Cyber-Resilient Control Structures in DC Microgrids with Cyber-Physical Threats

Basati, Amir

DOI (link to publication from Publisher):
10.54337/aau548142466

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

CYBER-RESILIENT CONTROL STRUCTURES IN DC MICROGRIDS WITH CYBER-PHYSICAL THREATS

BY
AMIR BASATI

DISSERTATION SUBMITTED 2023

AALBORG UNIVERSITY
DENMARK

Cyber-Resilient Control Structures in DC Microgrids with Cyber-Physical Threats

Ph.D. Dissertation

Amir Basati

Aalborg University
AAU Energy
Pontoppidanstræde 111
DK-9220 Aalborg

Dissertation submitted: June, 2023

PhD supervisor: Prof. Josep M. Guerrero
Aalborg University, Denmark

Assistant PhD supervisors: Professor Juan C. Vasquez
Aalborg University

Associate Professor Saeed Golestan
Aalborg University

Assistant Professor Najmeh Bazmohammadi
Aalborg University

PhD committee: Associate Professor Amin Hajizadeh (chair)
Aalborg University, Denmark

Associate Professor Nursyarizal Mohd Nor
Universiti Teknologi PETRONAS, Malaysia

Associate Professor Muzamir Isa
Universiti Malaysia Perlis, Malaysia

PhD Series: Faculty of Engineering and Science, Aalborg University

Department: AAU Energy

ISSN (online): 2446-1636
ISBN (online): 978-87-7573-676-8

Published by:
Aalborg University Press
Kroghstræde 3
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Stibo Complete, 2023

Curriculum Vitae

Amir Basati has been a member of the Center for Research on Microgrids (CROM) at Aalborg University since November 2019. Under the guidance of Prof. Josep M. Guerrero, and co-supervised by Prof. Juan C. Vasquez, Amir has been able to conduct research in the field of microgrid control systems. He has also benefited from the opportunity to study abroad for six months in the Division of Decision and Control Systems at KTH, hosted by Prof. Karl Henrik Johansson.

Amir's academic background includes an M.Sc. degree in Electrical Engineering Control Systems from QIAU, Iran, where he was supervised by Prof. Mohammad Bagher Menhaj. Additionally, he obtained his B.Sc. in Biomedical Engineering from the same university. Amir's research focuses on Microgrid Control Systems, with a specific interest in developing cyber-resilient control systems. He is also advancing the field of AI-based control systems for microgrid energy systems.

Abstract

In recent years, the power system has been undergoing increasing pressure to expand its capacity in line with the growth of electricity demand, which has posed significant difficulties for many power industry sectors. Although power generation technologies are improving rapidly, these challenges cannot be overcome without integrating renewable energy sources (RES) into the power grid. RESs, such as Photo Voltaic (PV) panels, wind turbines, etc., and energy storage technologies, can be integrated into the electricity system as a local power generation solution. There has been a growing awareness of the importance of local power generation in recent years, resulting in the emergence of the microgrid (MG) concept. MGs are promising solutions for improving power system efficiency and resilience, thanks to their versatility and controllability. In various applications, DC microgrid (DCMG) distribution systems are preferred over conventional AC microgrid (ACMG) systems for several reasons. These include a simpler control system as most RESs have DC outputs, easier integration for RESs, and the elimination of some of the most challenging issues in ACMGs, such as controlling the reactive power. DCMGs have many potential uses, including but not limited to distribution systems, data centers, electric ships, and transportation. Many concerns regarding the resiliency, reliability, and stability of DCMGs control have been raised in recent years due to the increased penetration of RESs into traditional power grids. To overcome these challenges, coordinated control of power generation resources, energy storage systems, and loads is necessary. Some of the crucial control tasks in DCMGs are balancing the state of charge of batteries, sharing the load current proportionally, regulating the DC bus voltage, and detecting and isolating faults, among others. Due to the diverse control tasks and their different time frames, hierarchical control schemes have received significant attention for DCMGs. In this structure, control tasks are commonly organized into three levels, namely primary, secondary, and tertiary control levels, where primary droop-based controllers are typically decentralized, while secondary and tertiary controllers are normally centralized. Distributed control schemes rely heavily on communication networks, are finding increasing use in the hierarchical control of MGs. Specifically, in DCMGs, the hierarchical control structure with distributed control strategies has been frequently implemented and attracted considerable attention compared with other control structures.

Although distributed control systems have many benefits one major concern is their vulnerability to malicious intrusion due to heavy reliance on data transmission via communication links. Consequently, there is significant interest in developing and employing attack detection strategies for DCMGs that make use of distributed control systems; however, there are still substantial technological gaps that need to be addressed.

This thesis investigates the identification and mitigation of cyber-resiliency challenges faced by DCMG. In this regard, several innovative methods to enhance the resiliency of DCMGs against various types of manipulation, ranging from unknown disturbances to false data injection (FDI) cyber-attacks, are proposed. In the proposed methods, the type and place of intrusion of cyber-physical threats are taken into account. The proposed control methods focus on improving system resilience in both the cyber and physical layers. This is particularly important in the presence of disturbance injections at the primary level of the hierarchical control system. Thus, the proposed methods can be classified as follows based on their level of operation in the hierarchical control system of DCMGs:

Secondary Level

- This project aims to enhance system resilience by developing a Data-driven (DD) framework in the cyber layer of the secondary control system of DCMGs. The proposed framework focuses on detecting and mitigating FDI attacks. First, the intrusion is detected, and then the manipulated signal is amended, and the approximation of the pre-attack value is provided to the control system to keep the system performance within a safe range. In the proposed method, the output voltage and current of the target unit are predicted using real-time machine learning (ML)-based estimators. The residual signal calculated from the real and predicted voltage and current values is then analyzed. The goal is to monitor the state of information exchange in communication links and to determine whether the system is under malicious attack. An online change point detection method is considered to detect any unusual change point in the error signals, which leads to raising the alarm for the presence of an attack in the cyber layer. Moreover, by utilizing a mitigation method, the secondary controllers, instead of receiving a manipulated signal, will receive an amended signal.

- A distributed secondary controller for DCMGs is proposed in this project, which reduces dependence on the information from neighboring units to achieve voltage consensus, current sharing, and reference voltage tracking. Distributed control schemes for DCMG systems rely heavily on data, which can negatively impact their cyber resilience. However, our proposed distributed control method can achieve the same performance with reduced reliance on data transfer. This is achieved by using a distributed finite-time secondary controller from the literature and leveraging the physical equations in the DCMG network to eliminate the

need for voltage information from neighboring units. Local measurements of load, corresponding unit currents, and line resistances are relied upon to achieve voltage consensus. The control law for the unit responsible for tracking reference voltage in an interconnected network setting is modified, freeing it from other responsibilities. Finally, a saturation function is included in the secondary controller with an integrator anti-windup logic to ensure system voltages remain at safe levels.

Primary Level

- To cope with the security challenges, which originate from the primary layer, two different model-based voltage control schemes are proposed in this thesis for local controllers at the primary level of the hierarchical control structures. The first can tackle a wide range of unknown external disturbances and fulfill the primary level control objectives, such as tracking the desired voltage setpoints received from the secondary controller.

- An improved robust voltage control strategy for DC-DC power converters is also proposed in this thesis that can accurately track voltage setpoints, even in the presence of measurement noise, delays, model parameter uncertainties, and external disturbances. This is a challenging task for DC-DC power converters in DCMGs, as the load changes occur instantaneously. By utilizing the proposed scheme, the system can achieve more reliable voltage tracking with lower tracking errors, resulting in improved system performance within the standard range set by the IEEE.

Resumé

I de senere år har elsystemet været udsat for et stigende pres for at udvide sin kapacitet i takt med væksten i elefterspørgslen, hvilket har givet betydelige vanskeligheder for mange elindustrisektorer. Selvom elproduktionsteknologier forbedres hurtigt, kan disse udfordringer ikke overvindes uden at integrere vedvarende energikilder (RES) i elnettet. RES'er, såsom PV paneler, vindmøller osv., og energilagringsteknologier, kan integreres i elsystemet som en lokal elproduktionsløsning. Der har været en voksende bevidsthed om vigtigheden af lokal elproduktion i de seneste år, hvilket har resulteret i fremkomsten af mikronet (MG) konceptet. MG'er er lovende løsninger til forbedring af kraftsystemets effektivitet og modstandsdygtighed takket være deres alsidighed og kontrollerbarhed. I forskellige applikationer foretrækkes DC-mikrogitter (DCMG) distributionssystemer frem for konventionelle AC-mikrogitter (ACMG) systemer af flere årsager. Disse inkluderer et enklere kontrolsystem, da de fleste RES'er har DC-udgange, lettere integration for RES'er og eliminering af nogle af de mest udfordrende problemer i ACMG'er, såsom styring af den reaktive effekt. DCMG'er har mange potentielle anvendelser, herunder men ikke begrænset til distributionssystemer, datacentre, elektriske skibe og transport. Mange bekymringer vedrørende modstandsdygtigheden, pålideligheden og stabiliteten af DCMGs kontrol er blevet rejst i de seneste år på grund af den øgede indtrængning af RES'er i traditionelle elnet. For at overvinde disse udfordringer er koordineret kontrol af elproduktionsressourcer, energilagringssystemer og belastninger nødvendig. Nogle af de afgørende kontrolopgaver i DCMG'er er afbalancering af batteriernes ladetilstand, deling af belastningsstrømmen proportionalt, regulering af DC-busspændingen og detektering og isolering af fejl, blandt andet. På grund af de forskellige kontrolopgaver og deres forskellige tidsrammer har hierarkiske kontrolordninger fået betydelig opmærksomhed for DCMG'er. I denne struktur er kontrolopgaver almindeligvis organiseret i tre niveauer, nemlig primære, sekundære og tertiære kontrolniveauer, hvor primære droopbaserede controllere typisk er decentraliserede, mens sekundære og tertiære controllere normalt er centraliserede. Distribuerede kontrolordninger er stærkt afhængige af kommunikationsnetværk, finder stigende brug i den hierarkiske kontrol af MG'er. Specifikt i DCMG'er er den hierarkiske kontrolstruktur med distribuerede kontrolstrategier ofte blevet implementeret og tiltrukket sig betydelig opmærksomhed sammenlignet med an-

dre kontrolstrukturer.

Selvom distribuerede kontrolsystemer har mange fordele, er en stor bekymring deres sårbarhed over for ondsindet indtrængen på grund af stor afhængighed af datatransmission via kommunikationsforbindelser. Som følge heraf er der en betydelig interesse i at udvikle og anvende angrebsdetekteringsstrategier til DCMG'er, der gør brug af distribuerede kontrolsystemer; der er dog stadig betydelige teknologiske huller, der skal løses.

Denne afhandling undersøger identifikation og afbødning af cyberresiliens-udfordringer, som DCMG står over for. I denne henseende foreslås adskillige innovative metoder til at forbedre modstandsdygtigheden af DCMG'er mod forskellige typer manipulation, lige fra ukendte forstyrrelser til falsk dataindsprøjtning (FDI) cyberangreb. I de foreslåede metoder tages der hensyn til typen og stedet for indtrængen af cyberfysiske trusler. De foreslåede kontrolmetoder fokuserer på at forbedre systemets modstandsdygtighed i både cyber- og fysiske lag. Dette er især vigtigt i tilstedeværelsen af forstyrrelsesindsprøjtninger på det primære niveau i det hierarkiske kontrolsystem. De foreslåede metoder kan således klassificeres som følger baseret på deres driftsniveau i det hierarkiske kontrolsystem af DCMG'er:

Sekundært Niveau

- Dette projekt har til formål at øge systemets modstandsdygtighed ved at udvikle en DD-ramme i cyberlaget i det sekundære kontrolsystem af DCMG'er. Den foreslåede ramme fokuserer på at opdage og afbøde FDI-angreb. Først detekteres indtrængen, og derefter ændres det manipulerede signal, og tilnærmelsen af præangrebsværdien leveres til kontrolsystemet for at holde systemets ydeevne inden for et sikkert område. I den foreslåede metode forudsiges udgangsspændingen og strømmen af målenheden ved hjælp af maskinindlæring (ML)-baserede estimatorer i realtid. Residualsignalet beregnet ud fra de reelle og forudsagte spændings- og strømværdier analyseres derefter. Målet er at overvåge tilstanden af informationsudveksling i kommunikationslinks og at afgøre, om systemet er under ondsindet angreb. En online ændringspunktsdetektionsmetode anses for at detektere ethvert usædvanligt ændringspunkt i fejlsignalerne, hvilket fører til, at der slås alarm for tilstedeværelsen af et angreb i cyberlaget. Ved at anvende en afbødningsmetode vil de sekundære styreenheder, i stedet for at modtage et manipuleret signal, desuden modtage et ændret signal.

- En distribueret sekundær controller til DCMG'er foreslås i dette projekt, som reducerer afhængigheden af informationen fra naboenheder for at opnå spændingskonsensus, strømdeling og referencespændingssporing. Distribuerede kontrolordninger for DCMG-systemer er stærkt afhængige af data, hvilket kan påvirke deres cyberresiliens negativt. Vores foreslåede distribuerede kontrolmetode kan dog opnå den samme ydeevne med reduceret afhængighed af dataoverførsel. Dette

opnås ved at bruge en distribueret finite-time sekundær controller fra litteraturen og udnytte de fysiske ligninger i DCMG-netværket for at eliminere behovet for spændingsinformation fra naboenheder. Lokale målinger af belastning, tilsvarende enhedsstrømme og linjemodstande er påberåbt for at opnå spændingskonsensus. Kontrolloven for den enhed, der er ansvarlig for sporing af referencespænding i en sammenkoblet netværksindstilling, er ændret og frigør den fra andre forpligtelser. Endelig er en mætningsfunktion inkluderet i den sekundære controller med en integrator-anti-windup-logik for at sikre, at systemspændingerne forbliver på sikre niveauer.

Primært Niveau

- For at klare sikkerhedsudfordringerne, som stammer fra det primære lag, foreslås to forskellige modelbaserede spændingsstyringsskemaer i dette speciale for lokale regulatorer på det primære niveau af de hierarkiske styringsstrukturer. Den første kan tackle en bred vifte af ukendte eksterne forstyrrelser og opfylde primære niveau kontrolmål, såsom sporing af de ønskede spændingssætpunkter modtaget fra den sekundære controller.

- En forbedret robust spændingsstyringsstrategi for DC-DC effektomformere er også foreslået i denne afhandling, som nøjagtigt kan spore spændingssætpunkter, selv ved tilstedeværelse af målestøj, forsinkelser, modelparameterusikkerheder og eksterne forstyrrelser. Dette er en udfordrende opgave for DC-DC strømomformere i DCMG'er, da belastningsændringerne sker øjeblikkeligt. Ved at bruge den foreslåede ordning kan systemet opnå mere pålidelig spændingssporing med lavere sporingsfejl, hvilket resulterer i forbedret systemydeevne inden for standardområdet fastsat af IEEE.

Contents

Thesis Details

Thesis Title:	Cyber-Resilient Control Structures in DC Microgrids with Cyber-Physical Threats
Ph.D. Student:	Amir Basati
Main Supervisor:	Prof. Josep M. Guerrero, Aalborg University
Co-supervisors:	Prof. Juan C. Vasquez, Aalborg University
	Associate Prof. Saeed Golestan, Aalborg University
	Assistant Prof. Najmeh Bazmohammadi, Aalborg University

The main body of this thesis consists of the following papers.

[A] Amir Basati, Najmeh Bazmohammadi, Josep M. Guererro, Juan C. Vasquez, "Real-Time Estimation in Cyber Attack Detection and Mitigation Framework for DC Microgrids," *Conference*, International Scientific Conference on Electric Power Engineering (EPE), Brno, Czech Republic, May 2023, **[C1]**.

[B] Amir Basati, Josep M. Guererro, Juan C. Vasquez, Najmeh Bazmohammadi, Saeed Golestan, "A Data-Driven Framework for FDI Attack Detection and Mitigation in DC Microgrids," *Energies Journal*, vol.15, no.22, pp. 8539, 2022, **[J1]**

[C] Amir Basati, Saeid Bashash, Josep M Guerrero, Juan C Vasquez, "Distributed Finite-Time Secondary Control for DC Microgrids with Reduced Internetwork Data Transmission Dependency," *Conference*, International Conference on Future Energy Solutions (FES2023), Vaasa, Finland, June 2023, **[C2]**.

[D] Amir Basati, Jingxuan Wu, Josep M. Guererro, Juan C. Vasquez, "Internal Model-based Voltage Control for DC Microgrids Under Unknown External Disturbances," *Conference*, International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, Netherlands, pp. 1–6, 2022, **[C3]**.

[E] Amir Basati, Josep M. Guererro, Juan C. Vasquez, Ahmad Fakharian, Karl Henrik Johansson, Saeed Golestan"Robust Internal Model-based Voltage Control for DC

Microgrids: An LMI Based H_∞ Control," *Sustainable Energy, Grids and Networks (SEGAN) - Elsevier Journal*, 101094, 2023, [**J2**].

In addition to the main papers, the following publications have also been made.

[1] Jingxuan Wu, Amir Basati, Josep M Guerrero, Juan C Vasquez, Shuting Li, "Kalman filter-based power compensation strategy for Microgrids under uncertain disturbance," *Conference*, International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, Netherlands, pp. 1–5, 2022.

Preface

The work presented in this thesis is a summary of the outcome of the Ph.D. project titled "Cyber-Resilient Control Structures in DC Microgrids with Cyber-Physical Threats." This research endeavor was undertaken at the AAU Energy Department, Aalborg University, Denmark. Throughout my journey, I had the privilege of being guided by the expertise and mentorship of Prof. Josep M. Guerrero as my main supervisor and Prof. Juan C. Vasquez, Associate Prof. Saeed Golestan, and Assistant Prof. Najmeh Bazmohammadi, who served as my co-supervisors, respectively, at Aalborg University.

The duration of this study spanned from November 2019 to June 2023, encompassing a significant milestone during which I had the opportunity to embark on a study abroad program from February 2022 to June 2022. This program took place at KTH University, Division of Decision and Control Systems, under the supervision of Prof. Karl Henrik Johansson. I am sincerely grateful to all my supervisors for their unwavering commitment and dedication throughout this study period. Their exceptional guidance and thoughtful supervision were invaluable to completing this research.

I would also like to express my deepest gratitude to my friends and colleagues in the CROM Research group and AAU-Energy, Aalborg University. Their wonderful companionship, motivation, and cooperative mindset have made this challenging task seem less daunting and more pleasant.

Lastly, but most importantly, I would like to convey my profound appreciation to my family. Their unwavering kindness, unyielding support, and unconditional love have been the guiding light throughout my entire life. I am at a loss for words to express the depth of my gratitude for their presence and influence on my journey.

With this thesis, I hope to contribute to the ever-growing field of distributed cyber-resilient control structures for DC microgrids, addressing the challenges posed by cyber-physical threats. I sincerely hope this work will be of value to researchers, practitioners, and decision-makers in the field, inspiring further advancements and fostering a safer and more secure energy landscape.

Amir Basati
Aalborg University, June 29, 2023

Part I

Extended Summary

List of Figures

List of Tables

Acronyms

ACMG AC Microgrid.

ANFIS Adaptive Neuro-fuzzy Inference System.

BCPD Bayesian Change Point Detection.

CC Conventional Controller.

CP Change Point.

DCMG DC Microgrid.

DD Data-driven.

DER Distributed Energy Resource.

DG Distributed Generator.

DOF Degree of Freedom.

DoS Denial of Service.

DT Decision Tree.

ESS Energy Storage System.

EV Electric Vehicle.

FDI False Data Injection.

FFNN Feed-forward Neural Network.

HMI Human Machine Interface.

IAE Integral Absolute Error.

IMC Internal Model-based Control.

IMVC Internal Model-based Voltage Control.

LAN Local Area Network.

MG Microgrid.

MITM Man In The Middle.

ML Machine Learning.

OCPD Online Change Point Detection.

PMU Phasor Measuring Unit.

PnP Plug-and-Play.

PV Photo Voltaic.

RES Renewable Energy Source.

RIMVC Robust Internal Model-based Voltage Control.

RMSE Root Mean Square Error.

RTU Remote Terminal Unit.

SCADA Supervisory Control and Data Acquisition.

SD Standard Deviation.

SM Smart Meter.

VSC Voltage Source Converter.

Chapter 1: Introduction

1.1 Motivation

In recent times, the integration of Microgrid (MG)s has been acknowledged as a practical approach to enhancing the reliability and efficiency of the power grid [1]. Also, MGs are ideal solutions for improving the resilience of electricity systems. During extreme events such as natural disasters or malicious cyber activities, MGs are highly effective due to their self-healing capabilities.

In the contemporary world, DC Microgrid (DCMG)s have become increasingly popular as compared to the traditional AC Microgrids (ACMGs) [2]. This shift in trend can be attributed to various factors that have contributed to the rise of DCMGs. DCMGs are a popular choice because of their simpler control systems, which work well with the majority of RESs such as PV systems, fuel cells, and batteries that have DC outputs [3], thereby facilitating their integration. Unlike ACMGs, DCMGs do not present challenges related to reactive power flow, power quality, and frequency regulation [4]. The adaptability and versatility of DCMGs have made them a compelling option for modernizing traditional power systems and making the green transition [3].

There is a wide variety of control system structures for DCMGs, including centralized, decentralized, distributed, etc. [5, 6], but thanks to the rapid progress in communication technologies, the distributed control systems, which rely on data transmission via the communication links between the various units, have been shown to be the most efficient approach [7].

Although distributed control systems have considerable advantages, it must be acknowledged that their heavy dependence on communication links for data transmission exposes them to substantial security threats. Cyber-attacks could have severe consequences for the entire system, leading to power production interruption that might endanger human lives and impose high costs on the system [8, 9].

