EV-based Load-altering Attacks and their Impacts on the Stability of Power Grids

Ahmadreza Abazari

A Thesis

in

The Concordia Institute

for

Information Systems Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy (Information Systems Engineering) at

Concordia University

Montréal, Québec, Canada

January 2025

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Mr. Ahmadreza Abazari**

Entitled: **EV-based Load-altering Attacks and their Impacts on the Stability of Power Grids**

and submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy (Information Systems Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Jassim Hassan

_____ External Examiner
Dr. Khalil El-Khatib

_____ External to Program
Dr. Jun Yan

_____ Internal Examiner
Dr. Walter Lucia

_____ Internal Examiner
Dr. Hamid Taghavifar

_____ Thesis Supervisor
Dr. Mohsen Ghafouri

_____ Thesis Supervisor
Dr. Chadi Assi

Approved by _____
Farnoosh Naderkhani, Graduate Program Director

Defense Time: January 2025

_____
Mourad Debbabi, Dean
Faculty of Engineering and Computer Science

Abstract

EV-based Load-altering Attacks and their Impacts on the Stability of Power Grids

Ahmadreza Abazari, Ph.D.

Concordia University, 2025

The extensive use of electric vehicles (EVs) provides energy-critical infrastructures with some advantages and drawbacks at the same time. The large-scale deployment of EVs can improve the reliability and efficiency of the power grid through, for instance, bidirectional energy transfers between grids and EVs, reduction in electricity bills, and ancillary services. The majority of these advantages are enabled by the use of communication and information technologies (ICTs) in the EV infrastructures and their associated smart power grids. Moreover, EV supplies equipment (EVSE) network, e.g., charging stations, including a variety of Internet of Things (IoT) devices and smartphone applications that facilitate the charging process for users. However, such a broad deployment of cyber devices and information technologies makes the EV ecosystem prone to cyber-attacks in the form of data manipulation, malware, and intrusions. The attacks against public and private EV charging stations, which are often designed without security concerns in mind, are threats against owners and can lead to complicated security issues for smart grids. Additionally, compromising the security of these large-scale EV infrastructures can propagate into the wide-area transmission power grid, cause resonance events, and result in instability and even blackouts. Studying potentially vulnerable points in the EV ecosystems that adversaries can exploit to impact the stability of power grids, and suggesting proper detection and mitigation strategies is of paramount importance. Finally, designing security metrics for distribution and transmission systems can assist power grid utilities in informing about the power grid security status in the presence of attacks originating from EV ecosystems.

Acknowledgments

First and foremost, I would like to thank Dr. Mohsen Ghafouri and Dr. Chadi Assi for kindly accepting the responsibility of being my supervisors. I would like to express my deepest gratitude to Dr. Ghafouri for his unwavering support, guidance, and encouragement throughout this journey. I am deeply appreciative of the time and effort he has invested in helping me refine my ideas and overcome challenges. I would also like to express my heartfelt appreciation to Dr. Danial Jafarigiv and Dr. Ribal Atallah, whose mentorship has had a profound impact on both my academic path and personal growth. Their invaluable comments, suggestions, guidance, and encouragement have been pivotal to the success of this work. I feel incredibly fortunate to have had the opportunity to work under their supervision, and I will forever be thankful for their dedication, support, and belief in my potential.

Finally, I would like to express my heartfelt gratitude to my MOTHER for her unwavering support and encouragement, despite the distance between us.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this chapter, we start by outlining the motivation behind this thesis, then a clear definition of the problem statement, and finally the key research contributions of this thesis.

1.1 Problem Statement

Electric vehicles (EVs) play an increasingly critical role in modern society due to their significant impact on reducing greenhouse gas emissions and fossil fuel consumption. Accordingly, the electrification of private and public transportation systems, e.g., through the use of EVs, is a crucial step towards achieving a sustainable future and reducing the negative environmental impacts of traditional transportation methods. As of 2021, there were approximately 7.2 million EVs worldwide, with a record 3.2 million EVs sold during the COVID-19 pandemic in 2020. Furthermore, global sales of electric cars have kept rising strongly in 2022, with 2 million sold in the first quarter, up 75% from the same period in 2021. It is projected that this number will rise to 170 $\sim$ 245 million at the end of 2030, which can provide a noticeable surface for different types of EV-based attacks [4].

Indeed, large-scale deployment of EVs provides power grid operators with several opportunities, such as bidirectional energy transfers and frequency and voltage ancillary services, that can improve the reliability and efficiency of power grids. However, to fully realize these advantages for EV ecosystems and power grids, information and communication technologies (ICTs) in the EV

infrastructure and smart power grids must be widely employed[5]. Moreover, the EV supply equipment (EVSE) network, which includes charging stations, relies on various Internet of Things (IoT) devices and smartphone applications to facilitate the charging process for EV users[6]. However, the widespread deployment of cyber devices and information technologies makes the EV ecosystem vulnerable to cyber attacks in the real world, including data manipulation, malware, and intrusions [7]. Attackers can maliciously exploit physical and wireless vulnerabilities in EV ecosystems to impact the EV charging process, to severely damage the stability of power grids, even in the presence of renewable energies[8]. The increasing use of high-power EV chargers and the growing number of EVs on the road have prompted researchers to consider the impact of EV loads on the stability of power grids[2]. In some research papers [9, 10, 11], the impact of load-altering attacks (LAAs) originating from cyber layers of the EV ecosystem has been only investigated without proposing effective detection and mitigation methods. On this basis, potential vulnerabilities in the EV ecosystem, which can be maliciously exploited by adversaries to impact the stability of power grids, should be first investigated. Then, model-based or learning-based methods must be developed for the estimation of EV-based attack vectors in a timely manner. Finally, wide-area damping controllers can be suggested to alleviate the impacts of such attack vectors on the stability of power grids.

1.2 State of The Art

The negative impacts of load-altering attacks (LAAs), which actually change consumers' power consumption, on power grid stability have been investigated in several existing studies[12, 13, 14]. These LAAs can be categorized into static, dynamic, and switching attacks. Reference [13] investigates a static LAA, in which a portion of aggregated high-wattage loads is manipulated to impact the power grid operation and cause blackouts. A dynamic LAA— which is crafted using specific states of the smart grid, i.e., the frequency of the grid—can impact the stability of the closed-loop system by transferring the lightly-damped modes of the system to the unstable area [14]. Switching attacks are another type of LAAs that excite unstable and lightly-damped modes of the power grid aiming to

cause unacceptable frequency deviation and oscillatory behaviours in the systems [12, 10, 11]. Several recent studies in the literature have shown that cyber-physical attacks can be launched from the EV ecosystem by compromising potential vulnerabilities and attack vectors, leading to critical problems in power grids [9, 15, 16]. One of the most frequent types of these threats is the load-switching attack, which has been analyzed and investigated in several papers [17, 12, 10, 11]. In [17], the authors demonstrated how, through a successful cyber intrusion and by having some knowledge about the grid, an adversary can compute and apply a coordinated switching sequence to a circuit breaker to disrupt the system's operation within a short interval of time. A coordinated switching attack—that targets loads of the two-area Kundur benchmark—is implemented in [12] to drive a group of synchronous generators (SGs) out of step and create inter-area instability. In reference [10], authors leveraged the EV ecosystems and aggregated EV loads to launch switching attacks on power grids. Moreover, authors in [11] developed a learning-based detection method in the cloud management system along with an H^{∞}-based mitigation approach to address the EV security issues. Recently, some researchers have developed a real-time co-simulation test-bed that emulates the components of the EV ecosystem and studies the impact of EV-based attacks on power grid stability [2]. In another work [8], a virtualization environment, which has been developed by the Hydro-Quebec research team, consists of a transmission system simulator, a distribution network simulator, and an EV ecosystem emulator. This environment studies the impacts of compromising aggregated EV loads in distribution networks that can be propagated into transmission system behaviours. It has been shown that the impact of cyber attacks on EV loads at the distribution networks can be seen as a disturbance in the frequency and voltage of the transmission buses. Based on two technical reports [18, 19] from SANDIA National Laboratories, the impacts of compromising EV loads at the distribution levels on the stability of transmission systems, have been illustrated by several practical examples. On this basis, it is important to investigate the impacts of EV-LAAs on the stability of power grids.

1.3 Targeted Research Gaps

Inspired by the above discussion, several research gaps can be investigated as follows:

- The impact of EV-LAAs on the inertia-area stability of the power grid has been studied by several works. New surfaces of these switching attacks can be developed that can lead to other instabilities in a power grid, e.g., subsynchronous resonance events.
- Introducing reconnaissance techniques that can be applied to obtain instability oscillation modes of the power grid in a stealthy manner instead of short circuit faults and apparent methods of obtaining information.
- Developing new strategies for issuing malicious charging and discharging commands in charging stations with the aim of more destructive impacts on the frequency and voltage response of power grids.
- Estimating EV-LAAs vectors through model-based methods during the availability of system parameters, or machine learning-based approaches during the availability of historical data.
- Introducing wide-area damping controllers in the mitigation phase to deliver the best performance in case of load-altering attacks.
- Studying EV-LAAs in the presence of renewable energy sources, e.g., wind farms, during different uncertainties in the power grids.
- Developing a security metric for potential attack vectors in EV ecosystems and their impacts on the stability of power grids.

1.4 Research Contributions

Based on the identified gaps, we make the following contributions which are explained briefly here and will be expanded in four chapters through this thesis.

1.4.1 Electric Vehicle Switching Attacks Against Subsynchronous Stability of Power Systems

In Chapter 3, first, the cyber-physical connections between the EV ecosystem and the power grid are discussed to represent a threat model for coordinated electric vehicle switching attacks (EVSAs)

that can excite the torsional modes of the system. Then, it will be demonstrated that a traditional proportional-integral (PI)-based subsynchronous resonance damping controller (SSRDC) cannot stabilize the power grid. With the help of a customized unknown input observer (UIO), an adaptive control framework is developed based on a model predictive control (MPC). This framework can generate online control signals and add them to the internal control framework of the synchronous generators (SGs). A modified IEEE Second Benchmark (M-IEEE-SBM) is used to demonstrate the EV-LAAs' consequences and evaluate the effectiveness of the developed adaptive technique. The proposed strategy is also studied through real-time simulations under a testbed that integrates a virtual sphere (vSphere) for an EV ecosystem with power grids simulated in a real-time simulator (i.e., OPAL-RT 5650). To demonstrate the feasibility of this switching attack vector in an actual power system and its impact on SSR stability, the Palo Verde Nuclear Generating Station (PVNGS) is also simulated in this real-time simulator, and the effectiveness of the proposed adaptive control framework is validated under the EV-LAAs.

1.4.2 Deep Learning Detection and Robust MPC Mitigation for EV-Based Load-Altering Attacks on Wind-Integrated Power Grids

Due to the high penetration of wind energy in traditional power systems, Chapter 4 studies the impact of the EV-based load-altering attacks (EV-LAAs) against the subsynchronous control interaction (SSCI) of the wind-integrated power grid. First, the cyber-physical connections between the EV ecosystem and the power grid are discussed in detail to represent a threat model for coordinated EV-LAAs that can excite the SSCI modes of the system. Then, a convolutional neural network (CNN) is trained based on data from phasor measurement units (PMUs) at wind farm substations for detecting this attack, separating it from benign events, e.g., fault or line disconnection, and estimating attack vectors. The developed CNN detection model may neglect a few EV-LAAs due to the huge number of attack vectors with different combinations of amplitudes and frequencies during uncertainties in wind speeds and the number of WTG outages, leading to generating false negatives. As such, a robust model predictive controller (RMPC) is developed as a supplementary solution for mitigation purposes based on linear-matrix inequalities (LMIs). Possible uncertainties in wind speed and wind turbine generator (WTG) outages during different amplitudes of EV-LAAs

are investigated when defining these LMIs. The performance of mitigation schemes is evaluated and compared with recent wide-area damping controllers, e.g., the two-degree freedom (2DOF), linear quadratic regulator (LQR), and H_∞ under the co-simulation of EMTP-RV and MATLAB/Simulink.

1.4.3 Developing a Security Metric for Assessing the Power Grid's Posture against Attacks from the EV Charging Ecosystem

After studying the impact of load-altering attacks originating from EV ecosystems on the stability of power grids, we have decided to design security metrics for power utilities to provide information about the security status of the systems. On this basis, Chapter 5 develops a metric that captures the security posture of EV ecosystems, considering the possible attacks and their associated impacts on distribution grids. First, potential attack graphs are obtained to show the connections between the adversaries' access points and the consequences of attack vectors. Then, a Markov decision process (MDP) tree is generated, using probabilities of adversaries' success rates for a specific attack vector and unique reward functions. The developed MDP tree is then resolved by a policy iteration algorithm to calculate the value function of each state, related subsequent adversarial actions from the attackers' viewpoint, and quantify the security posture of each state. Finally, using the obtained metric, a deep convolutional neural network (CNN) is trained offline to notify the distribution system operators (DSOs) of the security status of EV ecosystems, i.e., secure and alarm situations. DSOs can use the developed security metrics to design consequent corrective actions during critical cyber-attacks. To demonstrate the usefulness of the proposed security metric in quantifying the security status of the grid, a cyber-physical testbed is built. This testbed integrates a virtual sphere (vSphere) to simulate the cyber parts of the EV ecosystem as well as a real-time simulator to model two distribution networks, i.e., IEEE 33- and 141-bus, under DSO control center based on IEC 61850. For a distribution network with dynamic sections that can be created using the operation of tie-switches, a supplementary strategy has also been suggested. This strategy is evaluated under the IEEE 69-bus distribution network to calculate the related security metric and update the security monitoring framework.

1.4.4 Designing a Security Metric for EV-based Load-altering Attacks in Transmission Systems

Lastly, Chapter 6 uses the measurements of the transmission grid and information on its cyber layer to derive a security metric that can be used for diagnosis and condition monitoring of the transmission grid's security state. First, common vulnerabilities in EV ecosystems are analyzed to devise related attack graphs. Afterward, a Markov decision process (MDP) tree is established based on the obtained attack graphs to display the possible attacker's actions and their detrimental consequences. In this MDP, to calculate the probabilities of adversaries' success in each branch, a customized common vulnerability scoring system (CVSS) is developed. Furthermore, control input and measurement signals are used to identify the transmission systems' model. Using this model, the damping ratio, controllability, and observability of low-damping modes, as well as the number of compromised charging stations, can be obtained for calculating the terms of a reward function. The generated MDP tree is resolved by the Epsilon-Greedy Q-learning algorithm to calculate the value of each state in the MDP tree and the related optimal adversarial action. This metric is integrated into a back propagation neural network (BPNN) to provide a security monitoring framework for attacks originating from the EV ecosystem. The security monitoring framework is evaluated on a testbed to demonstrate its usefulness in quantifying the security status in the case of EV-LAAs. This testbed consists of a virtual sphere (vSphere) of an EV ecosystem with the New England 39-bus transmission system simulated in a real-time simulator (RTS).

1.5 Thesis Organization

The remainder of this thesis is organized as follows:

- **Chapter 2**: provides information about the cyber layers of EV ecosystems, potential vulnerabilities in such ecosystems, attack graphs related to attack vectors, and impact of EV-based attack on operation of power grids.
- **Chapter 3**: studies the impact of EV-based load altering attacks on the resonance stability of power grids and introduces an adaptive framework to mitigate their impacts.

- **Chapter 4**: investigates the impacts of load-altering attacks originating from EV ecosystems on the stability of wind-integrated power grids. Then it provides a machine-learning based model for detection and robust controller for mitigating these attacks.
- **Chapter 5**: defines a new metric for power grid utilities during EV-based attacks and designs an security monitoring framework to provide information about security status of distribution networks.
- **Chapter 6**: extends the security metric for transmission system in the presence of the load-altering attacks originating from EV ecosystems.
- **Chapter 7**: concludes the thesis and provides the possible future works.

Chapter 2

Background

This section first illustrates a layout of the physical and cyber layers of the EV ecosystem, which is supplied through a power grid. Then, vulnerabilities in cyber layers, which attackers can maliciously compromise to disrupt the performance of charging stations, are represented. Full attack graphs for vulnerable points in the EV ecosystem are obtained to show how attackers can penetrate this ecosystem and impact the stability of power grids. Finally, some recent cyber attacks that originated from EV cyber layers with the aim of disrupting the performance of power grids will be discussed.

2.1 Generic EV Ecosystem Model

EV ecosystems are connected to distribution networks and encompass a cyber-physical model with cyber and physical layers that are tangled together in an interdependent manner. In order to facilitate interactions between EV consumers and power grids, these ecosystems consist of essential elements that have been depicted in Fig. 2.1. In this configuration, EVCSs, which serve as an interface between the charging station management system (CSMS) and EVs, are IoT devices that host management firmware. EVCSs are generally categorized into three different categories based on their charging rate: (i) Level-1 chargers with a charging rate of 1.4 kW; (ii) Leve-2 chargers with a charging rate of up to 40 kW; and (iii) Level-3 direct current fast chargers with a charging rate of 40kW to 240 kW [5]. The communication protocol between the CSMS and EVCS is the open

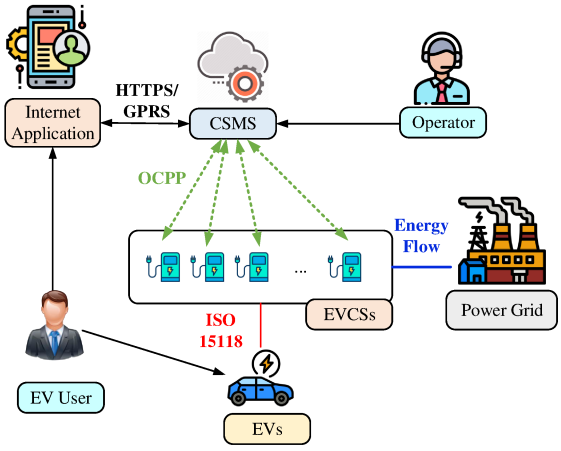


Figure 2.1: Overall layout of cyber and physical layers of EVs ecosystem in distribution networks connected to power grids.

charge point protocol (OCPP). EV users can also be notified of EVCS status and the availability of charging stations using smartphones and web applications that communicate with the CSMS using HTTPS/GPRS. EVs can communicate with EVCSs via the wired communication layer of a control area network (CAN) bus or power line communication (PLC) using the ISO 15118 protocol[15]. The energy required for the charging process will be provided to EVCS by the power grid based on the demand of users. The grid also supplies the required energy for this process (and other loads) using its generation units, which are often synchronous generators along with different RESs, e.g., wind farms and solar parks. The attacker can observe some of these inter-dependencies using mobile/web applications of the EVCS vendors and the CSMS that manage the interaction between EVCSs and EVs.

2.2 Common Vulnerabilities in EV Ecosystems

In this ecosystem, some vulnerabilities can be maliciously exploited to manipulate EV charging stations and impact the stability of the power grid. These adversarial actions are:

1) The OCPP, which enables the CSMS to remotely manage and control public EVCSs in different parts of power grids, can be potentially defined as one entry point for the adversary. Different

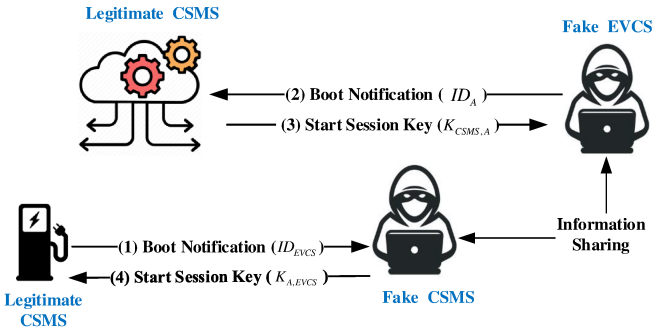


Figure 2.2: Attack against TLS session in OCPP V_2.0.1.

versions of OCPP, i.e., V_1.5, V_1.6, and V_2.0.1, have been released in 2012, 2015, and 2018, respectively [16]. Among these protocols, V_1.6 is the most commonly-used one in the industry and is built on top of a simple HTTP protocol with optional transport layer security (TLS). The last version is OCPP V_2.0.1, which benefits from several security improvements, e.g., secure firmware updates and mandatory usage of TLS. However, this mandatory usage of TLS does not provide security measures to mitigate man-in-the-middle (MitM) attacks [20]. In other words, TLS cannot provide long-term authenticity, non-repudiation, and secure certificate validation that allows adversaries to launch the MitM attack[16]. Algorithm 1 shows how attackers can launch the MitM in the presence of TLS in the latest version of OCPP V_2.0.1. The adversaries can deceive EVCS into accepting the communication as if it is communicating with a legitimate CSMS. At the same time, they can trick the CSMS into ensuring legal communication with EVCS. As a result, EVCSs can be fully controlled by the attacker while the CSMS is oblivious to the real status of the compromised EVCS. In Fig.2.2, the attacker successfully establishes 2 session keys, i.e., $K_{CSMS,A}$ and $K_{A,EVCS}$, for the encrypted TLS communication with the CSMS and EVCS, respectively. It should be noted that in most cases, operators also remove the TLS due to overhead and operational costs. Therefore, regardless of releasing new versions of OCPP, versions V_1.5 and V_1.6 have remained the dominant protocols in EV ecosystems due to the increased cost of switching from existing protocols to OCPP V_2.0.1[20].

2) Cyber vulnerabilities in frequent and well-known CSMS, e.g., EV-Link and CSWI Etrel, allow adversaries to compromise the EVCS and manipulate the characteristics of charging station commands, such as their initiation or stop times, creating delays in the charging and discharging

Algorithm 1: MitM Attack on TLS in OCPP V_2.0.1

1) EVCS $\rightarrow$ **A:** Communicating with attacker (**A**) as 'faked CSMS'

\# **A** tricks EVCS into connecting with him instead of real CSMS

2) A: Acquiring EVCS ID and timestamp

3) A $\rightarrow$ **CSMS:** Communicating with CSMS

\# **A** deceives CSMS into connecting with him instead of real EVCS

4) CSMS: Computing parameters and generating session key

5) CSMS $\rightarrow$ **A:** Responding to **A** as faked EVCS in TLS connection

\# Session key are exposed to attacker (**A**)

6) A: Computing parameters and related TLS session key $K_{CSMS,A}$

7) A $\rightarrow$ **EVCS:** Responding to EVCS for the connection in TLS

8) EVCS: Accepting connection with **A** and freshness of the message

9) A : Obtaining the session key $K_{A,EVCS}$

10) A: Switching on/off EVCS and launching EV-based attacks;

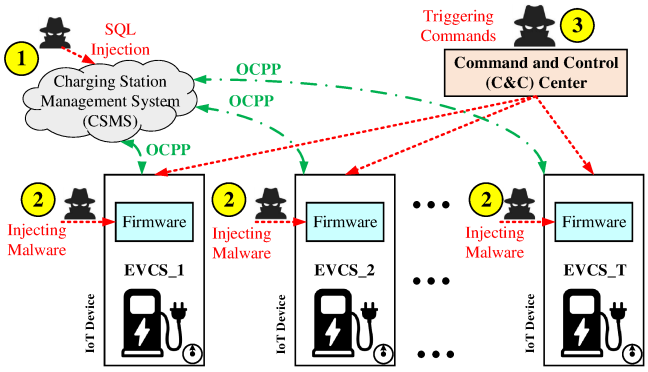


Figure 2.3: Obtaining privileged access to the CSMS, performing firmware manipulation in EVCSs.

actions. As a result, CSMS can be targeted by adversaries to acquire administrator access to the CSMS using the SQL injection technique[21]. Then, the attacker can downgrade the firmware of the CSMS by uploading a less secure version and then injecting malware into the targeted firmware of EVCSs similar to other IoT devices [22] to issue fake charging and discharging commands [8]. These fake commands can be triggered by an attacker's command and control (C&C) center in a coordinated manner[23]. Fig. 2.3 shows how adversaries can obtain privileged access to the CSMS and perform EVCS firmware manipulation with the aim of impacting the stability of power grids.

3) Mobile and web applications can communicate with the CSMS and allow EV users to remotely charge and discharge their EVs and use functionalities, such as start/stop charging sessions, payments, and locating charging stations, to name a few. On this basis, these applications can also be defined as a new access point for EV-based attacks on EV loads in EV ecosystems that can disrupt

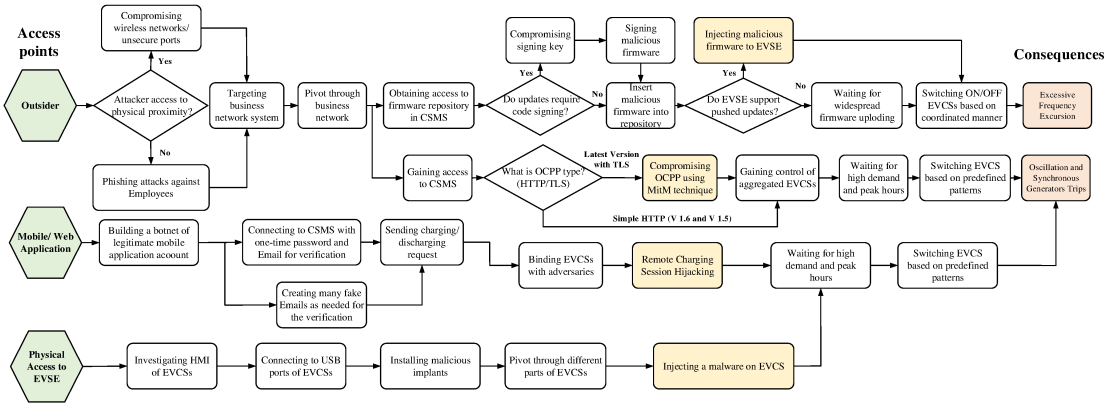


Figure 2.4: EVSE Ecosystem attack graph for four different access points, i.e., CSMS, OCPP, mobile and web applications, and physical USB ports.

the operation of distribution networks[24].

4) Adversaries can target public EVCSs using vulnerable physical points, e.g., Universal serial bus (USB) ports, Ethernet ports, and touchscreens mounted outside of EVCSs. As an example, USB ports can be used for changes in the configuration of EVCSs and charging station data manipulation. Recently, EVCSs in a council's car parks have been hacked to show an unrelated website on their screens[25], or Russian electric vehicle chargers have also been hacked to display messages supporting Ukraine [26]. Additionally, attackers can modify and update the existing firmware of EVCSs. Although these cyber intrusions can be carried out physically, they can also be initiated through remote access.

2.3 Attack Graphs and Consequences

The steps, that can be taken by adversaries to move from a system or network access point to consequent and destructive impacts on power grids, can be shown through attack graphs[18]. These attack graphs can be devised based on information about the topology of cyber layers, publicly available information regarding vulnerabilities, and knowledge about techniques and procedures used by adversaries[19]. Different attack graphs can be defined in EV ecosystems that show how adversaries can take steps to penetrate cyber layers and jeopardize the confidential information of EV users and the stability of the power grid. Based on the proposed vulnerabilities in EV ecosystems, an overall layout of attack graphs that connected adversarial actions to impacts on distribution networks has

Table 2.1: Cyber attacks on EV charging and impacts on power grids.

Reference	Threat	Impacts on power grids
[7]	Existing public data on power grid and EV ecosystems	Over frequency and cascading blackouts
[27]	Control systems of EVCSs	Low power factor, harmonic distortion and frequency instability
[28]	EV botnet	Under voltage and overloads in lines
[29]	EV botnet	Under-frequency events and power outages

been illustrated in Fig. 2.4.

2.4 Impacts of EV-based Attacks on Power Grids

Attackers can exploit physical and wireless vulnerabilities in EVs, EVCSs, or both to impact the EV charging and discharging actions and damage the stability of the power grid. For example, a data-driven attack mechanism was developed in [7] that has caused frequency instability by manipulating EVCS demands. The proposed attack benefited from publicly accessible EVCS and power grid data that allowed for a prior evaluation of the worst-case attack impact on the power grid. In another work, [27], the impacts of the cyber attacks on the EVCS control system on power quality were studied. In this cyber intrusion, coordination between different converters and power conditioning units of a 50 kW DC EVCS was interrupted, leading to unacceptable total harmonic distortions in the EVCS current fed by the power grid with a relatively low power factor. Furthermore, in [28], attackers have designed a botnet with the aim of comprising EVs and fast-charging direct current stations and interrupting the power grid. This research investigated 33-bus and 39-bus IEEE distribution and transmission networks, as well as real-life EV mobility and charging data obtained from the Toronto Parking Authority in Canada. Simulation results showed that the EV botnet could create under-voltage events and power outages in some parts of the mentioned networks. In [29], another botnet is investigated that consisted of 7 kW residential L2 EVCSs to create under-frequency outages in the California region as a part of the Western interconnection of the US power grid. The outcome of this study is that this botnet will need to simultaneously shut down 12% EVs in California to cause a frequency drop of 0.5 Hz, which is sufficient for triggering under-frequency alarms in the western interconnection. Table 2.1 summarizes the studies dedicated to the analysis of cyber attacks on the power grid that exploit vulnerabilities in EV ecosystems.

Chapter 3

Electric Vehicle Switching Attacks Against Subsynchronous Stability of Power Systems

3.1 Motivation

Wide-area power grids inherently have several physical vulnerabilities, i.e., resonance conditions, which can result in growing oscillations in system parameters, such as voltage and angular speed of generators. Among these instability issues, a frequent one is a subsynchronous resonance (SSR) that is created between components of synchronous generators, e.g., their mechanical structure, and fixed series capacitors in the power grid. The oscillations resulting from this resonance occur at frequencies lower than the grid's nominal frequency, e.g., between 5 and 55 Hz in a 60 Hz power grid. It is worth mentioning that fixed series capacitors are deployed in transmission lines to enhance the power transfer capacity and improve the voltage profile [30]. The first reported case of SSR occurred at Mohave Power Station in Arizona. In this incident, the generator shaft was subjected to a continuously increasing torque that finally led to a shaft fracture[31]. The rotors of two turbo-generators cracked due to SSR at the Dresden nuclear power plant in 2004, and several SSR

events also occurred at the Yimin power plant in China, which led to the shaft fracture of a turbo-generator in 2008 [32]. These potential real-world SSR instability events, along with EV charging stations that are widely distributed among power system loads, can persuade adversaries to compromise cyber vulnerabilities in the EV ecosystem and switch a portion of controlled EV loads with a specific frequency to excite *torsional modes* of steam turbine generators and create SSR events. Despite the numerous studies that have focused on designing SSR damping controllers (SSRDCs) to resolve SSR issues [33], their performance is only evaluated following abrupt one-time events in power grids, e.g., faults or line outages. Since the impact of continuous external events has been ignored in the framework of these controllers, they cannot generate online control input signals during LAA vectors, making them inadequate frameworks for mitigating continuous cyber events, such as EV-LAAs propagated into transmission systems[34, 35]. To the best of the authors' knowledge, an online attack vector estimation and adaptive mitigation technique for EV-LAAs, which excite torsional modes of the power grid, has not been studied yet.

3.2 Contributions

Inspired by the above discussion, this paper investigates a new family of EV-LAAs that originate from switching aggregated EV loads in distribution networks but impact the operation of transmission grids, create SSR conditions, and damage generators' mechanical parts. This switching attack vector is launched through manipulation of CSMS and changes in the EVCSs' firmware with the aim of injecting malicious malware into the targeted firmware of the EVCSs and sending fake charging and discharging commands in a coordinated manner. Initially, it will be demonstrated that the conventional PI-based damping controller cannot mitigate coordinated EVSAs due to ignoring external events in the state-space model of the system. Thus, by customizing an unknown input observer (UIO), which can estimate the system's state variables and components of the switching attack vector in a timely manner, an adaptive control framework is developed based on a model predictive controller (MPC) during continuous events. The MPC, with its multi-input and multi-output structure, is also suitable for a wide-area control framework. This controller can generate online and optimum control input signals by solving optimization problems, and add these supplementary

signals to the internal control framework of the synchronous generators (SGs). This collaboration between customized UIO and MPC to mitigate the implications of EV-LAAs is studied under a modified IEEE second benchmark model (M-IEEE-SBM). To show the impacts of EV-LAAs on the SSR stability of real power grids, the Palo Verde Nuclear Generating Station (PVNGS) is also simulated to validate the proposed attack vector estimation and adaptive mitigation technique for coordinated EVSAs. In summary, the main contributions of this paper are:

(1) Introducing a coordinated EV-LAAs that aims to excite the unstable or lightly-damped torsional modes of power grids based on a feasible threat model and demonstrating the incapability of a frequent type of SSRDCs, i.e., a PI-based damping controller, in mitigating this attack;

(2) Developing a UIO to update the system state variables and estimate components of the switching attack vector in a timely manner;

(3) Combining the developed UIO with an MPC framework to suggest an adaptive control technique for updating the system model and mitigating continuous switching attacks through generating online control input signals in the form of a wide-area damping controller. To demonstrate the impacts of EV-LAAs on the SSR stability of a real power grid, the PVNGS is simulated, and the effectiveness of the proposed adaptive technique is validated under this switching attack.

Threat Model for Switching Attack Vector

3.3 Threat Model for Switching Attack Vector

In this research, the proposed threat model is described as follows: **(i) Attacker's Objective:** The aim of adversarial actions is to create SSR oscillations, damage the turbo-generator shaft of a synchronous generator, and cause the outage of generation units, which can result in a mismatch between load and energy production capacity. **(ii) Attacker's Knowledge:** In a wide-area power grid that includes EV infrastructure, several pieces of information, i.e., the location and the total number of available charging stations as well as their charge rating, are entirely available for public use. As a result, attackers can monitor the interaction between the EV ecosystem and power

grids through mobile and web services for EVs or through the CSMS that is connected via OCPP to EVCSs. Furthermore, launching this EV switching attack requires a model of the power grid and the calculation of unstable modes. Such modeling needs parameters of the power grid, which can be obtained by gathering public knowledge about the power grid [7], reconnaissance activities [10], or developing system identification methods in control engineering [11]. **(iii) Attacker's Actions:** First, adversaries obtain privileged access to the CSMS, for example, through SQL injection, change the firmware of EVCSs to inject malware into the firmware and build switching attack vectors as outlined before in Section Background. Then, they will obtain the mathematical model of the grid using system identification methods and create an oscillatory behavior in the EV charging/discharging commands to excite the torsional modes of the system. **(iv) Formulation of EV Loads Switching Attacks:** Two mathematical equations for making components of the related switching attack vector are represented, i.e., sinusoidal and ON/OFF patterns. Based on (1) and Fig. 3.1. (a), the aggregated EV loads in distribution networks are manipulated and switched by a sinusoidal pattern, whose frequency is equal to the torsional mode of the power grid. The component of the switching attack vector for a sinusoidal EV load pattern is represented as follows:

$$A_{sin\_atck}(t) = \Delta P_{EV} \sin(2\pi f_{TM} t + \varphi) \tag{1}$$

where ΔP_{EV} is defined as the active power of EVCSs that are targeted by attackers for switching attacks. f_{TM}, t_{sw}, and φ are the torsional mode frequency, the period of EVSA, and the phase shift of the sinusoidal switching attack, respectively. Fig. 3.1. (b) shows aggregated EV loads that are switched based on the ON/OFF (charging/discharging) pattern with the torsional mode frequency. The related components of a switching attack vector for a specific area are:

$$A_{on\_atck}(t) = \begin{cases} \pm\Delta P_{EV} : 0 \leq t \leq D_{sw} t_{sw} \\ 0 : 1 - D_{sw} t_{sw} \leq t \leq t_{sw} \end{cases} \tag{2}$$

where D_{sw} is the duty cycle of attacks. To launch this attack, the number of required EVCSs for charging or discharging commands is calculated at each sampling time T_s:

$$N_{EVCS\_p} = \left\lfloor abs(\frac{\Delta P_{EV}(T_s)}{P_{n\_EVCS}}) \right\rfloor + 1 \tag{3}$$

where P_{n_EVCS} is the nominal power rate of the EVCS. The total number of EVCSs that are available in each area should surpass the number of required EVCSs for building the components of the

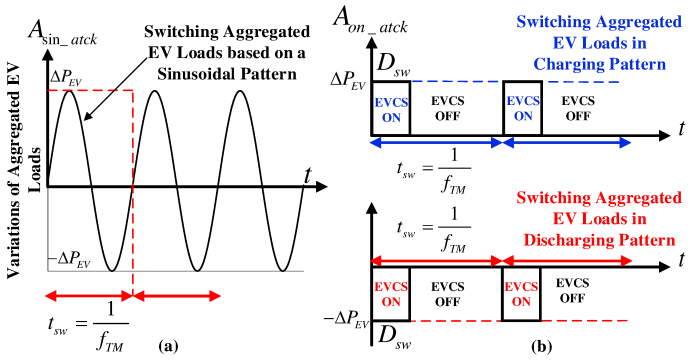


Figure 3.1: (a) Switching aggregated EV loads based on sinusoidal patterns (b) Switching aggregated EV loads based on charging/ discharging patterns.

Algorithm 2: Designing Components of ON/OFF Switching Attack Vector

Calculate: Frequency of torsional modes (f_{TM}) based on Threat Model

Initialize: $t_{sw} = \frac{1}{f_{sw}}$ as period of switching attack vector and T_s as sampling time

Select: Duty cycle of switching attack vector (D_{sw}) from 0% to 100%

Initialize: Nominal power rate of EVCS (P_{n_EVCS})

Initialize: Total number of available EVCSs (N_{EVCS_T})

Select: Number of cycles for repeating a switching attack vector ($Cycle$)

for $c = 1:1:Cycle$ **do**
  for $t = 0:T_s:t_{sw}$ **do**
    Determine ΔP_{EV} by attacker
    Calculate $N_{EVCS\_p} = \left\lfloor abs(\frac{\Delta P_{EV}(T_s)}{P_{n\_EVCS}}) \right\rfloor + 1$
    Ckeck first condition: $N_{EVCS\_T} \geq N_{EVCS\_p}$
    Ckeck second condition: $M_{C\&C} \geq \left\lfloor abs(\frac{\Delta P_{EV}(T_s)}{P_{n\_EVCS}}) \right\rfloor + 1$
    if $0 \leq t \leq D_{sw}t_{sw}$ **then**
      C&C center: Issue charging commnads for all N_{EVCS_p}
      if $1 - D_{sw}t_{sw} \leq t \leq t_{sw}$ **then**
        C&C center: Stop charging command for all N_{EVCS_p}
      end
    end
  end
  Build component of switching attack vector $A_{on\_atck}(t)$ for a specific area (2)
end

switching attack vectors:

$$N_{EVCS\_T} \geq N_{EVCS\_p} \tag{4}$$

Furthermore, the total number of charging or discharging commands that are triggered by the attacker's C&C during ($D_{sw}t_{sw}$), should not surpass N_{EVCS_p}, i.e.,

$$M_{C\&C} \geq \left\lfloor abs(\frac{\Delta P_{EV}(T_s)}{P_{n\_EVCS}}) \right\rfloor + 1 \tag{5}$$

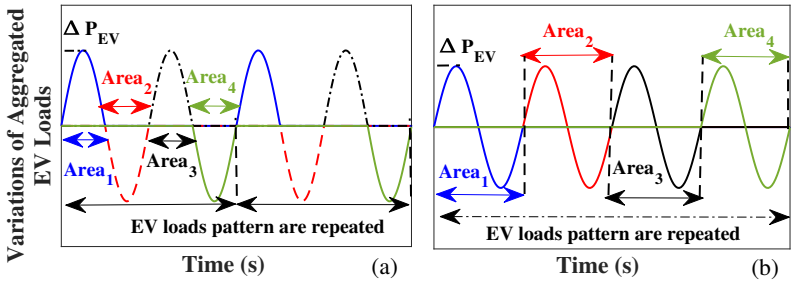


Figure 3.2: The pattern of changes in aggregated EV loads as EVSA for different 4 areas in a power grid: (a) attack model **A**, (b) attack model **B**.

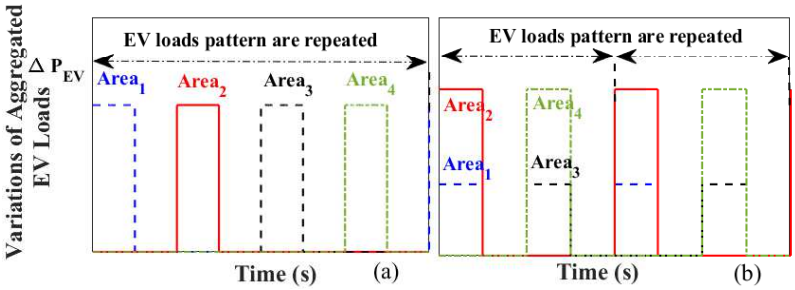


Figure 3.3: (a) ON/OFF (Charging and discharging) switching attack for 4 areas, (b) Pattern for dealing with amplitude problem of switching attack.

where $M_{C\&C}$ is defined as the communication capacity of the attacker's C&C in [23]. Algorithm 2 shows how adversaries can build components of a switching attack vector in different areas to impact the SSR stability of the power grid. **(v) Instruction for Implementing EV Loads Switching Attacks:** Since the frequency of torsional modes is relatively large ($f_{TM} < 60$Hz) compared to inter-area modes (0.1-1Hz) studied in [12], switching compromised EV loads can be carried out based on several strategies to reduce the switching attack's frequency and the amplitude of aggregated EV loads as follows: To deal with the frequency issue, aggregated EV loads of distribution networks can be switched at nominated areas with a sub-harmonic frequency of the torsional modes' frequency. This strategy can be divided into two subgroups for sinusoidal switching attacks, i.e., attack models **A** and **B**. In attack model **A**, the adversary divides the compromised power grid's areas (N_b) into N_p separate pairs. In each of these pair areas, the adversary manipulates aggregated EV loads based on a positive half-cycle of a sinusoidal pattern in the first area and a negative half-cycle in another area. This process continues for all the pair areas, and consequently, the frequency of participation for each area will be $f_{sw} = \frac{f_{TM}}{N_p}$, where f_{TM} is the frequency of the torsional mode. For instance, Fig. 3.2. (a) shows the attack model **A** for a four-area power grid, which has two pairs

of areas. In the attack model $\mathbf{B}$, adversaries manipulate EV loads based on full sinusoidal patterns in each area, one after the other, sequentially. In such a case, the frequency of participation for EVs in each area will be $\frac{f_{TM}}{N_b}$. This attack model for a 4-area power grid is shown in Fig. 3.2. (b). The attack model $\mathbf{B}$, where the attacker manipulates EV ecosystems and only turns ON/OFF the aggregated EV loads in different areas based on the frequency of torsional mode, is shown in Figs. 3.3. (a). To deal with the amplitude issue, the adversary can slightly change the attack models $\mathbf{A}$ and $\mathbf{B}$ by grouping existing areas and launching the same attack. For instance, in the attack model $\mathbf{A}$, each pair can consist of a cluster of areas with aggregated EV loads instead of a single area. Fig. 3.3. (b) shows the attack strategy $\mathbf{A}$ when an adversary switches ON/OFF a cluster of aggregated EV loads, e.g., Area_1 and Area_2 in one cluster and then Area_3 and Area_4 in another cluster. As a result, the amount of required EV loads for launching the proposed EV-LAAs decreases at the cost of increasing the frequency of switching.

3.4 Modeling SSR under EV-based Load-altering Attacks

The IEEE-SBM is often used for SSR studies in the literature [36]. Although this test system represents a small-scale transmission grid, larger grids can be converted to a similar model using the Thevenin equivalent technique. Thus, to investigate the impact of EV-LAAs in a coordinated manner on SSR events discussed in 3.3, the IEEE-SBM is extended to four areas that consist of equivalent synchronous generators (SGs), distribution networks with aggregated EV loads connected to EVCSs, transmission lines compensated by the series capacitor, OCPP communication, and CSMS as shown in Fig. 3.4. Each area of the power grid is assumed to have a total of 200 MW of different loads. Using the similar ratio for EVs to the total loads represented in [7] for the realistic case of the Manhattan grid in the U.S., we assumed that roughly 70,000 EVs exist in each area of the power grid. According to the International Energy Agency (IEA), governments and operators tend to maintain an average of 1 public EVCS for every 10 EVs on the road [4], which results in having 7,000 EVCSs in our grid. Assuming 24 kW as the average global charging rate of EVCSs [4] and approximately 30% chance of being compromised by adversaries, each of the areas will have around 50 MW as feasible aggregated EV loads for EV-LAAs. It is supposed that each area delivers 540 MW

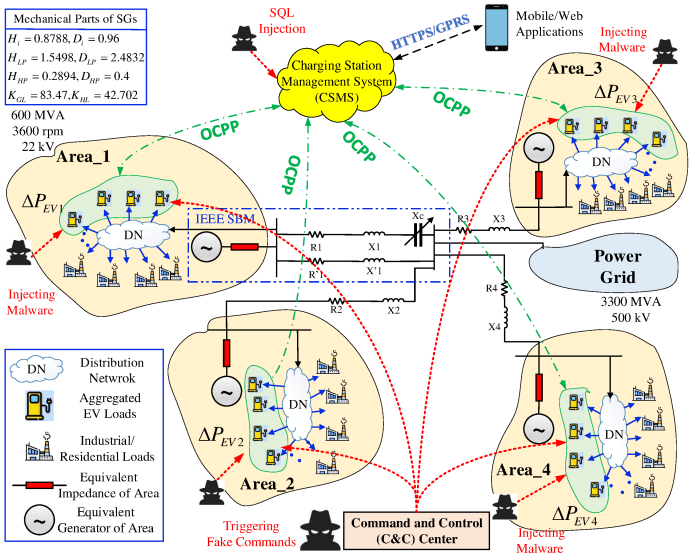


Figure 3.4: Modified IEEE Second Benchmark model for SSR studies.

of power to the transmission system, and 52% series capacitor compensation is considered for one of the parallel transmission lines. The state-space model of the modified IEEE-SBM is calculated by combining the differential equations of SGs, PSS, excitation system, mechanical parts of steam turbines, i.e., high-pressure (HP) and low-pressure (LP) sections, and series-compensated transmission lines [37]. To design damping controllers for multi-machine power grids, small-signal models, e.g., Heffron–Phillips, which are obtained by linearizing the differential equations, are frequently employed [38]. The small-perturbation transfer function of the Heffron–Phillips model along with the mechanical sections of the steam turbine governor to investigate the SSR events in the presence of EV-LAAs have been illustrated in Fig. 3.5. In this configuration, differential equations, which describe the angular speed of mechanical parts and consider torsional modes of the power grid for SSR studies, can be expressed as follows:

$$\begin{cases} \Delta\dot{\delta}_{LPi} = \omega_s \Delta\omega_{LPi} \\ \Delta\dot{\omega}_{LPi} = \frac{K_{GLi}}{2H_{LPi}}\Delta\delta_i - (\frac{K_{LHi}+K_{GLi}}{2H_{LPi}})\Delta\delta_{LPi} - \frac{D_{LPi}}{2H_{LPi}}\Delta\omega_{LPi} \\ + \frac{K_{LHi}}{2H_{LPi}}\Delta\delta_{HPi} \end{cases} \tag{6}$$

$$\begin{cases} \Delta\dot{\delta}_{HPi} = \omega_s \Delta\omega_{HPi} \\ \Delta\dot{\omega}_{HPi} = \frac{K_{LHi}}{2H_{HPi}}\Delta\delta_{LPi} - \frac{K_{LHi}}{2H_{HPi}}\Delta\delta_{HPi} - \frac{D_{HPi}}{2H_{HPi}}\Delta\omega_{HPi} \end{cases} \tag{7}$$

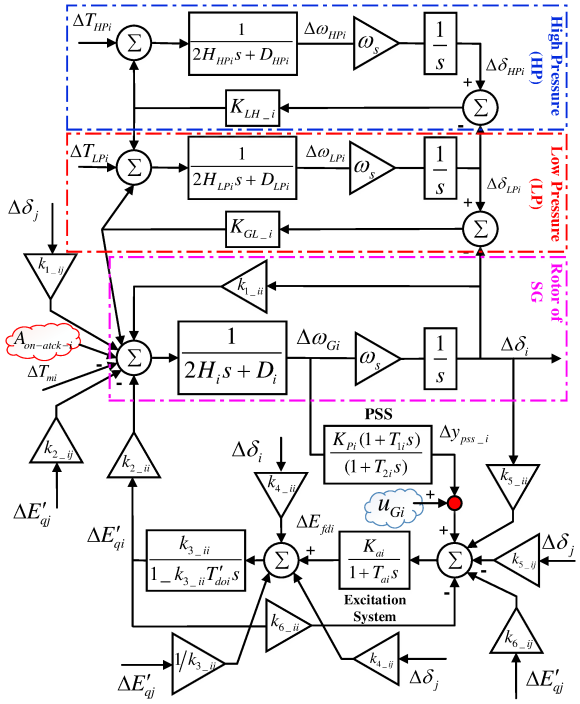


Figure 3.5: Dynamic block diagram of the multi-machine power grid to study SSR events crafted by components of EV-LAAs.

where $\Delta\delta_{LPi}$ and $\Delta\omega_{LPi}$ are the LP section's angle and speed deviations, respectively. Also, H_{HPi} and H_{LPi} are the inertia constants of the HP and LP sections for i^{th} machine, respectively. K_{GLi} and K_{LHi} are the stiffness of the shaft between the SG's rotor and LP as well as LP and HP sections, respectively. D_{HPi} and D_{LPi} are referred to as the damping coefficients of LP and HP sections for i^{th} machine. The parameters of these mechanical sections are represented in [37]. Furthermore, to represent the model of i^{th} synchronous machine in the presence of components of the switching attack vector, i.e., A_{on_atck}, the multi-order model is suggested along with modeling a PSS and excitation system:

$$\Delta\dot{E}'_{qi} = \frac{1}{T'_{doi}}\left(-\sum_{j=1}^{N}(k_{4\_ij}\Delta\delta_j) - \sum_{j=1}^{N}\left(\frac{1}{k_{3\_ij}}\Delta E'_{qj}\right) + \Delta E_{fdi}\right) \tag{8}$$

$$\begin{aligned}\Delta\dot{E}_{fdi} = {} & \tfrac{-K_{ai}}{T_{ai}}\sum_{j=1}^{N}(k_{5\_ij}\Delta\delta_j) - \tfrac{-K_{ai}}{T_{ai}}\sum_{j=1}^{N}(k_{6\_ij}\Delta E'_{qj}) \\ & -\tfrac{1}{T_{ai}}\Delta E_{fdi} + \tfrac{K_{ai}}{T_{ai}}\Delta y_{pss\_i} + \tfrac{K_{ai}}{T_{ai}}u_{Gi}\end{aligned} \tag{9}$$

$$\begin{aligned}\Delta\dot{y}_{pss\_i} = &-\tfrac{K_{Pi}T_{1i}}{2H_iT_{2i}}\sum_{j=1}^{N}(k_{1\_ij}\Delta\delta_j) - \tfrac{K_{Pi}T_{1i}}{2H_iT_{2i}}K_{GLi}(\Delta\delta_i)\\ &-\tfrac{K_{Pi}T_{1i}}{2H_iT_{2i}}\sum_{j=1}^{N}(k_{2\_ij}\Delta E'_{qj}) + \tfrac{K_{Pi}T_{1i}}{2H_iT_{2i}}(\Delta T_{mi}-A_{on\_atck-i})\\ &+\tfrac{K_{Pi}}{T_{2i}}(1-\tfrac{D_iT_{1i}}{2H_i})\Delta\omega_{Gi} - \tfrac{K_{Pi}T_{1i}}{2H_iT_{2i}}K_{GLi}(\Delta\delta_{LPi}) - \tfrac{1}{T_{2i}}\Delta y_{pss\_i}\end{aligned} \tag{10}$$

$$\begin{aligned}\Delta\dot{\omega}_{Gi} = &\tfrac{1}{2H_i}[D_i\Delta\omega_{Gi} - \sum_{j=1}^{N}(k_{1\_ij}\Delta\delta_j) - K_{GLi}\Delta\delta_i\\ &-\sum_{j=1}^{N}(k_{2\_ij}\Delta E'_{qj}) + K_{GLi}\Delta\delta_{LPi} + (\Delta T_{mi}-A_{on\_atck-i})\end{aligned} \tag{11}$$

$$\Delta\dot{\delta}_i = \omega_s\Delta\omega_{Gi} \tag{12}$$

where A_{on_atck-i} is defined as components of the switching attack vector ($\zeta(t)$) in Area$_i$ that is discussed in 3.3 and obtained from (1) or (2). $\Delta\delta_i$ and $\Delta\omega_{Gi}$ are the angle and speed deviations of the rotor, respectively. $\Delta E'_{qi}$ and ΔE_{fdi} are the internal voltage behind the d-axis transient reactance and equivalent excitation voltage, respectively. H_i and D_i are the machine inertia constant and damping coefficient, respectively. ω_s is the nominal synchronous speed. T'_{doi} is the d-axis open-circuit transient time constant and ΔT_{mi} is the mechanical torque. K_{ai} and T_{ai} are the automatic voltage regulator gain and time constant, respectively; k_{1_ij}–k_{6_ij} are the coefficients that can be obtained from the linearization of the algebraic stator equations and impedance of transmission lines in power grids. Δy_{pss_i} is the signal obtained from PSS for mitigation of oscillations. For a power system with N machines equipped with PSS and excitation systems, the state variables of i^{th} machine can be defined as follows:

$$\begin{aligned}x_i(t) = [\ &\Delta E'_{qi}\quad \Delta E_{fdi}\quad \Delta y_{pss\_i}\quad \Delta\delta_i\quad \Delta\omega_{Gi}\quad ...\\ &\Delta\delta_{LPi}\quad \Delta\omega_{LPi}\quad \Delta\delta_{HPi}\quad \Delta\omega_{HPi}\ ]^T\end{aligned} \tag{13}$$

where these variables can continue for $j = 1, .., N$ machine and interconnection between i^{th} and j^{th} machines should be also defined to make a comprehensive state variable vector $x(t)$. Finally, the state-space equations of the power grid can be summarized as follows:

$$\begin{cases}\dot{x}(t) = Ax(t) + Bu(t) + R_a\zeta(t)\\ \Delta\omega_G(t) = Cx(t) + Du(t)\end{cases} \tag{14}$$

where A, B, C, D, and R_a describe the state, control input, output, feed-forward, and EV-LAAs matrices, respectively. The output signals are the rotor speed deviation of four equivalent SGs, i.e.,

$$\Delta\omega_G(t) = [\ \Delta\omega_{G1} \quad \Delta\omega_{G2} \quad \Delta\omega_{G3} \quad \Delta\omega_{G4}\ ]^T \tag{15}$$

Control input signals—obtained from adaptive mitigation technique—are also added to the PSS of each equivalent generator of each area in an online manner, as shown in Fig. 3.5:

$$u(t) = [\ u_{G1} \quad u_{G2} \quad u_{G3} \quad u_{G4}\ ]^T \tag{16}$$

The $\zeta(t)$ is a switching attack vector that consists of some components. Each component of this vector is aggregated EV loads that are switched by intruders at nominated areas based on the suggested threat model and Algorithm 1. This vector is added to the state-space model of the power grid for sinusoidal switching attacks in four areas, as follows [11, 12]:

$$\zeta(t) = [\ A_{sin\_atck-1} \quad A_{sin\_atck-2} \quad A_{sin\_atck-3} \quad A_{sin\_atck-4}\ ]^T \tag{17}$$

From the state-space model, A can provide all modes of the system, where the real part of the torsional modes and their related frequency can be calculated as follows:

$$\sigma \pm j(2\pi f) = \det(\lambda I - A) \tag{18}$$

These torsional modes, which can be calculated by adding mechanical steam turbine equations (6 and 7) to the state-space model, have a low damping ratio. On this basis, EV-LAAs can be launched by adversaries with different strategies based on the proposed threat model to excite lightly-damped torsional modes of power grids and lead to SSR events. Using eigenvalue analysis, the torsional modes of the M-IEEE-SBM are $-0.29496 \pm j195.58$ with a damping ratio of 0.15% and torsional frequency of f_{TM1}=31.143 Hz, and $-0.062301 \pm j156.05$ with a damping ratio of 0.04% and torsional frequency of f_{TM2}=24.85 Hz. All modes of M-IEEE-SBM have been illustrated in Fig. 3.6 by the eigenvalue analysis.

