybersecurity analysis of EV charging stations with distributed control mechanism for DC link voltage regulation is another direction that will be pursued in our future research. In addition, cybersecurity of grid-connected solar-powered EV charging stations will be investigated in our future research. Cyberattacks against grid-connected EV charging stations not only impacts the transport sector but also creates problems for the utility grid.

References

[1] L. Hook, J. Pickard, and A. Raval, "UK stops short of 2040 ban on petrol and diesel vehicles," Financial Times, 2018.

[2] USA, Exec. Office of the President 2021, Executive Order on strengthening American Leadership in clean cars and trucks, Aug 5, 2021.

[3] S. Sautermeister, M. Falk, B. Baker, F. Gauterin and M. Vaillant, "Influence of Measurement and Prediction Uncertainties on Range Estimation for Electric Vehicles," in *IEEE Trans. on Intelligent Trans. Systems*, vol. 19, no. 8, pp. 2615–2626, Aug. 2018.

[4] Z. Liu, F. Wen and G. Ledwich, "Optimal Planning of Electric Vehicle Charging Stations in Distribution Systems," in *IEEE Trans. on Power Delivery*, vol. 28, no. 1, pp. 102–110, Jan. 2013.

[5] M. M. Mahfouz and M. R. Iravani, "Grid-Integration of Battery-Enabled DC Fast Charging Station for Electric Vehicles," in *IEEE Trans. on Energy Conversion*, vol. 35, no. 1, pp. 375–385, March 2020.

[6] S. Acharya, Y. Dvorkin, H. Pandzic and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," in *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[7] Sklyar, D., ChargePoint Home security research. 2018, Kaspersky Lab Security Services: Kaspersky.

[8] K. Harnett, "DoE/DHS/DoT volpe technical meeting on electric vehicle and charging station cybersecurity report," John Volpe Nat. Transp. Syst. Center (US), Cambridge, MA, USA, Tech. Rep. DOT-VNTSC–DOE–18–01, Mar. 2018.

[9] A. C. F. Chan and J. Zhou, "A Secure, Intelligent Electric Vehicle Ecosystem for Safe Integration With the Smart Grid," in *IEEE Trans. on Intelligent Transport. Syst.*, vol. 16, no. 6, pp. 3367–3376, Dec. 2015.

[10] S. Acharya, Y. Dvorkin and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?," in *IEEE Trans. on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[11] M. E. Kabir, M. Ghafouri, B. Moussa and C. Assi, "A Two-Stage Protection Method for Detection and Mitigation of Coordinated EVSE Switching Attacks," in *IEEE Trans. on Smart Grid*, vol. 12, no. 5, pp. 4377–4388, Sept. 2021.

[12] 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," in *IEEE Trans. on Smart Grid*, vol. 13, no. 5, pp. 3903–3914, Sept. 2022.

[13] M. Basnet and M. H. Ali, "Exploring cybersecurity issues in 5g enabled electric vehicle charging station with deep learning," *IET Generation, Transmission & Distribution*, vol. 15, no. 24, pp. 3435–3449, 2021.

[14] Z. Pourmirza and S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, Canada, 2021, pp. 111–116.

[15] O. G. M. Khan, E. El-Saadany, A. Youssef and M. Shaaban, "Impact of Electric Vehicles Botnets on the Power Grid," *2019 IEEE Electrical Power and Energy Conference*, Montreal, QC, Canada, 2019, pp. 1–5.

[16] M. A. Sayed, R. Atallah, C. Assi, M. Debbabi, "Electric vehicle attack impact on power grid operation," *International Journal of Electrical Power & Energy Systems*, Volume 137, Nov. 2022.

[17] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Comp & Security*, Vol. 112, Nov 2022.

[18] J. Smith, N. Kipp, D. Gammel, and T. Watkins, "Defense-in-Depth Security for Industrial Control Systems" *EEA Conference & Exhibition* 2016, 22–24 June, Wellington.