Similar to other real-life applications, a range of disturbances are expected to be present in MGs, potentially impacting their performance [10]. These disturbances may come in various forms, including but not limited to power surges, voltage fluctuations, electromagnetic interference, and mechanical vibrations. Therefore, operators must be

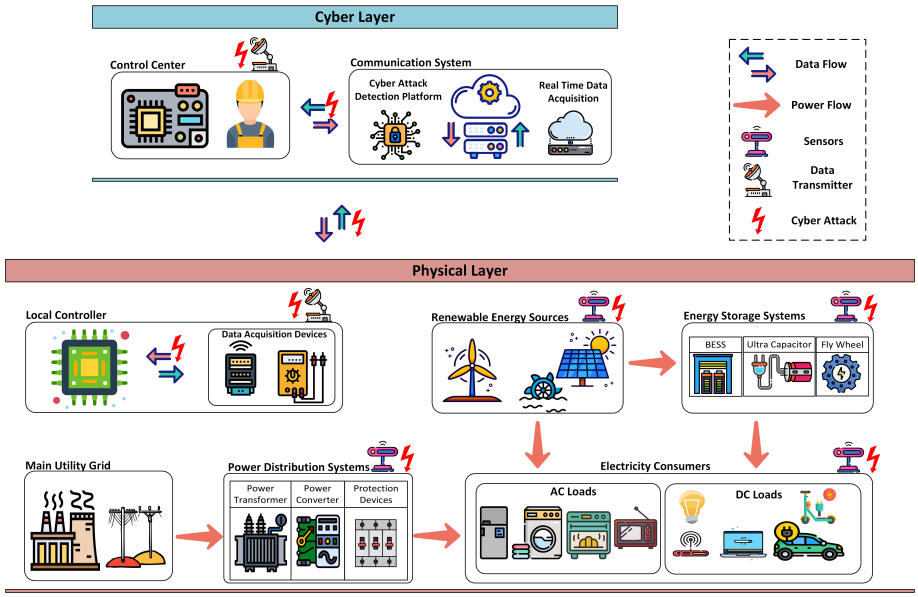

Fig. 1.1: MG integration into the power system.

aware of the potential sources of these disturbances and take appropriate measures to mitigate their effects to ensure optimal system performance and prevent any potential damage or downtime [11]. In Fig. 1.1, a power system that incorporates RESs, Energy Storage Systems (ESSs), and other components is illustrated. This system is typically divided into two layers: physical and cyber layers. The physical layer comprises the physical infrastructure, while the cyber layer involves the communication and control systems. The image also highlights areas of vulnerability that cyber-attacks could target [8].

According to the above discussion, it is imperative to design a robust and cyber-resilient control scheme to protect the DCMG systems in the presence of cyber-physical threats and ensure their efficient and reliable operation.

1.2 Background

This thesis report showcases the results of a Ph.D. project that has received support from the Villum Fonden. The study was conducted at the Center for Research On Microgrids (CROM). The main objective of this development initiative is to devise innovative cyber-resilient control detection and mitigation strategies for DCMG systems. The project aims to develop novel hierarchical control frameworks that can withstand both False

Data Injection (FDI) cyber attacks and external disturbances realizing cyber-resilient DCMGs. Here are the sub-objectives of this Ph.D. project:

- At the secondary level of the hierarchical DCMG control structure
  - Using data-driven techniques to develop a framework for both detecting the presence of FDI cyber-attacks and mitigating their destructive effects.
  - Developing a distributed finite-time secondary control for DCMGs with less reliance on network data transmission.
- At the primary level of the hierarchical DCMG control structure
  - Developing a model-based control scheme to enhance the robustness of the DCMG considering the wide range of disturbances and model parameter uncertainties.

1.3 DC Microgrids, Control Systems and Cyber Security Challenges

1.3.1 Why Microgrids?

The current need for MGs to modernize the conventional power systems can be attributed to several key factors. Firstly, there is an increasing demand for reliable and resilient power supply, particularly under extreme events such as cyber intrusion and natural disasters [1]. Conventional centralized power systems are becoming highly vulnerable to disruptions, as they rely on a complex network of transmission lines and substations, and are reaching their maximum capacity to respond to customer demands. Conversely, MGs operate as localized energy systems that can disconnect from the main grid and function autonomously. Therefore, they feature higher resilience, allowing critical facilities such as hospitals, emergency response centers, and remote communities to maintain power supply even during grid outages [12].

Secondly, integrating RESs into the power grid has gained significant momentum in recent years. Solar PV panels, wind turbines, and other clean energy technologies are becoming more affordable and accessible. However, their intermittent nature poses challenges to the stability and reliability of the conventional grid. MGs provide an effective solution by efficiently managing the integration of RESs. They can locally balance energy generation and demand, store excess power in batteries, and dispatch electricity as needed, thereby reducing the stress on the main grid and providing a more sustainable energy mix [1]. Furthermore, the rise of Distributed Energy Resources (DERs), such as rooftop solar panels and energy storage systems, has contributed to the popularity of MGs [13]. With the declining costs of solar and battery technologies, more individuals and businesses are adopting these decentralized energy solutions. MGs

offer an ideal platform for integrating and managing these DERs effectively [14]. They allow consumers to generate their own electricity, reduce reliance on the grid, and even sell excess energy back to the main grid. MGs empower individuals and communities to participate actively in the energy market, fostering a sense of energy independence and supporting the transition to a more decentralized energy system [15].

Thirdly, the increasing electrification of transportation systems, especially the growing adoption of Electric Vehicles (EVs), drives the need for more efficient and reliable charging infrastructure [16]. MGs can play a crucial role in supporting this transition by providing localized power supply for EV charging stations. MGs can ensure a sustainable and cost-effective charging infrastructure by integrating RESs and ESSs, reducing stress on the main grid and minimizing reliance on fossil fuels [17].

According to the factors mentioned above, the popularity of MGs in modernizing the conventional power system can be attributed to their ability to support EVs charging infrastructure, integrate DERs, and enable active consumer participation. As these trends continue to reshape the energy landscape, MGs play critical roles in future energy systems [18].

1.3.2 Typical DC Microgrids

MGs consist of various power generation sources, ESSs, and multiple loads, which are connected together through the distribution lines. The control system of MGs is implemented both locally at the device level and at higher levels relying on communication links [**Paper C**]. There are two modes of operation for MGs: grid-connected and islanded mode, depending on whether they are connected to the main grid or not. [19]. Due to the previously mentioned reasons, DCMGs have gained significant attention compared to ACMGs from academic and industry experts [20, 21]. As most of the RESs (like PVs and fuel cells) and ESSs (like batteries) and household loads are DC in nature [2], the development process of DCMGs is more straightforward. A typical DCMG configuration is shown in Fig. 1.2. [2, 22]. However, despite the potential advantages of DCMG, there are still significant gaps in their protection and cyber resiliency that must be addressed. This is essential to ensure that DCMGs remain reliable and stable even during extreme events.

1.3.3 Control Systems for DC Microgrids

1.3.3.1 Hierachical Control Structures of Microgrids

To ensure the efficient and cost-effective operation of DCMGs, it is necessary to coordinate multiple sources, loads, and energy storage devices. Hierarchical control schemes have gained significant attention in recent years due to their ability to meet various operating goals with different time scales, while ensuring the resilience, reliability, and

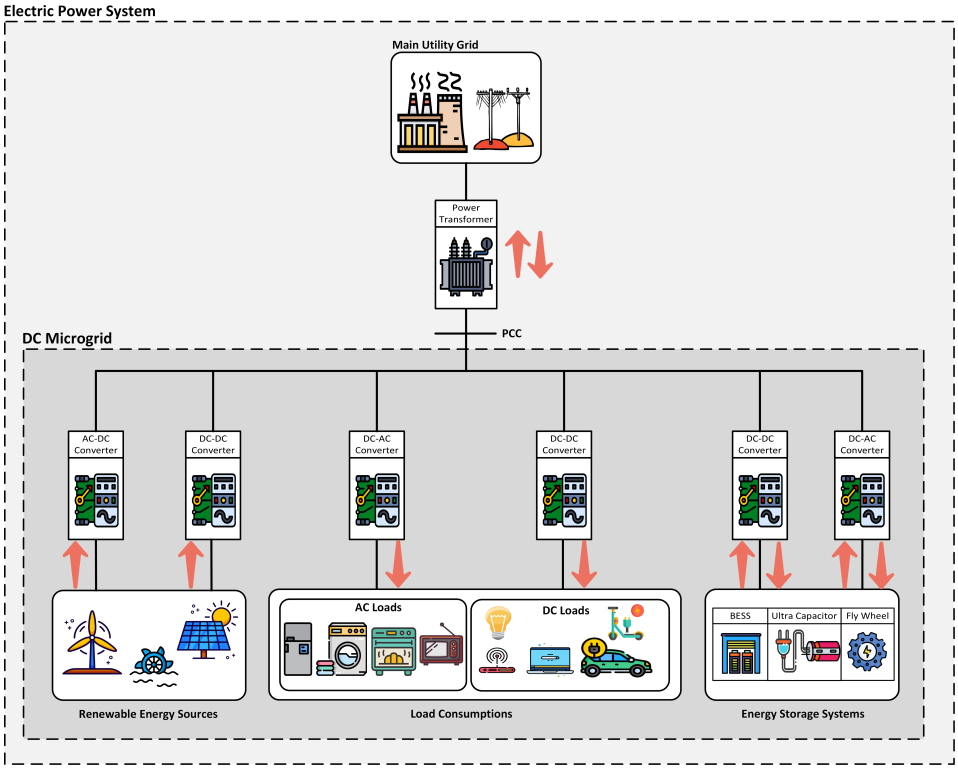

Fig. 1.2: A Typical DCMG.

stability of DCMGs [6]. Several different hierarchical control schemes have been investigated for DCMGs [23, 24]. In general, the primary, secondary, and tertiary control levels make up the three control levels of hierarchical control structures.

- **Primary Control** At the lowest level of control, local controllers such as voltage and current control are implemented to attain different control objectives, including current/voltage regulation, preliminary power-sharing, and fast response to converter dynamics. Primary control structures incorporate droop control to effectively eliminate circulating current consequences, which is not achievable with just voltage and current control. However, as primary controllers lack access to data from other connected units, upper-level controllers must provide them with the appropriate set-points based on the DCMG's overall status to ensure the required system performance. Another control objective of primary control is to regulate energy storage, such as the state of charge in batteries, which can modify

the droop coefficient and enhance power sharing between energy storage and the main power grid [25].

- **Secondary Control** In DCMGs, the secondary control level plays a crucial role in managing power flow between connected units, ensuring proper voltage levels, and improving power quality. It serves as a vital link between the primary and tertiary control levels, enhancing the overall performance of the hierarchical control structure [26, 27]. The secondary controller can enhance the primary control's effectiveness by providing appropriate voltage set-points. Due to line impendence, which might result in voltage drop and poor current sharing, the primary control alone may not maintain the desired system performance without the support of a proper secondary control system [28].

- **Tertiary Control** A system-level control is still required even though the primary and secondary controllers are used to control the voltage and current. This is especially important in the case with more than one DCMG, such as in DCMG clusters, where several DCMG are interconnected in both islanded and grid-connected modes. The third layer is typically used for high-level power management through communication links. This involves changing or modifying the parameters in lower layers according to important factors such as cost, user demands, weather conditions, etc. [29]. Power sharing among the Distributed Generators (DGs) of an islanded MG and management of power between the MG and the main grid are examples of tertiary control tasks in the context of power management [30].

The hierarchical control scheme with distributed control strategies has gained significant popularity in DCMGs [31]. However, there are still significant technological gaps that need to be addressed. Distributed secondary control involves generating the suitable control signal, which is the dynamic set-point for the primary controller, by utilizing the transmitted data from the connected neighbors. As previously stated, accomplishing the desired control objective for a hierarchical distributed control structure in DCMGs relies heavily on the precision of data [8, 9].

1.3.3.2 Communication Systems in Microgrids

Distributed control schemes have become increasingly popular in the control of MGs thanks to their massive advantages and the recent advancements in communication technologies. Distributed control systems involve the coordination and control of multiple devices and subsystems distributed across the MG. Thereby, a reliable communication system is of utmost importance for MGs Communication systems enable real-time monitoring, control, and coordination, allowing operators to respond promptly to changes and disturbances. There are various communication-dependent components in a MG, such as control centers, substations, Human Machine Interfaces (HMIs), Phasor Measuring Units (PMUs), Remote Terminal Units (RTUs), and Smart Meters (SMs) [32, 33].

These components need to communicate with each other to optimize the overall performance of the MG.

Wired and wireless communication technologies are the two primary options for communication in a MG system. Wired communication via Supervisory Control and Data Acquisition (SCADA) systems and Local Area Networks (LANs) provides reliable and secure data transmission, making it ideal for use in situations where security is the main concern. On the other hand, wireless communication technologies like Wi-Fi, Zigbee, and cellular networks are more flexible and enable mobility. Reliable communication links are necessary for real-time monitoring and control of various components, timely and accurate feedback, and effective coordination among distributed devices. Effective communication in a MG system enhances system stability, reliability, and resilience, enabling efficient energy management and integration of Renewable Energy Sources (RESs). To ensure the seamless operation of MG components, reliable communication links must be established to exchange critical control signals and data. Here are some key factors necessary for such links:

- A reliable communication link allows essential information, such as voltage levels, power generation, and load demand, to be shared promptly, enabling the system to respond quickly to any changes. For instance, if a sudden increase in load demand is detected in a specific region of the MG, the control system can communicate this information to relevant devices to adjust their output accordingly, thereby preventing instability or overload.

- In addition to prompt response, reliable communication links also ensure timely and accurate feedback from devices to the control system. This feedback is crucial for monitoring system performance and health, implementing control strategies to improve efficiency, and coordinating the operation of MG components. By maintaining a robust and uninterrupted communication link, the distributed control system can balance power generation and consumption and respond to grid disturbances or faults in a coordinated and efficient manner.

1.3.4 Cyber Vulnerabilities in DC Microgrids

The technological developments in communication and intelligent devices have allowed for the development of modern MG systems toward cyber-physical systems capable of the generation and distribution of electrical energy through the coordinated use of computational algorithms, physical devices, and inter-device communication. However, DCMGs are not immune to cyber vulnerabilities that might severely affect their operation and performance.

The possibility of unauthorized access to the control system and its associated components is a significant weakness. Access to the control system by an adversary opens

the door to the manipulation of crucial settings, disruption of communication, and potential physical damage to the MG infrastructure. This threatens the reliability of the MG and the safety of its users by increasing the likelihood of power outages and the loss of command.

The risk of data breaches is another cyber vulnerability in DCMGs. MGs are unable to operate without having the capability to remotely monitor and control their components. Sensitive data, such as energy consumption patterns or grid configurations, could be accessed or tampered with by unauthorized individuals if the communication network or data storage systems are not adequately secured.

In addition, misconfiguration makes the network extremely vulnerable to malicious activities, making it the most attractive point of attack. There may also be an increase in the cyber threat due to an increase in system connectivity and certain operational technical irregularities.

To mitigate these vulnerabilities, it is crucial to implement robust cybersecurity measures in DCMGs. This includes deploying firewalls, intrusion detection systems, and encryption protocols to safeguard the communication infrastructure and prevent unauthorized access. Additionally, establishing strong authentication and access control mechanisms, such as multi-factor authentication and role-based access, can significantly reduce the risk of unauthorized access. Overall, a comprehensive cybersecurity strategy that considers both technical and operational aspects is essential to protect DCMGs from cyber threats and ensure the reliable and secure delivery of electricity.

There are several types of cyber-attacks in DCMGs, namely FDI [34], Denial of Service (DoS) [35, 36], Hijacking [37], Replay [38], and Man In The Middle (MITM) attacks [39].

Measurements taken from the grid for usage in control systems and system control variables are common targets of intrusion and cyberattacks in a distributed control system [Paper B]. From the control perspective, cyber-attacks can lead to unbalanced power situations, bus voltage deviations, and grid instability. The most prominent type of cyber-attack that has been reported more recently is the FDI attack [40]. In FDI attacks, the attacker adds or subtracts false data from the real values from the sensor measurements or control variables. There are instances where malicious activities can be minimized or avoided by implementing physical protection methods. For instance, hard-wiring the sensor outputs can provide physical layer security [41].

1.4 Research questions and hypothesis

Due to the rapid increase in the integration of DCMGs in power systems to integrate as many RESs as possible, the vast majority of power system experts are increasingly concerned about the security of DCMGs due to the growing number of cyber-attacks. To mitigate the damage caused by these malicious events, it is critical to establish robust attack detection mechanisms capable of quickly detecting and isolating the affected

system components. This reduces the risk of power outages or disruptions and ensures that the MG system remains stable and reliable. It is important to note that in order to avoid misdiagnosis of an intrusion, effective malicious activity detection methods must be capable of distinguishing between the effects of system load changes and those caused by malicious activities.

In this regard, a number of research questions have been raised to investigate the cyber security of DCMGs and develop effective methods for detecting and mitigating cyber-attacks.

- What are the key requirements and measures for the resilient operation of DCMGs?
- How can DD techniques be employed to detect and mitigate cyber-attacks in DCMGs considering the massive data available from sensors?
- How to ensure a system performs as expected despite a wide range of disturbances, such as variations in the local load voltage, plug-and-play operation, uncertainties in the model parameters, noises in the measurements, and delays in the system as dictated by IEEE standards.
- How a cyber attack detection and mitigation method should distinguish between regular voltage changes caused by normal load profile changes and cyber-attack injection, considering that both of which have similar effects on data transmitted (each unit output voltage and current) in the cyber layer?

According to the abovementioned research questions, the following hypotheses are considered in this thesis.

- Among the wide range of cyber-attack types, the FDI attack, which has become increasingly common in recent years and is regarded as one of the most significant forms of cyber attacks [42], is considered in this study.
- Despite the fact that the internal and external disturbances, as well as the model parameters' uncertainties, are unknown, it is assumed that they are bounded to known constant values.

1.5 Outline of the Thesis

The thesis is meticulously crafted based on an in-depth review of the Ph.D. student-published papers. It provides an extended summary that covers a wide range of topics, including the project's motivation, background, research questions, hypotheses, and a detailed description of the papers extracted from this thesis. To present the papers published from this research systematically, Fig. 1.3 shows the thesis structure and each

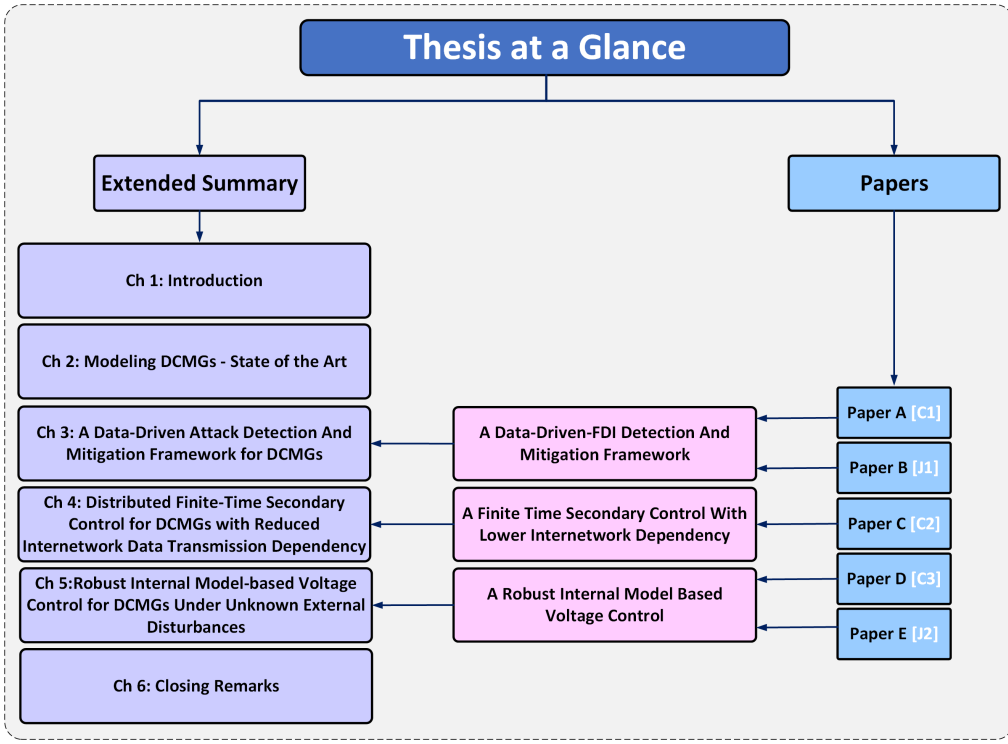

Fig. 1.3: Thesis at a glance.

chapter's connection to each published paper. This meticulous approach ensures that all relevant information on the published papers is presented clearly.

Paper A The primary objective of Paper A is to propose a reliable estimator that leverages the power of Adaptive Neuro-fuzzy Inference System (ANFIS) for the purpose of detecting and monitoring malicious activities in real-time, particularly those related to FDI Attacks in DCMGs with distributed control systems. By employing this estimator, it is possible to estimate the output voltage and current of each DG unit with a high level of accuracy. To determine its effectiveness, a comparative analysis is performed with two other Machine Learning (ML)-based estimators.

Paper B This paper presents a comprehensive real-time framework for detecting and mitigating FDI attacks in DCMGs. The proposed framework consists of DD methods and a supervised algorithm that accurately estimates all DGs' output voltage and current. The conducted analyses concluded that ANFISs are preferred due to their efficiency, simplicity, and low computational burden. The framework utilizes the On-

line Change Point Detection (OCPD) technique, which removes the requirement for a fixed threshold set by the user for residual analysis. This advanced feature ensures the framework is always up-to-date in detecting and preventing FDI attacks.

Paper C This paper aims to develop a distributed secondary controller for DCMGs that can achieve voltage consensus, current sharing, and reference voltage tracking with minimal reliance on information from neighboring units. A distributed finite-time secondary controller from the literature is employed. It is worth mentioning that leveraging the physical relationships within the DCMG network, removes local controllers' dependence on voltage information from adjacent units. Therefore, local measurements of load and unit currents, as well as line resistances, are used to attain voltage consensus throughout the network. Additionally, a modified version of the control law for the unit responsible for tracking the reference voltage from an external tertiary controller in the corresponding network setting is suggested. According to the proposed method, this unit is released from all other responsibilities except for reference voltage tracking. Moreover, a saturation function on the secondary controller with an integrator anti-windup logic is suggested to maintain system stability.