In previous works, e.g., [34, 39], authors have introduced a traditional SSRDC based on PI control framework with the aim of SSR mitigation in power grids. This PI-based damping controller

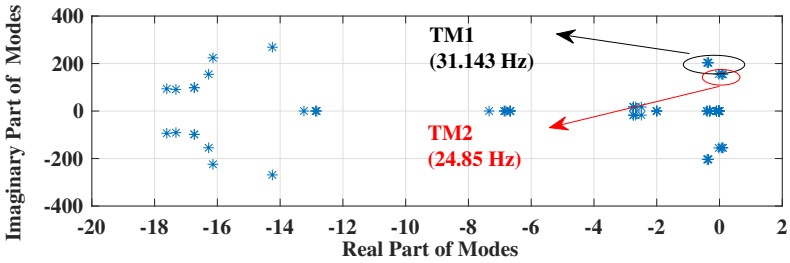


Figure 3.6: Eigenvalues analysis of M-IEEE-SBM for Torsional Modes (TM).

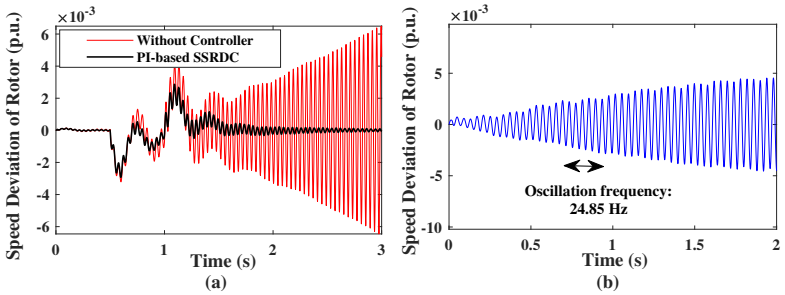


Figure 3.7: Rotor speed deviation of equivalent $G1$ (a) with and without PI-based damping controller during a line disconnection, and (b) with PI-based damping controller during EV loads switching attack.

can deliver an acceptable performance when the second line of the M-IEEE-SBM is disconnected and the SSR condition occurs. The deviation of the angular speed for the equivalent SG in Area_1 has been depicted in Fig. 3.7. (a). However, this controller can not perform well in the case of EV-LAAs with a frequency of 24.85 Hz using the strategy in Fig. 3.3. (a). To demonstrate the incapability of this controller, the angular speed of the rotor for $G1$ has been shown in Fig. 3.7. (b). Despite the acceptable performance of the PI-based damping controller in normal conditions, it cannot mitigate the impacts of continuous EV load switching attacks due to its limited design for a specific condition. On this basis, an adaptive and wide-area damping control framework can be developed with the integration of UIO and MPC to follow the components of the switching attack vector in a timely manner, update the state-space model, and then, generate the online and optimum control input signals to mitigate oscillations resulted from EV-LAAs.

3.5 Adaptive Technique for EV-LAA Mitigation

As before discussed, the previous damping controller cannot deliver acceptable performance in the case of continuous cyber events, e.g., EV-LAAs, that excite lightly-damped torsional modes

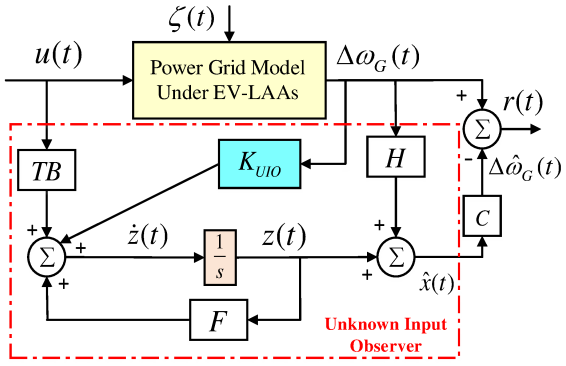


Figure 3.8: The structure of Unknown Input Observer.

due to their non-adaptive features. In this paper, with the help of a UIO, which can estimate state variables and components of a switching attack vector in a timely manner, an adaptive control framework can be developed based on model predictive control (MPC). This controller can generate online and optimum control input signals and establish an online method for mitigating the impacts of this attack on mechanical sections of SGs in the form of a wide-area damping controller. Benefiting from the control signals ($u(t)$) and output signals ($\Delta\omega_G$), the UIO can estimate the state variables that may not be possible or feasible for the system operator. Moreover, this observer can estimate components of the produced switching attack vector that can be used in the structure of the proposed wide-area damping controller. For the system defined in (14), the model of a UIO is customized as follows:

$$\begin{cases} \dot{z}(t) = Fz(t) + TBu(t) + K_{UIO}\Delta\omega_G(t) \\ \hat{x}(t) = z(t) + H\Delta\omega_G(t) \end{cases} \tag{19}$$

where $\hat{x}(t) \in R^{n\times 1}$ and $z(t) \in R^{n\times 1}$ are the estimated state variables vector and output variables of the UIO, and matrices F, T, K_{UIO}, and H are selected to design this observer [40]. A customized layout of the UIO is illustrated in Fig. 3.8. When the UIO (19) is applied to the (14), an estimation error, i.e., $(e(t) = x(t) - \hat{x}(t))$, is controlled using the following equation [41]:

$$\begin{aligned} &\dot{e}(t) = (A - HCA - K_1C)e(t) + [F - (A - HCA - K_1C)]z(t) \\ &+[K_2 - (A - HCA - K_1C)H]\Delta\omega_G(t) \\ &+[T - (I - HC)]Bu(t) + (HC - I)R_a\zeta(t) \end{aligned} \tag{20}$$

where $K_1 + K_2 = K_{UIO}$. The state estimation error ($\dot{e}(t) = Fe(t)$) can be equal to zero, provided that the following equations, i.e., $(HC - I)R_a = 0$, $I - HC = T$, $A - HCA - K_1C = F$, and $FH = K_2$, hold true. The estimation error, i.e., $e(t) = x(t) - \hat{x}(t)$, will approach zero asymptotically ($\hat{x}(t) \rightarrow x(t)$) when the eigenvalues of the UIO dynamic matrix (F) are located in the left-half plane. In this regard, UIO is designed by resolving a set of mentioned four equations, and ensuring that all eigenvalues of F are located in a stable area. Before discussing the necessary conditions for customizing the UIO of the under-study system, two lemmas are introduced:

Lemma 1: Equation $(HC - I)R_a = 0$ has a solid solution if $rank(CR_a) = rank(R_a)$. One solution that can be obtained for this matrix is $H^* = R_a[(CR_a)^T CR_a]^{-1}(CR_a)^T$. To find more proof related to these lemmas, one can refer to [42].

Lemma 2: Let to have, $C_1 = [\ C \quad CA\ ]^T$. It can be asserted that the detectability of the pair (C_1, A) is equivalent to that of the pair (C, A). It is important to mention that detectability is weaker compared to the observability condition. The C_1 is detectable, provided that all unobservable modes were located on the left side of the s plane [42].

Theorem 1: The necessary and adequate conditions for (19), that is a UIO for the system defined by (14), is:

- $rank(CR_a) = rank(R_a)$
- (C_1, A) is a detectable pair, and A_1 is defined as:

$$A_1 = A - R_a[(CR_a)^T CR_a]^{-1}(CR_a)^T CA \tag{21}$$

In this case, $F = A - HCA - K_1C = A_1 - K_1C$ is stable if the gain matrix K_1 is appropriately selected. To achieve acceptable stability during SSR events, K_1 is obtained by pole placement techniques that aim to move the torsional modes to the stable area of the s plane. For finding the proof of **Theorem 1**, please refer to [43]. Based on a consolidated definition of external inputs, the UIO has the ability to separate external signals from state variables. In this regard, the estimation of aggregated EV loads, that can be switched by attackers and added to the state-space model as components of a switching attack vector, i.e., $\hat{\zeta}(t)$, is calculated from the developed UIO[44]:

$$\hat{\zeta}(t) = (CR_a)^{-1}[\Delta\dot{\hat{\omega}}_G(t) - CA\hat{x}(t) - CBu(t)] \tag{22}$$

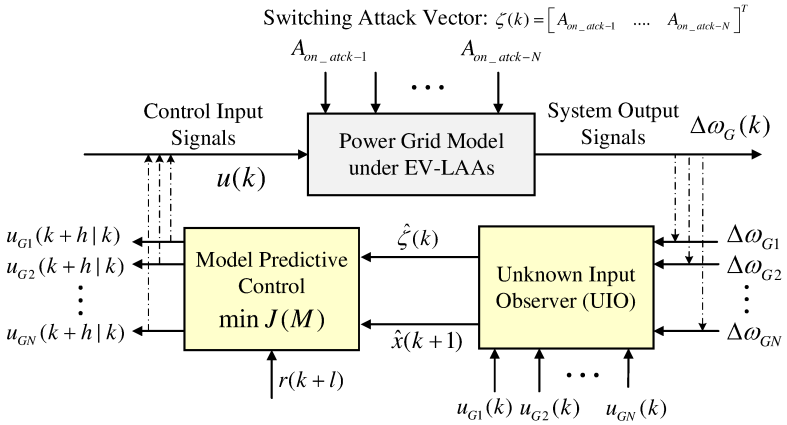


Figure 3.9: Layout of adaptive mitigation technique.

where components of this vector are used in the MPC to develop an adaptive mitigation framework. Since the proposed adaptive framework has a multi-input and multi-output feature, it is proper for designing wide-area controllers. This framework can optimize the control input signals following changes in components of the switching attack vector and state variables using an MPC. This collaboration between the UIO and MPC has been illustrated in Fig. 3.9. The estimation of state variables vector, i.e., $\hat{x}(k)$ which is calculated from the UIO, can be updated in an online manner at time step k as follows:

$$\begin{cases} \hat{x}(k) = \hat{z}(k) + H\Delta\hat{\omega}_G(k) \\ \Delta\hat{\omega}_G(k) = C\hat{x}(k) \end{cases} \tag{23}$$

Equations in the state-space model of the system with the estimation of the switching attack vector from (22) can be updated as follows:

$$\hat{x}(k+1|k) = A_d\hat{x}(k|k) + B_d u(k|k) + R_{ad}\hat{\zeta}(k|k) \tag{24}$$

$$\Delta\hat{\omega}_G(k+1|k) = C_d\hat{x}(k+1|k) \tag{25}$$

where $\hat{x}(k+1)$ and $\hat{x}(k)$ are referred to as the state variables from the current sampling time (k) to the following one $(k+1)$. Also, A_d, B_d, R_{ad}, and C_d are state-space matrices of the under-study system in the discrete form. In the layout of the MPC, an optimization problem is resolved to obtain the h^{th} step ahead of the future control input signals and the l^{th} step ahead of the future output signals in an online manner with the minimum variation rate in these control signals. These signals can be added to the internal control framework of the SGs for mitigation of EV-LAAs. As such, a

quadratic cost function $J(M)$ is defined:

$$J(M) = J_{\Delta\omega_G}(M) + J_u(M) + J_{\Delta u}(M) \tag{26}$$

where $J_{\Delta\omega_G}(M)$, $J_u(M)$, and $J_{\Delta u}(M)$ are defined to consider system output signals, control input signals, and variation rate in control signals, respectively, as follows [45]:

$$J_{\Delta\omega_G}(M) = \sum_{l=1}^{N_O} Q_l[\Delta\omega_G(k+l|k) - r(k+l)]^2 \tag{27}$$

$$J_u(M) = \sum_{h=0}^{N_C} \Lambda_h[u_G(k+h|k) - u_G(k+h-1)]^2 \tag{28}$$

$$J_{\Delta u}(M) = \sum_{h=0}^{N_C} \Phi_h[\Delta u_G(k+h-1)]^2 \tag{29}$$

where $\Delta\omega_G(k+l|k)$ is the predicted output signals and $r(k+l)$ is the future reference trajectory at the l^{th} future sample. Furthermore, $Q_l = W_l^{\Delta\omega_G}/S_l^{\Delta\omega_G}$, $\Lambda_h = W_h^u/S_h^u$ and $\Phi_h = W_h^{\Delta u}/S_h^{\Delta u}$ are introduced as balancing coefficients in the proposed cost function. The $W^{\Delta\omega_G}$, W^u, and $W^{\Delta u}$ are defined as weighted factors of output signals, control input signals, and variation rate in control signals, respectively. Besides, $S^{\Delta\omega_G}$, S^u, and $S^{\Delta u}$ are referred to as scaling factors that adjust output signals, control signals, and their changes, respectively. Two parameters, i.e., N_O and N_C, are referred to as the prediction horizon and the prediction control, respectively. Constraints on control input signals (u_{G1}, u_{G2}, u_{G3}, u_{G4}), the variation rate in control input signals (Δu_{G1}, Δu_{G2}, Δu_{G3}, Δu_{G4}) and the output signals ($\Delta\omega_{G1}$, $\Delta\omega_{G2}$, $\Delta\omega_{G3}$, $\Delta\omega_{G4}$) of the M-IEEE-SBM are assumed:

$$u_{\min} \leq u_G(k+h) \leq u_{\max}, h = 0, 1, ..., N_C \tag{30}$$

$$\Delta u_{\min} \leq \Delta u_G(k+h) \leq \Delta u_{\max}, h = 0, 1, ..., N_C \tag{31}$$

$$\Delta\omega_{G\min} \leq \Delta\omega_G(k+l) \leq \Delta\omega_{G\max}, l = 1, 2, ..., N_O \tag{32}$$

A summary of the collaboration between the customized UIO and MPC to establish an adaptive mitigation technique has been presented in Algorithm 3.

Algorithm 3: Adaptive Technique for EV-LAA Mitigation

Require: Model of power grid, matrices A, B, C, D, R_a using Threat Model

1) Compute: $H^* = R_a[(CR_a)^T CR_a]^{-1}(CR_a)^T$

2) Compute: $T = I - HC$ and $A_1 = T * A$

3) Check: Detectability of pair (C_1, A)

4) Calculate: K_1 gain using the pole placement method

5) Calculate: $F = A - HCA - K_1C = A_1 - K_1C$

6) Calculate: Matrix of UIO: $K_{UIO} = K_1 + K_2$

7) Initialize: Prediction horizon (N_O) and the prediction control (N_C)

8) Design: Adaptive technique based on integration of UIO and MPC

for $k = 1:1:\{\textit{Time interval}\}/T_s$ **do**

- **Measure:** $\Delta\omega_G(t)$ and $u(t)$ at time step k
- **Estimte:** State variable vector $\hat{x}(k)$ based on (23)
- **Estimate:** Switching attack vector $\hat{\zeta}(k|k)$ from customized UIO by (22)
- **Update:** components of $J(M)$
- **Check:** All constraints in (30)-(31)
- **Predict:** $u(k+h|k)$ and $\Delta\omega(k+l|k)$ for h^{th} and l^{th} step ahead, respectively
- **Implement:** Online control input and output signals to the power grid

end

3.6 Simulation Results and Discussion

In the first subsection, EVSAs are applied to the M-IEEE-SBM based on the proposed threat models, and the impacts of these attacks on different mechanical parts of SGs are studied. Afterward, the proposed adaptive technique is developed to estimate switching attack vectors and mitigate torque oscillation between mechanical sections, resulting from different EV-LAAs scenarios listed in Table 3.1. The impacts of EV-LAAs on the SSR stability of a real power grid, i.e., PVNGS are also studied to validate the proposed adaptive mitigation technique.

3.6.1 Impact of EV Loads Switching Attack on System's Stability

According to the proposed threat model, the attacker makes enough effort to control the EVCSs and switches aggregated EV loads in areas with a specific frequency to excite torsional modes. The speed deviation of the rotor and LP section is shown in Fig. 3.11 when the attack described in Scenario I is applied to the system. It can be observed that launching this attack creates continuous oscillations in the speed of the equivalent SG's rotor and other mechanical parts, e.g., LP and HP sections in the steam turbine, and the angular speed of the equivalent generator in the first area $(G1)$.

Table 3.1: A summary of different Scenarios (f_{TM}=24.85 Hz)

Scenario	EV loads	Duration	f_{sw} (Hz)	EVSA model
I	25MW	Continuous	6.2125	Model B (ON/OFF)
II	50MW	Continuous	6.2125	Model B (ON/OFF)
III	50MW	Continuous	12.425	Model A(Sinusoidal)
IV	50MW	[0,1]	12.425	Model A (Sinusoidal)
V	50MW	[0,1]	6.2125	Model B(Sinusoidal)
VI	50MW	Continuous	12.425	Model A (ON/OFF)

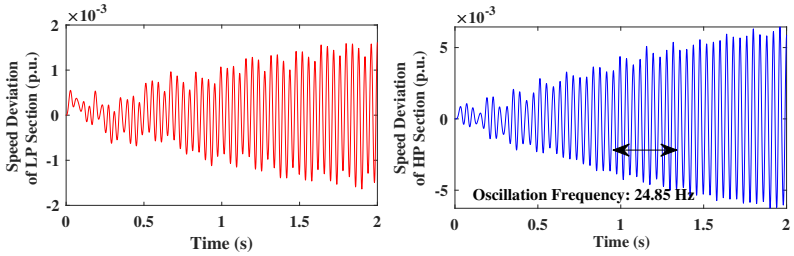


Figure 3.10: Speed deviation of mechanical parts of $G1$ (Scenario I)

3.6.2 Performance of Proposed Method during EVSAs

1) Charging/discharging Switching Attack: In this part, the attacker switches aggregated EV loads ON/OFF based on scenario II suggested in Table 3.1 at four nominated areas of the M-IEEE-SBM. From Fig. 3.11, it can be concluded that EV-LAAs in nominated distribution networks can be propagated into the transmission system and impact the voltage and frequency of related buses connected to 500 kV transmission lines. As a result, the customized UIO must estimate components of the attack vector within a phase shift of 40 ms between nominated areas that are shown in Fig. 3.12. The pole placement techniques are carried out to increase the damping ratio of the torsional mode (24.85 Hz) from its nominal value to more than three times, with the aim of achieving acceptable performance during the attack vector estimation. A comparison between the performance of PI-based SSRDC and the proposed method is also provided in Fig. 3.13. It can be observed that the proposed method can deliver an acceptable performance and keep the system response within acceptable limits. It is worth noting that since the attack remains continuously in the system, keeping the system parameters within the acceptable range provides enough time for the operator to preserve the grid operation and resolve the switching attack issue. Moreover, the angular speed deviation of the SG's rotor and LP section for $G1$ has been shown in Fig. 3.14. A 2.5% deviation in the angular speed of different mechanical sections of SGs is sufficient to cause trip SGs and instability in the power grid.

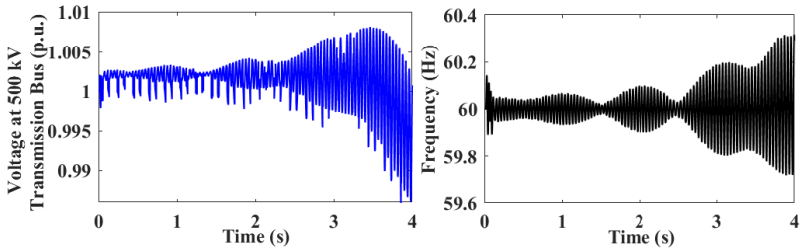


Figure 3.11: Voltage at 500kV transmission bus (p.u.) and frequency of transmission system (Hz) created by EV-LAAs (Scenario II).

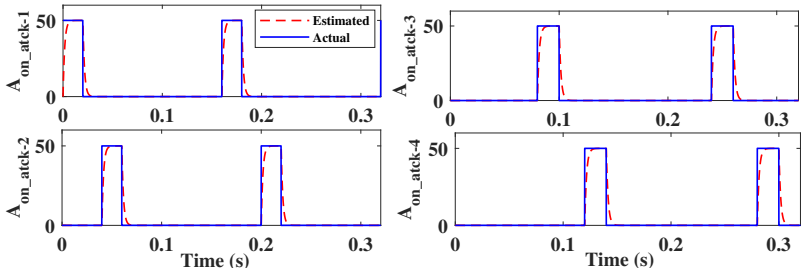


Figure 3.12: Estimation of switching attack vectors for Scenario II.

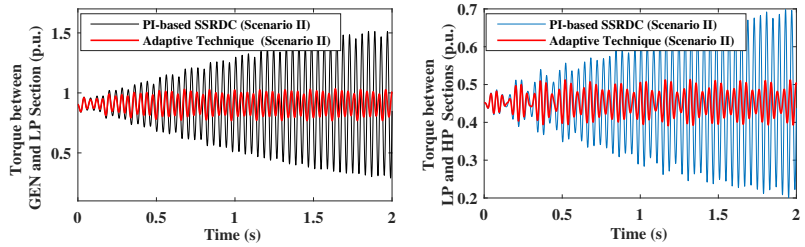


Figure 3.13: Comparison between the performance of proposed mitigation strategy and PI-based SSRDC during Scenario II for $(G1)$.

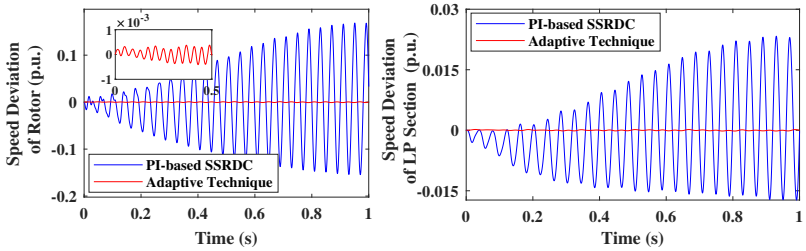


Figure 3.14: Angular speed of rotor and LP of $G1$ for Scenario II

2) Sinusoidal Switching Attack: In this part, adversaries switch aggregated EV loads in distribution networks with a sinusoidal pattern based on Scenarios III and IV in Table 3.1. In this regard, the amplitude of aggregated EV loads is changed based on a positive half cycle of a sinusoidal pattern in the first area pair to generate the first component of the switching attack vector (A_{sin_atck-1}), and the negative half cycle in another area to generate another component (A_{sin_atck-2}). This switching

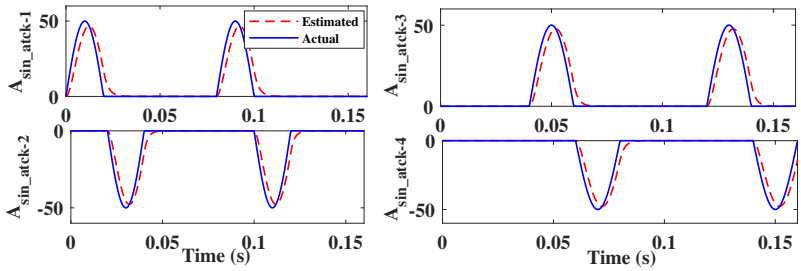


Figure 3.15: Estimation of switching attack vector for Scenario III.

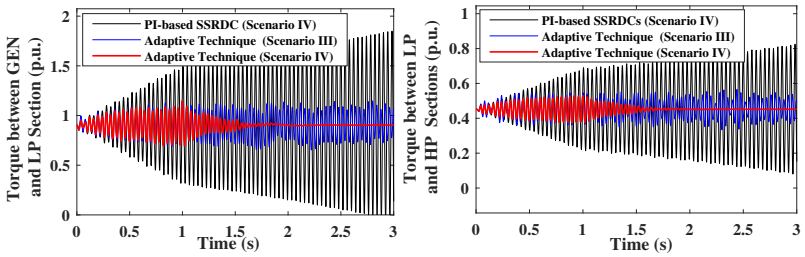


Figure 3.16: Comparison between the performance of the proposed method and PI-based SSRDC in case of Scenario III and IV for $(G1)$.

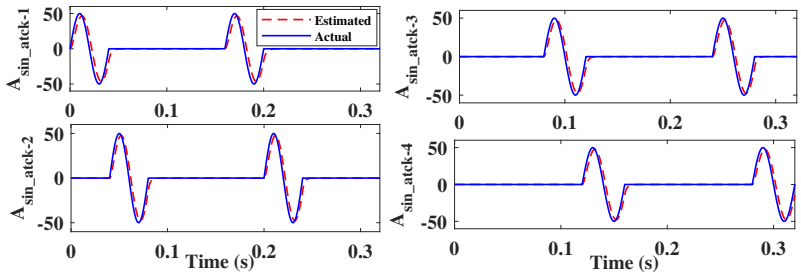


Figure 3.17: Estimation of sinusoidal EVSAs for Scenario V.

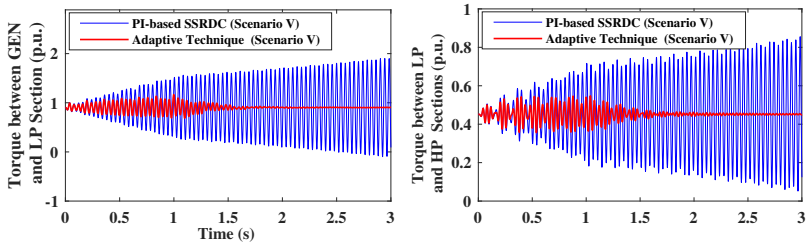


Figure 3.18: Comparison between the performance of adaptive technique and PI-based SSRDC in case of Scenario V.

of EV loads continues for other pairs of areas in the power grid to obtain related components, i.e., (A_{sin_atck-4} and A_{sin_atck-3}). It is clear that the frequency of EV loads switching attacks from the adversaries' viewpoint is 12.425 Hz, whereas the frequency of torsional mode is 24.85 Hz. The customized UIO can estimate components in an online manner as shown in Fig. 3.15. To compare

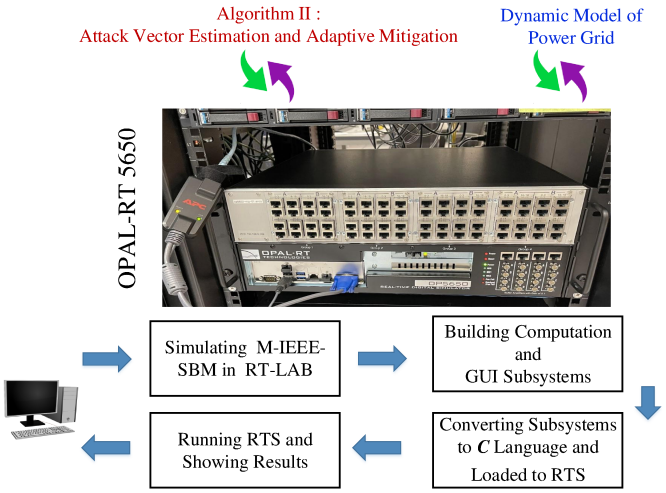
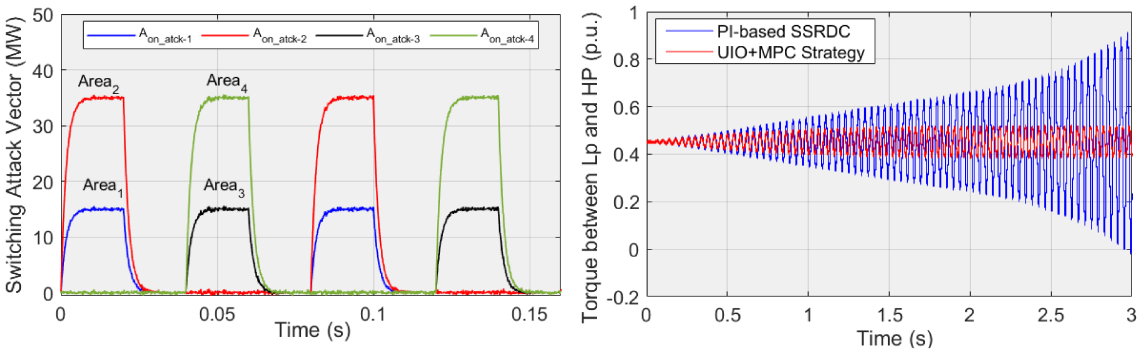


Figure 3.19: Real-time experimental setup of the M-IEEE-SBM.



(a) (b)

Figure 3.20: (a) Estimation of EV load switching attacks, (b) Torque between HP and LP section of the steam turbine in RTS (Scenario VI).

the performance of the proposed adaptive method with the PI-based SSRDC, torque oscillation between various sections of $G1$ and steam turbine have been illustrated in Fig. 3.16. It is evident that the proposed adaptive technique can alleviate oscillatory behaviours of torque between mechanical sections of SGs when an EV-LAA is applied to the M-IEEE-SBM for the predefined time interval [0, 1s], and when it continuously remains in the system. In the following, based on Scenario V, adversaries change EV loads based on a sinusoidal pattern in each area, one after the other, sequentially. The performance of the customized UIO in the estimation of EV-LAAs has been shown in Fig. 3.17. Also, the performance of the adaptive technique with the PI-based SSRDC is compared in Fig. 3.18.

3.7 Real-Time Simulation of M-IEEE-SBM

This section evaluates the performance of the adaptive technique based on the integration of the designed UIO and the MPC. For this purpose, a testbed for real-time simulations is developed, as shown in Fig. 3.19. This framework includes OPAL-RT-5650 as a real-time simulator for simulating the M-IEEE-SBM with realistic data, online UIO for attack vector estimation, and the proposed adaptive control mechanism. To consider the detailed transient behavior of the grid, the time step for this framework is considered to be 2.5 μs. To demonstrate the effectiveness of the developed techniques, it has been assumed that the adversary launches a switching attack based on Scenario VI in Table 3.1. In this scenario, an attacker classifies aggregated EV load areas into 2 clusters. Then, he/she switches aggregated EV loads in the first cluster with an ON/OFF (charging/discharging) pattern to obtain related components of the attack vector (A_{on_atck-1} and A_{on_atck-2}) with the 30% and 70% portion of total compromised EV loads, i.e., 15MW and 35MW, respectively. Then, another cluster of aggregated EV loads is switched with an ON/OFF pattern to generate remaining components, i.e., A_{on_atck-3} and A_{on_atck-4}. To show the performance of the proposed method in the attack estimation and mitigation, torque between HP and LP sections for $G1$ has been illustrated in Fig. 3.20. It can be concluded that the proposed method yields a satisfactory performance, compared to the PI-based SSRDC, and keeps the parameters of M-IEEE-SBM within the acceptable range. This will provide enough time for the operator to act and preserve the grid stability.

3.7.1 Realistic Power Grids under EV-LAAs

To show the possibility of this coordinated EV-LAAs in a real power grid with capacitor-compensated transmission lines, the Palo Verde Nuclear Generating Station (PVNGS) in Arizona state in the USA, is simulated, as shown in Fig. 3.21. This power plant consists of three equivalent synchronous generators with a capacity of 1270 MW (24 kV and 1800 rpm)—equipped with steam turbine governors—that supply several distribution networks, i.e., Phoenix, Los Angeles, and Imperial Valley and North Gila, through five transmission lines (two of them are series capacitor compensated) with a level of 500 kV. All technical data about transmission lines, synchronous

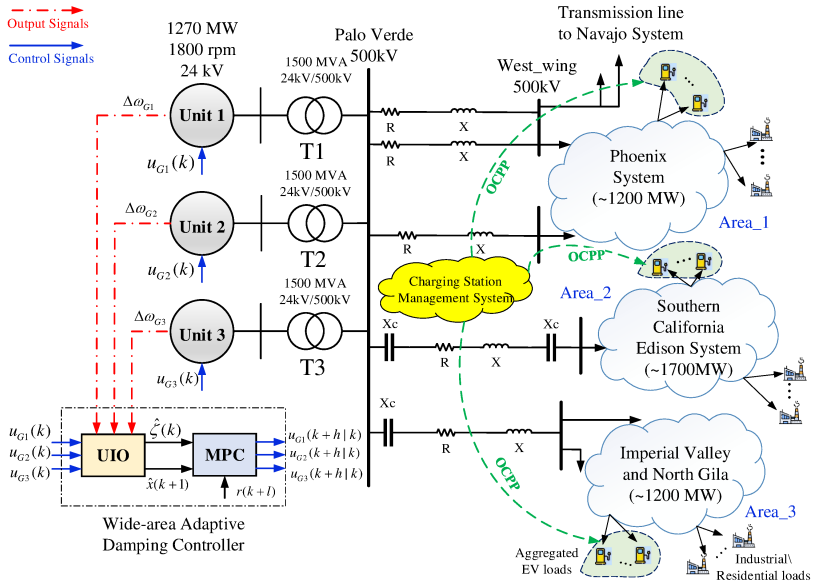


Figure 3.21: Single Line Diagram of the PVNGS and adaptive technique

Table 3.2: parameters of turbine-generator shaft model

Mechanical Section	Inertia Constant(s)	Damping (pu T/pu dω)	Shaft Section	Stiffness (pu/rad)
EXC	0.004253	0.001	EXC-GEN	0.985
GEN	0.868495	0.12	GEN_LP-B	30.458
LP-B	0.789521	0.120	LP-B_LP-A	15.038
LP-A	0.720189	0.120	LP-A_IP	10.929
IP	0.123699	0.028	IP-HP	6.303
HP	0.058712	0.008		

generators, and turbine-generator shaft models has been mentioned in [1]. In Fig. 3.22, the manufacturer has provided a 15-mass model for the Palo Verde turbine-generator shaft sections that is considered to be an alternate six-mode model for SSR studies [46]. The related parameters of the turbine-generator shaft model have been summarized in Table 3.2. Based on the suggested multi-order synchronous machine and differential equations for six equivalent mechanical sections of the steam turbine shaft model, the *Heffron–Phillips* is established to design an adaptive and wide-area damping controller. After eigenvalues analysis of the system, all modes of the PVNGS can be calculated as illustrated in Fig. 3.23. Using eigenvalue analysis, the torsional modes of the PVNGS are calculated as $0.27 \pm j59.98$ with a torsional frequency of f_{TM1}=9.55 Hz, $0.01 \pm j103.25$ with a torsional frequency of f_{TM2}=16.44 Hz, $0.082 \pm j131.69$ with a torsional frequency of f_{TM3}=20.96 Hz, and $-0.05 \pm j196$ with a torsional frequency of f_{TM4}=31.21 Hz.

Based on the topology of the PVNGS, aggregated EV loads are available for intruders to make

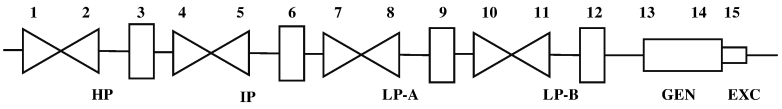


Figure 3.22: Palo Verde turbine-generator shaft model [1].

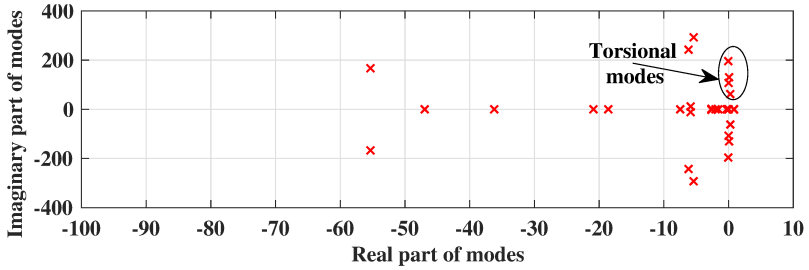


Figure 3.23: Eigenvalues analysis of Palo Verde Nuclear Generating Station.

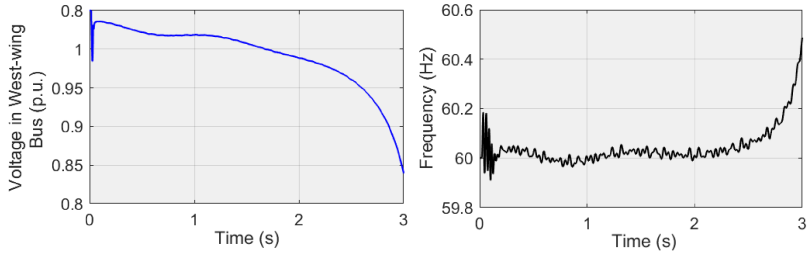


Figure 3.24: Voltage at West-wing transmission bus (p.u.) and frequency of transmission system (Hz) under EV-LAAs

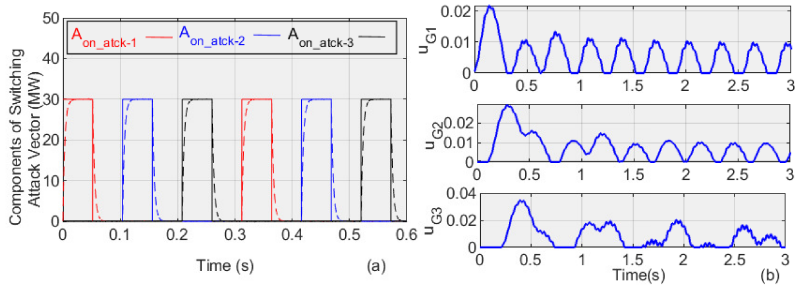


Figure 3.25: (a) Estimation of components of switching attack vector for 3 areas, (b) Control input signals generated by adaptive control framework.

components of a switching attack vector in each area. To obtain publicly available information about EVCSs and their locations, power ratings, and real-time and historical usage profiles, Alternative Fuels Data Center (AFDC), *ChargePoint* applications, and *PlugShare* website are suggested [7]. For example, Los Angeles in the U.S. state of California only has roughly 4,771 public charging stations, 486 of which are DC Fast Chargers (with an average power rate of 120 kW) [47]. Considering

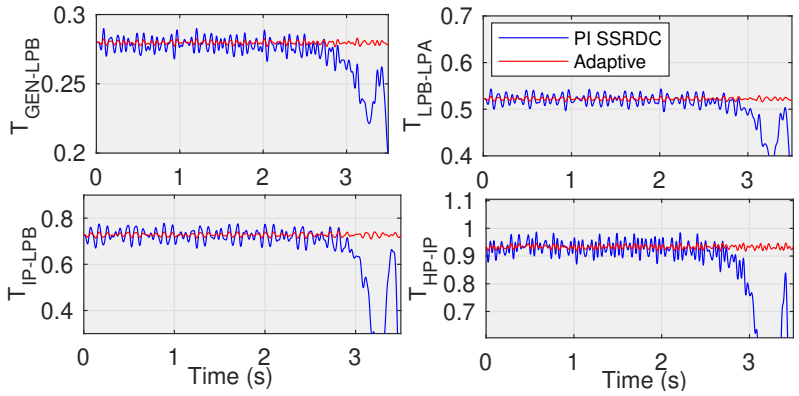


Figure 3.26: Torque Oscillation between different mechanical sections of turbo-shaft model (GEN, LP-B, LP-A, IP, and HP)

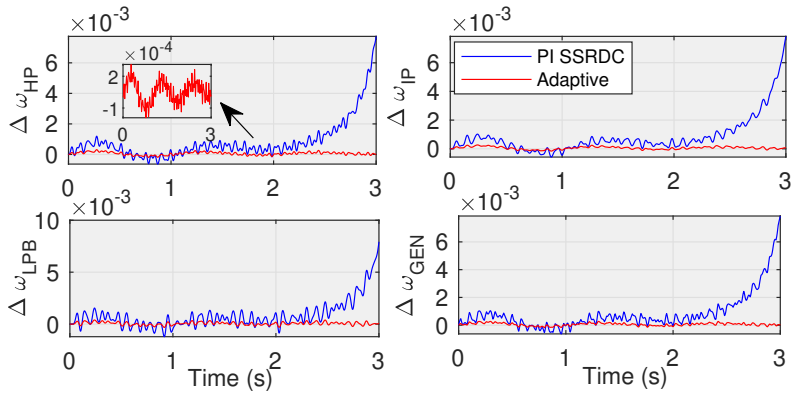


Figure 3.27: Speed deviation ($\Delta\omega$) of different mechanical sections of G_1.

at least 5% of the total loads as EV loads, a minimum amount of available EVCSs, that can be targeted based on the threat model for building components of an actual switching attack vector, i.e., ΔP_{EV}=30 MW, is defined in each distribution network. The frequency of the torsional modes and the number of distribution networks are selected as f_{TM}=9.55Hz and N_b=3. Using attack model **B**, the frequency of EVSA can be calculated as f_{sw}=$\frac{f_{TM}}{N_b}$=3.18 Hz, and this attack vector is applied to the PVNGS according to the ON/OFF strategy illustrated in Fig. 3.3. (a) for three different areas. Based on Algorithm 2, adversaries switch aggregated EV loads in different areas one after the other, sequentially, to make components of the switching attack vector. It can be shown from Fig. 3.24 that EVSA in the distribution networks can be propagated into the transmission system and impact the voltage and frequency of transmission buses, for example, the West-sing feeder connected to transmission lines. On this basis, the customized UIO for the PVNGS system can estimate these components in an online manner as shown by the dashed lines in Fig. 3.25. (a). As shown in

Fig. 3.21, the UIO estimates EV-LAA vectors and the state variables vector in an online manner and collaborates with the MPC to build an adaptive control framework. This adaptive technique can generate optimum control input signals based on Fig. 3.25. (b), and add them to the internal control frameworks of generation units to mitigate the impacts of switching attacks on mechanical parts of SGs. Torque oscillation of mechanical sections of the steam turbine shaft model in the presence of the PI-based SSRDC and the proposed adaptive technique have been illustrated in Fig. 3.26. It can be seen that the mechanical sections of steam turbine shafts are subjected to a continuously increasing torque that can finally lead to a shaft fracture. Furthermore, the angular speed deviation of four mechanical sections, i.e., HP, IP, LP-B, and rotor of G_1 has been shown in Fig. 3.27. The 2.5% deviation in the speed of SG's rotor speed can lead to tripping SGs and instability of the PVNGS. As such, the PI-based SSRDC fails to mitigate the SSR events crafted by EV-LAAs due to limitations in designing for limited operating points [48].

3.8 Conclusion

In this section, a new family of EV-based load-altering attacks, that could be launched by compromising charging stations, was introduced. The crafted EV switching attacks (EVSAs) aim at exciting torsional modes of the grid and create SSR events to damage the mechanical part of the generators. First, it was shown that the PI-based SSRDC could not alleviate the developed switching attacks. Then, using an unknown input observer (UIO), which estimated switching attack vectors online, an adaptive control framework was developed based on a model predictive controller (MPC). This controller could generate control input signals and mitigate the impacts of EVSAs through a wide-area controller. The effectiveness of the proposed adaptive technique was evaluated using M-IEEE-SBM designed for SSR studies. To show the impacts of EV-LAAs on the SSR stability of realistic power grids, the Palo Verde Nuclear Generating Station (PVNGS) was simulated to validate the proposed adaptive mitigation technique for coordinated EVSAs.

Chapter 4

Deep Learning Detection and Robust MPC Mitigation for EV-Based Load-Altering Attacks on Wind-Integrated Power Grids

4.1 Motivation

In modern power systems, the integration level of renewable energy sources is increasing [49]. Such integration can create several stability and resonance issues in the grid, for instance, due to the interaction between the grid and control systems of wind farms [50]. Among these issues, subsynchronous control interaction (SSCI) is one of the most important and frequent ones, evidenced by numerous incidents in the U.S. and China [51, 52]. Thus, the subsynchronous modes of wind-integrated grids can be also excited if the appropriate load behavior is injected into the grid by EVs with a similar frequency to those modes. Therefore, it is of paramount importance to develop detection and mitigation techniques against switching EVCSs in EV ecosystems that target the subsynchronous stability of wind-integrated power grids. Recently, several data-driven approaches have been developed to detect cyber-physical attacks against wide-area power systems using the data

obtained from phasor measurement units (PMUs) [53, 54]. For example, cyber threats in power systems with sparse monitoring sensors are detected using a data-driven hierarchical monitoring scheme in [55]. A data-driven strategy is also suggested to detect oscillations using robust principal component analysis in [56]. However, the performance of these data-driven methods is heavily dependent on their internal parameters that make them inappropriate for online detection. In addition, these solutions neglect the cyber threats originating from the EV ecosystem along with their unique specifications. On this basis, there is a lack of online data-driven methods to estimate the switching attack vector and increase the operator's awareness during an attack considering existing uncertainties in the power grid. Following the SSCI events, wide-area mitigation strategies were introduced to alleviate subsynchronous oscillations in power grids, e.g., a linear quadratic regulator (LQR) technique [3], a two-degree-of-freedom damping control loops [57], a data-driven adaptive method [58], and μ-synthesis method [59]. The mentioned control frameworks are generally developed for a specific operating point without considering uncertainties stemming from possible load-altering attacks during different wind speeds and WTGs outages. In other words, their performance is only evaluated following abrupt one-time events, e.g., faults in power grids. As a result, these instability events along with cyber vulnerabilities and attack cases on EV ecosystems highlight the importance of having rigorous learning-based detection to notify the security status of the system and robust mitigation techniques to counter these possible switching attacks on the stability of wind-integrated power grids.

4.2 Contributions

Motivated by the above discussions, this paper discusses a surface of switching attacks that can be launched by adversaries through manipulation of EVCS's firmware and switching aggregated EV loads ON/OFF based on the frequency of unstable or lightly-damped SSCI modes of the wind-integrated power grid. It will be shown that this attack can excite SSCI modes of the transmission system and cause instability in wind-integrated power grids, even in the presence of frequent damping wide-area controllers. In the detection phase, a deep convolutional neural network (CNN) is trained based on a set of voltage and current measurements obtained from the PMU at the wind

farm point of interconnection (POI). During the learning process, a wide range of uncertainties, e.g., wind speed and the number of wind turbine generators (WTGs), which impact SSCI modes, are also considered in the case of the different amplitude of switching attacks. This customized CNN is used to estimate the switching attack vector and to notify the operator of the security status of the power grid, i.e., EV-based load-altering attacks, normal operation, or fault and line disconnection. Due to the lack of 100% accuracy of the detection method (which is also the case in all data-driven methods), a robust model predictive controller (RMPC) is developed by solving linear matrix inequalities (LMIs) equations to guarantee the stability of the power grid under different uncertainties. In summary, the main contributions of this paper are as follows:

(1) Introducing new coordinated EV-based load-altering attacks (EV-LAAs), where adversaries can downgrade the firmware repository of the CSMS by uploading a less secure version. Afterward, they can upload malware to the targeted firmware of EVCSs and build a botnet for EVSE to inject fake charging and discharge commands. These fake charging and discharging commands can be triggered by an attacker's command and control (C&C) center in a coordinated manner based on a predefined time pattern, i.e., the frequency required to excite the unstable or lightly-damped SSCI modes of wind-integrated power grids.

(2) Developing a CNN model as a classification tool to determine the source of the event that results in oscillations (i.e., fault, line disconnection, or switching attack). This model is also used as a regression tool to estimate the switching attack vector. This neural network model with consecutive convolutional layers can extract better features from input data for classification and regression tasks, making it an online detection framework in the presence of different uncertainties in the operation of wind-integrated power girds.

(3) This detection framework may neglect a few EV load switching attack vectors and generate false negatives due to the huge number of attack vectors with different combinations of amplitudes and frequencies during uncertainties in wind speeds and the number of WTG outages. Also, EV-LAAs can lead to SSCI events during uncertainties in the operation of the wind-integrated power grid. On this basis, a robust model predictive controller (RMPC) is also

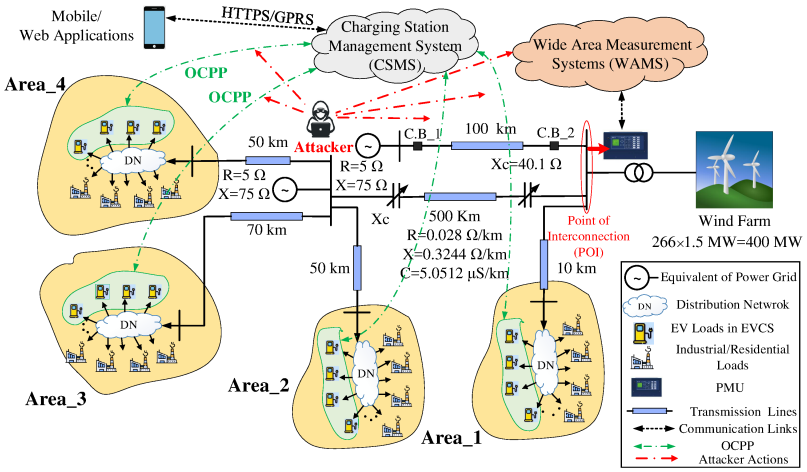


Figure 4.1: Schematic of the wind-integrated power grid with physical and cyber layers of EV ecosystems along with attacker's actions.[2, 3]

suggested as a supplementary solution to mitigate the switching attack impacts. Possible uncertainties in wind speed and the WTG outages during different amplitudes of EV-LAAs are investigated when defining linear matrix inequalities (LMIs). Moreover, constraints on control input and output signals are also studied. After solving this set of LMIs, state-feedback controllers are designed to mitigate the impacts of such attacks in the presence of uncertain dynamical systems with external disturbances. This controller is designed in MATLAB and imported into the EMTP-RV using functional mockup interface kits (FMIKits) and the Simulink toolbox to compare its performance with frequent damping controllers, e.g., the 2DOF, LQR, and H_∞.

4.3 Power Grid Model Under Switching Attack

A well-known wind-integrated power grid is used to study the SSCI phenomenon [3, 60]. Without loss of generality, to investigate the impact of EV-based load-altering attacks in a coordinated manner, this grid is extended to four areas that consist of equivalent generators, distribution networks with aggregated EV loads, OCPP communication, and CSMS as shown in Fig. 4.1. The total capacity of the wind farm is 400MW, which consists of 266 WTGs, each with a nominal capacity of 1.5MW. Two important uncertainties, i.e., changes in wind speed from 0.6 p.u. to 1 p.u. (V_w =[0.6

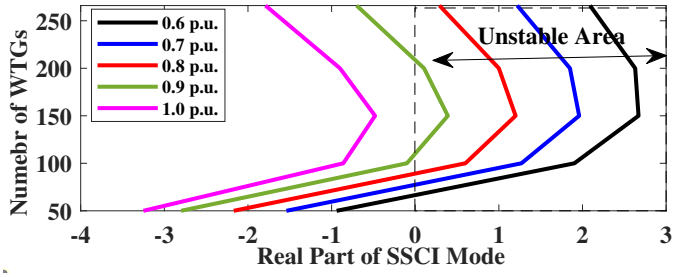


Figure 4.2: Impact of WTGs outage on SSCI mode at different wind speeds.

p.u., 1 p.u.]) and the number of WTGs from 266 to 50 (N_{wtg} =[266, 50]), are assumed during the operation of the power grid. It is assumed that the system's operator has installed a PMU—which captures 50 samples per second—at the wind farm substation. This PMU communicates with the wide-area measurement system (WAMS) to transmit the measured data for monitoring and control of the power grid. Since the main purpose of research is to study the oscillation events, voltage and current measurements of this substation can provide valuable data regarding the operation of the power grid. Moreover, it is considered that each area of the system has a total of 200MW of different loads. We assume that there are around 70,000 EVs in each area using a comparable ratio for EVs to the total loads mentioned in the realistic scenario of the *Manhattan* system in the US[7]. The International Energy Agency (IEA) estimates that governments and operators typically maintain 1 public EVCS for every 10 EVs on the road, which results in our wind-integrated power grid having 7,000 EVCSs. Considering 24kW as the average charging rate of commercial level 2 chargers [2, 4] and approximately 30% chance of being compromised by attackers, each of the areas can be estimated to have approximately 50MW as viable aggregated EV loads for switching attacks. Adversaries can monitor the communication interaction between the wide-area controller and the power grid by penetrating the WAMS and deploying system identification methods based on prediction error minimization technique [10, 61] to obtain unstable SSCI modes of systems as illustrated in Fig. 4.2.

