Securing Control of Clustered DC Microgrids with Multiple Interlinking Converters

Ramin Babazadeh Dizaji

A Thesis

in

The Department

of

Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Applied Science (Information Systems Security) at

Concordia University

Montréal, Québec, Canada

March 2025

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Ramin Babazadeh Dizaji**

Entitled: **Securing Control of Clustered DC Microgrids with Multiple Interlinking Converters**

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

Master of Applied Science (Information Systems Security)

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. Jun Yan

_____ Examiner
Dr. Jun Yan

_____ Examiner
Dr. Dr. Nizar Bouguila

_____ Thesis Supervisor
Dr. Mohsen Ghafouri

Approved by _____
Chun Wang, Chair
Department of Concordia Institute for Information Systems Engineering (CIISE)

_____ 2025

_____
Mourad Debbabi, Dean
Faculty of Engineering and Computer Science

Abstract

Securing Control of Clustered DC Microgrids with Multiple Interlinking Converters

Ramin Babazadeh Dizaji

The integration of multiple direct current (DC) microgrids offers a resilient and efficient solution for modern energy demands, particularly with the increasing adoption of intermittent renewable energy sources. However, the reliance on communication networks for coordinating multiple interlinking converters (MICs) introduces vulnerabilities, particularly to False Data Injection Attacks (FDIAs), which can significantly disrupt system stability and operation.

This thesis presents AI-driven cyber-defense strategies to protect clustered DC microgrids interconnected via MICs against FDIAs.

At the primary control level, a Support Vector Machine (SVM)-based anomaly detection framework is developed to identify FDIAs in real time. Once an attack is detected, the system autonomously transitions to a localized power-balancing control to maintain operational stability.

At the secondary control level, an Adaptive Neuro-Fuzzy Inference System (ANFIS)-based signal estimation strategy is proposed to detect injected FDIAs and subsequently reconstruct compromised control signals, thereby maintaining MIC coordination.

Extensive simulation studies validate the effectiveness of the proposed methods, demonstrating their ability to enhance microgrid resilience against various FDIA scenarios, including time-varying and unbounded attacks. The results confirm the efficacy of both the SVM and ANFIS frameworks in safeguarding clustered DC microgrids interconnected via Multiple Interlinking Converters against cyber threats, ensuring stable and secure operation.

Acknowledgments

I am deeply grateful to everyone who has supported and encouraged me throughout my academic journey. Above all, I extend my deepest gratitude to my supervisor, Dr. Mohsen Ghafouri, for his invaluable guidance, unwavering support, and insightful advice, which have profoundly shaped my research. The knowledge I have gained from his expertise and wisdom is immeasurable. I am truly grateful for his patience, encouragement, and the inspiration he has provided throughout this journey.

I am profoundly grateful to my family and friends for their unconditional love, encouragement, and steadfast belief in me. Their unwavering support has been the foundation of my achievements, serving as a constant source of strength and motivation. I truly appreciate the pivotal role they have played in my educational journey and am forever thankful for their presence in my life.

Contents

List of Figures

List of Tables

List of Acronyms

MICs Multiple Interlinking Converters

DC Direct Current

PV Photovoltaic

ANFIS Adaptive Neuro-Fuzzy Inference System

FDIAs False Data Injection Attacks

SVM Support Vector Machine

ICs interlinking converters

ANN Artificial Neural Networks

D-tree Decision Tree

Chapter 1

Introduction

1.1 Introduction and Related Work

A microgrid is a localized power network that consists of multiple distributed generators (DGs), energy storage systems, and various types of loads [7]. Typically, microgrids are categorized into two main types: AC and DC [16]. Given the DC nature of most renewable energy sources and the absence of challenges such as reactive power, power quality, and frequency regulation, DC microgrids have gained significant traction globally and are increasingly regarded as a viable approach for realizing smart grid systems [2, 12]. Nevertheless, DC microgrids face power imbalances between generation and consumption, primarily caused by 1) the intermittent nature of power generation from photovoltaic (PV) and wind systems, and 2) uncertainties in load demand [7]. It is important to note that such power imbalances can result in voltage drops, compromising reliability and stability. Therefore, mitigating these imbalances is crucial [35].

To address these challenges, the concept of multiple DC microgrids has been introduced. This approach aims to maximize the utilization of renewable energy sources, reduce the dependency on energy storage systems [27], and enhance reliability and stability, particularly during emergencies [21]. In this configuration, each microgrid can act as an energy backup for neighboring microgrids, ensuring a continuous and reliable power supply [18, 40]. In the domain of DC microgrid clusters, two DC microgrids operating at the same nominal voltage level can be directly interconnected using a cable [45, 28] while the interconnection of DC microgrids operating at different voltage levels is

achieved through the deployment of interlinking converters [26, 38, 11, 31]. In the context of DC microgrids with multiple voltage levels, two critical aspects must be addressed. The first is the selection of a suitable overlay interconnection topology to improve stability, reliability, and power availability. The second is the development of a secure control scheme to ensure reliable power sharing among interconnected microgrids and to optimize the utilization of distributed energy resources [6].

Regarding the first challenge, an isolated bi-directional DC–DC converter has been introduced in [4, 34] to enable flexible coupling between DC microgrids, while [20, 13] propose a non-isolated bi-directional DC–DC converter for connecting two DC microgrids. It is worth mentioning that MICs are usually employed in parallel to interconnect subgrids, rather than relying on a single interlinking converters (ICs) [23]. This topology is advantageous since employing a single interlinking converter might not have the capability to effectively transfer a significant power load between two DC microgrids, given the constrained current/voltage capacity of the switching devices and the inherent limitations of its associated controller [29, 22]. Moreover, the use of MICs connections provides inherent redundancy, offering increased capacity and providing the system's ride-through ability in case one of the ICs fails [41].

When it comes to the second challenge, developing a secure control scheme for MICs is crucial for the smooth operation of coupled DC microgrids, as power exchange relies entirely on MICs. To this end, a hierarchical control strategy, which employs either a centralized or distributed method, is typically used to achieve load-sharing between interconnected DC microgrids and to facilitate coordination among MICs [5, 6]. Centralized control systems, while simplifying management by centralizing data processing and decision-making, face significant challenges including high computational loads, susceptibility to single-point failures, and increased vulnerability due to their reliance on extensive communication networks [8]. In response to these limitations, distributed secondary control strategy, which only require local data exchanges between adjacent nodes, eliminating the need for a central controller and a complex communication network [19, 44, 46], has been proposed for DC microgrids connected through multiple converters to enhance system flexibility and robustness [5].

due to the extensive information exchanges and computational processes involved [10, 2].

However, the dependence on communication networks and the computational processes involved in distributed strategies significantly heightens the risk of cyber threats [10, 2]. Such threats could disrupt MIC coordination, cause substantial economic losses, and even render the entire microgrid inoperable.

Potential cyber attacks that undermine the distributed control of DC microgrids mainly include false data injection (FDI) attacks [36], replay attacks [14], denial of service (DoS) attacks [48, 9, 24], hijacking [32], and man-in-the-middle (MITM) attacks [33]. FDIA aims to maliciously disrupt control operations by injecting false data into sensors, actuators, or communication links, altering the system state and compromising stability [33, 42, 3]. Replay attacks compromise the integrity of communication by capturing and storing sensor readings over a period of time, then retransmitting the recorded data as current information, leading to incorrect system responses and long communication delays [15]. DoS attacks interfere with communication channels by delaying or blocking information transmission, which disrupts coordination between sensors, controllers, and actuators, leading to instability in microgrids and reduced system responsiveness [17, 43]. Hijacking attacks completely replace existing control signals within the communication network, causing compromised agents to deviate from their intended operation and disrupting the iterative consensus process, leading to power imbalances and instability in DC microgrids [37]. MITM attacks infiltrate communication between two nodes, allowing a third party to manipulate transmitted data, which can lead to inconsistent microgrid performance and operational disruptions [1].

Given that FDIAs are prevalent and critical cyber intrusions in the communication networks of distributed control systems [2, 36, 25, 8], this thesis focuses on FDIAs in clustered DC microgrids interconnected via MICs. These attacks can maliciously falsify communication signals, disrupting the power balance between microgrids, compromising MIC coordination, and potentially rendering the entire microgrid inoperable. This thesis will focus on cyber-threats in the context of conventional distributed hierarchical control strategies for MIC-connected DC microgrids and will present defense mechanisms to deal with FDIA in its control strategy.

1.2 Objectives

The main objectives of this thesis are as follows:

- To analyze the impact of FDIAs on the distributed hierarchical control of MICs in DC microgrid clusters.
- To develop a SVM model for detecting FDIA at the primary control level and transitioning to localized power balancing control between microgrids.
- To propose an ANFIS-based strategy for mitigating FDIAs at the primary control level in MICs within clustered DC microgrids, leveraging its capability to address complex, uncertain, and non-linear behaviors.

1.3 Methodology

The methodology employed in this thesis is structured into the following steps:

- System Modeling: A model of a DC microgrid cluster interconnected via MICs, incorporating the dynamics of the conventional distributed hierarchical control strategies and the cyber vulnerabilities posed by FDIAs, is developed.
- Cyber Threat Mitigation with ANFIS: The proposed strategy utilizes an ANFIS as a signal estimator to mitigate the effects of FDIAs. During offline training, the ANFIS is developed using local time-series voltage measurements and communicated signals to predict the sum of signals entering each converter. In the online phase, a reference tracking approach is employed to recover attacked signals based on these estimations, ensuring robust cyber-attack mitigation with reduced computational overhead.
- FDIA Detection with SVM: A linear SVM model is introduced to detect FDIAs at the primary control level. Trained offline with historical time-series data, including normalized voltage readings and interlinking converter measurements, the SVM establishes decision boundaries

to differentiate between normal and attack scenarios. In the online phase, it serves as a real-time monitoring tool, transitioning to localized power balancing control between microgrids upon detecting intrusions.

- Validation and Testing: Both ANFIS and SVM-based strategies are tested under various simulated attack scenarios to assess their effectiveness. Performance metrics such as detection accuracy, system reliability, and voltage stability are analyzed.

1.4 Contributions

The main contributions of this thesis are as follows:

- Developing an ANFIS-based strategy to mitigate FDIAs in MICs within clustered DC microgrids, combining fuzzy reasoning with neural network learning for robust control under cyber threats.
- Introducing a linear SVM model for real-time FDIA detection and transitioning to localized power balancing control, leveraging SVM's strengths in high-dimensional, noisy datasets.
- Demonstrating the effectiveness of these proposed strategies through extensive simulation-based validation, showcasing improvements in system reliability, and cyber-attack resilience.

1.5 Thesis Structure

This thesis is structured into six chapters, each focusing on a different aspect of the research.

- **Chapter 2** provides a comprehensive cyber-physical model of DC microgrids interconnected via MICs. It establishes the foundation for analyzing cyber-attack vulnerabilities and presents a conventional distributed control strategy.
- **Chapter 3** discusses cyber-attack modeling on MIC controllers in DC microgrid clusters. It specifically addresses FDIAs at both the primary and secondary control levels.

- **Chapter 4** presents defense mechanisms against FDIAs on MIC controllers. It proposes a SVM-based anomaly detection framework for real-time detection at the primary control level and an ANFIS-based approach for mitigating FDIAs at the secondary control level.
- **Chapter 5** contains the results of simulation studies that validate the proposed methods under different cyber-attack scenarios. The effectiveness of the SVM-based and ANFIS-based strategies is evaluated in terms of detection accuracy, system reliability, and microgrid stability.
- **Chapter 6** concludes the thesis by summarizing the key findings and contributions.

1.6 Publications

This thesis is based on two manuscripts, both of which have been accepted as conference papers.