Paper D This paper investigates the possibility of implementing a two-Degree of Freedom (DOF) Internal Model-based Voltage Control (IMVC) system for DCMGs. The main issue regarding voltage control in DC/DC converters is the ability to maintain voltage reference tracking in the presence of unknown external disturbances and measurement noise while the load is continuously changing. To address this problem, a voltage control framework is proposed in this paper that leverages a plug-and-play model-based voltage controller for Voltage Source Converters (VSCs) at the primary control level. The efficacy of this control scheme is evaluated by testing it against unknown external disturbances, rapid voltage reference changes, and load profile changes across multiple case study scenarios, which allows for a comprehensive assessment of the system's capabilities.

Paper E The aim of Paper E is to develop a Robust Internal Model-based Voltage Control (RIMVC) strategy for DCMGs that can withstand internal and external disturbances of an unknown magnitude within the known boundaries. Maintaining a steady voltage reference in the presence of model parameter uncertainties in DC-DC converters of DCMGs can be quite challenging. This challenge is further complicated by measurement noise, system delays, and load changes. In response to this challenge, this thesis proposes a voltage control scheme with Plug-and-Play (PnP) capability. The proposed approach involves developing a modified Internal Model-based Control (IMC) for regulating the voltage of DC-DC converters, which aims to improve the overall performance and robustness of the system. The proposed control method follows a cascade structure consisting of two crucial components. The first component is a modified IMC

strategy that aims to appropriately track the voltage set-points generated by the secondary control in the hierarchical control structure. This control system is crucial, as it provides the foundation for the control scheme and ensures that the system operates optimally under normal conditions. The second component involves incorporating the H_∞ control method to enhance the system's robustness against the DC-DC converter parameter uncertainties and disturbances. This feedback control component is designed to mitigate the impact of unknown disturbances and parameter variations, ensuring that the system remains stable and reliable. The proposed control scheme significantly improves the voltage control capabilities of DCMGs as well as their overall performance and robustness.

Chapter 2: DCMGs Modeling and Formulations

In this chapter, the main focus is to present the system configuration of DCMGs that is used in this thesis and their mathematical model. In order to evaluate the effectiveness of the proposed methods in this thesis following various control goals within multiple layers of the hierarchical control scheme, two distinct DCMG testbeds with different system configurations and the number of DG units will be used.

2.1 System Description

In order to accurately assess the effectiveness of the control system for DCMGs, it is common practice to utilize a test system that incorporates RES units, typically with a DC source, that is connected via DC-DC converters. Additionally, DC loads are connected to all DG units through impedance-distributed lines, creating a comprehensive system for evaluating the performance of the control system. This approach allows for a thorough analysis of the efficiency of the DCMGs control systems in real-world scenarios. The diagram depicted in Fig. 3.1 represents a DCMG system that utilizes a hierarchical control system with a distributed control strategy in the secondary layer. This hierarchical scheme involves multiple levels of control and coordination, allowing for effective management and optimization of the MG's distributed energy resources.

2.2 Mathematical Modeling

The overall configuration of the DCMG testbed being studied in this thesis can be seen in Fig. 2.2. To facilitate the modeling process, a simple DCMG consisting of two units, i and j, is considered in this section. These two DG units are linked together through a distribution line (R_{ij} and L_{ij}). The model presented in this section comprises two time-varying DC sources, namely $V_{dci}(t)$ and $V_{dcj}(t)$. Moreover, two DC-DC buck converters are incorporated into the model. These converters have appropriate filter parameter

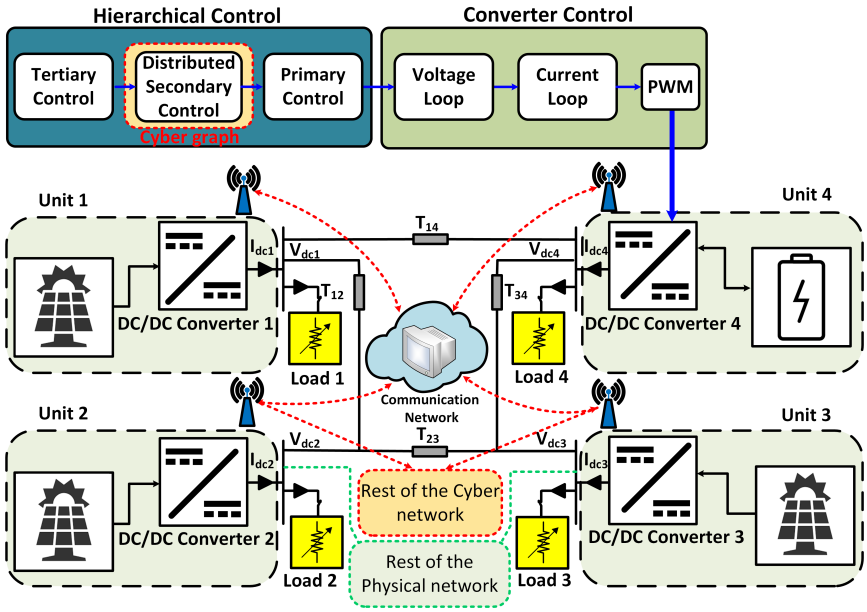

Fig. 2.1: A typical DCMG with a hierarchical control system [Paper B].

values such as R_i, L_i, and C_i. The mathematical equations of the model may differ depending upon the type of DC-DC converter employed. In addition, two controlled current sources, denoted $I_L i$ and $I_L j$, represent the local loads.

Fig. 2.2 and 2.3 display the comprehensive layout of two DCMG testbeds in which a distribution line with R_{ij} and L_{ij} connects two DG units i and j. The two distinct DCMG models in Fig. 2.2 and Fig. 2.3 incorporate two DC-DC buck converters and two DC-DC boost converters, respectively.

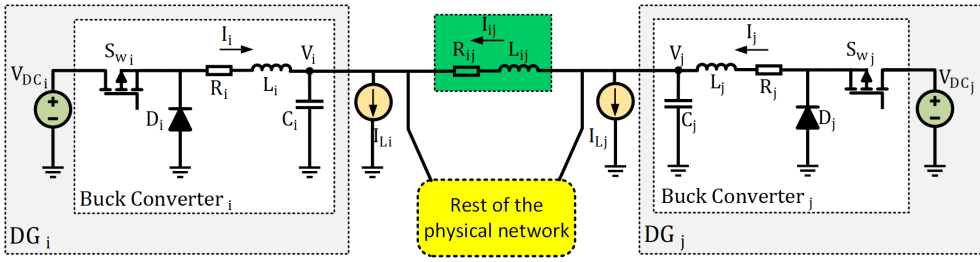

Fig. 2.2: The configuration of the DCMG under study with Buck DC-DC converters [Paper E].

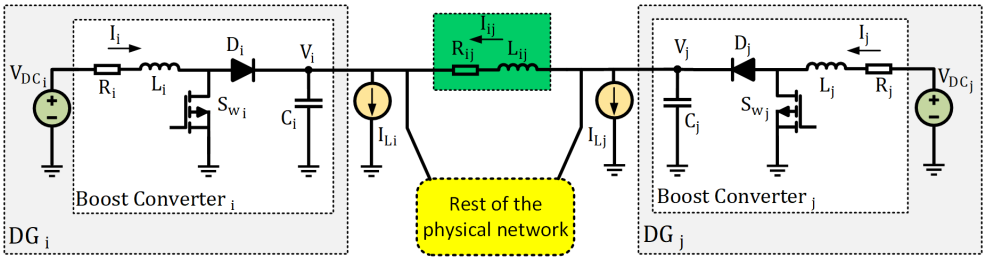

Fig. 2.3: The configuration of the DCMG under study with Boost DC-DC converters [Paper E].

The parameters of the two considered DCMG systems, one with DC-DC boost converters and one with DC-DC buck converters, are chosen using the model provided in [43].

• **DCMG with DC-DC Buck Converter**

$$\text{DG}\, i: \begin{cases} \frac{dV_i}{dt} & = \frac{1}{C_i} I_i - \frac{1}{C_i} I_{L_i} + \frac{1}{C_i} I_{ij} \\ \frac{dI_i}{dt} & = -\frac{1}{L_i} V_i - \frac{R_i}{L_i} I_i + \frac{d_{buck_i}}{L_i} V_{dc_i} \end{cases} \tag{2.1}$$

$$\text{Line}\, ij: \frac{dI_{ij}}{dt} = -\frac{R_{ij}}{L_{ij}} I_{ij} + \frac{1}{L_{ij}} V_j - \frac{1}{L_{ij}} V_i \tag{2.2}$$

This thesis considers a quasi-stationary model for the understudied DCMG, inspired by [44, 45]. If line transients have fast time constants, we can simplify distribution lines models by neglecting line dynamics and using quasi-stationary dynamics with small inductance parameters.

$$\frac{dI_{ij}}{dt} = 0 \tag{2.3}$$

Therefore, Eq. (2.2) can be simplified as follows:

$$I_{ij} = \frac{V_j - V_i}{R_{ij}} \tag{2.4}$$

The governing differential equations of DG_i are obtained by substituting Eq. (2.4) into Eq. (2.1) as follows:

$$\text{DG}\, i: \begin{cases} \frac{dV_i}{dt} & = \frac{1}{C_{t_i}} I_{t_i} - \frac{1}{C_{t_i}} I_{L_i} + \frac{1}{C_{t_i} R_{ij}} V_j - \frac{1}{C_{t_i} R_{ij}} V_i \\ \frac{dI_{t_i}}{dt} & = -\frac{1}{L_{t_i}} V_i - \frac{R_{t_i}}{L_{t_i}} I_{t_i} + \frac{d_{buck_i}}{L_{t_i}} V_{dc_i} \end{cases} \tag{2.5}$$

• **DCMG with DC-DC Boost Converter**

$$\mathrm{DG}\, i : \begin{cases} \frac{dV_i}{dt} & = \frac{1-d_{boost_i}}{C_i} I_i - \frac{1}{C_i} I_{L_i} + \frac{1}{C_i} \sum_{j \in N_i} \frac{V_j - V_i}{R_{ij}} \\ \frac{dI_i}{dt} & = -\frac{1-d_{boost_i}}{L_i} V_i - \frac{R_i}{L_i} I_i + \frac{1}{L_i} V_{dc_i} \end{cases} \tag{2.6}$$

where d_{buck_i} and d_{boost_i} are the duty cycles of the DC-DC buck converter and DC-DC boost converter of the DG_i, respectively.

2.2.1 DCMG State Space Model

The state-space model of a system with disturbance in the time domain can be represented as follows:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) + En(t) \end{aligned} \tag{2.7}$$

This model is commonly used in various applications such as control systems, signal processing, and estimation problems. It accurately predicts the behavior of complex systems while considering any external disturbances that may affect the system's dynamics [46]. Using the differential equation mentioned earlier for DCMG, the state-space equations for DG_i with Buck converter can be obtained from Eq. (2.5), as follows:

$$\begin{bmatrix} \dot{V}_i \\ \dot{I}_i \end{bmatrix} = \begin{bmatrix} -\sum_{j \in N_i} \frac{1}{C_i R_{ij}} & \frac{1}{C_i} \\ \frac{1}{L_i} & \frac{R_i}{L_i} \end{bmatrix} \begin{bmatrix} V_i \\ I_i \end{bmatrix} + \begin{bmatrix} -\frac{1}{C_i} & \sum_{j \in N_i} \frac{1}{C_i R_{ij}} & 0 \\ 0 & 0 & \frac{1}{L_i} \end{bmatrix} \begin{bmatrix} I_{L_i} \\ V_j \\ d_{buck_i} V_{dc_i} \end{bmatrix} \tag{2.8}$$

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_i \\ I_i \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I_{L_i} \\ V_j \\ d_{buck_i} V_{dc_i} \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} n_i(t) \tag{2.9}$$

The states are represented by $\begin{bmatrix} V_i & I_i \end{bmatrix}^T$, with $u_i = d_{buck_i} V_{dc_i}$ as the input, and unknown external disturbances $n_i(t)$.

2.2.2 Studied DC Microgrids testbed

- The first testbed system specification with 4 DG units is represented in Fig. 2.4 and the specification are given in tables 2.1 and 2.2, which is employed for evaluation of the proposed control scheme in Chapters 3 to 5.

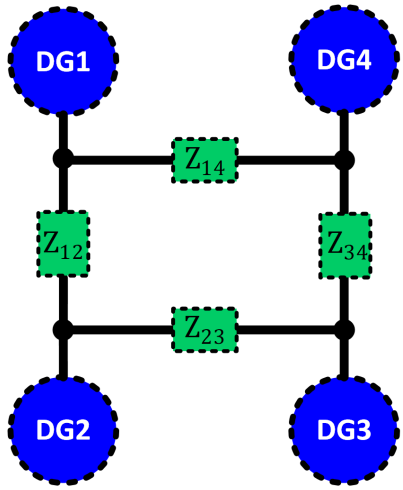

Fig. 2.4: Testbed 1 [Paper B].

Table 2.1: Specifications of Testbed 1 [Paper B].

DG #	DC-DC Boost Converter Parameters			DC Source	Nominal Power
	C_t (μF)	L_t (mH)	I_{dc}^{max}(A)	(V)	(kW)
1	270	3.1	15	110	$\simeq 4.7$
2	250	3.0	15	105	$\simeq 4.7$
3	270	3.1	5	110	$\simeq 3.1$
4	250	3.0	5	105	$\simeq 3.1$

Table 2.2: Settings for distribution lines [Paper B].

Line Impedance $\mathbf{T}_{ij}$	$R_{ij}(\Omega)$	$L_{ij}(\mu\text{H})$
T_{12}	0.6	50
T_{14}	1.0	60
T_{23}	1.8	65
T_{34}	3.0	75

- The second testbed system specification with 6 DG units is presented graphically in Fig. 2.5 and the specifications are given in tables 2.3 and 2.4, which is employed for evaluation of the proposed control scheme in Chapter 5.

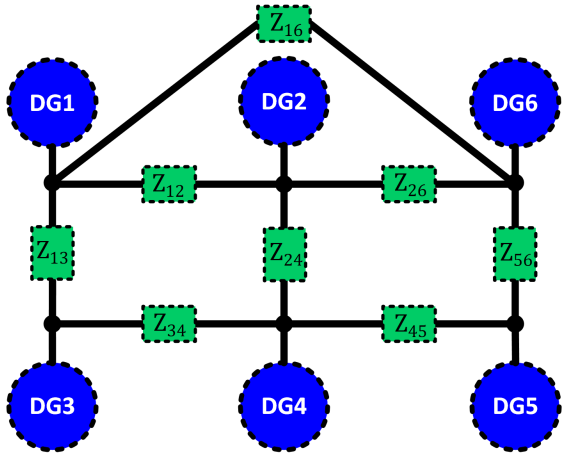

Fig. 2.5: Testbed 2 [Paper E].

Table 2.3: Specifications of Testbed 2 [Paper E].

DG #	DC-DC Buck Converter Parameters			Load (Ω)	Voltage reference (V)
	$R_t(\Omega)$	L_t (mH)	C_t (mF)		
1	0.2	1.8	2.2	9	47.9
2	0.2	2.0	2.1	7	48.0
3	0.3	2.0	1.9	18	47.7
4	0.1	1.8	1.8	4	48.0
5	0.6	2.8	2.2	6	47.8
6	0.2	1.8	2.1	7	48.1

Table 2.4: Settings for distribution lines [Paper E].

Line Impedance $\mathbf{Z}_{ij}$	$R_{ij}(\Omega)$	L_{ij}(mH)
Z_{12}	0.05	1.8
Z_{13}	0.06	1.7
Z_{34}	0.07	1.7
Z_{24}	0.08	1.8
Z_{45}	0.07	1.8
Z_{16}	0.06	1.5
Z_{56}	0.05	1.3

Chapter 3: Data-Driven Cyber Secured Guard for DCMGs: An Attack Detection and Mitigation Framework

3.1 Introduction

The main objective of this chapter is to introduce a framework for detecting and mitigating cyber attacks that inject false data to the system. The framework is designed to ensure the secondary controller receives secure input data, even when an attacker adds false data to the system. To achieve this, we use ANFIS to estimate the voltage and current output of each unit. Additionally, an OCPD scheme is employed to identify any malicious activity following the differences between the estimated and real data.

3.2 Real-Time Output Estimation for Attack Detection and Mitigation

To detect cyber-attacks on distributed control systems accurately, it is crucial to have accurate and efficient real-time voltage and current estimators that do not impose high stress on computational resources. These systems are often targeted by hackers who manipulate measurement and control variables, introducing false data into critical components. To tackle this problem, a framework is developed that utilizes residual analysis to compare estimated and actual sensor measurements. To implement this framework, an efficient online estimator is necessary. After evaluating several DD-based estima-

tors based on criteria such as accuracy, precision, recall[1], and F1 score[2], ANFIS was selected as a supervised method with a satisfactory compromise between computation affordability, reliability, robustness, and accuracy for output voltage and current estimation. The performance of the proposed attack detection framework is evaluated using the abovementioned criteria.

3.2.1 Adaptive Neuro-Fuzzy Inference Systems (ANFIS) Design

In various power grid and MG applications, both ANNs and FIS are utilized for different purposes like load forecasting and state estimations. ANFIS combines the learning ability of ANNs with the inference ability of rule-based fuzzy logic control, as explained in [47, 48]. Fuzzy theory-based FIS components map inputs to outputs, as illustrated in Fig. 3.1. Standard ANFIS architecture comprises fuzzification, implication, normalization, defuzzification, and combination, as depicted in Fig. 3.2.

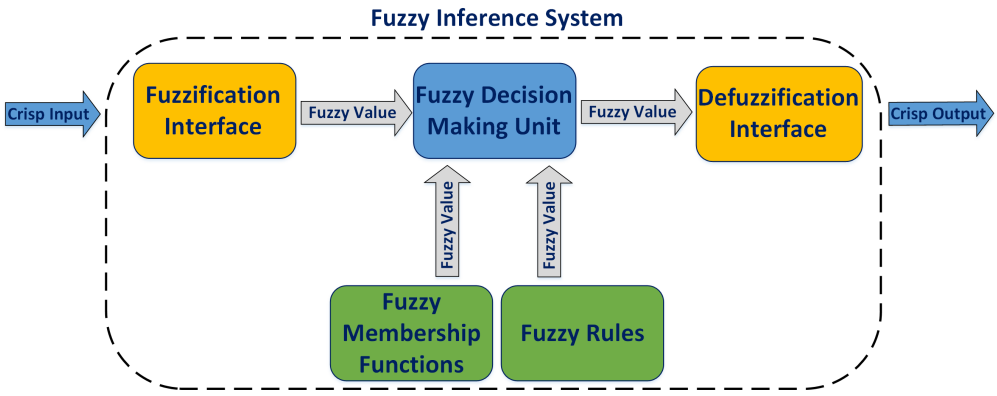

Fig. 3.1: Fuzzy inference system block diagram [Paper A].

Only the first and fourth layers can be adjusted in this design, while the rest remain constant. The adaptive layers use membership functions, weights, and evaluation rules to determine how much importance to assign to each input's reliance on a given membership function. The first layer transforms the crisp input into fuzzy inputs, and after conducting the necessary fuzzy calculations in the intermediate layers, the final layer converts the fuzzy output value back to a crisp output value. Depending on the problem type, the implication layer multiplies the inputs from the preceding layer to produce outputs in various ways. In the third layer, a process is carried out to determine the

[1]The percentage of total instances where an attack was correctly predicted from a set of positive samples.

[2]The F1-score metric is an effective evaluation tool that considers both precision and recall. This allows to simultaneously evaluate a model's accuracy and sensitivity.

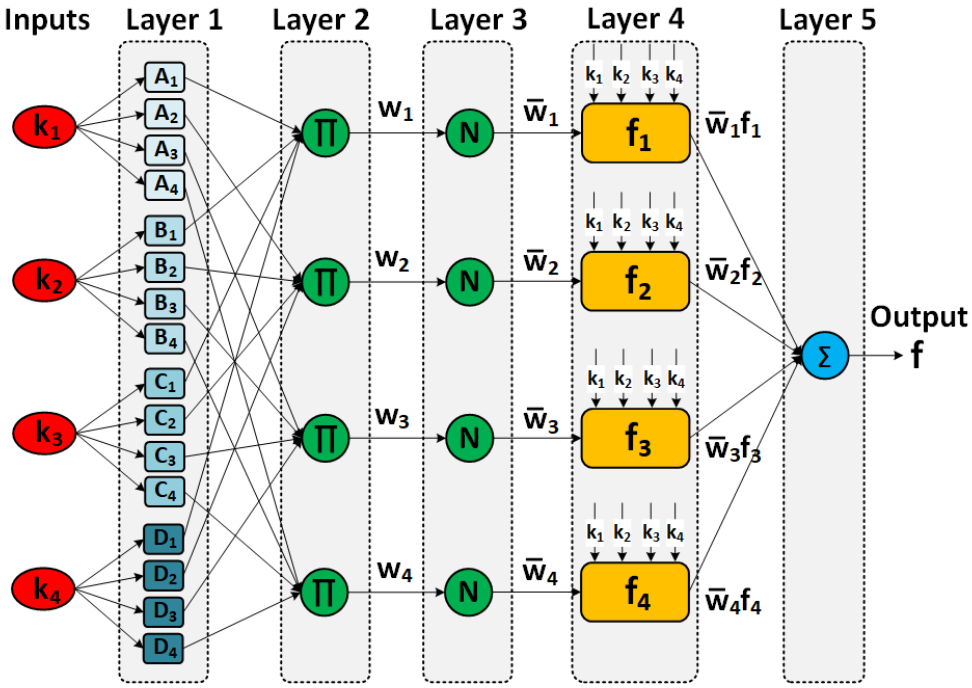

Fig. 3.2: ANFIS architecture [Paper B].

true value of each rule for generating the output. For a more detailed explanation of the ANFIS design process and training phase, please refer to [48].