4.4 Feasibility of Coordinated EV Loads Switching Attacks

To investigate the feasibility of this attack, three important assumptions must be discussed: (i) The adequate number of installed EVCSs in distribution networks of power grids: Based on [2, 4], the global number of EVs on the road has increased to more than 17 million in 2021. It is projected that this number will rise to roughly 200 million at the end of 2030 across the world that can provide a noticeable surface for this switching attack [8]; (ii) Resonance conditions in wind-farm integrated power grids: Subsynchronous oscillations have been observed in several real-world wind farms around the world, e.g., in US and China [50, 51, 52]; (iii) Availability of vulnerable points in the cyber layer of the EV ecosystem: Different attack graphs can be defined in the EV ecosystem that shows how adversaries can take steps to penetrate into cyber layers and jeopardize the stability of the power grids[18]. To run a switching attack with the aim of exciting unstable SSCI modes of the system, a generic botnet can be designed based on Fig. 2.3. As mentioned in [21], several vulnerable points in well-known CSMSs, e.g., EV-Link and CSWI Etrel, can be maliciously targeted by attackers to launch this attack. In fact, adversaries can exploit SQL injection vulnerabilities to obtain access to the database of the CSMS, which consists of user records including high-privilege user account information and administrator credentials, and change the firmware hosted by EVCS similar to other IoT devices (Step 1) [22]. Then, malware/ransomware—like BlackEnergy malware injected into Ukraine's power grid or Stuxnet Malware infected Iran's nuclear power plants–with the aim of sending charging and discharging commands can be injected into EVCSs at different areas of the power grid in an offline manner (Step 2)[8]. Finally, these charging and discharging commands can be triggered from the attackers' command and control (C&C) center based on a predefined time pattern, i.e., the frequency of unstable or lightly-damped SSCI modes (Step 3)[23]. Since the frequency of SSCI modes is relatively large ($f_{SSCI} < 60$Hz) compared to inter-area modes (0.1-1Hz) studied in [12], switching aggregated EV loads can be carried out based on several strategies to reduce the switching frequency and the amplitude of aggregated EV loads. As discussed in [23], due to compromising the CSMS, adversaries can have access to EVCSs in more than one area practically and implement two attack models as follows: In attack model $\mathbf{A}$, to deal with the problem of SSCI mode's frequency, attackers compromise aggregated EV loads in each area, one after the

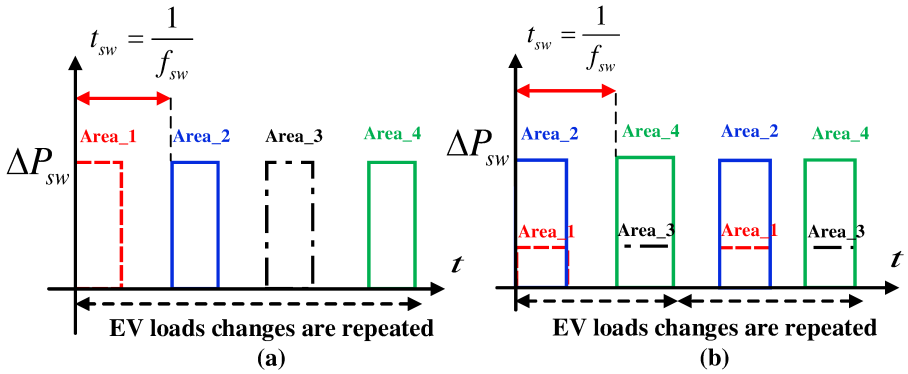


Figure 4.3: (a) Switching attack vector for 4 areas, (b) Pattern for dealing with amplitude problem of EV loads switching attack.

other, sequentially. On this basis, the frequency of switching EV loads in each area will reduce from f_{SSCI} to $\frac{f_{SSCI}}{N_a}$ (N_a is the number of areas) as shown in Fig. 4.3. (a). In attack model $\mathbf{B}$, to deal with the amplitude of aggregated EV loads in each area, EVCSs in two areas of power grids can be categorized into one group and switched with amplitudes less than the nominal capacity of compromised EV loads in each area. Based on Fig. 4.3. (b), attackers can compromise aggregated EV loads of two areas, e.g., Area_1 and Area_2 in the first group and afterward, Area_3 and Area_4 in another group to have coordinated switching attacks.

4.5 Design of Attack Detection Framework

4.5.1 Motivation for Multi-dimensional Input Data

The behavior of voltage and current measurement signals under different amplitudes of switching attack for a particular uncertainty, i.e., V_w =0.6 p.u. and N_{wtg} =150, has been illustrated in Fig. 4.4 using an LQR controller[3]. At this operating point of the system, the SSCI mode is calculated using system identification[61] as $2.67 \pm j253.41$, which is unstable. It can be observed that the switching attack at different areas with the frequency of the calculated SSCI mode, i.e., 40.52HZ, can result in rapid growth in voltage and current signals during a short time interval even in the presence of a common damping wide-area controller. Therefore, estimation of the switching attack vector, $[\Delta\hat{P}_{sw}, \hat{f}_{sw}]$, can be carried out in a timely manner. To achieve this aim, several indexes can be calculated from voltage and current measurements of PMU at the wind farm substation and attributed to switching attack vectors considering existing uncertainties in the power grid.

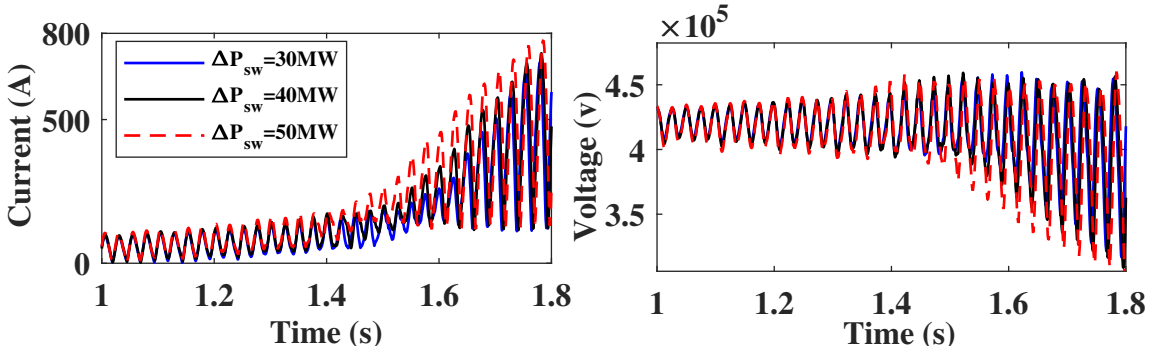


Figure 4.4: Current and voltage measurements of PMU at wind farm bus for several amplitudes of EV-based load-altering attacks using an LQR controller.

These indexes are defined as the mean and standard deviation of voltage and current of PMU's data $[\mu_v, \sigma_v, \mu_i, \sigma_i]$. Finally, the input data are reshaped into a multi-dimensional structure to effectively interpret them during the training phase for both regression and classification.

4.5.2 Data Generation for Training Phase

As can be seen from Fig. 4.2, different uncertainties can cause unstable SSCI modes in the system. These uncertainties along with the possible attack amplitudes and frequencies can be used to cover all possible situations during the learning process. Based on the topology of the under-study power grid, aggregated EV loads are switched between different areas from 25 MW (minimum level of EV load to have SSCI impacts) to 50 MW (maximum level of existing compromised EV loads defined in each area) in the presence of uncertainties. To calculate the mean and standard deviation of voltage and current sample data during transient behaviors, the observation window is defined to be 1.5s. Considering PMU's sampling frequency to be 50 samples/second, the total samples will be 75 for each voltage and current data in each window. Since CNNs are generally designed for image processing applications, input data are similarly arranged to a set of images with different dimensions. For this customized deep CNN, raw data can be arranged in the form of matrices with dimensions of $4 \times n_{sw} \times n_{unc}$, where n_{sw} and n_{unc} indicate the discrete step changes in aggregated EV load compromised by adversaries and the total number of uncertainties in the wind-integrated power grid that can cause unstable or lightly-damped SSCI modes. The target (output) data are also arranged in the form of matrices with dimensions of $2 \times n_{sw} \times n_{unc}$, where the number 2 indicates the amplitude of EV load switching attack (ΔP_{sw}) and the frequency of switching attack

Algorithm 4: Online Attack Vector Estimation and Notification of Security Status

Inputs: Voltage and current measurements of PMU

Uncertainties: $V_w = [0.6 - 1]p.u.$ and N_{wtg}=[266,...,50]

Output: Estimating ΔP_{sw} and f_{sw} and notifying security status of system

Location of PMU: At wind farm substation with 50 samples per second

while *Monitoring the PMU at wind farm substation* **do**

  Calculate μ and σ of measured data $[\ \mu_v \quad \sigma_v \quad \mu_i \quad \sigma_i]$

  Update μ_{new} and σ_{new} and replace with old ones

  Discriminate between different operations of system (normal,

  under switching attack or fault) using **Classification Layer**

  if *Electric Vehicle Switching Attack detected* **then**

    Estimate $\hat{\Delta}P_{sw}$ and $\hat{f}_{sw}$ using **Regression Layer**

    Display attack detection and attack vector: $[\ \hat{\Delta}P_{sw} \quad \hat{f}_{sw}\ ]$

    if *Fault and Line Disconnection detected* **then**

      Display no switching attack $\rightarrow$ fault detection

    else

      It is a normal operation of wind-integrated power grid

    end

  end

end

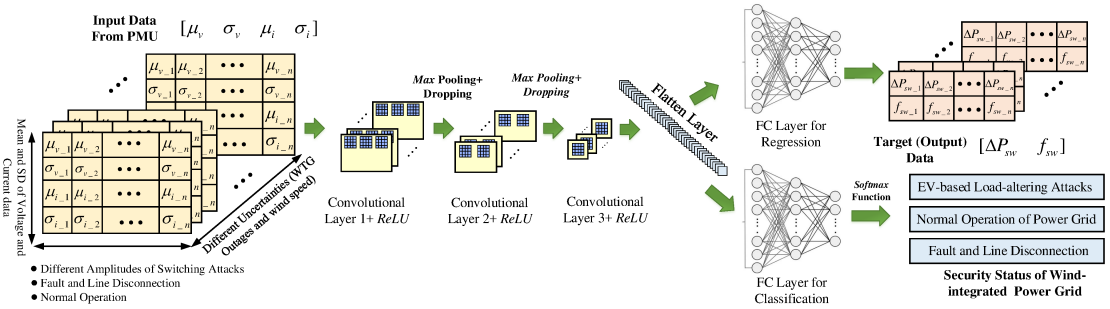


Figure 4.5: Deep CNN structure for different uncertainties (wind speed and WTGs outages) in the presence of a wide range of EV-based load-altering attacks.

(f_{sw}) in the power grid. For the classification layer, three possible situations are also defined and the related samples under different conditions are labeled with (i) the normal operation of the power grid without switching attacks; (ii) EV loads switching attack, and (iii) fault and line disconnection. During fault and line disconnection, different single- and three-phase faults with various ranges of circuit breaker operations are also considered to enrich datasets for a more accurate prediction of the security status.

4.5.3 Designing a Customized Deep CNN Structure

The structure of customized deep CNN for regression and classification of the system has been shown in Fig. 4.5. This structure includes three convolutional layers (Conv) for feature extraction from the mean and standard deviation of PMU's data. Each Conv layer consists of learnable kernel functions which conduct the convolution operation to calculate the feature of input data. In the customized deep CNN, the convolutional kernel sizes for three layers are [4,4,1,16], [4,4,2,32], and [2,2,1,64], respectively. In this format, the first, second, and third number is referred to as the height, width, and depth of the kernel function, and the last one indicates the number of kernel functions. To maintain the height and width of kernel functions, zero padding is also considered. Since the relationship between inputs and target data is non-linear, rectified linear unit *ReLU* is implemented as an activation function in this structure. This function can be deployed in deep CNN due to its quasi-linearity property, which keeps it as generalizable as linear models. The output of the third convolutional layer will go through two fully connected layers allocated for regression and classification purposes. The first output is the estimation of the switching attack vector. In the second output, after the FC layer, the *softmax* function is also deployed to give information about the situation of the power grids and distinguish different classes based on the PMU measurement data. Since the proposed deep CNN structure is a multi-task learning model used for both regression and classification processes, the related loss function during training can be calculated as:

$$\begin{aligned} L_{reg} = \tfrac{1}{N_s} \sum_{s=1}^{N_s} (\tfrac{1}{n_{unc}} \sum_{j=1}^{n_{unc}} (\Delta \hat{P}_{sw}(j,s) - \Delta P_{sw}(j,s))^2) \\ +... \sum_{j=1}^{n_{unc}} (\hat{f}_{sw}(j,s) - f_{sw}(j,s))^2)^{1/2} \end{aligned} \tag{33}$$

$$L_{cls} = \tfrac{-1}{N_s} \sum_{s=1}^{N_s} \hat{y}_s \log(y_s) \tag{34}$$

where N_s and n_{unc} are, respectively, the numbers of training samples and different uncertainties during a wide range of switching attacks. L_{reg} is the root mean square error (RMSE) of the switching attack vector, where $\Delta \hat{P}_{sw}(j,s)$ and $\Delta P_{sw}(j,s)$ are referred to as the estimated and actual amplitude of compromised EV loads, respectively. Moreover, $\hat{f}_{sw}(j,s)$ and $f_{sw}(j,s)$ are the estimated and actual frequency of the attack. Finally, L_{cls} is the cross-entropy that is used for the loss function of multi-classification problems. In this equation, $\hat{y}_s$ and y_s are referred to as the predicted and real security status of the wind-integrated power grid, respectively. To have online performance, Algorithm 4 with the help of customized CNN is implemented in the WAMS structure of the system

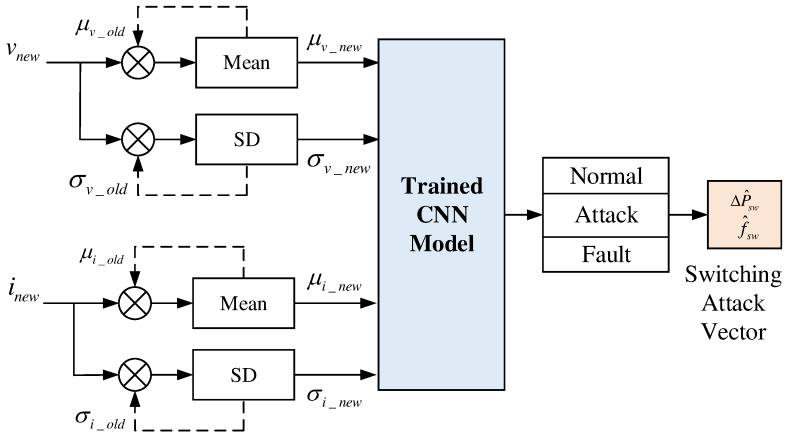


Figure 4.6: Online switching attack vector estimation based on Algorithm 4.

and provides online instructions on how to notify the operator of the security status of the power grid, and then to calculate switching attack vectors based on Fig. 4.6.

4.6 Mitigation Strategy

4.6.1 Control Layer of Wind Farm connected to Power Grid

The overall layout of the control mechanism designed for the wind farm has been illustrated in Fig. 4.7. At the local control level of each wind turbine, two inner and outer control loops are implemented to regulate its active power, terminal voltage, the voltage of the DC link, and the reactive power of the grid side converter (GSC) based on the corresponding reference signals, i.e., $\Gamma_{ref} = \{P_{WT}^{ref}, (1+\Delta)V_{WT}^{ref}, V_{DC}^{ref}, Q_{gsc}^{ref}\}$. The main task of the outer PI control loop is to acquire reference for currents in the d-axis and q-axis, while the inner PI controller loop produces converter AC voltage reference in a fast manner. The components of reference signals, Γ_{ref} can be calculated as follows. The P_{WT}^{ref} is obtained based on the maximum power point tracking (MPPT) algorithm. Reference for the $(1+\Delta)V_{WT}^{ref}$ and V_{DC}^{ref} can be obtained from the wind farm controller. It is important to mention that the reactive power of the GSC (Q_{gsc}^{ref}) is zero in practical applications, and it is reserved for dealing with under and over-voltage conditions. In this regard, the corresponding value for this parameter is zero in Γ_{ref}. In DFIG-based wind turbines, the control system is decoupled into the dq-framework for both the rotor side converter (RSC) and GSC using control

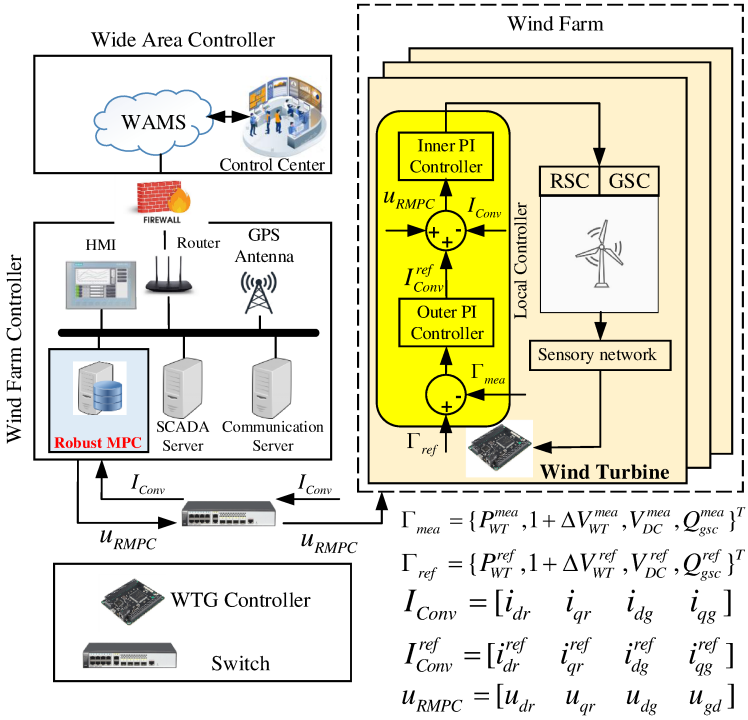


Figure 4.7: Different control layers in the wind-integrated power grid.

vector techniques[59]. In the RSC, the q-axis and d-axis currents, i.e., i_{qr} and i_{dr}, are employed to control active power and positive sequence of voltage in the terminal of DFIG, respectively. In the GSC, the q-axis and d-axis of current, i.e., i_{qg} and i_{dg}, are also used to control the reactive power during the WTG's over- and under-voltage and the DC bus voltage regulation, respectively. At the local controller level, a WTG considers the determined reference signal, i.e., Γ_{ref} as set points and compares them with the measurement signals, i.e., Γ_{mea}. Differences between these signals are transmitted to the outer PI controller loop to calculate the reference points of the RSC and GSC currents, i.e., $I^{ref}_{Conv} = [i^{ref}_{dr}, i^{ref}_{qr}, i^{ref}_{dg}, i^{ref}_{qg}]$. At the wind farm level, the converters' currents, i.e., $I_{Conv} = [i_{dr}, i_{qr}, i_{dg}, i_{qg}]$, are sent to the developed RMPC controller using the communication switches. These signals are already measured for the local control scheme of the wind turbines, and thus our proposed method does not require new measurements. The generated command signals from RMPC, i.e., $u_{RMPC} = [u_{dr}, u_{qr}, u_{dg}, u_{qg}]$, are added to the inner PI control loops to mitigate the SSCI phenomenon resulted from EV load switching attack.

4.6.2 Designing Robust Model Predictive Controller

The state-space model of the wind-integrated power grid can be obtained using system identifications as follows:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) \\ y(k) = Cx(k), \quad x(0) = x_0 \end{cases} \tag{35}$$

where $x(k)$, $u(k) = u_{RMPC}(k)$, $y(k) = I_{Conv}(k)$, and x_0 are defined as state variables, control input signals, output signals, and initial state variable vector, respectively. Different EV load switching attacks, uncertainties in wind speed, and the number of WTGs can create a family of uncertain subsystems. These subsystems, shown by K, are defined as the convex hull of the nominal state-space model with poly-topic uncertainties[62]:

$$K = Convex\_hull\{[A_1, B_1], ...[A_{n_v}, B_{n_v}]\} \tag{36}$$

If $[A, B] \in K$, for $0 < \lambda_l < 1$, we can have:

$$[A, B] = \sum_{l=1}^{n_v} \lambda_l [A_l, B_l] \tag{37}$$

where subscript l is a natural number between 1 and n_v that indicates different vertex subsets of K for the total number of vertices n_v. For example, $\{A_1, B_1\}$ is the nominal state-space model to evaluate the control performance of the uncertain system.

Main Problem: The problem of designing a robust MPC is to compute a state-feedback controller with the gain matrix $F(k)$ that ensures the robust stability of the closed-loop system for each subset of the K as follows:

$$u(k+h|k) = F(k)x(k+h|k) \tag{38}$$

where $u(k+h|k)$ and $x(k+h|k)$ are control input and state signals at time $k+h$, predicted based on the measurement at time k. A quadratic quality criterion is used to evaluate the control performance for different uncertainties during prediction horizon p:

$$\begin{aligned} J_p(k) = \sum_{h=1}^{p} [x(k+h|k)^T W_x x(k+h|k) + \\ u(k+h|k)^T W_u u(k+h|k)] \end{aligned} \tag{39}$$

where W_x and W_u are symmetric weighting matrices of the state variable and control input signals, respectively. The main aim is to calculate the set of optimum control input signals for a control

horizon m, i.e., $u(k+h|k), h = 0, ..., m$. These control signals should minimize the maximum value of the quadratic function over the set K, corresponding to several variable models, i.e., $[A(k+h), B(k+h)] \in K, h \geq 0$. On this basis, the control law for the m can be obtained by minimization of a robust performance objective, as follows:

$$\underset{u(k+h|k),h=0,...,m}{Min} \ \underset{[A(k+h),B(k+h)]\in K,h\geq 0}{Max} J_p(k) \tag{40}$$

To resolve this *min-max* problem, we first derive an upper bound on the robust performance objective. Then, this upper bound can be minimized by calculating a state-feedback control law, i.e., $u(k+h|k) = F(k)x(k+h|k)$.

Lemma 1: Schur complements can convert convex quadratic inequalities into linear matrix inequalities (LMIs). It is assumed that $R(x)$ and $A(x)$ are symmetric and positive-definite. Also, $S(x)$ depends affinely on variable x. Then matrix inequalities, i.e.,

$$A(x) - S(x)R(x)^{-1}S(x)^T > 0, R(x) > 0 \tag{41}$$

or, equivalently,

$$R(x) - S(x)^T A(x)^{-1}S(x) > 0, A(x) > 0 \tag{42}$$

are equivalent to this LMI as follows[63]:

$$\begin{bmatrix} A(x) & S(x) \\ S(x)^T & R(x) \end{bmatrix} > 0 \tag{43}$$

Deriving upper bound on robust performance objective: A quadratic Lyapunov function, i.e., $V(x) = x^T Px$, $P = P^T > 0$ of state $x(k|k)$ is considered. At sampling time k, it is supposed that for all $x(k+h|h)$, $u(k+h|h)$, and any $[A(k+h), B(k+h)] \in K, h \geq 0$, the convergence condition of system's states hold true[62]:

$$\begin{aligned} &V(x(k+h+1|k)) - V(x(k+h|k)) \leq \\ &-[x(k+h|k)^T W_x x(k+h|k) + u(k+h|k)^T W_u u(k+h|k)] \end{aligned} \tag{44}$$

For the mentioned robust performance objective function to be finite, we must have $x(\infty|k) = 0$,

and so $V(x(\infty|k)) = 0$ [62]. Finally, we can sum equation (44) from $h = 0$ to $h = \infty$ as follows:

$$\begin{aligned} &\sum_{h=1}^{\infty} V(x(k+h+1|k)) - V(x(k+h|k)) \leq \\ &\sum_{h=1}^{\infty} -[x(k+h|k)^T W_x x(k+h|k) + u(k+h|k)^T W_u u(k+h|k)] \end{aligned} \tag{45}$$

At the final stage, we can summarize the above equation as follows:

$$-V(x(k|k)) \leq -J_{\infty}(k) \Rightarrow J_{\infty}(k) \leq V(x(k|k)) \tag{46}$$

Since we want to calculate the maximum value of the quadratic function over the set of K, we select the maximum value of $V(x(k|k))$ equal to a parameter ξ as follows:

$$\underset{[A(k+h),B(k+h)]\in K, h\geq 0}{Max} J_{\infty}(k) \leq V(x(k|k)) \leq \xi \tag{47}$$

Thus, equation (40) can be summarized in a simpler form:

$$\underset{u(k+h|k)=F(k)x(k+h|k)}{Min} \xi \tag{48}$$

Theorem 1: It is assumed that $x(k|k) = x(k)$ is the state of the power grid in (35) under a set of uncertainty that is modeled by a convex hull, i.e., K. The state feedback matrix that minimizes the upper bound of $V(x(k|k))$ at each sampling time k is given by:

$$F(k) = Y(k)Q^{-1}(k) \tag{49}$$

where $Q > 0$ and Y can be obtained from the following linear objective minimization problem as follows:

$$\underset{\xi,Q,Y}{Min} \ \xi \tag{50}$$

Subject to two different LMIs as follows:

$$\begin{bmatrix} 1 & x(k)^T \\ x(k) & Q \end{bmatrix} \geq 0 \tag{51}$$

and

$$\begin{bmatrix} Q & * & * & * \\ A_lQ + B_lY & Q & * & * \\ {W_x}^{1/2}Q & 0 & \xi I & * \\ {W_u}^{1/2}Y & 0 & 0 & \xi I \end{bmatrix} \geq 0, l = 1, 2, .., n_v \tag{52}$$

where $*$ is used to show the symmetric structure of a matrix.

Proof (LMI-1): As already mentioned, minimizing the function of $V(k|k) = x(k|k)^T P x(k|k)$, $P = P^T > 0$ can be equivalent to:

$$\underset{\xi, P}{Min} \quad \xi \tag{53}$$

subject to $x(k|k)^T P x(k|k) \leq \xi$. With defining $Q^{-1} = P\xi^{-1}$ and using lemma 1, this will be equivalent to:

$$\underset{\xi, Q, Y}{Min} \quad \xi \tag{54}$$

Subject to:

$$\begin{bmatrix} 1 & x(k)^T \\ x(k) & Q \end{bmatrix} \geq 0 \tag{55}$$

Proof (LMI-2): In this section, the proof for equation (52) is represented. The control law and state-space model are first substituted in (44). As a result, we will have:

$$\begin{aligned} &x(k+h)^T[(A(k+h) + B(k+h)F)^T P(A(k+h)) \\ &+B(k+h)F - P + W_x + F^T W_u F]x(k+h) \leq 0 \end{aligned} \tag{56}$$

That is satisfied for all $h \geq 0$ if,

$$\begin{aligned} &(A(k+h) + B(k+h)F)^T P(A(k+h)) \\ &+B(k+h)F - P + W_x + F^T W_u F \leq 0 \end{aligned} \tag{57}$$

Then, $P = \xi Q^{-1}$ and $Y = FQ$ are substituted in the equation (57) and pre- and post-multiplying by Q. Finally, we use lemma 1 to have this equation:

$$\begin{bmatrix} Q & * & * & * \\ A(k+h)Q + B(k+h)Y & Q & * & * \\ {W_x}^{1/2}Q & 0 & \xi I & * \\ {W_u}^{1/2}Y & 0 & 0 & \xi I \end{bmatrix} \geq 0 \tag{58}$$

This inequality is affine in $[A(k+h), B(k+h)]$. Hence it is satisfactory for all $[A(k+h), B(k+h)] \in K, h \geq 0$, and this equation is also proven.

Theorem 2 (Constraints on Control Input and Output Signals): The following equations can define constraints on control input signals $u(k)$ and output signals $y(k)$:

$$\|u(k+h|k)\|_2 \leq u_{\max}, \|y(k+h|k)\|_2 \leq y_{\max} \tag{59}$$

where u_{max} and y_{max} are the maximum values of the control input and output signals, respectively. $\|\|$ is defined as a norm-2 matrix. It is worth noting that constraints on the control input and output signals of the system can be equal to the following LMIs as well:

$$\begin{gathered}\begin{bmatrix} u_{\max}^2 I & Y \\ Y^T & Q \end{bmatrix} \geq 0, \\ \begin{bmatrix} y_{\max}^2 I & C(A_l Q + B_l Y) \\ (A_l Q + B_l Y)^T C^T & Q \end{bmatrix} \geq 0, l = 1, ..., n_v\end{gathered} \tag{60}$$

Proof for Control Input signals: At sampling time h, and based on $F = YQ^{-1}$, we can have:

$$\begin{aligned}&\max_{h\geq 0} \|u(k+h|k)\|_2^2 = \max_{h\geq 0} \left\|YQ^{-1}x(k+h|k)\right\|_2^2 \\ &\leq \max_{z\in\Psi} \left\|YQ^{-1}z\right\|_2^2 = \alpha_{\max}(Q^{-1/2}Y^T Y Q^{-1/2})\end{aligned} \tag{61}$$

where the predicted states of the uncertain system can be proved to be always bound to a $z \in \Psi$ value. Then,

$$Q^{-1/2}Y^T Y Q^{-1/2} \leq u_{\max}^2 \rightarrow u_{\max}^2 I - Y^T Q^{-1} Y \geq 0 \tag{62}$$

Consequently, we can convert the above equation to the first LMI related to constraints on control input signals using the Schur complements.

Proof for Output Signals: For any $[A(k+h), B(k+h)] \in K, h \geq 0$, we can have:

$$\begin{aligned}&\max_{h\geq 0} \|y(k+h|k)\|_2 \\ &= \max_{h\geq 0} \|C(A(k+h) + B(k+h)F)x(k+h|k)\|_2 \\ &\leq \max_{z\in\psi} \|C(A(k+h) + B(k+h)F)z\|_2 = \\ &\alpha'_{\max}[(C(A(k+h) + B(k+h)YQ^{-1})] \leq y_{\max}\end{aligned} \tag{63}$$

We can rewrite this inequality based on norm-2 of both sides of the previous inequality:

$$\begin{aligned}&[C(A(k+h)+B(k+h)YQ^{-1})] \leq y_{\max} \rightarrow \\ &Q^{-1/2}[A(k+h)+B(k+h)Y]^T C^T C[A(k+h) \\ &+B(k+h)Y]Q^{-1/2} \leq y_{\max}^2 I\end{aligned} \tag{64}$$

We can use the Schur complements to prove the second LMI relating to output signals. The above equation can satisfy all convex hulls ($l = 1, ..., n_v$).

4.7 Simulation Results and Discussion

4.7.1 Performance of Deep CNN Model

Training a deep CNN model under imbalanced data samples during the classification task can lead to poor performance in minority classes and misleading metrics, e.g., accuracy. In other words, the accuracy metric can be calculated as a high value for imbalanced data samples, even if the model fails to accurately predict minority classes. To prevent such problems, we have provided a balanced data sample for three main classes, i.e., normal operation of the system (7,650 samples), EV-based load-altering attacks (7,650 samples), and fault and line disconnection (7,500 samples). All data have been collected from the co-simulation platform developed in the EMTP-RV. The training and testing datasets are partitioned by 80% and 20% of the total datasets, respectively. The accuracy and loss function behavior for the training and testing dataset of the classification task has been depicted in Fig. 4.8. To show the trained CNN model's performance during classification, several evaluation metrics, i.e., balanced accuracy (BACC), precision, recall, and F_1 score, can be suggested. The main reason for selecting balanced accuracy is that it can provide a more acceptable evaluation of the proposed deep CNN, especially in the presence of imbalanced data samples. These metrics for

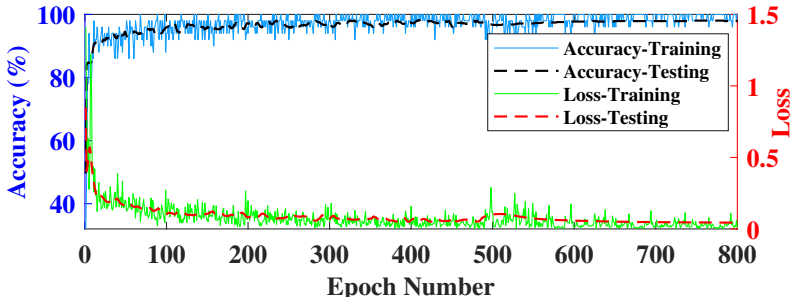


Figure 4.8: Plot of accuracy and loss function for training and testing dataset.

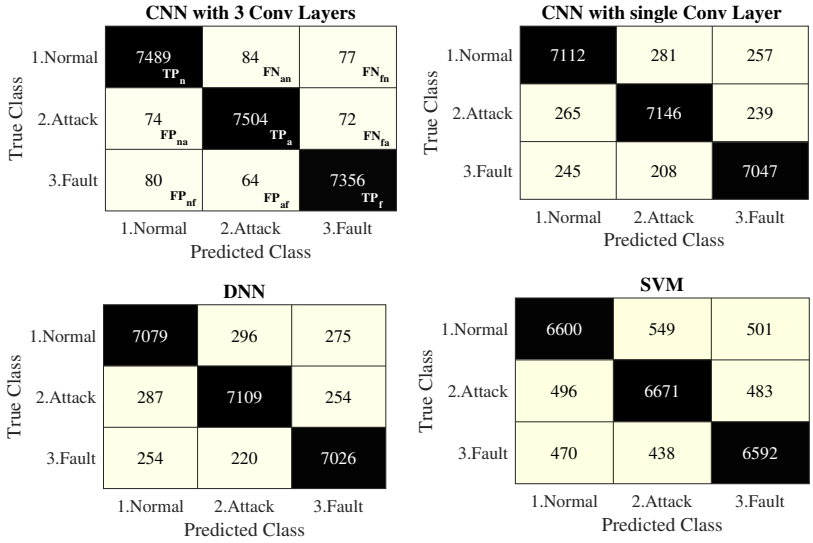


Figure 4.9: Confusion matrix for different methods of the classification task.

three classes can be calculated as follows[64]:

$$
\begin{aligned}
&BACC = \frac{1}{3}\left(\frac{TP_n}{TP_n+FN_{an}+FN_{fn}} + \frac{TP_a}{TP_a+FN_{fa}+FP_{na}}\right.\\
&\left.+\frac{TP_f}{TP_f+FP_{nf}+FP_{af}}\right)\\
&Precision = \frac{TP_n+TP_a+TP_f}{TP_n+TP_a+TP_f+FP_{na}+FP_{nf}+FP_{af}}\\
&Recall = \frac{TP_n+TP_a+TP_f}{TP_n+TP_a+TP_f+FN_{an}+FN_{fn}+FN_{fa}}\\
&F_1score = \frac{2\times Precision\times Recall}{Precision+Recall}
\end{aligned}
\tag{65}
$$

where TP_n, TP_a, and TP_f are true positive labels for normal, attack, and fault classes, respectively. Also, FN_{an}, FN_{fn}, and FN_{fa} are false negative labels, and FP_{na}, FP_{nf}, and FP_{af} are defined

Table 4.1: Comparison Between Different Methods for Classification Task

Approach	**Balanced Accuracy**	**Precision**	**Recall**	**F_1 score**
CNN with 3 Conv Layers	98.02 %	99.03 %	98.97 %	99.00 %
CNN with single Conv Layer	93.45 %	96.74 %	96.48 %	96.61 %
DNN	93.05 %	96.54 %	96.26 %	96.40 %
SVM	87.12 %	93.40 %	92.84 %	93.12 %

Table 4.2: Comparison Between Different Methods for Regression Task

Approach	**Number of samples**		**Error**	
	Training	Testing	$\Delta\hat{P}_{sw}$	$\hat{f}_{sw}$
CNN with 3 Conv Layers	6120	1530	5.7e-3	2.0e-4
CNN with single Conv Layer	6120	1530	1.7e-1	5.7e-1
SVM	6120	1530	23e-1	11e-1
MLP	6120	1530	35e-1	13e-1

to represent interaction between different classes. The confusion matrices for our proposed model and several techniques used in classification tasks, e.g., the CNN model with one $Conv$ layer that consists of learnable kernel functions for convolution operation, a deep neural network (DNN), and a support vector machine (SVM) [65], have been illustrated in Fig. 4.9. These matrices can summarize the performance of a classification task by comparing true and predicted classes for the testing dataset. It can be seen that true positive labels for normal, attack, and fault classes for our proposed CNN model are higher than other techniques. Moreover, a numerical analysis has been represented for the proposed CNN model and the techniques mentioned in classification tasks in Table 4.1. Based on this table, the proposed model possesses a higher level of evaluation metrics for giving information about the security status of the power grid. The main reason is that a deep CNN structure including multiple convolutional layers can extract better features for classification and regression, making this framework a proper tool for complicated applications with many uncertainties in operation. Another evaluation metric is AUC (area under curve), which can be used to evaluate the performance of the trained model in scenarios where the classes might be imbalanced [64]. To calculate this metric, we must first plot the receiver operating characteristic (ROC) curve, representing the true positive rate against the false positive rate for different classes. These ROC curves have been illustrated in Fig. 4.10 for the three mentioned classes. As a result, the AUC of normal, attack, and fault classes are calculated as 0.9590, 0.9873, and 0.9808, respectively.

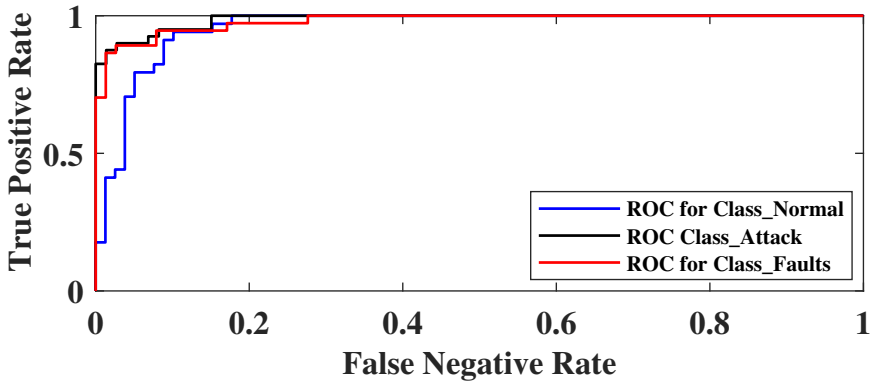


Figure 4.10: ROC curves for three different classes

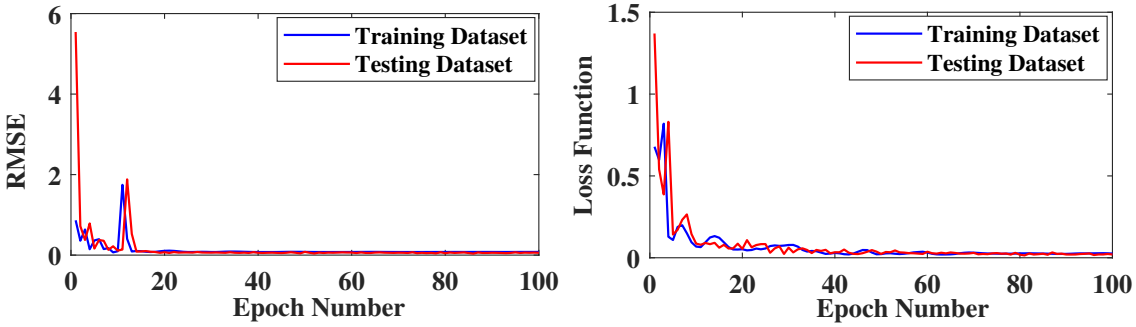


Figure 4.11: Plot of RMSE and loss function for training and testing dataset.

According to the online switching attack vector estimation framework in Fig. 4.6, after completing the above classification task, the amplitude and frequency of switching attacks must only be predicted for the attack class. For this regression task, we have also considered 7,650 total samples during uncertainties in the system's operation, e.g., different wind speeds and WTG outages in the wind farm versus amplitudes of EV load switching attacks. In Table 4.2, the level of error for the amplitude and the frequency of the switching attack over the testing dataset have been shown. It can be seen that the proposed deep CNN with three Conv layers delivers the best performance compared to the CNN with a single Conv layer, SVM, and Multi-Layer Perceptron (MLP) models. The root mean square error (RMSE) and loss function of the training and testing datasets for the regression task have been shown in Fig. 4.11. After training this dataset for regression purposes, it can be seen that the RMSE and loss function values have converged rapidly. The main reason for this rapid convergence is that the number of convolutional layers and their sizes, along with the Max pooling and dropping layers, have been appropriately selected, capturing the hierarchical features

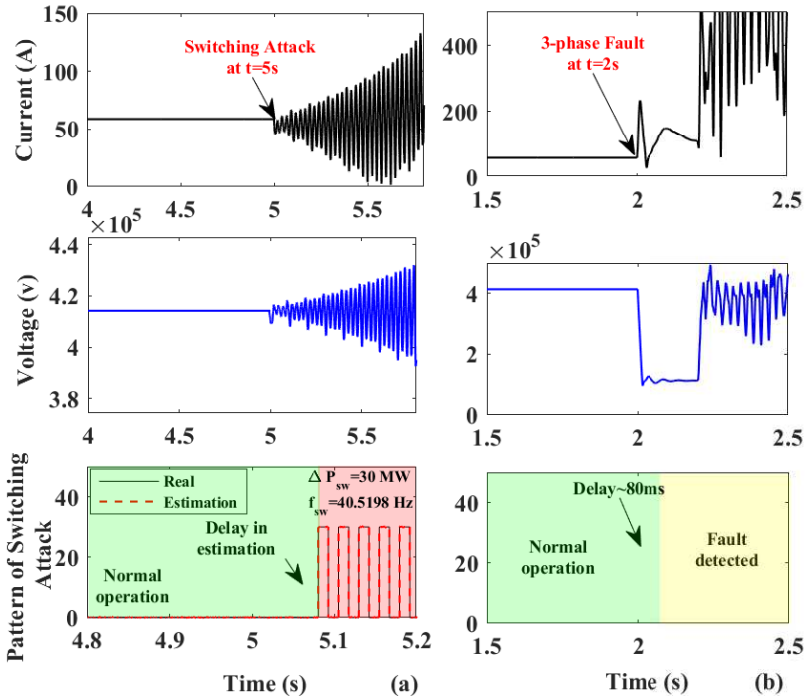


Figure 4.12: Performance of Algorithm 3 in notifying the system's security status and estimating the amplitude and frequency of a switching attack.

of the generated dataset. Moreover, instead of the prolonged data samples of voltage and current during observation windows (i.e., 90 samples for voltage and 90 samples for current), we have used the mean and standard deviation of these samples (i.e., the mean and standard deviation of voltage and current, $[\mu_v, \sigma_v, \mu_i, \sigma_i]$) as input data, making the training of these datasets easier and more efficient.

To show the performance of the proposed CNN with three $Conv$ layers in the case of a specific uncertainty, V_w =0.6 p.u. and N_{wtg} =150, an EV load switching attack with the amplitude of 30 MW at t =5s is applied to the system. Algorithm II can determine the security status of the power grid and then estimate the switching attack vector, as shown in Fig. 4.12. (a). It can be seen that the delay for estimating the switching attack vector is about 5 cycles ($\sim$ 80ms), making this algorithm a model for online detection purposes. Moreover, the performance of the proposed algorithm in detecting a three-phase fault occurred at t =2s, and distinguishing faults from the normal operation has been shown in Fig. 4.12. (b).

4.7.2 Performance of Proposed Mitigation Technique

Due to the lack of 100% accuracy of the proposed method for detecting EV-LAAs, a wide-area damping controller can also be developed. To demonstrate the superiority of our proposed controller, its performance can be compared with recent wide-area damping controllers in power grids:

- A two-degree of freedom (2DOF) approach has been suggested in[57] to mitigate subsynchronous resonances in wind-integrated power grids. This 2DOF controller consists of derivative blocks added to the current control loop of the RSC.

- Another wide-area damping controller deployed for mitigating the SSCI in wind-integrated power grids is the linear quadratic regulator (LQR) [3] in the industrial environment. This controller is an optimal state-feedback strategy that minimizes a quadratic cost function by calculating an optimal control gain matrix through the solution of the algebraic Riccati equation. The LQR controller balances control efforts and state deviations to achieve acceptable performance in power grid applications.

- H_∞ controller as a robust technique has been used in various power system applications[11]. In this controller, the main aim is to design a gain matrix that ensures external disturbances, e.g., load-altering attacks, do not disrupt the power grid's performance. During the design of this controller, a set of objectives in time and frequency domains, such as closed-loop system poles restricted into a desired region of the s-plane, can be defined using linear matrix inequality (LMIs).

- Finally, a robust supplementary technique based on MPC is designed for online control optimization at the wind farm level during EV load switching attacks, considering the uncertainties in wind speed and WTG outages.

To design our controller and obtain a convex hull from the nominal model with poly-topic uncertainties based on (36), different wind speeds (V_w = [0.6 p.u., 1 p.u.]) and WTG outages (N_{wtg} = [266, 50]) are first studied. As such, their corresponding state-space models, i.e., matrices A_l, B_l ($l \in n_v$), and C, can be extracted using system identification approaches based on the

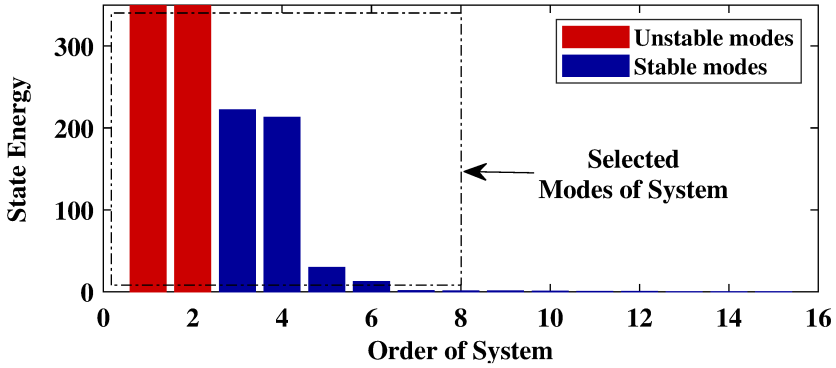


Figure 4.13: Hankel singular value (HSV) of the wind farm-integrated power grid for selecting a proper order for the system as 8 states.

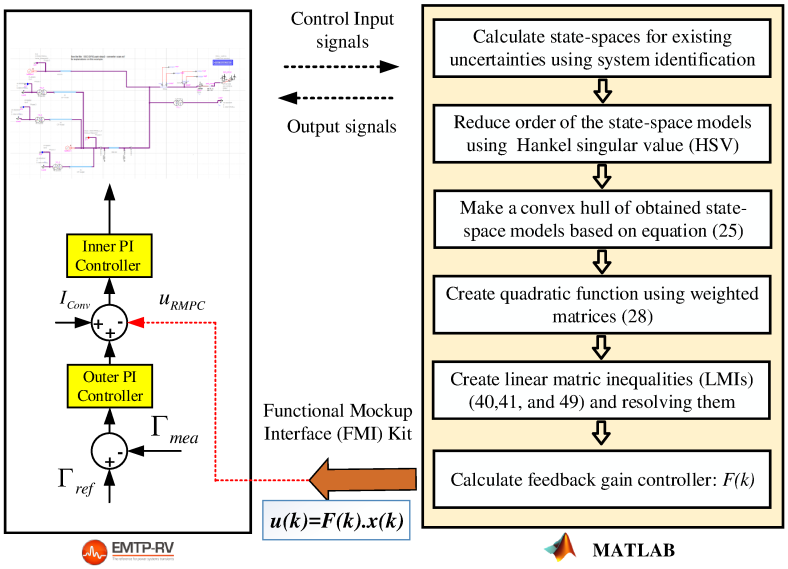


Figure 4.14: Co-simulation between EMTP-RV and MATLAB software.

prediction error minimization technique[61]. Then, the Hankel singular value (HSV) technique is used to reduce the order of the obtained state-space models and consider states of the power grid that possess unstable modes, i.e., SSCI modes. The analysis of HSV, as illustrated in Fig. 4.13, shows that a reduced order model with 8 states can preserve most of the system's dynamic behaviors. The main reason for deploying the HSV technique is that designing a controller for a high-order system can be sensitive to noise and impractical in industrial environments. After solving a set of LMIs, i.e., equations (51, 52, and 60), the feedback controller matrix $F(k)$ is calculated using equation (49) by selecting a proper value of ξ based on (50). This gain matrix can be transferred to the EMTP-RV using the FMIKits-Simulink toolbox. The overall layout of collaboration between the

Algorithm 5: Robust Control Technique for Switching Attack Mitigation

for $1:1:n_{unc}$ *(number of uncertities in system)* **do**

Transfer: Control input and output signals from EMTP-RV to MATLAB

Calculate: State-space model of the system for different uncertainties

Reduce: order of model by Hankel singular value (HSV) technique

end

1) Build: a convex hull of all calculated state-spaces, i.e., $K = Convex\_hull\{[A_1, B_1], ...[A_{n_v}, B_{n_v}]$ for the total number of vertices n_v

2) Select: weighting matrices W_x and W_u

3) Select: matrices u_{max} and y_{max} based on (59)

4) Build: quadratic quality criterion based on (39): $J_p(k)$ for prediction horizon p

5) Resolve: LMIs equations, i.e., (51, 52, and 60), using YALMIP Toolbox

6) Calculate: $Q(k)$ and $Y(k)$ as auxiliary matrices by resolving LMIs

7) Calculate: gain matrix based on (49): $F(k) = Y(k)Q^{-1}(k)$

8) Transfer: gain matrix $F(k)$ from MATLAB to EMTP-RV using FMIKits

EMTP-RV and MATLAB has been illustrated in Fig. 4.14. It can be seen that the calculated control input signal, i.e., $u_{RMPC} = [u_{dr}, u_{qr}, u_{dg}, u_{qg}]$, is added to the inner PI control loop to mitigate the SSCI impacts created by EV load switching attacks. As a practical example, the matrices of a linearized model of the wind-integrated power grid for a particular uncertainty, e.g., V_w =0.6 p.u. and N_{wtg} =150, after the order reduction HSV technique, are obtained as follows:

$$A = \begin{bmatrix} 6.207 & -50.857 & -96.2419 & 156.80 & 235.57 & -290.395 & -17.687 & -51.722 \\ 39.514 & -2.020 & -75.86 & 108.855 & -51.923 & 184.792 & -160.190 & 100.613 \\ 77.563 & 64.584 & -13.8080 & 162.033 & -196.766 & 205.10 & -198.34 & 117.2809 \\ -152.063 & -159.255 & -250.932 & -90.724 & 207.458 & 311.27 & 98.145 & -96.831 \\ -357.41 & 17.492 & 37.90 & -833.966 & -432.193 & -2457.3 & -876.887 & 2639.8 \\ 624.178 & -264.442 & -204.096 & 507.796 & 225.393 & -897.726 & 1144.5 & -2488.3 \\ -11.555 & 100.427 & 49.800 & -495.985 & 22.998 & -1732.7 & -323.38 & 1318.3 \\ 130.572 & -51424 & 109.951 & 989.728 & -2088.2 & 5256.8 & -177.187 & -2617.1 \end{bmatrix} \quad (66)$$

Table 4.3: Different Selections of Weighting Matrices for Optimizing Performance of RMPC

Different W_x and W_u	**Time of solving (s)**	$J_p(k)$	ξ
W_x=diag[0.5,0.5,0.5,0.5], W_u=diag[0.2,0.2,0.2,0.2]	1.269	15.295	1.57 $\times 10^4$
W_x=diag[1,1,1,1], W_u=diag[0.2,0.2,0.2,0.2]	1.256	15.258	1.61 $\times 10^4$
W_x=diag[1.5,1.5,1.5,1.5], W_u=diag[0.2,0.2,0.2,0.2]	1.256	15.255	1.61 $\times 10^4$
W_x=diag[1.5,1.5,1.5,1.5], W_u=diag[0.25,0.25,0.25,0.25]	1.253	15.312	1.58 $\times 10^4$
W_x=diag[1.5,1.5,1.5,1.5], W_u=diag[0.15,0.15,0.15,0.15]	1.251	15.128	1.61 $\times 10^4$
W_x=diag[1.5,1.5,1.5,1.5], W_u=diag[0.1,0.1,0.1,0.1]	**1.249**	**14.988**	**1.63** $\times 10^4$
W_x=diag[1.5,1.5,1.5,1.5], W_u=diag[0.05,0.05,0.5,0.05]	1.251	15.012	1.61 $\times 10^4$

$$B = \begin{bmatrix} 22.526 & 10.719 & -70.696 & 222.55 & -28.218 & -12.636 & -32.148 & -0668.77 \\ 23.363 & 9.4403 & -71.355 & 223.872 & -28.08 & -13.598 & -32.129 & -667.251 \\ 22.402 & 9.715 & -70.094 & 2525.11 & -26.581 & -14.281 & -31.782 & -660.987 \\ 22.0435 & 8.588 & -71.253 & 223.48 & -21.568 & -12.68 & -30.698 & -658.369 \end{bmatrix}^T \tag{67}$$

Considering the same steps, a convex hull of the nominal state-space models, i.e., $[A, B] \in K$, can be obtained under existing uncertainties in wind speed and WTG outages of the wind farm. The weighting matrices that are used in the quadratic quality criterion, (39), can be selected from Table 4.3 with a minimum value of the quadratic quality criterion ($J_p(k)$) and a maximum value of the upper bound of the Lyapunov function (ξ). It is worth mentioning that trade-offs between tracking a desired reference trajectory and minimum control efforts have been considered when selecting the weighting matrices for both state and control input signals in the proposed quality criterion. In some cases, increasing the output weighting matrix may lead to higher control efforts. As a result, the maximum control input signals and output signals are considered to be $u_{max} = [0.1, 0.1, 0.1, 0.1]^T$ and $y_{max} = [0.15, 0.15, 0.15, 0.15]^T$, respectively. Constraints on control input signals can prevent saturation of the RSC and GSC used in the wind-integrated power grid. Constraints on output or measurement signals can lead the wind farm to remain connected to the power grid and maintain its continuous operation against cyber attacks. In other words, the wind farm through monotonic active power generations can mitigate the impacts of EV-LAAs that want to excite the SSCI mode of the

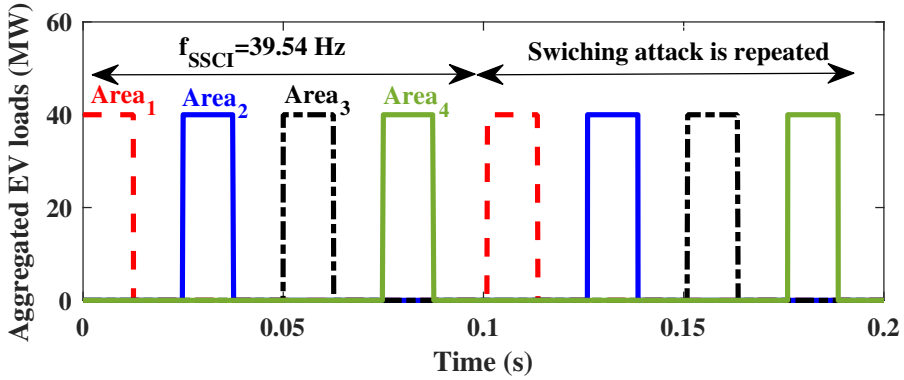


Figure 4.15: The pattern of aggregated EV load switching attacks for two consecutive periods.

wind-integrated power grid. The output matrix, i.e., C, is also obtained as:

$$C = \begin{bmatrix} -13.534 & -2.1078 & -1.0350 & -3.567 & -11.589 & -0.429 & 18.7614 & 0.3477 \\ 0.6592 & 27.659 & 2.076 & -1.198 & 1.088 & 0.055 & -2.0008 & -0.0364 \\ -1.0878 & -1.192 & 3.841 & 0.0785 & -0.0147 & -0.0019 & 0.0001 & -0.0005 \\ 0.5253 & 0.226 & -0.065 & -0.0324 & 0.0116 & -0.0059 & 0.0002 & 0.0001 \end{bmatrix} \tag{68}$$

Finally, the proposed RMPC is designed using the MUP toolbox [66] and the optimization problem is formulated by the YALMIP toolbox and resolved by SeDuMi[67]. In this regard, the feedback controller gain, $F(k)$, is calculated accordingly:

$$F = \begin{bmatrix} 23.802 & 64.663 & 0.374 & 2.707 & 20.354 & 0.765 & -33.469 & -0.613 \\ 25.933 & -17.780 & 7.884 & 8.428 & 23.868 & 0.838 & -38.569 & -0.708 \\ 22.246 & 0.601 & 1.109 & 6.171 & 18.205 & 0.744 & -29308 & -0.561 \\ 10.738 & -56.664 & -11.741 & 5.065 & 6.306 & 0.192 & -9.661 & -0.176 \end{bmatrix} \tag{69}$$

A summary of steps that can be taken to design this robust LMI-based control framework has been represented in Algorithm 5. To show the performance of the RMPC, two different scenarios are discussed based on attack models $\mathbf{A}$ and $\mathbf{B}$ defined in Section 4.4, respectively:

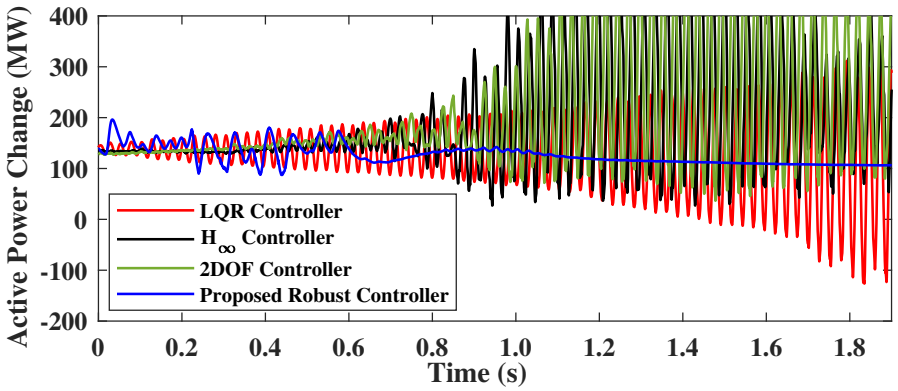


Figure 4.16: Performance of different controllers during EV load switching attacks under uncertainty (i.e., V_w=0.8 p.u., N_{wtg}=150).