- R. Babazadeh-Dizaji, M. B. Vavdareh and M. Ghafouri, "Support Vector Machine-Based False Data Injection Attacks Detection in Interconnected DC Microgrids", 2024 IEEE 3nd Industrial Electronics Society Annual On-Line Conference (ONCON), 2024
- R. Babazadeh-Dizaji and M. Ghafouri, "Mitigating False Data Injection Attacks in DC Microgrids with Multiple Interlinking Converters", IECON 2024- 50th Annual Conference of the IEEE Industrial Electronics Society, 2024

Chapter 2

Cyber-Physical Model of DC Microgrids Interconnected via MICs

This chapter presents a comprehensive cyber-physical model of DC microgrids interconnected via MICs and the developed conventional distributed control strategy Fig. 2.1 [6], establishing the basis for analyzing cyber-attack vulnerabilities.

The system consists of two DC microgrids connected through MICs, as shown in Fig. 2.2. The control structure includes inner voltage control, local droop control, and two hierarchical levels: the primary controller for power balancing and the secondary controller for current coordination across ICs. The primary controller sets a reference current i_{ref} based on microgrid data, which leader ICs use to adjust their outputs. The secondary controller facilitates consensus among other ICs via communication with the leaders.

2.1 Primary-Level Controller for Power Balancing Between Microgrids

The primary-level distributed controller is responsible for determining both the direction and magnitude of the reference current i_{ref} for the leader ICs to achieve power balance between the two microgrids. As illustrated in Fig. 2.2, this controller processes voltage readings from the slack

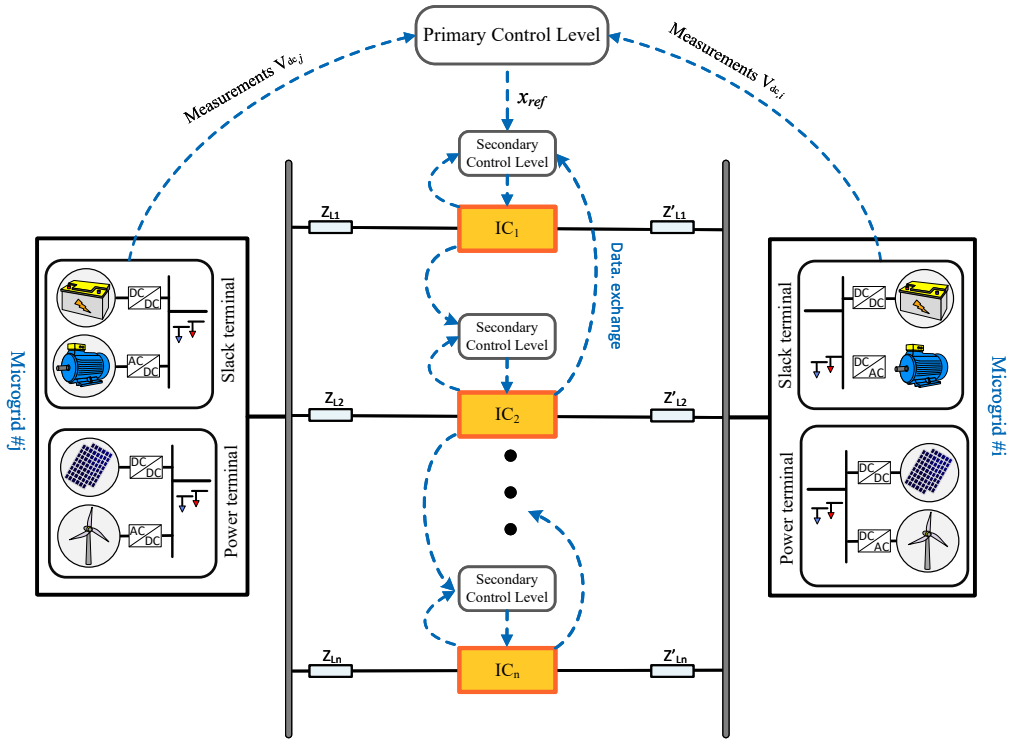

Figure 2.1: Cyber-physical model of DC microgrids interconnected via MICs.

terminals of both microgrids. These slack terminals, which include voltage source converters, contribute to voltage support and load sharing to achieve power balance between supply and demand. In the primary-level controller, the voltages of the slack terminals of both microgrids are normalized using the DC voltage normalization process, expressed as:

$$V_{pu} = \frac{V_{dc} - 0.5(V_{max} + V_{min})}{0.5(V_{max} - V_{min})} \tag{1}$$

where V_{min} and V_{max} represent the minimum and maximum allowable DC voltages, respectively. The normalized voltages of both microgrids are then compared, generating an error term Δv_{pu}, as shown in Fig. 2.2. The error term is processed by a PI controller, which is tasked with eliminating the steady-state error, Δv_{pu}, to ensure that $V_{pu,i} = V_{pu,j}$. A magnitude of Δv_{pu} signifies that the normalized power is balanced on both sides of the IC. Mathematically, this can be expressed as:

$$\lim_{t\to\infty} [V_{pu,i} - V_{pu,j}] = \lim_{t\to\infty} \Delta v_{pu} = 0 \tag{2}$$

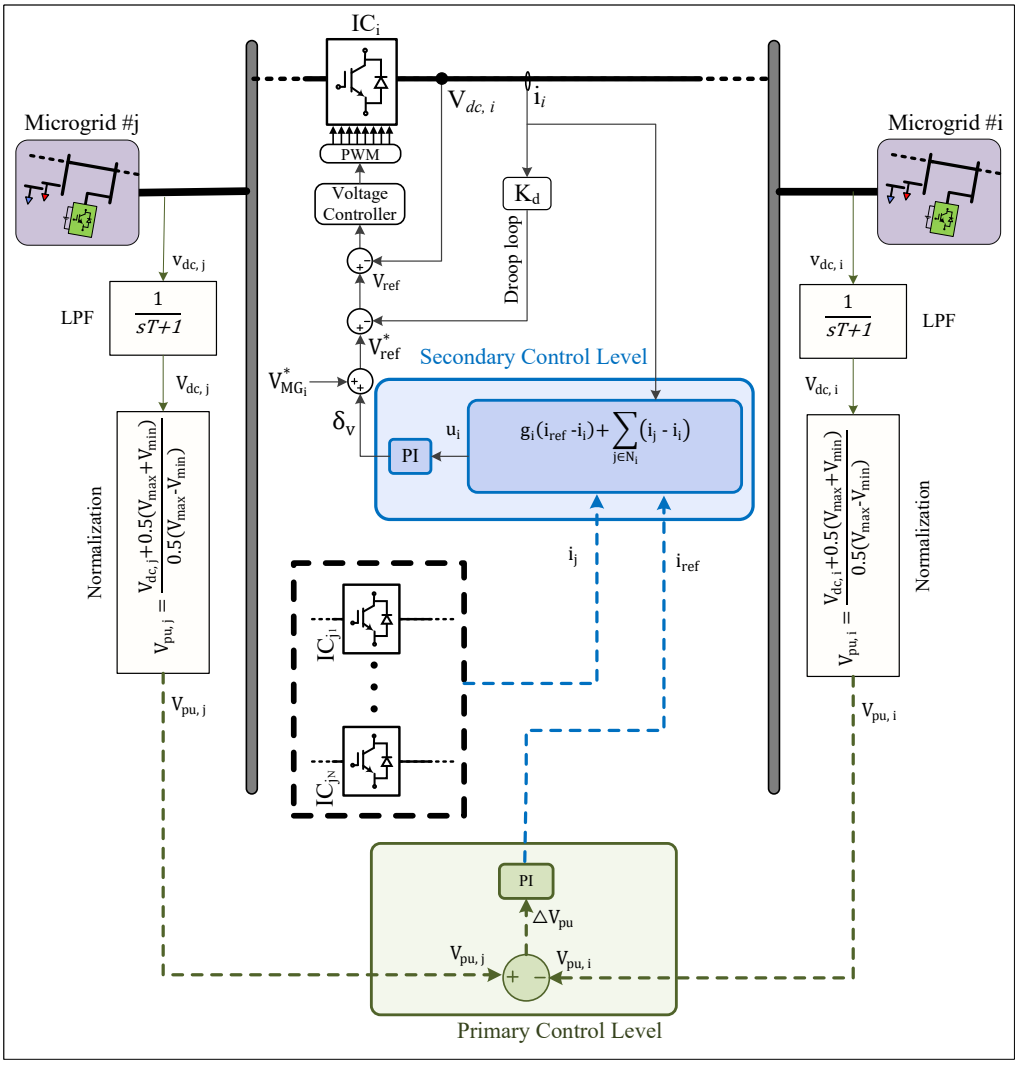

Figure 2.2: The conventional two-level distributed control strategy for MICs [6].

The output of the PI controller generates the reference current i_{ref}, which aligns with the current that must be transferred between the two microgrids through the IC to balance power. This reference is then communicated to the leader ICs, while the remaining ICs adjust their operations by following the leader IC through secondary-level distributed control communication.

2.2 Secondary-Level Distributed Controller for Coordinated Operation of MICs

In this subsection, a brief review of the distributed secondary control for DC microgrids interconnected via multiple converters is provided.

2.2.1 Basic Notion of Graph Theory and Distributed Cooperative Control

The under-study system is a dual-layer system, integrating both a physical and a cyber layer. Within this architecture, each interlinking converter system functions as an entity of the cyber-physical network, where interactions among converters are represented through a directed graph $G = (V, E)$ with nodes $V = \{1, 2, ..., N\}$ and edges $E \subseteq V \times V$. In this digraph, the ICs are represented as nodes, while edges signify communication links. The edge (i, j) (pointing from j to i) mplies that node i receives information from node j with an associated weight a_{ij}. The set of neighboring nodes for a given node i is denoted as N_i, comprising all nodes that transmit data to node i such that $j \in N_i$ if $(j, i) \in E$. The data exchange structure among nodes is represented using an adjacency matrix $A = [a_{ij}] \in R^{N\times N}$, where $a_{ij} = 1$ if node i acquires data from node j, and $a_{ij} = 0$ otherwise. The Laplacian matrix of the graph is determined as $L = D - A$, where D is the in-degree matrix, defined as a diagonal matrix $D = \text{diag}(d_i) \in \mathbb{R}^{N\times N}$, with d_i representing the in-degree of node i, formulated as $d_i = \sum_{j\in N_i} a_{ij}$. In other words, d_i is the cumulative weights of all incoming edges directed toward node i.

In this framework, each node is characterized as a single-state component, denoted by x_i. Each node requires its own data as well as the data from its neighbors $j(j \in N_i)$ on the directed graph to regulate its state x_i. Within the consensus control framework with a predefined reference value x_{ref}, the system states must converge to this reference value. To achieve this, an external synchronization controller is employed, generating a control signal that enforces convergence toward x_{ref} for a selected subset of nodes, termed as leader nodes. The pinning gain g_i is assigned such that it holds a positive value for leader nodes and is set to zero for non-leader nodes. Consequently, the tracking synchronization framework can be expressed as:

$$\dot{x}_i = -g_i(x_i - x_{ref}) - \sum_{j=1}^{n} a_{ij}(x_i - x_j) \tag{3}$$

If the communication graph includes at least one spanning tree, the states of all nodes x_i will converge to a global consensus, matching the reference value x_{ref}.

2.2.2 Distributed Cooperative Control for Coordinate Operation of MICs

The primary role of traditional distributed secondary control is to manage the current of MICs, which must be shared between two microgrids. Additionally, the circulating current will be inherently suppressed. The reference current i_{ref} is exclusively obtained by the leader ICs, which must adjust their current to match this reference value. With an embedded control loop incorporated into the leader ICs, they are tasked with ensuring power balance between the two microgrids. Meanwhile, the remaining ICs regulate their current based on the leader ICs' current. The conventional distributed secondary control for the MICs is shown in Fig. 2.2.

