False Data Injection Cyberattacks Targeting Electric Vehicles in Smart Power Distribution Systems

Ehsan Naderi
Department of Electrical Engineering, College of Engineering and Computer Science
Arkansas State University
Jonesboro, AR, USA
enaderi@astate.edu

Arash Asrari
Department of Electrical and Computer Engineering
Purdue University Northwest
Hammond, IN, USA
aasrari@pnw.edu

Poria Fajri
Electrical and Biomedical Engineering Department
University of Nevada
Reno, NV, USA
pfajri@unr.edu

***Abstract*—This paper presents a false data injection (FDI) attack model to target a selection of plugged-in electric vehicles (EVs) in a smart power distribution system resulting in a range of operational issues including but not limited to voltage collapse. To reduce the total cost and difficulty of the cyberattack, attacker utilizes a pre-attack analysis via generating PV and VQ curves for the buses of the distribution system in order to precisely recognize the weakest buses of the system (i.e., the most vulnerable ones) and also the required active and reactive power to be injected into the targeted buses to result in voltage collapse. The effectiveness of the proposed attack model is validated on an IEEE test distribution system modified to contain distributed generation (DG) and EV aggregators.**

Keywords—Electric vehicle (EV), false data injection (FDI) attack, frequency unbalance, operational issues, voltage collapse.

I. INTRODUCTION

A. Background and Motivation

Electric vehicles (EVs) are among the building blocks of modern power systems thanks to their dual roles as flexible load and mobile energy storage system through the concept of vehicle-to-grid [1]. Such a mechanism will need a sophisticated communication infrastructure to remotely control different assets of the system (e.g., the IoT-based devices) [2]. Although EV charging/discharging can be considered as an ancillary service in modern power systems, this is where adversaries can take advantage of the cyber layer of the power grid to penetrate into the EV charging stations and compromise the information causing a range of operational issues in the power grid [3], [4]. Thus, it is essential for power system operators to proactively simulate different scenarios of cyberattacks, including but not limited to false data injection (FDI) attacks, targeting EV charging stations and analyze the consequences of such cyberattacks from the power system operation standpoint [5].

B. A Selection of Related Works

1) Cyberattacks Targeting EV Charging Stations

In [6], a cyberattack model was investigated to increase the amount of load shedding in a distribution system based on a bi-level optimization framework targeting ultra-fast charging stations via manipulating the charging price. In [7], the negative effects of the Open Charge Point Protocol, one of the most popular protocols implemented in EV fast charging stations, were scrutinized through cyberattacks targeting smart microgrid integrated with renewable energy. A cyberattack framework was introduced in [8] where the critical information of EV users was compromised pushing the energy management system of the EV charging stations toward falsified operating situations and incorrect electricity cost. In [9], a set of safety regulations were proposed to tackle cybersecurity issues of EV charging processes in the context of smart power systems. Finally, a comprehensive review associated with cybersecurity of onboard charging systems for fleet of EVs was presented in [10], where different types of cyberattacks and the corresponding countermeasures were discussed.

2) Cyberattacks Causing Operational Issues in Smart Power Systems

In [11], an FDI framework that needed limited information about the power grid was proposed to target AC estate estimation in distribution networks. In [12], a multi-objective FDI framework was developed to minimize the investment and maximize the economic loss in a three-phase unbalanced distribution system. An FDI model was introduced in [13] to target active and reactive power set points of power inverters in a renewable-based microgrid, resulting in instability of voltage and frequency of the standalone microgrid. In [14], a load redistribution attack framework was introduced to cause overloading risk to power systems. Moreover, three evaluation metrics were proposed in [14] to scrutinize the correlation and underlying dependencies associated with malicious data injected into the system, leading to different rates of overloading. In addition, in the previous steps of this research, we introduced FDI models leading to power outage [15], voltage violation [16], and market power [17] in smart distribution systems.

C. Knowledge Gap, Research Question, and Contribution of This Work

Despite extensive research efforts in the fields of cybersecurity of EV charging stations (e.g., [6]-[10]) and smart power systems (e.g., [11]-[17]), the following research question is yet to be addressed:

This research was supported in part by the National Science Foundation under Grant No. 2348420.