3.2.2 Performance Evaluation and Comparison with other ML-based Estimators

In this section, the effectiveness of the designed ANFIS is compared with two other frequently employed ML-based estimators. The first estimator, Feed-forward Neural Network (FFNN), is composed of input nodes and hidden layers to propel input data in one direction (forward) to the output node, producing the output result. Decision Tree (DT), the second estimator, employs tree structures similar to flowcharts to make decisions and select the best course of action based on attribute selection measures.

The results of the research conducted in [48] reveal that the estimators employing ANFISs achieved a higher rate of accuracy (99.40%) than both the FFNN- and DT-based estimators. The results of the comparison analysis are presented in Tables 3.1 and 3.2 and Fig. 3.3 to 3.5. Table 3.3 provides more information about the hardware

system used for evaluation.

Table 3.1: Comparison analysis [Paper A].

Estimator type	Precision	Recall	Accuracy	F1-Score
ANFIS	92.31	96.00	99.40	94.12
FFNN	30.00	36.00	92.60	32.73
DT	53.35	67.89	81.01	73.03

Table 3.2: Comparison of computational cost

Estimator type	Offline Training Time (Sec)	Online Output Prediction Time (Sec)	Attack Detection Time (Sec)
ANFIS	7.18	0.00012	0.0964
FFNN	9.96	0.00311	0.134
DT	10.15	0.01111	0.114

Table 3.3: Hardware system specifications

Processor	Installed Memory (RAM)	System Type
Intel(R) Core(TM) i7 – 8565U CPU 1.80 GHz 1.99 GHz	16.00 GB (15.8 GB usable)	64 bit operating system, x64based processor

Based on the evaluation results presented in Tables 3.1 and 3.2, it is evident that the ANFIS-based technique outperforms other estimators like FFNN and DT-based estimators. The ANFIS-based technique has a lower computing burden, lower Root Mean Square Error (RMSE) and Standard Deviation (SD), as well as higher accuracy and F1-score. However, other supervised DD-based systems can also be used if they are well-trained and have acceptable real-time performances for a given application. For a detailed analysis of each model's characteristics, please refer to [Paper A].

3.3 FDIA Modeling

Generally, DCMG systems are vulnerable to FDIAs, in which the measured data of current and voltage sensors can be manipulated by an attacker, compromising the system's safety and performance. The FDIA model expressions in this thesis have been

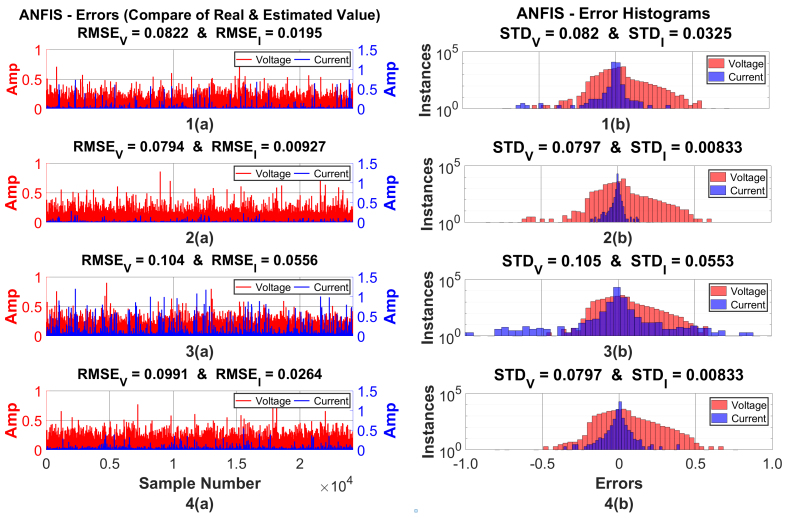

Fig. 3.3: Error evaluation of ANFIS system [Paper A].

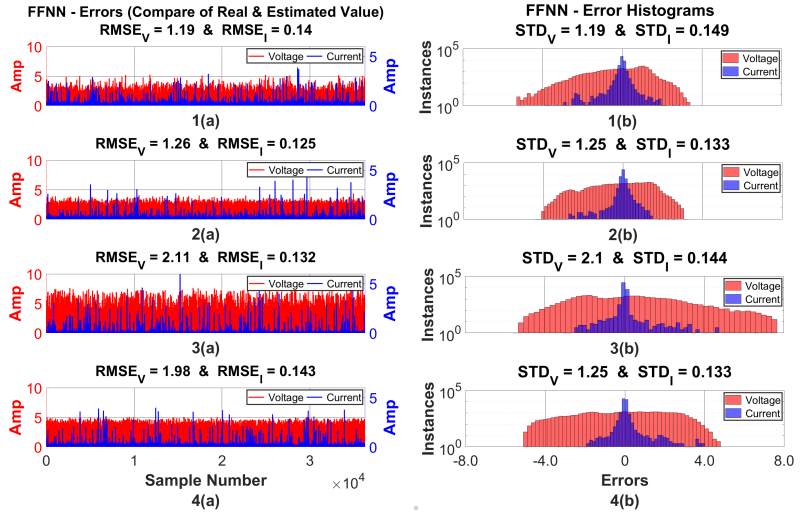

Fig. 3.4: Error evaluation of FFNN [Paper A].

categorized into two states: Attacked and Normal, which are determined by analyzing the signals received from the voltage or current sensors. The following equations model FDIA with consideration for the location of the malicious activity in voltage or current

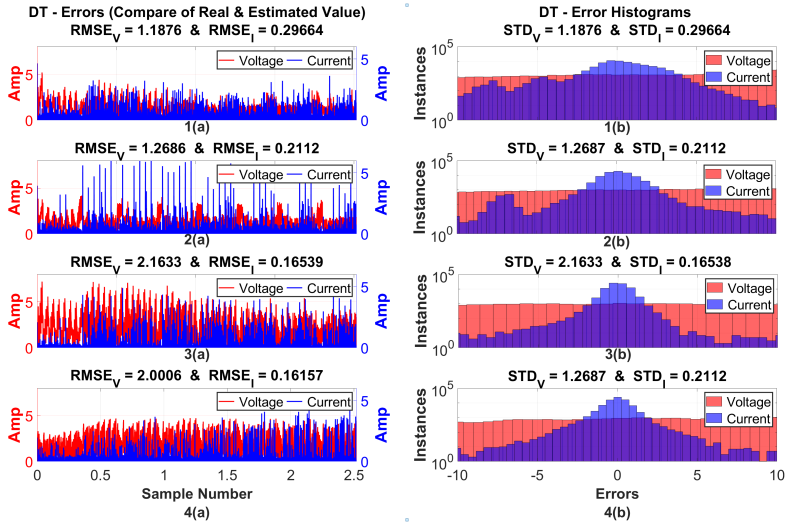

Fig. 3.5: Error evaluation of DT approach [Paper A].

sensors. Because of its ability to fully show the precise place of intrusions, this modeling method allows for a clearer understanding of the system's state.

$$V_{dc_j}(t) = \begin{cases} V_{dc_j}(t) + C_j^V(t) & \delta = 1 \quad (Attacked) \\ V_{dc_j}(t) & \delta = 0 \quad (Normal) \end{cases} \tag{3.1}$$

$$I_{dc_j}(t) = \begin{cases} I_{dc_j}(t) + C_j^I(t) & \delta = 1 \quad (Attacked) \\ I_{dc_j}(t) & \delta = 0 \quad (Normal) \end{cases} \tag{3.2}$$

Utilizing this mathematical model for FDIAs can represent all types of FDIAs, whether they are dynamic or static, and even hijacking attacks. Essentially, there are two main forms of FDIA attacks:

- Altering original information earlier than using it in the system.
- Completely substituting false data for the original data.

Both the abovementioned forms represent the different types of FDIAs in the understudied DCMG system. In the first case, the measured value can be assumed to have an equal value with an opposite sign ($-V_{dc_j}(t)$), and in the second case, the data can be assumed to be false data ($C_j^V(t)$). In this thesis, it is presumed that the attacker has ample access to the system's information to intelligently create and append FDIs to the current and voltage measurements. As a result, the attack model expressions that include voltage and current measurements can include various types of FDIs by writing them as $C_j^V(t)$ and $C_j^I(t)$, respectively.

3.4 Proposed FDIA Detection and Mitigation Framework

Generally, for a typical DCMG system with a distributed control strategy, all the data necessary for maintaining the system performance is collected at the monitoring center (MC). Two different DD estimators, each accounting for estimating the DC/DC converters' output voltage and current, are used in each DG. Detecting and mitigating FDIAs in a DCMG system with N DGs can be accomplished thanks to the scalability of the proposed framework. The proposed framework is displayed in Fig. 3.6.

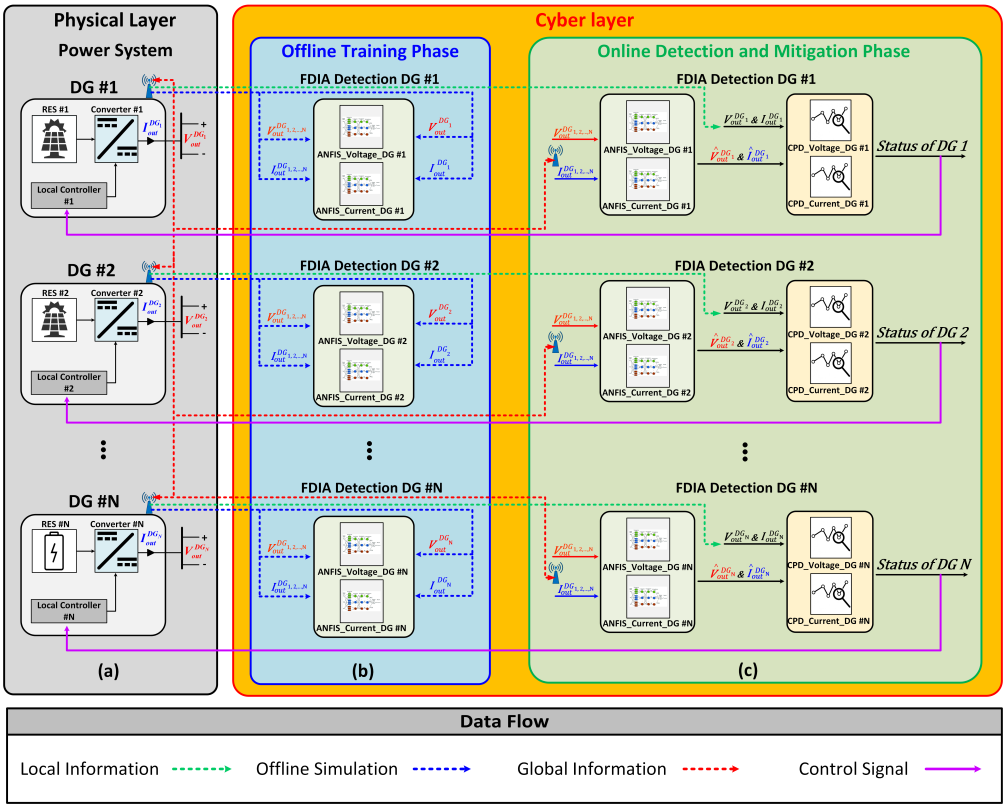

Fig. 3.6: The proposed framework: (a) Physical layer, (b) Cyber layer (Offline phase), (c) Cyber layer (Online phase) [Paper B].

The proposed framework is divided into two distinct layers, namely physical and cyber layers, as shown in Fig. 3.6. In the following, five major steps of the proposed

method are discussed. The ANFIS estimators are trained in the offline phase, and in the online phase, the ANFIS is employed to predict the jth DC-DC converter's voltage and current outputs. As previously stated, the output current and voltage in DCMGs are both vulnerable to cyber-attacks; thus, two independent ANFIS models are used to detect the FDIA presence in the system and the precise place of malicious activity (which sensor measurement in which DG unit). When two ANFIS models are used for each DG unit, the computational time of output estimations is drastically reduced, and the system is better able to pinpoint the precise location of an intrusion using either voltage or current sensors.

3.4.1 Data Collection

During the data collection phase, an input vector is created by combining all DGs' voltage and current output measurements. The data is collected by DC bus-mounted smart meters in the DCMG system. Effective FDIA detection depends on the quality of the input data, which is why collecting the data at a high sampling rate is recommended. However, this increases the computational burden, so a trade-off between computational burden and input quality must be made. To address this, a long offline simulation was performed to obtain data for training sets under various conditions. It is worth noting that choosing a long offline simulation with a wide range of different conditions allows for the consideration of all data points that represent the transition from one scenario to the next, resulting in a precise transient response for ANFIS performance. Eight input variables (four voltages and four load values) ranging from 0% to 100% of their nominal values were used, resulting in 8! distinct scenarios (= 40320). It was found that the most accurate input data was provided by a Gaussian distribution [8], and ten samples were collected for each scenario to represent the average performance of the simulated system. This means that each training set includes 40320*10 input samples. For detailed information about the training sets' characteristics, please refer to [Paper A].

3.4.2 Offline Training

During the data collection phase, the ANFISs are trained offline using the information gathered, as depicted in Fig. 3.6(b). To ensure optimal performance and prevent overfitting, which can lead to inaccurate predictions and high errors during testing, it's crucial to randomly divide the data into three sets: training, validation, and testing. After each epoch, the error should be compared against the validation data set to avoid overfitting. The data is divided into 70% for training, 15% for validation, and 15% for testing, and the sum of square errors is used as the error-index to monitor the training's success and improve the mapping quality. The error plots for all eight ANFISs' output voltage and current estimations are shown in Fig. 3.7. For more detailed information on

ANFIS training, including the method for FIS generation and learning approach, please refer to [Paper B].

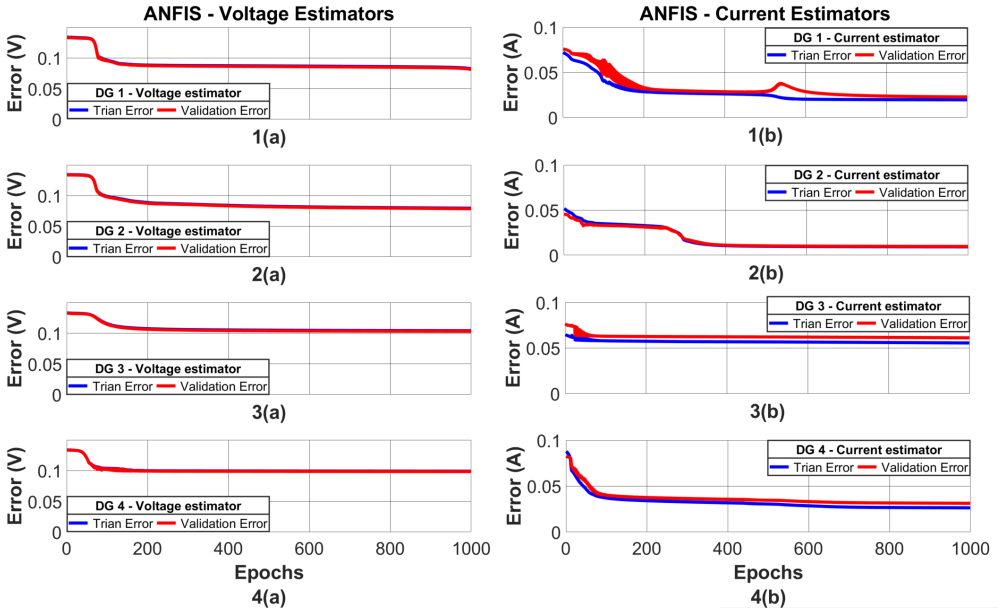

Fig. 3.7: ANFISs' training error [Paper A].

3.4.3 Online Output Prediction

To estimate the real output voltage and current of each DC-DC converter, the proposed online prediction scheme makes use of two trained estimators for each DG unit, as shown in Fig. 3.6(c). In order to identify any significant discrepancy between the predicted and actual values for the jth DC-DC converter, two residual signals are considered, as shown below.

$$error_V^{DG_j} = V_{out}^{DG_j}(t) + \hat{V}_{out}^{DG_j}(t) \approx \hat{C}_j^V(t) \tag{3.3}$$

$$error_I^{DG_j} = I_{out}^{DG_j}(t) + \hat{I}_{out}^{DG_j}(t) \approx \hat{C}_j^I(t) \tag{3.4}$$

For the jth DC-DC converter, the following are the estimated voltage and current output ($\hat{V}_{out}^{DG_j}(t)$, $\hat{I}_{out}^{DG_j}(t)$), actual voltage and current output ($V_{out}^{DG_j}(t)$, $I_{out}^{DG_j}(t)$), and the approximation of voltage and current attack values ($\hat{C}_j^V(t)$, $\hat{C}_j^I(t)$), as well as their real voltage and current attack values ($C_j^V(t)$, $C_j^I(t)$). The above error signal expressions

(Eq. (3.3) and (3.4)) show that when a cyber-attack is present, the error signals are very close to the attack values and very close to zero when no attack has been detected.

3.4.4 Online Detection

In this step, the proposed framework employs the information from the generated error signals $error_V^{DG_j}$ and $error_I^{DG_j}$ from the online output prediction phase to identify the current status of the system (normal or attacked). Any Change Points (CPs) in the error signals can be considered as an attack indicator employing an OCPD technique. A Bayesian Change Point Detection (BCPD) is employed in this OCPD to detect any CPs in the error signals by partitioning all sample data into non-overlapping sections and assuming that each section's probability distributions are independent and identical. For more in-depth information, please check [8, 49].
When false data is introduced into a system while it is operating in its normal state, the probability distribution of the residual signals starts to fluctuate. It is important to note that any deviations in the residual signals point to the possibility of compromised DG units. For example, if a cyber-attack initiates in a measurement of the current sensor at DG 1, the corresponding error signal for the current sensor in DG 1 starts to change.

3.4.5 Attack Mitigation

After detecting a cyber-attack and identifying its location in the cyber layer, the control system must take an action to mitigate the destructive effects of the FDIA for reliable system performance. Given that the attacked DG's control system can access false and estimated output data via the online ANFIS estimators, the following compensatory measure is implemented.

$$V_{dc_j}^{amended}(t) = \begin{cases} V_{dc_j}(t) & (Normal) \\ V_{dc_j}^{attack}(t) - sign(\hat{C}_j^V(t)) \left|\hat{C}_j^V(t)\right| & (Attacked) \end{cases} \tag{3.5}$$

$$I_{dc_j}^{amended}(t) = \begin{cases} I_{dc_j}(t) & (Normal) \\ I_{dc_j}^{attack}(t) - sign(\hat{C}_j^I(t)) \left|\hat{C}_j^I(t)\right| & (Attacked) \end{cases} \tag{3.6}$$

where $V_{dc_j}^{amended}(t), I_{dc_j}^{amended}(t), V_{dc_j}^{attack}(t)$, and $I_{dc_j}^{attack}(t)$ represent the amended and attacked signals for the jth DG unit. Moreover, to obtain an approximation of the actual data from neighboring systems, the absolute value of the residual signals with the opposite sign is added to the attacked data. This amended data is then provided to the secondary controller, ensuring the control subsystem receives accurate and secure data, thereby maintaining system functionality despite the attack.

3.5 Simulation Results

In this section, the DCMG system will be examined to evaluate the effectiveness of the proposed defense strategies against possible attacks, which has been previously discussed in section 2.2.2. Four different attack scenarios will be tested using the proposed framework, with common characteristics as described in [8]. Each scenario will be tested with multiple instances that vary in attack characteristics. For a comprehensive analysis of each case study, please refer to [8].

3.5.1 Case Study 1: Rapid Load Fluctuations

When false data is injected into the network by an attacker during unexpected shifts in load, it can severely compromise the reliability of the network. For instance, when DG 1 is under attack, Loads 4 and 2 increase by 45% and 25%, respectively, at t = 3.6s and t = 4.6s. Since these changes have similar effects to attacks, such as fluctuations in average output voltage and current sharing, it is crucial that these two really similar situations be distinguishable by the proposed framework. Fig. 3.8(b) shows how the DCMG's output voltage and current values differ without and with the proposed framework. As can be seen in Fig. 3.8(c), the detection approach does not take into account two other unexpected load shifts happening both prior to and during the presence of the attacks. The DG error signals are presented in Fig. 3.8(e).

3.5.2 Case Study 2: Dynamic FDIA

In this case study, the measurements are manipulated by injecting false data in DG 2 and DG 4 current measurements. Based on the data in Fig. 3.9(a), it is assumed that the attacker has the capability to insert fake data into current measurements when there are rapid fluctuations in load between $t = 4s$ and $t = 6s$. Furthermore, two other unexpected load shifts occur, as shown in Fig. 3.9(b), before the actual intrusion, which the detection system fails to recognize. Fig. 3.9(b) illustrates the output currents in the absence of an attack detection scheme. It is clear that the affected DGs would be unable to share information as they do when the proposed framework is not used because their control units are receiving false data from the cyber communication layer. The error signals for DGs are depicted in Fig. 3.9(e). Some CPs detected by the OCPD scheme may be the result of a change in the related error signals caused by FDIAs.

