Power Grid Protection Solution Against Load Altering Cyberattack via EV Charging Stations

Samira Chouikhi, Lyes Khoukhi

Power Grid Protection Solution Against Load Altering Cyberattack via EV Charging Stations

Samira Chouikhi, and Lyes Khoukhi
Université Caen Normandie, ENSICAEN, CNRS, Normandie Univ, GREYC UMR 6072, F-14000 Caen, France.

***Abstract*—With the widespread adoption of electric vehicles (EVs), EV charging infrastructure has become more advanced. Unfortunately, this cyber-physical system is vulnerable to physical or cyberattacks. In this work, we focus on load-altering (LA) attacks that affect the operation of the power grid. We propose a distributed multi-agent Deep Reinforcement Learning (DRL) based solution to detect, identify, and mitigate LA attacks. The defense system responds to the sudden change in charging/discharging behavior using an event-based approach to preserve power stability throughout the charging process. The proposed approach allows the system to identify and counteract the impact of LA attacks on the electrical grid. After the compromised entities are identified, they are isolated, and a backup charging strategy is applied to fully or partially recover the operation of the charging system. According to the performance evaluation, the proposal reduces the effect of LA attacks while producing good detection accuracy rates.**

***Index Terms*—Electric vehicles, charging stations, attack detection, attack mitigation, deep reinforcement learning, load-altering attack.**

I. Introduction

The increasing popularity of intelligent electric vehicles has created new opportunities for research and development. By 2040, it is projected that one-third of cars globally will be electric. Some of the biggest manufacturers in the world plan to introduce several new electric car models over the next 10 years. The current infrastructure for EV charging has to be enhanced and expanded as the global automotive fleet transitions to electric vehicles (EVs). Open standards and a common EV charging infrastructure are necessary to integrate services provided by independently operated charging stations. Thanks to this unification, EVs will be able to use a wide range of cross-vendor charging stations, charge frequently, and operate flawlessly. Coordination of the services and activities provided by the various pricing system firms is therefore necessary for this approach. However, when smart energy and smart transportation systems are integrated to form a complex system with numerous coexisting components and technologies, new threats and vulnerabilities are created by the interconnection of mobile devices, autonomous vehicles, and heterogeneous cyber-physical systems. Several defense methods and tactics have already been implemented by different charging ecosystem entities [1], [2], [3]. To address the particular security concerns with EV charging infrastructure, we still need to modify current practices and create new approaches.

Charging stations are vulnerable to physical, cyber, and hybrid threats since they are cyber-physical systems. The main issue with this ecosystem is that it might be used to target more critical systems, such as the infrastructure of the electrical grid. To interrupt grid operations and possibly induce blackouts, attackers may control and adjust the grid power [4], [5].

In this work, we concentrate on safeguarding the electrical grid to avoid, detect, and mitigate attacks utilizing EV charging systems. Our goal is to stop or lessen the effects of cyberattacks on the stability and operation of the electrical grid. We specifically handle grid stability-causing Load-Altering (LA) threats. These assaults change the load and interfere with the regular functioning of the power system by using infected EVs and charging stations. Two of the most well-known LA attacks are: switching or oscillatory attacks and load injection attacks. In the initial attacks, the attackers intentionally add a significant quantity of energy to the system by simultaneously draining the batteries of electric vehicles using the two-way energy flow. Frequency increases and voltage violations are caused by the load injection. In contrast to electricity supplied by a generator, the injected power cannot be managed or regulated by the system, hence, its effect on the grid is more detrimental than a rise in power demand. Power injection and rising demand are quickly switched between to carry out the oscillatory attacks. This attack's initial phase lowers the frequency by sharply raising the power usage. Subsequently, the attacker cancels the demands and executes power injection while concurrently discharging EVs as the system begins to modify the turbines' frequency and speed to recover. The frequency increases as a result of this step. The frequency and voltage within the power grid oscillate as a result of the attacker's frequent switching between the two steps in a short amount of time. The abrupt changes in the demand for electricity not only affect the functioning of the power system but also significantly alter the output of power producers. This variance affects the generators' lifespan and maintenance schedule.