The conventional approach to distributed secondary control adjusts the current of IC#i to match the reference value i_{ref}. As a result, the total current required to be transferred between microgrids is proportionally allocated among the MICs. Accordingly, the cooperative tracking error function is defined as:

$$u_i = -g_i(i_i - i_{ref}) - \sum_{j=1}^{n} a_{ij}(i_i - i_j) \tag{4}$$

where a_{ij} represents the adjacency matrix and g_i is non-zero for the leader ICs, which are responsible for receiving the reference current i_{ref}. Additionally, i_i and i_j indicate the exchanged current through the ith and jth ICs, respectively. This error term u_i is processed through the PI controller to produce the voltage correction term δ_v. Finally, the PI forces e_i to zero at steady-state. Consequently, the current of all ICs with identical capacity ratios converges to a uniform value, ensuring proportional current sharing between the microgrids and among the MICs. The resulting correction term δ_v is added with the global reference voltage $V^*_{MG_i}$ to establish the voltage reference for the inner control loops as:

$$V_{ref} = V^*_{MG_B} - K_{d_i} i_i + \delta_v \tag{5}$$

where V_{ref} denotes the designated voltage reference for the inner control loop, i_i represents the current transmitted via the ith IC, and K_{d_i} corresponds to the droop gain of the IC. By implementing the protocol presented in (4), the current transferred by the ICs, namely $i_1, i_2, \ldots, i_n$, will align proportionally with their respective capacity ratios. This means that $k_1 i_1 = k_2 i_2 = \cdots = k_n i_n$.

Chapter 3

Cyber Attack Modeling on MIC Controllers in DC Microgrid Clusters

The conventional two-level distributed control strategy for MICs [6] ensures balanced power sharing between DC microgrids and proportional current sharing among ICs. However, integrating communication links increases their vulnerability to cyber-attacks. This chapter examines FDIAs—common and critical cyber intrusions into communication networks—that target both the primary and secondary controllers.

3.0.1 FDIA Modeling in Primary Control Level

This section examines FDI attacks targeting the primary controller, which can destabilize power balance between two microgrids, leading to overloads and system instability. We focus on advanced FDIAs where the attacker, with detailed system knowledge, manipulates communication signals using step, sinusoidal, and ramp functions generated by linear dynamic systems [47].

The objective of the distributed control system at the primary level is to maintain power balance between interconnected DC microgrids. This paper demonstrates how FDIAs can compromise the effectiveness of the primary-level distributed controller, resulting in power imbalances across the DC microgrids. Such imbalances may overload one of the microgrids, potentially leading to a shutdown of multiple DC microgrids interconnected by MICs. FDIAs aim to introduce malicious

data into the primary-level distributed controller input data, i.e., $V_{pu,i}$ and $V_{pu,j}$. In this work, the focus is on attacks targeting $V_{pu,i}$. Consequently, if λ represents the false data being injected, the mathematical formulation of the FDIA model is as follows:

$$V_{pu,i}^{a} = V_{pu,i} + \lambda \tag{6}$$

In (6), λ denotes the false data injected by the attacker into the system. Meanwhile, $V_{pu,i}^{a}$ represents the altered value of the normalized voltage of the ith microgrid, which is subsequently transmitted to the primary-level distributed controller for processing. Consequently, at the primary level, equation (2) is revised as follows:

$$\lim_{t\to\infty} \left[V_{pu,i}^{a} - V_{pu,j}\right] = 0 \tag{7}$$

If the normalized voltage of the ith microgrid is not subjected to an FDIA (i.e., $\lambda = 0$), we have:

$$V_{pu,i}^{a} = V_{pu,i} \tag{8}$$

Consequently, based on (7) and (8), the normalized voltages of both microgrids will converge to the same value as:

$$\lim_{t\to\infty} V_{pu,i} = \lim_{t\to\infty} V_{pu,j} \tag{9}$$

Thus, power balance between the two microgrids is achieved.

However, under a FDIA on the normalized voltage of the ith microgrid (where $\lambda \neq 0$ is a constant), we have:

$$V_{pu,i}^{a} = V_{pu,i} + \lambda \tag{10}$$

Thus, considering the attack as indicated in (10), equation (7) can be rewritten as:

$$\lim_{t\to\infty} \left[(V_{pu,i} + \lambda) - V_{pu,j}\right] = 0 \tag{11}$$

Consequently, we arrive at:

$$\lim_{t\to\infty} V_{pu,i} + \lambda = \lim_{t\to\infty} V_{pu,j} \tag{12}$$

This implies that power balance between the two microgrids is not achieved. In other words, we have:

$$\lim_{t\to\infty} V_{pu,i} \neq \lim_{t\to\infty} V_{pu,j} \tag{13}$$

Thus, by tuning the value of λ in (12), the power of one of the microgrids can exceed its maximum generation capacity, potentially leading to overloading and system shutdown in the worst-case FDIA scenario.

3.1 FDIA Modeling in Secondary Control Level

This section examines FDI attacks targeting the secondary controller, which could deviate proportional active power sharing and potentially result in violations of IC power rating limits, leading to subsequent instability within the entire system.

In a clustered DC microgrid interconnected through MICs, the involved ICs communicate with neighboring ICs through a distributed control system. As mentioned in (4), the power-sharing information of each participating IC is shared through a sparse communication network, influencing the current set point adjustment as stated in (5). However, data exchanges also increase the vulnerability to cyberattacks on communication links during the data transmission process. In the following two subsections, we will explore FDIA on communication links between ICs, denoted as i_j, and on the reference signal, denoted as i_{ref}, examining its impact on microgrid performance, particularly concerning proportional active power sharing. We explore an advanced type of FDI attack where the attacker has insight into the system and the capability to manipulate communicated information. The attack signal can either be a varying signal or a fixed signal. These attack signals can be represented as step signals, sinusoidal signals, ramp signals, or a finite combination of them to manipulate the control variables [47].

3.1.1 FDIAs on Communication Links Among ICs

If the communication link between two ICs is compromised with false data injection, the controller receives inaccurate current information. The FDIA on communication links can be represented and modeled as follows:

$$i_j^F = i_j + \eta\, \mu_{ij} \tag{14}$$

where i_j^F is the falsified current of jth IC which is received by ith IC. $\eta = 1$ if a FDIA is present, and $\eta = 0$ otherwise. The μ_{ij} is the malicious signals injected into the communication link by the attackers and can be in the form of $\mu_{ij} = \lambda i_j + \psi$, with $\lambda \in [\alpha_-, \alpha_+]$ representing a nonzero bounded change in the gain coefficient, and $\omega \in [\psi_-, \psi_+]$ is a bounded signal injected by attackers.

Let's assume that the communication link from the jth IC to the ith IC is subjected to an attack, and a malicious communication signal is imposed on the current information. As a result, the received current in the ith IC from jth IC will be i_j^F as stated in (14); and consequently, the current sharing control input in (4) is altered in the following manner:

$$u_i = -g_i(i_i - i_{ref}) - \sum_{j=1}^{n} a_{ij}(i_i - (i_j + \mu_{ij})) \tag{15}$$

where the first term $-g_i(i_i - i_{ref})$ indicates the reference control signal sent from the upper control level, while the subsequent term $-\sum_{j=1}^{n} a_{ij}(i_i - (i_j + \mu_{ij}))$ relates to the data received from neighboring ICs.

Define the state error as the discrepancy between the current of ith IC and the reference value, expressed as $e_i = (i_i - i_{ref})$. To maintain generality, we assume that the ith IC is chosen to be pinned. The evolution of state errors in the presence of communication link attacks is outlined as follows:

$$\dot{\mathbf{e}}(t) = -(\mathbf{L} + \mathbf{G})\mathbf{e}(t) + \mathbf{B}\boldsymbol{\mu}(t) \tag{16}$$

where $\mathbf{L}$ signifies the Laplacian matrix associated with the communication network. $\mathbf{G} = \text{diag}(g_1, \ldots, g_N)$ is the pinning matrix, where $g_i = 1$ for leader nodes and, and $g_i = 0$ otherwise. Also, let

$\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_n)$, where $\mu_i \neq 0$ only if the communication link from the jth node to the ith node is compromised. Furthermore, $\mathbf{B}$ is defined as the matrix $(\mathbf{B})_{mn} = |(\mathbf{M})_{mn}|$, where $\mathbf{M}$ stands for the incidence matrix of the communication network. Accordingly, the dynamics of state errors can be obtained as follows:

$$\mathbf{e}(t) = e^{-(\mathbf{L}+\mathbf{G})t}\mathbf{e}(t_0) + \int_{t_0}^{t} e^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\, \mathbf{B}\boldsymbol{\mu}(\tau)\mathrm{d}\tau \tag{17}$$

Given the negative-definite and invertible nature of the matrix $-(\mathbf{L}+\mathbf{G})$, the initial term of (17), $e^{-(\mathbf{L}+\mathbf{G})t}\mathbf{e}(t_0)$, is driven to approach zero [30]. Without compromising generality, it is assumed that the false signals (i.e., $\mu(\tau)$) are positive, denoted as $(\mu_i > \mu_0 > 0)$, $\forall (i,j) \in \mathcal{E}$. As all components of matrix $\mathbf{B}$ are non-negative, we can conclude:

$$\begin{aligned}
&\lim_{t\to\infty} \mathbf{e}(t) = \lim_{t\to\infty} \int_{t_0}^{t} e^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\, \mathbf{B}\boldsymbol{\mu}(\tau)\mathrm{d}\tau \\
&> \lim_{t\to\infty} e^{-(\mathbf{L}+\mathbf{G})t}\, (e^{-(\mathbf{L}+\mathbf{G})t} - e^{-(\mathbf{L}+\mathbf{G})t_0})\, (\mathbf{L}+\mathbf{G})^{-1}\mathbf{B}\boldsymbol{\mu}_0 \\
&= (\mathbf{L}+\mathbf{G})^{-1}\mathbf{B}\boldsymbol{\mu}_0 > 0
\end{aligned} \tag{18}$$

The state errors described in (18) do not reach a convergence towards zero, indicating that cyber-attacks on communication links would hinder the coordination of proportional current sharing among ICs. This proves that if an IC receives corrupted links from neighboring ICs, the tracking error for that IC is non-zero.

3.1.2 Cyber-Attacks Targeting Leader IC

Imagine a scenario where the reference signal directed to the leader IC is compromised due to a FDIA, and a malicious signal represented by γ_i is injected into i_{ref}. The current sharing control inputs for these leader ICs are subsequently adjusted as:

$$u_{\delta i} = -\sum_{j=1}^{N} a_{ij}(i_i - i_j) - g_i(i_i - (i_{\text{ref}} + \gamma_i)) \tag{19}$$

The dynamic response of the state errors due to cyberattacks on the leader IC can be described

by:

$$\dot{\mathbf{e}}(t) = -(\mathbf{L} + \mathbf{G})\mathbf{e}(t) + \mathbf{G}\boldsymbol{\gamma}(t) \tag{20}$$

Here, $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_N)^T$ with $\gamma_1 = 0$ specifically when the communication pathway to the leader IC has been compromised.

Furthermore, it is hypothesized that the attack vectors imposed on the leader IC are positive, expressed as $\gamma_i > \gamma_0 > 0$. Given that every component of the matrix $\mathbf{G}$ is non-negative, the state errors will not stabilize at zero, indicated by the following analysis:

$$\begin{aligned}
&\lim_{t\to\infty} \mathbf{e}(t) = \lim_{t\to\infty} \int_{t_0}^{t} e^{-(\mathbf{L}+\mathbf{G})(t-s)} \mathbf{G}\boldsymbol{\gamma}(s)\, ds \\
&> \lim_{t\to\infty} e^{-(\mathbf{L}+\mathbf{G})t} \left(e^{(\mathbf{L}+\mathbf{G})t} - e^{(\mathbf{L}+\mathbf{G})t_0} \right) (\mathbf{L} + \mathbf{G})^{-1} \mathbf{G}\gamma_0 \\
&= (\mathbf{L} + \mathbf{G})^{-1} \mathbf{G}\gamma_0 \geq 0
\end{aligned} \tag{21}$$

From this, it can be deduced that the disruptions induced by cyber-attacks on the reference signal obstruct the proportional current sharing among the ICs.