Scenario I

In this scenario, EV load switching attacks with an amplitude of 40 MW are applied to four areas of the power grid under a specific uncertainty, i.e., V_w =0.8 p.u. and N_{wtg} =150. The mentioned uncertainty causes an unstable SSCI mode, i.e., $1.2 \pm j248.36$. The patterns of aggregated EV loads, which can be switched based on rectangular patterns with the frequency of the SSCI mode ($f_{SSCI} = 39.54$Hz), have been illustrated in Fig. 4.15. This switching attack vector can excite the mentioned mode, leading to changes in active power generated by the wind farm. The performance of the robust MPC framework has been compared to recent wide-area damping controllers, e.g., the 2DOF, LQR, and H_∞ controllers in the case of mitigating oscillations, as illustrated in Fig. 4.16. It can be seen that the 2DOF cannot reduce the impacts of switching attacks effectively. The main reason is that this controller can deliver acceptable performance for a single operating condition when the power grid's model remains constant. Moreover, high-frequency disturbances can impact the controller's action due to existing derivative blocks in the structure of the 2DOF controller. Regarding the performance of the LQR, it can be seen that this controller cannot mitigate the impact of such attacks, and from the first moments, the active power generated by the wind farm starts to oscillate. Since we cannot model control objectives, e.g., disturbance rejection and noise attenuation, in the framework of the LQR controller, it fails to provide satisfactory performance during external disturbances and uncertainties in the state-space model of the system. Moreover, for the H_∞ controller with a more complex control structure, control objectives, e.g., disturbance rejection, noise attenuation, and minimizing the control effort, can be satisfied. On this basis, it can be ob-

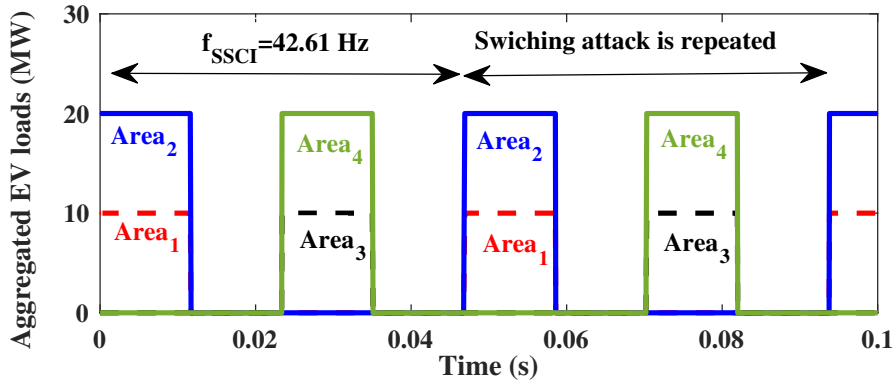


Figure 4.17: The pattern of switching aggregated EV load switching attacks to deal with the amplitude of this attack.

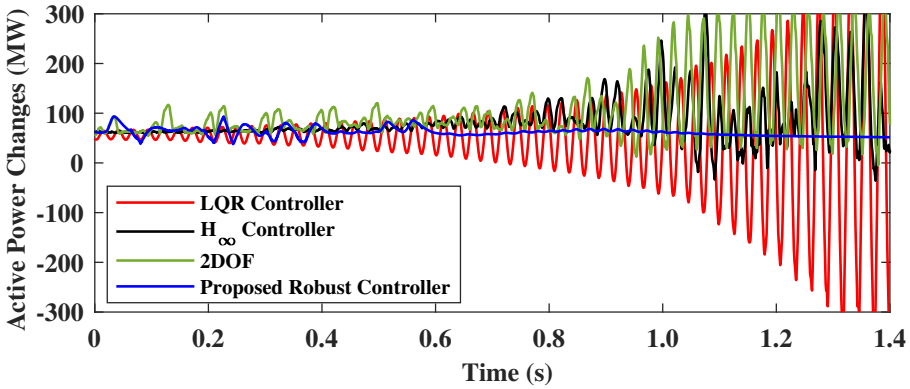


Figure 4.18: Performance of different controllers during EV load switching attacks under uncertainty (i.e., V_w=0.6 p.u., N_{wtg}=100).

served that this controller can be resilient to this switching attack vector until 0.6 seconds, and then it moves toward instability. In designing H_∞, some external disturbances, e.g., EV load switching attacks, can be modeled. However, other uncertainties, e.g., wind speed and WTG outages, which can lead to changes in the components of the matrix A in the state-space model of the system, cannot be modeled using the H_∞ controller. In summary, an accurate and fixed mathematical model of the system must be available to implement the H_∞ framework in wind-integrated power girds. Using the proposed robust method, poly-topic uncertainties in the power grid's operations can be represented as a convex hull of the nominal state-space model (K). From Fig. 4.16, it takes about 0.8 seconds for the proposed control technique to adjust control input signals at the wind farm's level and mitigate the impacts of the EV loads switching attack during the mentioned uncertainties. However, the conventional wide-area controllers, i.e., the 2DOF, the LQR, and the H_∞, cannot actively participate in the mitigation schemes due to their limited stability margins. In contrast, the

proposed robust controller can harness the active power oscillation and reach a stable point, leading wind farms to remain connected to the power grid and participate in continuous active power generation.

Scenario II

In this scenario, an additional pattern is implemented to decrease the amplitude of manipulated EV loads in different areas of the power grid for EV load switching attacks, as discussed and illustrated in Fig. 4.3. (b). In this scenario, the wind speed and the number of WTGs are V_w =0.6 p.u. and N_{wtg} =100, respectively. This uncertainty can result in a pair of unstable SSCI modes, i.e., $1.903 \pm j267.62$, that can be calculated using the system identification approaches. The pattern of this EV load switching attack with the aim of exciting the SSCI mode ($f_{SSCI} = 42.61$Hz) is shown in Fig. 4.17. In this figure, 10 MW and 20 MW of EV loads in Area$_1$ and Area$_2$ are compromised to launch this switching attack. Similarly, this pattern is also repeated for EV loads in Area$_3$ and Area$_4$ of the power grid. As such, the required EV loads for launching the proposed switching attack can be distributed among four areas. To compare the performance of the proposed RMPC with the mentioned controllers, the active power generated by the wind farm during this switching attack vector is shown in Fig. 4.18. It can be seen that the 2DOF cannot stabilize the power grid due to its dependency on a single operating point. The LQR controller cannot guarantee stability in the presence of new uncertainty. Therefore, it cannot stabilize the subsynchronous oscillations for the proposed wind-integrated power grid. Also, subsynchronous oscillations in the power grid cannot be mitigated using the H_∞ controller due to existing uncertainties in the system's model that can lead to several SSCI modes with different damping values and frequencies. In contrast, the proposed RMPC can cover all lightly damped or unstable SSCI modes in the form of a convex hull and calculate the gain matrix to stabilize the system effectively. Since this uncertainty (i.e., V_w =0.6 p.u. and N_{wtg} =100) contributes to the SSCI mode near the imaginary axis of the s-plane, fluctuations in active power generated by the wind farm in this uncertainty are lower compared to the first scenario. Since the system's model is fixed during the design of the 2DOF, the LQR, and H_∞ controllers, their stability margins are limited compared to the case when the model of the wind farm is continuously updated. As a result, traditional controllers cannot deliver acceptable

performance in mitigating oscillations originating from EV load switching attacks [68].

4.8 Conclusion

In this chapter, adversaries could maliciously exploit EV charging stations (EVCSs) and inject malicious malware into their firmware to launch coordinated EV-LAAs based on the frequency of subsynchronous control interaction (SSCI) modes in a wind-integrated power grid. A deep convolutional neural network (CNN) was trained based on voltage and current measurements obtained from the phasor measurement unit (PMU) at the wind farm substations. This trained model could classify the source of the event that results in oscillation with a balanced accuracy of 98.02% and then estimate the switching attack vectors. This model included consecutive convolutional layers to extract better features from input data, making it a detection framework in the presence of different uncertainties in the operation of wind-integrated power girds. Since this CNN model might neglect a few EV-LAAs due to the huge number of attack vectors with varying combinations of amplitudes and frequencies during uncertainties in wind speeds and the number of WTG outages, a robust model predictive controller (RMPC) was defined as a supplementary solution. Existing uncertainties in wind speeds and WTG outages during different amplitudes of EV-LAAs and constraints on control input and output signals were investigated when defining linear matrix inequalities (LMIs). After solving this set of LMIs, a state-feedback controller was obtained to alleviate the impacts of such attacks in the presence of uncertain dynamical systems with external disturbances. The authors have conducted a performance comparison between the proposed robust controller and recent wide-area controllers, such as 2DOF, LQR, and H_∞ controllers, which proved ineffective in handling uncertainties and attacks. However, designing this robust controller needs the state-space model of the system during different uncertainties, and its performance is not optimal in the wide range of different load-altering attacks. From this perspective, one future research direction can be developing a reinforcement learning control framework that helps operators design a controller without an accurate model of the system. This controller can mitigate the impacts of such attacks during different uncertainties by interacting with the environment and updating control input signals. Another future research direction is to design an adaptive control framework, where this load-altering attack vector

can be estimated to design online control signals in the case of different uncertainties and external disturbances.

Chapter 5

Developing a Security Metric for Assessing the Power Grid's Posture against Attacks from the EV Charging Ecosystem

5.1 Motivation

Providing reliable and efficient services for EV users necessitates the use of cyber layers on top of physical layers in EV ecosystems. The deployment of such cyber layers, however, makes these ecosystems an appealing target for various cyber-attacks—e.g., data manipulation, malware injection, and intrusions—which are crafted to deteriorate the operation of power distribution networks. On this basis, this chapter develops a metric that captures the security posture of EV ecosystems, considering the possible attacks and their associated impacts on distribution grids. First, potential attack graphs are obtained to show the connections between the adversaries' access points and the consequences of attack vectors. Then, a Markov decision process (MDP) tree is generated, using probabilities of adversaries' success rates for a specific attack vector and unique reward functions.

The developed MDP tree is then resolved by a policy iteration algorithm to calculate the value function of each state, related subsequent adversarial actions from the attackers' viewpoint, and quantify the security posture of each state. Finally, using the obtained metric, a deep convolutional neural network (CNN) is trained offline to notify the distribution system operators (DSOs) of the security status of EV ecosystems, i.e., secure and alarm situations. DSOs can use the developed security metrics to design consequent corrective actions during critical cyber-attacks. To demonstrate the usefulness of the proposed security metric in quantifying the security status of the grid, a cyber-physical testbed is built. This testbed integrates a virtual sphere (vSphere) to simulate the cyber parts of the EV ecosystem as well as a real-time simulator to model two distribution networks, i.e., IEEE 33- and 141-bus, under DSO control center based on IEC 61850. For a distribution network with dynamic sections that can be created using the operation of tie-switches, a supplementary strategy has also been suggested. This strategy is evaluated under the IEEE 69-bus distribution network to calculate the related security metric and update the security monitoring framework.

5.2 Contribution

Recently, the possible attack vectors have persuaded researchers to scrutinize the impacts of compromising components of the EV ecosystem on power grid operation. As such, they have introduced detection and mitigation strategies to alleviate these impacts [69, 11]. However, the mentioned approaches cannot cover all possible attack vectors in EV ecosystems. Moreover, operators should have a monitoring system and related metrics to measure the security posture of their cyber-physical systems. The importance of security metrics has recently motivated researchers to design security evaluation techniques. These metrics can be used to infer information from system operations and warnings from installed security monitoring systems with the intent of quantifying overall system security[70, 71]. As such, two main approaches have been suggested in the literature to define security metrics for power grids. In the first method, a set of mathematical equations, which are generally obtained from state estimations and load flow analysis, are used to formulate the security status of the power grids. For example, in [72], authors have introduced a security metric that quantifies cyber attack impacts on IP-based substations and identified compromised substations that

can pose a significant risk to power grids. In another work [73], a security index is defined based on mathematical load flow equations that can measure the margin between normal operation and critical situations of the power grids. A security-oriented risk management technique, i.e., CPIndex, has been developed in [74]. It calculates cyber-physical security indices using generated logs and topological information about the power network configuration using Bayesian network models. However, the performance of proposed security metrics is limited to a single contingency, and they cannot consider all probable security situations in cyber-physical models[75]. In the second approach, researchers have used the Markov Decision Process (MDP) to quantify the physical impact of cyber attacks on different components of power grids and define a security metric accordingly. In [76], cyber and physical network topologies are used to define a security metric, i.e., the SOCCA metric, representing the overloading of transmission lines in the case of cyber attacks. Another security metric is designed in [77], which associates cyber alerts received by an operator with their potential physical impacts on the grid operation using an MDP tree. Moreover, a definition for a cyber-physical resilience metric is suggested in [78]. This metric can quantify the resilience level of the cyber-physical model based on the MDP as well as formulate compromised components of power grids and their inter-dependencies. The benefit of using the MDP tree in these works is that during cyber attacks, there are decisions that can be partly randomized based on different attack vectors and partly under the control of attackers as decision-makers. The states and branches in those MDP trees are formed to model compromised components of power grids and the behavior of adversaries in such systems. However, a security metric has not yet been tailored to consider the unique vulnerabilities of cyber layers in the EV ecosystem. Moreover, the existing metrics have been designed for transmission systems while neglecting the need for a security metric for power distribution networks in the presence of the mentioned EV-based attacks.

In light of this discussion and considering the mentioned research gaps, this chapter investigates possible attack vectors in EV ecosystems. This chapter also explores their corresponding impacts on the operations of distribution networks by developing an EV-based attack security metric. First, cyber and physical vulnerabilities in EV ecosystems are studied to obtain attack graphs and analyze compromised components of EV ecosystems and related adversarial actions. Second, an MDP tree is developed using the common vulnerability scoring system (CVSS) to assign the probabilities of

adversaries' success rates to each branch of this tree. Moreover, a reward function is calculated and allocated to each branch for sabotaging EVCSs in the distribution network based on voltage deviation at different buses, excessive active power losses of lines, and unavailability of charging stations for EV users. Then, the proposed MDP tree is solved by the modified policy iteration algorithm to calculate the value of each state in the MDP tree and the related optimal adversarial action. These numerical values for each state provide a security index that quantifies cyber threats that compromise charging stations in different zones of distribution networks. This metric not only considers compromised EVCSs in a single zone of distribution networks but also investigates multiple contingencies that may occur in different zones of such networks. Finally, for different operations of distribution networks in the presence of EV-based attacks, i.e., secure and alarm, the developed MDP tree can be resolved to gather a collection of raw data for training a deep convolutional neural network (CNN). The trained deep CNN will be deployed to inform DSOs about the security status of the grid. This information can be used for preventing potential power outages and taking remedial action during emergency conditions. A real-time testbed that integrates the distribution network model with cyber and physical layers of the EV ecosystem is used to show the usefulness of the proposed security metric in quantifying the security status of IEEE 33-bus and 141-bus of Caracas. The topology of the distribution network may change due to multiple switching scenarios, creating dynamic sections. As such, a supplementary strategy has also been introduced to calculate our security metric and update the security monitoring system in the looped IEEE 69-bus distribution network. In summary, the main contributions of this chapter can be summarized as follows:

(1) Investigating cyber vulnerabilities in EV ecosystems and obtaining attack graphs to analyze the impacts of EV-based attacks on the operation of distribution grids;

(2) Developing a metric that quantifies the security status of EV ecosystems and their associated distribution grids using an MDP tree. This tree is formed based on power flow equations, vulnerabilities in the cyber layers of EV ecosystems, and multiple contingencies in different zones of distribution networks;

(3) Solving the customized MDP tree using a policy iteration algorithm to quantify the security status of distribution networks. Then, a deep CNN is trained offline based on the obtained set

of different results from the MDP trees to infer the system's security status, i.e., secure and alarm situations. To do this, a testbed that integrates the cyber layers of the EV ecosystem in the virtual sphere (vSphere) with a real-time model of distribution networks in OPAL-RT 5650 is used to illustrate the application of the developed metric in the DSO control center.

(4) Since the topology of the distribution networks may change due to multiple switching scenarios, the voltage profiles are not necessarily related to closed buses in fixed zones. As such, a supplementary strategy has also been suggested to calculate our security metric and update the security monitoring framework in the presence of dynamic sections in the looped IEEE 69-bus distribution network.

5.3 Customizing MDP Tree for EV Ecosystems

An MDP tree is a graphical representation that can be employed to illustrate the decision-making process under different contingencies. This tree can provide a mathematical framework to model cyber attack paths where decisions are partly randomized based on potential vulnerabilities in EV ecosystems and partly under the knowledge and control of attackers. In the MDP tree, a decision-maker (i.e., attacker) can move from the first state s (i.e., component) to the second state s' (i.e., another component) by taking action a with the probability of $P_a(s, s')$. For this transition, the decision-maker may obtain a reward, i.e., $RF_a(s, s')$. Based on potential vulnerabilities in the EV ecosystem discussed in Section 2.2, states of the MDP tree can be mapped to the components of this system that can be maliciously targeted by adversaries. Moreover, logical branches, which are compatible with adversarial actions, can be established among states of an MDP tree. Initially, adversaries may have no access to the cyber layers of EV ecosystems; however, they will obtain adequate privilege to cause detrimental impacts on the operation of such networks. The main aim of building this MDP tree based on states and branches is to show how attackers can compromise components of the EV ecosystem sequentially, penetrate cyber or physical layers of charging stations, and finally manipulate EV loads in distribution networks. Generally, an MDP tree includes a set of components, i.e., $\{\mathcal{S}, \mathcal{A}, P_a(s, s'), RF_a(s, s'), \gamma\}$, that can be described as follows:

5.3.1 Set of States

States in an MDP tree represent environmental configurations or circumstances that can consist of different factors, such as location and time. In this work, we define a finite set of states for the MDP tree as compromised components of EV ecosystems and indicate them by $\mathcal{S}$. As mentioned before, cyber components—such as CSMS, OCPP, mobile and web applications, and physical USB ports—can be defined as the attacker's access points and accessible primary states in the MDP tree. The states of this MDP tree can also reflect the attack propagation in the cyber-physical model of our EV ecosystem and the privileges that can be obtained through performing adversarial actions. For example, in the first attack graph, OCPP and charging stations in different zones of the power grid are defined as the states of the MDP tree. In the second attack graph, CSMS, firmware repository, and charging stations, that can be compromised to impact the distribution network, are defined as states.

5.3.2 Set of Adversarial Actions

$\mathcal{A}$ is a set of adversarial actions that an attacker might select. Each adversarial action is defined as known or zero-day vulnerability explorations in cyber-physical models. An attacker can use different techniques, e.g., MitM attack and SQL injection, to penetrate the cyber layers of the EV ecosystems and obtain access to further states of systems to achieve more malicious purposes. When attackers take action and move from one component to another, they can leverage the system's inter-dependency and connectivity. In other words, they can take control of an additional component of the EV ecosystem that augments their reward and brings them closer to their target.

5.3.3 Transition Probability Function

$P_a(s, s')$ is defined as the transition probability function for a successful transfer from the current state (s) to a new state (s') by taking action $a \in \mathcal{A}$. The CVSS V3.1 can be deployed to allocate probabilities to the transition between the current and new state [77, 79]. This scoring system includes three index groups, i.e., base, temporal, and environmental indexes, that can be determined to calculate a risk score for a specific vulnerability from 0 to 10. Since the environmental index can cover items in base and temporal indexes, it represents the overall CVSS score with several

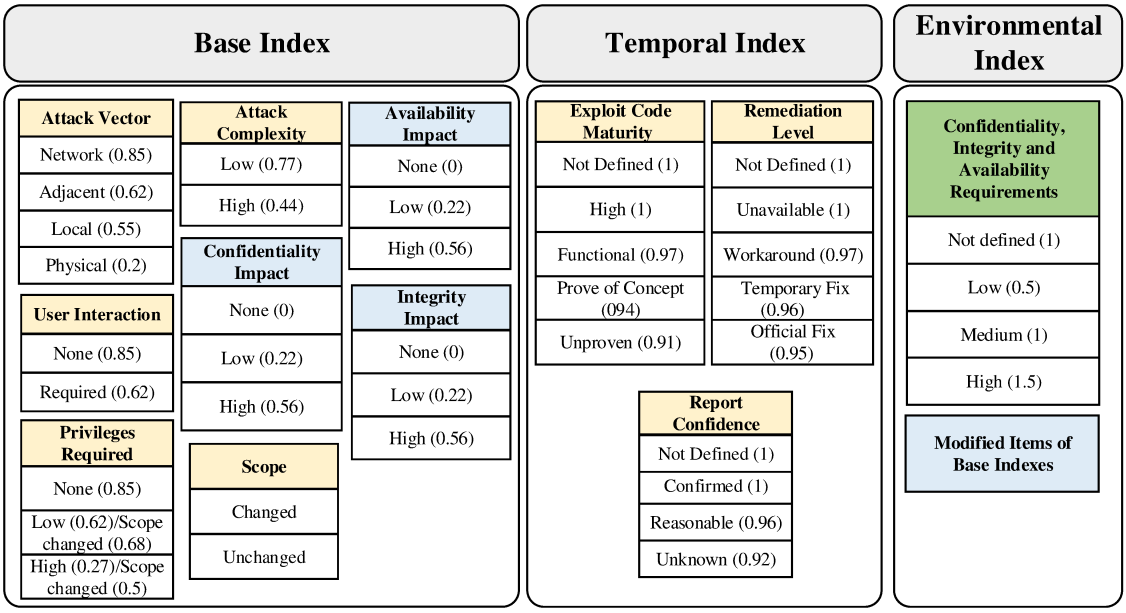


Figure 5.1: Overall common vulnerability scoring system (CVSS V3.1).

modifications that have been shown in Fig. 5.1. The permissible range of CVSS scores is between 0 and 10 where higher values show the severity of cyber events. This score can be divided into five levels: none (N, 0), low (L, 0.1–3.9), medium (M, 4.0–6.9), high (H, 7.0–8.9), and critical (C, 9.0–10.0) [80]. The base index represents the intrinsic characteristics of the vulnerability, which remain unchanged for different time intervals and users. This index can be obtained based on the combination of exploitability and impact items: (i) **Attack vector:** This vector demonstrates the potential for exploiting a vulnerability. (ii) **Attack complexity:** The requirements that must be met to take advantage of the vulnerability. (iii) **Privileges required:** The level of privileges an attacker shall possess when exploiting the vulnerability. (iv) **User interaction:** The requirement for users to participate in the compromise of a vulnerable component. (v) **Scope:** Whether a vulnerability impacts components beyond its security scope. (vi) **Impact metrics:** The impacts of an exploited vulnerability on the component are studied in terms of confidentiality, integrity, and availability. The temporal index represents the characteristics of a vulnerability that may change over time. This metric includes three different items. The first item, i.e., **exploit code maturity**, captures the likelihood of the vulnerability being attacked. The second item, i.e., **remediation level**, is an essential factor for vulnerability prioritization, and the last item, i.e., **report confidence**, captures confidence in the existence of a vulnerability and the known technical details. The environmental index provides background information for the vulnerability and reflects the specific features of the user's environment. This index can modify all the items mentioned in the base index, and it also includes

confidentiality, integrity, and availability requirements. The environmental index in CVSS V3.1 represents the severity of a vulnerability within a specific environment and takes into account additional factors, i.e., the impact on confidentiality, integrity, and availability in the understudy environment. It is important to mention that a numerical value has been allocated to each item, as illustrated in Fig. 5.1, that will be used in the following formulations. The environmental index is calculated based on the base index and additional items related to the environment. On this basis, first, the base index, which depends on sub-formulas for impact sub-score (ISS), impact, and exploitability, is defined as follows [81]:

$$\begin{aligned} ISS = 1 - [(1 - Confidentiality) \times (1 - Integrity) \\ \times (1 - Availability)] \end{aligned} \tag{70}$$

Then, the impact and exploitability coefficients can be calculated as follows:

$$\begin{cases} Scope \rightarrow Unchanged: \\ 6.42 \times ISS \\ Scope \rightarrow Changed: \\ 7.52 \times (ISS - 0.029) - 3.25 \times (ISS - 0.02)^{15} \end{cases} \tag{71}$$

$$\begin{aligned} Exploitability = \ & 8.22 \times AttackVector \times AttackComplexity \times \\ & PrivilegesRequired \times UserInteraction \end{aligned} \tag{72}$$

Finally, the base index can be calculated based on the following equation:

$$\begin{cases} Impact \leq 0 : 0 \\ \quad Scope \rightarrow Unchanged: \\ \quad R\_up\left(Min\left[\left(Impact + Exploitability\right), 10\right]\right) \\ \quad Scope \rightarrow Changed: \\ \quad R\_up\left(Min\left[1.08 \times \ \left(Impact + Exploitability\right), 10\right]\right) \end{cases} \tag{73}$$

where Min returns the smaller of its two arguments. Also, R_up returns the smallest number, specified to 1 decimal place, that is equal to or higher than its input. The environmental index depends on a modified impact sub-score (MISS), modified impact (Impact_M), and modified exploitability

(Exploitability$_M$) as follows:

$$\begin{aligned} MISS = Min(1 - [(1 - Confidentiality_{Req} \times \\ Confidentiality_M) \times (1 - Integrity_{Req} \times \\ Integrity_M) \times (1 - Availability_{Req} \times \\ Availability_M)], 0.915) \end{aligned} \tag{74}$$

where subscript Req means requirement. In this section, Impact$_M$ and Exploitability$_M$ can be calculated as follows:

$$\begin{cases} Scope_M \rightarrow Unchanged: \\ 6.42 \times MISS \\ Scope_M \rightarrow Changed: \\ 7.52 \times (MISS - 0.029) - 3.25 \times (MISS \times 0.9731 - 0.02)^{13} \end{cases} \tag{75}$$

$$\begin{aligned} Exploitability_M = 8.22 \times AttackVector_M \\ \times AttackComplexity_M \times PrivilegesRequired_M \\ \times UserInteraction_M \end{aligned} \tag{76}$$

Finally, we can calculate the environmental index as follows:

$$\begin{cases} Scope_M \rightarrow Unchanged: \\ \quad R\_up\left(R\_up\left[Min[\,Impact_M + Exploitability_M\right], 10)\right] \times \\ \quad ExploitCodeMaturity \times RemediationLevel \\ \quad \times ReportConfidence) \\ Scope_M \rightarrow Changed: \\ \quad R\_up\left(R\_up\left[Min(1.08 \times [\,Impact_M + Exploitability_M\right], \right. \\ \quad \left. 10)\right] \times ExploitCodeMaturity \times RemediationLevel \times \\ \quad ReportConfidence) \end{cases} \tag{77}$$

It is worth noting that operators select the mentioned items in base, temporal, and environmental indexes according to their needs and available resources within their infrastructure. Given that our infrastructure is an EV ecosystem, we used the National Vulnerability Database (NVD) [82] to identify similar existing attacks within this system. Consequently, these items are chosen based on the data from similar existing attacks. For more information about how these factors are calculated

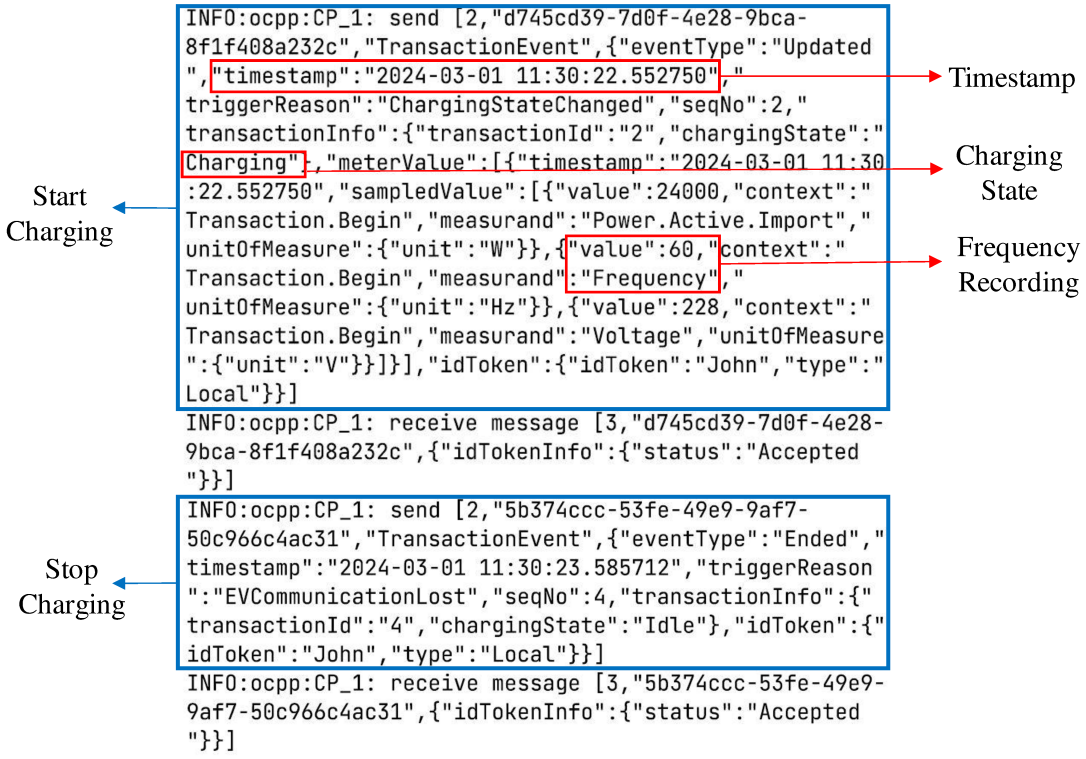


Figure 5.2: Snippet of OCPP logs in a changing station

and descriptions of items mentioned in Fig. 5.1, reference [81] is suggested. After calculating this environmental index, it can be divided by 10 to acquire the transition probability function, i.e., $P_a(s, s')$, for different branches of the customized MDP tree, similar to several works [83, 84].

5.3.4 Reward Function and Discount Factor

A reward that is given to attackers after taking adversarial action $a \in \mathcal{A}$ and moving from the current state (s) to a new state (s') in the MDP tree is defined as a reward function, i.e., $RF_a(s, s')$. In other words, this reward can be given to adversaries for reducing the distribution network's performance. Compromising the cyber layers of EV ecosystems can have different outcomes in distribution networks. For instance, targeting EVCSs and manipulating EV loads can result in excessive voltage deviation at different buses, increase active power losses on lines, and make in-service charging stations unavailable to EV users. As such, this reward function can consist of terms to cover the mentioned outcomes as follows:

Table: OCPP_Logs

	Command	Timestamp
	Filter	Filter
1	Start Charging	2024-03-01 11:30:22.553
2	Stop Charging	2024-03-01 11:30:23.586
3	Start Charging	2024-03-03 17:29:55.000
4	Stop Charging	2024-03-03 17:29:55.746
5	Start Charging	2024-03-03 17:29:56.492
6	Stop Charging	2024-03-03 17:29:57.238
7	Start Charging	2024-03-03 17:29:57.984
8	Stop Charging	2024-03-03 17:29:58.730
9	Start Charging	2024-03-03 17:29:59.476
10	Stop Charging	2024-03-03 17:30:00.222

Figure 5.3: A sample of SQLite3 database to store OCPP charging commands

Term for Manipulated Charging Stations:

Since adversaries are interested in compromising charging stations in distribution networks, the number of manipulated EVCSs can be defined as a term in the reward function to consider the concerns of the DSO about secure and on-time services for EV users. Based on the discussed potential vulnerabilities in the EV ecosystem, charging stations can be manipulated to reduce the performance of power grids. To achieve this aim, attackers should gain control of charging stations through multiple vulnerabilities and change the charging commands that can be visible in the client-side OCPP logs of EVCSs, as shown in Fig. 5.2. In these OCPP logs, a set of different logging information, such as the time and number of start charging and stop charging commands, frequency, and active power meter values, can be extracted during a charging session on EVCSs. These data can be stored in an SQL database, i.e., SQLite3, which has been illustrated in Fig. 5.3. To enumerate the number of compromised EVCSs during this manipulation, we have developed a framework that is the combination of a SQL database and a machine-learning (ML) local detector at each EVCS, as illustrated in Fig. 5.4. To make predictions based on the different OCPP logs, a Long Short-Term Memory (LSTM) is trained based on historical EV charging session data, i.e., stop and start charging sessions that have been converted to numerical values. This local detector at each charging

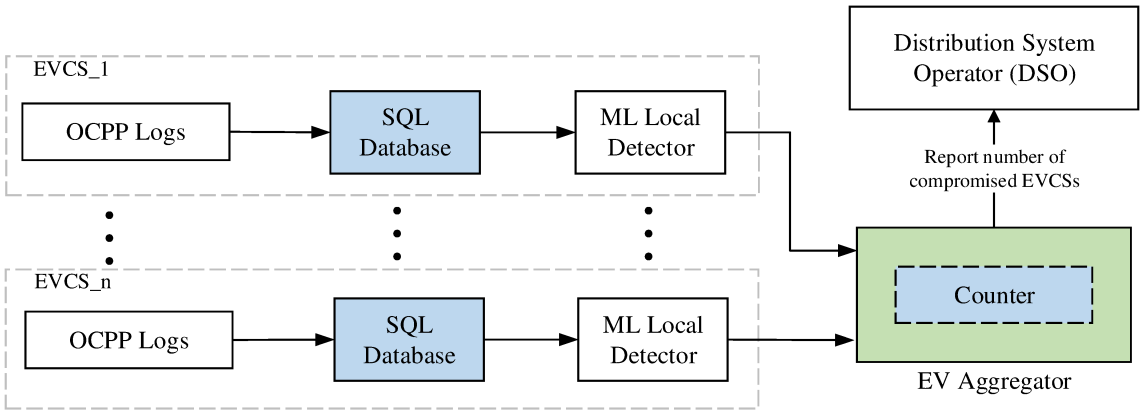


Figure 5.4: Framework for calculating the number of EVCS manipulated in the control center of distribution networks.

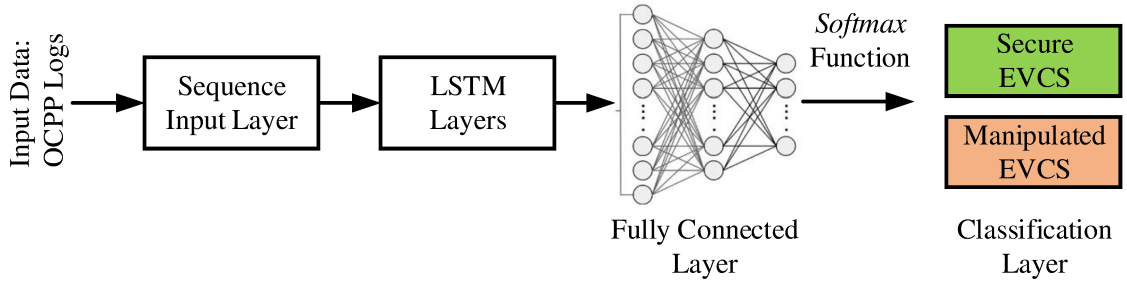


Figure 5.5: Architecture of an LSTM neural network for classification

station analyzes the SQL database and detects abnormal patterns of charging-discharging actions. In our study, a predefined array that consists of a sequence input layer, two LSTM layers with dropout layers (10%), a fully connected layer, a *softmax* function, and a classification output layer can be employed to build an LSTM network for sequence-to-label classification. The number of hidden units for the first and second LSTM layers is 150 and 100, respectively. The number of classifications is also chosen as two, i.e., secure and manipulated charging stations. The overall layout of the proposed LSTM network for sequence-to-label classification has been illustrated in Fig. 5.5. Finally, on the EV aggregator side, one counter is deployed to report the number of compromised EVCSs for the DSO.

Terms for Distribution Network Operation:

To investigate the terms impacting the operation of distribution networks, power flow analysis is required to determine the behavior of different buses, i.e., voltages and their corresponding phase

angles. Then, the power flow is calculated under normal operating conditions or different contingency attack scenarios for the customized MDP tree in the DSO control center. Different loads in the system are assumed to absorb current I_k when their terminal voltage is equal to V_k, representing as follows:

$$I_k = I_k^R + jI_k^I = (\frac{P_k + P_{EV_k} + jQ_k + jQ_{EV_k}}{V_k})^* \tag{78}$$

where I_k^R and I_k^I are real and imaginary parts of the load currents, respectively. $P_k + jQ_k$ is the power consumption of residential/industrial loads in complex format, while $P_{EV_k} + jQ_{EV_k}$ are the power consumption of EV loads connected to charging stations that can be readily compromised by different potential vulnerabilities in EV ecosystems. Kirchhoff Current and Voltage laws (KVL/KCL) can be applied to the distribution network to establish the relationship between load current and branch current (I_B) as[85]:

$$\begin{bmatrix} I_{B_1} & I_{B_2} & ... & I_{B_{N_b}} \end{bmatrix}^T = [\mathbf{BIBC}] \begin{bmatrix} I_1 & I_2 & ... & I_{N_L} \end{bmatrix}^T \tag{79}$$

where N_L and N_b are referred to as the number of loads and branches in the distribution network, respectively. $\mathbf{BIBC}$ is the bus-injection to the branch-current matrix that represents the connections and topology of the distribution networks. Moreover, the connection between the bus voltages and the branch currents can be obtained as follows:

$$\begin{bmatrix} V_1 & V_1 & ... & V_1 \end{bmatrix}^T - \begin{bmatrix} V_2 & V_3 & ... & V_{N_L} \end{bmatrix}^T = [\mathbf{BCBV}] \begin{bmatrix} I_{B_1} & I_{B_2} & ... & I_{B_{N_b}} \end{bmatrix}^T \tag{80}$$

where $\mathbf{BCBV}$ matrix is branch-current to bus-voltage that is also dependent on the topology of the distribution network. Using equations (109) and (80) and load characteristics, the relationship between bus current injections and bus voltages can be expressed as:

$$V = V_1 + [\mathbf{BCBV}][\mathbf{BIBC}]I = V_1 + [\mathbf{DLF}]I \tag{81}$$

where $\mathbf{DLF}$ is a multiplication matrix of $\mathbf{BCBV}$ and $\mathbf{BIBC}$ that can be solved iteratively to obtain states of systems, i.e., voltages and their corresponding phase angles[85]. From this perspective, the summation of the bus voltage deviated from the reference voltage, i.e., ΔV_d^{Ave}, can be calculated

for all buses ($l \in \{1, ..., N_{bus}\}$) after compromising charging stations as follows:

$$\begin{cases} \Delta V_d^{Ave} = \sum_{l=1}^{N_{bus}} \Delta V_d \\ \Delta V_d = \left| \frac{V_a^l(s,s') - V_{nom}^l}{V_{nom}^l} \right| \end{cases} \tag{82}$$

where V_{nom}^l is the nominal voltage defined in buses of distribution networks, and $V_a^l(s, s')$ is the bus voltage after manipulating EVCSs in the EV ecosystem and moving from state s to state s' by taking action a. Active power losses of each branch ($p \in \{1, ..., N_b\}$) can be calculated as:

$$\Delta P_p^{Loss} = I_p^2 R_p \tag{83}$$

By summing up all of the active power losses of each branch, the total active power losses for the distribution network can be calculated:

$$\Delta P_T^{Loss} = \sum_{p=1}^{p=N_b} \Delta P_p^{Loss} \tag{84}$$

In summary, to consider the concerns of the DSO, a reward function for each of the two consecutive states in the MDP tree can be defined as follows:

$$\begin{aligned} &RF_a(s, s') = \alpha_1 \left(\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}}\right) + \alpha_2 \Delta V_d^{Ave} + ... \\ &\alpha_3 \left(\frac{\Delta P_a^{Loss}(s,s') - \Delta P_T^{Loss}}{\Delta P_T^{Loss}}\right) \end{aligned} \tag{85}$$

where N_T^{EVCS} and $N_a^{Comp}(s, s')$ are the total number of charging stations installed in distribution networks and the number of targeted EVCSs after moving from state s to s' by taking adversarial action a, respectively. $\Delta P_a^{Loss}(s, s')$ is also defined as the total active power loss of the distribution network after compromising EVCSs connected to EV loads by taking action a. Also, α_1, α_2, and α_3 are coefficients that can be used to weigh the terms of the proposed reward function. It is worth mentioning that the DSO can set the value of each coefficient to zero or one based on his opinion and the priority of the DSO control center. In our work, EV users' satisfaction and quality of services are important. As such, the α_1 can be set to the same value as the α_2 and α_3 when generating and solving the MDP tree. Finally, the distinction in importance between present and future rewards can be considered by defining a discount factor (γ). This discount factor can be tuned between 0 and

1 ($0 \leq \gamma \leq 1$) to control the balance between immediate and future rewards during the decision-making process in the MDP tree. A higher discount factor prioritizes long-term rewards, while a lower discount factor prioritizes immediate rewards. This factor also ensures the convergence of the algorithm for solving the MDP tree. Generally, a discount factor of less than 1 ensures that the expected cumulative rewards remain bounded.

5.3.5 Generating MDP Tree for Different Contingencies

To generate the proposed MDP tree, an initial state, i.e., $s_1 = \phi$, is defined as a starting point where no component of the EV ecosystem is targeted. In the first stage, the power distribution network can be divided into several zones to investigate the impact of cyber attacks on charging stations in single and multiple zones of the power grid. Dividing a distribution network into different zones is a common approach in power system planning and operation to deliver better management, control, and maintenance of these systems[86]. In our work, buses located in a geographical region and lateral branches have the same behavior in voltage deviation, and they can be treated as separate zones for planning and operation purposes [87]. It is important to mention that the number of zones, i.e., Z_T, can be changeable based on the DSO's opinion. However, the number of zones can increase the burden of calculations and complexities. When attackers decide to compromise EVCSs in different zones of the distribution network, they may select charging stations in a single zone or multiple zones, leading to single or multiple contingencies, respectively. On this basis, we will have a combination of different zones in the developed MDP tree, that is, a selection of single or multiple zones from total separate zones, as follows:

$$\begin{bmatrix} Z_T \\ 0 \end{bmatrix} + \begin{bmatrix} Z_T \\ 1 \end{bmatrix} + \begin{bmatrix} Z_T \\ 2 \end{bmatrix} ... + \begin{bmatrix} Z_T \\ Z_T \end{bmatrix} = 2^{Z_T} \tag{86}$$

It can be proven that the sum of this combination is equal to 2^{Z_T}[88]. Furthermore, a single contingency in the MDP tree is the combination of one event from total zones as follows:

$$\begin{bmatrix} Z_T \\ 1 \end{bmatrix} = Z_T \tag{87}$$

Algorithm 6: MDP Tree Generator for Different Contingencies

Determine: Number of zones in distribution network (Z_T)
Calculate: Combination of different contingencies $2^{Z_T} - 1$
Initialize: Number of attackers' access points in ecosystem(n_v)
Create: Initial state (ϕ) in MDP tree

```
for i = 1 : 1 : n_v do
    for z = 1 : 1 : 2^{Z_T} − 1 do
        if (i is an attacker's access point) then
            Build a new reachable state s_i
            for j as a compromised component do
                if (i is not connected to j) then
                    Continue  Serach for new connection
                end
                if (i and j connected) then
                    Build new state s_j  Define a transition between s_i and s_j
                    Determine P_a(s_i, s_j) using CVSS
                    Calculate RF_a(s_i, s_j) using (85)  Continue for new connection with s_r
                    Build new state and transition among them
                end
            end
        end
    end
end
```

To calculate multiple contingencies in the MDP tree, this mathematical equation can be represented as follows:

$$\begin{bmatrix} Z_T \\ 2 \end{bmatrix} + ... + \begin{bmatrix} Z_T \\ Z_T \end{bmatrix} = 2^{Z_T} - \begin{bmatrix} Z_T \\ 1 \end{bmatrix} - \begin{bmatrix} Z_T \\ 0 \end{bmatrix} = 2^{Z_T} - Z_T - 1 \tag{88}$$

In the following, Algorithm 6 can be organized to create all states and define transitions among them. Based on this algorithm, the attacker's access points (s_i), extracted from attack graphs, can be considered an accessible state in the MDP tree. Then, a new reachable state (s_j) can be added to the tree starting from the attacker's access point whenever compromised component j is associated with component i. Making a new state can be continued until the final state is obtained where charging stations in a specific zone have been compromised. For example, to build a branch of the customized MDP tree, we can randomly select an attacker's access point like CSMS in the EV ecosystem and move from the initial state (ϕ) to the new state (CSMS). On this basis, the CSMS can be considered an accessible state from the attackers' viewpoint. Then, adversaries can move from

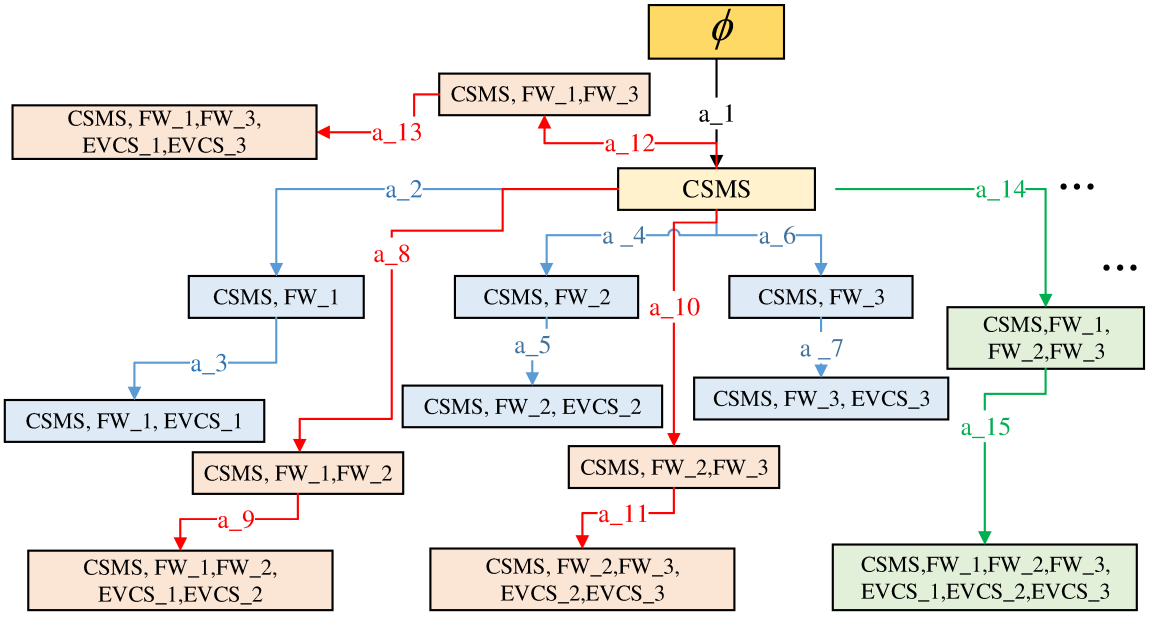


Figure 5.6: A branch of MDP tree including states and transition among them based on potential vulnerabilities in EV ecosystem for multiple contingencies

the CSMS to the firmware repository of EVCSs as a reachable state by targeting the EVSE business network and injecting malicious malware into EVCSs in the first zone. Based on this description, the next state will be the firmware repository (CSMS, FW_1). Finally, adversaries can take control of EVCSs in the proposed zone of the distribution network and trigger EV loads connected to EVCSs to impact the operation of the distribution network. Thus, the final state can be obtained as the name of (CSMS, FW_1, $EVCS_1$) in the MDP tree. For the second zone of the distribution network, we can define a new state as (CSMS, FW_2, $EVCS_2$). This algorithm can also enumerate multiple contingencies and produce related states, e.g., (CSMS, $FW_{1,2}$, $EVCS_{1,2}$), in the customized MDP tree due to definition of for loop in this algorithm. A branch of the MDP tree by applying Algorithm 6 to the cyber layers of the EV ecosystem for a distribution network with three zones, $Z_T = 3$, has been illustrated in Fig. 5.6. Other branches of the MDP tree can be completed by considering other vulnerabilities in the EV ecosystem as shown by the flowchart in Fig. 5.7.