3.5.3 Case Study 3: Hijacking Attack

In cases of FDIA, the hijacking attack is particularly challenging since it involves replacing actual data with fake information. In contrast to the scenario presented in Case study 1, the manipulated data in this case has none of the same properties as the original data, including the limited amplitude and the slope of change. The voltage sensor

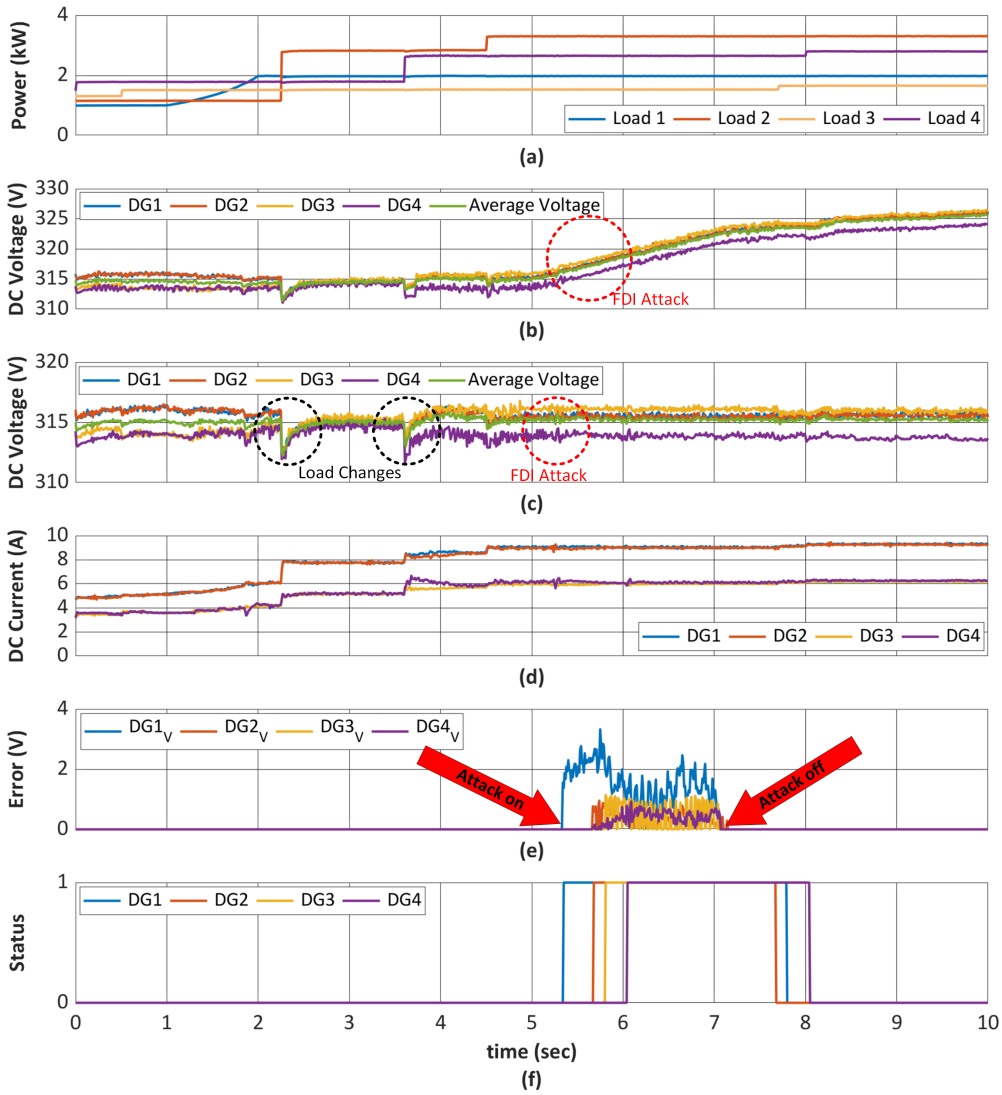

Fig. 3.8: System responses in the face of FDI attack in the voltage measurement while the loads vary rapidly: (a) Profiles of load. (b) Standard secondary controller's output voltage without the proposed framework. (c) Standard secondary controller's output voltage with the proposed framework. (d) Standard secondary controller's output current with the proposed framework. (e) Residual signals. (f) System status [Paper B].

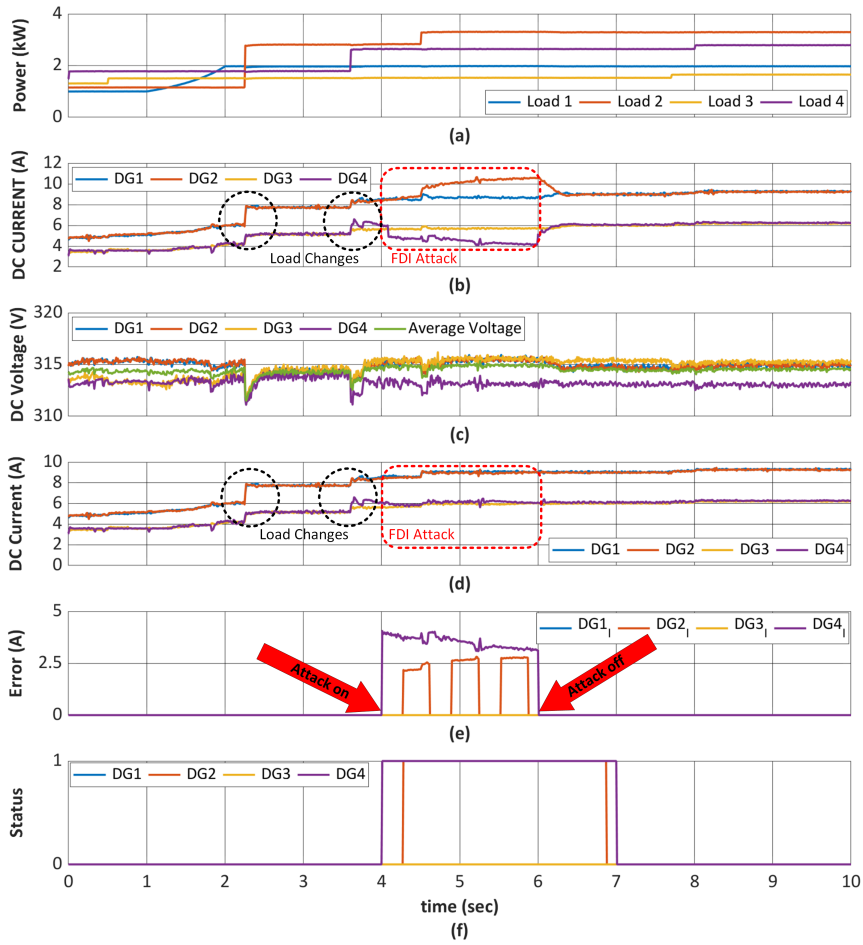

Fig. 3.9: System responses in the face of dynamic FDI attack in the current measurement: (a) Profiles of load. (b) Standard secondary controller's output voltage without the proposed framework. (c) Standard secondary controller's output voltage with the proposed framework. (d) Standard secondary controller's output current with the proposed framework. (e) Residual signals. (f) System status [Paper B].

in DG 2 is targeted in this hypothetical attack. The suggested method's efficacy in detecting hijacking attacks is illustrated in Fig. 3.10. Findings from Case study 3 are

similar to those from Case study 1, which show that the proposed method can accurately distinguish hijacking attacks from other types of unexpected load shifts or intrusions.

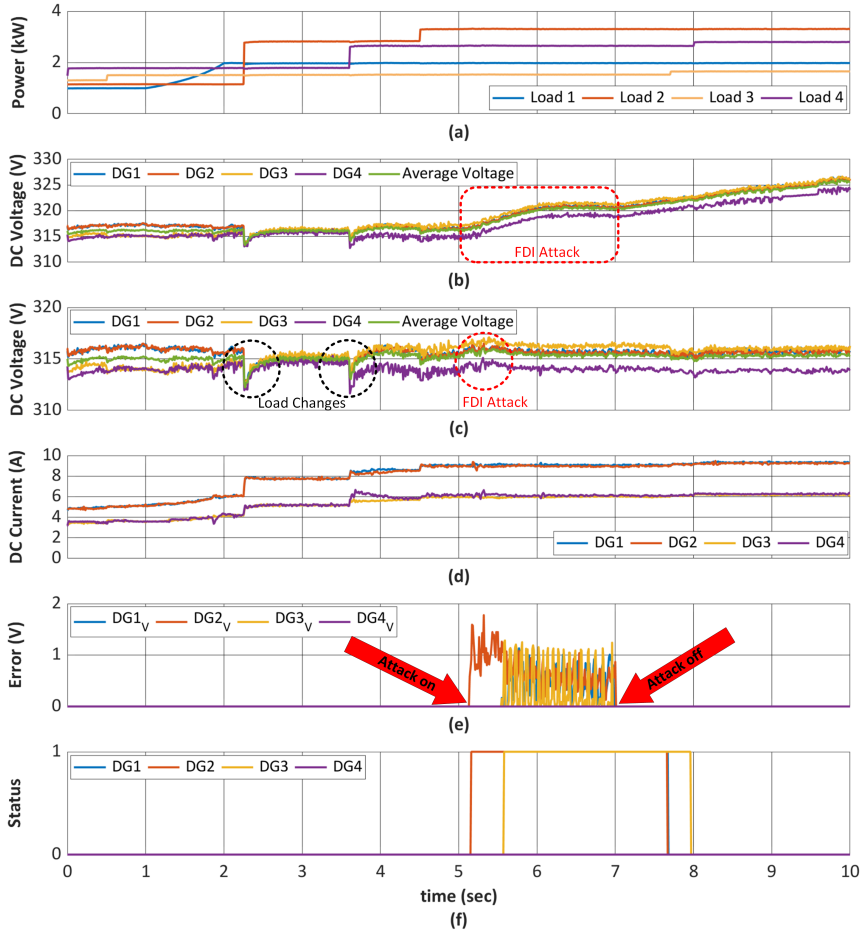

Fig. 3.10: System responses in the face of Hijacking attack in the voltage measurement: (a) Profiles of load. (b) Standard secondary controller's output voltage without the proposed framework. (c) Standard secondary controller's output voltage with the proposed framework. (d) Standard secondary controller's output current with the proposed framework. (e) Residual signals. (f) System status [Paper B].

3.5.4 Case Study 4: FDIA with Different Distribution

In this case study, a common and challenging type of FDIA that appears in DCMGs will be analyzed. Performance is assessed in the face of a Gaussian distribution attack by injecting false data that resemble normal changes in the load profile. By injecting false data that mimics the appearance of normal, normal changes to the load profile and follows a pattern that is strikingly similar to the Gaussian distribution, the attacker hopes to hide the true nature of its malicious actions. The effectiveness of the proposed method in detecting Gaussian distributed attacks is illustrated in Fig. 3.10. Similar results to previous case studies are observed in Case study 4, indicating that Gaussian distributed attacks can be accurately distinguished from other forms of unexpected load shifts or intrusions by the proposed method.

3.6 Conclusions

In this chapter, a framework was presented for identifying FDIA in DCMGs deploying a DD method. All voltage and current measurements in a DCMG were estimated with an impressive 99.40% accuracy using the proposed ANFIS-based method. When false information is introduced into the DCMG, the proposed framework can identify the location of the malicious activities by analyzing the residual signals, thereby mitigating the negative impact of FDIA on the system. Importantly, by utilizing the proposed framework, no additional channels of communication are required to pinpoint the origin of the intrusion, while it is possible to identify different types of FDIA without the need for attack models for training.

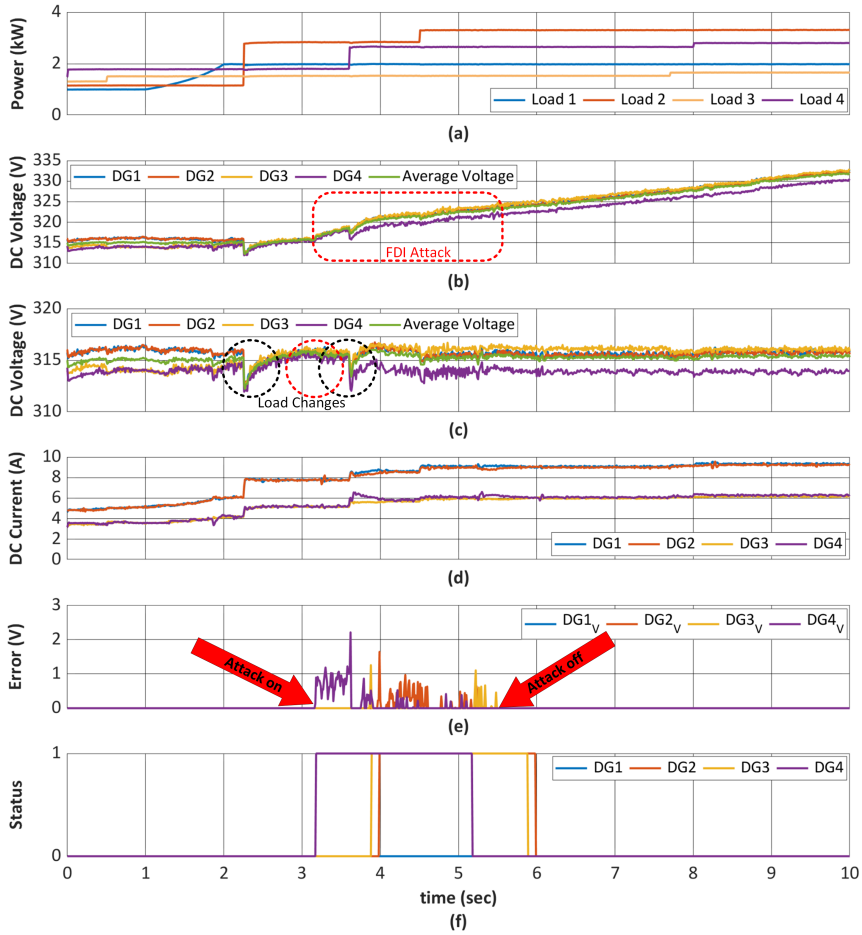

Fig. 3.11: System responses in the face of FDI attack with Gaussian distribution characteristic in the voltage measurement: (a) Profiles of load. (b) Standard secondary controller's output voltage without the proposed framework. (c) Standard secondary controller's output voltage with the proposed framework. (d) Standard secondary controller's output current with the proposed framework. (e) Residual signals. (f) System status [Paper B].

Chapter 4: Reduced Reliance on Network Data Transmission: A Novel Secondary Control for DCMGs

4.1 Introduction

In this chapter, a distributed secondary controller for DCMGs is proposed, which can achieve voltage consensus, current sharing, and reference voltage tracking with minimum reliance on input from neighboring units. To accomplish this, a distributed finite-time secondary controller accompanied by physical relations in the DCMG network from the existing literature is used to reduce local controllers' dependency on voltage information from neighboring units. It is worth noting that exploiting physical relationships within the DCMG network eliminates the need for local controllers to rely on voltage information from neighboring units. To achieve voltage consensus throughout the network, local measurements of load and unit currents, as well as line resistances, are used. In addition, a modified version of the control law for the unit responsible for tracking the reference voltage from an external tertiary controller in the corresponding network setting is suggested. Furthermore, to maintain system stability, a saturation function on the secondary controller with integrator anti-windup logic is suggested.

4.2 System Architecture and Distributed Secondary Control

4.2.1 System Architecture

This chapter discusses an autonomous DCMG with a hierarchical control scheme, as represented in Section 2.2.2 and illustrated in Fig. 4.1 and 4.2. The DCMG configuration in

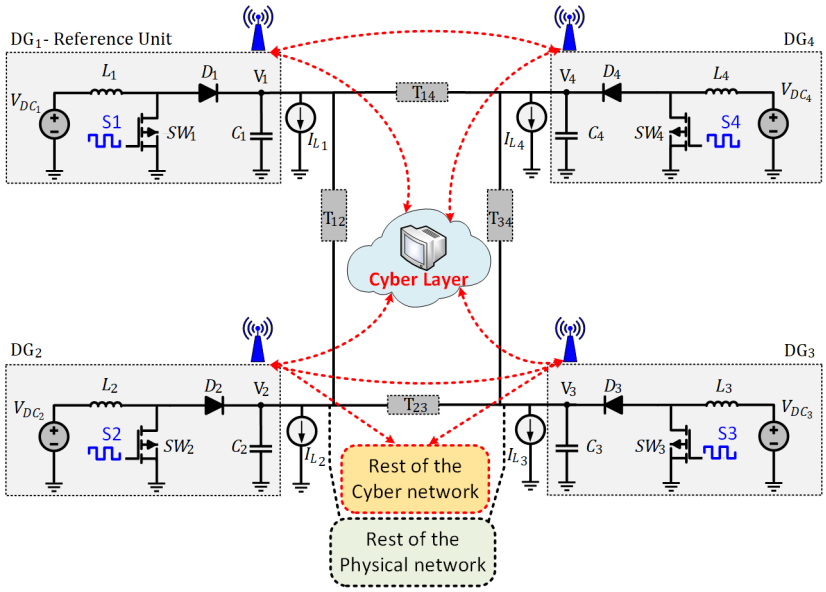

Fig. 4.1: DCMG configuration in which the DG_1 as the reference unit is connected to the other $DG_{2,3,4}$ via the distribution lines [Paper C].

Fig. 4.1 illustrates the connection of four DC sources to four DC-DC converters and four local loads through resistive lines. To enable data transmission between units, a cyber layer is required, and a set of communication links with an undirected ring topology is considered. The secondary controller generates an appropriate voltage reference for each bus to maintain the desired output voltage, and the communication link ensures the transmission of local voltage and current measurements between neighboring nodes.

As earlier stated, a number of communication links for exchanging information between units are taken into account by the cyber layer. By employing each of the generation sources as an agent in the multi-agents theory, the communication graph representing the connectivity of the communication links can be viewed as a digraph with edges and links, which are defined by the adjacency matrix $A = [a_{ij}] \in R^{N*N}$. The communication weights can be defined as follows:

$$a_{ij} = \begin{cases} > 0 & \text{if } (x_i, x_j) \in \mathbf{E} \\ 0 & \text{else} \end{cases} \tag{4.1}$$

In this context, $\mathbf{E}$, N, x_i, and x_j denote the edge connecting two adjacent nodes, the total number of nodes in the main graph, the parent node, and the neighboring node, respectively. It is important to note that the reference set-point provided by the

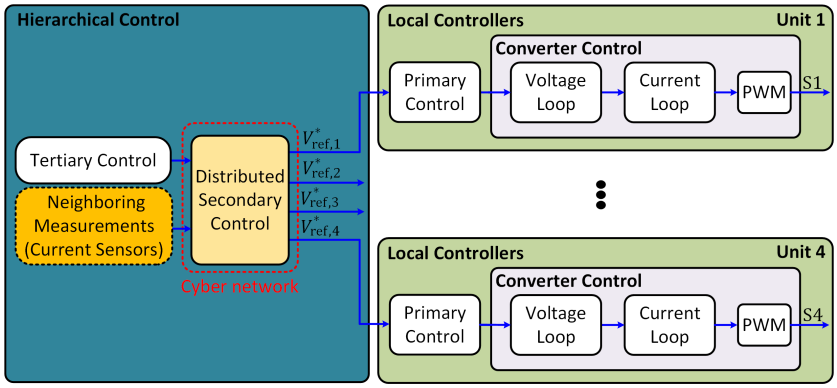

Fig. 4.2: Hierarchical control scheme [Paper C].

tertiary controller can only be accessed by the reference unit, which, in this chapter, is Unit 1 as depicted in Fig. 4.1.

4.2.2 Finite Time Distributed Secondary Control

In [50], a nonlinear distributed secondary control scheme for a typical DCMG system is proposed. This scheme is able to provide for the fine-time convergence of the DCMG's states to their desired values. The following expression serves as the governing control law for the reference voltages:

$$V^*_{ref,i} = \int \Big(sat_{\sigma_1}\big(k_1 sgn_\alpha(e_{Vi})\big) + sat_{\sigma_2}\big(k_2 sgn_\gamma(\dot{e}_{Vi})\big) + R_i sat_{\sigma_3}\big(k_3 sgn_\alpha(e_{Ii})\big)\Big) \quad (4.2)$$

The three control gains are represented by k_1, k_2, and k_3, while the saturation levels for each term in the control law are σ_1, σ_2, and σ_3. Additionally, there is a tuning parameter represented by α, which is used to calculate the value of γ. It should be noted that γ is determined by the equation $\gamma = \frac{2\alpha}{1+\alpha}$. Also

$$e_{Vi} = \begin{cases} (\bar{V}_i - V_{ref}) + \sum_{j\in N_i} a_{ij}(\bar{V}_j - \bar{V}_i), & i = 1 \\ \sum_{j\in N_i} a_{ij}(\bar{V}_j - \bar{V}_i), & i \in 2, \cdots, N \end{cases} \quad (4.3)$$

$$e_{Ii} = \sum_{j\in N_i} c_i a_{ij}\left(\frac{I_j}{I_{j,max}} - \frac{I_i}{I_{i,max}}\right), \qquad i \in 1, \cdots, N \quad (4.4)$$

where $\bar{V}$ represents average voltage, c_i pertains to the coupling gain for current sharing, and N_i refers to the indices of the units connected to unit i. The initial unit has the

responsibility of tracking the reference voltage V_{ref} demanded by the tertiary controller, and thus, the first two terms inside the integral controller for this unit are computed differently. In [50], the stability and performance of the aforementioned control technique have been thoroughly studied. It is worth noting that the control law for each unit necessitates the use of voltage and current data from all the adjacent units. This means that a communication network must be established to exchange the adjacent units' current and voltage information, which can expose the system to cyber attacks, as analyzed in [8]. To address this issue, a revised formula for the distributed controller has been derived in this chapter, which relies only on the adjacent unit currents, thereby reducing the communication network's workload and mitigating potential cybersecurity threats. Additionally, a modification to the first unit is proposed to enhance its reference tracking performance. Lastly, the addition of control saturation with an integrator anti-windup mechanism is recommended to further enhance the stability and response quality of the proposed control law in practical applications.

4.2.3 Proposed Method

In this section, some modifications to the finite-time controller explained in the previous section are suggested. These adjustments will result in a modified control law that necessitates less information exchange among the units in the DCMG. As previously mentioned in Section 2.2, assuming the quasi-stationary model for distribution lines Section 2.2, the line currents can be expressed as:

$$I_{ij} = \frac{V_i - V_j}{R_{ij}} \tag{4.5}$$

The relationship between the currents and voltages can be determined by summing the two sides of the equation over j:

$$\sum_{j \in N_i} \frac{1}{R_{ij}}(V_i - V_j) = \sum_{j \in N_i} I_{ij} = I_i - I_{Li} \tag{4.6}$$

where I_{Li} is the load current at unit i. By considering the bellow expression:

$$a_{ij} = \frac{1}{R_{ij}} \tag{4.7}$$

the term for voltage consensus in the distributed control framework can be expressed as follows:

$$\sum_{j \in N_i} a_{ij}(V_i - V_j) = I_i - I_{Li} \tag{4.8}$$

To eliminate cybersecurity risks associated with transmitting voltage data, it is possible to replace the voltage consensus control term with a term based on the local

converter voltage and load currents. This term can be measured locally. According to Eq. (4.8), each unit in the network must balance its own load current (i.e., $I_i = I_{Li}$) to achieve full voltage consensus. This is a logical conclusion based on the physics of the network. In addition to this proposal, we suggest modifying the control law for Unit 1.