979-8-3503-1766-4/24/$31.00 ©2024 IEEE

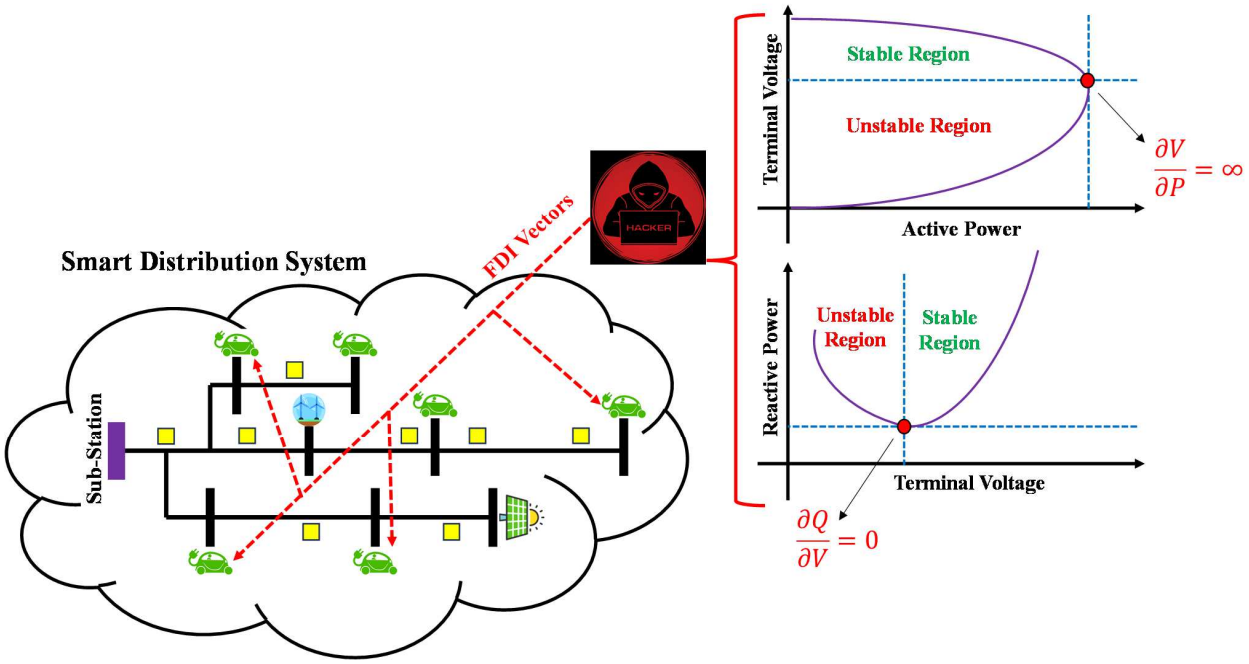

Fig. 1. The proposed framework to target EVs in a smart distribution grid (yellow squares denote the IoT-based devices (e.g., phasor measurement units) to monitor the measurements throughout the system).

- How to target EV charging stations via FDI cyberattacks, compromising the charging sessions and the corresponding charging features (e.g., the rate of charging, etc.), to result in operational issues in the power grid (e.g., voltage collapse, frequency unbalance, etc.)?

To address the indicated research question, we utilize the concept of PV and VQ curves to (*i*) assess the vulnerability of system's buses at which charging stations are installed and (*ii*) propose a FDI cyberattack framework to target EV charging stations via injecting false load data, obtained in the PV and VQ evaluation step, pushing the power grid toward voltage collapse.