There have been several intriguing studies devoted to this subject to defend the power grid against load-altering attacks. The authors of [6] conducted a thorough analysis of the risks and vulnerabilities in the EV ecosystem that affect the power grid's ability to function. They also looked into how oscillatory load attacks initiated by the CSs affected the electrical grid. They thus showed how the threat to the essential power infrastructure is significantly increased by a weak charging ecosystem. This could lead to unstable systems, line tripping, etc.A centralized Back Propagation Neural Network-based method for identifying oscillatory load attacks was presented by Kabir

et al. [7]. The neural network model analyzes charging and discharging requests to detect risks. However, when the attacks are less than 20 seconds in duration, this method has a false negative rate of 30% . The issue of load-altering attack under uncertainty in photovoltaic power generation was investigated in [8]. The authors formulated the problem as a Wasserstein metric-integrated robust optimization-based Volt/VAR optimization (DRO-VVO) problem. PV planning and curtailment are also employed to mitigate the attack's negative effects on voltage stability. The authors of [9] proposed a distributed edge-based method to identify and detect oscillatory load attacks. They use deep learning techniques to examine the behavioral traits of the system's constituent parts to identify the threats. To mitigate the effects of an attack on the power network, a charging process scheduling system was suggested [10]. The authors employed particle swarm optimization to determine the optimal scheduling strategy. The authors did not include a detection and mitigation approach against load-altering assaults, even though they use scheduling to keep the power system stable. An intrusion detection technique was introduced to identify cyber-physical attacks against fast charging stations early on, taking into account V2G operation for service delivery in microgrids with renewable energy resources [11].

In our work, we focus on proposing a distributed defense approach against LA attacks based on Deep Reinforcement Learning (DRL). The proposal aims to detect and mitigate LA attacks using compromised EVs and charging stations. This mechanism is based on behavior and event analysis with a multi-agent DRL model.

The attack and defense models are presented in Section II. We present the multi-agent DRL model-based detection, isolation, and recovery approach against load manipulation attacks in Section III. Section IV provides the performance evaluation results. Section V concludes the paper.

II. Methodology And System Model

As illustrated in Fig. 1, our EV charging system consists of a Charging Station Management System (CSMS), a set $\mathcal{M}$ of M Charging Stations (CSs), and a set $\mathcal{N}$ of N Electric Vehicle Supply Equipment (EVSE). A CS m hosts a set $\mathcal{N}_m$ of N_m EVSEs. We also Consider a set of V EVs that request charging service.

A. Attack Model

An attacker who can monitor and control a large number of hacked EVs and CSs is considered. Numerous attack vectors can be used to initiate an attack against the electrical system. The different attack vectors are as follows:

- The attacker leverages the connected internal vehicle components, such as the On-Board Diagnostics (OBD) port, to hack EVs. The latter can be physically and remotely managed by getting access to the Controller Area Network (CAN) bus, which allows for control over the vehicle and charging procedure.

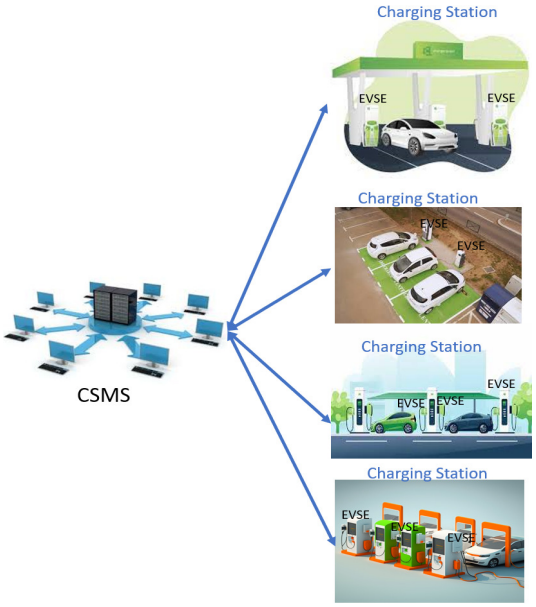


Fig. 1. EV Charging System.