The equation Eq. (4.9) states that Unit 1 will attempt to follow the desired reference voltage set by the tertiary controller.

$$V^*_{ref,1} = V_{ref} \tag{4.9}$$

Therefore, the current sharing task falls to the remaining units in the network. The revised distributed controller for these units can be expressed as follows:

$$V^*_{ref,i} = \int \Big(sat_{\sigma_1}\big(k_1 sgn_\alpha(e_{I_{Li}})\big) + sat_{\sigma_2}\big(k_2 sgn_\gamma(\dot{e}_{I_{Li}})\big) + R_i sat_{\sigma_3}\big(k_3 sgn_\alpha(e_{Ii})\big)\Big), \; i \in 2, ..., N \tag{4.10}$$

where

$$e_{I_{Li}} = I_{Li} - I_i, \quad i \in 2, ..., N \tag{4.11}$$

$$e_{Ii} = \sum_{j \in N_i} \frac{c_i}{R_{ij}} (I_j/I_{j,max} - I_i/I_{i,max}), \quad i \in 2, ..., N \tag{4.12}$$

and sat_σ and sgn_α are nonlinear functions defined as [50]:

$$sat_\sigma(x) = \begin{cases} x & \text{if } |x| < \sigma \\ \sigma sgn(x) & \text{othrewise} \end{cases} \tag{4.13}$$

$$sgn_\alpha(x) = sgn(x)\,|x|^\alpha, \quad 0 < \alpha < 1 \tag{4.14}$$

Noise and bias can be introduced into the measured data in practice. It is also possible for the integral controller to receive unbounded control signals as a result of the error residuals. To prevent long-term instability in the network, it is important to establish upper and lower bounds on the reference voltage for each unit. Additionally, anti-windup logic is required for optimal performance since an integrator is a component of the controller. To address these issues, we propose the following modifications to the control law:

$$V^*_{ref,i} = V_{ref,nom} + \int Proj_{\Delta V_{ref,i}}\big[sat_{\sigma_1}\big(k_1 sgn_\alpha(e_{I_{Li}})\big) + sat_{\sigma_2}\big(k_2 sgn_\gamma(\dot{e}_{I_{Li}})\big) + R_i sat_{\sigma_3}\big(k_3 sgn_\alpha(e_{Ii})\big)\big], \quad i \in 2, ..., N \tag{4.15}$$

where $V_{ref,nom}$ is the nominal reference voltage (e.g. 315 V), and

$$\Delta V_{ref,i} = V^*_{ref,i} - V_{ref,nom} \tag{4.16}$$

$$Proj_{\Delta V_{ref,i}}[e] = \begin{cases} 0 & \text{if } \Delta V_{ref,i} \geq \Delta V_{ref,max} \quad and \quad e > 0 \\ 0 & \text{if } \Delta V_{ref,i} \leq \Delta V_{ref,min} \quad and \quad e < 0 \\ e & \text{otherwise} \end{cases} \tag{4.17}$$

The upper and lower limits on the deviation of the reference voltage from the nominal reference voltage are represented by $\Delta V_{ref,max}$ and $\Delta V_{ref,min}$. To prevent integrator wind-up in the event of control saturation, the control law uses a projection operator. This operator sets the term inside the integrator to zero when the controller is about to exceed its limits, which halts the integration process until the controller returns to its acceptable range.

4.3 Simulation Results

The effectiveness of the proposed secondary control scheme for the DCMG system, as discussed in Section 2.2.2, will be evaluated in this section. To accomplish this, three different case studies with common characteristics described in [51] will be examined. These case studies will feature abrupt load changes, voltage reference tracking, and control saturation and integrator anti windup effects. The aim is to determine how well the DCMG system performs with the proposed method while having limited accessibility to the neighbors' measurements (only current sensors measurement is required) compared to conventional secondary control schemes. For a thorough analysis of each case study, please refer to [51].

4.3.1 Rapid Load Fluctuations

In order to test the understudy DCMG system, a combination of abrupt and continuous load changes, as depicted in Fig. 4.3(a), will be utilized. Fig. 4.3(b) and Fig. 4.3(c) display the unit voltages and currents for the conventional finite-time secondary controller. While the controller is successful in maintaining the average voltage around the reference voltage set by the tertiary controller, it falls short in following the commanded voltage for the reference unit, DG 1. Nonetheless, current sharing is achieved effectively, as shown in Fig. 4.3(c). On the other hand, Fig. 4.3(d) and Fig. 4.3(e) illustrate the voltage and current trajectories of the proposed controller. DG 1 is capable of maintaining the voltage around the reference value, and current sharing is achieved with a slightly improved transient response in comparison to the conventional controller.

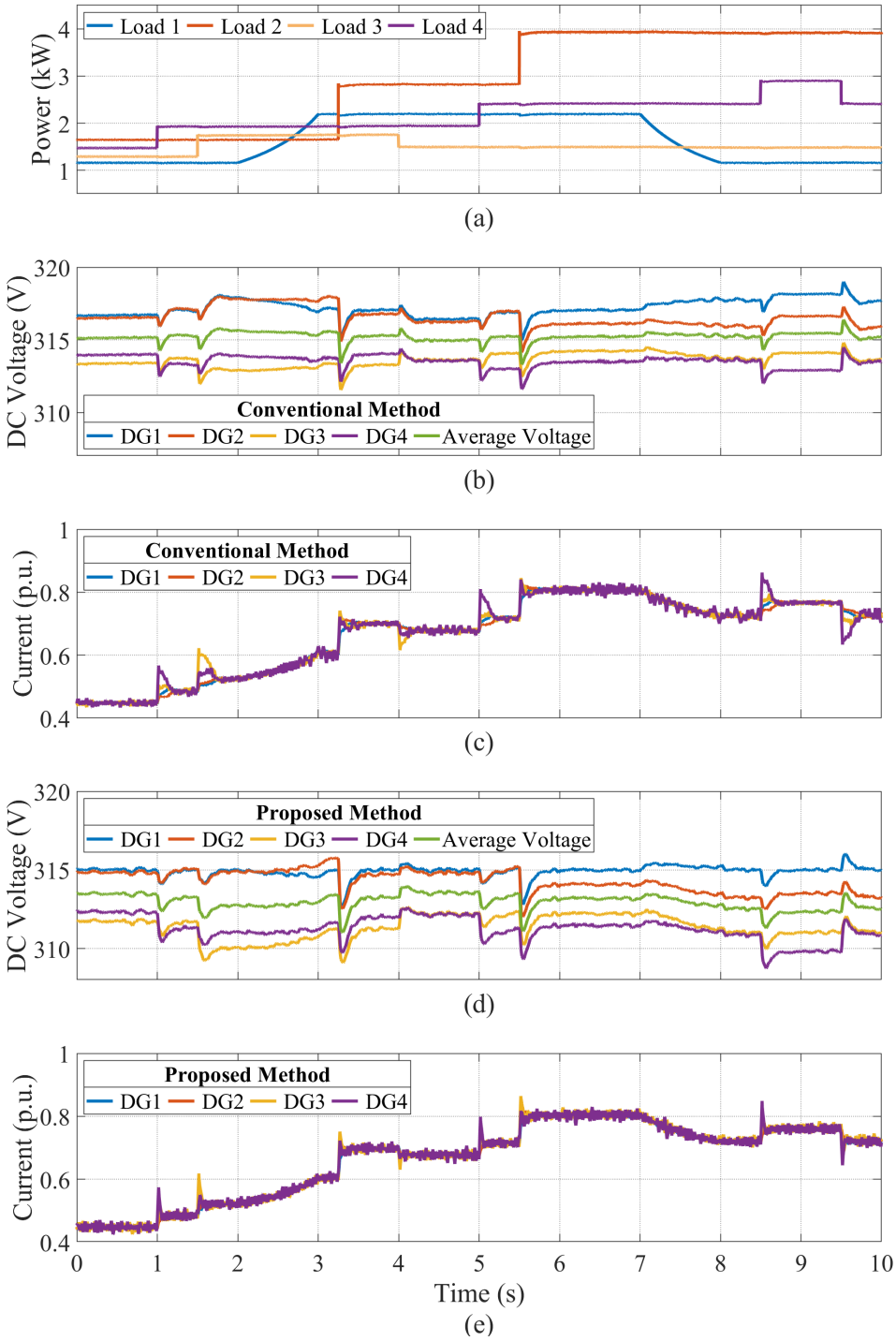

Fig. 4.3: System responses in the face of rapid load fluctuations: (a) Profiles of load. (b) Standard secondary controller voltage output. (c) Standard secondary controller current output. (d) Voltages at the output using the proposed method. (e) Currents at the output using the proposed method [Paper C].

4.3.2 Tracking Voltage Reference Changes

This part is dedicated to discussing the management of voltage trajectory for the tertiary controller in the context of smoothly varying loads. Fig. 4.4(a) shows the load changes. Fig. 4.4(b) showcases the voltage response of the Conventional Controller (CC), indicating unit 1 does not react to tertiary reference voltage changes. Conversely, Fig. 4.4(c) portrays the successful current sharing under the CC. The proposed controller's voltage response is presented in Fig. 4.4(d), demonstrating its ability to track the reference voltage for DG 1 through its primary controller. The proposed method also achieves current sharing, with only a few intermittent transient intervals that occur due to sudden changes in the reference voltage.

4.3.3 Control Saturation and Integrator Anti Windup Effects

In this section, the proposed controller's reference voltage range was set at 310-320 V, while the CC remained unrestricted. The designed loads were intended to initiate under normal balanced conditions for a duration of 0.5 seconds. This would be followed by an abrupt load change to the extreme limits for a period of 15 seconds. Subsequently, the loads would return to the balanced condition after 15.5 seconds, as illustrated in Fig. 4.5(a). The aforementioned circumstance resulted in the suggested controller entering the control saturation zone, which could potentially result in the integrator windup issue if no anti-windup logic had been incorporated.

The CC was able to achieve voltage consensus and current sharing among the units, as demonstrated in Fig. 4.5(b) and Fig. 4.5(c), following the return of loads to the normal range after 15.5 seconds due to the saturation-free controller. Fig. 4.5(d) and Fig. 4.5(e) illustrate that the proposed controller, in the absence of an integrator anti-windup logic, was unable to restore the consensus voltage and current sharing state owing to integration windup during the period of extreme loading. Upon implementation of the integrator anti-windup logic, as depicted in Fig. 4.5(f) and Fig. 4.5(g), the objectives of achieving voltage consensus and current sharing were successfully met. Furthermore, the transient response was observed to be marginally improved in comparison to the CC.

The impact of control saturation on the proposed controller and the effect of lacking it on the CC were investigated, and the reference voltage trajectories for both controllers were analyzed. In Fig. 4.6(a), it can be observed that the reference voltages under the CC tend to drift over time, which may lead to significant voltage deviations in the long run. This is due to the weak enforcement of the tertiary controller's reference voltage tracking by DG 1, causing the error residuals to integrate over time without any hard limits during transient periods. On the other hand, the reference voltages in the proposed method without integrator anti-windup remain stable, but the integrator windup prevents the reference voltage of the strained unit (DG 3) from returning to the normal range after the loads have been balanced, as shown in Fig. 4.6(b). However,

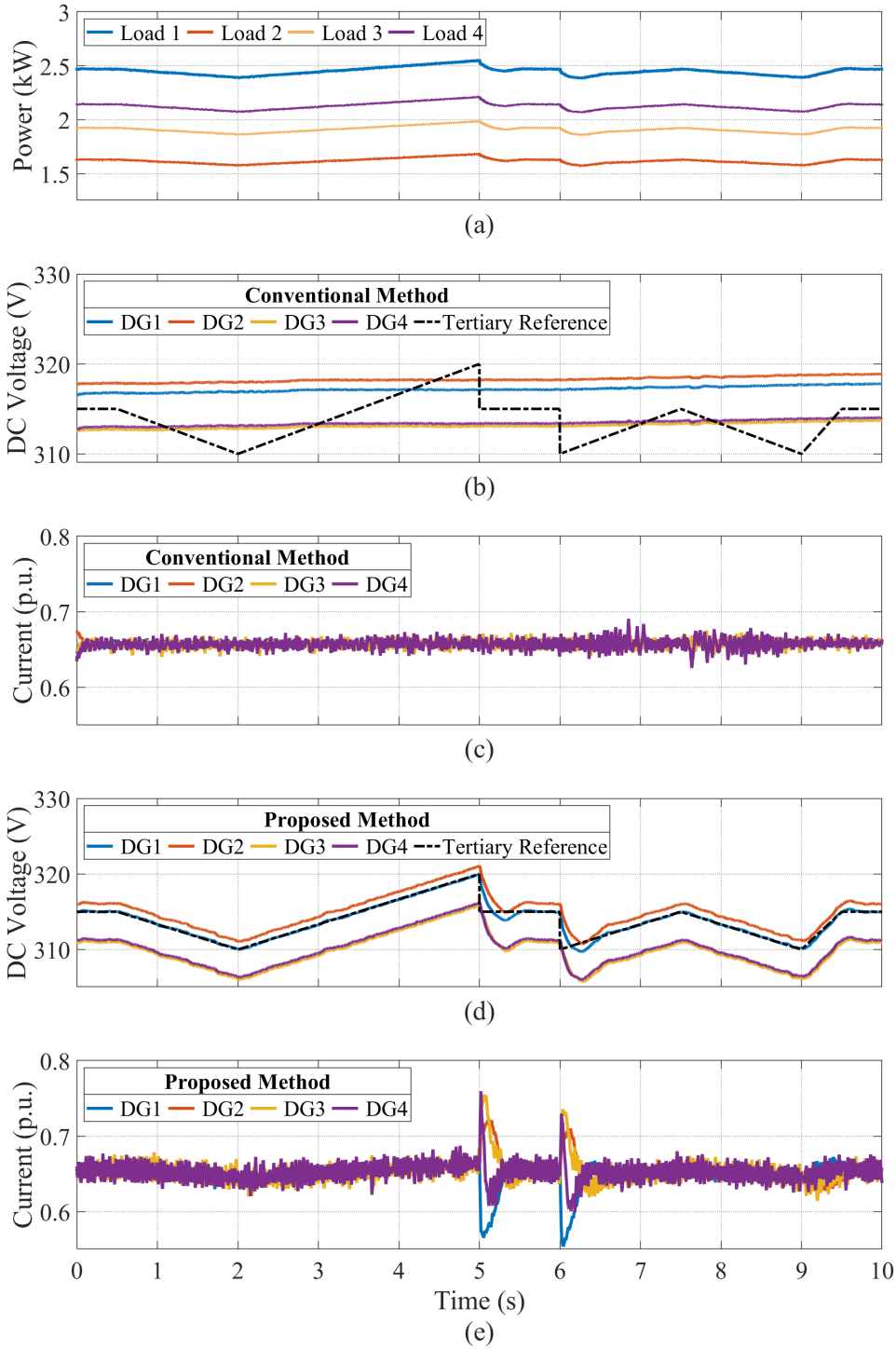

Fig. 4.4: System responses in the face of rapid changes in voltage references: (a) Profiles of load. (b) Standard secondary controller voltage output. (c) Standard secondary controller current output. (d) Voltages at the output using the proposed method. (e) Currents at the output using the proposed method [Paper C].

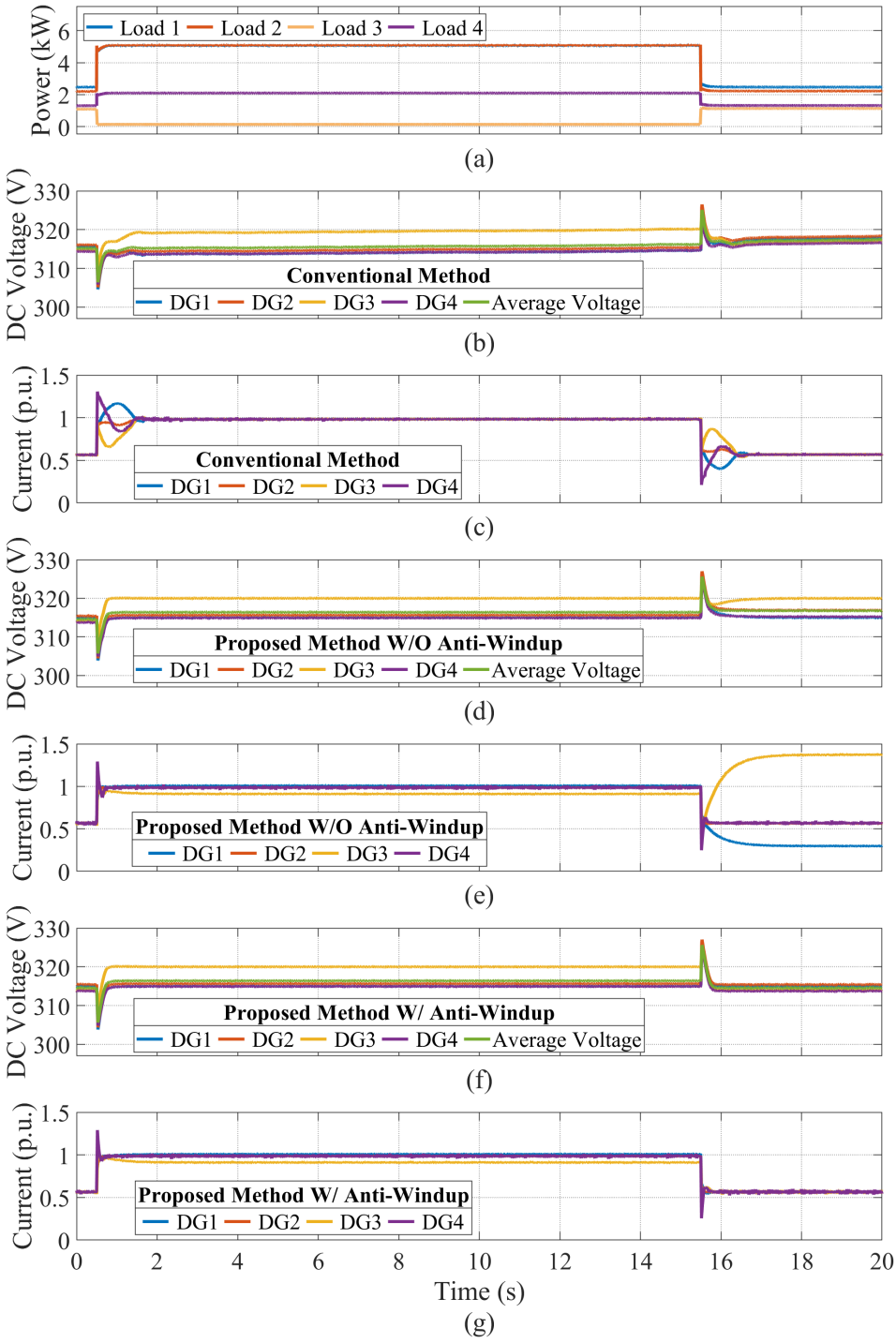

Fig. 4.5: System responses in the face of saturation in the controllers: (a) Profiles of load. (b) Standard secondary controller voltage output. (c) Standard secondary controller current output. (d) Voltages at the output using the proposed method without an integrator anti-windup logic. (f) The voltages at the output of the system after applying the anti-windup scheme. (g) Currents at the output using the proposed method with the anti-windup scheme [Paper C].

with the proposed integrator anti-windup logic, the reference voltages for the proposed method remain stable and quickly return to the normal range once the load returns to normal. The importance of limiting the voltage range and implementing an anti-windup logic for the stable performance of the distributed controller in the long term is highlighted by this simulation.

4.4 Conclusions

This chapter presents an enhanced distributed secondary controller for DCMGs that efficiently achieves voltage tracking, voltage consensus, and current distribution within the network. To address inter-unit communication risks and cybersecurity concerns, modifications were made to an existing literature-based distributed DCMG controller. Specifically, the voltage consensus formulation was replaced with a local current-based equivalent, reducing the reliance on inter-unit communication. The control law of the reference unit was also adjusted to respond solely to voltage commands from the tertiary controller, while other units played a role in establishing network conditions for voltage consensus and current sharing. Additionally, the inclusion of anti-windup logic was suggested to ensure system voltages remain within a safe range over extended periods. Through simulations on a DCMG system with four units, it was demonstrated that the proposed method successfully achieves all the abovementioned control goals.