Chapter 4

Cyber Attack Defense Methods Against FDIAs on MIC Controllers in DC Microgrid Clusters

In this chapter, we propose AI-based methods to defend against FDIAs in the primary and secondary controllers of the conventional two-level distributed control strategy for MICs, as discussed in the previous chapter.

4.1 Proposed Defence Approach for FDIA Occurrence in the Primary Control Level

In this section, we propose an AI-based Linear SVM model to detect FDIA at the primary control level and subsequently transition to a localized power balancing control operation between the two microgrids.

4.1.1 Linear Support Vector Machine (SVM) for FDIA Detection

The Linear SVM is a powerful method for binary classification, effectively distinguishing between attack scenarios and normal operations by analyzing key input features. In multiple DC

microgrids, where the system size is larger compared to a single DC microgrid, the high penetration of power converters and renewable energy sources introduces high-frequency switching noise and significant uncertainties, increasing the complexity of system dynamics. Consequently, SVM is particularly well-suited for such a system, as it excels in handling complex datasets, allowing it to capture subtle variations in power converter behavior and detect anomalies within noisy operational data. Additionally, the resilience of SVM in scenarios where attack samples are scarce is crucial for reducing both false positives (misclassifying normal operations as attacks) and false negatives (failing to detect attacks). Compared to other AI-based classification methods, which may struggle with overfitting in large and complex power systems with a high penetration of renewable energy resources or require extensive labeled training datasets, SVM offers a computationally efficient and scalable solution for real-time cyberattack detection.

The core principle of Linear SVM is to identify the optimal hyperplane that maximally separates data points from different classes. In the context of attack detection, the SVM seeks to establish a decision boundary that distinguishes between data points representing attacks and those reflecting normal operations. The hyperplane is constructed to maximize the margin between the two classes, thereby ensuring that the classification model is not only accurate but also generalizes effectively to unseen data.

The Linear SVM model operates by solving an optimization problem that maximizes the margin between the support vectors, which are the data points nearest to the hyperplane from both classes. This optimization seeks to minimize the following objective function:

$$min\frac{1}{2}\left\|W\right\|^2 \ \ s.t.\ y_i(W^T x_i + b) \geq 1 \tag{22}$$

where, W denotes the weight vectors, x_i represents the feature vectors of the data points, b is bias term. The margin is inversely proportional to $\frac{1}{\|W\|}$ indicating that minimizing the norm of $\|W\|$ will maximize the margin. The classifier employs this hyperplane to predict whether new data points belong to the normal operation class or suggest the presence of an attack by calculating the sign of $W^T x_i + b$.

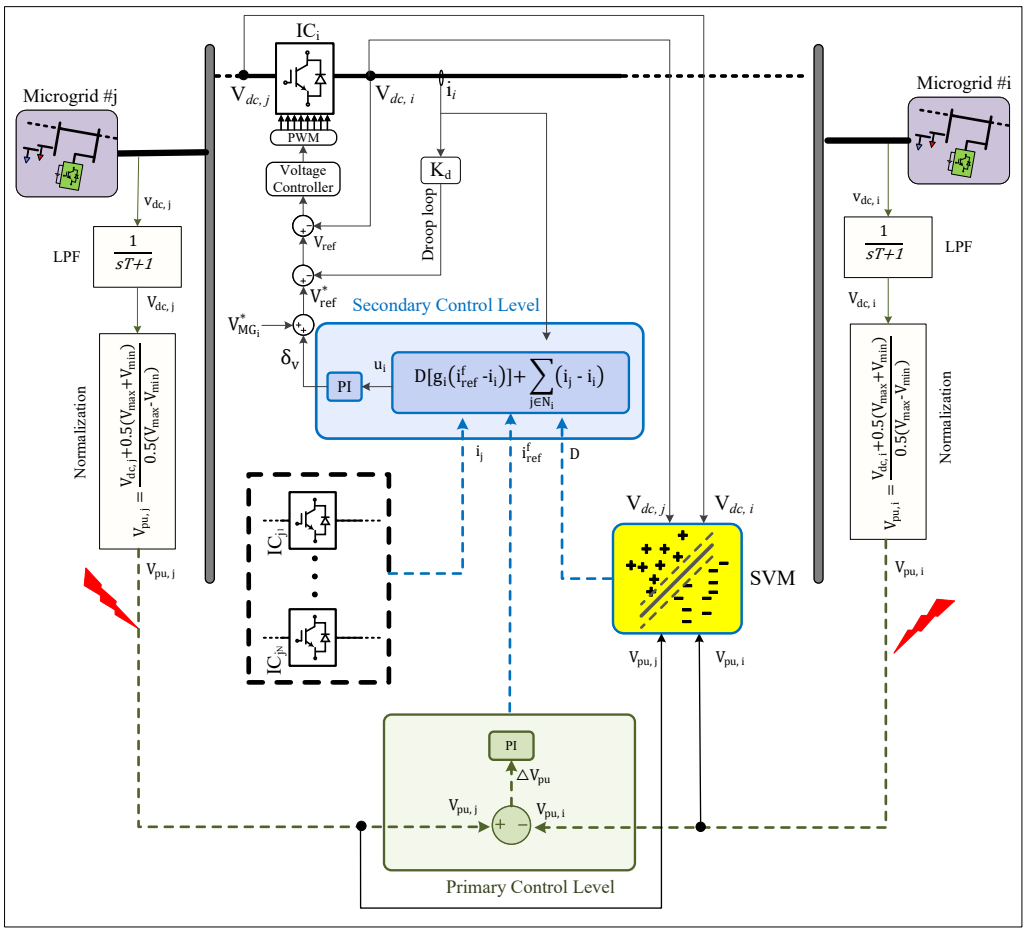

Figure 4.1: The overall structure of MICs in DC microgrids cluster with the proposed SVM-based FDIA detection strategy.

4.1.2 Offline Training Phase

The proposed SVM framework includes two stages: offline training and online implementation. During the offline training phase, the SVM classifier is trained on time-series data of normalized voltages from both microgrids, which serve as inputs to the primary level controller, as well as local voltage measurements taken from each bidirectional interlinking converter. A comprehensive dataset, generated by simulating various operational scenarios in DC microgrids interlinked via multiple ICs, includes both genuine and attack data across conditions such as load and generation fluctuations. This dataset enables the SVM model to effectively distinguish between normal and compromised states.

4.1.3 Online Detection Phase

In the online phase, as shown in Fig. 4.1, the SVM classifier analyzes real-time normalized voltage data from both microgrids, along with local voltage measurements from each bidirectional interlinking converter. This real-time assessment enables the SVM model to identify potential FDIAs by distinguishing between normal operations and attack scenarios. If an intrusion is detected, as illustrated in Fig. 5, the SVM output, denoted as D, will be set to zero. Consequently, under detected intrusion conditions, the reference current i_{ref} generated by the primary control level will be decoupled from the secondary control layer, effectively rendering the primary control output non-contributory to the secondary control layer. As a result, the leader ICs will no longer receive the reference current i_{ref} from the primary-level controller. In this situation, the cooperative tracking error function in (4) is modified as (23), meaning that the secondary-level controller will coordinate current sharing only among the ICs, without attempting to balance power between the two microgrids:

$$u_i = \sum_{j=1}^{n} a_{ij}(i_j - i_i) \tag{23}$$

In this isolated, leaderless state, power balance between the two microgrids remains stable as long as load and generation do not change. This stability is maintained because the system had already reached a steady state before the FDIA. However, if any fluctuations in load or power generation occur, the system's reliance on local droop control will lead to a loss of precise power balance between the microgrids, as local droop control cannot achieve exact balance between the interconnected microgrids.

Once the FDIA is suspended by the attacker, the SVM model will identify the system as secure, setting $D = 1$. At this point, the primary control level resumes its role, and the reference signal i_{ref} is communicated to the leader ICs, thereby establishing precise power balance between the two microgrids. The leader ICs set the target current, while the remaining ICs adjust their current based on the output of the leader ICs, ensuring coordinated control across the microgrids.

4.2 Proposed Defence Approach for FDIA Occurrence in the Secondary Control Level

In this section, we propose a novel AI-based control scheme is designed to mitigate FDIAs in MICs within clustered DC microgrids. It consists of two phases: offline training and online implementation. During offline training, an ANFIS-based estimator, trained on time-series local voltage measurements from each bidirectional interlinking converter, estimates the sum of communicated signals (including data from adjacent ICs and the reference value). In the online phase, the estimator uses real-time data to estimate the sum of signals, which then serves as the reference for a PI-based approach that adjusts the actual signals to counteract FDIA impacts on communication links. Implementation details of the ANFIS estimator and PI controller are provided in subsequent subsections.

4.2.1 Adaptive Network Fuzzy Inference System (ANFIS)

The ANFIS represents a sophisticated amalgamation of the principles of fuzzy logic with the adaptive capabilities inherent in neural networks. This integration is particularly advantageous for modeling complex systems where the relationships between variables are nonlinear and data sets exhibit variability and imprecision. In multiple DC microgrids, where the system size is larger compared to a single DC microgrid, the high penetration of power converters and renewable energy sources introduces high-frequency switching noise, significant uncertainties, increased complexity, and higher dimensionality to the system dynamics. Consequently, ANFIS is particularly well-suited for such a system, as it combines fuzzy inference with adaptive learning to estimate and reconstruct control signals. ANFIS utilizes a Sugeno-type fuzzy system enhanced with a neural learning framework, enabling the system to refine its parameters through iterative learning and adaptation. The system architecture is built around a series of if-then rules that form the foundation of the fuzzy logic inference process, supplemented by the learning algorithms of artificial neural networks (ANN) for effective training and supervision.

In this work, a signal estimator based on ANFIS is developed. The goal of the estimation is the sum of communicated signals received by the IC from its neighboring ICs and the reference

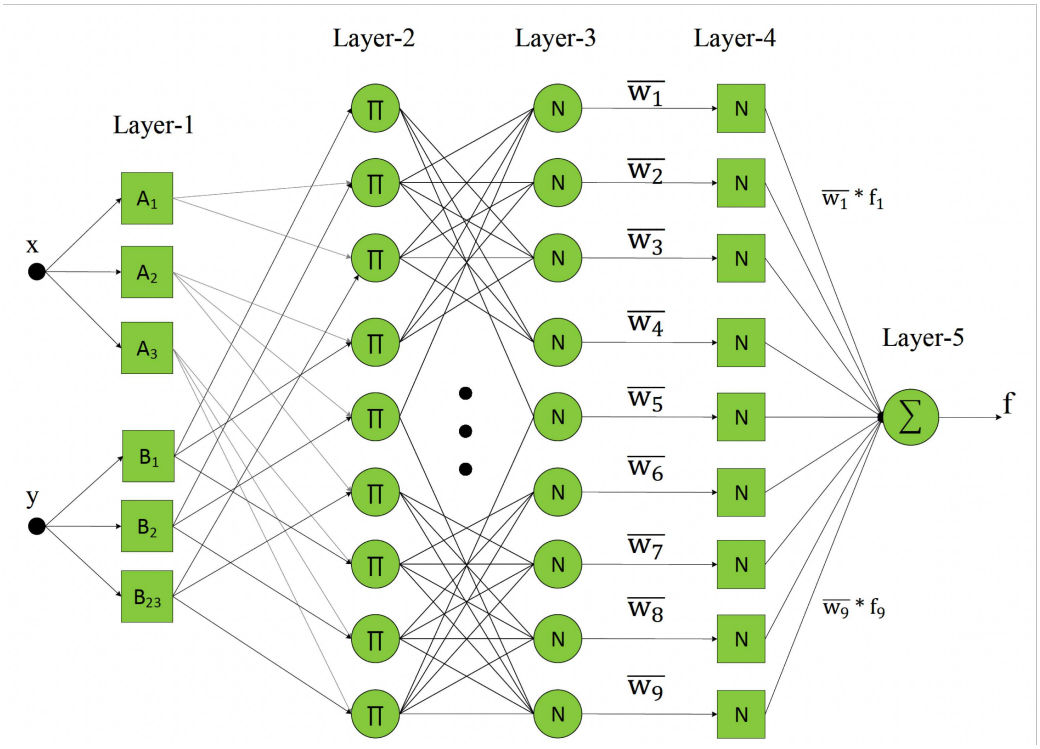

Figure 4.2: ANFIS architecture with two inputs and nine rules.

controller for distributed control, as given in (4), i.e.,

$$I_{\text{sum}} = g_i i_{\text{ref}} + \sum_{j=1}^{n} a_{ij} i_j \tag{24}$$

Therefore, each IC has only one localized ANFIS-based estimator, which estimates I_{sum} and is denoted by $\hat{I}_{sum}$. The structure of the proposed ANFIS structure includes two inputs, each associated with three membership functions, and a total of nine rules, as shown in Fig. 4.2. The rule base consists of three fuzzy (if-then) rules of the Takagi-Sugeno type:

(1) If x is A_1 and y is B_1, then $z_1 = p_1 x + q_1 y + r_1$,

(2) If x is A_2 and y is B_2, then $z_2 = p_2 x + q_2 y + r_2$,

(3) If x is A_3 and y is B_3, then $z_3 = p_3 x + q_3 y + r_3$.