- The adversary could exploit the mobile application, which is the driving force behind the commercialization of the EV charging ecosystem, by taking advantage of the absence of end-to-end authentication between the user and his vehicle. This would allow the adversary to exploit vehicles connected to the charging station opportunistically.
- The attacker can take control of the CSs by physically and remotely hacking.
- By controlling a sizable distributed CSMS botnet, the attacker can launch attacks against the power grid and take advantage of one or more operators' management systems (multi-operator). By using several CSMSs, the attacker might develop several attack combinations.
- The attacker exploits the vulnerabilities of the communication protocol OCPP against the Man-In-The-Middle attack to bypass the centralized defense systems.

The adversary can leverage public charging stations as well as private charging stations to launch the LA attacks. However, the attacker needs to collect data about the grid operation and the response of the existing physical layer detection mechanism hosted by the utility operator. He may use interception and false data injection attacks to gather the required data to deceive the physical layer defense mechanism.

B. Defense Model

The goal of the defender is to prevent, detect, and lessen attacks that try to disrupt the electric grid's operation. In our proposal, we use machine learning techniques and propose a multi-agent DRL model, where we dedicate an agent to each charging station. This agent will be responsible for detecting and identifying local and large-scale attacks by analyzing the

events that occur at the charging stations and observing the parameters of the surrounding environment.

When a new event is observed (new request, behavior change, request cancellation, etc.), the agent retrieves information about previous events and the frequency of the electrical network from a log file stored at the charging station. This information is integrated into a DRL learning model to detect whether events are malicious or not. Simultaneous attacks can also be detected and identified using this information. The DRL-based defense system will be presented in the next section.

III. Multi-Agent DRL Based Attack Prevention, Detection and Mitigation Approach

For the implementation of the DRL-based defense system, we opt for a multi-agent distributed model where the DRL agents are located at the CS level. The distribution of the solution prevents the issues related to the centralized execution, such as the increasing complexity, the huge number of exchanged messages, and the amount of data transmitted to the central server. In addition to the fact that the central server must get global network knowledge, which is impractical given the volume of data to exchange, some security issues (Man-In-The-Middle) may worsen the situation instead of solving it.

A. Markov Decision Process

For each DRL agent, we formulate the problem as a Markov Decision Process (MDP). Typically, an MDP is represented as $< \mathcal{S}_m, \mathcal{A}_m, \mathcal{F}_m, \mathcal{R}_m, \mathcal{S}_m^{'} >$.

In the state space $\mathcal{S}_m$, a state vector represents the perception of the environment. The action $a_m(t) \in \mathcal{A}_m$ represents the action taken by the agent when the system's current state is $s_m(t)$. The probability distribution $\mathcal{F}_m$ includes the transition probabilities. Note that the agents cannot predict the states, rewards, and transitions before they make a decision. Consequently, we propose a model-free deep Q-learning model with an unknown transition probability distribution.

The immediate feedback that the environment provides for activities is reflected in the reward function. In the defense model, the objective is to increase the detection of attacks and identification of events; hence, the reward function will be inversely proportional to the detection and identification error functions.

The optimal Q-value can be found by iteratively updating the Bellman equation. After $t \rightarrow \infty$, the Q-value rises and tends to the optimum value. However, it is not feasible to iterate ∞ times, and this could result in a deviation from the optimal strategy. This problem can be resolved by employing a deep neural network as a non-linear function that approximates complex states, which greatly reduces the search space.

B. Deep Q-Learning Model

The primary benefit of the DRL model is its ability to solve complex problems by merging deep learning and Q-learning, which solves the problem of dimensionality in Q-learning. In this paradigm, a Deep Neural Network (DNN) represents the input states, and the probability of any possible action is computed concurrently. Based on interactions with the environment and these probabilities, the agents decide what to do.