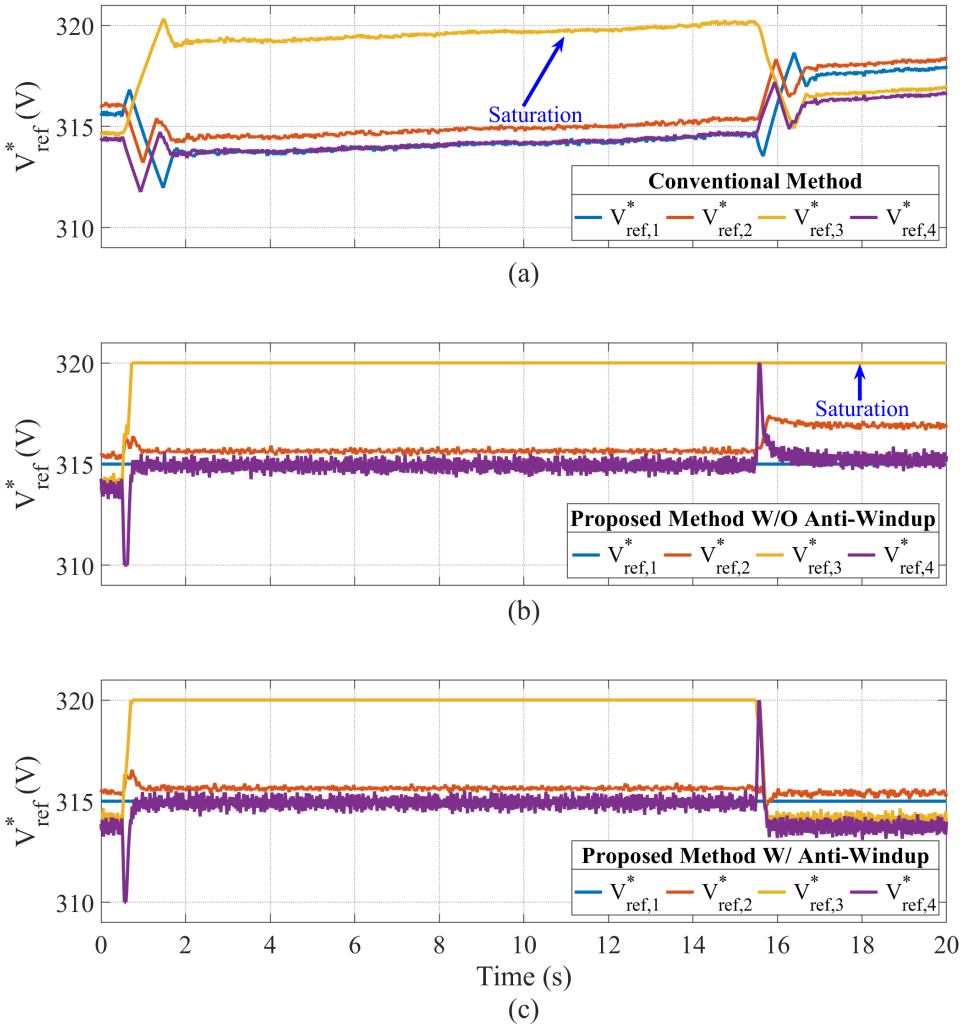

Fig. 4.6: Reference voltage profiles generated by the secondary controllers: (a) a conventional secondary controller. (b) Proposed secondary controller which does not include an integrator anti-windup logic. (c) Proposed secondary controller which includes the integrator anti-windup scheme [Paper C].

Chapter 5: DCMG Voltage Regulation: A LMI-based $H\infty$ Robust Control

5.1 Introduction

The main aim of this chapter is to formulate a model for voltage control of DC-DC power converters that can accurately track the voltage set-points received from the secondary control, even in the presence of noise in the sensor measurements and system delays. It is even more crucial to maintain acceptable performance according to IEEE standards when the load is simultaneously changing [52, 53]. To solve this problem, a PnP, robust voltage control scheme for DC-DC converters is suggested using a modified internal model.

5.2 Proposed RIMVC Strategy

As previously stated, this section for VSCs introduces a novel cascade control scheme with two distinct control loops, namely IMC and H_∞ robust control. The main goal of the suggested control scheme is to enhance the accuracy of voltage regulation and make it more resilient to model uncertainties by proficiently adhering to the secondary controller's set points.

To summarize the design procedure:

- A modified IMC scheme is employed to attain the required voltage setpoints tracking, according to the problem objectives (Inner loop).
- In order to enhance the system's capability to withstand different disturbances and uncertainties that cannot be addressed by the proposed IMC in the inner control loop, a H_∞ control scheme has been employed to compensate for the IMC shortcomings (Outer loop).

The following sections contain a brief discussion of the design procedures. Please refer to [Paper E] for more information on designing procedures of the IMC and H_∞ robust control systems utilized in this section.

5.2.1 IMC Design

The proposed IMC scheme's block diagram, employed as a voltage control scheme at the inner control loop of the main proposed cascade control system, is shown in Fig. 5.1.

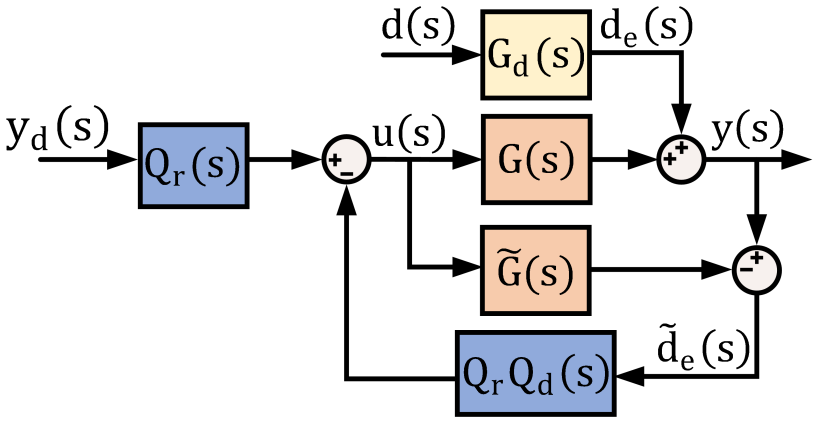

Fig. 5.1: Internal model control block diagram [Paper E].

The following assumptions must be taken into account in order to determine the output transfer function for each DG and move forward with the design process for modified IMC control in the inner loop.

Assumption 1: It is assumed that the external disturbance $n_i(t)$, where i belongs to the range of 1 to N, is restricted by $|n_i| \leq \rho$ and $|\dot{n}_i| \leq \sigma$. Here, ρ and σ are positive constants [54].

To simplify the IMC design procedure, it is necessary for the system matrix dimension to be squared, resulting in an equal number of inputs and outputs. For this reason, I_{L_i} and V_j are deemed as external inputs, requiring the inclusion of two virtual outputs in output vector $y_i = \begin{bmatrix} V_i & I_{L_i} & d_{buck_i} V_{dc_i} \end{bmatrix}^T$ to maintain a squared system matrix.

Following is a transfer function that outlines the input-output relationship for DG units:

$$\underbrace{\begin{bmatrix} Y_1(s) \\ Y_2(s) \\ Y_3(s) \end{bmatrix}}_{Y(s)} = \underbrace{\begin{bmatrix} G_{11}(s) & G_{12}(s) & G_{13}(s) \\ G_{21}(s) & G_{22}(s) & G_{23}(s) \\ G_{31}(s) & G_{32}(s) & G_{33}(s) \end{bmatrix}}_{G(s)} \underbrace{\begin{bmatrix} U_1(s) \\ U_2(s) \\ U_3(s) \end{bmatrix}}_{U(s)} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} N_i(s) \tag{5.1}$$

The outputs vector, inputs vector, sub-transfer functions, and external disturbance for each DG unit are represented by Y_i, U_i, G_{ij}, and N_i, respectively.

Assumption 2: We can safely assume that the elements of $G(s)$ are stable and that $G^{-1}(s)$ exists because we are dealing with a squared system. Furthermore, it is assumed that the equivalent model of $G(s)$ is perfect in order to have perfect control, which requires a perfect model. $\tilde{G}(s) = G(s)$ [55].

Additionally, to account for the system delay, the updated model's transfer function $G(s)$ can be reformulated using the Pade approximation. This involves incorporating the term $e^{-\tau s}$, as demonstrated below:

$$e^{-\tau s} \approx (\frac{1 - \frac{\tau}{2}s}{1 + \frac{\tau}{2}s}) \tag{5.2}$$

$$\tilde{G}(s) = G(s)(\frac{1 - \frac{\tau}{2}s}{1 + \frac{\tau}{2}s}) \tag{5.3}$$

Based on the control method shown in Fig. 5.1, the output equation can be determined as follows:

$$Y(s) = Q_r(s)\tilde{G}(s)Y_d(s) + (1 - Q_rQ_d(s)\tilde{G}(s))G_d(s)D(s) \tag{5.4}$$

The first part of this output equation, which comprises $Q_r(s)$ tracks desired changes in the voltage set-point, while the second part comprises $Q_d(s)$ keeps disturbance rejection at a certain level.

Even with the design of an ideal IMC controller and $G(s)$ perfectly modeled, achieving an inverse model of a process with integration elements is complicated. A stable and robust filter, such as $F(s)$, can compensate for mismatches between the main model ($G(s)$) and its equivalent ($\tilde{G}(s)$) [55]. According to [56], ensuring closed-loop stability in the presence of a mismatch can be achieved by setting the filter constants to sufficiently large values. The filter equation can be written as follows:

$$F(s) = \frac{as + b}{(1 + \lambda s)^n} \tag{5.5}$$

In order to ensure that tracking error remains zero even during rapid reference fluctuations like ramp changes, it is necessary to calculate values for a, b, λ, and n. More

information on how to appropriately choose these control parameters can be found in [Paper E]. According to the block diagram represented in Fig. 5.1, the following equations are obtained:

$$Q_r(s) = F(s)G_-^{-1}(s) \tag{5.6}$$

$$Q_d(s) = \frac{1 + \alpha_1 s + ... + \alpha_m s^m}{(\lambda s + 1)^m} \tag{5.7}$$

The values of $\alpha_1, ..., \alpha_m$ and λ must be determined in a way that strikes a balance between the speed of the system and the amount of effort exerted by the controller in order to guarantee complete disturbance rejection. According to the dynamics of the disturbances (with the assumed values of ρ and σ), a low-pass filter with a large time constant of $G_d(s) = \frac{1}{10s+1}$ and $\lambda = 0.05$ was selected for our study.

According to the block diagram represented in Fig. 5.1, the following equation can be obtained:

$$T_{dy}(s) = \frac{Y(s)}{D(s)} = (1 - Q_r Q_d(s)\tilde{G}(s))G_d(s) \tag{5.8}$$

The transfer function $T_{dy}(s)$, suggests that optimal performance is achieved when no frequencies from the input disturbances $D(s)$ are transmitted to the output $Y(s)$.

To ensure quick disturbance rejection, where no frequencies from the input disturbances are transmitted to the output, the parameters $Q_d(s)$ must be selected appropriately. This requires satisfying the following condition:

$$T_{dy}(s)|_{\substack{s=-0.1 \\ \lambda=0.05}} = 0 \tag{5.9}$$

By analyzing the transfer functions $G_d(s)$ and $T_{dy}(s)$, it can be seen that if the zero of $T_{dy}(s)$ is equal to the pole of $G_d(s)$ at $s = -0.1$, then the output $y(s)$ cannot be affected by the disturbance.

5.2.2 Robust Control Design

By combining modified IMC control with H_∞ feedback control, the anti-disturbance capability and robustness are enhanced even in the presence of model uncertainties and unknown disturbances. This proposed control method minimizes the H_∞ norm of the system transfer function, which effectively reduces the impact of external disturbances. This systematic approach is ideal for designing robust controllers for complex systems, which can handle nonlinearities and uncertainties in various applications. The general formulation for the robust control, as depicted in Fig. 5.2, is provided below.

$$\begin{bmatrix} z \\ y \end{bmatrix} = P(s) \begin{bmatrix} w \\ u \end{bmatrix} = \begin{bmatrix} P_{11}(s) & P_{12}(s) \\ P_{21}(s) & P_{22}(s) \end{bmatrix} \begin{bmatrix} w \\ u \end{bmatrix} \tag{5.10}$$

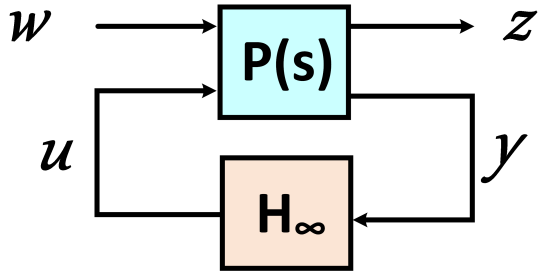

Fig. 5.2: Schematic of a typical robust control system [Paper E].

$P(s)$ is calculated using the following formula:

$$P(s) = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} + \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} (sI - A)^{-1}(B_1 B_2) \tag{5.11}$$

In the standard robust control configuration shown in Fig. 5.3, $G_{new}(s)$ can be interpreted as $P(s)$. To solve the H_∞ control problem, the controller $K(s)$ can be obtained by treating all the elements within the dashed lines as $G_{new}(s)$. Where u is the new control input, while u_1, u_2, $\tilde{V}_o$, ω, Z_i, and W_i are the IMC output signal, H_∞ feedback controller output signal, estimated output voltage, external disturbance input signal, weighted performance output, and weighting factors, respectively. The state-space model of $G_{new}(s)$ is needed for further design steps. The bellow equations apply to the generalized plant $G_{new}(s)$ description in state space realization.

$$G_{new,i}(s) : \begin{cases} \dot{x} &= (A_i + \Delta A_i)x + (B_{2,i} + \Delta B_{2,i})u + (B_{1,i} + \Delta B_{1,i})w \\ z_\infty &= (C_{1,i} + \Delta C_{1,i})x + (D_{12,i} + \Delta D_{12,i})u + (D_{11,i} + \Delta D_{11,i})w \\ y &= (C_{2,i} + \Delta C_{2,i})x + (D_{22,i} + \Delta D_{22,i})u + (D_{21,i} + \Delta D_{21,i})w \end{cases} \tag{5.12}$$

The system comprises several states $x = [x_1, x_2, x_3, x_4, x_5, x_6, x_7]^T$, control outputs $z_\infty = [z_1, z_2, z_3]^T$, measured outputs $y = [y_1, y_2]^T$, and control input vectors $u = [u_2]$, and disturbances vector $w = [\omega, u_1]^T$. For the i^{th} DGs, the system matrices comprise of A_i, $B_{1,i}$, $B_{2,i}$, $C_{1,i}$, $C_{2,i}$, $D_{11,i}$, $D_{12,i}$, $D_{21,i}$, and $D_{22,i}$. Additionally, the model uncertainties are expressed by ΔA_i, $\Delta B_{1,i}$, $\Delta B_{2,i}$, $\Delta C_{1,i}$, $\Delta C_{2,i}$, $\Delta D_{11,i}$, $\Delta D_{12,i}$, $\Delta D_{21,i}$, and $\Delta D_{22,i}$. It is important to note that these details are specific for the i^{th} DGs.

Assumption 3: The uncertainties components described in Eq. (5.12), should satisfy the following conditions:

- $\left\|\Delta A_i^T \Delta A_i\right\|_\infty \leq 1$.

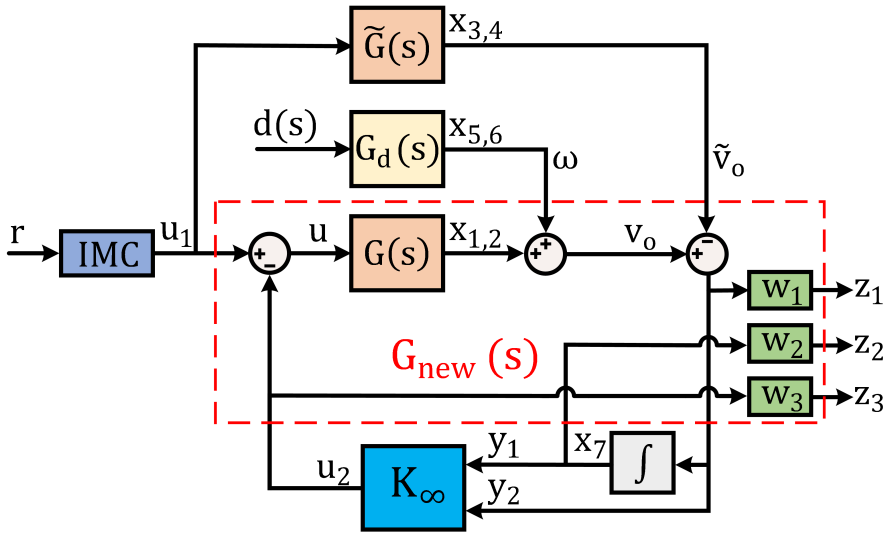

Fig. 5.3: The proposed H_∞ controller block diagram [Paper E].

- $\left\|\Delta B_{1,i}^T \Delta B_{1,i}\right\|_\infty \leq 1$ and $\left\|\Delta B_{2,i}^T \Delta B_{2,i}\right\|_\infty \leq 1$.
- $\left\|\Delta C_{1,i}^T \Delta C_{1,i}\right\|_\infty \leq 1$ and $\left\|\Delta C_{2,i}^T \Delta C_{2,i}\right\|_\infty \leq 1$.
- $\left\|\Delta D_{11,i}^T \Delta D_{11,i}\right\|_\infty \leq 1$ and $\left\|\Delta D_{12,i}^T \Delta D_{12,i}\right\|_\infty \leq 1$.
- $\left\|\Delta D_{21,i}^T \Delta D_{21,i}\right\|_\infty \leq 1$ and $\left\|\Delta D_{22,i}^T \Delta D_{22,i}\right\|_\infty \leq 1$.

The infinity norm is denoted by $\|\|_\infty$. Appendix A of [Paper E] contains all the matrices for the nominal systems.

Assumption 4: The following presumptions are made in accordance with [57], which states:

- The pair (A, B_1) is stabilizable and (C_1, A) is detectable.
- The pair (A, B_2) is stabilizable and (C_2, A) is detectable.
- $D_{12}^T \begin{bmatrix} C_1 & D_{12} \end{bmatrix} = \begin{bmatrix} 0 & I \end{bmatrix}$.

To keep it brief, the necessary calculations to verify Assumption 4, can be found in Appendix B of [Paper E].

To obtain a unique solution for the H_∞ control problem, it is necessary to consider $u_2 = K(s)y$, and ensure that $K(s)$ meets the inequality condition stated below:

$$\|T_{\omega\to z}(s)\|_\infty \triangleq \underset{s=jw}{sup} \frac{\|z(s)\|_2}{\|w(s)\|_2} \leq \gamma \tag{5.13}$$

$$T_{\omega\to z}(s) = P_{11} + P_{12}K(I - P_{22}K)^{-1}P_{21} \tag{5.14}$$

The function $T_{\omega\to z}(s)$ represents the relationship between a singular input *omega* and various outputs z. This means that $T_{\omega\to z}(s)$ has a H_∞ norm that is less than the minimum necessary value $\gamma > 0$. When selecting the weighting factors (W_i) for an $H\infty$ controller, it is important to consider both system robustness and performance. After making several iterations of testing, the final values of $W_1 = 30$, $W_2 = 20$, and $W_3 = 1$ were settled on as providing the optimal trade-off between stability and efficiency.

5.2.3 LMI Formulation

The LMI formulation utilized to calculate the controller $K(s)$ will be discussed in this section. A lemma that can convert $H\infty$ constraints into an LMI will be used to obtain the controller's $K(s)$ parameters.

Here are the five main stages involved in developing the LMI formulations needed to obtain the controller's $K(s)$ parameters [58]:
I) The parameters γ, Y, and X can be determined by solving the following optimization problem:

min γ
subject to:

$$\begin{cases} \begin{bmatrix} N_c & 0 \\ 0 & I \end{bmatrix}^T \begin{bmatrix} AY + YA^T & YC_1^T & B_1 \\ C_1Y & -\gamma I & D_{11} \\ B_1^T & D_{11}^T & -\gamma I \end{bmatrix} \begin{bmatrix} N_c & 0 \\ 0 & I \end{bmatrix} < 0 \\ \begin{bmatrix} N_o & 0 \\ 0 & I \end{bmatrix}^T \begin{bmatrix} A^TX + XA & XB_1 & C_1^T \\ B_1^TX & -\gamma I & D_{11}^T \\ C_1 & D_{11} & -\gamma I \end{bmatrix} \begin{bmatrix} N_o & 0 \\ 0 & I \end{bmatrix} < 0 \\ \begin{bmatrix} X & I \\ I & Y \end{bmatrix} \geq 0 \end{cases} \tag{5.15}$$

The bases of the null spaces of $(B_2^T D_{12}^T)$ and $(C_2 D_{21})$ are represented by N_c and N_o, respectively.

II) The following matrices are defined:

$$X_d = \sqrt{X - Y^{-1}} \qquad X_{cl} = \begin{bmatrix} X & X_d \\ X_d^T & I \end{bmatrix} \qquad \overline{A}_\infty = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$$

$$\underline{B}_\infty = \begin{bmatrix} 0 & B_2 \\ I & 0 \end{bmatrix} \qquad \overline{C}_{1\infty} = \begin{bmatrix} C_1 & 0 \end{bmatrix} \qquad \overline{B}_\infty = \begin{bmatrix} B_1 \\ 0 \end{bmatrix}$$

$$\underline{C}_{1\infty} = \begin{bmatrix} 0 & I \\ C_3 & 0 \end{bmatrix} \qquad \underline{D}_{12\infty} = \begin{bmatrix} 0 & D_{12} \end{bmatrix} \qquad \underline{D}_{21\infty} = \begin{bmatrix} 0 \\ D_{21} \end{bmatrix}$$

III) The following matrices must be calculated based on the above-mentioned matrices in order to have the LMIs:

$$\begin{cases} H_{X_{cl}} & = \begin{bmatrix} \overline{A}_\infty^T X_{cl} + X_{cl}\overline{A}_\infty & X_{cl}\overline{B}_\infty & \overline{C}_\infty^T \\ \overline{B}_\infty^T X_{cl} & -\gamma I & D_{11}^T \\ \overline{C}_\infty & D_{11} & -\gamma I \end{bmatrix} \\ P_{X_{cl}} & = \begin{bmatrix} \underline{B}_\infty^T X_{cl} & 0 & \underline{D}_{12\infty}^T \end{bmatrix} \\ Q_\infty & = \begin{bmatrix} \underline{C}_{1\infty} & \underline{D}_{21\infty} & 0 \end{bmatrix} \end{cases} \tag{5.16}$$

IV) The K_∞ can be obtained by satisfying the following LMI condition.

$$H_{X_{cl}} + Q_\infty^T K_\infty^T P_{X_{cl}} + P_{X_{cl}}^T K_\infty Q_\infty < 0 \tag{5.17}$$

where

$$K_\infty = \begin{bmatrix} A_{k\infty} & B_{k\infty} \\ C_{k\infty} & D_{k\infty} \end{bmatrix} \tag{5.18}$$

V) Finally, the matrices for the state space model of a closed-loop system are obtained as follows:

$$A_{cl_\infty} = \overline{A}_\infty + \underline{B}_\infty K_\infty \underline{C}_\infty \tag{5.19}$$

$$B_{cl_\infty} = \overline{B}_\infty + \underline{B}_\infty K_\infty \underline{D}_{21\infty} \tag{5.20}$$

$$C_{cl_\infty} = \overline{C}_\infty + \underline{D}_{12\infty} K_\infty C_1 \tag{5.21}$$

$$D_{cl_\infty} = D_{11} + \underline{D}_{12\infty} K_\infty \underline{D}_{21\infty} \tag{5.22}$$

In order to be concise, you can find the K_∞ matrices for unit 1 in Appendix C of [Paper E]. In [59], the LMI formulation is discussed in greater detail.