II. Proposed Framework and Problem Formulation

A. Proposed Framework

The proposed attack framework is displayed in Fig. 1, where an attacker targets EV charging stations in a smart distribution system in order to disrupt the normal operation of the power grid. It is noted that attacker is aware of the exact location of the charging stations since such information is publicly accessible [18]. According to Fig. 1, the attacker obtains the PV and VQ curves of the system buses to determine the most vulnerable buses as well as the amount of false data (i.e., active and reactive power). For example, the knee point, illustrated by red circle in the PV curve of Fig. 1 (i.e., the top curve), indicates the maximum extra power that can be injected to the bus before voltage collapse happens as a consequence. Likewise, the red circle of the VQ curve in Fig. 1, which represents the valley point, is the criterion of the maximum reactive power drawn from the bus before voltage collapse starts to show up. In the next step, the attacker hacking into the user account of the EV owners (or the EV aggregator on behalf of the EV owners), launches a coordinated FDI cyberattack in order to manipulate the charging sessions. Hence, the false load data, obtained in the previous step, will be visualized into the distribution system by manipulating the charging sessions and the corresponding charging rates. The result of such a coordinated FDI cyberattack will be a set of operational issues including but not limited to missing the equilibrium between generation and demand throughout the distribution system.

B. Problem Formulation (System Operator in Attacker's Shoe)

To obtain a better perspective about the developed framework (i.e., Fig. 1), this section presents the problem formulation on a 2-bus system, which can be considered as part of a radial distribution system. In that regard, the voltage at the load end (i.e., receiving end), where the EV charging station is located, can be mathematically written in (1)-(3), where X is the reactance of the distribution branch connecting sending end to the receiving end; P and Q are, respectively, the active and reactive powers associated with the charging station located at the receiving end (i.e., load end); and ± signs indicate two solutions corresponding to specific active power and power factor (PF) [19].

$$V_R = \sqrt{-\frac{2QX + V_S^2}{2} \pm \frac{1}{2}\sqrt{(2QX - V_S^2)^2 - 4X^2(P^2 + Q^2)}} \quad (1)$$

$$V_S = |V_S|\angle\delta \quad (2)$$

$$V_R = |V_R|\angle 0 \quad (3)$$

According to (1)-(3) as well as the PV curve depicted in Fig. 1, one can infer that $\frac{\partial P}{\partial V}$ is greater than zero for the lower section of the PV curve, meaning that the system is operating in the

unstable voltage zone. Hence, the voltage stability limit can be assessed by (4), where S denotes complex power at the receiving end (i.e., the bus at which the EV charging station is located); and Y^*_{SS} is the admittance of the receiving end [19].

$$\left|\frac{S}{Y^*_{SS} \times V_R^2}\right| = 1 \tag{4}$$

From (4), it can be concluded that if the left side of the equation is very close to 1.00, the voltage stability margin will be small enough in order to push the system toward voltage instability. Therefore, the loading limit on the distribution branch ending at the EV charging station can be presented in (5), where V_C is the critical voltage at the charging station end; and X_C indicates critical reactance of the branch.

$$S = \frac{V_C^2}{X_C} \tag{5}$$

Thus, if the attacker increases the loading beyond S, via manipulating the charging sessions leading to false active and reactive power of the charging station, the system will definitely fall into the voltage instability region. To that end, (6)-(7) represent the active and reactive power of the bus at which the charging station is installed, and (8) presents the objective function of the FDI cyberattack from the attacker's point of view.

$$\tilde{P}_R = P_R + \Delta P \tag{6}$$

$$\tilde{Q}_R = Q_R + \Delta Q \tag{7}$$

$$\min\left\{\sqrt{\sum_{t=1}^{T}\sum_{i=1}^{N_{Bus}} \Delta P_{i,t}^2 + \Delta Q_{i,t}^2}\right\} \tag{8}$$

where $\tilde{P}_R$ and $\tilde{Q}_R$ are, respectively, the active and reactive power of the charging station after injecting the malicious data (i.e., ΔP and ΔQ) into the clean measurements (i.e., P_R and Q_R).

The objective function of the FDI cyberattack (i.e., (8)) needs to be minimized subject to a set of technical constraints, which are provided in (9)-(13), to ensure the normal operation of the distribution system.