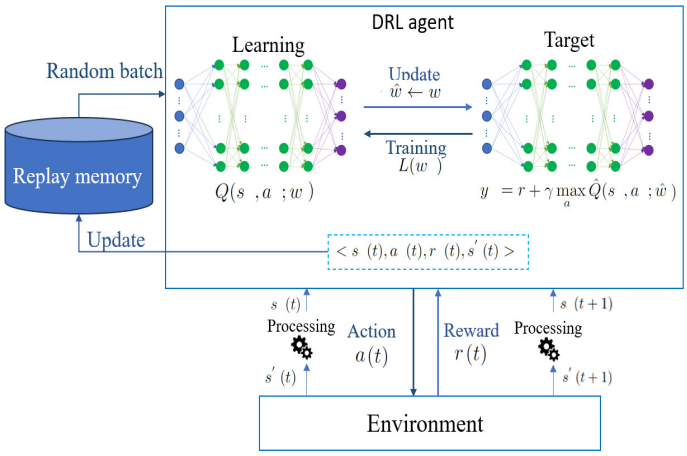


Fig. 2. The DRL model

We show the proposed DRL model for each agent in Figure 2. In the suggested model, the approximation function is a neural network, also called a Q-Network, with parameters w. However, combining reinforcement learning with a Deep Q Network (DQN) makes training the model more challenging because of the variable feedback from a dynamic environment. Fixation strategies are introduced to solve this issue and avoid divergence during training. An approximator neural network, sometimes referred to as the primary or local learning network, has a copy with fixed parameters ∇_w, in which the weights remain constant for a predefined number of episodes. This duplicate network is referred to as the target network. The learning network continues to learn from the replay memory data, and the weights w are copied to the target network after each Z episode.

The DQN's output is $Q(s(t), a(t); w(t))$ for each input state $s(t)$ and action $a(t)$ in the agent's DRL model, where $w(t)$ represents the DQN weights. Using the ϵ-greedy policy, the agents use a greedy algorithm with probability $1 - \epsilon$ to select the best actions, and randomly choose other actions with a probability of ϵ.

Additionally, the agent saves the experience $< s(t), a(t), r(t), s^{'}(t) >$ in a replay memory $\mathcal{D}$ each time $s(t)$ is updated to $s^{'}(t)$. In each training phase, a mini-batch of size B is chosen at random from $\mathcal{D}$ to update the DQN parameters. The goal is to minimize the loss function, also known as the mean-square error, between the current and target Q values.

The multi-agent DRL models are trained offline in the CSMS and then sent to the CSs for decision-making.

C. Multi-Agent DRL-Based Attack Detection and Mitigation

To identify anomalies and attacks initiated by EVs and CSs that have been compromised, the defense system monitors

the charging system in real time. It determines if an event is suspicious, malevolent, or normal based on the analysis of events that have occurred. We choose Deep Reinforcement Learning for the decision-making process, and for each CS, we define a DRL agent. The DRL model characterizes the event using data like charging schedules, the state of EVSEs, request types, previous events, CS logs, etc. In addition to the local parameters, the C-DS can immediately record the power grid frequency, which is directly related to the speed of the generators, with high granularity by measuring the duration of the voltage waveforms that are sampled over time. This information is recorded in the log file of each CS. The main events that can occurs in one or more EVSEs are the following:

- New request of charging/discharging arrived;
- The request for charging/discharging is canceled;
- The request changes from charging to discharging or vice versa;
- EVSE status changes from ON to OFF or vice versa;

The information about the event and the data extracted from the interaction with the environment are fed into the DRL model to detect the maliciousness of the events that occurred. In general, local data and events are used to detect and identify local attacks, while the grid frequency is an addition to detect cooperative large-scale LA attacks.

The action taken by the C-DS will depend on the output of the DRL model:

- Cancel the demand for one or many EVs identified as malicious.
- Isolate the CSs identified as compromised.
- Accept the new request and start the charging/discharging service immediately;
- Postpone the start of the charging/discharging for some time;
- Switch EVSEs' status from charging to discharging or vice versa;
- Replace the canceled demands with backup EVSEs' demands;
- If a sequence of events is identified as malicious, the agent creates a switching block that will randomly switch charging stations between on and off to disrupt the synchronization of attacks.

For the recovery strategy, the defense system replaces the canceled power demands with new demands. It either uses new charging requests or backup EVSEs. This strategy makes it possible to re-stabilize the system with little changes to its current functioning. The system decides to use the backup EVSEs to replace the canceled EVSEs when there aren't any new EVs joining the charging network or not enough of them to produce a stable situation. The backup EVSEs are chosen from the operational EVSEs whose requests are postponed. The DRL agents also inform the CSMS and grid operator of the LA attacks, and the identities and locations of the compromised CSs.

IV. Performance Evaluation

The WSCC 9-bus system 3, a widely used system in academic research, is the system on which we execute our simulation. We consider a 0.6 lagging EV charging power factor pf.