5.4 Optimal Response Selection for MDP Tree

To solve the MDP tree and calculate the values of each state and adversarial actions, the modified policy iteration algorithm is suggested [89]. Using this iteration algorithm, which includes policy

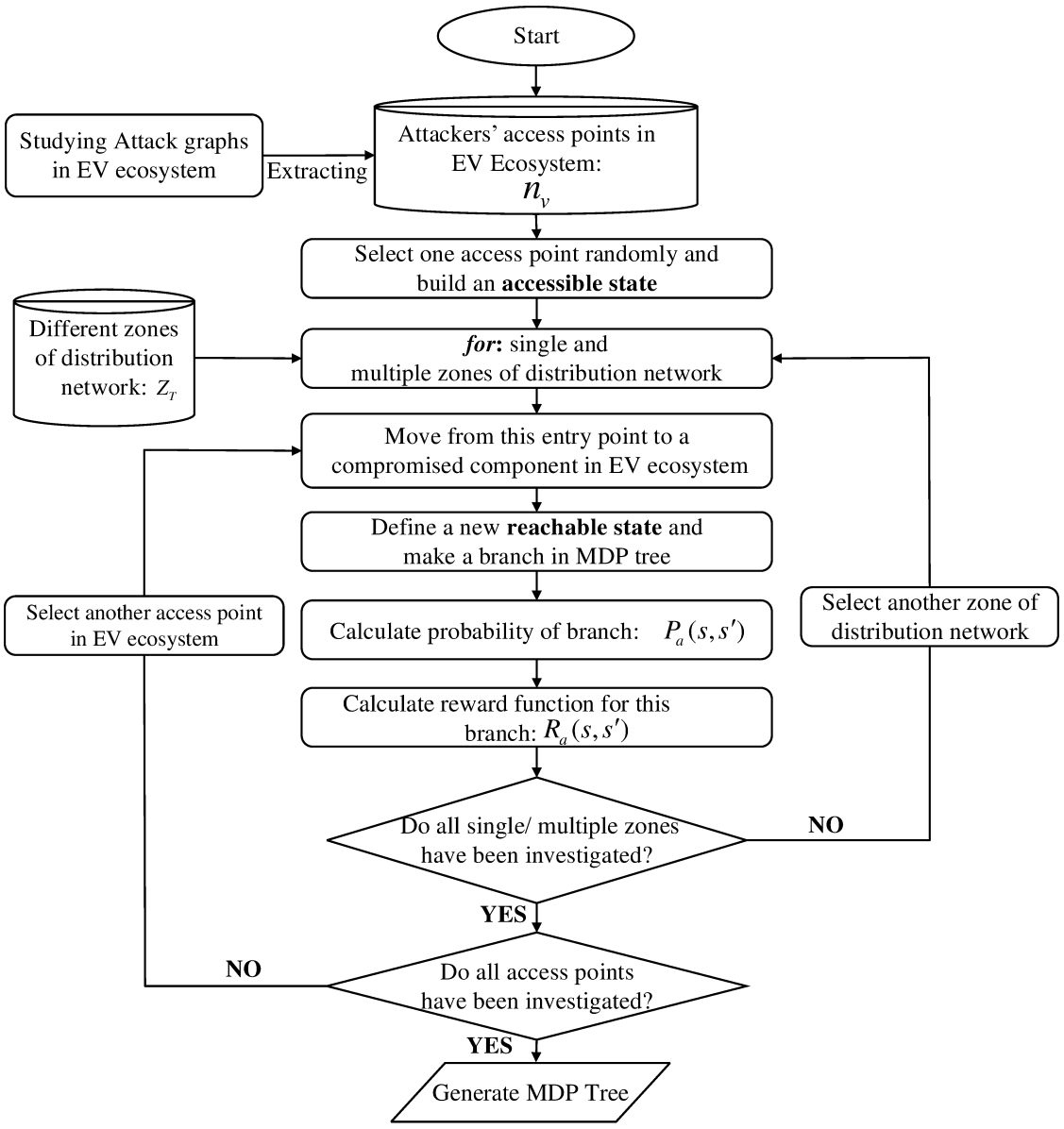


Figure 5.7: Steps to generate MDP tree based on vulnerabilities in EV ecosystem and multiple zones in distribution network

evaluation and policy improvement stages, the expected cumulative reward after a sequence of states ($s \in \mathcal{S}$) and actions ($a \in \mathcal{A}$) is maximized. These stages lead to faster convergence especially when generating an MDP tree for large-scale distribution networks. Firstly, value functions and adversarial actions are initialized randomly. In the policy evaluation stage, for each state in the MDP tree, the value function can be calculated using modified *Bellman equations* by taking the

Algorithm 7: Modified Policy Iteration Algorithm (2 Stages)

Initialize: $V(s)$ and $\pi(s)$ arbitrarily for $s \in \mathcal{S}$

Initialize: θ as positive small number **Results:** Optimal policy π^* and optimal value function V^* for $\mathcal{S}$

1. Policy Evaluation $\Delta_{int} \leftarrow 0$ **while** $\Delta < \theta$ **do**
  for *each* $s \in \mathcal{S}$ **do**
    $V_{new}(s) \leftarrow \sum_{s'} P_{\pi(s)}(s, s')[RF_{\pi(s)}(s, s') + \gamma V(s')]$
    $\Delta_{new} \leftarrow Max(\Delta_{int}, |V_{old}(s) - V_{new}(s)|)$
  end
end
2. Policy Improvement
Policy Stable $\leftarrow$ True
for *each* $s \in \mathcal{S}$ **do**
  π_{old}
  $\pi_{new}(s) \leftarrow \arg\max_a \sum_{s'} P_a(s, s')[R_a(s, s') + \gamma V(s')]$
  if $\pi_{old} \neq \pi_{new}$ **then**
    Policy Stable $\leftarrow$ false
  end
end
if *Policy Stable* **then**
  Return optimal policy π^* and optimal value function V^*
else
  Go to Policy Evaluation
end

policy, $\pi(s)$, as follows:

$$V(s) = \sum_{s'} P_{\pi(s)}(s, s')[RF_{\pi(s)}(s, s') + \gamma V(s')] \tag{89}$$

where $P_{\pi(s)}(s, s')$ and $RF_{\pi(s)}(s, s')$ are the transition probability from state s to s' and reward received after action $\pi(s)$, respectively. The proposed algorithm can check for convergence by measuring the difference between the new computed value function, i.e., $V_{new}(s)$, and the previous value function, i.e., $V_{old}(s)$. Then the algorithm can calculate this change and compare it with the previous one as follows:

$$Max(\Delta_{int}, |V_{old}(s) - V_{new}(s)|) \rightarrow \Delta_{new} \tag{90}$$

where Δ_{int} is initialized to zero at the first iteration. If the change in the calculated value function is lower than a predefined threshold θ, i.e., ($\Delta_{new} < \theta$), the algorithm stops indicating that the algorithm has converged. Otherwise, it continues iterating. The algorithm performs the policy

improvement stage when the value function is updated. It updates the $\pi(s)$ policy to select the action in each state that maximizes the expected cumulative reward according to the updated value function, i.e., $V_{new}(s)$. This step is crucial for iteratively refining the policy to make better decisions:

$$\pi(s) = \arg\max_a \sum_{s'} P_a(s, s')[R_a(s, s') + \gamma V(s')] \tag{91}$$

where $\arg\max_a$ stands for the adversarial action a that results in the maximum expected cumulative reward when taken from the state s according to the updated value function. This iteration continues until $\pi_{old} = \pi_{new}$, leading the algorithm to stop. In other words, this algorithm creates a series of policies, where each policy is improved compared to the old ones. To show how this approach can evaluate and improve the policy, Algorithm 7 is represented. The final results of this algorithm are the optimal value function (V^*) and the optimal policy (π^*) for each state in the customized MDP tree.

5.5 Monitoring Framework Implementation

5.5.1 Deep CNN Model for Security Monitoring

To design a monitoring framework that can notify DSOs of the system's security status, a deep CNN is trained based on a wide range of results obtained from the customized MDP trees. To generate a training data set, the MDP tree is established by Algorithm 6 and resolved by Algorithm 7 for different EV load penetrations in an offline manner. The raw data (i.e. input data) for training this deep CNN model is the calculated value of states in the MDP tree, i.e. N_{st}, when single and multiple contingencies are investigated and the compromised EV load penetration changes from 0% until 25% with the N_{EV} step. On this basis, raw data can be arranged in the form of matrices with dimensions of $N_{comb} \times N_{st}$, where N_{comb} indicates the total combination of different EV load penetration levels for each single or multiple zones of the distribution network. When attackers select a single zone of the distribution network, they may compromise different levels of EV loads in single zones as follows:

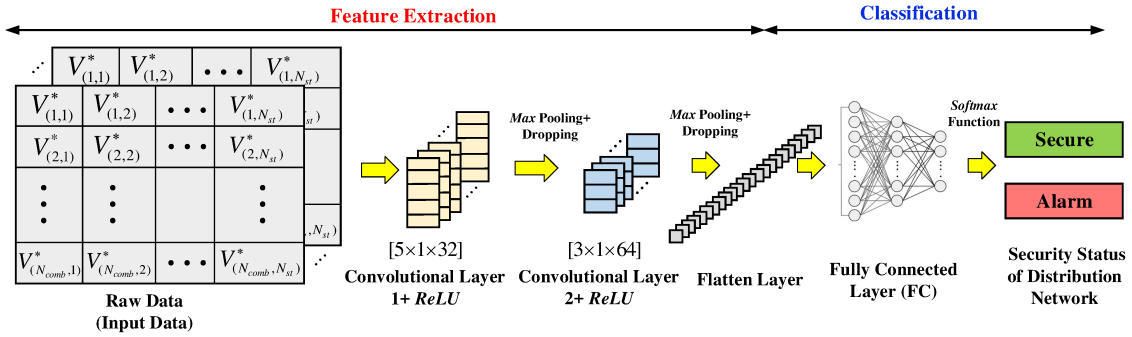


Figure 5.8: Deep CNN structure for different EV loads compromised by adversaries to impact the operation of the distribution network.

Table 5.1: Classification of Distribution Network Security During EV-based Attacks

Situation	Percentage of manipulated EVCSs to total EVCSs	Voltage deviation at each bus		Total active power loss
Secure	$\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}} < \Psi_{th}$	$\frac{V_a^l(s,s')-V_{nom}^l}{V_{nom}^l}$	$< V_{th}$	$\frac{\Delta P_a^{Loss}}{\Delta P_T^{Loss}} < \Delta P_{th}^{Loss}$
Alarm	$\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}} \geq \Psi_{th}$	$\frac{V_a^l(s,s')-V_{nom}^l}{V_{nom}^l}$	$\geq V_{th}$	$\frac{\Delta P_a^{Loss}}{\Delta P_T^{Loss}} \geq \Delta P_{th}^{Loss}$

$$\begin{bmatrix} Z_T \\ 1 \end{bmatrix} \times (N_{EV})^1 \tag{92}$$

For different multiple zones (i.e., double, triple,..., $M^{'}$), we can have this general formulation as follows:

$$\begin{bmatrix} Z_T \\ M' \end{bmatrix} \times (N_{EV})^{M'} \tag{93}$$

where $M^{'}$ indicates the number of zones in multiple contingencies of distribution networks. The target data is also defined as secure and alarm situations. Considering the following three conditions, we can define and assign secure and alarm conditions to distribution networks after compromising charging stations across different zones:

1. The number of manipulated charging stations is reported to DSOs based on OCPP logs on the client side in EVCSs using our developed framework in Fig. 5.4. Then, the ratio of manipulated charging stations to installed charging stations can be calculated. For an alarm situation, this ratio must exceed a predefined value as follows:

$$\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}} \geq \Psi_{th} \tag{94}$$

where Ψ_{th} is a threshold for this ratio, initializing to 5% in this work without loss of generality. This threshold has been selected based on several works that studied the impact of compromising aggregated EV loads on the operation of power grids [90, 91]. However, it can be changed based on the opinion of DSOs or EV vendors.

2. A nominal voltage, i.e., V^l_{nom}, has been defined for each bus. We can calculate the deviation from this nominal voltage when adversaries manipulate EV loads in different buses, i.e., $V^l_a(s, s')$, and divide it by the nominal voltage. This ratio for at least one bus is supposed to exceed the predefined threshold, i.e., V_{th}. In this case, it can be defined as a condition for an alarm situation in the distribution network, as follows:

$$\left| \frac{V^l_a(s, s') - V^l_{nom}}{V^l_{nom}} \right| \geq V_{th} \tag{95}$$

Otherwise, we can define a secure situation for distribution networks. In this study, the V_{th} can be adjusted within a 5% range, thus setting the threshold at $V_{th} = \pm 2.5\%$. For sensitive electronic equipment, including EV charging stations, the voltage fluctuation limit is often set within $\pm 2.5\%$ to 5% of the nominal voltage based on IEC 61000-3-3 standard[92]. It is worth noting that this allowable range can be set lower than this value, depending on the sensitivity of distribution operators and the presence of sensitive industrial loads in power grids [93].

3. The total active power loss on all branches compared to the total loss can be measured using several micro phasor measurement units (PMUs) installed in different branches of distribution networks [94]. For the alarm situation, this value must exceed a predefined threshold as follows:

$$\frac{\Delta P^{Loss}_a}{\Delta P^{Loss}_T} \geq \Delta P^{Loss}_{th} \tag{96}$$

where this threshold, i.e., ΔP^{Loss}_{th}, for total active power loss, is defined as 8%. According to IEEE standards [95], the total losses in a distribution system are typically expected to be in the range of 5% to 10% of the total input power for well-designed systems. Without loss of generality, considering losses in switches, capacitors, and other EV loads equipment, in our manuscript, we have assumed that 8% can be defined as the value of the threshold for active power loss. However, distribution network operators can select another value while designing the security metric for their network. In summary, two different situations of a distribution network after compromising charging stations in

all buses can be defined in Table. 5.1.

The structure of a customized deep CNN for classification of the security status of distribution networks under EV-based attacks is depicted in Fig. 5.8. This model consists of two convolutional layers (Conv) for feature extraction from the value functions obtained from resolving the MDP trees. First, a two-dimensional (2D) convolutional layer with 32 kernel functions of size 5×1 is applied to the raw data for learning spatial features. Another 2D convolutional layer with 64 kernel functions of size 3×1 is applied to learn more advanced features in the data. Since the relationship between inputs and target data is non-linear, this structure implements the rectified linear unit *ReLU* as an activation function. The 2D Maxpooling layer is also employed to down-sample the feature maps and further reduce the dimension of the under-processed data. A flattened layer is added to the deep CNN model to convert the multi-dimensional output from the previous layers into a 1D vector for the next dense layer. The output of the final layer goes through a fully connected layer (FC) allocated for classification purposes. After the FC layer, the *softmax* function is deployed to provide information about the situation of the distribution networks. Finally, a cross-entropy loss function L_{cls} is defined to update the weights of the neural network for three classes as follows:

$$L_{cls} = -\frac{1}{N_t}\sum_{t=1}^{N_t}\hat{y}_t \log(y_t) \tag{97}$$

where N_t is the total number of training samples and $\hat{y}_t$ and y_t are actual security classification and estimated security classification, respectively.

5.5.2 Application of Security Metric in DSO Control Center

All the mentioned subsections can be integrated to build a framework for monitoring the security status of distribution networks using the developed metric, as shown in Fig. 5.9. This metric can be implemented in the DSO control center of real-world power grids, where all data is collected for power flow analysis, system planning, and issuing control commands for different parts of power grids. The security metric thoroughly scans the integrated cyber-physical components in the EV ecosystem and identifies single and multiple contingencies based on measurement signals obtained from distribution network topologies and the cyber layers of charging stations. On this basis, our

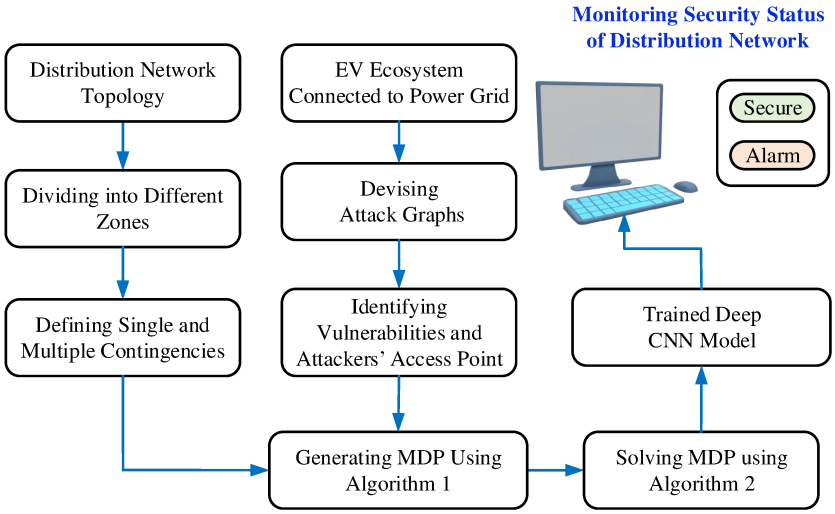


Figure 5.9: A system monitoring using developed security metric

security metric can generate and resolve the MDP tree regardless of the size of the distribution network. Also, this metric can be updated when a new potential vulnerability is identified in one of the components of the EV ecosystem or a change in the distribution system topology has been made. The DSO control center can resolve the MDP tree to acquire the value of each state and optimal adversarial actions during single and multiple contingencies in distribution networks. However, interpreting these values and policies is difficult and time-consuming, especially when the dimensions of the EV ecosystem and distribution networks increase. As a result, we have resolved this limitation during different contingencies and introduced the well-trained deep CNN model. This model can help the DSO control center design a monitoring system during secure or alarm situations. In our security metric, first, the framework (Fig. 5.4) reports the number of manipulated charging stations online, and then, voltage deviation and excessive active power loss will be derived from the analytics unit in the DSO control center to establish the MDP tree and calculate the security metric of the system. It can increase the DSO's awareness about targeted charging stations, encourage remedial actions, and decrease the inconvenience to EV customers.

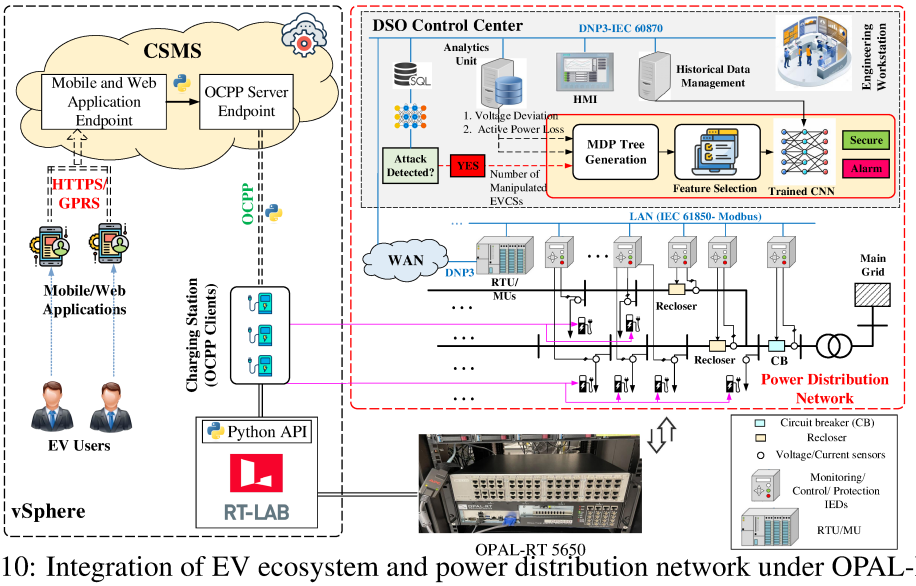


Figure 5.10: Integration of EV ecosystem and power distribution network under OPAL-RT 5650

5.6 Simulation Results and Discussion

5.6.1 Real-time Testbed of EV Ecosystem and Power Grid

In this section, the developed EV-based attack security metric is evaluated for two IEEE 33-bus and 141-bus distribution networks in Caracas. A general schematic of the cyber and physical layers of the EV ecosystem integrated into a power distribution network has been illustrated in Fig. 6.6. This layout consists of the OPAL-RT 5650 as a real-time simulator (RTS) for simulating the power grid and a virtual sphere (vSphere) to show the connection between different layers of the EV ecosystem using Python scripts. A Python application programming interface (API) is also developed to allow the virtual machine of charging stations to control EV loads in the proposed distribution network implemented in OPAL-RT 5650. The CSMS, which is typically hosted on cloud computing platforms, can provide two services for communication between mobile and web applications and EVCSs. The first service is the mobile and web application endpoint for sending and receiving requests from the mobile application. The second service is the OCPP server endpoint, where CSMS translates the actions triggered by the mobile application to the OCPP commands to manage the EVCSs. WebSockets, which enable full-duplex communication over a TCP connection, are generally used by the OCPP. As a practical application, we have provided a Python script for the central server and one script for the OCPP client server. These Python scripts can communicate to

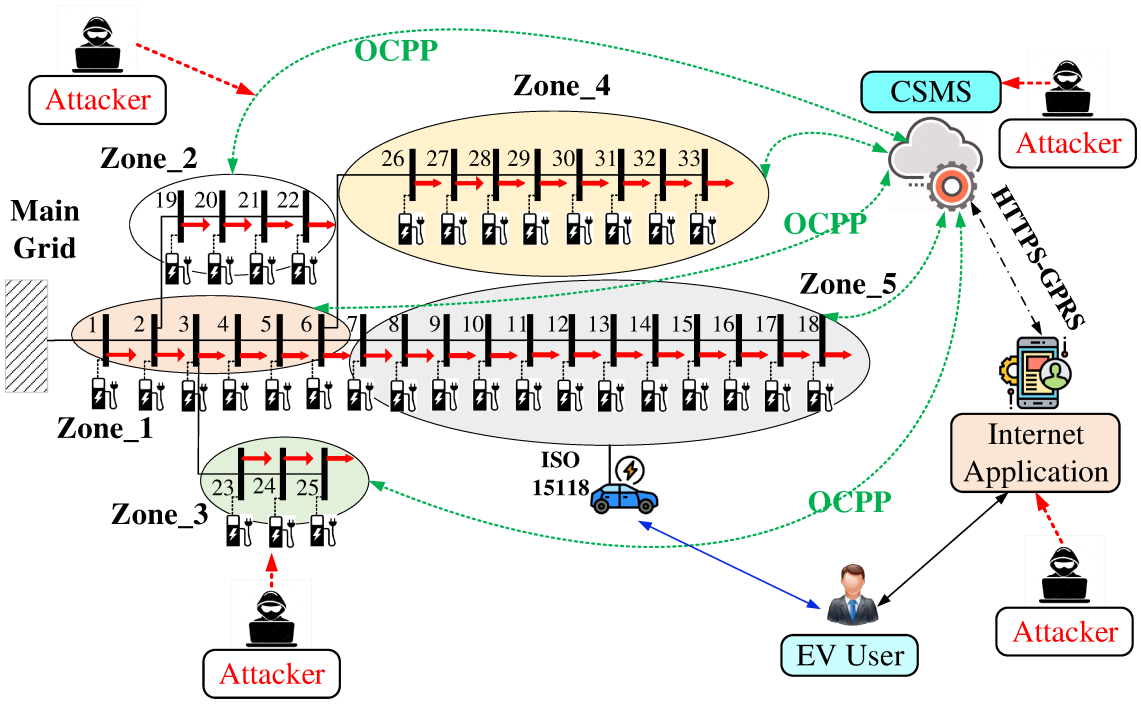


Figure 5.11: EV ecosystem connected to modified IEEE 33-bus distribution network with different five zones

make a real connection between CSM and EVCSs and maintain internal information in a database, e.g., EVCS OCPP logs, to display the status of the EVCS and transactions with the CSMS for our framework (Fig. 5.4). We have also provided a Python API file to control EV loads in the model implemented in our RTS, i.e., OPAL-RT 5650 [96]. The DSO control center in distribution networks with the architecture of the developed security metric has been shown in Fig. 6.6. In this testbed, intelligent electronic devices (IEDs) are used to collect measurement signals, i.e., current, voltage, and frequency from nearby measurement transformers, as well as the status of any associated circuit breaker and recloser. A set of protection IEDs is related to the main feeder and reclosers in the lateral lines of distribution networks. Also, another group of these IEDs monitors and controls the situation of different load buses in the system. The data gathered from all monitoring and protection IEDs is continuously communicated to different remote terminal units (RTUs) and merging units (MUs) over the local area network (LAN) using substation communication standards (e.g., IEC 61850, Modbus). In the following, the RTUs and MUs deploy common communication protocols, i.e., DNP3, IEC61850, and IEC 60870, to transmit the collected data to the DSO control center across a

wide area network (WAN) [97]. Using the analytics unit, first, the number of manipulated EVCSs is reported, and then the reward functions are calculated to generate a related MDP tree and resolve it. Finally, the numerical values of all states are obtained and passed through a trained CNN model to provide information about the security status of the power distribution network.

5.6.2 IEEE 33-bus Distribution Network

Building MDP Tree: To study the impact of manipulating EV loads connected to charging stations on the operation of the distribution network, an EV ecosystem including cyber and physical layers is integrated into the IEEE 33-bus system, as shown in Fig. 6.6. In this cyber-physical model, CSMS, OCPP, mobile/web applications, and USB ports mounted on charging stations can be considered the attacker's access points. The number of vulnerabilities in EV ecosystems and zones in the distribution network can be defined as 4 and 5 ($n_v = 4$, $Z_T = 5$), respectively, as shown in Fig. 5.11. Since we are going to evaluate the proposed security metric for the IEEE 33-bus system in the presence of different events, the number of single and multiple contingencies can be calculated as 5 and 26, i.e., $(2^{Z_T} - 1) - Z_T = 26$, respectively. The number 5 shows five single zones, including Zone_1, Zone_2, Zone_3, Zone_4, and Zone_5. The number 26 indicates different combinations of zones in the distribution network where their charging stations can be manipulated by adversaries in multiple zones, leading to multiple contingencies in the MDP tree: $\{\text{Zone}_{1,2}$, $\text{Zone}_{1,3}$, $\text{Zone}_{1,4}$, $\text{Zone}_{1,5}$, $\text{Zone}_{2,3}$, $\text{Zone}_{2,4}$, $\text{Zone}_{2,5}$, $\text{Zone}_{3,4}$, $\text{Zone}_{3,5}$, $\text{Zone}_{4,5}$, $\text{Zone}_{1,2,3}$, $\text{Zone}_{1,2,4}$, $\text{Zone}_{1,2,5}$,..., $\text{Zone}_{1,2,3,4,5}\}$. Based on Algorithm 6 and considering four well-known vulnerabilities in the EV ecosystem, an MDP tree with 36 states and 56 actions can be obtained for targeting single zones of the IEEE 33-bus distribution network, as illustrated in Fig. 5.12.

Calculating Probabilities: To assign the probabilities of adversaries' success rates for a wide range of adversarial actions and add these numbers to the branches of the MDP tree, the CVSS V3.1 is deployed. To show how we can calculate this probability for each branch of the MDP tree, a numerical example can be provided as follows: it is assumed that adversaries decide to compromise mobile and web application networks and move from the initial state (ϕ) to state (Mb) in the MDP tree, as shown in Fig. 5.12. As such, items of the base index, i.e., Attack vector,

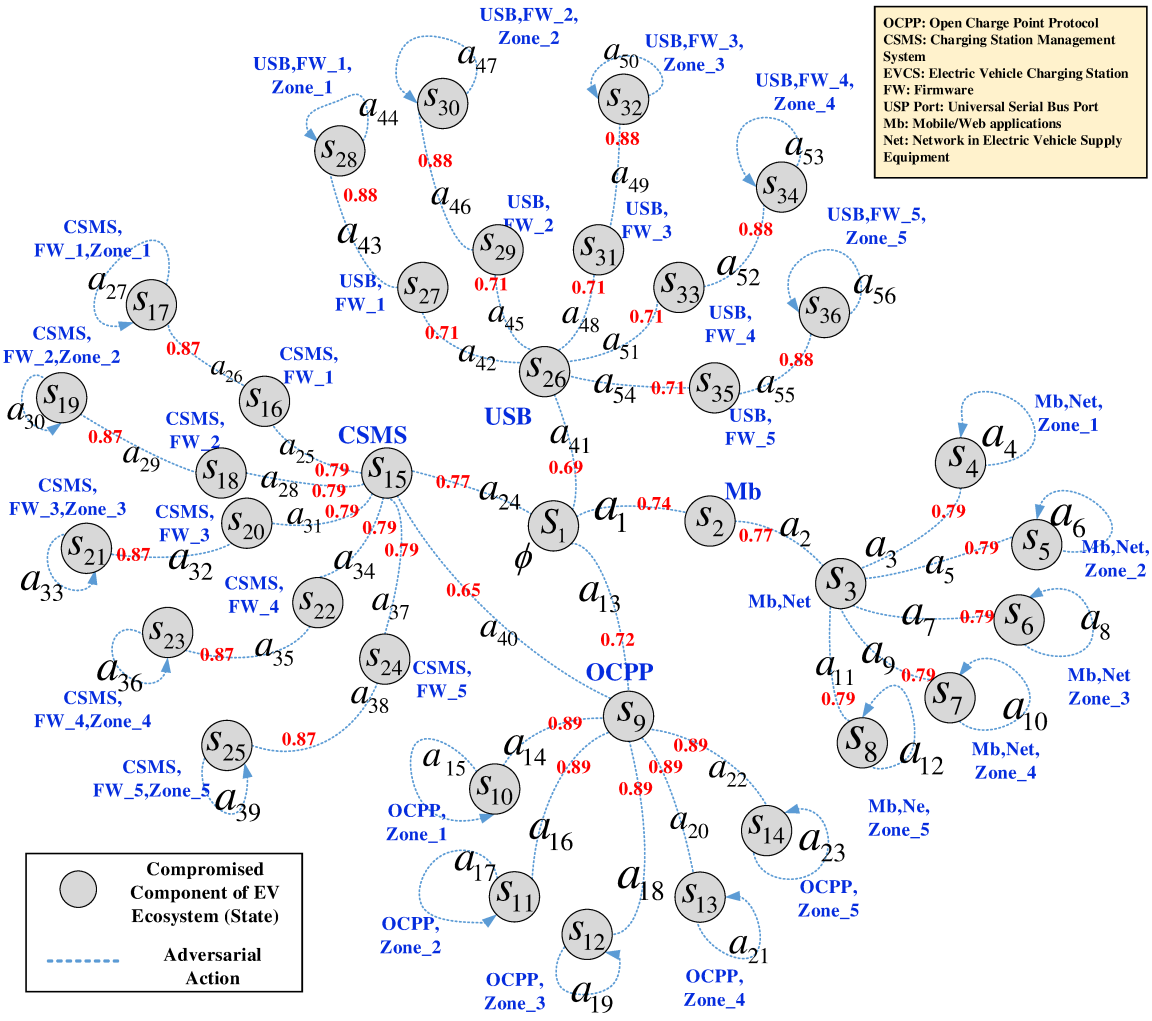


Figure 5.12: MDP tree generated by Algorithm 6 for enumerating states and transition among them for a distribution network with Z_T=5 zones

Attack complexity, Privileges required, User interaction, and Scope are selected as network, high, high, required, and changed, respectively, based on real features of this vulnerability (Mb) in EV ecosystem reported by the National Vulnerability Database (NVD) [82]. Moreover, Confidentiality, Integrity, and Availability are assumed to be high, low, and low, respectively. It is also supposed that the characteristics of the proposed vulnerability may not change over time. As a result, all items of the temporal index are chosen as not defined. Based on (103), the base index can be calculated as 6.8 using impact and exploitability terms. The temporal index is also calculated similarly, i.e., 6.8. Finally, the $MISS$ is calculated as 0.8733 based on this standard, and Impact_M and Exploitability_M are obtained as 5.8826 and 0.9530, respectively. It is important to mention that $\text{Confidentiality}_{Req}$,

Table 5.2: Calculating probabilities of each branch in MDP Tree using CVSS V3.1

Action	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$
a_1	0.74	a_{13}	0.72	a_{25}	0.79	a_{37}	0.79	a_{49}	0.88
a_2	0.77	a_{14}	0.89	a_{26}	0.87	a_{38}	0.87	a_{50}	1
a_3	0.79	a_{15}	1	a_{27}	1	a_{39}	1	a_{51}	0.71
a_4	1	a_{16}	0.89	a_{28}	0.79	a_{40}	0.65	a_{52}	0.88
a_5	0.79	a_{17}	1	a_{29}	0.87	a_{41}	0.69	a_{53}	1
a_6	1	a_{18}	0.89	a_{30}	1	a_{42}	0.71	a_{54}	0.71
a_7	0.79	a_{19}	1	a_{31}	0.79	a_{43}	0.88	a_{55}	0.88
a_8	1	a_{20}	0.89	a_{32}	0.87	a_{44}	1	a_{56}	1
a_9	0.79	a_{21}	1	a_{33}	1	a_{45}	0.71		
a_{10}	1	a_{22}	0.89	a_{34}	0.79	a_{46}	0.88		
a_{11}	0.79	a_{23}	1	a_{35}	0.87	a_{47}	1		
a_{12}	1	a_{24}	0.77	a_{36}	1	a_{48}	0.71		

Integrity$_{Req}$, and Availability$_{Req}$ are selected as High, Low, and Low, respectively [82]. Finally, the environmental index can be calculated at 7.6 using equation (77). This final number is divided by 10 and allocated to the mentioned branch of the MDP tree. To calculate probabilities for other branches with different adversarial actions, we can use the CVSS V3.1 [81], as listed in Table. 5.2.

Calculating Reward Functions: To acquire the reward function for each transition between the current and subsequent state in this tree, the behavior of bus voltage and active power losses is measured in the DSO control center. The number of compromised charging stations is also reported using the framework in Fig. 5.4. Using this framework, if adversaries manipulate charging stations and issue malicious charging and discharging commands, the proposed ML detector can determine this abnormal pattern in charging and discharging commands. To show how we can calculate the reward function for each branch of the proposed MDP tree, it is assumed that 25% of the total loads in each zone of the IEEE 33-bus system can be defined as EV loads. To calculate this EV load penetration rate, it can be seen that the first zone of the IEEE 33-bus distribution network supplies about 430 kW of different loads. Based on technical discussions in [4, 7, 69], we can assume that there are around 150 electric vehicles (EVs) in this zone of the IEEE 33-bus distribution network using a comparable ratio for EVs to the total loads mentioned in the realistic scenario of the *Manhattan* system of New York City in the US[7]. The International Energy Agency (IEA) estimates that governments and operators typically maintain 1 public EVCS for every 10 EVs on the road, which results in this zone including around 15 EVCSs. Considering 22 kW as the average charging rate of commercial level 2 and level 3 chargers [69, 4] and approximately 30% chance of EVCS availability, this zone of the network can be estimated to consist of roughly 5 viable charging

Table 5.3: Calculating terms of developed reward function for five different zones

Action	**From s to s'**	$\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}}$	ΔV_d^{Ave}	$\frac{\Delta P_a^{Loss}(s,s')-\Delta P_T^{Loss}}{\Delta P_T^{Loss}}$	$RF_a(s,s')$
a_3	s_3 to s_4	0.1064	1.5467	0.0196	1.6727
a_5	s_3 to s_5	0.0851	1.5356	0.0049	1.6256
a_7	s_3 to s_6	0.2553	1.5599	0.0562	1.8714
a_9	s_3 to s_7	0.2553	1.6305	0.1395	2.0253
a_{11}	s_3 to s_8	0.2979	1.6709	0.1654	2.1342

Table 5.4: Security Metric Evaluation of Single Contingency MDP Tree for Two Discount Factors

State	V^*	π^*	V^*	π^*	**State**	V^*	π^*	V^*	π^*
	$\gamma = 0.95$		$\gamma = 0.5$			$\gamma = 0.95$		$\gamma = 0.5$	
s1	37.1798	a24	1.0309	a13	s19	32.5120	a30	3.2512	a30
s2	30.9029	a2	1.2846	a2	s20	37.1504	a32	3.4826	a32
s3	33.0152	a3	2.9529	a3	s21	37.4280	a33	3.7428	a33
s4	33.4540	a4	3.3454	a4	s22	40.2056	a35	3.7690	a35
s5	32.5120	a6	3.2512	a6	s23	40.5060	a36	4.0506	a36
s6	37.4280	a8	3.7428	a8	s24	42.3675	a38	3.9717	a38
s7	40.5060	a10	4.0506	a10	s25	42.6840	a39	4.2684	a39
s8	42.6840	a12	4.2684	a12	s26	39.4691	a54	1.6591	a54
s9	41.7462	a22	3.4854	a22	s27	33.2274	a43	3.1319	a43
s10	33.4540	a15	3.3454	a15	s28	33.4540	a44	3.3454	a44
s11	32.5120	a17	3.2512	a17	s29	32.2918	a46	3.0437	a46
s12	37.4280	a19	3.7428	a19	s30	32.5120	a47	3.2512	a47
s13	40.5060	a21	4.0506	a21	s31	37.1745	a49	3.5039	a49
s14	42.6840	a23	4.2684	a23	s32	37.4280	a50	3.7428	a50
s15	39.7211	a37	1.7529	a37	s33	40.2317	a52	3.7921	a52
s16	33.2059	a26	3.1128	a26	s34	40.5060	a53	4.0506	a53
s17	33.4540	a27	3.3454	a27	s35	42.3949	a55	3.9959	a55
s18	32.2709	a29	3.0252	a29	s36	42.6840	a56	4.2684	a56

stations for attacks that are equal to about 25% of the total loads in the first zone of the network. To display the worst-case attack scenario, all mentioned EV loads are compromised by adversaries. After manipulating EV loads, the voltage deviates from its nominal values in different buses of the distribution network, and their average can be calculated using power flow analysis based on (82). Furthermore, the active power loss of each branch in the system will increase, leading to more total active power losses. Based on these calculations, the active power loss of the system during normal operation is 181.2 kW. However, during cyber attacks on EV loads in Zone_1, Zone_2, Zone_3, Zone_4, and Zone_5, this number increases to 184.8 kW, 182.1 kW, 191.4 kW, 206.5 kW, and 211.2 kW, respectively. According to the calculated numbers in the DSO control center, each term of the reward function can be obtained using (85) and summarized in Table. 5.3 under the assumption $\alpha_1 = \alpha_2 = \alpha_3 = 1$. For branches a_1 and a_2, we have no reward. Since attackers stay in states s_4, s_5, s_6, s_7, s_8 and repeat the same actions, related branches, i.e., $a_4, a_6, a_8, a_{10}, a_{12}$, will receive the same reward functions. This calculation will also be repeated for other vulnerabilities.

Numerical Analysis: The sets of $\mathcal{S} = \{s_1, ..., s_{36}\}$ and $\mathcal{A} = \{a_1, ..., a_{56}\}$ have been referred to as states and adversarial actions of the MDP tree, respectively. The s_1 is the initial state where no

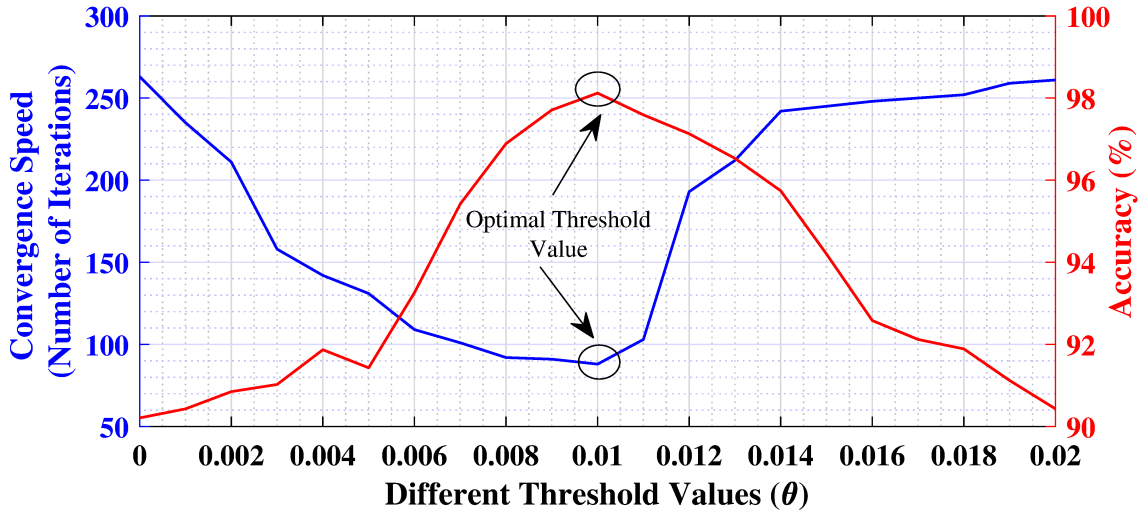


Figure 5.13: Accuracy and convergence speed against different thresholds (θ).

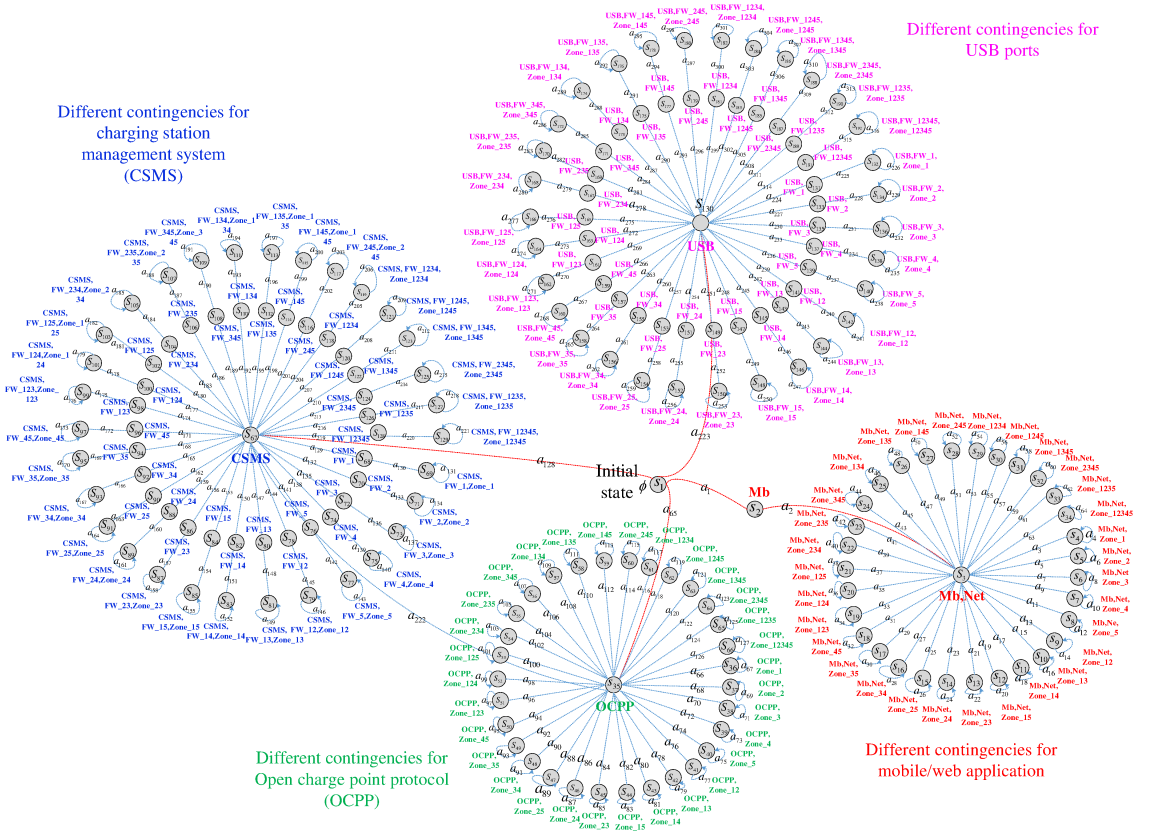


Figure 5.14: MDP tree for multiple contingencies in IEEE 33-bus system and four vulnerabilities in EV ecosystem

Table 5.5: Security Metric Evaluation for Multiple Contingencies with γ=0.95

State	V^*	π^*	State	V^*	π^*	state	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*
s1	59.4158	a65	s29	52.5480	a54	s57	50.2360	a109	s85	45.5500	a155	s113	52.4280	a197	s141	35.4713	a240	s169	50.1418	a282
s2	59.1581	a2	s30	58.0460	a56	s58	52.4280	a111	s86	39.3885	a157	s114	55.1670	a199	s142	35.7600	a241	s170	51.8540	a283
s3	63.2017	a63	s31	62.6660	a58	s59	55.7320	a113	s87	39.7360	a158	s115	55.7320	a200	s143	39.9409	a243	s171	57.7675	a285
s4	33.4540	a4	s32	62.0560	a60	s60	55.1360	a115	s88	42.0192	a160	s116	54.5771	a202	s144	40.2660	a244	s172	59.7400	a286
s5	32.5120	a6	s33	54.7400	a62	s61	52.5480	a117	s89	42.3900	a161	s117	55.1360	a203	s145	43.0179	a246	s173	48.5773	a288
s6	37.4280	a8	s34	64.5560	a64	s62	58.0460	a119	s90	44.5965	a163	s118	51.9388	a205	s146	43.3680	a247	s174	50.2360	a289
s7	40.5060	a10	s35	63.7590	a126	s63	62.6660	a121	s91	44.9900	a164	s119	52.5480	a206	s147	45.1822	a249	s175	50.6969	a291
s8	42.6840	a12	s36	31.9265	a67	s64	62.0560	a123	s92	46.9438	a166	s120	57.3731	a208	s148	45.5500	a250	s176	52.4280	a292
s9	35.7600	a14	s37	32.5120	a69	s65	54.7400	a125	s93	47.3580	a167	s121	58.0460	a209	s149	39.4152	a252	s177	53.8918	a294
s10	40.2660	a16	s38	37.4280	a71	s66	64.5560	a127	s94	49.1087	a169	s122	61.9395	a211	s150	39.7360	a253	s178	55.7320	a295
s11	43.3680	a18	s39	40.5060	a73	s67	59.4248	a219	s95	49.5420	a170	s123	62.6660	a212	s151	42.0478	a255	s179	53.3155	a297
s12	45.5500	a20	s40	42.6840	a75	s68	33.2059	a130	s96	52.3620	a172	s124	61.3366	a214	s152	42.3900	a256	s180	55.1360	a298
s13	39.7360	a22	s41	35.7600	a77	s69	33.4540	a131	s97	52.8240	a173	s125	62.0560	a215	s153	44.6268	a258	s181	51.8993	a300
s14	42.3900	a24	s42	40.2660	a79	s70	32.2709	a133	s98	42.1444	a175	s126	54.1054	a217	s154	44.9900	a259	s182	52.5480	a301
s15	44.9900	a26	s43	43.3680	a81	s71	32.5120	a134	s99	42.5760	a176	s127	54.7400	a218	s155	46.9756	a261	s183	57.3294	a303
s16	47.3580	a28	s44	45.5500	a83	s72	37.1504	a136	s100	44.7933	a178	s128	63.7092	a220	s156	47.3580	a262	s184	58.0460	a304
s17	49.5420	a30	s45	39.7360	a85	s73	37.4280	a137	s101	45.2520	a179	s129	64.5560	a221	s157	49.1420	a264	s185	61.1615	a306
s18	52.8240	a32	s46	42.3900	a87	s74	40.2056	a139	s102	46.9532	a181	s130	59.1786	a314	s158	49.5420	a265	s186	62.6660	a307
s19	42.5760	a34	s47	44.9900	a89	s75	40.5060	a140	s103	47.4340	a182	s131	33.2274	a225	s159	52.3975	a267	s187	61.2899	a309
s20	45.2520	a36	s48	47.3580	a91	s76	42.3675	a142	s104	48.7428	a184	s132	33.4540	a226	s160	52.8240	a268	s188	62.0560	a310
s21	47.4340	a38	s49	49.5420	a93	s77	42.6840	a143	s105	49.2420	a185	s133	32.2918	a228	s161	41.1702	a270	s189	54.0642	a312
s22	49.2420	a40	s50	52.8240	a95	s78	35.4472	a145	s106	51.3283	a187	s134	32.5120	a229	s162	42.5760	a271	s190	54.7400	a313
s23	51.8540	a42	s51	42.5760	a97	s79	35.7600	a146	s107	51.8540	a188	s135	37.1745	a231	s163	43.7578	a273	s191	63.7590	a315
s24	59.7400	a44	s52	45.2520	a99	s80	39.9138	a148	s108	59.1344	a190	s136	37.4280	a232	s164	45.2520	a274	s192	64.5560	a316
s25	50.2360	a46	s53	47.4340	a101	s81	40.2660	a149	s109	59.7400	a191	s137	40.2317	a234	s165	45.8678	a276			
s26	52.4280	a48	s54	49.2420	a103	s82	42.9887	a151	s110	49.7268	a193	s138	40.5060	a235	s166	47.4340	a277			
s27	55.7320	a50	s55	51.8540	a105	s83	43.3680	a152	s111	50.2360	a194	s139	42.3949	a237	s167	47.6161	a279			
s28	55.1360	a52	s56	59.7400	a107	s84	45.1516	a154	s112	51.8965	a196	s140	42.6840	a238	s168	49.2420	a280			

components of the EV ecosystem have been targeted. Based on the mentioned attacker's access points, adversaries may take the first action (a_1) and move from the initial state (s_1) to the Mb/web application state (s_2) randomly. Then, they can target the business network of EVSE, i.e., s_3, using the attack graphs discussed in Section 2.3 by taking the next adversarial action (a_2). Afterward, the attacker acts a_3 and gains control of EVCSs in the first zone, reaching state s_4 and issuing charging or discharging commands. They can also repeat this adversarial action (a_4) causing more impact on the distribution network operation. The proposed MDP tree is resolved by Algorithm 7, and the values of each state (V^*) and optimal adversarial action (π^*) for $\alpha_1 = \alpha_2 = \alpha_3 = 1$ and two values of discount factor $\gamma = 0.95$ and $\gamma = 0.5$ are listed in Table. 5.4. A series of preliminary experiments are performed to identify an optimal range for the threshold value, i.e., θ [98]. The choice of θ can be based on a balanced performance in terms of convergence speed (i.e., the number of algorithm iterations to converge) and accuracy [99]. To quantify the impact of θ on convergence speed, we have measured the number of iterations required for the algorithm to converge under different threshold values. Furthermore, to calculate the accuracy of the modified policy iteration algorithm against changes in the threshold value, we can run the algorithm with a specific threshold value and calculate the error by comparing the obtained state values to the benchmark values. For this purpose, we can compare the state values obtained from the algorithm with the benchmark state values and calculate the error using a metric such as mean squared error (MSE):

$$MSE = \frac{1}{N_{st}} \sum_{s=1}^{N_{st}} \left(V_\theta(s) - V_{nom}(s) \right)^2 \tag{98}$$

where N_{st} is the number of states in the generated MDP trees, $V_\theta(s)$ and $V_{nom}(s)$ can be defined as the values for state s from the algorithm and benchmark, respectively. Finally, we can normalize the error values and convert them into accuracy percentages, as follows[99]:

$$Accuracy = 100\% - (\frac{MSE}{Maximum \quad vlaue \quad of \quad MSE} \times 100\%) \tag{99}$$

where the maximum possible MSE can be defined as a value that represents the worst-case scenario, i.e., comparing all state values to zero. This process can be repeated for each threshold value to obtain a set of accuracy values. Finally, both accuracy and convergence speed of the modified policy iteration algorithm for different threshold values have been illustrated in Fig. 5.13. It can be concluded that minor deviations from the chosen threshold, i.e., θ=0.01, cannot significantly impact the overall performance of our algorithm, indicating that our selection of θ can be optimal and reliable. At this threshold, the number of iterations is about 88, and the state accuracy value has been obtained at about 98.12%. The variation of γ depicts the attacker's interest in future rewards (γ=0.95) instead of immediate rewards (γ=0.5). It can be seen that a discount factor near 1 assigns more weight to future rewards, encouraging the agent of the proposed iteration algorithm to prioritize long-term rewards, leading to more numerical values for states. Moreover, when the adversaries prefer one term of the reward function over the other terms, the related coefficient, i.e., $\{\alpha_1, \alpha_2, \alpha_3\}$, can be initialized to one in the related term. Based on the results from Table. 5.4, this security metric can quantify the impacts of attacks originating from the EV ecosystem by calculating a value for each state resembling the compromised parts of EV ecosystems. For example, in this table, for γ=0.95, the value function (V^*) for the first state (s_1) and next optimal adversarial action (π^*) are obtained as 37.1798 and a_{24}, respectively. It means that the second action after this state to achieve the highest cumulative reward function and severe impacts on the system operation is a_{24}. By taking this action, the attackers compromise the CSMS and move to a new state, i.e., s_{15}. The next adversarial action for the state s_{15} is a_{37}, which means targeting the firmware repository of EVCSs in the Zone_5 of the IEEE 33-bus system and moving to state s_{24}. The value function of this state is 42.3675, and the next adversarial action is a_{38}. This action means adversaries take control of EVCS in the Zone_5 of the system and issue the charging-discharging commands. They can stay in the state s_{25} for more severe impacts and continue these commands by taking action a_{39}.

With the definition of another value for the discount factor, the value function for each state and the next adversarial action may differ. In the following, the developed security metric is evaluated in the presence of multiple contingencies, where adversaries can manipulate more than one zone in the distribution network by compromising 25% of the total loads as EV loads. In this situation, the number of states and adversarial actions for the customized MDP tree will increase to 192 and 316, respectively. The related MDP tree generated through Algorithm 6 has been shown in Fig. 5.14. The result of resolving this MDP tree by Algorithm 7 has been summarized in Table. 5.5. It can be concluded from this table that multiple contingencies put the IEEE 33-bus system at more risk from several vulnerabilities in the EV ecosystem, and the value of each state is greater than a single contingency MDP tree that was previously developed. Moreover, adversaries can select more states of the MDP tree to cause severe impacts on the operation of the distribution network.