$$V_i \sum_{i,j\in N_{Bus}} V_j(G\cos\varphi + B\sin\varphi) + P_L = \begin{Bmatrix} P_{EV} + \\ P_{SP} + \\ P_{WT} + \\ P_G \end{Bmatrix} \tag{9}$$

$$V_i \sum_{i,j\in N_{Bus}} V_j(G\sin\varphi - B\cos\varphi) + Q_L = \begin{Bmatrix} Q_{EV} + \\ Q_{SP} + \\ Q_{WT} + \\ Q_G \end{Bmatrix} \tag{10}$$

$$V_{min} \le V_i \le V_{max}, \forall i \tag{11}$$

$$P_{min} \le P_{ij} \le P_{max}, \forall i,j, i \ne j \tag{12}$$

$$\left|I_{ij}\right| \le I_{max}, \forall j,j, i \ne j \tag{13}$$

where P_{EV}, P_{SP}, P_{WT}, and P_G, are, respectively, the aggregated power associated with electric vehicles, solar panels, wind turbines, and the gird; G and B are conductance and susceptance of the branches, respectively; V_i is the voltage magnitude at bus i; φ is the voltage phase angle at bus i; and P_{ij} and I_{ij} are, respectively, the magnitude of power and current flowing into line connecting buses i and j.

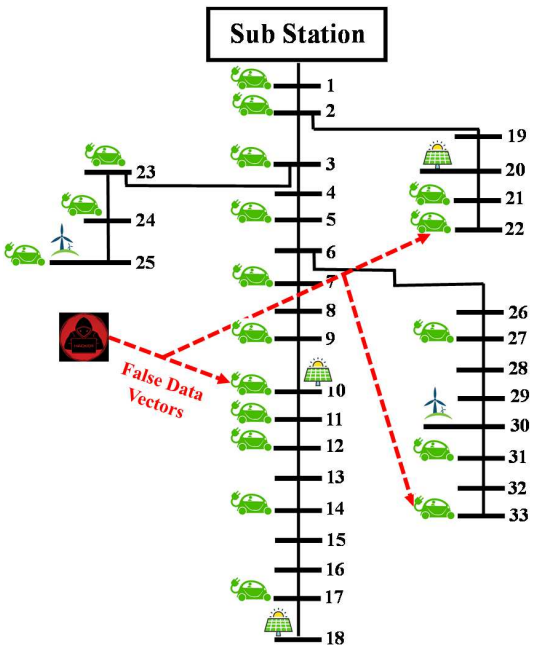

Fig. 2. IEEE 33-bus test system modified to encompass electric vehicles (EVs), solar panels (SPs), and wind turbines (WTs).

TABLE I
OBTAINED RESULTS FROM TARGETING IEEE 33-BUS SYSTEM VIA FDI CYBERATTACK LEADING TO VOLTAGE COLLAPSE

Vulnerable Bus #	Active Power (kW)	Reactive Power (kVAR)
10	-12.55	5.20
22	9.31	-6.38
33	8.14	6.44

III. INITIALIZATIONS, SIMULATION RESULTS, AND ANALYSES

A. Initialization

The IEEE 33-bus test system is modified to contain solar panels, wind turbines, and EVs at different buses and throughout the system. It is noted that the distributed generation units and EVs are able to supply 50% of the demand of the system (i.e., 3,715 kW of active power and 2,300 kVAR of reactive power). The single-line diagram of the case study is provided in Fig. 2, and the rest of the system's information can be found in [15]. After performing the pre-attack evaluation by the attacker, buses #10, #22, and #33 are determined as the most vulnerable buses to voltage collapse since the knee points of the PV and VQ curves associated with these three buses are very close to the critical positions, as displayed in Fig. 1. Hence, the attacker needs to inject a lower amount of false data (i.e., active and reactive power) to push the system toward voltage instability region (see Fig. 1 and (1)). In this regard, TABLE I presents the amount of necessary false data to trigger a voltage collapse in the IEEE 33-bus test system under study. According to TABLE I, it can be inferred that positive sign indicates addition of false data to the original power of load point, and negative sign shows subtraction from the original amount. As an illustration, respectively, 8.14 kW and 6.44 kVAR active and reactive power