Thus, the ANFIS structure can be organized into five layers, aligning with the configuration shown in Fig. 4.2, explained as follows:

Layer 1 - Fuzzification: Each input variable is converted into fuzzy membership values using Gaussian membership functions. These functions are defined as follows:

$$\mu_{A_i}(x) = \exp\left(-\frac{(x - c_i)^2}{2\sigma_i^2}\right) \tag{25}$$

where c_i and σ_i are the center and width of the Gaussian curve, respectively. This process transforms crisp inputs into degrees of membership ranging across linguistic variables such as 'Low', 'Medium', and 'High'.

Layer 2 - Rule Base: This layer combines the fuzzy inputs from the previous layer to compute the firing strength of each rule, typically using a t-norm operator like the product:

$$w_i = \mu_{A_i}(x) \times \mu_{B_i}(y) \tag{26}$$

Each rule's firing strength represents the degree to which the conditions of the rule are satisfied.

Layer 3 - Normalization: The firing strengths calculated in Layer 2 are normalized to ensure that their sum is unity, which supports an equitable contribution to the model's output:

$$\overline{w}_i = \frac{w_i}{\sum_j w_j} \tag{27}$$

Layer 4 - Defuzzification: Outputs for each rule are computed by weighting the inputs with the normalized firing strengths:

$$f_i = p_i x + q_i y + r_i \tag{28}$$

where p_i, q_i, and r_i are parameters learned through training.

Layer 5 - Output Synthesis: The final model output is an aggregation of all rule outputs, computed as:

$$f = \sum_{i=1}^{9} \overline{w}_i f_i \tag{29}$$

In our work, the output is the estimation of the sum of communicated signals received by the IC from

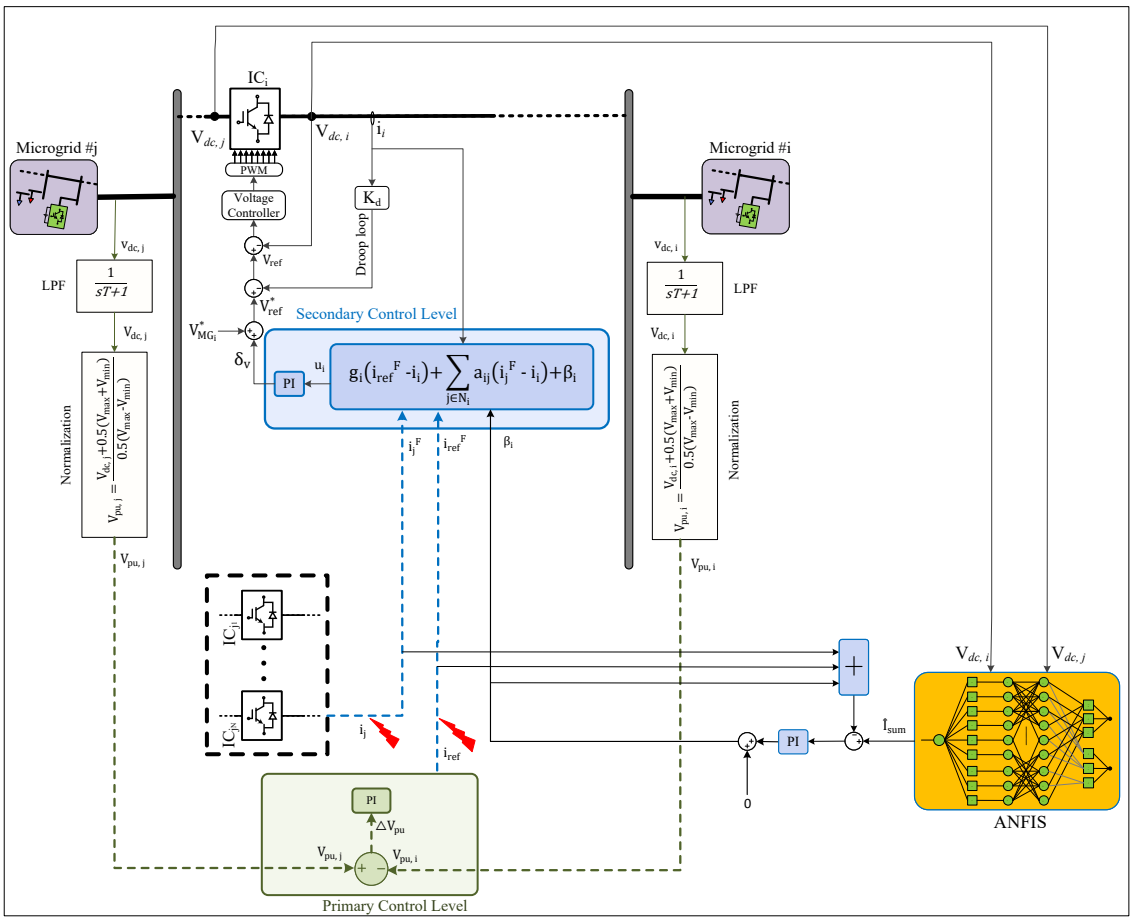

Figure 4.3: The overall structure of MICs in DC microgrids cluster with the proposed ANFIS-based FDIA detection and mitigation strategy.

its neighboring ICs and the reference value, i.e., $\hat{I}_{sum}$, representing a crisp value that reflects the inferred system response based on the fuzzy rules applied. The training of ANFIS involves adjusting the parameters of the model to reduce the difference between the actual outputs and the desired outputs. This learning process is facilitated by algorithms typical of ANN, such as backpropagation combined with least-squares methods, ensuring effective parameter optimization over time.

4.2.2 PI-based Reference Tracking Approach

This work develops a localized PI-based reference tracking approach tailored for online applications within the framework of our proposed method, as depicted in Fig. 4.3. The core concept revolves around utilizing the estimated sum of communicated signals as the reference to compensate

for any signal corruption induced by cyberattacks.

During scenarios where an attack compromises communication links, including both the reference signal and the link between interlinking converters, the sum of the communicated signals received by the IC based on (15) and (19) is given by:

$$I_{\text{sum}}^{F} = g_i(i_{\text{ref}} + \gamma_i) + \sum_{j=1}^{n} a_{ij}(i_j + \mu_{ij}) \tag{30}$$

This value is crucial as it directly affect the current sharing and coordination of MICs. In the presence of the proposed attack mitigation stategy in the i-th IC as seen in Fig. 4.3, the sum of communicated signals will be adjusted as follows:

$$I_{\text{sum}}^{*} = I_{\text{sum}}^{F} + \beta_i \tag{31}$$

In this equation, β_i is the output of the PI controller in the i-th IC, designed to to add into the sum of the under attack signal I_{sum}^{F} for mitigation. The collected signal will approach the reference $\hat{I}_{\text{sum}}$ as follows:

$$\lim_{t\to\infty} \left[I_{\text{sum}}^{F} + \beta_i\right] = \hat{I}_{\text{sum}} \tag{32}$$

Hence, if the estimator operates ideally with negligible error ($\hat{I}_{\text{sum}} \approx I_{\text{sum}}$), then this collected signal will tend towards the standard signal I_{sum}. This convergence helps mitigate the impact of cyberattacks and ensures the safety of the system.

Chapter 5

Simulation Results and Analysis

In this chapter, simulations of the system under FDIAs, using the developed control strategies, are studied with MATLAB Simulink and the PLECS Blockset. The control strategy's effectiveness is validated with the system in Fig. 5.1, developed using MATLAB Simulink and the PLECS Blockset. This configuration connects two DC microgrids via three ICs, where IC#3 has a power rating twice that of IC#1 and IC#2, which are rated equally. Fig. 5.1 also illustrates the communication network, with IC#1 and IC#2 receiving reference signals from the primary control level, while the primary control level collects data from both microgrids.

5.1 Simulation Results of FDIAs on Primary Control Level

In this section, simulation validation comprises two case studies: the first scenario examines FDIA at the primary control level using the conventional two-level distributed control strategy for MICs, whereas the second scenario evaluates FDIA at the primary control level utilizing the proposed SVM-based FDIA detection strategy. To train the support vector machine (SVM) classifier, simulation data was collected over a total duration of 60 seconds. The sampling interval was set to 2 ms, resulting in a dataset comprising 30,000 samples. The dataset includes four input features. The SVM classifier is trained on time-series data of normalized voltages from both microgrids, which serve as inputs to the primary-level controller, as well as local voltage measurements taken from each bidirectional interlinking converter. The data reflects different system conditions and

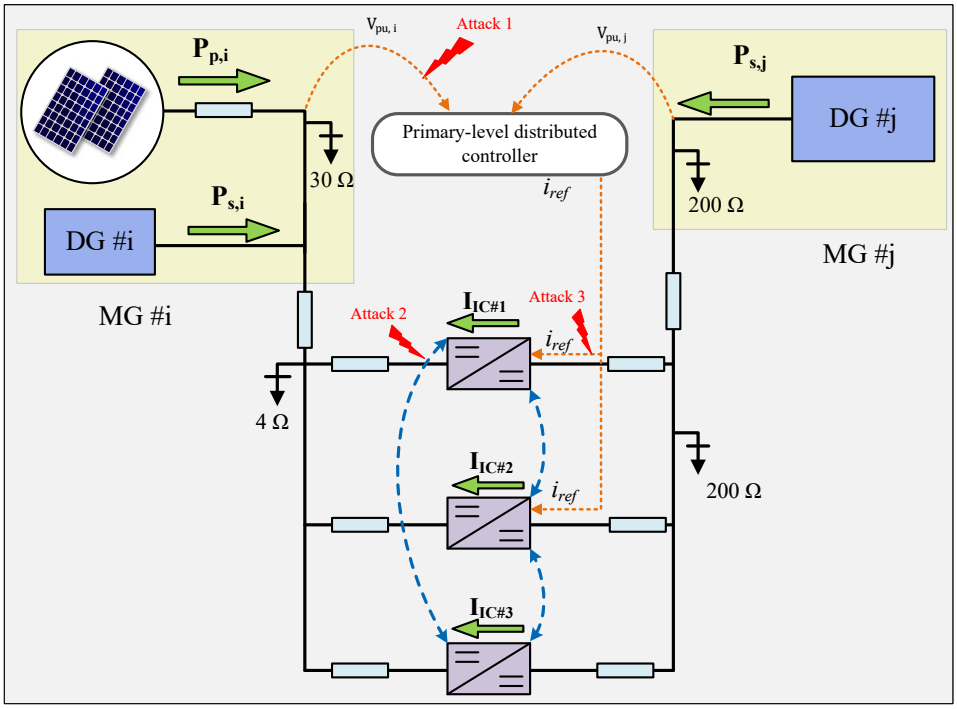

Figure 5.1: Structure of the test system.

includes a labeled output that identifies whether an attack is present (0) or absent (1). Among the collected samples, 20% are labeled as attack scenarios, while 80% correspond to normal operating conditions. Various operational scenarios were considered during data collection to ensure the classifier effectively captures both normal and attack conditions. The dataset was split into 85% for training and 15% for testing.