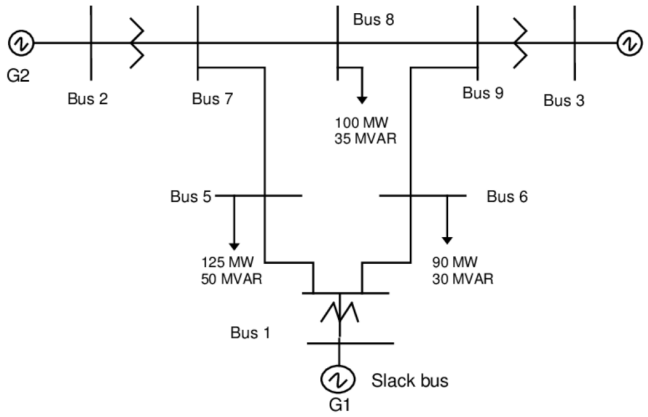


Fig. 3. WSCC 9-Bus system

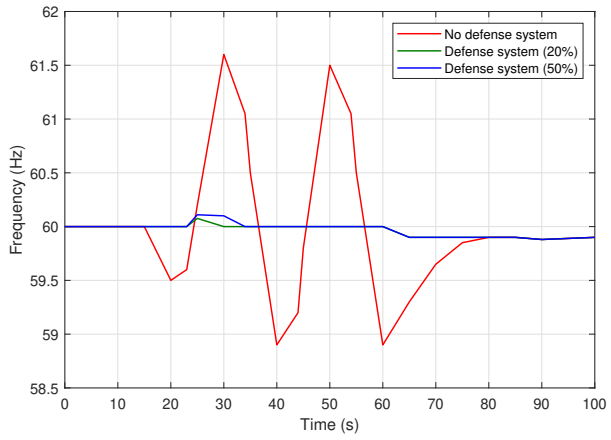
First, we replicated an oscillation attack to demonstrate its effects on the power grid by adding 21 MW to bus 6, which equates to 2900 EVs charging at 7.2 kW. Then, we inject 60 MW of negative load in bus 5, which corresponds to 8300 EVs discharging. Closing bus 6 and then opening it and closing bus 5 at t=15 s, t=35 s, t=45 s, and t=55 s is how the attack is executed.

Fig 4(a) illustrates how the frequency varies over time in tandem with the charging/discharging load's oscillation. Fig 4(b) for bus 8 illustrates how the voltage at the load buses changed as well. Therefore, we may say that even in the absence of a large power load, such an attack can affect the electrical system. Even when there are fewer EVs, this attack can still harm the turbines because of the rapid acceleration and deceleration times.

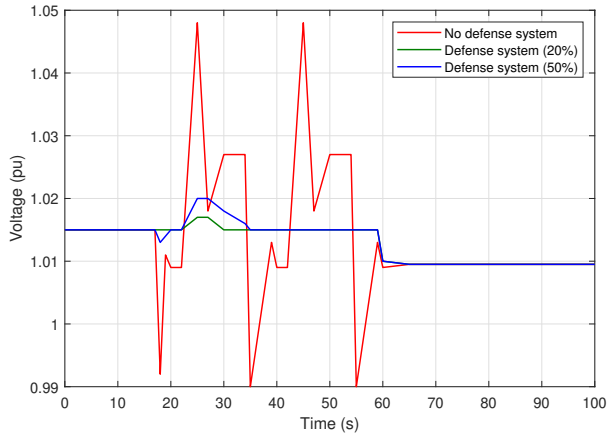
To test the effectiveness of our approach, we carried out the same attack on the system while using the developed DRL-based model for attack detection and neutralization. We compare and contrast two scenarios: In the first scenario, 20% of the entities that request charging and discharging services at the same time are compromised EVs and CSs. The percentage of compromised entities was then increased to 50%.

In both cases, the attack is identified as soon as it starts, but it takes a few seconds to be mitigated, as Figure 4 demonstrates. Furthermore, the recovery and replacement procedures can minimize frequency and voltage variations even before the attack is neutralized. The distinctions between the scenarios with and without a defense system are therefore more noticeable. On the other hand, the system re-stabilizes more slowly when the attackers' percentage is higher.