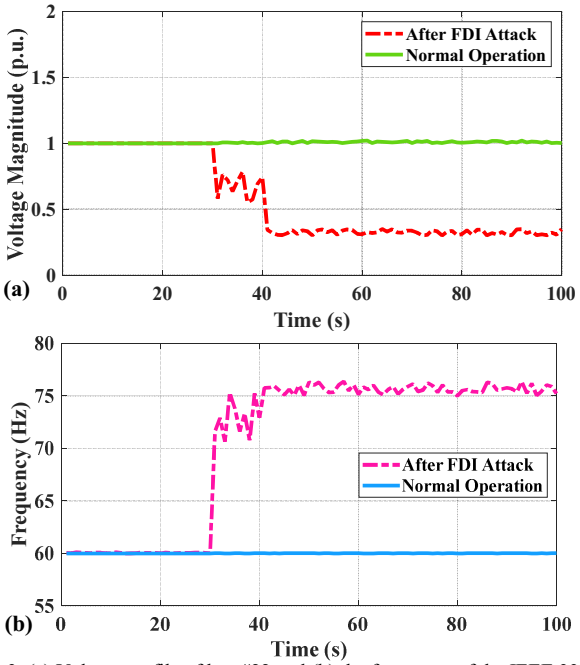

Fig. 3. (a) Voltage profile of bus #22 and (b) the frequency of the IEEE 33-bus distribution system before and after the FDI Cyberattacks targeting charging stations.

(i.e., false data) needs to be injected into the charging stations associated with bus #33 to push the distribution system toward operational issues.

B. Obtained Simulation Results

To obtain a better perspective, Fig. 3 illustrates the voltage magnitude of bus #22 and the corresponding frequency of the entire system before and after the FDI attack targeting charging stations located at bus #22. From this figure, it can be seen that only injecting a small vector of malicious data (i.e., active and reactive power in this study) can push the power grid toward intended operational issues (e.g., voltage collapse, as shown in Fig. 3 (a) and frequency unbalance, as depicted in Fig. 3 (b)). According to Fig. 3 (b), one can perceive that although there is enough level of generation in the IEEE 33-bus distribution system (i.e., in reality, the system is neither under generation nor over generation), the malicious frequency increases by 25% after the FDI attack. This stems from the fact that false load data, injected by the attacker, are processed in the operation of the power system, pretending that power grid suffers from lack of generation based on the malicious signals from the charging stations (see TABLE I). This is where the importance of false data detection systems and remedial action mechanisms (i.e., the scope of our future work) come under the spotlight to track the presence of malicious data in real time and keep the functionality of the targeted power grid intact.

To obtain a deeper view on the impacts of FDI cyberattack on the power flow in distribution branches, Fig. 4 illustrates the active power flow in all the branches in IEEE 33-bus test system. From this figure, one can perceive that the majority of the branches experience higher power flow after the FDI attack. However, branches #7, #17, and #25 are severely overloaded. For example, loading of branch #25 increases by 46.4%, which

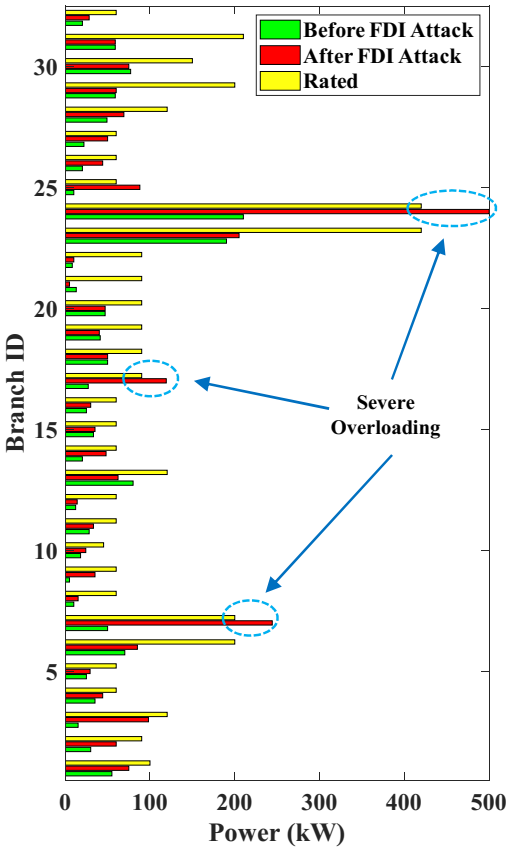

Fig. 4. Power flows in distribution branches before and after the FDI cyberattack leading to voltage collapse.