5.1.1 FDIAs at the Primary Control Level of the Conventional Two-Level Distributed Control Strategy for MICs

In this study, the conventional two-level distributed control strategy for MICs [6] is tested through several scenarios. At $t = 0\,\text{s}$, the system begins under the distributed cooperative control strategy, achieving power balance between microgrids and proportional current sharing among ICs, as shown in Fig. 5.5 (a) and (b). At $t = 1.5\,\text{s}$, the load changes from $4\,\Omega$ to $2.5\,\Omega$, while proportional current sharing and power balance between the microgrids are maintained, as illustrated in

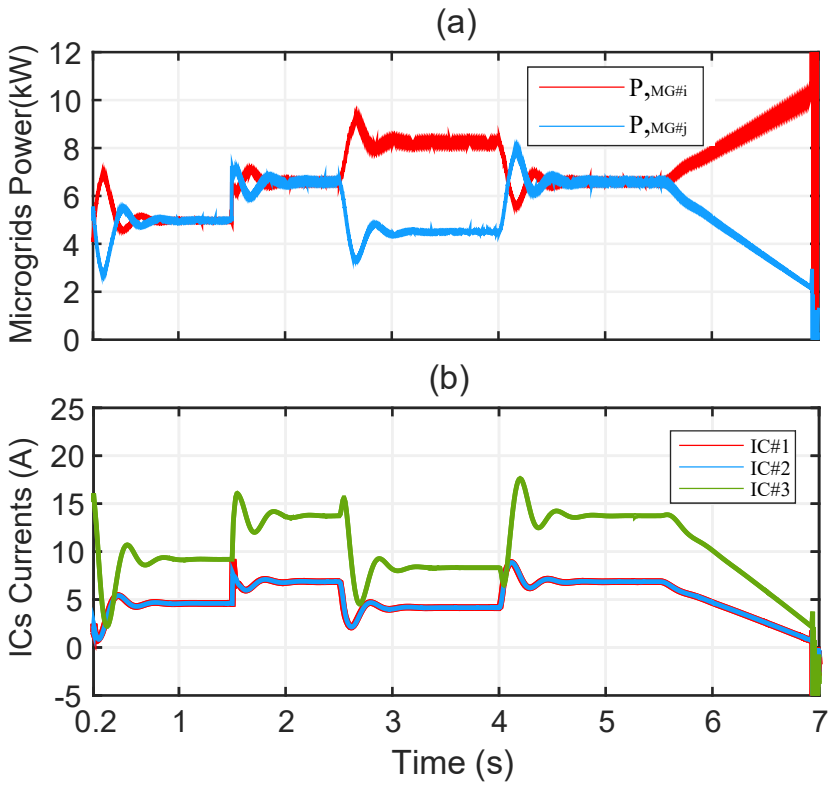

Figure 5.2: Performance of the conventional two-level distributed control strategy for MICs under FDIA:(a) Powers of microgrids , (b) Current transferred by ICs.

Fig. 5.5 (a) and (b). At $t = 2.5\,\text{s}$, a bounded FDIA signal with $\lambda = 0.4$ is introduced to the communication link from the i-th microgrid to the primary controller, , i.e., Attack 1 in Fig. 5.1, disrupting power balance between the microgrids, as seen in Fig. 5.5 (a). At $t = 4\,\text{s}$, the attack signal is removed, returning the system to its normal state. Finally, at $t = 5.5\,\text{s}$, the communication link from the i-th microgrid to the primary controller is targeted with a time-varying FDIA $\lambda = 0.6t$, leading to overload in one microgrid and eventual system collapse, as shown in Fig. 5.5 (a) and (b). These results indicate that the conventional two-level distributed control strategy for MICs is vulnerable to FDIAs at the primary level, with potential system collapse in severe cases.

5.1.2 Evaluation of the Proposed SVM-Based Control Strategy

In this study, the proposed SVM-based control strategy is evaluated under the same load changes and FDIA scenarios applied in the conventional two-level control strategy. For offline SVM training and testing, data collected under varied load conditions include both normal and attack data,

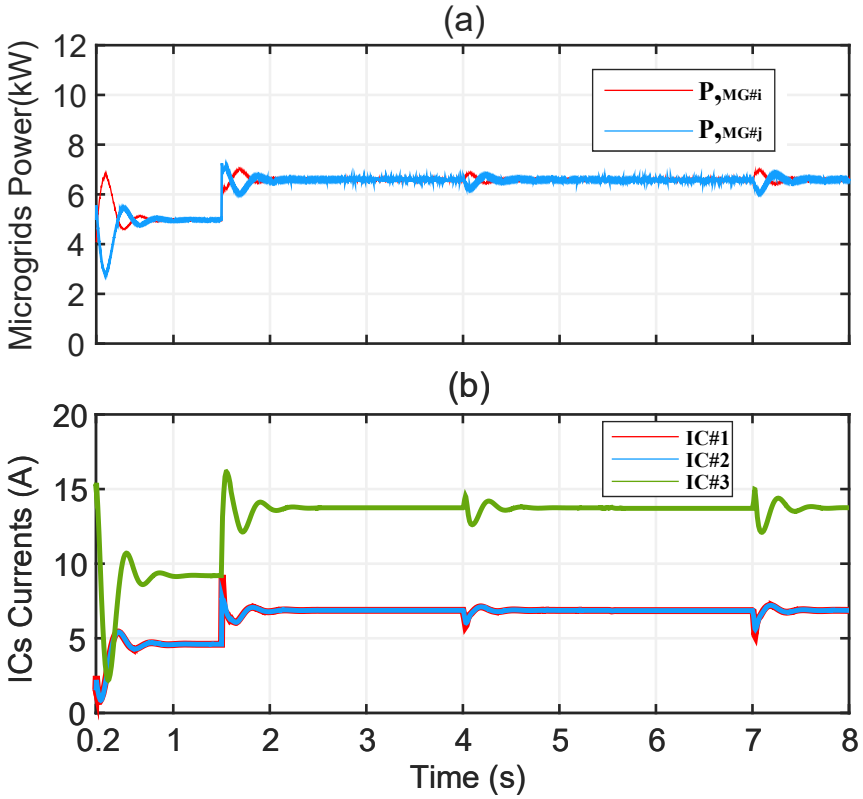

Figure 5.3: Performance of the proposed SVM-Based control strategy under FDIA:(a) Powers of microgrids , (b) Current transferred by ICs.

featuring normalized voltage readings from the microgrids and local voltage measurements from each converter. At $t = 0\,\text{s}$, the system operates under the distributed cooperative control, achieving power balance between microgrids and proportional current sharing among ICs, as shown in Fig. 5.8 (a) and (b). At $t = 1.5\,\text{s}$, the load changes from $4\,\Omega$ to $2.5\,\Omega$, with the system maintaining both power balance and current sharing, illustrating the SVM-based strategy's effectiveness to load disturbances, as depicted in Fig. 5.8 (a) and (b).

At $t = 2.5\,\text{s}$, a bounded FDIA with $\lambda = 0.4$ is introduced to the communication link from the i-th microgrid to the primary controller, i.e., Attack 1 in Fig. 5.1. Unlike the conventional control approach, the SVM model quickly detects the FDIA, prompting an immediate transition to a localized control mode. This adaptive response isolates the primary control layer, ensuring that proportional current sharing and power balance between microgrids remain intact despite the FDIA. Fig. 5.8 (a) and (b) confirm this continuity in operation. Once the FDIA is lifted at $t = 4\,\text{s}$, the

system reverts to normal operation, with minor oscillations indicating the primary control's reactivation and re-establishment of reference currents. A second FDIA is launched at $t = 5.5\,\text{s}$, this time with a time-varying amplitude $\lambda = 0.6t$. The SVM model again detects the intrusion, transitioning the system to localized control and effectively isolating the FDIA's impact. Proportional current sharing and power balance are preserved throughout the attack, as seen in Fig. 5.8 (a) and (b). Upon termination of the FDIA at $t = 7\,\text{s}$, the system re-engages the primary control, with slight oscillations indicating the primary control's reactivation and re-establishment of reference currents.

These results highlight the effectiveness of the SVM-based control strategy in enabling real-time detection of FDIAs. By transitioning to localized control upon detection, the SVM-based approach preserves stability in current sharing and power balance, thereby preventing overload conditions and potential system collapse, even under severe FDIA scenarios.

5.1.3 Result of Attack Detection System

As shown in Fig. 5.4, we evaluated the performance of our proposed attack detection system with two different machine learning models, i.e. decision tree (D-tree), and artificial neural network (ANN), using standard performance metrics including accuracy, precision, and recall [39]. The SVM model demonstrated superior performance across all metrics, achieving 99.90% accuracy, 99.94% precision, and 99.90% recall. The D-Tree classifier also showed acceptable performance with 99.72% accuracy, 99.76% precision, and 99.77% recall. While, the ANN model showed slightly lower metrics with 99.37% accuracy, 98.91% precision, and 99.51% recall. The consistently high performance across all three models, particularly above 99% for most metrics, suggests robust classification capabilities, with SVM exhibiting marginally better results in this particular application. Additionally, the minimal variation between accuracy, precision, and recall for SVM indicates well-balanced classification performance with low false positive and false negative rates. On this basis, SVM has been selected as the detection method to distinguish between attack scenarios and the normal operation of the grid.

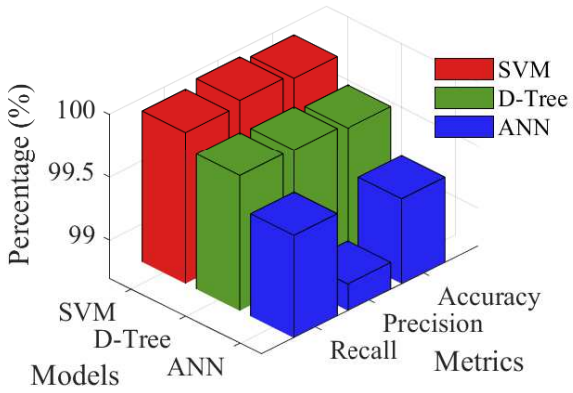

Figure 5.4: Comparison of the proposed model with D-Tree and ANN based on accuracy, recall, and precision.

5.2 Simulation Results of FDIAs on Secondary Control Level

In this section, the simulation validation comprises two case studies. The first scenario examines FDIA in the communication links between ICs at the secondary control level (i.e., Attack 2 in Fig. 5.1), whereas the second scenario evaluates FDIA in the reference signal of ICs at the secondary control level (i.e., Attack 3 in Fig. 5.1). In both cases, the system performance with and without the proposed ANFIS-based control strategy is evaluated. It is worth mentioning that for offline training and testing of the ANFIS model with the structure shown in Fig. 4.2, a dataset was collected, consisting of voltage measurements from each bidirectional interlinking converter as inputs and the sum of communicated signals from other converters as the output. To ensure comprehensive data collection, the simulation time interval was set to 50 seconds. Simulations were conducted for 50 seconds with a sampling time of $50\ ms$, resulting in 1000 collected samples of input-output data. The training dataset was obtained under normal operating conditions (without attacks), incorporating 15 load change scenarios in both microgrids and fluctuations in power generation within each microgrid. This diverse dataset ensures that the trained model can generalize effectively under varying operational conditions.