Comparative Analysis with Existing Security Metrics: The performance of our metric can also be compared with the SOCCA metric [76] to represent a numerical analysis and highlight the advantages of the proposed security metric. In the SOCCA metric, the reward function is based on overloaded transmission lines after cyber attacks. First, in SOCCA's reward function, it is impossible to distinguish between overloading originating from peak loads or manipulated charging stations due to the lack of a framework to report compromised EVCSs. As a result, SOCCA fails to quantify the security posture of the distribution network during EVCS manipulation. Moreover, the calculated value of states in the MDP tree obtained from SOCCA's reward function for the EV ecosystem integrated into distribution networks is lower than our proposed security metric. This can lead to confusion in the interpretation of states during the design of the monitoring security system and DSOs. For example, the SOCCA's reward function calculates the first state value (s_1) as 1.6084, compared to the value state obtained from our security metric which is 37.1789.

Designing Monitoring Framework: The customized deep CNN can be trained on a total data sample of 7,775, which is generally collected from resolving different MDP trees using the policy iteration algorithm. The previous three conditions can give meaningful margins for the security status of distribution networks under EV-based attacks. To assign secure and alarm labels, the

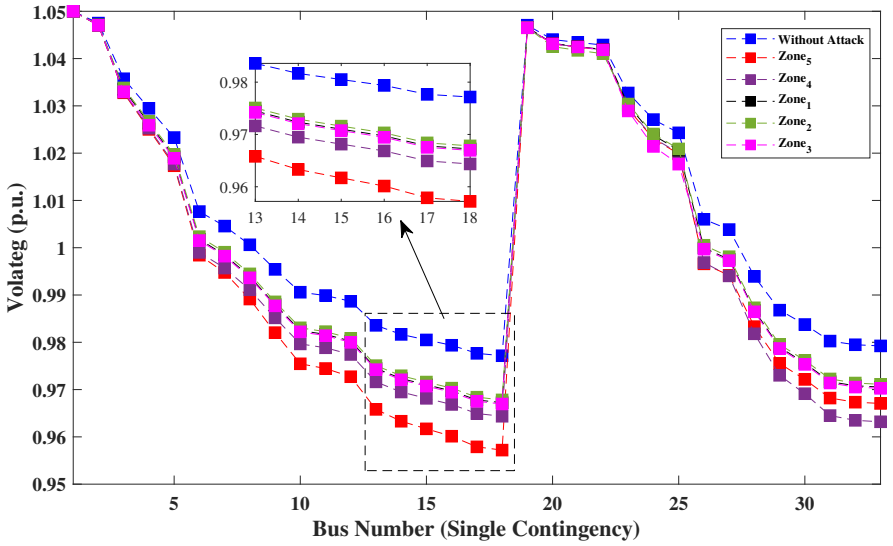


Figure 5.15: Voltage deviation at different buses of the IEEE 33-bus system under cyber attacks on EV loads in single zones.

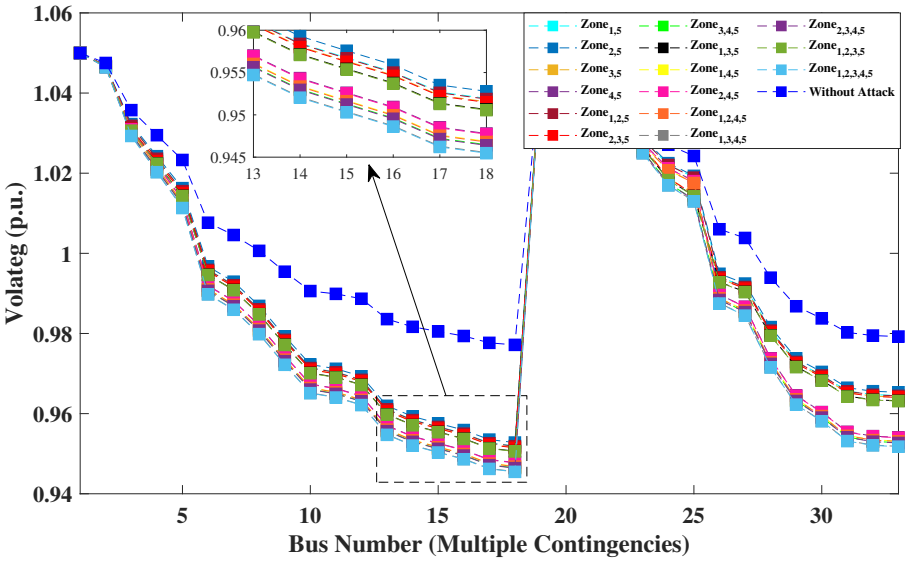


Figure 5.16: Voltage deviation at different buses of the IEEE 33-bus system under cyber attacks on EV loads in multiple zones.

voltage deviation at different buses of IEEE 33-bus for five zones and critical multiple zones after manipulating 25% of EV loads has been illustrated in Fig. 5.15 and Fig. 5.16, respectively. It can be concluded from Fig. 5.15 that targeting EVCSs in Zone_5 among single contingencies can lead to the most voltage deviation. Without manipulating EV loads, the nominal voltage of Bus 18 is 0.9770 p.u. If attackers can manipulate EV loads located in buses of Zone_5, the bus voltage decreases

Table 5.6: Metrics for Trained Deep CNN Model

Approach	Accuracy	Precision	Recall	F-Score
Multi-layer deep CNN	98.314	94.079	92.556	93.311
SVM [65]	92.497	91.289	88.058	89.644

to 0.9570 p.u., leading to a deviation of 2.01%. From Fig. 5.16, among multiple contingencies, manipulating EV loads in $\text{Zone}_{1,2,3,4,5}$ can lead to the most voltage deviation. Also, manipulating EV loads in 15 combinations of multiple contingencies, e.g., $\text{Zone}_{1,5}$, $\text{Zone}_{2,5}$, $\text{Zone}_{3,5}$, $\text{Zone}_{4,5}$,..., $\text{Zone}_{1,2,3,4,5}$, causes an unacceptable voltage deviation from its nominal value of more than 2.5% at Bus 18. For example, without manipulating EV loads, the nominal voltage of Bus 18 is 0.9770 p.u. When adversaries manipulate the EV loads of buses in both Zone_2 and Zone_5, this voltage decreases to 0.9525 p.u., leading to a deviation of 2.51%. Moreover, the percentage of manipulated EVCS to total EVCS (40%) and the total active power loss (21.2%) after manipulating EV loads in these zones are bigger than their thresholds. As such, this situation can be labeled as an alarm for the offline training process. For $\text{Zone}_{1,2,3,4,5}$, this voltage also decreases to 0.9454 p.u., which leads to a deviation of 3.28%, labeling it an alarm situation. To train the CNN model in an offline manner, the training, validation, and testing data sets are partitioned by 80%, 10%, and 10% of the total data sets, respectively. The cross-entropy loss and accuracy plots of training and validation data sets have been illustrated in Fig. 5.17 for the IEEE 33-bus distribution network. It can be observed that the cross-entropy loss function decreases gradually in the initial epochs of the validation process, while the binary classification accuracy plot increases during training. This behaviour means the CNN model can deliver acceptable performance in providing information about the security status of the power grid for DSOs during EV-cyber attacks. After offline training of the developed deep CNN model, its performance can also be compared with support vector machine (SVM) [65] using several criteria, e.g., accuracy, precision, recall, and the F-score that has been calculated in Table. 5.6. The proposed deep CNN model provides higher accuracy in giving information about the security status of the distribution network. The main reason is that multiple convolutional layers, along with a deep CNN structure, can extract better features for classification, making this framework a proper tool for applications of security status monitoring.

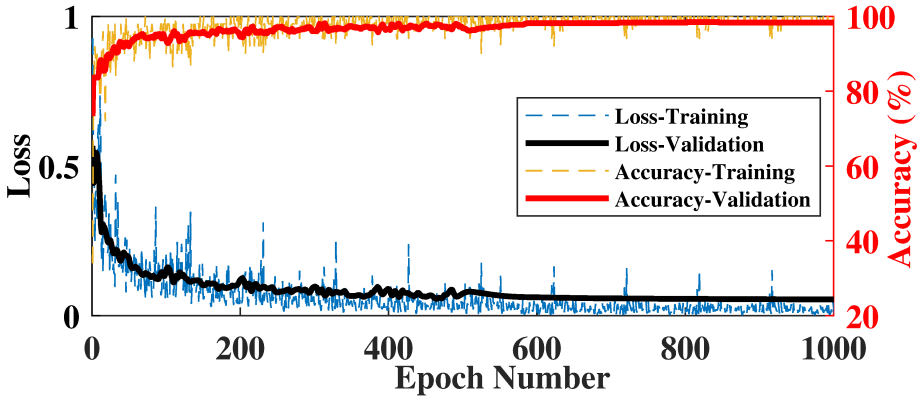


Figure 5.17: Training and validation accuracy and loss for the deep CNN.

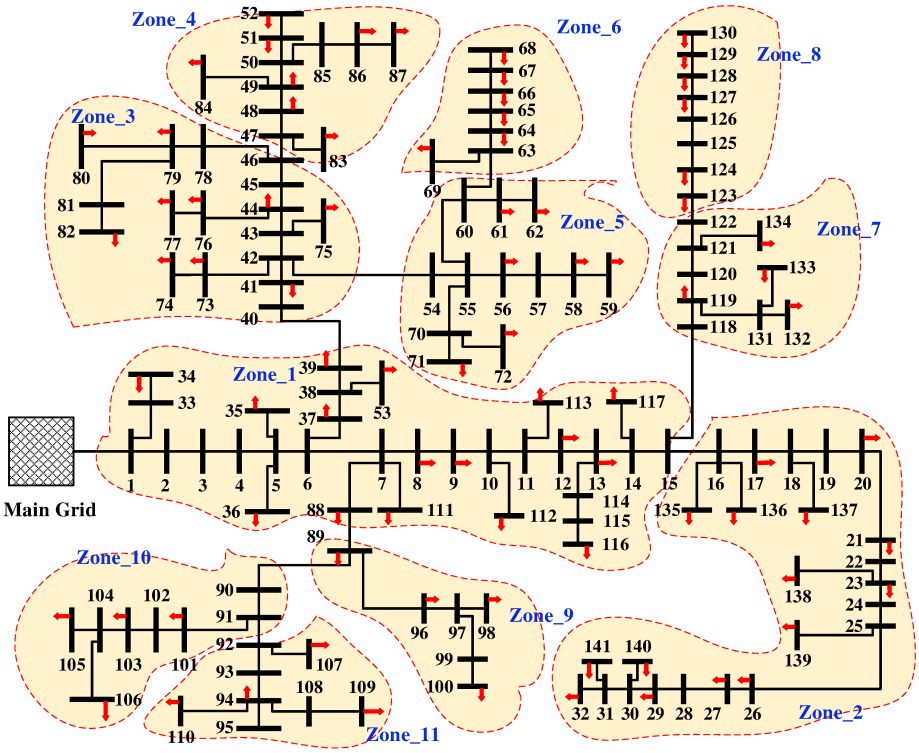


Figure 5.18: Standard 141-bus distribution network in Caracas

5.6.3 Scalability of Security Metric

In this part, the 141-bus distribution network in Caracas [100] is selected to investigate the scalability of the developed security metric, as shown in Fig. 5.18. As already discussed, the number of vulnerabilities that attackers can maliciously exploit to impact the operation of the distribution network are CSMS, OCPP, mobile/web applications, and USB ports. In this network, buses located in the same geographical region and lateral branches are defined as separate zones. On this basis,

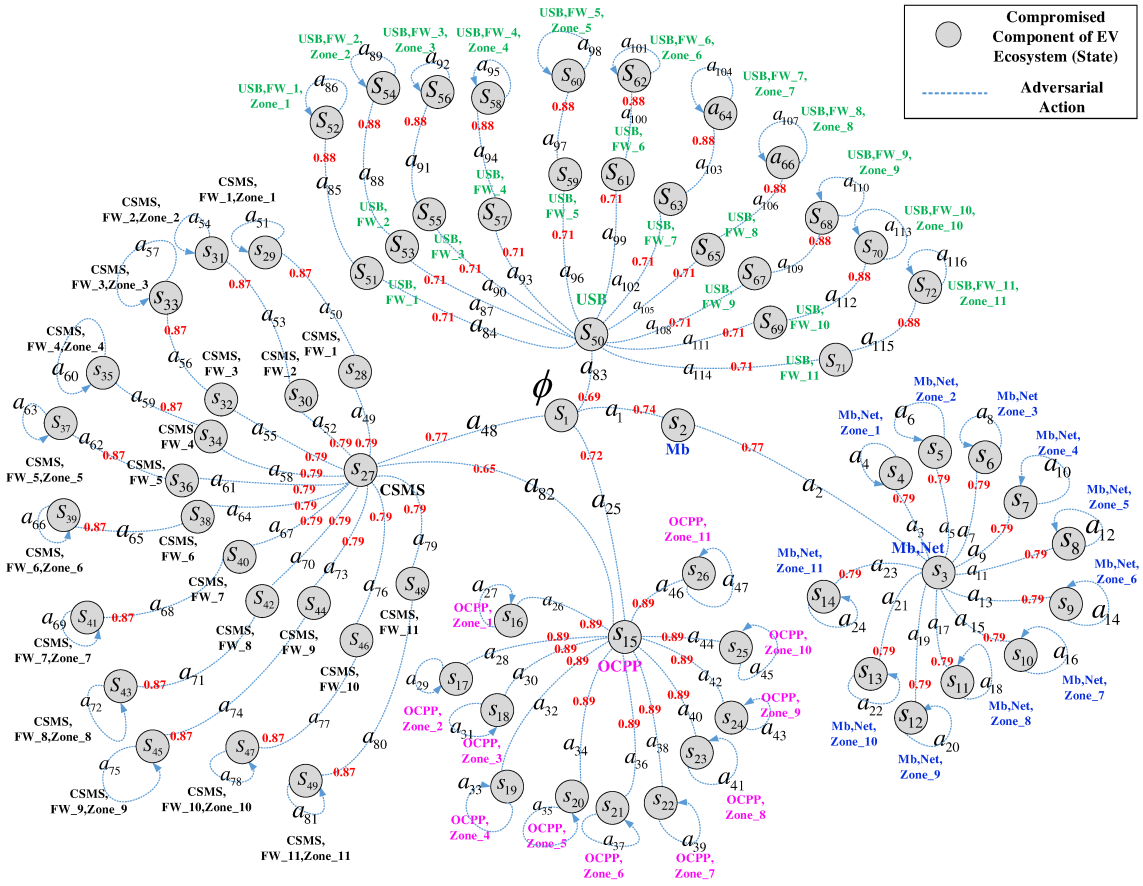


Figure 5.19: MDP tree generated by Algorithm 6 for enumerating states and transition among them for a distribution network with Z_T=11 distinct zones

Table 5.7: Calculating terms of reward function for 11 separate zones

Action	**From** s **to** s'	$\frac{N_a^{Comp}(s,s')}{N_T^{EVCS}}$	ΔV_d^{Ave}	$\frac{\Delta P_a^{Loss}(s,s') - \Delta P_T^{Loss}}{\Delta P_T^{Loss}}$	$RF_a(s,s')$
a_3	s_3 to s_4	0.1349	2.8780	0.6409	3.6537
a_5	s_3 to s_5	0.0929	2.8880	0.6411	3.6220
a_7	s_3 to s_6	0.1706	2.9337	0.6552	3.7595
a_9	s_3 to s_7	0.1014	2.8941	0.6468	3.6422
a_{11}	s_3 to s_8	0.1014	2.8892	0.6456	3.6362
a_{13}	s_3 to s_9	0.0801	2.8767	0.6430	3.5998
a_{15}	s_3 to s_{10}	0.0189	2.8383	0.6343	3.4915
a_{17}	s_3 to s_{11}	0.0425	2.8536	0.6364	3.5325
a_{19}	s_3 to s_{12}	0.0580	2.8472	0.6363	3.5415
a_{21}	s_3 to s_{13}	0.0420	2.8421	0.6354	3.5195
a_{23}	s_3 to s_{14}	0.1503	2.8803	0.6425	3.6732

this network can be divided into 11 distinct zones. Considering four well-known vulnerabilities in the EV ecosystem, an MDP tree with 72 states and 116 adversarial actions can be obtained using Algorithm 6 during single contingencies in the 141-bus distribution network, as illustrated

Table 5.8: Security Metric Evaluation for IEEE 141-bus with γ=0.95

State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*
s1	65.4941	a48	s19	72.8440	a33	s37	72.7240	a63	s55	74.6808	a91
s2	69.4562	a2	s20	72.7240	a35	s38	71.4621	a65	s56	75.1900	a92
s3	74.2037	a7	s21	71.9960	a37	s39	71.9960	a66	s57	72.3507	a94
s4	73.0740	a4	s22	69.8300	a39	s40	69.3122	a68	s58	72.8440	a95
s5	72.4400	a6	s23	70.6500	a41	s41	69.8300	a69	s59	72.2315	a97
s6	75.1900	a8	s24	70.8300	a43	s42	70.1261	a71	s60	72.7240	a98
s7	72.8440	a10	s25	70.3900	a45	s43	70.6500	a72	s61	71.5084	a100
s8	72.7240	a12	s26	73.4640	a47	s44	70.3047	a74	s62	71.9960	a101
s9	71.9960	a14	s27	69.9708	a55	s45	70.8300	a75	s63	69.3571	a103
s10	69.8300	a16	s28	72.9192	a50	s46	69.8680	a77	s64	69.8300	a104
s11	70.6500	a18	s29	73.4640	a51	s47	70.3900	a78	s65	70.1716	a106
s12	70.8300	a20	s30	71.9028	a53	s48	72.9192	a80	s66	70.6500	a107
s13	70.3900	a22	s31	72.4400	a54	s49	73.4640	a81	s67	70.3503	a109
s14	0	a1	s32	74.6324	a56	s50	69.5269	a90	s68	70.8300	a110
s15	74.2037	a30	s33	75.1900	a57	s51	72.5791	a85	s69	3.4957	a112
s16	73.0740	a27	s34	72.3038	a59	s52	73.0740	a86	s70	0	a1
s17	72.4400	a29	s35	72.8440	a60	s53	71.9494	a88	s71	72.9665	a115
s18	75.1900	a31	s36	72.1847	a62	s54	72.4400	a89	s72	73.4640	a116

in Fig. 5.19. It is also assumed that 10% of the total load in each bus is EV loads that attackers can maliciously target. To allocate the probabilities for each branch of the MDP tree, the proposed CVSS V3.1 is used, as shown by the red numerical values in Fig. 5.19. Furthermore, the voltage deviation of different buses, active power loss, and the number of compromised charging stations are measured in the DSO control center, and the related reward function for each adversarial action can be calculated as shown in Table. 5.7. The generated MDP tree for the 141-bus network can be resolved using the modified policy iteration algorithm with γ=0.95. The results obtained for each state's value and optimal adversarial action can be summarized in Table 5.8. According to this table, the value of the first state is 65.4941, and the best adversarial action is a_{48}. It means that if adversaries take action a_{48}, they must compromise the CSMS of the EV ecosystem and move toward state s_{27}. The value of this state is 69.9708, and the best action that can be taken to cause a severe impact will be a_{55}. With this action, adversaries could compromise the firmware repository of the EV ecosystem in the third zone of the 141-bus distribution network and access to state s_{32}. In this state, the best action is a_{56}, which means targeting charging stations in this zone and manipulating the EV loads in this zone. Finally, they can stay in the state s_{33} and repeat their action to have the most severe impact. For two states, i.e., s_{14} and s_{70}, the state value is calculated as 0 with the next adversarial action a_1. It means that the best strategy for the attacker is to return to state s_1 and take action a_{48}.

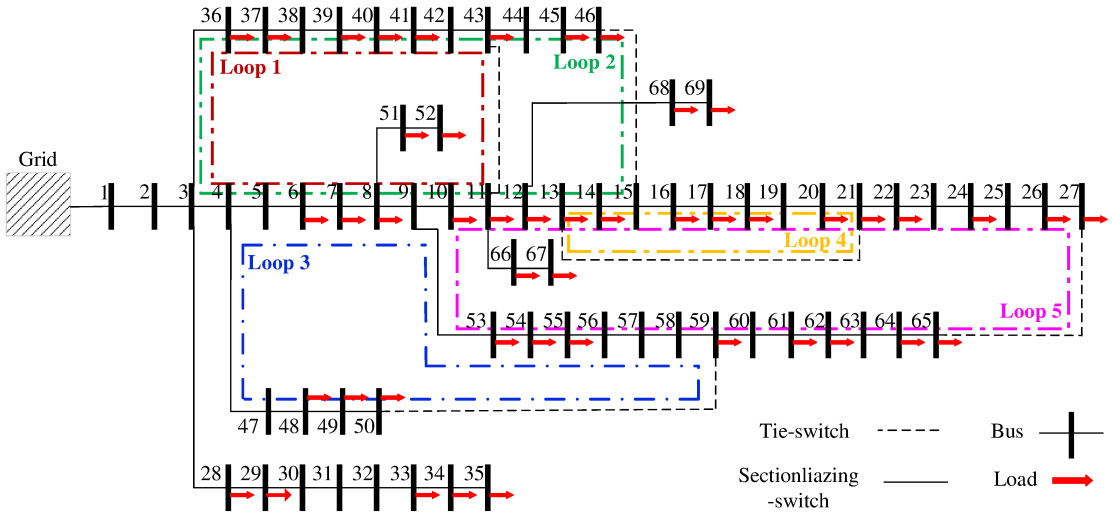


Figure 5.20: Dynamic sections of IEEE 69-bus distribution network during five loops

5.6.4 Security Metric for Distribution Network with Dynamic Sections

Since the topology of the distribution networks may change due to multiple switching scenarios, the voltage profiles are not necessarily related to closed buses in fixed (or static) zones. On this basis, dividing distribution networks into several static zones may not be practical for multiple switching scenarios and variable topologies of distribution networks. From this perspective, a supplementary strategy has been suggested to calculate the security metric for all load buses (N_L) instead of zones (Z_T). For this section, we have simulated the looped IEEE 69-bus distribution network using tie-switches and sectionalizing switches and changed the situation of the mentioned switches to create dynamic sections in power grids. When distribution networks operate in radial form, sectionalizing switches are normally closed and tie switches are normally open [101]. However, the topology of distribution networks can change and turn into several dynamic sections based on fault isolation and maintenance capabilities, improving the distribution networks' reliability, efficiency, and flexibility.

The IEEE 69-bus distribution network with a voltage level of 12.66 kV includes 68 normally closed and 5 normally open switches. In this network, first, we have assumed that all tie-switches are closed to provide five loops, i.e., {Loop 1, Loop 2,..., Loop 5}, as shown in Fig. 5.20. These tie-switches have been located between 5-pair buses, i.e., (11-43), (13-21), (15-46), (50-59), and (27-65). Other important information about this network can be extracted from this reference [102]. In the first stage, we study the attackers' interest in the existing 48-load buses (N_L=48) that can

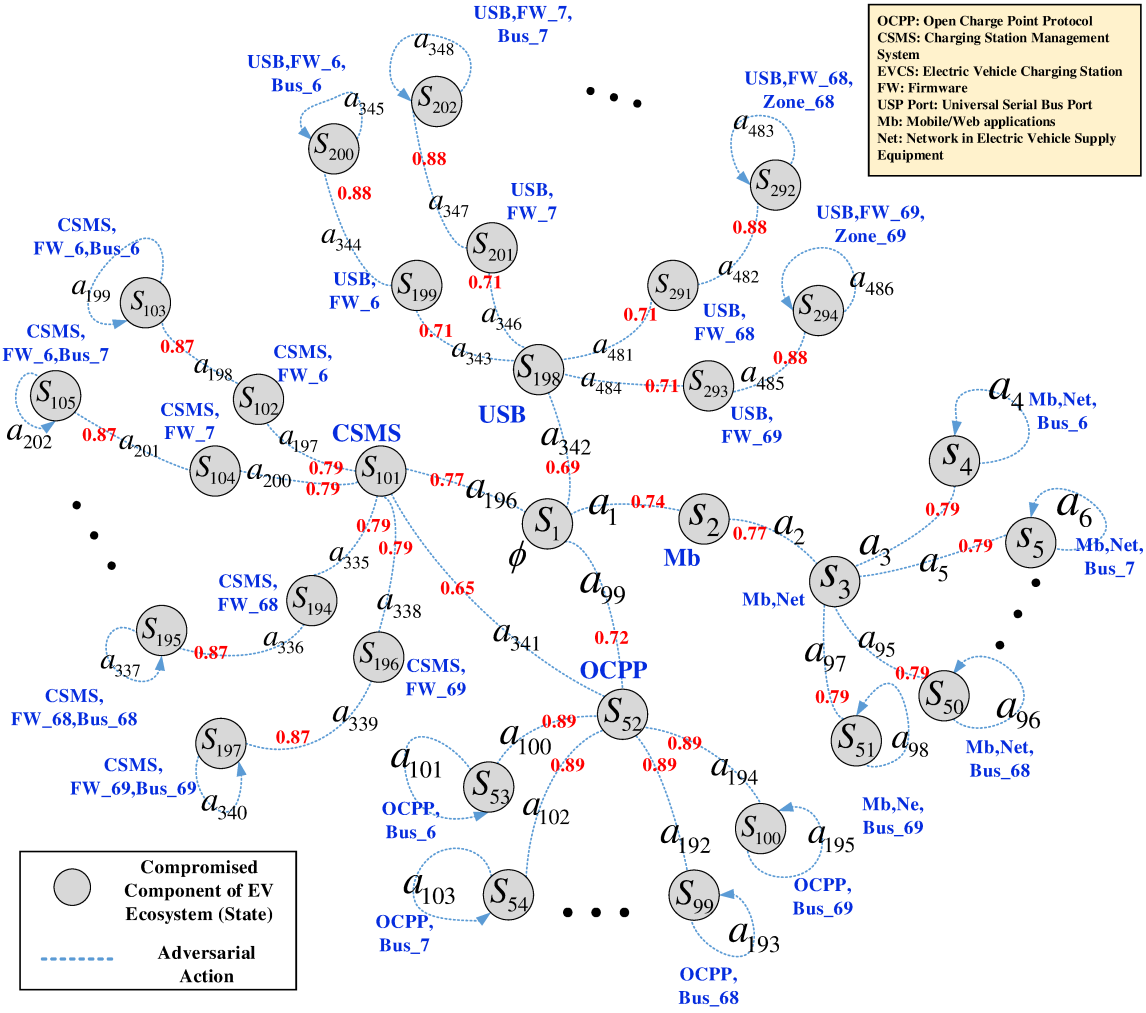


Figure 5.21: IEEE 69-bus distribution network in the form of looped operation

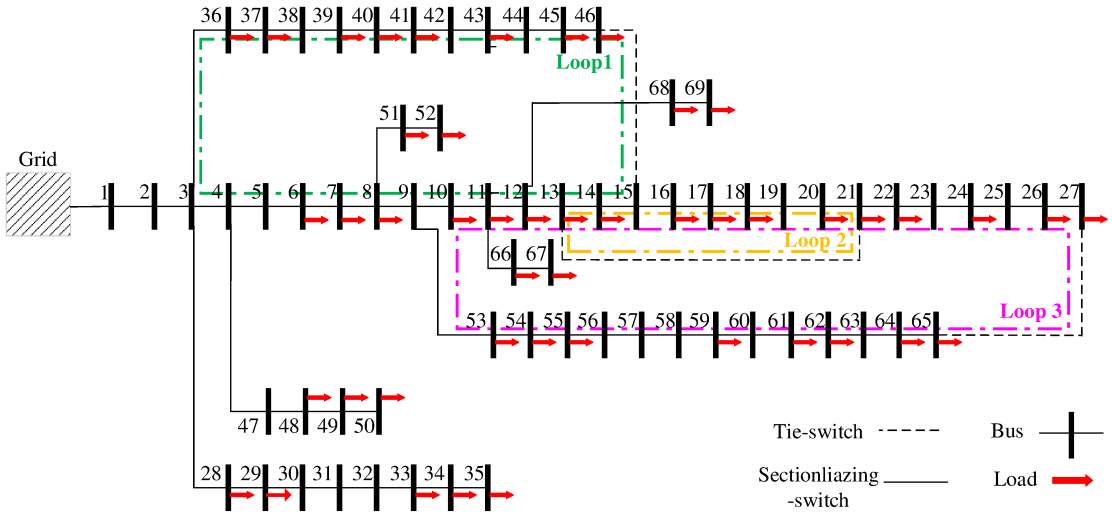


Figure 5.22: Dynamic sections of IEEE 69-bus distribution network during three loops

Table 5.9: Security Metric Evaluation for Dynamic 69-bus Distribution Network (Five Loops)

State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*
s1	45.1263	a196	s43	44.9870	a82	s85	47.4298	a165	s127	28.6002	a235	s169	47.8952	a298	s211	45.0098	a362	s253	29.2787	a425
s2	44.3698	a2	s44	50.9624	a84	s86	47.8952	a167	s128	45.0789	a237	s170	43.1578	a300	s212	45.1216	a363	s254	29.5587	a426
s3	51.1598	a83	s45	44.2597	a86	s87	43.5102	a169	s129	45.3902	a238	s171	43.5102	a301	s213	29.1220	a365	s255	29.7138	a428
s4	29.3671	a4	s46	46.5703	a88	s88	29.5071	a171	s130	29.4428	a240	s172	29.4110	a303	s214	29.6987	a366	s256	29.9300	a429
s5	43.1574	a6	s47	44.1890	a90	s89	29.6631	a173	s131	29.7418	a241	s173	29.5071	a304	s215	29.3346	a368	s257	42.8907	a431
s6	43.9658	a8	s48	42.9348	a92	s90	43.2078	a175	s132	43.3389	a243	s174	29.2281	a306	s216	29.6988	a369	s258	43.0278	a432
s7	44.0025	a10	s49	42.9966	a94	s91	42.8118	a177	s133	43.8564	a244	s175	29.6631	a307	s217	43.0720	a371	s259	42.7207	a434
s8	43.9812	a12	s50	43.5648	a96	s92	44.9870	a179	s134	42.4412	a246	s176	43.0099	a309	s218	43.2687	a372	s260	42.9287	a435
s9	45.1215	a14	s51	43.2080	a98	s93	50.9624	a181	s135	42.5701	a247	s177	43.2078	a310	s219	43.9661	a374	s261	43.7782	a437
s10	45.1216	a16	s52	51.1598	a180	s94	44.2597	a183	s136	42.0733	a249	s178	42.4579	a312	s220	44.2888	a375	s262	44.0213	a438
s11	29.6987	a18	s53	29.8971	a101	s95	46.5703	a185	s137	42.3399	a250	s179	42.8118	a313	s221	44.1045	a377	s263	47.1144	a440
s12	29.6988	a20	s54	43.1574	a103	s96	44.1890	a187	s138	42.8122	a252	s180	44.7712	a315	s222	44.2678	a378	s264	47.4298	a441
s13	43.2687	a22	s55	43.9658	a105	s97	42.9348	a189	s139	43.0189	a253	s181	44.9870	a316	s223	28.2789	a380	s265	47.7701	a443
s14	44.2888	a24	s56	44.0025	a107	s98	42.9966	a191	s140	42.8712	a255	s182	50.6007	a318	s224	28.6002	a381	s266	47.8952	a444
s15	44.2678	a26	s57	43.9812	a109	s99	43.5648	a193	s141	43.1009	a256	s183	50.9624	a319	s225	45.0789	a383	s267	43.1578	a446
s16	28.6002	a28	s58	45.1215	a111	s100	43.208	a195	s142	42.3317	a258	s184	44.0013	a321	s226	45.3902	a384	s268	43.5102	a447
s17	45.3902	a30	s59	45.1216	a113	s101	51.2489	a317	s143	42.6987	a259	s185	44.2597	a322	s227	29.4428	a386	s269	29.4110	a449
s18	29.7418	a32	s60	29.6987	a115	s102	28.9187	a198	s144	42.6668	a261	s186	46.4129	a324	s228	29.7418	a387	s270	29.5071	a450
s19	43.8564	a34	s61	29.6988	a117	s103	29.8971	a199	s145	42.9037	a262	s187	46.5703	a325	s229	43.3389	a389	s271	29.2281	a452
s20	42.5701	a36	s62	43.2687	a119	s104	43.0142	a201	s146	29.6129	a264	s188	43.9910	a327	s230	43.8564	a390	s272	29.6631	a453
s21	42.3399	a38	s63	44.2888	a121	s105	43.1574	a202	s147	29.9401	a265	s189	44.1890	a328	s231	42.4412	a392	s273	43.0099	a455
s22	43.0189	a40	s64	44.2678	a123	s106	43.2581	a204	s148	42.9100	a267	s190	42.7008	a330	s232	42.5701	a393	s274	43.2078	a456
s23	43.1009	a42	s65	28.6002	a125	s107	43.9658	a205	s149	43.1463	a268	s191	42.9348	a331	s233	42.0733	a395	s275	42.4579	a458
s24	42.6987	a44	s66	45.3902	a127	s108	43.8000	a207	s150	43.0789	a270	s192	42.8102	a333	s234	42.3399	a396	s276	42.8118	a459
s25	42.9037	a46	s67	29.7418	a129	s109	44.0025	a208	s151	43.2039	a271	s193	42.9966	a334	s235	42.8122	a398	s277	44.7712	a461
s26	29.9401	a48	s68	43.8564	a131	s110	43.7128	a210	s152	42.5518	a273	s194	43.3309	a336	s236	43.0189	a399	s278	44.9870	a462
s27	43.1463	a50	s69	42.5701	a133	s111	43.9812	a211	s153	42.8735	a274	s195	43.5648	a337	s237	42.8712	a401	s279	50.6007	a464
s28	43.2039	a52	s70	42.3399	a135	s112	45.1014	a213	s154	42.4403	a276	s196	43.1199	a339	s238	43.1009	a402	s280	50.9624	a465
s29	42.8735	a54	s71	43.0189	a137	s113	45.1215	a214	s155	42.7203	a277	s197	43.2080	a340	s239	42.3317	a404	s281	44.0013	a467
s30	42.7203	a56	s72	43.1009	a139	s114	45.0098	a216	s156	29.2787	a279	s198	51.1007	a463	s240	42.6987	a405	s282	44.2597	a468
s31	29.5587	a58	s73	42.6987	a141	s115	45.1216	a217	s157	29.5587	a280	s199	28.9187	S344	s241	42.6668	a407	s283	46.4129	a470
s32	29.9300	a60	s74	42.9037	a143	s116	29.1220	a219	s158	29.7138	a282	s200	29.8971	a345	s242	42.9037	a408	s284	46.5703	a471
s33	43.0278	a62	s75	29.9401	a145	s117	29.6987	a220	s159	29.9300	a283	s201	43.0142	a347	s243	29.6129	a410	s285	43.9910	a473
s34	42.9287	a64	s76	43.1463	a147	s118	29.3346	a222	s160	42.8907	a285	s202	43.1574	a348	s244	29.9401	a411	s286	44.1890	a474
s35	44.0213	a66	s77	43.2039	a149	s119	29.6988	a223	s161	43.0278	a286	s203	43.2581	a350	s245	42.9100	a413	s287	42.7008	a476
s36	47.4298	a68	s78	42.8735	a151	s120	43.0720	a225	s162	42.7207	a288	s204	43.9658	a351	s246	43.1463	a414	s288	42.9348	a477
s37	47.8952	a70	s79	42.7203	a153	s121	43.2687	a226	s163	42.9287	a289	s205	43.8000	a353	s247	43.0789	a416	s289	42.8102	a479
s38	43.5102	a72	s80	29.5587	a155	s122	43.9661	a228	s164	43.7782	a291	s206	44.0025	a354	s248	43.2039	a417	s290	42.9966	a480
s39	29.5071	a74	s81	29.9300	a157	s123	44.2888	a229	s165	44.0213	a292	s207	43.7128	a356	s249	42.5518	a419	s291	43.3309	a482
s40	29.6631	a76	s82	43.0278	a159	s124	44.1045	a231	s166	47.1144	a294	s208	43.9812	a357	s250	42.8735	a420	s292	43.5648	a483
s41	43.2078	a78	s83	42.9287	a161	s125	44.2678	a232	s167	47.4298	a295	s209	45.1014	a359	s251	42.4403	a422	s293	43.1199	a485
s42	42.8118	a80	s84	44.0213	a163	s126	28.2789	a234	s168	47.7701	a297	s210	45.1215	a360	s252	42.7203	a423	s294	43.2080	a486

cause a single contingency in the developed cyber-physical model. To achieve this aim, 25% of the total loads are defined as accessible EV loads for adversaries that can be manipulated in each load bus. First, the number of manipulated charging stations is reported using the OCPP logs on the client side of charging stations. Then, the DSO conducted a power flow analysis to extract the voltage deviation for each bus and the excessive active power loss, calculating the related items of the reward function. Based on the attacker's success rate and obtained reward functions, we can generate the MDP tree for a single contingency and resolve it to quantify the security status of the IEEE 69-bus distribution network in the presence of dynamic sections based on close situations of five tie-switches. Considering four well-known vulnerabilities in the EV ecosystem, an MDP tree with 294 states and 486 actions can be obtained for targeting EV loads in single buses during dynamic changes in the distribution network, as shown in Fig. 5.21. The generated MDP tree is resolved using the modified policy iteration algorithm with the assumption of γ=0.95, and the results

Table 5.10: Security Metric Evaluation for Dynamic 69-bus Distribution Network (Three Loops)

State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*	State	V^*	π^*
s1	43.1317	a196	s43	42.9986	a82	s85	45.3334	a165	s127	27.3361	a235	s169	45.7782	a298	s211	43.0204	a362	s253	27.9846	a425
s2	42.4087	a2	s44	48.7099	a84	s86	45.7782	a167	s128	43.0864	a237	s170	41.2502	a300	s212	43.1272	a363	s254	28.2522	a426
s3	48.8985	a83	s45	42.3034	a86	s87	41.5870	a169	s129	43.3840	a238	s171	41.5870	a301	s213	27.8348	a365	s255	28.4005	a428
s4	28.0690	a4	s46	44.5119	a88	s88	28.2029	a171	s130	28.1414	a240	s172	28.1110	a303	s214	28.3860	a366	s256	28.6071	a429
s5	41.2498	a6	s47	42.2358	a90	s89	28.3520	a173	s131	28.4272	a241	s173	28.2029	a304	s215	28.0380	a368	s257	40.9949	a431
s6	42.0225	a8	s48	41.0371	a92	s90	41.2980	a175	s132	41.4233	a243	s174	27.9362	a306	s216	28.3861	a369	s258	41.1260	a432
s7	42.0576	a10	s49	41.0962	a94	s91	40.9195	a177	s133	41.9179	a244	s175	28.3520	a307	s217	41.1682	a371	s259	40.8324	a434
s8	42.0372	a12	s50	41.6392	a96	s92	42.9986	a179	s134	40.5653	a246	s176	41.1089	a309	s218	41.3562	a372	s260	41.0313	a435
s9	43.1271	a14	s51	41.2982	a98	s93	48.7099	a181	s135	40.6885	a247	s177	41.2980	a310	s219	42.0228	a374	s261	41.8432	a437
s10	43.1272	a16	s52	48.8985	a180	s94	42.3034	a183	s136	40.2137	a249	s178	40.5813	a312	s220	42.3312	a375	s262	42.0756	a438
s11	28.3860	a18	s53	28.5756	a101	s95	44.5119	a185	s137	40.4685	a250	s179	40.9195	a313	s221	42.1551	a377	s263	45.0319	a440
s12	28.3861	a20	s54	41.2498	a103	s96	42.2358	a187	s138	40.9199	a252	s180	42.7923	a315	s222	42.3112	a378	s264	45.3334	a441
s13	41.3562	a22	s55	42.0225	a105	s97	41.0371	a189	s139	41.1175	a253	s181	42.9986	a316	s223	27.0290	a380	s265	45.6587	a443
s14	42.3312	a24	s56	42.0576	a107	s98	41.0962	a191	s140	40.9763	a255	s182	48.3641	a318	s224	27.3361	a381	s266	45.7782	a444
s15	42.3112	a26	s57	42.0372	a109	s99	41.6392	a193	s141	41.1958	a256	s183	48.7099	a319	s225	43.0864	a383	s267	41.2502	a446
s16	27.3361	a28	s58	43.1271	a111	s100	41.2982	a195	s142	40.4606	a258	s184	42.0564	a321	s226	43.3840	a384	s268	41.5870	a447
s17	43.3840	a30	s59	43.1272	a113	s101	48.9837	a317	s143	40.8114	a259	s185	42.3034	a322	s227	28.1414	a386	s269	28.1110	a449
s18	28.4272	a32	s60	28.3860	a115	s102	27.6405	a198	s144	40.7809	a261	s186	44.3614	a324	s228	28.4272	a387	s270	28.2029	a450
s19	41.9179	a34	s61	28.3861	a117	s103	28.5756	a199	s145	41.0074	a262	s187	44.5119	a325	s229	41.4233	a389	s271	27.9362	a452
s20	40.6885	a36	s62	41.3562	a119	s104	41.1130	a201	s146	28.3040	a264	s188	42.0466	a327	s230	41.9179	a390	s272	28.3520	a453
s21	40.4685	a38	s63	42.3312	a121	s105	41.2498	a202	s147	28.6167	a265	s189	42.2358	a328	s231	40.5653	a392	s273	41.1089	a455
s22	41.1175	a40	s64	42.3112	a123	s106	41.3461	a204	s148	41.0134	a267	s190	40.8134	a330	s232	40.6885	a393	s274	41.2980	a456
s23	41.1958	a42	s65	27.3361	a125	s107	42.0225	a205	s149	41.2392	a268	s191	41.0371	a331	s233	40.2137	a395	s275	40.5813	a458
s24	40.8114	a44	s66	43.3840	a127	s108	41.8640	a207	s150	41.1748	a270	s192	40.9180	a333	s234	40.4685	a396	s276	40.9195	a459
s25	41.0074	a46	s67	28.4272	a129	s109	42.0576	a208	s151	41.2943	a271	s193	41.0962	a334	s235	40.9199	a398	s277	42.7923	a461
s26	28.6167	a48	s68	41.9179	a131	s110	41.7807	a210	s152	40.6710	a273	s194	41.4157	a336	s236	41.1175	a399	s278	42.9986	a462
s27	41.2392	a50	s69	40.6885	a133	s111	42.0372	a211	s153	40.9785	a274	s195	41.6392	a337	s237	40.9763	a401	s279	48.3641	a464
s28	41.2943	a52	s70	40.4685	a135	s112	43.1079	a213	s154	40.5644	a276	s196	41.2140	a339	s238	41.1958	a402	s280	48.7099	a465
s29	40.9785	a54	s71	41.1175	a137	s113	43.1271	a214	s155	40.8321	a277	s197	41.2982	a340	s239	40.4606	a404	s281	42.0564	a467
s30	40.8321	a56	s72	41.1958	a139	s114	43.0204	a216	s156	27.9846	a279	s198	48.8420	a463	s240	40.8114	a405	s282	42.3034	a468
s31	28.2522	a58	s73	40.8114	a141	s115	43.1272	a217	s157	28.2522	a280	s199	27.6405	S344	s241	40.7809	a407	s283	44.3614	a470
s32	28.6071	a60	s74	41.0074	a143	s116	27.8348	a219	s158	28.4005	a282	s200	28.5756	a345	s242	41.0074	a408	s284	44.5119	a471
s33	41.1260	a62	s75	28.6167	a145	s117	28.3860	a220	s159	28.6071	a283	s201	41.1130	a347	s243	28.3040	a410	s285	42.0466	a473
s34	41.0313	a64	s76	41.2392	a147	s118	28.0380	a222	s160	40.9949	a285	s202	41.2498	a348	s244	28.6167	a411	s286	42.2358	a474
s35	42.0756	a66	s77	41.2943	a149	s119	28.3861	a223	s161	41.1260	a286	s203	41.3461	a350	s245	41.0134	a413	s287	40.8134	a476
s36	45.3334	a68	s78	40.9785	a151	s120	41.1682	a225	s162	40.8324	a288	s204	42.0225	a351	s246	41.2392	a414	s288	41.0371	a477
s37	45.7782	a70	s79	40.8321	a153	s121	41.3562	a226	s163	41.0313	a289	s205	41.8640	a353	s247	41.1748	a416	s289	40.9180	a479
s38	41.5870	a72	s80	28.2522	a155	s122	42.0228	a228	s164	41.8432	a291	s206	42.0576	a354	s248	41.2943	a417	s290	41.0962	a480
s39	28.2029	a74	s81	28.6071	a157	s123	42.3312	a229	s165	42.0756	a292	s207	41.7807	a356	s249	40.6710	a419	s291	41.4157	a482
s40	28.3520	a76	s82	41.1260	a159	s124	42.1551	a231	s166	45.0319	a294	s208	42.0372	a357	s250	40.9785	a420	s292	41.6392	a483
s41	41.2980	a78	s83	41.0313	a161	s125	42.3112	a232	s167	45.3334	a295	s209	43.1079	a359	s251	40.5644	a422	s293	41.2140	a485
s42	40.9195	a80	s84	42.0756	a163	s126	27.0290	a234	s168	45.6587	a297	s210	43.1271	a360	s252	40.8321	a423	s294	41.2982	a486

obtained for each state's value and optimal adversarial action are summarized in Table 5.9. Based on this table, the value of the first state, i.e., s_1, can be defined as 45.1263, and the best adversarial action is a_{196}. It means that if adversaries take action a_{196}, they can compromise the CSMS of the EV ecosystem and move toward a new state s_{101}. The value of this state is 51.2489, and the next effective adversarial action that can be taken to cause a severe impact on the operation of the power grid will be a_{317}. With this action, adversaries could compromise the firmware repository of the EV ecosystem in Bus 61 of the IEEE 69-bus distribution network and access to state s_{182} even if the topology of the distribution network changes due to the operation of tie-switches. In this state, the best action is a_{318}, which means targeting charging stations in this load bus, manipulating their EV loads, and moving to the final state, i.e., s_{183}. Finally, they can stay in the state s_{183} and repeat their action to have the most severe impact. As another example, the situation of the mentioned tie-switches changes where two of them are open between buses (11, 43) and (50, 59), and the three

Algorithm 8: MDP for Network with Dynamic Sections

Identify: Number of tie-switches in distribution network (N_{sw})
Determine: Number of load buses in distribution network (N_L)
Calculate: Combination of different contingencies ($2^{N_L}-1$)
Initialize: Number of attackers' access points in ecosystem (n_v)
for $0:1:2^{N_{sw}}$ **do**
  Assume: 0 : when all tie-switches are open
  Assume: $2^{N_{sw}}$: when all tie-switches are close
  Create: Initial state (ϕ) in MDP tree
  for $i=1:1:n_v$ **do**
    for $z=1:1:2^{N_L}-1$ **do**
      if *(i is an attacker's access point)* **then**
        Build a new reachable state s_i
        for *j as a compromised component* **do**
          if *(i is not connected to j)* **then**
            Continue Serach for new connection
          end
          if *(i and j connected)* **then**
            Build new state s_j Define a transition between s_i and s_j
            Determine $P_a(s_i, s_j)$ using CVSS
            Calculate $RF_a(s_i, s_j)$ using (16)
            Continue for new connection with s_r Build new state and transition among them
          end
        end
      end
    end
  end
end

remaining tie-switches are close, as illustrated in Fig. 5.22. For these dynamic changes in the IEEE 69-bus with three loops ({Loop 1, Loop 2, Loop 3}), the related MDP tree can also be generated and resolved, and the obtained results can be summarized, as shown in Table 5.10. This process can be repeated for different combinations of open or close tie-switches (i.e., $2^{N_{sw}}$) to produce various dynamic sections of a distribution network and investigate all probable situations for generating their related MDP trees. To achieve this aim, Algorithm 8 has been provided to show how state values can be calculated for a wide range of MDP trees when dynamic sections exist in the topology of distribution networks.

In the final stage, we have trained the CNN model for numerous MDP trees that have been resolved for the IEEE 69-bus network, taking into account the dynamic sections created by changes in the distribution network's topology. In other words, we can generate MDP trees and identify all

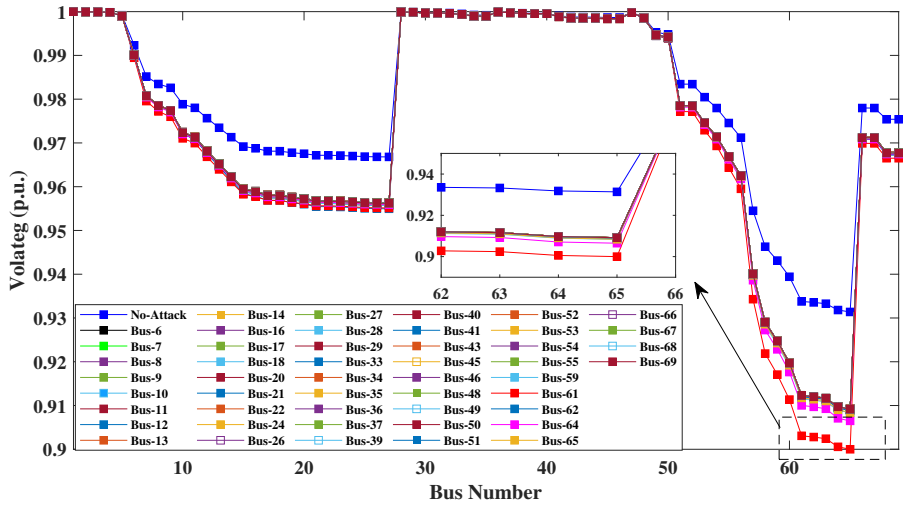


Figure 5.23: Voltage deviation at different buses of IEEE-69 bus distribution network with dynamic sections.

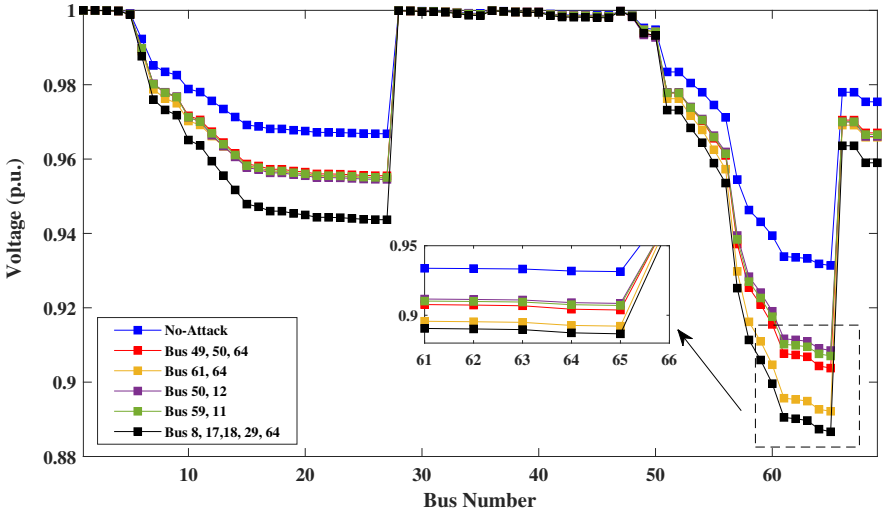


Figure 5.24: Voltage deviation at different buses of IEEE 69-bus distribution network with dynamic sections.

labels to classify the system's security status into secure and alarm situations based on Table 5.1. To clarify, the voltage deviation at buses in the IEEE 69-bus system when all tie-switches are closed and the EV ecosystem is under cyber attacks on EV loads for single buses has been illustrated in Fig. 5.23. This figure provides a comparison between under-attack load buses and the normal operation of the distribution network. Manipulating EV loads in several single-load buses, e.g., Bus 61, Bus 64, Bus 49, and Bus 50, leads to an unacceptable voltage deviation from its nominal value of more than a 2.5% at the nominated Bus 65. Using three conditions in Table 5.1, we

can define the mentioned situations as alarm labels, while other single buses are labeled as secure situations. Furthermore, the voltage deviation after manipulating several load buses at the same time (i.e., multiple contingencies) in the proposed network has been illustrated in Fig. 5.24. Since manipulating EV loads in several combinations, e.g., Bus {49, 50, 46}, Bus {61, 64}, Bus {50, 12}, Bus {59, 11}, Bus {8, 7, 18, 29, 64}, can lead to a voltage deviation of more than 2.5%[92], these situations can also be labeled as alarms in the IEEE 69-bus distribution network. For example, without manipulating EV loads, the nominal voltage of the nominated Bus 65 is 0.9315 p.u. When adversaries manipulate the EV loads of buses in both Bus 61 and Bus 64, this voltage decreases to 0.8920 p.u., leading to a deviation of 4.24%. For training this CNN model in an offline manner, the training, validation, and testing data sets are partitioned by 80%, 10%, and 10% of the total data sets, respectively. The cross-entropy loss and accuracy plots of training and validation data sets have been illustrated in Fig. 5.25 for the IEEE 69-bus distribution network. It can be observed that the cross-entropy loss function decreases gradually in the initial epochs of the validation process, while the binary classification accuracy plot increases during training. This behavior means the CNN model can deliver acceptable performance in providing information about the security status of the power grid for DSOs during EV-cyber attacks. To show the trained CNN model's performance during classification, evaluation metrics, i.e., accuracy, precision, recall, and F-score, can be calculated as 98.629 %, 97.776 %, 93.120 %, and 95.391 %, respectively.

As a last point, when adversaries manipulate EVCSs in load buses of distribution networks, it can cause different impacts on the voltage profiles and equivalent power losses. For instance, greater voltage deviations can be observed at the ends of the laterals of each section. This is primarily because the current has to travel the entire distance to the substation, passing through numerous lines, impacting the voltage at other buses, and resulting in more line power losses. However, if adversaries compromise the same EV loads in buses connected to the main feeder, changes in voltage and active power loss are minimal. In the IEEE 33-bus and IEEE 69-bus distribution networks, we can see that manipulating charging stations has the most severe impacts on Bus 18 and Bus 65, respectively [103].