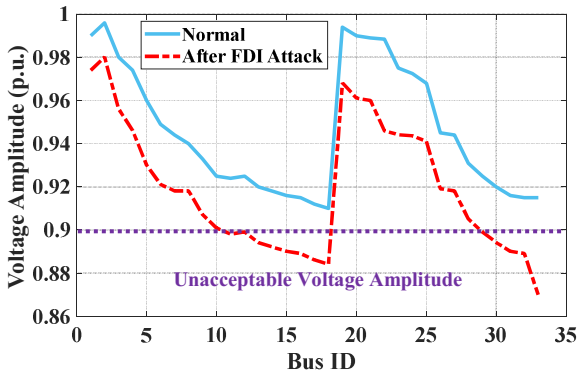

Fig. 5. The voltage profile of IEEE 33-bus test system before and after the FDI attacks targeting EV's charging stations.

can be considered more than enough to trigger the protective overcurrent relays associated with this branch. Such distributed overloading issues in the system, which can lead to declining voltage, paves the way for a noticeable power shortage or blackout, in extreme cases. In other words, the adjusted power, flowing into the branches in IEEE 33-bus test system (see Fig. 4), is falsified after the FDI attack (see the red bars in Fig. 4), which indirectly changes the magnitude of voltage in almost all the systems' buses, obtained from a power flow analysis, as depicted in Fig. 5. From this figure it can be concluded that the majority of the system's buses have reduced voltage magnitudes after launching the FDI attack (see the red dash-dotted line);

however, buses #10-#18 and also #28-#33 are in the critical zones since their voltage magnitudes are less than 0.9 p.u., as indicated by purple dotted line in Fig. 5.

IV. Conclusion

Based on the results obtained from the simulations, when the charging stations of the vulnerable buses were the target of a coordinated FDI cyberattack, the power distribution system lost its synchronism. This is due to the fact that the control mechanisms, managing the energy throughout the system, processed false data received from the targeted charging stations. The following summarizes the conclusion drawn from this study.

- The obtained results confirmed that, in the pre-attack evaluation, buses #10, #22, and #33 were identified as the most vulnerable buses to voltage instability in the IEEE 33-bus test system. Although these three buses experienced different rates of undervoltage after launching the coordinated FDI cyberattack targeting the EV charging stations, only buses #10 and #33 fell into the voltage instability region. This is due to the fact that bus #22 is closer to the substation compared to buses #10 and #33.
- It was also verified that the FDI attack led to a frequency increase by 25%, which stems from processing false data, injected by the attacker into the charging stations. This falsified data processing can pretend that power grid suffers from lack of generation, which is not actually the case.
- Such a coordinated FDI attack, targeting the EV charging stations, disrupted the power flow of the IEEE 33-bus test system such that branches #7, #17, and #25 experienced more than 20% overloading with respect to the rating of the distribution branches. Such amount of overloading can be equivalent to trip current associated with the overcurrent relays. Therefore, the system may experience power outages in different regions if such cyberattacks are not cleared in a timely manner.

In the future step of this research, we will take advantage of hardware-in-the-loop (HIL) testbeds to experimentally validate the impacts of the investigated FDI attack on EV charging stations on a lab-scale smart grid. More importantly, we will propose a remedial action scheme (RAS), oriented toward controlling the under-load tap chaining transformer installed in the substation, against such FDI cyberattacks in real time in order to mitigate the negative impacts and recover the voltage profile of the targeted power system to normal operation in a timely manner.

References

[1] Plug-In Electric Vehicles. [Online]. Available: https://www.smartgrid.gov/the_smart_grid/electric_vehicles.html. (Last visited: December 11, 2023).

[2] M. Girdhar, J. Hong, Y. You, and T.-J. Song, "Anomaly detection for connected and automated vehicles: accident analysis," *IEEE Transportation Electrification Conference & Expo (ITEC)*, Detroit, MI, USA, 2023, pp. 1-5.

[3] A. Sanghvi and T. Markel, "Cybersecurity for electric vehicle fast-charging infrastructure," *IEEE Transportation Electrification Conference & Expo (ITEC)*, Chicago, IL, USA, 2021, pp. 573-576.