Using the MATLAB ANFIS toolbox, the input and training data were uploaded to train the ANFIS model. A Sugeno-type inference system was implemented, consisting of two input variables, each with three membership functions, and a single output variable with a constant membership function. The model was trained using the hybrid optimization method for 10 epochs. A total of

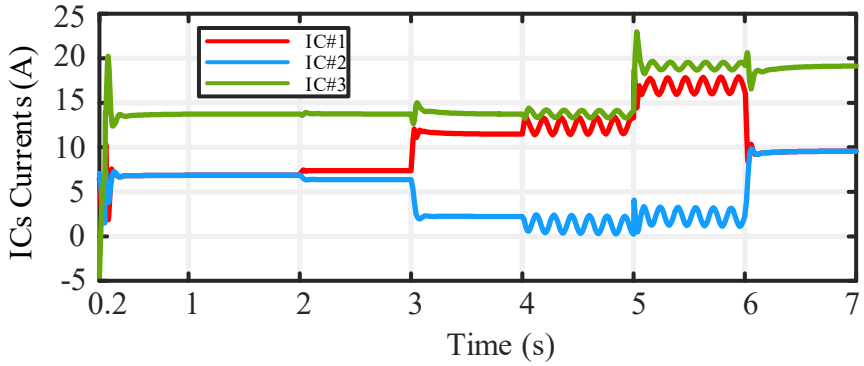

Figure 5.5: Current of ICs with the conventional distributed secondary control under communication links attacks

nine fuzzy rules were generated to define the input-output relationships, ensuring accurate system modeling and response.

5.2.1 FDIAs between Communication Links of ICs

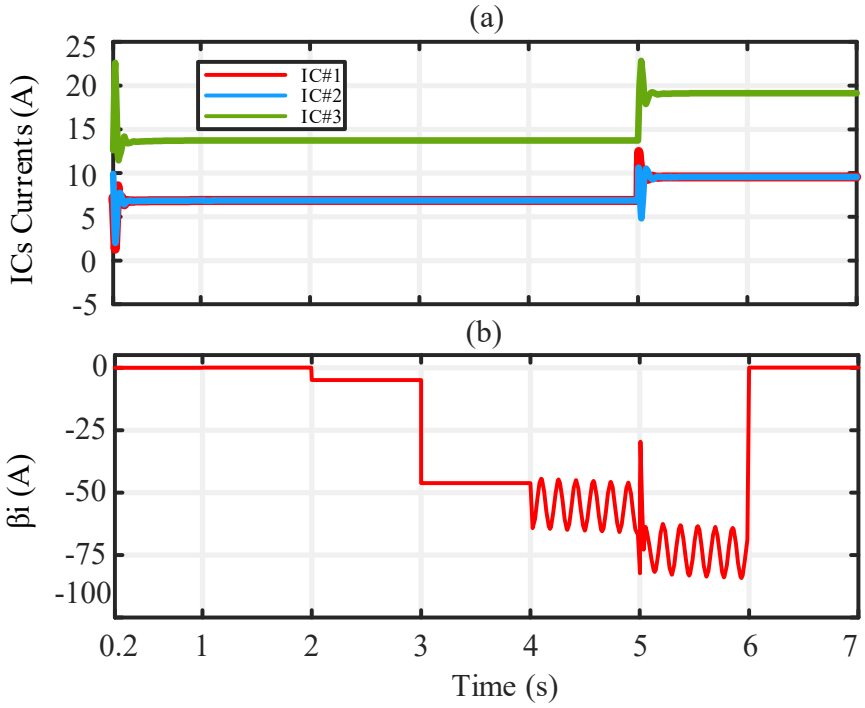

Figure 5.6: Performance of the proposed control strategy for attacks on communication links: (a) Current of ICs; (b) β_i (Output of the PI controller)

In this case, the communication link from IC#3 to IC#1 is attacked, and the comparison of the

simulation with and without the proposed control strategy is carried out. Assume that the communication link from IC#3 to IC#1 under attack is presented as $i_j^F = i_j + (\alpha i_j + \psi)$. The following scenarios occur:

(1) At $t = 0s$, the system operates with conventional distributed cooperative control strategy and $i_3^F = i_3$.

(2) At $t = 2s$, the FDIA as $i_3^F = i_3 + 5$ is engaged.

(3) At $t = 3s$, the FDIA as $i_3^F = i_3 + 5 + 3\ i_3$ is engaged.

(4) At $t = 4s$, the FDIA as $i_3^F = i_3 + 5 + 3\ i_3 + 2\ t + 10 \sin(6t)$ is engaged.

(5) At $t = 5s$, load 3 Ω changes to 2.5 Ω.

Fig. 5.5 shows the performance of the test system without the proposed method under FDIAs on communication links, and as seen, the current of ICs without the proposed method diverges under these attacks, and proportional current sharing among ICs is not established. In contrast, as seen in Fig. 5.6, proportional current sharing is always maintained using the proposed control strategy. According to Fig. 5.6 (a), the attack is consistently mitigated in the compromised IC. Additionally, as indicated in (32), Fig. 5.6 (b) shows β_i, which denotes the output of the PI controller, used to mitigate the effect of FDIA in IC#1. In summary, the proposed method accurately estimates the false data values, effectively neutralizing the FDIA with outstanding performance.

5.2.2 FDIAs on the reference signal

In this case, the reference signal to IC#1 is attacked, and the comparison of the simulation with and without the proposed control strategy is carried out. Assume that the reference signal to IC#1 is presented as $i_{\text{ref}}^F = i_{\text{ref}} + \gamma_i$. The following scenarios occur:

(1) At $t = 0s$, the system operates with conventional distributed cooperative control strategy and $i_{\text{ref}}^F = i_{\text{ref}}$.

(2) At $t = 1s$, the proposed control strategy is activated.

(3) At $t = 2s$, the FDIA as $i_{\text{ref}}^F = i_{\text{ref}} + 5$ is engaged.

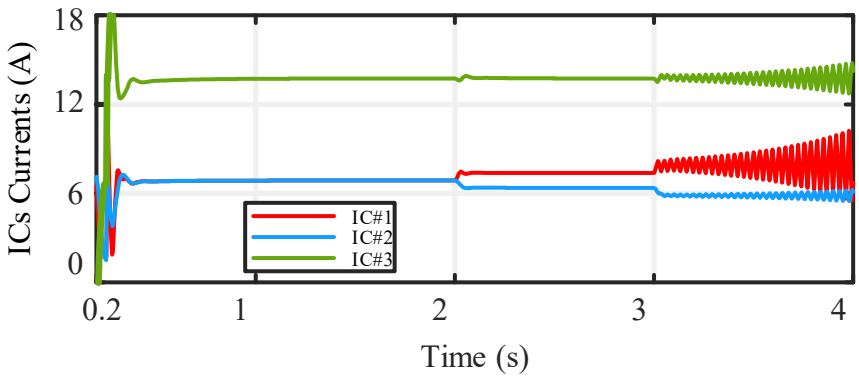

Figure 5.7: Current of ICs with the conventional distributed secondary control under attacks on reference signal.

(4) At $t = 3s$, the FDIA as $i^F_{\text{ref}} = i_{\text{ref}} + 5 + 3\ i_{\text{ref}}$ is engaged.

Fig. 5.7 shows the performance of the test system without the proposed method under FDIAs on the reference signal. As illustrated in Fig. 5.7, the current of ICs without the proposed method diverges under these attacks, and proportional current sharing among ICs is not established. Furthermore, at $t = 3s$, by applying the second FDIA, an oscillatory behavior occurs, causing the system to become unstable. In contrast, as seen in Fig. 5.8(a), proportional current sharing is always maintained using the proposed control strategy. According to Fig. 5.8(a), the attack is consistently mitigated in the compromised IC. In summary, the proposed method accurately mitigate the FDIA with outstanding performance.

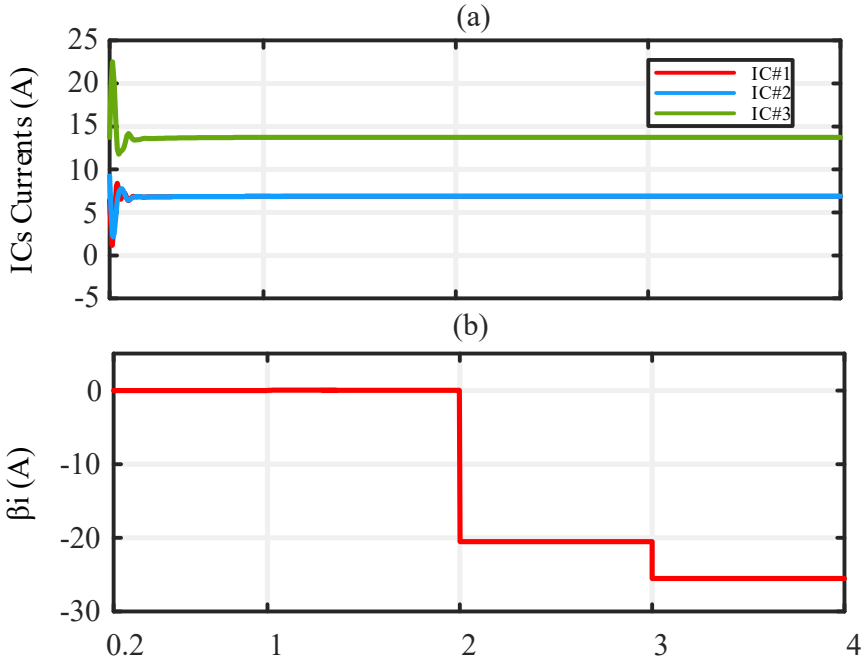

Figure 5.8: Performance of the proposed control strategy for attacks on reference signal: (a) Current of ICs; (b) β_i (Output of the PI controller)

Chapter 6

Conclusion

This thesis has presented an AI-driven cyber-defense framework to enhance the security of interconnected DC microgrids against FDIAs. Two independent strategies were proposed: an SVM-based anomaly detection system for real-time FDIA detection at the primary control level and an ANFIS-based signal estimation method for FDIA mitigation at the secondary control level. These methods provide distinct solutions for securing MICs coordination in clustered DC microgrids.

At the primary control level, a SVM model was developed to detect FDIAs in real time. The proposed SVM-based approach was trained on time-series data from interconnected DC microgrids, effectively distinguishing between normal and compromised system states. Upon detection of an FDIA, the system transitions to a localized power control mode, isolating the primary control and ensuring continued operation. Simulation results confirm that the SVM model achieves high classification accuracy across various FDIA scenarios, maintaining proportional current sharing and power balance between microgrids.

At the secondary control level, an ANFIS-based approach was implemented to estimate and mitigate injected FDIAs in the communication network of the secondary control level for MICs coordination. The ANFIS model, trained on local voltage measurements, enables real-time estimation of the sum of communicated signals entering each interlinking converter. A PI-based reference tracking mechanism then corrects compromised signals, ensuring proper MICs coordination. Extensive simulation studies validate the robustness of this method against different FDIA scenarios, including time-varying and unbounded attacks.

Each of these two strategies effectively enhances the resilience of clustered DC microgrids by addressing cyber threats at different control levels. The results demonstrate that the proposed SVM-based detection method successfully isolates FDIAs at the primary control level, while the ANFIS-based mitigation strategy provides accurate correction for compromised signals at the secondary control level. This research contributes to the advancement of secure and intelligent microgrid systems, paving the way for more cyber-resilient power networks.

Bibliography

[1] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine. A survey of security attacks in information-centric networking. *IEEE Communications Surveys Tutorials*, 17(3):1441–1454, 2015. doi: 10.1109/COMST.2015.2392629.

[2] A. J. Abianeh, Y. Wan, F. Ferdowsi, N. Mijatovic, and T. Dragičević. Vulnerability identification and remediation of fdi attacks in islanded dc microgrids using multiagent reinforcement learning. *IEEE Transactions on Power Electronics*, 37(6):6359–6370, 2022. doi: 10.1109/TPEL.2021.3132028.

[3] Z. Ali, T. Hussain, C.-L. Su, M. Sadiq, A. D. Jurcut, S.-H. Tsao, P.-C. Lin, Y. Terriche, and M. Elsisi. A new paradigm for adaptive cyber-resilience of dc shipboard microgrids using hybrid signal processing with deep learning method. *IEEE Transactions on Transportation Electrification*, 11(1):4280–4295, 2025. doi: 10.1109/TTE.2024.3459856.