We evaluate the detection accuracy by implementing two scenarios depending on the types of events that occur: S1 (70% malicious, 30% benign) and S2 (30% malicious, 70% benign), as indicated in Table I. The results showed that



(a) Frequency



(b) Voltage at bus 8

Fig. 4. Transient response to the oscillatory attack with DRL-based defense system.

TABLE I
DETECTION ACCURACY, FALSE NEGATIVE RATE, AND FALSE POSITIVE RATE

	ACC	**FNR**	**FPR**
Simultaneous attacks	S1: 100% S2: 100%	S1: 0% S2: 0%	S1: 0% S2: 0%
Small-scale attacks	S1: 99.65% S2: 98.5	S1: 2% S2: 4%	S1: 3% S2: 5%

we achieved a 100% detection rate of large-scale load manipulation or simultaneous cooperative attacks in all cases. However, certain individual or small-scale attacks are not detected, and their false negative rates (FNR) are 2% and 4% for the two cases, respectively. For the two cases, the defense system produces false positive rates (FPR) of 3% and 5%, respectively. The DRL agents determine the current event's character based on previous occurrences, and it is evident that the agents categorize more events as malicious as the number of malicious events rises. Most likely, the electrical grid is unaffected by these attacks. On the other hand, as the number of harmful events rises, the FPR rises as well because the DRL agents become more watchful and suspicious of the significant number of anomalies and aberrant events, which causes them to mistakenly label certain regular behaviors as suspicious or malicious. Given the system's scalability and the fact that these rates have no effect whatsoever on the electrical grid, the number of false positives and false negatives is still extremely low.

V. CONCLUSION

The infrastructure of the power grid is more vulnerable to attacks as the number of EVs rises. These latter undermine the grid's stability and functionality by taking advantage of the weaknesses in the EV charging infrastructure. Load manipulation or alteration is one of the most well-known attacks that use EV charging stations to target the electrical infrastructure. By switching between charging and discharging, these attacks affect loads and cause grid instability. To detect, identify, isolate, and mitigate load-altering assaults, we developed a behavior and event-based defense system. We opt for Deep Reinforcement Learning as an effective distributed technique for securing the power grid against LA attacks. In addition of the identification and isolation of the compromised entities, the defense system ensures the recovery of the grid stability using a backup strategy. We demonstrate that the proposed method reduces the impact of load manipulation attacks and achieves good detection accuracy that equals 100% with a 0% false negative rate for simultaneous cooperative attacks based on the results of performance evaluation.

ACKNOWLEDGMENT

This work is partly financed by Région Normandie, France, under the SHARP project.

REFERENCES

[1] A. Bourass, S. Cherkaoui, and L. Khoukhi, "Secure optimal itinerary planning for electric vehicles in the smart grid," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3236–3245, 2017.

[2] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Fog-based distributed intrusion detection system against false metering attacks in smart grid," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[3] C. D. Abd Eldjalil and K. Lyes, "Optimal priority-queuing for ev charging-discharging service based on cloud computing," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[4] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.

[5] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[6] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, "Electric vehicle attack impact on power grid operation," *International Journal of Electrical Power & Energy Systems*, vol. 137, p. 107784, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521010048

[7] M. E. Kabir, M. Ghafouri, B. Moussa, and C. Assi, "A two-stage protection method for detection and mitigation of coordinated evse switching attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4377–4388, 2021.

[8] P. Prabawa and D.-H. Choi, "Distributionally robust pv planning and curtailment considering cyber attacks on electric vehicle charging under pv/load uncertainties," *Energy Reports*, vol. 11, pp. 3436–3449, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484724001677

[9] K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised ev charging stations," *International Journal of Electrical Power & Energy Systems*, vol. 156, p. 109735, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061523007925

[10] N. M. M. Mohamed, H. M. Sharaf, D. K. Ibrahim, and A. El'gharably, "Proposed ranked strategy for technical and economical enhancement of evs charging with high penetration level," *IEEE Access*, vol. 10, pp. 44 738–44 755, 2022.

[11] Z. Warraich and W. Morsi, "Early detection of cyber-physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids," *Sustainable Energy, Grids and Networks*, vol. 34, p. 101027, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352467723000358