[4] N. Damianakis, Y. Yu, G.C.R. Mouli, and P. Bauer, "Frequency regulation reserves provision in EV smart-charging," *IEEE Transportation Electrification Conference & Expo (ITEC)*, Detroit, MI, USA, 2023, pp. 1-6.

[5] E. Naderi and A. Asrari, "Integrated power and transportation systems targeted by false data injection cyberattacks in a smart distribution network," in *Electric Transportation Systems in Smart Power Grids - Integration, Aggregation, Ancillary Services, and Best Practices*, CRC Taylor & Francis Publisher, Boca Raton, FL, USA, 2023.

[6] A. Akbarian, M. Bahrami, M. Vakilian and M. Lehtonen, "Vulnerability of EV charging stations to cyber attacks manipulating prices," *International Conference on Future Energy Solutions (FES)*, Vaasa, Finland, 2023, pp. 1-6.

[7] K. Gandhi and W.G. Morsi, "Impact of the open charge point protocol between the electric vehicle and the fast charging station on the cybersecurity of the smart grid," *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Halifax, NS, Canada, 2022, pp. 235-240.

[8] S.I. Jeong and D.-H. Choi, "Electric vehicle user data-induced cyber attack on electric vehicle charging station," *IEEE Access*, vol. 10, pp. 55856-55867, May 2022.

[9] B. Wang, P. Dehghanian, S. Wang, and M. Mitolo, "Electrical safety considerations in large-scale electric vehicle charging stations," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6603-6612, Nov.-Dec. 2019.

[10] A. Chandwani, S. Dey, and A. Mallik, "Cybersecurity of onboard charging systems for electric vehicles - review, challenges and countermeasures," *IEEE Access*, vol. 8, pp. 226982-226998, Dec. 2020.

[11] S. Jin, "False data injection attack against smart power grid based on incomplete network information", *Electric Power Syst. Res.*, vol. 230, p. 110294, May 2024.

[12] P.L. Bhattar, N.M. Pindoriya, and A. Sharma, "False data injection in distribution system: Attacker's perspective," *Int. J. Crit. Infrastruct. Prot.*, vol. 45, p. 100672, Jul. 2024.

[13] M. Beikbabaei, M. Montano, A. Mehrizi-Sani, and C.-C. Liu, "Mitigating false data injection attacks on inverter set points in a 100% inverter-based microgrid," *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2024, pp. 1-5.

[14] X. Wei, J. Lei, J. Shi, M. Shahidehpour, and S. Gao, "A data-driven approach for quantifying and evaluating overloading dependencies among power system branches under load redistribution attacks," *IEEE Trans. Smart Grid*, Early Access, 2023, doi: 10.1109/TSG.2023.3344556.

[15] A. Asrari, E. Naderi, J. Khazaei, P. Fajri, and V. Cecchi, "Modern heat and electricity incorporated networks targeted by coordinated cyberattacks for congestion and cascading outages," in *Coordinated Operation and Planning of Modern Heat and Electricity Incorporated Networks*, IEEE, Piscataway, NJ, USA, 2023, pp.115-155.

[16] E. Naderi, S. Pazouki, and A. Asrari, "A coordinated cyberattack targeting load centers and renewable distributed energy resources for undervoltage/overvoltage in the most vulnerable regions of a modern distribution system," *Sustain. Cities Soc.*, vol. 88, p. 104276, Jan. 2023.

[17] E. Naderi and A. Asrari, "A remedial action scheme to mitigate market power caused by cyberattacks targeting a smart distribution system," *IEEE Trans. Ind. Inform.*, vol. 20, no. 3, pp. 3197-3208, Mar. 2024.

[18] M.A. Sayed, R. Atallah, C. Assi, and M. Debbadi, "Electric vehicle attack impact on power grid operation," *Int. J. Electr. Power Energy Syst.*, vol. 137, p. 107784, May 2022.

[19] A.A.I. Ahmed, "Voltage collapse modes in power networks," M.S. Thesis, College of Engineering and Computer Science, University of Tennessee, Chattanooga, TN, USA, 2019. Available: https://scholar.utc.edu/cgi/viewcontent.cgi?article=1774&context=theses