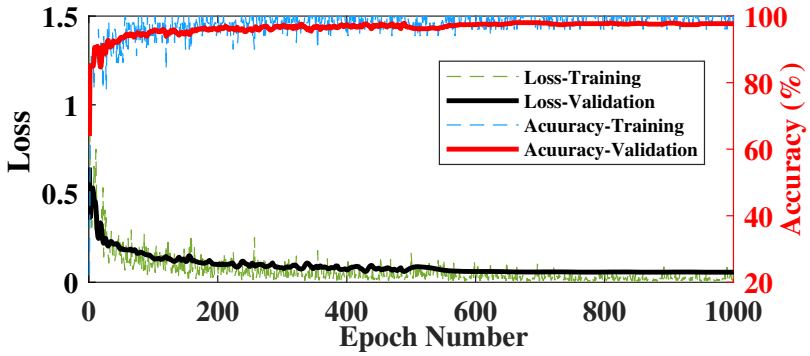


Figure 5.25: Training and validation accuracy and loss for the deep CNN.

5.7 Conclusion

In this chapter, first, cyber vulnerabilities in EV ecosystems that could be maliciously exploited to impact the normal operation of distribution networks were studied, and several attack graphs were generated to analyze compromised components of this ecosystem and related adversarial actions. Then, a security metric was developed based on a Markov decision process (MDP) tree. In this tree, a common vulnerability scoring system and a comprehensive reward function are developed to assign the probabilities of adversaries' success rates and rewards for sabotaging the operation of the distribution network, respectively. Finally, this MDP tree is solved by the modified policy iteration algorithm to calculate the value of each state and related adversarial action. This metric showed the detrimental impacts of EV-based attacks can be exposed in the form of voltage deviations, excessive active power loss, and the unavailability of EVCSs for EV users. Finally, a deep CNN was trained based on a set of different results from the MDP trees to infer the security status of the system, i.e., secure and alarm situations. Since the topology of the distribution network may change due to multiple switching scenarios, a supplementary strategy has also been introduced to calculate our security metric and update the security monitoring system in the looped IEEE 69-bus distribution network. This metric was evaluated under a testbed that integrated the cyber layers of the EV ecosystem in the virtual sphere (vSphere) with a real-time model of distribution networks in OPAL-RT 5650.

Chapter 6

Designing a Security Metric for EV-based Load-altering Attacks in Transmission Systems

6.1 Motivation

Due to their cyber vulnerabilities, the increasing integration of electric vehicles (EVs) and their related electric vehicle supply equipment (EVSE) makes power grids prone to a variety of cyber attacks. Among possible threats, adversaries can observe frequency measurements and alter the consumption of EVs accordingly, creating an EV-based load-altering attack (EV-LAA). On this basis, in this chapter, research uses the measurements of the transmission grid and information on its cyber layer to derive a security metric that can be used for diagnosis and condition monitoring of the transmission grid's security state. First, common vulnerabilities in EV ecosystems are analyzed to devise related attack graphs. Afterward, a Markov decision process (MDP) tree is established based on the obtained attack graphs to display the possible attacker's actions and their detrimental consequences. In this MDP, to calculate the probabilities of adversaries' success in each branch, a customized common vulnerability scoring system (CVSS) is developed. Furthermore, control input and measurement signals are used to identify the transmission systems' model. Using this model,

the damping ratio, controllability, and observability of low-damping modes, as well as the number of compromised charging stations, can be obtained for calculating the terms of a reward function. The generated MDP tree is resolved by the Epsilon-Greedy Q-learning algorithm to calculate the value of each state in the MDP tree and the related optimal adversarial action. This metric is integrated into a back propagation neural network (BPNN) to provide a security monitoring framework for attacks originating from the EV ecosystem. The security monitoring framework is evaluated on a testbed to demonstrate its usefulness in quantifying the security status in the case of EV-LAAs. This testbed consists of a virtual sphere (vSphere) of an EV ecosystem with the New England 39-bus transmission system simulated in a real-time simulator (RTS).

6.2 Contribution

According to our studies in this area, we realized that exiting generic metrics developed for transmission systems do not account for the unique vulnerabilities of cyber layers in the EV ecosystem that can be maliciously exploited to launch EV-LAAs, impacting the frequency stability of transmission systems. On this basis, these metrics cannot be applied to transmission systems integrated with EV ecosystems, and a new security metric must be designed to investigate the impact of compromising EV loads on transmission systems. As a result, this chapter develops a security metric to quantify the security status of the transmission system in the case of EV-LAAs. In this type of attack, attackers measure frequency signals and manipulate EV loads periodically to cause frequency instability. To achieve this aim, first, potential vulnerabilities in EV ecosystems are studied to devise related attack graphs. An MDP tree is established based on the obtained attack graphs to display the possible attacker's actions and their consequences on the stability of power grids. To calculate the probabilities of adversaries' success in branches of the MDP tree, a common vulnerability scoring system (CVSS) is developed. This scoring system is based on real features of vulnerabilities reported in the National Vulnerability Database (NVD) concerning the EV ecosystem. Control input and output measurement signals can be employed to estimate the transmission system's state-space model using the system identification approach. Using this approach, the damping ratio, controllability, and observability of low-damping modes can be extracted. Another framework

is also designed based on OCPP logs of charging stations to report the number of compromised charging stations in each load bus of the power grid. Since EV-LAAs can transfer low damping modes of the system from a stable to an unstable area of the s-plane, this ratio can be defined in the formulation of the reward function. Moreover, launching EV-LAAs from a different load bus using a specific measurement signal, i.e., the rotor speed deviation of synchronous generators, can cause different impacts on power grid stability. As such, the observability and controllability of low-damping modes for different attack vectors and measurement signals are also added as new terms to the reward function. Finally, the generated MDP tree is resolved by the Epsilon-Greedy Q-learning algorithm to calculate the value of each state in the MDP tree and the related optimal adversarial action. The advantage of this algorithm is its effectiveness in balancing exploration and exploitation, making it a broadly used technique in reinforcement learning applications. This security metric can be integrated into a back propagation neural network (BPNN) to provide a security monitoring framework when cyber attacks originating from the EV ecosystem occur. To demonstrate the usefulness of the proposed security metric in quantifying the security status, EV-LAAs are applied to the 39-bus New England transmission system that is implemented in the real-time simulator (RTS). In summary, the main contributions of this paper can be summarized as follows:

(1) Investigating cyber vulnerabilities in EV ecosystems and obtaining attack graphs to analyze the impacts of EV-LAAs on the stability of transmission systems;

(2) Developing a security metric that quantifies the security posture of transmission systems under EV-LAAs using an MDP tree. In this MDP tree, a customized CVSS is deployed to assign probabilities of adversaries' success in launching EV-LAAs. A reward function is also formulated based on the damping ratio of low damping modes, the controllability and observability of these modes for different attack vectors, and measurement signals in the reward function. The number of compromised charging stations in load buses is also considered in this reward function;

(3) Resolving the customized MDP tree using a reinforcement learning method, i.e., the Epsilon-Greedy Q-learning algorithm, to quantify the security status of transmission systems under

EV-LAAs. The proposed EV ecosystem and the transmission system are simulated in the virtual sphere (vSphere) and the real-time simulator (OPAL-RT 5650), respectively, to demonstrate security metric usefulness in quantifying the security status during such attacks.

(4) A BPNN is trained based on the calculated state values of different MDP trees to develop a security monitoring framework and provide information about the security status of transmission systems. The robustness of the monitoring system is evaluated against noisy measurement signals, missing data, and outlier data.

6.3 Transmission System under EV-LAAs

A transmission system with total buses, i.e., $N = N_G \cup N_L$ can be studied, where N_G and N_L are the numbers of generator buses and load buses, respectively. Using linear swing equations, the synchronous generator dynamics at each generator bus ($i \in N_G$) can be modeled as follows[104]:

$$\frac{d\delta_i}{dt} = \dot{\delta}_i = \omega_i \tag{100}$$

$$2H_i^G \frac{d\omega_i}{dt} = 2H_i^G \dot{\omega}_i = P_i^M - D_i^G \omega_i - P_i^G \tag{101}$$

where ω_i, H_i^G, and D_i^G are referred to as the rotor speed deviation of a generator, inertia constant, and damping coefficient, respectively. The P_i^G is power injected by a synchronous generator at bus i that can be calculated using power flow equations:

$$P_i^G = \sum_{j \in N_G} Y_{ij}(\delta_i - \delta_j) + \sum_{j \in N_L} Y_{ij}(\delta_i - \theta_j) \tag{102}$$

where δ_i and δ_j are phase angles at the i-th and j-th generator bus, and θ_j-th is referred to as the phase angle of the j load bus. Y_{ij} is the transmission line's admittance between buses i and j. Furthermore, P_i^M is the mechanical power of the synchronous generator at bus i that can be calculated as follows:

$$P_i^M = -K_i^P \omega_i - K_i^I \int \omega_i dt \tag{103}$$

In transmission systems, uncontrollable and controllable but frequency-insensitive loads can be shown by P_i^L. Moreover, controllable and frequency-sensitive loads can be expressed using the $-D_i^L \dot{\theta}_i$. On this basis, for each load bus ($i \in N_L$), load flow equations can be summarized as

follows [105]:

$$-D_i^L\dot{\theta}_i - P_i^L = \sum_{j\in N_G} Y_{ij}(\theta_i - \delta_j) + \sum_{j\in N_L} Y_{ij}(\theta_i - \theta_j) \tag{104}$$

Finally, the state-space model of the system is defined by the combination of (100)-(104):

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ \Delta\omega_G = Cx(t) \end{cases} \tag{105}$$

where $x(t) = [\ \delta \quad \theta \quad \omega\ ]^T$ is the state variable of the power grid, and $u(t) = P^L$ is an input vector that consists of power consumption of all load buses. Matrix A and B can be defined as follows:

$$\begin{aligned} A = &\begin{bmatrix} I & 0 & 0 \\ 0 & (D^L)^{-1} & 0 \\ 0 & 0 & -(M^G)^{-1} \end{bmatrix} \\ &\times \begin{bmatrix} 0 & 0 & I \\ Y^{LG} & Y^{LL} & 0 \\ K^I + Y^{GG} & Y^{GL} & K^P + D^G \end{bmatrix}, B = \begin{bmatrix} 0 \\ (D^L)^{-1} \\ 0 \end{bmatrix} \end{aligned} \tag{106}$$

where D^L,M^G,K^I, and K^P are diagonal matrices with proper dimensions. Y^{LG}, Y^{LL}, Y^{GG}, and Y^{GL} are components of imaginary part of the admittance matrix:

$$Y_{bus} = \begin{bmatrix} Y^{GG} & Y^{GL} \\ Y^{LG} & Y^{LL} \end{bmatrix} \tag{107}$$

Generally, $u(t) = P^L$ can be divided into two parts: (i) EV loads that can be manipulated by adversaries (P_i^{EV}) and (ii) secure part of loads or other normal loads (P_i^S) for a load bus:

$$P_i^L = P_i^{EV} + P_i^S, i \in N_L \tag{108}$$

In EV-LAAs, it is supposed that adversaries can have access to measurement signals at the generator bus ($i \in N_G$), i.e., rotor speed deviation of generators, and launch an attack vector at some nominated load buses ($i \in N_L$) of the transmission system as follows:

$$\Delta P_i^{atck} = \sum_{j\in N_G} -K_{ij}^{atck}\Delta\omega_j \tag{109}$$

where K_{ij}^{atck} is the coefficient of EV-LAAs, where adversaries measure the frequency deviation of the generator ($\Delta\omega_j$) at bus j and compromise EV loads at nominated load bus i. When the attack

vector ΔP_i^{atck} is applied to transmission systems, it can cause the transfer of low-damping modes of the system from stable to unstable area of the s-plane, leading to frequency instability [7, 106, 14].

6.4 MDP Tree Components for EV-LAAs

To establish an MDP tree to quantify the security posture of transmission systems under EV-LAAs, potential vulnerabilities in EV ecosystems, discussed in Section 2.2, are defined as states of the MDP tree, and attackers' actions are considered as branches of this tree. The main aim of the MDP tree is to show how adversaries can penetrate the cyber and physical layers of EV ecosystems and disrupt the operation of power grids by taking several consecutive adversarial actions and compromising charging stations. The MDP tree provides a mathematical framework to model cyber attack paths, where decisions are partly randomized based on different potential attack vectors in EV ecosystems and partly under the control and policy of attackers. Generally, an MDP tree includes a set of components, i.e., $\{\mathcal{S}, \mathcal{A}, RF_a(s, s'), P_a(s, s'), \gamma\}$, that can be described as follows:

6.4.1 Set of States

A set of states in the MDP tree, that is shown by $\mathcal{S}$, are physical or cyber components that can be targeted by attackers to launch EV-LAAs with the aim of instability in transmission systems. For example, the CSMS can be defined as an important state in the MDP tree, where adversaries can start manipulating the cyber layers of the EV ecosystem and impact the operation of power grids. Also, charging stations, which are compromised in a specific load bus of the transmission system, are defined as final states in the MDP tree. These states can be linked together by meaningful branches that can show attack propagation in the cyber-physical model and privileges obtained through performing adversarial actions.

6.4.2 Set of Adversarial Actions

Adversaries may choose from a set of adversarial actions, which can be denoted as $\mathcal{A}$. Exploring known or zero-day vulnerabilities in cyber-physical models can be defined as adversarial actions. Some techniques, e.g., MitM attacks or SQL injections, can be employed by intruders to gain access

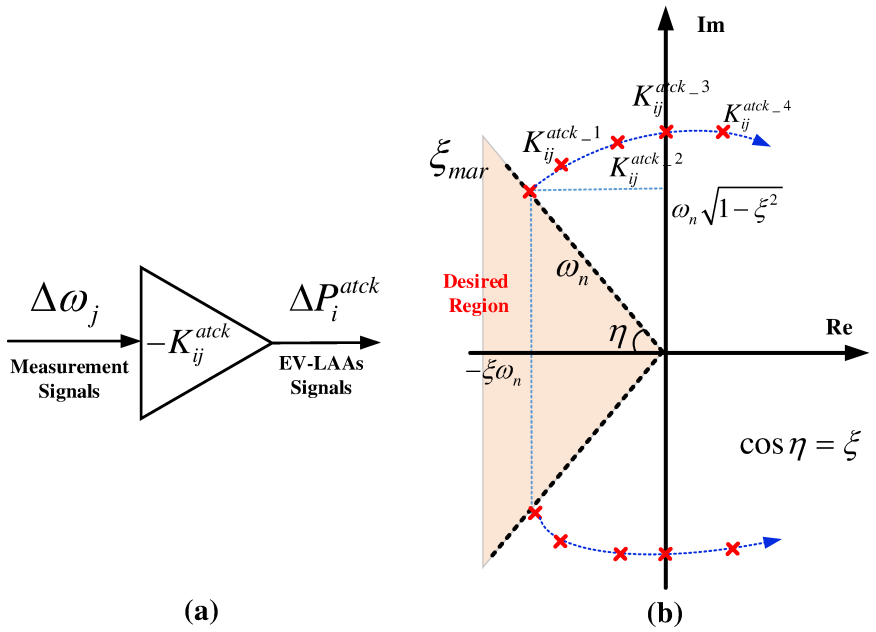


Figure 6.1: (a) EV-LAAs as attack vector implemented to transmission systems from load buses, (b) Impacts of EV-LAAs on the damping ratio of low-damping modes in the s-plane

to more states of the developed MDP tree and launch EV-LAAs with more destructive impacts on the frequency stability of transmission systems.

6.4.3 Reward Function

A reward function, i.e., $RF_a(s, s')$, in the developed MDP tree is given to the attackers following an adversarial action, i.e., $a \in \mathcal{A}$, that takes it from s to s'. This reward function consists of stability and cyber-related terms that can be calculated using system identification approaches, as follows:

Stability-related Terms

As mentioned in prior works[7, 106] and based on (109), compromised EV loads can be considered to be an attack vector that is implemented into load buses of the transmission systems, as shown in Fig. 6.1. (a). The coefficient of this attack vector, i.e., K_{ij}^{atck}, that is proportional to the number of compromised EV loads, can relocate low-damping modes of the transmission system to the unstable area of the s-plane, as shown in Fig. 6.1. (b). This relocation of low-damping modes of the system can lead to oscillations in the rotor speed of synchronous generators. It can be seen

that for a set of consecutive coefficients, i.e., $\{K_{ij}^{atck\_1}, K_{ij}^{atck\_2}, K_{ij}^{atck\_3}, ...\}$, the location of low-damping modes moves from the left side to the right side of the s-plane, leading to changes in the damping ratio (ξ) of the low-damping modes. The ξ_{mar} is a margin value for the damping ratio of the power grid's modes that can be defined based on standards or TSO's opinion [107].

Calculating Damping Ratio: System identification is a measurement-based approach to estimating the state-space model of dynamic systems from control input and output measurement signals. The goal is to determine the parameters of a mathematical model that describes the power grid's behaviour. To achieve this aim, first, input data and output data for $t = 1, 2, ..., N_s$ samples can be collected for $\Delta\omega_G(t)$ and $u(t)$ at each time step t. To represent the state-space model of the system, the auto-regressive with exogenous inputs (ARX) strategy is used as follows [108]:

$$\begin{aligned} &\Delta\omega_G(t) + a_1\Delta\omega_G(t-1) + ... + a_h\Delta\omega_G(t-h) = \\ &b_1u(t-1) + ... + b_lu(t-l) + e(t) \end{aligned} \tag{110}$$

where a_1,...,a_h and b_1,...,b_l are model parameters and $e(t)$ is the error function. For multiple time steps, the regression problem can be defined as follows:

$$\Delta\omega'_G = \Phi\phi + E \tag{111}$$

where $\Delta\omega'_G$ is the actual output measurements for t from $h+1$ until N_s:

$$\Delta\omega'_G = \begin{bmatrix} \Delta\omega_G(h+1) & .... & \Delta\omega_G(N_s) \end{bmatrix}^T \tag{112}$$

Also, the Φ matrix, which includes previous output and input values, can be used to form the regression problem, as follows:

$$\begin{bmatrix} -\Delta\omega_G(2) & -\Delta\omega_G(1) & u(2) & u(1) \\ \vdots & \vdots & \vdots & \vdots \\ -\Delta\omega_G(h) & -\Delta\omega_G(h-1) & u(l) & u(l-1) \\ \vdots & \vdots & \vdots & \vdots \\ -\Delta\omega_G(N_s-1) & -\Delta\omega_G(N_s-2) & u(N_s-1) & u(N_s-2) \end{bmatrix} \tag{113}$$

The ϕ is the vector of parameters that must be be estimated:

$$\phi = [\ a_1 \quad ... \quad a_h \quad b_1 \quad ... \quad b_l\ ]^T \tag{114}$$

The E matrix also represents the difference between the actual measurements and the system identification's predictions. The main aim of this method is to minimize the sum of squared residuals:

$$J(\phi) = E^T E = (\Delta\omega'_G - \Phi\phi)^2 \tag{115}$$

To calculate ϕ, we can minimize $J(\phi)$ by setting the gradient for ϕ to zero:

$$\frac{\partial J(\phi)}{\partial \phi} = -2\Phi^T(\Delta\omega'_G - \Phi\phi) = 0 \rightarrow \Phi^T\Phi\phi = \Phi^T\Delta\omega'_G \tag{116}$$

Finally, we will obtain a solution for calculating the parameters of the system:

$$\phi = (\Phi^T\Phi)^{-1}\Phi^T\Delta\omega'_G \tag{117}$$

In the following, the state-space model of the power grid, i.e., matrices A, B, C, and D, can be calculated using canonical forms[108]. The modes of the system using the estimated state matrix, i.e., A, can be calculated as follows:

$$\det(\lambda I - A) = \sigma \pm j(2\pi f) \tag{118}$$

Finally, the damping ratio for the system's mode in the form of $\sigma \pm j(2\pi f)$ is calculated accordingly:

$$\xi = \cos\eta = \frac{-\sigma}{\sqrt{\sigma^2 + (2\pi f)^2}} \tag{119}$$

where σ and $2\pi f$ are the real and imaginary parts of the system's mode, respectively.

Calculating Controllability and Observability: Launching EV-LAAs from some load and generator buses in the transmission systems compared to other buses might have different impacts on the frequency excursion. As a result, adversaries might be more motivated to launch this attack from specific load or generator buses of power grids [109]. From this perspective, controllability and observability concepts are introduced to examine which input and output signals have a greater

influence on low-damping modes of transmission systems. The controllability of a low-damping mode, i.e., m, in the transmission system for a specific input signal (i.e., EV-LAA vector) at bus $p \in N_L$ can be calculated using a geometric approach as follows [110]:

$$Ctrb_m(p) = \frac{\left|b_p^T \Psi_m\right|}{\|\Psi_m\| \left\|b_p^T\right\|}, \quad p \in N_L \tag{120}$$

where b_p is the p-th column of the estimated matrix B using the proposed system identification and Ψ_m is the left eigenvector of the proposed low-damping mode of the transmission system. Also, superscript T, $|.|$, and $\|.\|$ are referred to as the transpose operator, the modulus, and Euclidean norms of a matrix, respectively. The observability of the low-damping mode, i.e., m, for a specific output measurement signal (i.e., rotor speed deviation of synchronous generators) at generator bus $q \in N_G$ can be calculated using a geometric approach as follows [110]:

$$Obsv_m(q) = \frac{|c_q \Phi_m|}{\|\Phi_m\| \|c_q\|}, \quad q \in N_G \tag{121}$$

where c_q is the q-th row of the estimated matrix C and Φ_m is the right eigenvector of the proposed low-damping mode of the transmission system. Finally, to show the impact of launching EV-LAAs from different buses on the operation of the transmission system, two coefficients can be defined as follows:

$$\frac{Ctrb_m(p)}{\sum\limits_{k \in N_L} Ctrb_m(k)}, \quad \frac{Obsv_m(q)}{\sum\limits_{k \in N_G} Obsv_m(k)} \tag{122}$$

The first term represents the ratio of the controllability of a low-damping mode, m, for a load bus, where an attack vector is implemented, to the summation of all load buses' controllability ($k \in N_L$). The second term indicates the ratio of the observability of a low-damping mode, m, for a nominated generator bus to the summation of all generator buses' observability ($k \in N_G$). It is important to say that the mentioned terms can be calculated based on system identification approaches carried out in the TSO control center using control input and measurement output signals[10, 11].

Formulation of Reward Function: In summary, to consider the concerns of the TSO about the stability and security issues of transmission systems, a reward function for each of the two consecutive states (s,s') after taking adversarial action a in the MDP tree, can be developed as

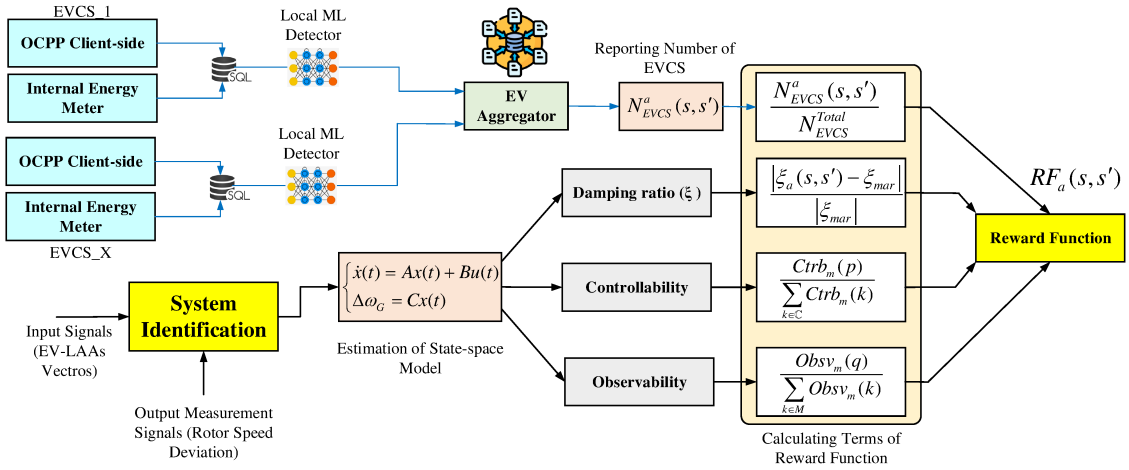


Figure 6.2: Calculation flow diagram for reward function terms in MDP tree.

follows:

$$RF_a(s,s') = \beta_1 \frac{N^a_{EVCS}(s,s')}{N^{Total}_{EVCS}} + \beta_2 \frac{|\xi_a(s,s')-\xi_{mar}|}{|\xi_{mar}|} + \beta_3 \frac{Ctrb_m(p(s,s'))}{\sum_{k\in N_L} Ctrb_m(k)} + \beta_4 \frac{Obsv_m(q(s,s'))}{\sum_{k\in N_G} Obsv_m(k)} \tag{123}$$

where $N^a_{EVCS}(s,s')$ is the number of targeted EVCSs after moving from state s to s' by taking adversarial action a. $\xi_a(s,s')$ is the damping ratio of low-damping mode, m, after implementing EV-LAAs in a specific bus in the transmission system and moving from state s to s'. The controllability and observability of the low-damping mode, i.e., m, after moving from state s to s' by implementing EV-LAAs in a specific bus using a specific generator bus can be calculated and added as third and fourth terms to the reward function for each branch of the MDP tree. The parameters $\beta_1, \beta_2, \beta_3$, and β_4 are coefficients that can be used to weight the four terms of the proposed reward function. A calculation flow diagram to show how the terms of the reward function can be calculated at the substation level of the transmission system has been provided in Fig. 6.2.

6.5 Generating and Solving MDP Tree

6.5.1 Generating States and Branches of MDP Tree

In the MDP tree, an initial state (ϕ) is defined as a state where no components of the EV ecosystem have been compromised by adversaries. To generate an MDP tree, first, one attacker's access point based on the obtained attack graphs is selected as an accessible state. Then, the attacker starts

Algorithm 9: MDP Tree Generator for Transmission System

Determine: Number of load buses in transmission system (N_L)

Initialize: Number of vulnerabilities in EV ecosystem (N_v)

Create: Initial state (ϕ) in MDP tree

for $h = 1:1:N_v$ **do**
  for $z = 1:1:N_L$ **do**
    if *(h is an attacker's access point)* **then**
      Build a new state s_h
      for *r as a compromised component* **do**
        if *(h is not connected to r)* **then**
          Continue Search for new connection
        end
        if *(h and r connected)* **then**
          Build state s_r Define a transition between s_h and s_r
          Calculate $RF_a(s_h, s_r)$ using (123)
          Assign $P_a(s_h, s_r)$ using CVSS
          Continue for new connection with s_r
          Build new state and transition among them Calcualte new $RF_a(s, s')$ and $P_a(s, s')$
          Continue
        end
      end
    end
  end
end

penetrating the physical or cyber layers from the accessible state and taking several adversarial actions to gain control of the charging stations in a specific load bus of the transmission system and launch EV-LAAs to cause frequency instability in the power grid. To generate this tree, Algorithm 9 has been developed to create logical connections between different states of the MDP tree and consider transitions among these states. In this algorithm, the attacker's access point can be defined as an accessible state under s_h. Afterward, a new reachable state (s_r) can be searched in the attack graph spaces where there is a logical connection between component r and compromised component h, and adversaries can move from the previous state s_h to new state s_r. This new state can be added to the tree starting from the attacker's access point by using a new branch. Finally, for the established branch between states s_h and s_r, the reward function $RF_a(s_h, s_r)$ can be calculated using (123), and the success probability of this transition $P_a(s_h, s_r)$ is obtained through the proposed CVSS. For more clarification, a branch of the developed MDP tree is illustrated in Fig. 6.3. As such, it is assumed that a Mobile/web application can be selected as the accessible state (Mb) in the

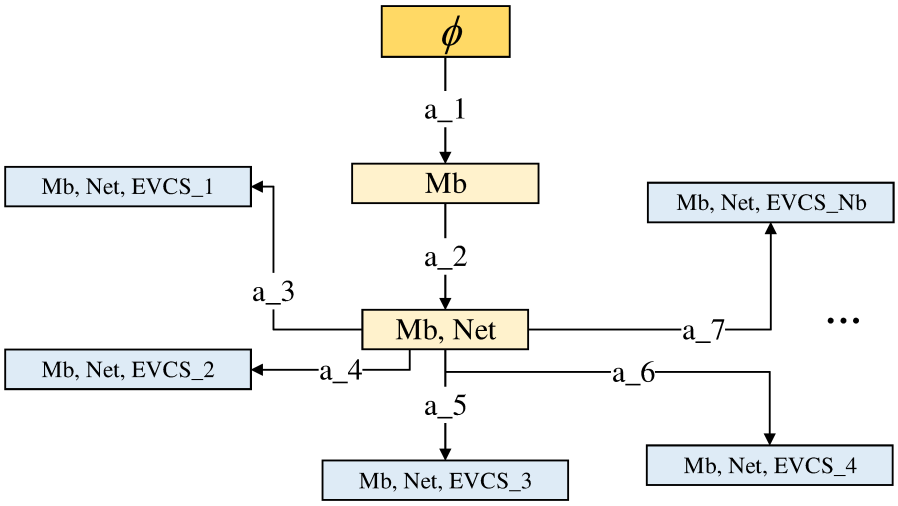


Figure 6.3: A branch of the MDP tree including states and transition among them based on potential vulnerabilities in the EV ecosystem.

MDP tree where adversaries can move from the initial state (ϕ) to this state (Mb). Then, they can target the EVSE and penetrate the network of the EV ecosystem in different buses of transmission systems, producing a new state as (Mb, Net). Finally, intruders can gain control of EV charging stations in the proposed load bus of the transmission system and manipulate EV loads to impact the frequency stability of power grids. Thus, the final state can be obtained for the first load bus under the name of (Mb, Net, EVCS_1) in the MDP tree. This algorithm can be repeated for all load buses in the transmission system, making an MDP tree that considers all probable EV-LAAs originating from different physical or cyber layers of EV ecosystems.

6.5.2 MDP Tree Optimal Response using Q-learning Method

To solve the MDP tree and calculate the values of each state as well as adversarial actions that can cause EV-LAAs and frequency instability of transmission systems, a reinforcement learning technique based on the Epsilon-Greedy Q-learning algorithm is utilized [111]. The application of this algorithm involves building and updating a Q-value function, i.e., $Q(s, a)$, for state-action pairs, optimizing the agent's policy to maximize cumulative rewards over time intervals. Additionally, the Epsilon-Greedy strategy balances exploration and exploitation during adversarial action selection. The algorithm chooses the action with the highest Q-value (exploitation) with probability $1-\epsilon$, while it selects a random action, allowing for exploration with probability ϵ. It is important to mention that ϵ is a small constant representing greedy exploration. The Q-learning update rule, considering

Algorithm 10: Epsilon-Greedy Q-Learning Algorithm for MDP Tree

Parameters: Learning rate: α, Discount factor: γ, Greedy exploration: ϵ

Outputs: A table including optimal state-action values: $V(s)$, a_{opt}

Initialize: Values of $Q(s,a)$ randomly and $Q(terminal,0) \rightarrow 0$

Calculate and Update: Q-value for each step in each episode

for *Each episode* **do**

  Initialize state $s \in \mathcal{S}$ by resetting the environment

  for *each step in episode* **do**

    Choose adversarial action $a \in \mathcal{A}$ using epsilon-greedy policy

    Take adversarial action $a \in \mathcal{A}$ from $s \in \mathcal{S}$

    Observe $P_a(s,s')$

    Observe $RF_a(s,s')$ and $s' \in \mathcal{S}$

    Calculate: $(1-\alpha).Q_{old}(s,a) + ... \quad \alpha(RF_a(s,s') + \sum_{s'} P_a(s,s').\max_{a'} Q(s',a'))$

    Replace: $Q_{new}(s,a)$ with the calculated number

    Update: new state ($s \leftarrow s'$)

    While $s \in \mathcal{S}$ is not terminal state

  end

end

transition probabilities in different branches of the proposed MDP tree, can be expressed as follows:

$$\begin{aligned} &Q_{new}(s,a) \leftarrow (1-\alpha).Q_{old}(s,a) + \\ &\alpha(RF_a(s,s') + \textstyle\sum_{s'} P_a(s,s').\max_{a'} Q(s',a')) \end{aligned} \tag{124}$$

where $Q_{new}(s,a)$ and $Q_{old}(s,a)$ are the current and old versions of the state-action pair, respectively. The term $\max_{a'} Q(s',a')$ is the maximum Q-value among possible actions in the next state s'. Moreover, the term $\sum_{s'} P_a(s,s').\max_{a'} Q(s',a')$ represents the expected future cumulative reward, taking into account the probabilities of transitioning to different next states in the tree. The term α is the learning rate that controls the weight given to the new information. To illustrate how this approach can update the Q-value and calculate the value of each state and optimal adversarial action in each step, Algorithm 10 has been summarized. Based on this algorithm, the agent first takes action in the current state and observes the resulting immediate reward in the next state. Then, it updates the Q-value for the current state-action pair using the update rule, where the transition probabilities influence the computation of the expected future reward.

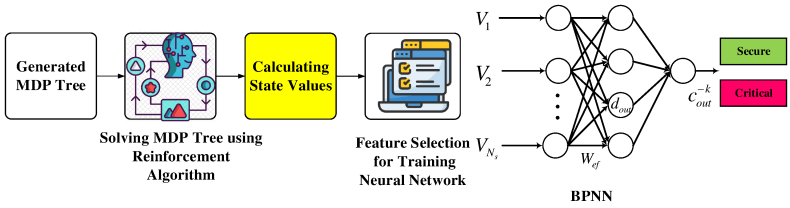


Figure 6.4: Training a back propagation neural network for EV-LAAs using MDP tree

6.6 Security Monitoring Framework

6.6.1 Training a Neural Network for Monitoring

A back propagation neural network (BPNN) can be trained to develop a security monitoring framework based on the calculated state values of different MDP trees. The BPNN provides a powerful tool for binary classification tasks, leveraging its robust learning capabilities to effectively distinguish between security threats and the normal operation of transmission systems. As such, the proposed MDP tree is first generated using Algorithm 1, then resolved by Algorithm 2 for a wide range of EV load penetrations offline. The input data for training this BPNN model is the obtained state values in the MDP tree, i.e., N_{st}, where adversaries targeted different EV load penetration in the range of 0% until 25% with the N_{EV} step. On this basis, all input data can be formalized as $N_{st} \times N_{EV}$. The output data (i.e., target data) is defined as the normal operation of the transmission system and the critical situation when EV-LAAs can cause rotor speed deviation of the synchronous generator to exceed 2.5% of its nominal value and frequency instability in the transmission system. This BPNN consists of an input layer tailored to the values of states, multiple hidden layers to capture the complexity of MDP trees, and a binary output layer that categorizes secure and critical conditions. In this neural network, input data features are passed through multiple layers of neurons. Each neuron computes a weighted sum of its inputs, adds a bias value, and applies an activation function (i.e., softmax). For a neuron in a specific layer, the output can be calculated as follows [112]:

$$c_{out}^{-k} = softmax(d_{out} + \sum_{e} y_e) \tag{125}$$

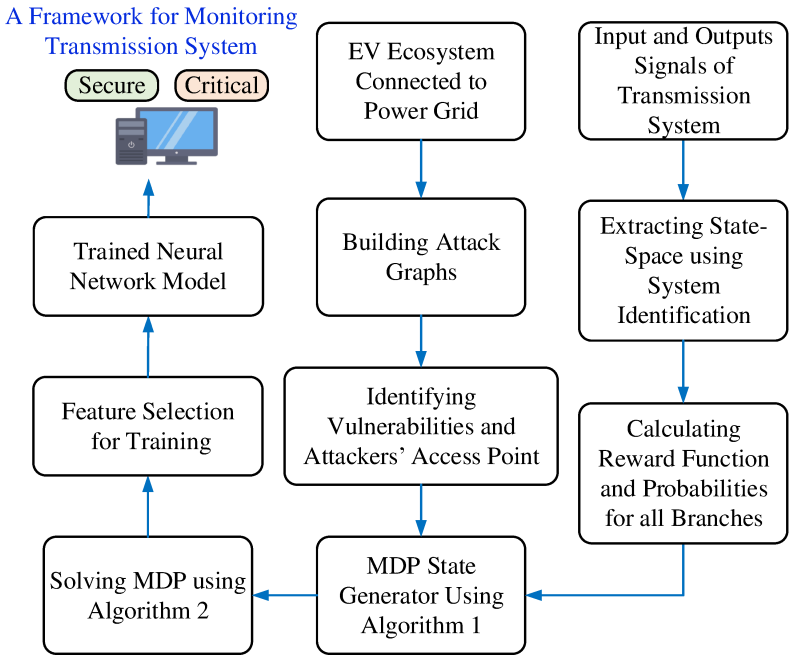


Figure 6.5: A framework for monitoring power grid under EV-LAAs

where d_{out} is the bias of the output node and y_e is the output of the hidden node e, as expressed in the following:

$$y_e = ReLU(d_{in} + \sum_{N_{st}} W_{ef} V_{N_{st}}) \tag{126}$$

where $V_{N_{st}}$ is the input from the set of nodes, i.e., $\{1, 2, ..., N_{st}\}$, under the input layer. The W_{ef} are the weights connecting neurons from two different layers, and d_{in} is the bias of node e in the hidden layer. It is important to mention that c_{out}^{-k} is compared with the known c_{out}^{k}. If these two values do not align, the back propagation algorithm will adjust the values of weighting and bias across the entire training set to achieve the goal of making $c_{out}^{-k} = c_{out}^{k}$, distinguishing between secure and critical scenarios. To show how this metric is calculated and used to train the BPNN and provide information about the security status of transmission systems in the presence of EV-LAAs, a sequential diagram has been illustrated in Fig. 6.4.

6.6.2 Real-time Application of Security Metric

All discussed sections can be integrated to provide a security monitoring framework for transmission systems during attacks originating from the EV ecosystem and guarantee the real-time performance of the proposed security metric. The requirements for data collection to generate the

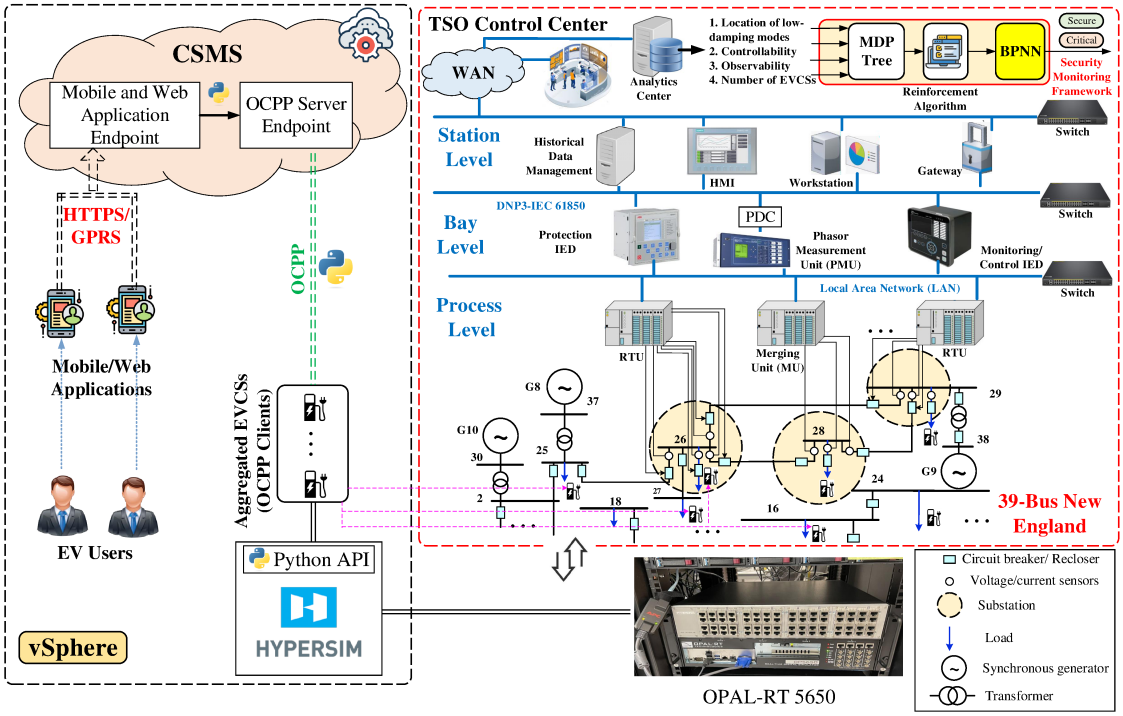


Figure 6.6: Integration of EV ecosystem and transmission system using virtual sphere (vSphere) and real-time simulator (OPAL-RT 5650).

proposed MDP tree can be effectively handled by the state-of-the-art communication infrastructure maintained by DSOs and TSOs through a combination of advanced smart meters (e.g., merging units), robust communication networks (e.g., wide-area networks), IoT devices (e.g., switches), phasor measurement devices (PMUs), and client-side OCPP logs based on web-socket communication [69]. Also, modern smart grids at TSO and DSO levels deploy big data technologies to manage the vast amounts of data collection. These technologies provide efficient storage, processing, and data analysis, facilitating real-time insights and predictive analytics. Our designed security metric has been implemented at the highest level of the supervisory control and data acquisition (SCADA) system of the transmission system implemented in OPAL-RT 5650, where all data is gathered for data analysis and storage. The metric scans different vulnerabilities in the EV ecosystem and generates related states and branches of the MDP tree. Afterward, this MDP tree is resolved using the Epsilon-Greedy Q-learning algorithm to obtain a set of values and optimal adversarial actions. Since the transmission systems in real-time applications are relatively large and complicated, numerous states and actions may be generated within the MDP tree, making interpreting these state values and optimal policies more challenging and time-consuming. Moreover, we require a tool

that helps operators use this metric effectively to detect attacks in real applications. To address this issue, these state values pass through the well-trained BPNN to provide information about the security status of the transmission system. When a new potential vulnerability is identified in one of the components of the EV ecosystem or a change in the power grid topology has been made, this metric can be easily updated at the station level. This framework for monitoring the security status of power grids has been illustrated in Fig. 6.5.

6.7 Simulation Results and Discussion

6.7.1 Co-simulation Platform of EV Ecosystem and Transmission Systems

A general schematic of the cyber and physical layers of the EV ecosystem integrated into a transmission system, i.e., the 39-bus New England system, has been illustrated in Fig. 6.6. This layout consists of the OPAL-RT 5650 as an RTS for simulating components of the transmission system as well as a virtual sphere (vSphere) to show the interaction between different parts of this ecosystem using Python software. The SCADA system of the transmission system based on IEC 61850 with the architecture of the developed security metric has been shown in Fig. 6.6. Based on the proposed standard, three different levels, i.e., process, bay, and station, can be defined to design and implement communication protocols for substation automation systems. At the process level, critical parameters such as voltage, current, and power flow across the network are collected to ensure optimal performance and reliability. All measurement data (i.e., control inputs and output measurement signals) can be collected through merging units (MUs) and remote terminal units (RTUs) and transmitted to the upstream level[97]. At the bay level, protection and monitoring/control intelligent electronics (IEDs) are widely used to facilitate a fast and efficient exchange of status information between bay-level devices for rapid decision-making and response to dynamic operational conditions. Additionally, PMUs can measure real-time electrical signals on transmission lines and monitor voltage, current, frequency, and phase angle using the phasor data concentrator (PDC). According to the IEEE C37.118 standard, the typical sample rates for PMUs range from 1 sample per cycle (e.g., 60 samples per second). However, for our security metric, we need to have one sample per second for both control input and output measurement signals to generate the proposed MDP tree. At the

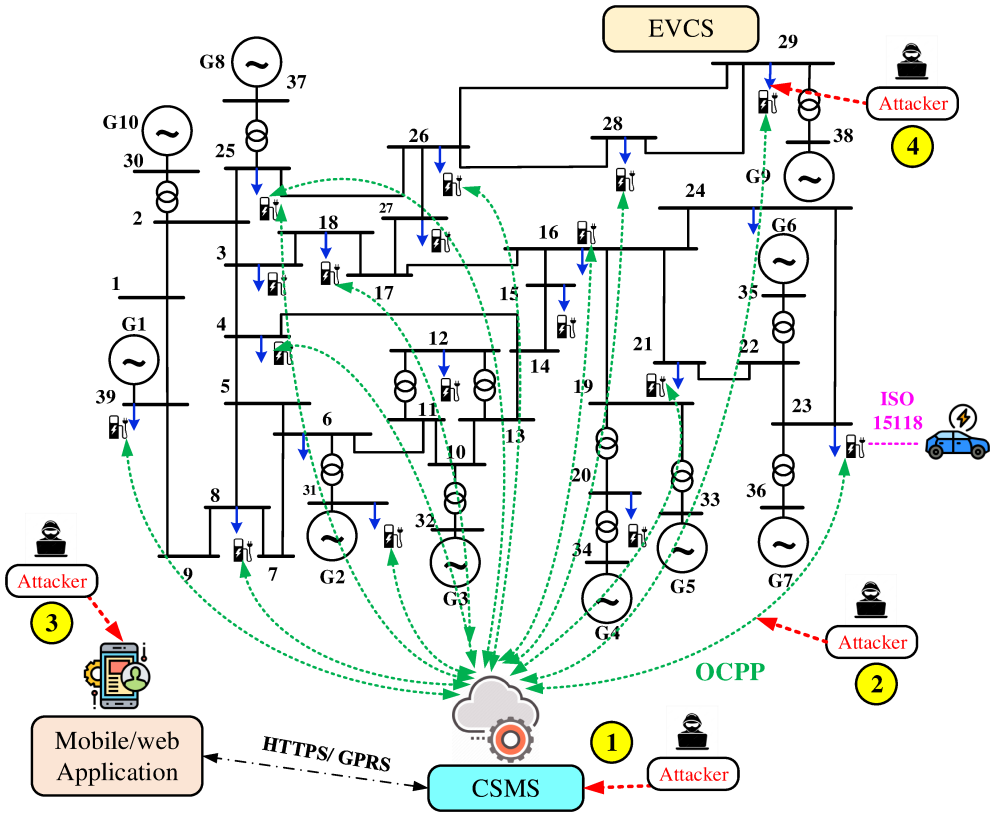


Figure 6.7: 39-bus New England transmission system integrated with an EV ecosystem including cyber or physical vulnerabilities exploited by attackers.

station level, the SCADA system operates as the hub for monitoring and controlling the entire substation. This system aggregates data from multiple bays and substations, providing the TSO control center with a comprehensive view of the network's status and performance. In the control center of the transmission system, where final decisions are made, the analytics center can calculate all related terms of the proposed reward function using system identification approaches and deploy them to make the proposed MDP tree. After resolving the generated MDP tree using the proposed reinforcement algorithm, the numerical values of all states are obtained and passed through the well-trained neural network to provide information about the security status of the transmission systems under EV-LAAs.

A Python application programming interface (API) is also developed in the HYPERSIM environment to allow the virtual machine of charging stations to control aggregated EV loads in different substations of the proposed transmission system in OPAL-RT 5650. The CSMS, which is typically

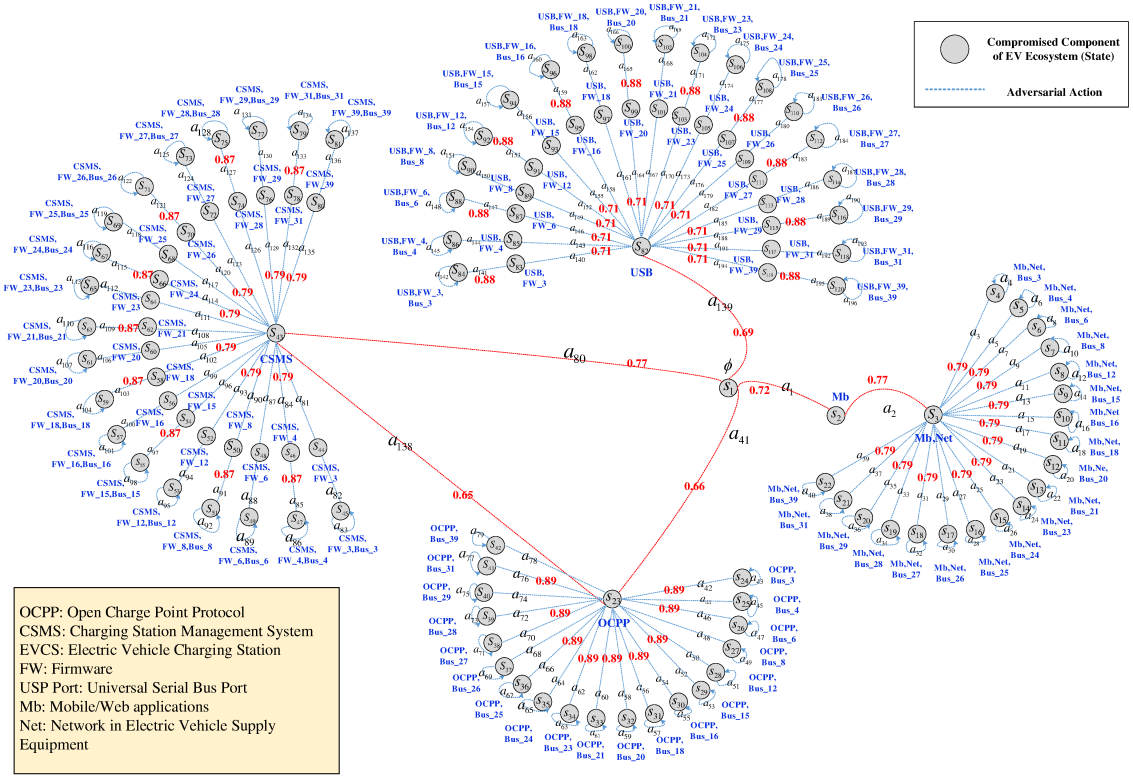


Figure 6.8: MDP tree generated by Algorithm 9 to study the impact of EV-LAAs on 39-bus New England transmission system

hosted on cloud computing platforms, can provide two services for communication between mobile/web applications and EVCSs. The first service is the mobile and web application endpoint for sending and receiving requests from the mobile application. The second service is the OCPP server endpoint, where CSMS translates the actions triggered by the mobile application to the OCPP commands to manage the EVCSs. WebSockets, which enable full-duplex communication over a TCP connection, are generally used by the OCPP. This OCPP endpoint is implemented into the official standard release of Python 3.10 and the fundamental OCPP library. Moreover, the EVCS OCPP client is emulated to connect with the CSMS for all subsequent requests and maintain internal information in a database, e.g., EVCS OCPP logs to display the status of the EVCS and transactions with the CSMS.