[4] R. Babazadeh-Dizaji and M. Hamzeh. Distributed hierarchical control for optimal power dispatch in multiple dc microgrids. *IEEE Systems Journal*, 14(1):1015–1023, 2020. doi: 10.1109/JSYST.2019.2937836.

[5] R. Babazadeh-Dizaji, M. Hamzeh, and A. Hekmati. Power sharing in multiple dc microgrids based on concentrated control. In *Electrical Engineering (ICEE), Iranian Conference on*, pages 1304–1309, 2018. doi: 10.1109/ICEE.2018.8472436.

[6] R. Babazadeh-Dizaji, M. Hamzeh, and K. Sheshyekani. A consensus-based cooperative control for dc microgrids interlinked via multiple converters. *IEEE Systems Journal*, 15(4):4918–4926, 2021. doi: 10.1109/JSYST.2020.3034091.

[7] H. R. Baghaee, M. Mirsalim, G. B. Gharehpetian, and H. A. Talebi. Decentralized sliding mode control of wg/pv/fc microgrids under unbalanced and nonlinear load conditions for on- and off-grid modes. *IEEE Systems Journal*, 12(4):3108–3119, 2018. doi: 10.1109/JSYST.2017.2761792.

[8] J.-W. Chang, S. Chae, and G.-S. Lee. Distributed optimal power sharing strategy in an islanded hybrid ac/dc microgrid to improve efficiency. *IEEE Transactions on Power Delivery*, 38(1):724–737, 2023. doi: 10.1109/TPWRD.2022.3197434.

[9] X. Chen, J. Zhou, M. Shi, Y. Chen, and J. Wen. Distributed resilient control against denial of service attacks in dc microgrids with constant power load. *Renewable and Sustainable Energy Reviews*, 153:111792, 2022.

[10] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang. A fdi attack-resilient distributed secondary control strategy for islanded microgrids. *IEEE Transactions on Smart Grid*, 12(3):1929–1938, 2021. doi: 10.1109/TSG.2020.3047949.

[11] D. Das, M. J. Hossain, S. Mishra, and B. Singh. Bidirectional power sharing of modular dabs to improve voltage stability in dc microgrids. *IEEE Transactions on Industry Applications*, 58(2):2369–2377, 2022. doi: 10.1109/TIA.2022.3144653.

[12] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero. Dc microgrids—part i: A review of control strategies and stabilization techniques. *IEEE Transactions on Power Electronics*, 31(7):4876–4891, 2016. doi: 10.1109/TPEL.2015.2478859.

[13] M. Farhadi, A. Mohamed, and O. Mohammed. Connectivity and bidirectional energy transfer in dc microgrid featuring different voltage characteristics. In *2013 IEEE Green Technologies Conference (GreenTech)*, pages 244–249, 2013. doi: 10.1109/GreenTech.2013.45.

[14] A. J. Gallo, M. S. Turan, F. Boem, G. Ferrari-Trecate, and T. Parisini. Distributed watermarking for secure control of microgrids under replay attacks. *IFAC-PapersOnLine*, 51(23):182–187, 2018.

[15] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate. A distributed cyber-attack detection scheme with application to dc microgrids. *IEEE Transactions on Automatic Control*, 65(9):3800–3815, 2020. doi: 10.1109/TAC.2020.2982577.

[16] A. Gupta, S. Doolla, and K. Chatterjee. Hybrid ac–dc microgrid: Systematic evaluation of control strategies. *IEEE Transactions on Smart Grid*, 9(4):3830–3843, 2018. doi: 10.1109/TSG.2017.2727344.

[17] G. B. Hong and S. H. Kim. Resilient adaptive event-triggered control of nonlinear dc-microgrids under dos attacks: Local stabilization approach. *IEEE Transactions on Automation Science and Engineering*, pages 1–1, 2025. doi: 10.1109/TASE.2025.3532087.

[18] B. John, A. Ghosh, M. Goyal, and F. Zare. A dc power exchange highway based power flow management for interconnected microgrid clusters. *IEEE Systems Journal*, 13(3):3347–3357, 2019. doi: 10.1109/JSYST.2019.2911625.

[19] M. Kachhwaha, H. Modi, M. K. Nehra, and D. Fulwani. Resilient control of dc microgrids against cyber attacks: A functional observer based approach. *IEEE Transactions on Power Electronics*, 39(1):459–468, 2024. doi: 10.1109/TPEL.2023.3326308.

[20] M. Kumar, S. C. Srivastava, S. N. Singh, and M. Ramamoorty. Development of a control strategy for interconnection of islanded direct current microgrids. *IET Renewable Power Generation*, 9(3):284–296, 2015.

[21] X. Li, L. Guo, Y. Li, C. Hong, Y. Zhang, Z. Guo, D. Huang, and C. Wang. Flexible interlinking and coordinated power control of multiple dc microgrids clusters. *IEEE Transactions on Sustainable Energy*, 9(2):904–915, 2018. doi: 10.1109/TSTE.2017.2765681.

[22] X. Li, M. Wang, C. Dong, W. Jiang, Z. Xu, X. Wu, and H. Jia. Distributed unified control for global economic operation and resilience reinforcement of hybrid ac–dc microgrids. *IEEE Transactions on Power Electronics*, 38(7):9077–9089, 2023. doi: 10.1109/TPEL.2023.3259969.

[23] P. Lin, P. Wang, C. Jin, J. Xiao, X. Li, F. Guo, and C. Zhang. A distributed power management strategy for multi-paralleled bidirectional interlinking converters in hybrid ac/dc microgrids. *IEEE Transactions on Smart Grid*, 10(5):5696–5711, 2019. doi: 10.1109/TSG.2018.2890420.

[24] X.-K. Liu, S.-Q. Wang, M. Chi, Z.-W. Liu, and Y.-W. Wang. Resilient secondary control and stability analysis for dc microgrids under mixed cyber attacks. *IEEE Transactions on Industrial Electronics*, 71(2):1938–1947, 2024. doi: 10.1109/TIE.2023.3262893.

[25] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu. Intrusion detection in distributed frequency control of isolated microgrids. *IEEE Transactions on Smart Grid*, 10(6):6502–6515, 2019. doi: 10.1109/TSG.2019.2906573.

[26] J. Ma, M. Zhu, X. Cai, and Y. W. Li. Configuration and operation of dc microgrid cluster linked through dc-dc converter. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, pages 2565–2570, 2016. doi: 10.1109/ICIEA.2016.7604026.

[27] S. Moayedi and A. Davoudi. Cooperative power management in dc microgrid clusters. In *2015 IEEE First International Conference on DC Microgrids (ICDCM)*, pages 75–80, 2015. doi: 10.1109/ICDCM.2015.7152013.

[28] S. Moayedi and A. Davoudi. Distributed tertiary control of dc microgrid clusters. *IEEE Transactions on Power Electronics*, 31(2):1717–1733, 2016. doi: 10.1109/TPEL.2015.2424672.

[29] C. Nie, Y. Wang, W. Lei, M. Chen, and Y. Zhang. An enhanced control strategy for multiparalleled grid-connected single-phase converters with load harmonic current compensation capability. *IEEE Transactions on Industrial Electronics*, 65(7):5623–5633, 2018. doi: 10.1109/TIE.2017.2779420.

[30] R. Olfati-Saber and R. Murray. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, 49(9):1520–1533, 2004. doi: 10.1109/TAC.2004.834113.

[31] J. Qin, Z. Xin, Z. Dong, and H. Liu. Cooperative control of dc microgrid cluster with different voltage levels. In *2023 IEEE 14th International Symposium on Power Electronics for*

Distributed Generation Systems (PEDG), pages 897–900, 2023. doi: 10.1109/PEDG56097.2023.10215219.

[32] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragičević. Distributed screening of hijacking attacks in dc microgrids. *IEEE Transactions on Power Electronics*, 35(7):7574–7582, 2020. doi: 10.1109/TPEL.2019.2957071.

[33] S. Sahoo, T. Dragičević, and F. Blaabjerg. Multilayer resilience paradigm against cyber attacks in dc microgrids. *IEEE Transactions on Power Electronics*, 36(3):2522–2532, 2021. doi: 10.1109/TPEL.2020.3014258.

[34] P. Sanjeev, N. P. Padhy, and P. Agarwal. Autonomous power control and management between standalone dc microgrids. *IEEE Transactions on Industrial Informatics*, 14(7):2941–2950, 2018. doi: 10.1109/TII.2017.2773507.

[35] F. Shahnia, S. Bourbour, and A. Ghosh. Coupling neighboring microgrids for overload management based on dynamic multicriteria decision-making. *IEEE Transactions on Smart Grid*, 8(2):969–983, 2017. doi: 10.1109/TSG.2015.2477845.

[36] P. S. Tadepalli, D. Pullaguram, and M. N. Alam. Resilient dynamic average secondary control for dc microgrids against fdi attacks. *IEEE Transactions on Industry Applications*, pages 1–12, 2025. doi: 10.1109/TIA.2025.3541995.

[37] G. D. L. Torre and T. Yucelen. Adaptive architectures for resilient control of networked multi-agent systems in the presence of misbehaving agents. *International Journal of Control*, 91(3): 495–507, 2018.

[38] U. Vuyyuru, S. Maiti, and C. Chakraborty. Active power flow control between dc microgrids. *IEEE Transactions on Smart Grid*, 10(5):5712–5723, 2019. doi: 10.1109/TSG.2018.2890548.

[39] S. Wei, Y. Jia, Z. Gu, M. Shafiq, and L. Wang. Extracting novel attack strategies for industrial cyber-physical systems based on cyber range. *IEEE Systems Journal*, 17(4):5292–5302, 2023. doi: 10.1109/JSYST.2023.3303361.

[40] C. Weng and Y. Peng. Adaptive and decentralized control strategy to support coordination of multiple dc microgrids considering transmission line impedance. *IEEE Transactions on Smart Grid*, pages 1–1, 2025. doi: 10.1109/TSG.2025.3536159.

[41] Y. Xia, W. Wei, Y. Peng, P. Yang, and M. Yu. Decentralized coordination control for parallel bidirectional power converters in a grid-connected dc microgrid. *IEEE Transactions on Smart Grid*, 9(6):6850–6861, 2018. doi: 10.1109/TSG.2017.2725987.

[42] F. Xiao, S. Liu, B. Wei, F. Fang, and J. Qin. Resilient cooperative control of multiple dc microgrids with interconnection networks against cyber attacks. *IEEE Transactions on Industrial Cyber-Physical Systems*, 3:116–126, 2025. doi: 10.1109/TICPS.2024.3522881.

[43] F. Xiao, Y. Liu, X. Zhang, and B. Wei. Fully distributed event-triggered security control for dc microgrids subject to dos attacks. *IEEE Transactions on Smart Grid*, 16(2):929–941, 2025. doi: 10.1109/TSG.2025.3526835.

[44] G. Yang, L. Herrera, and X. Yao. False data injection attack detection in dc microgrids based on data-driven unknown input observers. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pages 1–1, 2025. doi: 10.1109/JESTPE.2025.3539958.

[45] M. Zaery, P. Wang, W. Wang, and D. Xu. Distributed global economical load sharing for a cluster of dc microgrids. *IEEE Transactions on Power Systems*, 35(5):3410–3420, 2020. doi: 10.1109/TPWRS.2020.2975378.

[46] J. Zhou, M. Shi, Y. Chen, X. Chen, J. Wen, and H. He. A novel secondary optimal control for multiple battery energy storages in a dc microgrid. *IEEE Transactions on Smart Grid*, 11(5): 3716–3725, 2020. doi: 10.1109/TSG.2020.2979983.

[47] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah. A cyber-attack resilient distributed control strategy in islanded microgrids. *IEEE Transactions on Smart Grid*, 11(5): 3690–3701, 2020. doi: 10.1109/TSG.2020.2979160.

[48] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu. Cross-layer

distributed control strategy for cyber resilient microgrids. *IEEE Transactions on Smart Grid*, 12(5):3705–3717, 2021. doi: 10.1109/TSG.2021.3069331.