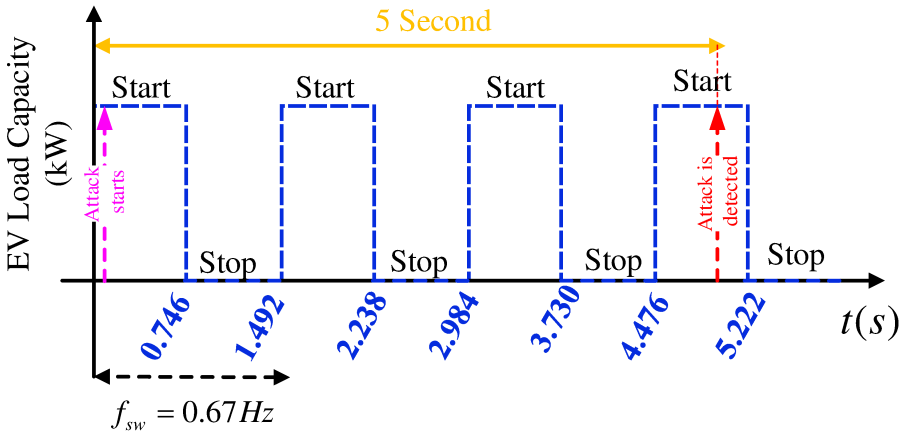


Figure 6.9: Performance of the local LSTM detector during EV-LAAs on a charging station

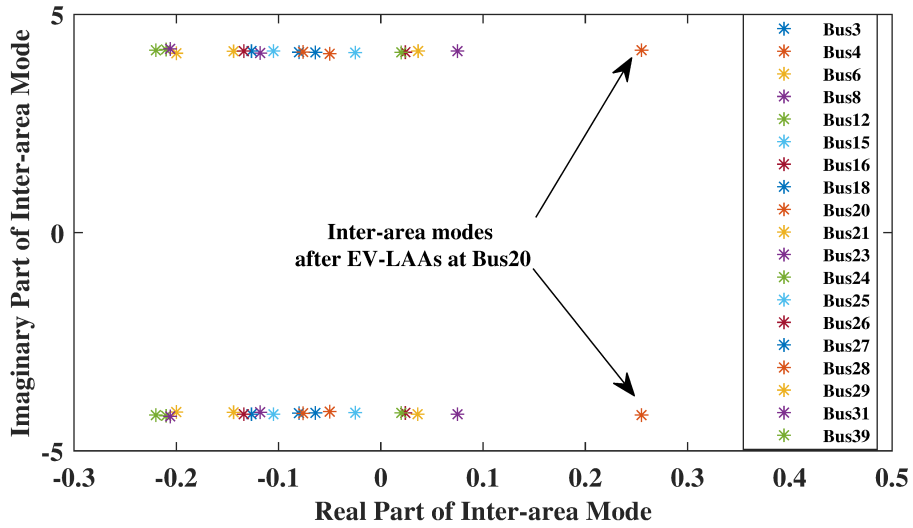


Figure 6.10: Location of low-damping modes after implementing EV-LAAs at different load buses of 39-bus New England system

6.7.2 Generating MDP Tree

In this section, the developed security metric is evaluated for the 39-bus New England transmission system under EV-LAAs originating from EV loads in the EV ecosystem. As illustrated in Fig. 6.7, in this integrated cyber-physical model, CSMS, OCPP, mobile/web applications, and USB ports mounted on charging stations are defined as the attacker's access points. This system includes 39 buses, 10 generator buses, and 19 load buses. Since electric car markets are witnessing exponential growth as sales exceeded 10 million in 2022 and it is projected that this number will rise to 170 $\sim$ 245 million at the end of 2030, we are assuming that 20% of each load bus can be allocated to EV loads [4, 23]. On this basis, half of this value can be compromised by attackers to launch EV-LAAs

using the potential attack vectors discussed in Section 2.2. It is important to mention that this value can be changeable based on the opinion of TSO, and our proposed security metric can quantify the security of power grids under different penetration levels of EV loads in power grids. First, the number of vulnerabilities in EV ecosystems and load buses in the 39-bus New England system is assumed to be 4 and 19 ($n_V = 4$, $N_L = 19$), respectively. Then, Algorithm 9 is deployed to generate the related MDP tree and enumerate accessible states and transitions among states. To assign the probabilities of adversaries' success rates during launching EV-LAAs from the potential attack vectors to the branches of the MDP tree, the CVSS is deployed based on the table shown in Fig. 5.1 (Chapter 5). Also, for each transition between the current and the subsequent state in this tree, the value of the damping ratio, controllability, and observability of low-damping mode (i.e., -0.2 $\pm$ j 4.2) in the proposed power grid are calculated using system identification. Based on Algorithm 9 and considering four well-known vulnerabilities in the EV ecosystem, an MDP tree with 120 states and 196 adversarial actions, as shown in Fig. 6.8, can be generated where adversaries manipulate EV loads in all 19 load buses of the proposed transmission system and launch EV-LAAs. We have provided two next sections to calculate the probabilities and reward function for each branch of the generated MDP tree in detail, as follows:

Calculating Reward Functions: First, the number of EVCS compromised in each load bus is reported using the framework that has already been developed in Fig. 5.4 (Chapter 5). As an example, if adversaries compromise charging stations and issue malicious charging and discharging commands with a specific frequency, e.g., the frequency of the proposed low-damping mode ($f_{mode} = 0.67$ Hz), it can cause EV-LAAs that impact the stability of the power grid. The proposed detector can determine this abnormal pattern in charging and discharging commands, as illustrated in Fig. 6.9. Since this local detector will identify LAAs with different frequencies, e.g., the frequency of low-damping modes, the proper observation window can be assigned in the range of 5 seconds. Finally, each branch's reward function can be calculated using (123). For example, the location of the low-damping mode after compromising 10% of EV loads and implementing EV-LAAs in all 19 load buses of the New England transmission system has been illustrated in Fig. 6.10. It can be observed that compromising EV loads at Bus 20 can have a more severe impact on the location

Table 6.1: Calculating Reward function for Adversarial Actions

From s to s'	**Action**	$RF_a(s,s')$	**From s to s'**	**Action**	$RF_a(s,s')$
s_1 to s_2	a_1	0	s_3 to s_{13}	a_{21}	1.4046
s_2 to s_3	a_2	0	s_3 to s_{14}	a_{23}	1.6009
s_3 to s_4	a_3	0.8089	s_3 to s_{15}	a_{25}	1.3246
s_3 to s_5	a_5	0.9521	s_3 to s_{16}	a_{27}	0.6871
s_3 to s_6	a_7	0.4994	s_3 to s_{17}	a_{29}	0.5574
s_3 to s_7	a_9	0.6271	s_3 to s_{18}	a_{31}	0.8964
s_3 to s_8	a_{11}	0.1777	s_3 to s_{19}	a_{33}	0.8404
s_3 to s_9	a_{13}	1.0921	s_3 to s_{20}	a_{35}	0.2111
s_3 to s_{10}	a_{15}	1.3427	s_3 to s_{21}	a_{37}	0.2088
s_3 to s_{11}	a_{17}	0.5940	s_3 to s_{22}	a_{39}	0.3410
s_3 to s_{12}	a_{19}	2.5333	s_1 to s_{23}	a_{41}	0

of low-damping mode, causing a large value of damping ratio (ξ) compared to other load buses in the system. Moreover, the controllability and observability of the low-damping mode are illustrated in Fig. 6.11 and Fig. 6.12, respectively. It can be concluded that if adversaries manipulate EV loads at load Bus 20 and measure the rotor speed deviation signal at generator Bus 1, respectively, it can cause the highest values of observability and controllability of this low-damping mode compared to when they compromise EV loads in other load and generator buses. For each transition between different states, the amount of the reward function has been calculated with the assumption that $\beta_1 = \beta_2 = \beta_3 = \beta_4 = 1$ in Table. 6.1. We have not defined rewards for branches a_1 and a_2. The main reason is that we have used these actions to achieve the final states of the MDP tree. Since adversaries will stay at final states in the MDP tree, e.g., s_4, s_5, s_6, s_7, and repeat their actions to cause the most severe impact on the stability, the reward function for these actions, e.g., s_4, s_6, s_8, ..., received the same reward. For other vulnerabilities, this reward function can be calculated in the same manner.

Calculating Probabilities: To calculate the success rate of each adversarial action in the proposed MDP tree, a numerical example is provided. For instance, adversaries have decided to compromise the mobile and web applications of the EV ecosystem, moving from the initial state s_1 to the next state s_2. In the following, we will discuss how the items in CVSS can be selected. When adversaries target this vulnerability to launch load-altering attacks, they must have access to the network. As a result, the attack vector is a network. Implementing such an attack is complicated, and attack complexity is defined as high. The level of privileges an attacker must possess when exploiting the vulnerability is defined as high. Moreover, adversaries may contact EV users. On this basis, user

Table 6.2: Calculating Probabilities of Each Branch in MDP Tree using CVSS V 3.1

Action	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$	**Action**	$P_a(s,s')$
a_1	0.76	a_{40}	1	a_{79}	1	a_{118}	0.87	a_{157}	1
a_2	0.77	a_{41}	0.66	a_{80}	0.77	a_{119}	1	a_{158}	0.71
a_3	0.79	a_{42}	0.89	a_{81}	0.79	a_{120}	0.79	a_{159}	0.88
a_4	1	a_{43}	1	a_{82}	0.87	a_{121}	0.87	a_{160}	1
a_5	0.79	a_{44}	0.89	a_{83}	1	a_{122}	1	a_{161}	0.71
a_6	1	a_{45}	1	a_{84}	0.79	a_{123}	0.79	a_{162}	0.88
a_7	0.79	a_{46}	0.89	a_{85}	0.87	a_{124}	0.87	a_{163}	1
a_8	1	a_{47}	1	a_{86}	1	a_{125}	1	a_{164}	0.71
a_9	0.79	a_{48}	0.89	a_{87}	0.79	a_{126}	0.79	a_{165}	0.88
a_{10}	1	a_{49}	1	a_{88}	0.87	a_{127}	0.87	a_{166}	1
a_{11}	0.79	a_{50}	0.89	a_{89}	1	a_{128}	1	a_{167}	0.71
a_{12}	1	a_{51}	1	a_{90}	0.79	a_{129}	0.79	a_{168}	0.88
a_{13}	0.79	a_{52}	0.89	a_{91}	0.87	a_{130}	0.87	a_{169}	1
a_{14}	1	a_{53}	1	a_{92}	1	a_{131}	1	a_{170}	0.71
a_{15}	0.79	a_{54}	0.89	a_{93}	0.79	a_{132}	0.79	a_{171}	0.88
a_{16}	1	a_{55}	1	a_{94}	0.87	a_{133}	0.87	a_{172}	1
a_{17}	0.79	a_{56}	0.89	a_{95}	1	a_{134}	1	a_{173}	0.71
a_{18}	1	a_{57}	1	a_{96}	0.79	a_{135}	0.79	a_{174}	0.88
a_{19}	0.79	a_{58}	0.89	a_{97}	0.87	a_{136}	0.87	a_{175}	1
a_{20}	1	a_{59}	1	a_{98}	1	a_{137}	1	a_{176}	0.71
a_{21}	0.79	a_{60}	0.89	a_{99}	0.79	a_{138}	0.65	a_{177}	0.88
a_{22}	1	a_{61}	1	a_{100}	0.87	a_{139}	0.69	a_{178}	1
a_{23}	0.79	a_{62}	0.89	a_{101}	1	a_{140}	0.71	a_{179}	0.71
a_{24}	1	a_{63}	1	a_{102}	0.79	a_{141}	0.88	a_{180}	0.88
a_{25}	0.79	a_{64}	0.89	a_{103}	0.87	a_{142}	1	a_{181}	1
a_{26}	1	a_{65}	1	a_{104}	1	a_{143}	0.71	a_{182}	0.71
a_{27}	0.79	a_{66}	0.89	a_{105}	0.79	a_{144}	0.88	a_{183}	0.88
a_{28}	1	a_{67}	1	a_{106}	0.87	a_{145}	1	a_{184}	1
a_{29}	0.79	a_{68}	0.89	a_{107}	1	a_{146}	0.71	a_{185}	0.71
a_{30}	1	a_{69}	1	a_{108}	0.79	a_{147}	0.88	a_{186}	0.88
a_{31}	0.79	a_{70}	0.89	a_{109}	0.87	a_{148}	1	a_{187}	1
a_{32}	1	a_{71}	1	a_{110}	1	a_{149}	0.71	a_{188}	0.71
a_{33}	0.79	a_{72}	0.89	a_{111}	0.79	a_{150}	0.88	a_{189}	0.88
a_{34}	1	a_{73}	1	a_{112}	0.87	a_{151}	1	a_{190}	1
a_{35}	0.79	a_{74}	0.89	a_{113}	1	a_{152}	0.71	a_{191}	0.71
a_{36}	1	a_{75}	1	a_{114}	0.79	a_{153}	0.88	a_{192}	0.88
a_{37}	0.79	a_{76}	0.89	a_{115}	0.87	a_{154}	1	a_{193}	1
a_{38}	1	a_{77}	1	a_{116}	1	a_{155}	0.71	a_{194}	0.71
a_{39}	0.79	a_{78}	0.89	a_{117}	0.79	a_{156}	0.88	a_{195}	0.88

interaction is defined as required. Since exploiting this vulnerability impacts components beyond their security scope, the scope has been changed. This attack can impact the confidentiality of EV users considerably. However, the integrity and availability of data may not be considerably affected by attackers for EV-LAAs. As such, confidentiality, integrity, and availability are defined as high, low, and low, respectively. This selection can be customized based on the real features of this vulnerability (mobile and web applications) that have already been reported in the National Vulnerability Database (NVD) [82]. After selecting these items and deploying the CVSS V3.1 website, the scoring for this adversarial action can be calculated as 7.6. This amount can be divided by 10 to provide the probabilities of each branch in the MDP tree. To calculate probabilities for other branches with different adversarial actions, we have used this standard and summarized the calculated probabilities in Table. 6.2. This probability has also been added to each branch of the MDP by using red numbers.

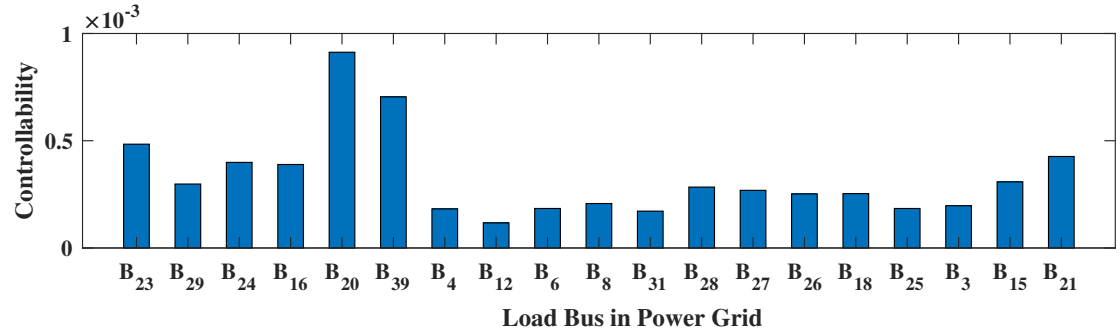


Figure 6.11: Controllability of different 19 load buses of transmission system

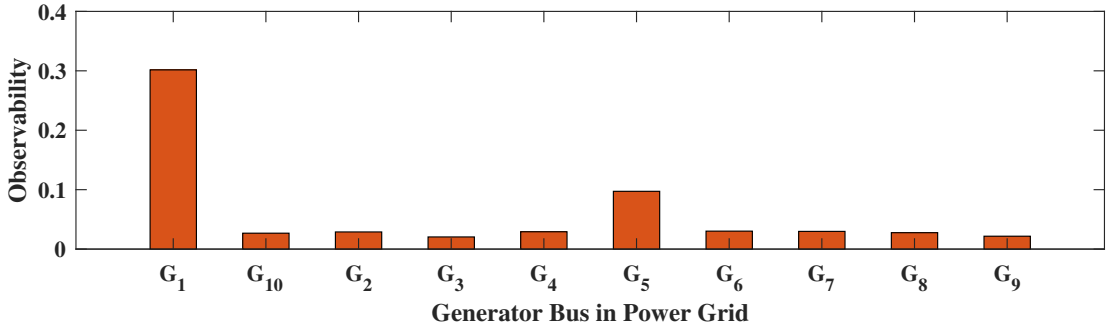


Figure 6.12: Observability of 10 different generator buses.

6.7.3 Numerical Evaluation

The set of $\mathcal{S} = \{s_1, ..., s_{120}\}$ has been referred to as compromised components of the EV ecosystem (i.e., states of the MDP tree). Also, adversarial actions taken by attackers have been shown through the set of $\mathcal{A} = \{a_1, ..., a_{196}\}$. The s_1 is the initial state where intruders can penetrate the cyber and physical layers of the EV ecosystem and manipulate charging stations to launch EV-LAAs, leading to frequency instability in the 39-bus New England system. As such, the attacker takes the first action (a_1) and moves from the initial state (s_1) to the Mb/web application state (s_2) as a vulnerable point. Then, intruders can target the business network of EVSE (s_3) using attack graphs mentioned in Section 2.3 by taking another adversarial action (a_2) and having access to EVCSs at Bus 3 of the proposed transmission system (s_4). By taking adversarial action (a_3), the attackers take control of the targeted EVCSs at Bus 3 and launch EV-LAAs from this load bus. For more severe impacts, adversaries can stay in state s_4 and repeat this adversarial action (a_4). The proposed MDP tree is resolved by Algorithm 10, and the values of each state, $V(s)$, and optimal adversarial action, a_{opt}, for $\beta_1 = \beta_2 = \beta_3 = \beta_4 = 1$ and two values of discount factors, i.e., $\gamma =$

Table 6.3: Security Metric Evaluation of Customised MDP Tree for Two Discount Factors γ=0.95 and γ=0.5

State	$V(s)$	a_{opt}	$V(s)$	a_{opt}	State	$V(s)$	a_{opt}	$V(s)$	a_{opt}	State	$V(s)$	a_{opt}	$V(s)$	a_{opt}	State	$V(s)$	a_{opt}	$V(s)$	a_{opt}
	γ=0.95		γ=0.5			γ=0.95		γ=0.5			γ=0.95		γ=0.5			γ=0.95		γ=0.5	
s1	44.1325	80	0.9051	80	s31	11.8800	57	1.1880	57	s61	50.6660	107	5.0666	107	s91	3.5299	153	0.3327	153
s2	46.8024	2	1.9455	2	s32	50.6660	59	5.0666	59	s62	27.8837	109	2.6139	109	s92	3.5540	154	0.3554	154
s3	50.0014	19	4.4722	19	s33	28.0920	61	2.8092	61	s63	28.0920	110	2.8092	110	s93	21.6941	156	2.0448	156
s4	16.1780	4	1.6178	4	s34	32.0180	63	3.2018	63	s64	31.7806	112	2.9792	112	s94	21.8420	157	2.1842	157
s5	19.0420	6	1.9042	6	s35	26.4920	65	2.6492	65	s65	32.0180	113	3.2018	113	s95	26.6721	159	2.5140	159
s6	9.9880	8	0.9988	8	s36	13.7420	67	1.3742	67	s66	26.2955	115	2.4650	115	s96	26.8540	160	2.6854	160
s7	12.5420	10	1.2542	10	s37	11.1480	69	1.1148	69	s67	26.4920	116	2.6492	116	s97	11.7995	162	1.1122	162
s8	3.5540	12	0.3554	12	s38	17.9280	71	1.7928	71	s68	13.6401	118	1.2787	118	s98	11.8800	163	1.1880	163
s9	21.8420	14	2.1842	14	s39	16.8080	73	1.6808	73	s69	13.7420	119	1.3742	119	s99	50.3229	165	4.7432	165
s10	26.8540	16	2.6854	16	s40	4.2220	75	0.4222	75	s70	11.0653	121	1.0373	121	s100	50.6660	166	5.0666	166
s11	11.8800	18	1.1880	18	s41	4.1760	77	0.4176	77	s71	11.1480	122	1.1148	122	s101	27.9018	168	2.6299	168
s12	50.6660	20	5.0666	20	s42	6.8200	79	0.6820	79	s72	17.7950	124	1.6682	124	s102	28.0920	169	2.8092	169
s13	28.0920	22	2.8092	22	s43	47.1491	105	2.0806	105	s73	17.9280	125	1.7928	125	s103	31.8012	171	2.9974	171
s14	32.0180	24	3.2018	24	s44	16.0580	82	1.5053	82	s74	16.6834	127	1.5640	127	s104	32.0180	172	3.2018	172
s15	26.4920	26	2.6492	26	s45	16.1780	83	1.6178	83	s75	16.8080	128	1.6808	128	s105	26.3126	174	2.4801	174
s16	13.7420	28	1.3742	28	s46	18.9008	85	1.7718	85	s76	4.1907	130	0.3928	130	s106	26.4920	175	2.6492	175
s17	11.1480	30	1.1148	30	s47	19.0420	86	1.9042	86	s77	4.2220	131	0.4222	131	s107	13.6489	177	1.2865	177
s18	17.9280	32	1.7928	32	s48	9.9139	88	0.9294	88	s78	4.1450	133	0.3886	133	s108	13.7420	178	1.3742	178
s19	16.8080	34	1.6808	34	s49	9.9880	89	0.9988	89	s79	4.1760	134	0.4176	134	s109	11.0725	180	1.0436	180
s20	4.2220	36	0.4222	36	s50	12.4490	91	1.1670	91	s80	6.7694	136	0.6346	136	s110	11.1480	181	1.1148	181
s21	4.1760	38	0.4176	38	s51	12.5420	92	1.2542	92	s81	6.8200	137	0.6820	137	s111	17.6608	183	1.6715	183
s22	6.8200	40	0.6820	40	s52	3.5276	94	0.3307	94	s82	46.8500	164	1.9694	164	s112	17.9280	184	1.7928	184
s23	50.3548	58	4.7717	58	s53	3.5540	95	0.3554	95	s83	16.0684	141	1.5145	141	s113	16.6942	186	1.5735	186
s24	16.1780	43	1.6178	43	s54	21.6800	97	2.0324	97	s84	16.1780	142	1.6178	142	s114	16.8080	187	1.6808	187
s25	19.0420	45	1.9042	45	s55	21.8420	98	2.1842	98	s85	18.9130	144	1.7827	144	s115	4.1934	189	0.3953	189
s26	9.9880	47	0.9988	47	s56	26.6549	100	2.4987	100	s86	19.0420	145	1.9042	145	s116	4.2220	190	0.4222	190
s27	12.5420	49	1.2542	49	s57	26.8540	101	2.6854	101	s87	9.9204	147	0.9350	147	s117	4.1477	192	0.3909	192
s28	3.5540	51	0.3554	51	s58	11.7919	103	1.1054	103	s88	9.9880	148	0.9988	148	s118	4.1760	193	0.4176	193
s29	21.8420	53	2.1842	53	s59	11.8800	104	1.1880	104	s89	12.4571	150	1.1741	150	s119	6.7738	195	0.6385	195
s30	26.8540	55	2.6854	55	s60	50.2903	106	4.7144	106	s90	12.5420	151	1.2542	151	s120	6.8200	196	0.6820	196

0.95 and $\gamma = 0.5$, are listed in Table. 6.3. The variation of γ depicts the attacker's interest in future rewards (γ=0.95) instead of immediate rewards (γ=0.5). Moreover, when the adversaries prefer one term of the reward function over the remaining terms, the related coefficient $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ can be initialized in the related term. Based on the results from Table. 6.3, the proposed security metric can investigate different vulnerable points and their impacts on the frequency stability of the power grid during EV-LAAs and quantify cyber attack impacts by calculating a value for each state resembling the compromised parts of EV ecosystems. For example, in this table, for γ=0.95, the value function, i.e., $V(s)$, for the first state (s_1) and next optimal adversarial action (a_{opt}) are obtained as 44.1325 and 80, respectively. It means that the second action from this state to achieve the highest value function and severe impacts on the frequency stability of the power grid is a_{80}. By taking this action, the attackers compromise the CSMS and move to a new state, i.e., s_{43}. The next adversarial action from the state s_{43} is a_{105}, which means targeting the firmware repository of EVCSs at the Bus 20 of the New England system and moving to state s_{60}. The value function of this state is 50.2903, and the next adversarial action is a_{106}. This action means adversaries take control of the system's charging stations at Bus 20, launch the EV-LAAs, and reach state s_{61}. They can stay in the state s_{61} for more severe impacts and continue another EV-LAA by taking action a_{107}. With the definition of another value for the discount factor, the value function for each state and the next adversarial action may differ.

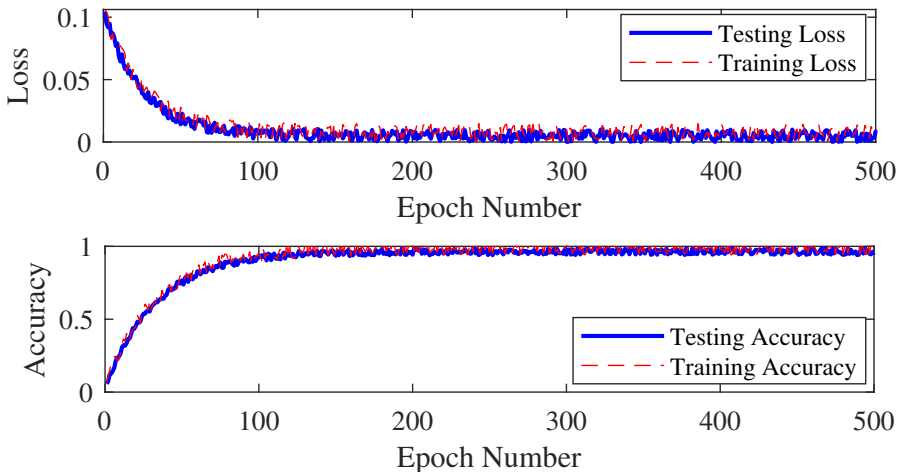


Figure 6.13: Loss function and accuracy for training and testing dataset during 500 epoch number

6.7.4 Developing Security Monitoring Framework

In this section, a BPNN is trained for different EV load penetrations in an offline manner to provide the security status of the transmission system when EV-LAAs occur in the EV ecosystems. To achieve this aim, we have resolved the proposed MDP tree for different EV-LAAs and collected 3,780 data samples for the training phase. During the training, the BPNN model will be fed a comprehensive dataset containing state values of MDP trees that can be labeled as the normal operation of the transmission system or frequency instability when EV-LAAs occur in real-time (i.e., critical class). The loss function and accuracy plots for training and testing datasets have been illustrated in Fig. 6.13 for the 39-bus New England system. It can be seen that the loss function gradually decreases, and accuracy for both testing and training datasets has increased during epoch number. Since the ReLU functions have been used in hidden layers of the BPNN, the non-linear and complex relationship between input data (i.e., state values of the MDP tree) and target data can be modeled. To evaluate the performance of the proposed neural network, evaluation metrics, e.g., accuracy, precision, recall, and F-score, have also been calculated as follows:

$$Accuracy = \frac{(\mathrm{TP} + \mathrm{TN})}{(\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN})} \tag{127}$$

$$Precision = \frac{\mathrm{TP}}{(\mathrm{TP} + \mathrm{FP})} \tag{128}$$

Table 6.4: Evaluation Metrics for Different Hidden Layers

Number of Hidden Layers	Accuracy	Precision	Recall	F score
50	92.52	92.98	92.46	92.72
100	95.12	96.11	95.74	95.79
150	96.25	96.89	96.02	96.45
200	96.83	97.40	96.84	97.12

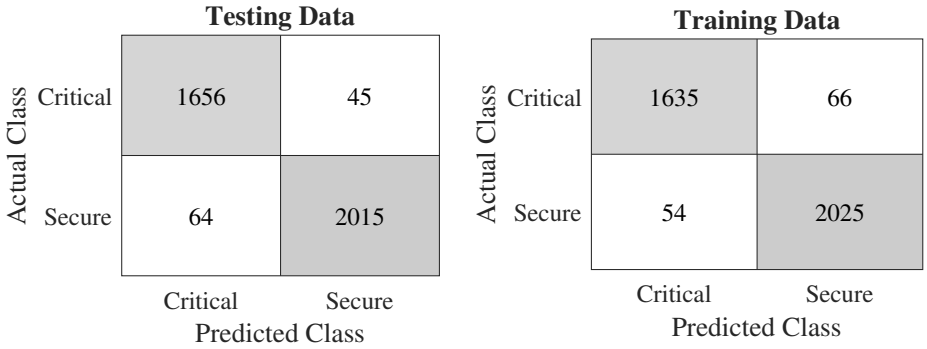


Figure 6.14: Confusion matrix for training and testing datasets

$$Recall = \frac{\text{TP}}{(\text{TP} + \text{FN})} \tag{129}$$

$$Fscore = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{130}$$

where TP, TN, FP, and FN are referred to as true positive, true negative, false positive, and false negative, respectively. These evaluation metrics for different hidden layers have been calculated and listed in Table. 6.4. It can be seen that when the number of hidden layers increases, the BPNN can learn complex values of states during different EV-LAAs in transmission systems and deliver better performance in terms of accuracy, precision, recall, and F score. Moreover, confusion matrices for secure and critical classes during testing and training datasets have been shown in Fig. 6.14.

6.7.5 Verifying Robustness of Security Monitoring With Data Quality Issues:

In this section, the robustness of the proposed security monitoring framework using the BPNN against (i) noisy input and output measurement signals, (ii) missing data measurements, and (iii) outliers of these data, and their impacts on the reliability of the security monitoring framework, will be discussed. As already studied in [113], the Gaussian noise can be used to model measurement devices' noise, such as PMUs in the SCADA of the transmission systems. The accuracy of our

monitoring framework when the signal-to-noise ratio (i.e., SNR = 20 log(signal/noise)) changes in the range of 10-60 dB has been illustrated in Fig. 6.15. It can be seen that with low SNR, the accuracy of the security monitoring is generally lower. In other words, noise in input and output measurement signals can distort the input features and labels, leading the BPNN to learn incorrect mappings. This can result in poor performance on both training and test datasets. However, the obtained results demonstrate that our security monitoring framework's accuracy does not change significantly in the presence of noise. In the following, we have evaluated the proposed framework's performance for other practical problems, such as missing and outlier data measurements due to equipment failures. Therefore, the terms of the reward function are calculated when 5% of randomly selected data measurements are missing, and the MDP tree is generated and resolved. Afterward, the obtained state values pass through the well-trained BPNN to provide information about the security status of the transmission system. It is important to mention that the missing data is set to zero. Furthermore, the reward function terms are calculated when 5% - 10% of the randomly selected data measurements consist of outlier data. To generate outlier data measurements, we multiply the true signal value by a specific random value in the range of 0.01 and 0.1. Afterward, we replace the corresponding data measurements with these manipulated values. The accuracy of the proposed method for different hidden layers during missing and outlier data measurements has also been shown in Fig. 6.16. It can be seen that the well-trained monitoring framework delivers an acceptable performance for missing and outlier data. The main reason is that the proposed MDP tree can quantify the security status of the system and map accurately a set of value states to the secure and critical labels during offline training, making our monitoring framework robust against data quality issues. It is important to mention that outlier data points differ greatly from the surrounding data measurements compared to missing data. Consequently, the training of the BPNN can be more affected by outliers in the input data than by missing data. This can lead to extended training time and a less precise security monitoring framework [114].

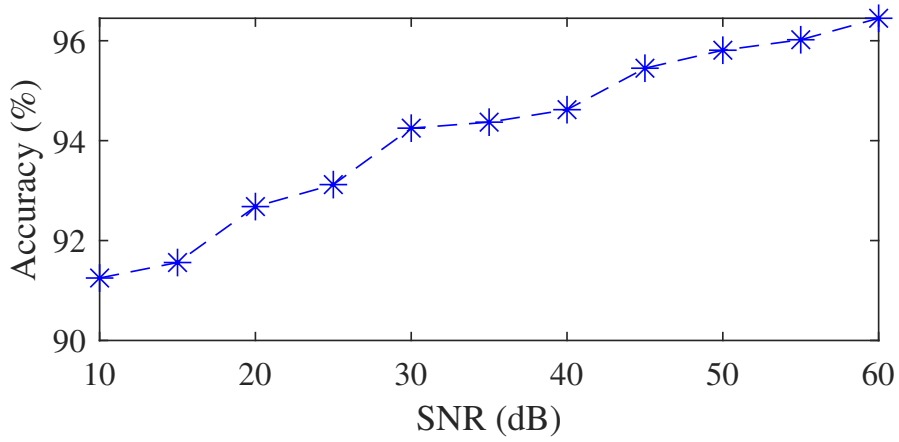


Figure 6.15: Robustness of security monitoring framework against noise in data measurement

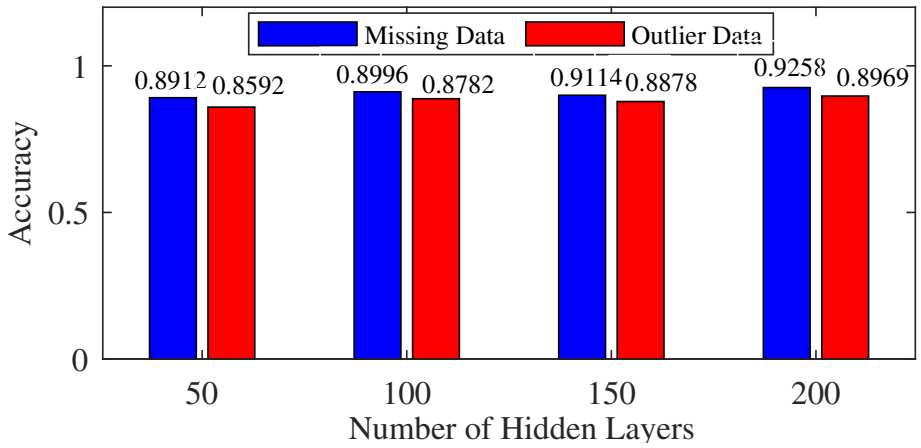


Figure 6.16: Robustness of security monitoring framework against missing and outlier data measurements

6.8 Conclusion

In this paper, we first examined cyber vulnerabilities in EV ecosystems that adversaries could maliciously exploit to apply EV-based load-altering (EV-LAAs) and impact the frequency stability of transmission systems. On this basis, to quantify the security posture of power grids in the presence of such attacks, several attack graphs were devised to determine potential components of the EV ecosystem that can be targeted and related adversarial actions that can be taken by adversaries in a customized Markov decision process (MDP) tree. In this tree, a common vulnerability scoring system (CVSS) was used to assign the probabilities of adversaries' success rates to the branches of this tree. Since EV-LAAs could cause the transfer of low-damping modes in the s-plane, the value

of the mode's damping ratio, controllability, and observability of low-damping modes, as well as the number of compromised charging stations, was formulated in a reward function to give a score to attackers for sabotaging power grid stability. Finally, this MDP tree was resolved by the Epsilon-Greedy Q-learning algorithm to calculate the value of each state and the related optimal adversarial action in the MDP tree. The developed security metric integrated into a neural network was evaluated under the 39-bus New England system to quantify the security status and make a security monitoring framework for providing information about the situation of the transmission system. This security monitoring framework is developed based on two distinct measurement signals, i.e., (i) signals for reporting manipulated EVCSs and (ii) signals for calculating stability-related terms. Even if adversaries bypass the framework for reporting manipulated EVCSs, the impacts of such attacks on stability terms remain detectable. In other words, the attack's impact can be assessed using other measurement devices and system identification techniques.

Chapter 7

Conclusion and Future Directions

In this PhD program, we presented a new surface of load-altering attacks (LAA) originating from EV cyber layers that can impact the stability of power grids. First, we have shown that this type of attack can excite the unstable or lightly-damped torsional modes of the system, leading to increasing torque between mechanical sections of the turbine governor model and subsynchronous resonance (SSR) events. Using an unknown input observer (UIO), which estimated switching attack vectors in an online manner, an adaptive control framework was developed based on a model predictive controller (MPC). This controller could generate control input signals and mitigate the impacts of switching attacks in the form of a wide-area controller. The effectiveness of the proposed adaptive technique was evaluated using M-IEEE-SBM designed for SSR studies. Then, it has been shown that this type of attack can impact the subsynchronous control interaction (SSCI) stability in wind-integrated power grids. In the detection phase, a deep CNN was trained based on a set of voltage and current measurements obtained from the phasor measurement unit (PMU) at the wind farm bus. During this learning process, several uncertainties, e.g., wind speed and the number of WTG, which could cause unstable SSCI modes, were also considered for different amplitude of switching attacks. This customized CNN was deployed to estimate the switching attack vector and inform the operator about the security status of the under-study power grid. Due to the lack of accuracy of the detection method, a robust model predictive controller (RMPC) was designed by resolving as a set of linear matrix inequalities (LMIs) equations to guarantee the stability of the power grid under different switching attacks and uncertainties. Based on the obtained potential

Table 7.1: List of Publications during PhD Program

Title	Venue	Situation
Electric Vehicle Switching Attacks Against Subsynchronous Stability of Power Systems	IEEE Transactions on Industrial Informatics	Accepted
Electric Vehicle-based Load-altering Attacks and their Impacts on Power Grids Operations	IEEE Reliability Magazine	Accepted
Deep Learning Detection and Robust MPC Mitigation for EV-based Load-altering Attacks on Wind-integrated Power Grids	IEEE Transactions on Industrial Cyber-Physical System	Accepted
Developing a Security Metric for Assessing the Power Grid's Posture against Attacks from the EV Charging Ecosystem	IEEE Transactions on Smart Grid	Accepted
Data-Enabled Modeling and PMU-Based Real-Time Localization of EV-Based Load-Altering Attacks	IEEE Transactions on Smart Grid	Accepted
Designing a Security Metric for EV-based Load-altering Attacks in Transmission Systems	IEEE Transactions on Instrumentation and Measurement	Accepted

vulnerabilities in EV ecosystems, we have developed a security metric that captures the security posture of EV ecosystems considering the possible attacks and their associated impacts on distribution grids. This security metric has leveraged the Markov decision process (MDP) tree based on power flow equations, vulnerabilities in the cyber layers of EV ecosystems, attack graphs, and multiple contingencies that can occur in different zones of distribution networks. Using this metric we will demonstrate the detrimental impacts of EV-based attacks in the form of voltage deviations, excessive active power loss, and the unavailability of EVCSs for EV users in distribution networks. Lastly, we have designed this metric for transmission systems where the operators had different stability concerns. The developed security metric integrated into a neural network was evaluated under the 39-bus New England system to quantify the security status and make a security monitoring framework for providing information about the situation of the transmission system. The results of these chapters have been six papers that have been recently published in different IEEE journals, as listed in Table. 7.1.

In the future, we are going to develop Attack-defense trees (ADTs) as hierarchical models to illustrate the potential routes an attacker might follow within the proposed cyber-physical system to reach their goal (i.e., frequency instability in power grids), alongside the defensive actions (detection or mitigation strategies) that can be implemented to thwart these adversarial actions. These trees depict potential vulnerabilities that attackers exploit as leaf nodes, which are connected through logical operators such as AND and OR, culminating in the root node that signifies the ultimate objective of the attackers. The probability of each leaf node in ATDs can be calculated using CVSS discussed in the previous chapters. The attacker's cost to exploit the potential vulnerability in the node of ADTs and the defender's cost to secure the system against the attacker's action can be

also defined for each leaf node. Finally, ADT adopts a game-theoretic approach to model attacker-defender interactions, enabling defenders to identify the most optimal strategies based on the newly proposed payoff calculation technique to have an accurate and practical result.

Bibliography

[1] [Online]. Available: https://www.nrc.gov/docs/ML0722/ML072250202.pdf

[2] K. Sarieddine, M. A. Sayed, D. Jafarigiv, R. Atallah, M. Debbabi, and C. Assi, "A real-time cosimulation testbed for electric vehicle charging and smart grid security," *IEEE Security & Privacy*, pp. 2–11, 2023.

[3] M. Ghafouri, U. Karaagac, H. Karimi, S. Jensen, J. Mahseredjian, and S. O. Faried, "An lqr controller for damping of subsynchronous interaction in dfig-based wind farms," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4934–4942, 2017.

[4] "Global ev outlook 2022," *IEA 2022, https://www.iea.org/reports/global-ev-outlook-2022*, 2022.

[5] 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, no. 3, pp. 200–207, 2020.

[6] S. Acharya, R. Mieth, C. Konstantinou, R. Karri, and Y. Dvorkin, "Cyber insurance against cyberattacks on electric vehicle charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1529–1541, 2022.

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

[8] D. Jafarigiv and et al., "An integrated transmission and distribution grid model for the cyber-security analysis of an ev ecosystem," in *2023 icSmartGrid*, 2023, pp. 1–7.

[9] M. Sayed, R. Atallah, C. Assi, and M. Debabbi, "Electric vehicle attack impact on power grid operation," *Int. J. Electr. Power Energy Syst.*, vol. 137, no. 107784, 2022.

[10] M. Ghafouri, M. E. Kabir, B. Moussa, and C. Assi, "Coordinated charging and discharging of electric vehicles: A new class of switching attacks," *ACM Trans. on Cyber-Physical Systems*, vol. 6, no. 3, pp. 1–26, 2022.

[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," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4377–4388, 2021.

[12] E. Hammad, A. M. Khalil, A. Farraj, D. Kundur, and R. Iravani, "A class of switching exploits based on inter-area oscillations," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4659–4668, 2018.

[13] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," *27th USENIX Security Symposium (USENIX Security 18)*, pp. 15–32, 2018.

[14] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

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

[16] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–59, 2017.

[17] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, 2013.

[18] J. Johnson and B. Anderson, "Cybersecurity for electric vehicle charging infrastructure," *SANDIA Technical Report*, 2022.

[19] B. Anderson, "Securingvehicle charging infrastructure against cybersecurity threats," *SANDIA Technical Report*, 2022.

[20] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp)," *IEEE Communications Surveys & Tutorials*, 2022.

[21] T. Nasr and et al., "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers Security*, vol. 112, no. 102511, 2022.

[22] M. Antonakakis and et al., "Understanding the mirai botnet," *26th USENIX Security Symp*, p. 1093–1110, 2017.

[23] F. Wei and X. Lin, "Cyber-physical attack launched from evse botnet," *IEEE Trans. Power Syst.*, pp. 1–12, 2023.

[24] K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Investigating the security of ev charging mobile applications as an attack surface," *ACM Trans. on Cyber-Physical Systems*, 2023.

[25] [Online]. Available: https://www.bbc.com/news/uk-england-hampshire-61006816

[26] [Online]. Available: https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-.html.

[27] K. W. Rohde, "Cyber security of dc fast charging: Potential impacts to the electric grid," *Idaho National Lab. (INL), Idaho Falls, ID, USA, Tech. Rep. INL/CON-18-52242-Revision-0*, 2019.

[28] O. G. M. Khan, E. El-Saadany, A. Youssef, and M. Shaaban, "Impact of electric vehicles botnets on the power grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*, 2019, pp. 1–5.

[29] G. S. Morrison, "Threats and mitigation of ddos cyberattacks against the us power grid via ev charging," in *M.S. thesis, Wright State Univ., Dayton, OH, USA*, 2018.

[30] F. Bizzarri, A. Brambilla, and F. Milano, "Simplified model to study the induction generator effect of the subsynchronous resonance phenomenon," *IEEE Trans. Energy Convers.*, vol. 33, no. 2, pp. 889–892, 2018.

[31] R. N. Damas, Y. Son, M. Yoon, S.-Y. Kim, and S. Choi, "Subsynchronous oscillation and advanced analysis: A review," *IEEE Access*, vol. 8, 2020.

[32] W. Chen, X. Xie, D. Wang, H. Liu, and H. Liu, "Probabilistic stability analysis of subsynchronous resonance for series-compensated dfig-based wind farms," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 400–409, 2018.

[33] P. Mahish and A. K. Pradhan, "Mitigating subsynchronous resonance using synchrophasor data based control of wind farms," *IEEE Trans. Power Del.*, vol. 35, no. 1, pp. 364–376, 2020.

[34] A. Ghorbani and S. Pourmohammad, "A novel excitation controller to damp subsynchronous oscillations," *Int. J. Electr. Power Energy Syst.*, vol. 3, no. 33, pp. 411–419, 2011.

[35] X. Wu, M. Wang, M. Shahidehpour, S. Feng, and X. Chen, "Model-free adaptive control of statcom for sso mitigation in dfig-based wind farm," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5282–5293, 2021.

[36] "First benchmark model for computer simulation of subsynchronous resonance," *IEEE Trans. Power App. Syst.*, vol. 96, no. 5, pp. 1565–72, 1977.

[37] "Second benchmark model for computer simulation of subsynchronous resonance," *IEEE Trans. Power App. Syst.*, vol. PAS-104, no. 5, pp. 1057–1066, 1985.

[38] P. Sauer, M. P. Pai, and J. Chow, *Power System Dynamics and Stability*. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.

[39] F. Salehi, A. Golshani, I. B. M. Matsuo, P. Dehghanian, M. Aghazadeh Tabrizi, and W.-J. Lee, "On mitigation of sub-synchronous control interactions in hybrid generation resources," *IEEE Trans. Ind. Informal.*, vol. 18, no. 7, pp. 4372–4382, 2022.

[40] R. J. P. J. Chen, *Robust model-based fault diagnosis for dynamic systems*. Springer, 1999.

[41] P. F. R. Clark R. Patton, *Fault diagnosis in dynamic systems: Theory and applications*. Prentice Hall, 1989.

[42] M. Hou and P. Muller, "Design of observers for linear systems with unknown inputs," *IEEE Transactions on Automatic Control*, vol. 37, no. 6, pp. 871–875, 1992.

[43] J. Cehn, R. Patton, and H. ZHANG, "Design of unknown input observers and robust fault detection filters," *International Journal of Control*, vol. 63, no. 1, 1996.

[44] B. Shafai and M. Saif, *Proportional-integral observer in robust control, fault detection, decentralized control of dynamic systems*. Springer, 2015.

[45] E. F. Camacho and C. B. Alba, *Model predictive control*. Springer science & business media, 2013.

[46] P. Anderson, B. Agrawal, and J. Van Ness, *Subsynchronous Resonance in Power Systems*. New York, NY, USA: IEEE Press, 1990.

[47] [Online]. Available: https://www.plugshare.com

[48] A. Abazari, K. Sarieddine, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Electric vehicle switching attacks against subsynchronous stability of power systems," *IEEE Transactions on Industrial Informatics*, pp. 1–12, 2024.

[49] J. Bialek, "What does the power outage on 9 august 2019 tell us about gb power system," 2020.

[50] R. Gagnon and et al., "Hydro-québec strategy to evaluate electrical transients following wind power plant integration in the gaspésie transmission system," *IEEE Trans. Sustain. Energy*, vol. 3, no. 4, pp. 880–889, 2012.

[51] J. Adams, C. Carter, and S.-H. Huang, "Ercot experience with sub-synchronous control interaction and proposed remediation," in *PES TD 2012*, 2012, pp. 1–5.

[52] L. Wang and et al., "Investigation of ssr in practical dfig-based wind farms connected to a series-compensated power system," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2772–2779, 2015.

[53] S. Amini and et al., "Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2036–45, 2019.

[54] H. Jahangir and et al., "A deep learning-based solution for securing the power grid against load altering threats by iot-enabled devices," *IEEE Internet of Things Journal*, 2023.

[55] Q. Li and et al., "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2369–80, 2022.

[56] T. Huang and et al., "A synchrophasor data-driven method for forced oscillation localization under resonance conditions," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 27–39, 2020.

[57] P.-H. Huang and et al., "Subsynchronous resonance mitigation for series-compensated dfig-based wind farm by using two-degree-of-freedom control strategy," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1442–1454, 2015.

[58] X. Shi and et al., "Data-driven wide-area model-free adaptive damping control with communication delays for wind farm," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5062–5071, 2020.

[59] M. Ghafouri and et al., "Robust subsynchronous interaction damping controller for dfig-based wind farms," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 6, pp. 1663–1674, 2019.

[60] A. Amini and et al., "Secure sampled-data observer-based control for wind turbine oscillation under cyber attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3188–3202, 2022.

[61] A. Tangirala, *Principles of System Identification: Theory and Practice*. CRC Press, 2014.

[62] M. V. Kothare, V. Balakrishnan, and M. Morari, "Robust constrained model predictive control using linear matrix inequalities," *Automatica*, vol. 32, no. 10, pp. 1361–1379, 1996.

[63] Z. Wan and M. V. Kothare, "An efficient off-line formulation of robust model predictive control using linear matrix inequalities," *Automatica*, vol. 39, no. 5, pp. 837–846, 2003.

[64] A. M. Carrington *et al.*, "Deep roc analysis and auc as balanced average accuracy to improve model selection, understanding and interpretation," *arXiv preprint arXiv:2103.11357*, 2021.

[65] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[66] J. Oravec and M. Bakosova, "Alternative lmi-based robust mpc design approaches," *IFAC-PapersOnLine*, vol. 48, no. 14, pp. 180–185, 2015.

[67] [Online]. Available: https://bitbucket.org/oravec/mup/wiki/Home

[68] A. Abazari, M. M. Soleymani, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Deep learning detection and robust mpc mitigation for ev-based load-altering attacks on wind-integrated power grids," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 244–263, 2024.

[69] K. Sarieddine, M. A. Sayed, D. Jafarigiv, R. Atallah, M. Debbabi, and C. Assi, "A real-time cosimulation testbed for electric vehicle charging and smart grid security," *IEEE Security & Privacy*, pp. 2–11, 2023.

[70] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[71] [Online]. Available: https://csrc.nist.gov/pubs/ir/8473/ipd

[72] C.-W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040–3050, 2016.

[73] S. R, R. S. Kumar, and A. T. Mathew, "Online static security assessment module using artificial neural networks," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4328–4335, 2013.

[74] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[75] Tushar, V. Venkataramanan, A. Srivastava, and A. Hahn, "Cp-tram: Cyber-physical transmission resiliency assessment metric," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5114–5123, 2020.

[76] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[77] P. Akaber, B. Moussa, M. Ghafouri, R. Atallah, B. L. Agba, C. Assi, and M. Debbabi, "Cases: Concurrent contingency analysis-based security metric deployment for the smart grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2676–2687, 2020.

[78] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1671–1684, 2019.

[79] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security Privacy*, 2006.

[80] Y. Wang, B. Yu, H. Yu, L. Xiao, H. Ji, and Y. Zhao, "Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and bayesian network model," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2880–2891, 2023.

[81] [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[82] "Nvd," *https://cve.mitre.org/cve/search*$_{c}ve_{l}ist.html$.

[83] P. Cheng, L. Wang, S. Jajodia, and A. Singhal, "Aggregating cvss base scores for semantics-rich network security metrics," in *2012 IEEE 31st Symposium on Reliable Distributed Systems*, 2012, pp. 31–40.

[84] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," in *in Proc. IFIP Annu. Conf. Data Appl. Security Privacy*, 2008, pp. 283–296.

[85] T. Thakur and J. Dhiman, "A new approach to load flow solutions for radial distribution system," in *2006 IEEE/PES Transmission Distribution Conference and Exposition: Latin America*, 2006, pp. 1–6.

[86] L. Bertling, R. Allan, and R. Eriksson, "A reliability-centered asset maintenance method for assessing the impact of maintenance in power distribution systems," *IEEE Transactions on Power Systems*, vol. 20, no. 1, pp. 75–82, 2005.

[87] L. Vargas, J. Quirós-Tortós, and G. Valverde, "Voltage regulation of active distribution networks considering dynamic control zones," in *2020 IEEE PES Transmission Distribution Conference and Exhibition*, 2020, pp. 1–6.

[88] [Online]. Available: https://en.wikipedia.org/wiki/Combination

[89] H. S. Chang, H.-G. Lee, M. Fu, and S. Marcus, "Evolutionary policy iteration for solving markov decision processes," *IEEE Transactions on Automatic Control*, vol. 50, no. 11, pp. 1804–1808, 2005.

[90] M. A. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, and C. Assi, "Grid chaos: An uncertainty-conscious robust dynamic ev load-altering attack strategy on power grid stability," *Applied Energy*, vol. 363, p. 122972, 2024.

[91] M. M. Soleymani, A. Abazari, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Data-enabled modeling and pmu-based real-time localization of ev-based load-altering attacks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2024.

[92] International Electrotechnical Commission, "IEC 61000-3-3: Electromagnetic Compatibility (EMC) - Part 3-3: Limits - Limitation of Voltage Changes, Voltage Fluctuations and Flicker in Public Low-Voltage Supply Systems, for Equipment with Rated Current $\leq$16 A per Phase and Not Subject to Conditional Connection," IEC, 2013.

[93] K. Sakthivel, S. Das, and K. Kini, "Importance of quality ac power distribution and understanding of emc standards iec 61000-3-2, iec 61000-3-3 and iec 61000-3-11," in *8th International Conference on Electromagnetic Interference and Compatibility*, 2003, pp. 423–430.

[94] L. Chen, M. Farajollahi, M. Ghamkhari, W. Zhao, S. Huang, and H. Mohsenian-Rad, "Switch status identification in distribution networks using harmonic synchrophasor measurements," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2413–2424, 2021.

[95] "Ieee recommended practice for electric power distribution for industrial plants," *IEEE Standards Board*, 1993.

[96] [Online]. Available: https://github.com/EVecosystem/EVCS_OCPP

[97] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang, and M. Debbabi, "Modeling supply chain attacks in iec 61850 substations," in *2019 IEEE SmartGridComm*, 2019, pp. 1–6.

[98] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, "Countering fdi attacks on ders coordinated control system using fmi-compatible cosimulation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1640–1650, 2021.

[99] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization." *Journal of machine learning research*, vol. 13, no. 2, 2012.

[100] T. Gangwar, N. P. Padhy, and P. Jena, "Storage allocation in active distribution networks considering life cycle and uncertainty," *IEEE Trans. on Industrial Inform.*, vol. 19, no. 1, pp. 339–350, 2023.

[101] M. Rahimipour Behbahani and A. Jalilian, "Reconfiguration of harmonic polluted distribution network using modified discrete particle swarm optimization equipped with smart radial method," *IET Generation, Transmission & Distribution*, vol. 17, no. 11, pp. 2563–2575, 2023.

[102] N. Sahoo and K. Prasad, "A fuzzy genetic approach for network reconfiguration to enhance voltage stability in radial distribution systems," *Energy Conversion and Management*, vol. 47, no. 18-19, pp. 3288–3306, 2006.

[103] A. Abazari, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Developing a security metric for assessing the power grid's posture against attacks from ev charging ecosystem," *IEEE Transactions on Smart Grid*, vol. 16, no. 1, pp. 254–276, 2025.

[104] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[105] J. Duncan Glover, T. Overbye, and M. Sarma, *Power System Analysis and Design*. Cengage Learning, 2016.

[106] M. A. Sayed, M. Ghafouri, M. Debbabi, and C. Assi, "Dynamic load altering ev attacks against power grid frequency control," in *2022 IEEE Power Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.

[107] M. A. Tabrizi, N. Prakash, M. Sahni, H. Khalilinia, P. Saraf, and S. Kolluri, "Power system damping analysis on large power system networks: An entergy case study," in *2017 IEEE Power Energy Society General Meeting*, 2017, pp. 1–5.

[108] G. Li, C. Wen, W. X. Zheng, and Y. Chen, "Identification of a class of nonlinear autoregressive models with exogenous inputs based on kernel machines," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2146–2159, 2011.

[109] T. Surinkaew and I. Ngamroo, "Adaptive signal selection of wide-area damping controllers under various operating conditions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 639–651, 2018.

[110] A. Heniche and I. Kamwa, "Assessment of two methods to select wide-area signals for power system damping control," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 572–581, 2008.

[111] A. Gopalan and G. Thoppe, "Demystifying approximate value-based rl with ϵ-greedy exploration: A differential inclusion view," *ArXiv*, 2023.

[112] R. Hecht-Nielsen, "Theory of the backpropagation neural network," in *Neural networks for perception*. Elsevier, 1992, pp. 65–93.

[113] Z. Li, H. Liu, J. Zhao, T. Bi, and Q. Yang, "A power system disturbance classification method robust to pmu data quality issues," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 130–142, 2022.

[114] A. Abazari, R. Reghunath, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Designing a security metric for ev-based load-altering attacks in transmission systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 74, pp. 1–18, 2025.