5.2.4 Proposed RIMVC for DCMGs using Boost Converters

In this section, we consider using the DC-DC boost converter in the DCMG system with RIMVC. However, it should be noted that the use of a DC-DC boost converter

in the new system configuration introduces nonlinearity. This nonlinearity arises from the presence of two terms, $(1 - d_{boost_i})V_i$ and $(1 - d_{boost_i})I_i$ in their model equations (Eq. (2.6)). The RIMVC scheme is smartly designed that allow it to effectively manage nonlinearities during the design process. This is achieved by utilizing the nominal model ($\tilde{G}(s)$) as a close approximation of the actual system ($G(s)$). As a result, the design steps for RIMVC remain consistent regardless of whether the DCMG utilizes linear or nonlinear converters.

5.3 Simulation Results

In this section, the effectiveness of the proposed RIMVC scheme for the DCMG system presented in Section 2.2.2 will be assessed. To achieve this, seven different simulation scenarios sharing the characteristics listed in [Paper E] will be analyzed. To keep things brief, a brief evaluation of each simulation scenario is presented here. For a more in-depth discussion of the effectiveness of the proposed RIMVC in a variety of challenging situations, refer to [Paper E, section 4]. Furthermore, as mentioned previously in Chapter 2, a summary of the parameters for the DG units and the connected distribution network of the DCMG under study is provided in Table 2.3 and Table 2.4, respectively.

5.3.1 Scenario 1: Tracking Voltage Reference Changes

This study compares the reference tracking quality of DGs 1 and 3 using the proposed RIMVC to the CC mentioned in [44]. The results displayed in Fig. 5.4 show that both the proposed RIMVC and the CC effectively track changes in the reference voltage with precision and speed. However, it is important to note that the proposed RIMVC outperforms the conventional method with a lower voltage tracking error and reduced energy consumption.

5.3.2 Scenario 2: Performance evaluation in the presence of rapid load fluctuations

Ensuring that output voltage deviation remains within an acceptable range during significant load shifts is a crucial aspect of voltage control schemes, which will be examined in this case study. The results depicted in Fig. 5.5 and Fig. 5.6 illustrate that all DG units function well with both RIMVC and CC, even under rapid load fluctuations. However, it is clear that RIMVC performs better in both transient and steady-state responses, effectively keeping output voltage deviations within the permissible range specified by the IEEE standard [53].

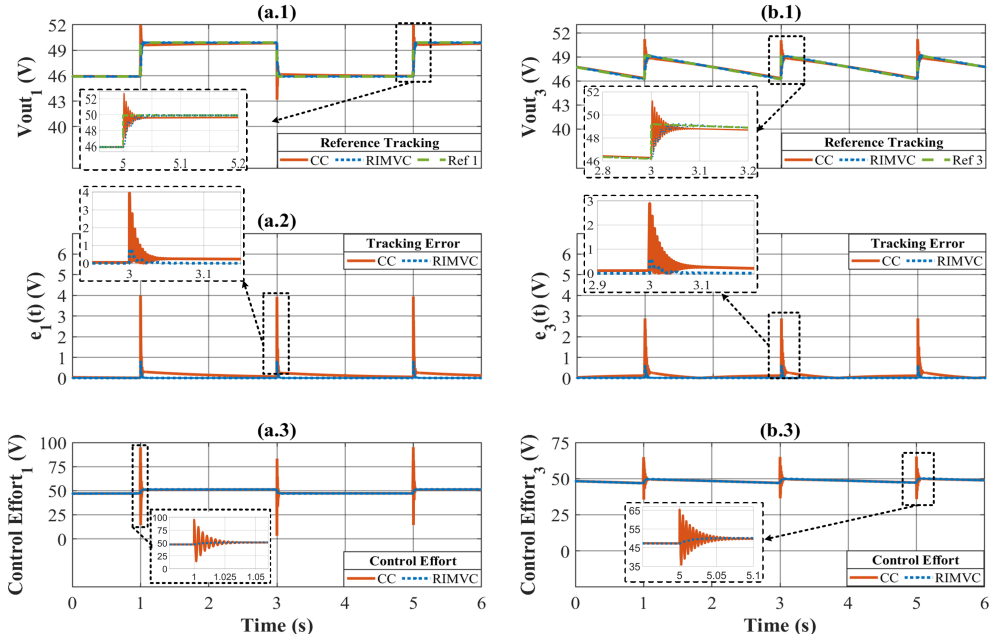

Fig. 5.4: Comparing the DG 1 and DG 3 in terms of their responsiveness to changes in the voltage reference: (a.1) The DG1 output voltage, (a.2) the DG1 voltage tracking error, and (a.3) the DG1 controller's effort, (b.1) The DG3 output voltage, (b.2) the DG3 voltage tracking error, and (b.3) the DG3 controller's effort [Paper E].

5.3.3 Scenario 3: PnP Capability Evaluation

In this case study, the capability of the RIMVC in terms of PnP functionality is compared to the CC. For this purpose, we unplug DG 5 at $t = 2s$ and plug it back in at $t = 4s$ (as depicted in Fig. 5.7). The topology changes affect DGs connected to DG 5 directly or indirectly. It is worth mentioning that all comparisons are made using an unbumped transfer scheme to ensure that the controller variables do not suddenly change, and the unplugging and re-plugging process goes off without a hitch. In [60], the bumpless transfer scheme procedure is delved into further, which was initially investigated for manual switching between various PIDs. As depicted in Fig. 5.8, RIMCV performs better in terms of voltage regulation for these DGs, all within IEEE standards for voltage and current deviations. After careful analysis, it has been determined that there is no need to make any adjustments to the local controller. The DCMG system is operating smoothly and the PnP capabilities of DG5 do not impact its overall performance.

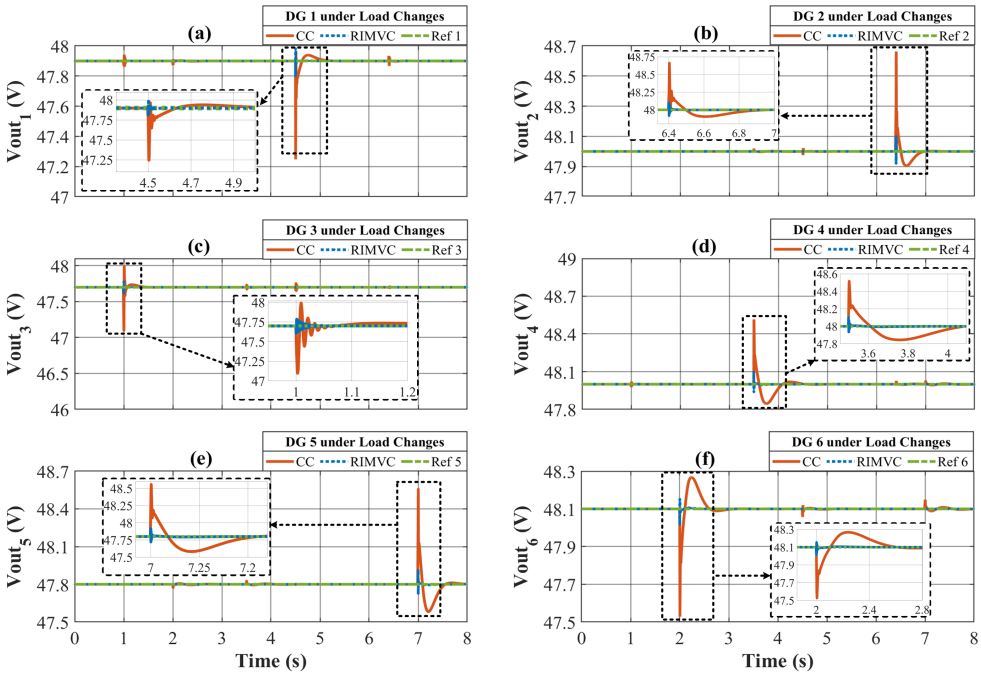

Fig. 5.5: The output voltages of the DGs varied with the load: (a) DG 1, (b) DG 2, (c) DG 3, (d) DG 4, (e) DG 5, and (f) DG 6 [Paper E].

5.3.4 Scenario 4: Robustness Evaluation in the Presence of Model Uncertainties

In this section, the RIMVC's ability to handle uncertainties in the parameters is analyzed. Since C_i, L_i and R_i are three common converter parameters that fluctuate frequently in practice, their uncertainty is being investigated. Transient stability (for a short period of time) and normal operation of a load connected to the dc bus of the DCMG system with 48 V can be maintained by supplying voltage in the range of 36 to 58 volts, as specified by the IEEE standards [53]. The RIMVC was tested by changing the converter parameters by 40%, as shown in Fig. 5.9, and the system remained stable throughout the test. However, the CC was unable to handle this level of instability. These results confirm the superior resiliency of the RIMVC in dealing with this level of uncertainty.

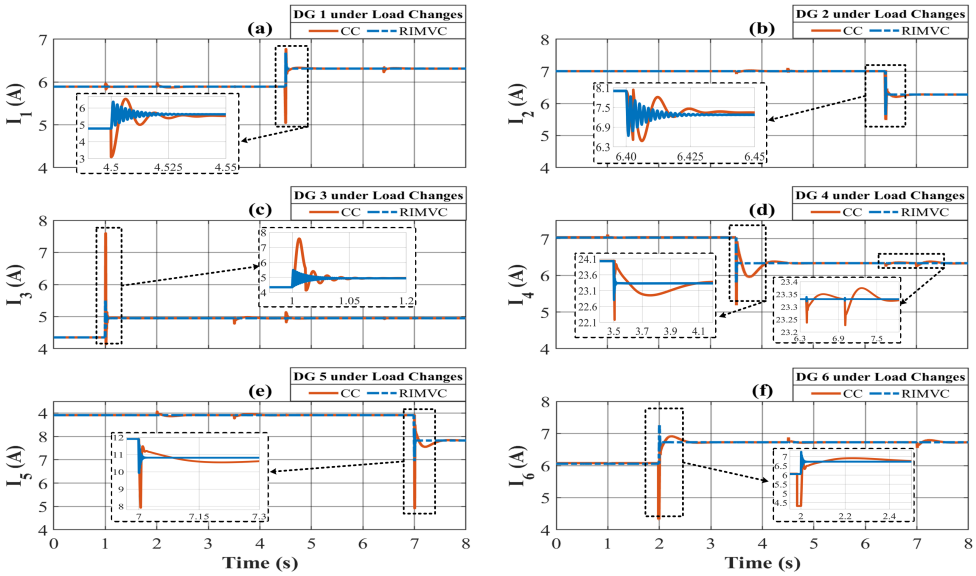

Fig. 5.6: The output currents of the DGs varied with the load: (a) DG 1, (b) DG 2, (c) DG 3, (d) DG 4, (e) DG 5, and (f) DG 6 [Paper E].

5.3.5 Scenario 5: RIMVC Performance Evaluation Using CPLs

This simulation scenario aims to evaluate the performance of RIMVC in handling various CPLs. Given that the IMC controller's control signal is defined as $u_i = d_{buck_i} V_{dc_i}$ (as earlier mentioned in Section 5.2.1), it follows that fluctuations in the input voltage source (V_{dc_i}) could be interpreted as internal disturbances that have a negative impact on the generated IMC control signal. These disturbances can cause the IMC to deviate from its desired control goals, so an additional control loop (H_∞ control) is required to ensure optimal system performance even in the presence of both model parameter uncertainties and unmodeled internal disturbances. The effectiveness and robustness of the RIMVC are demonstrated in Case Study 5, as shown in Fig. 5.10 and Fig. 5.11. The H_∞ controller (U2) compensated for the negative effects of the injected internal disturbances, while the final control effort signals (U) for the remaining DG units (DG 2, DG 4, DG 5, and DG6) remained constant. For units experiencing reference changes, the control effort is adjusted accordingly to guarantee a suitable reaction to the setpoint shifts.

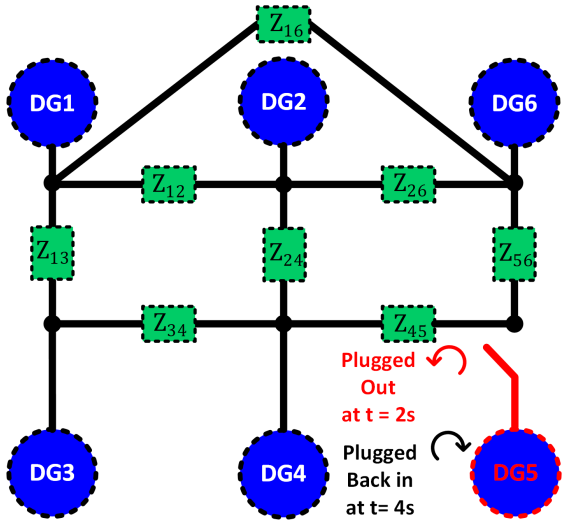

Fig. 5.7: DCMG configuration with the necessary changes for evaluating the PnP capabilities of the DG 5 [Paper E].

5.3.6 Scenario 6: DCMG with Boost Converters

This case study evaluates the RIMVC's adaptability for a DCMG with DC-DC boost converters in DG 1 and DG 2. It was previously stated that the use of step-up converters, such as boost converters, can introduce nonlinearities into the system model. As a result, by repeating simulation scenario 2 with internal disturbances caused by normal deviation in voltage sources, this case study investigates the effectiveness of RIMVC for this type of system. The proposed RIMVC ensures satisfactory functionality even for DCMG with step-up converters, as shown in Fig. 5.12 and 5.13.

5.3.7 Scenario 7: Performance Evaluation of the RIMVC for the DCMG with Internal Delay

In this case study, the proposed RIMVC is employed to assess the performance of two units (DG 1 and DG 5) under conditions where an external disturbance is injected simultaneously with a significant internal delay of 1 second (e^{-s}). The modified IMC controller generates the proper control signal to accomplish the desired control goals and keep the system performing acceptably, as was discussed in Section 5.2.1. Since time delay is a non-minimum phase term, the revised DG 5 model transfer function within the pade approximation (see Eq. (5.2)), can be written as follows:

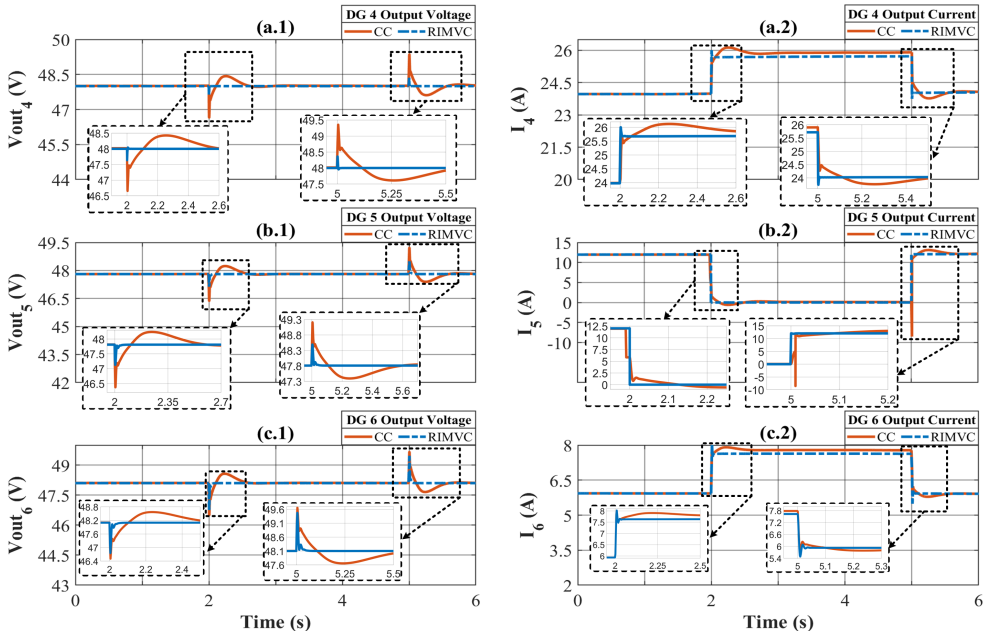

Fig. 5.8: Checking the DGs' PnP capabilities: (a) DG4's output voltage, (b) DG4's output current, (c) DG5's output voltage, (d) DG5's output current, (f) DG6's output voltage, and (g) DG6's output current [Paper E].

$$G_{5+}(s) = e^{-s} \tag{5.23}$$

$$G_{5-}(s) = G_5(s)G_{5+}^{-1}(s) \tag{5.24}$$

$$\tilde{G}_5(s) = G_5(s)\left(\frac{1-\frac{1}{2}s}{1+\frac{1}{2}s}\right) \tag{5.25}$$

The U1 and U2 collaborate together as shown in both Fig. 5.14(a.3) and Fig. 5.14(b.3) to remove the disturbances (Fig. 5.14(a.4) and Fig. 5.14(b.4)). In the presence of delay, however, IMC responds swiftly to changes in reference signals. In this case, despite the controller's reaction to reference changes at $t = 1$, the system output will change after a 1-second delay at $t = 2$. This delay affects the system's future, as shown in Reference Fig. 5.14(a.1) and Fig. 5.14(b.1).

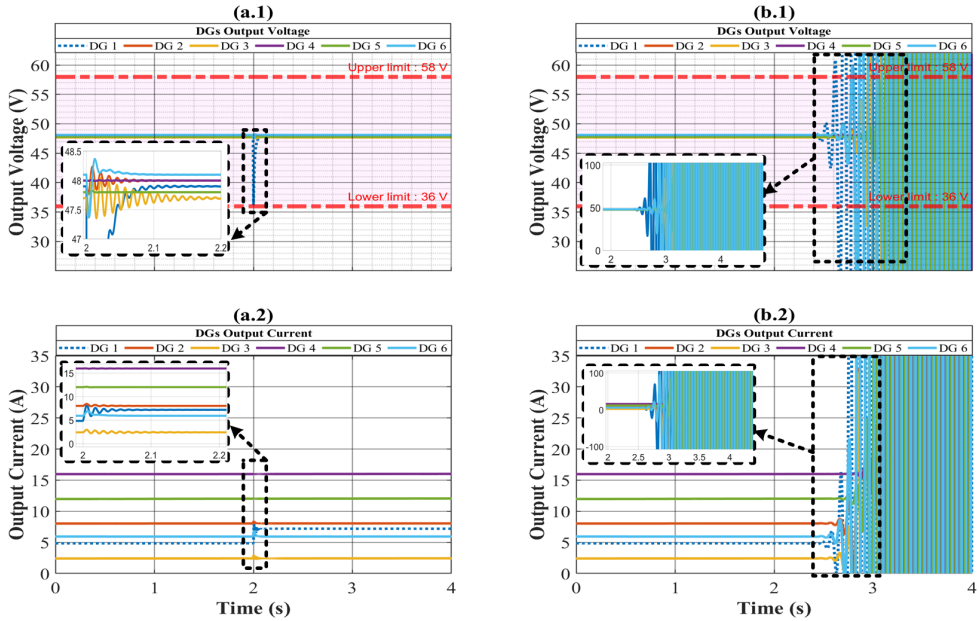

Fig. 5.9: Comparison of the proposed RIMVC's performance under varying DC-DC converter parameters due to model uncertainty in DG 1: Output voltage (a.1) and current (a.2) from DGs under RIMVC; (b.1) and (b.2) from DGs under conventional control; and (c.1) and (c.2) from DGs under RIMVC [Paper E].

5.4 Discussion

In Table 5.1, the Integral Absolute Error (IAE) and 2-norm of control effort of the RIMVC and CC are compared for performance evaluation of the considered DCMG. Due to its superior voltage tracking and ability to withstand the effects of parameter uncertainty, RIMVC consistently outperforms CC in all simulated scenarios. However, CC demonstrates instability in some simulation scenarios (scenarios 4, 5, 6, and 7), making these performance indices irrelevant.

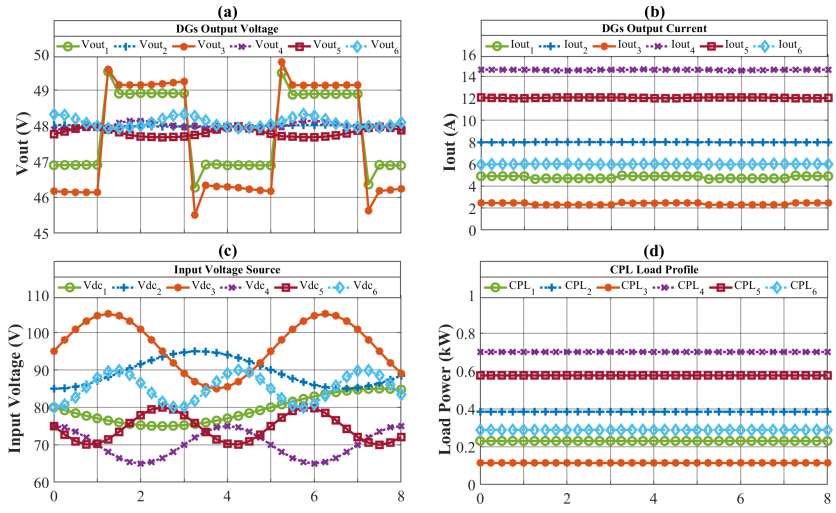

Fig. 5.10: Comparison of the proposed RIMVC's performance with CPLs under model parameters uncertainties: Output voltage (a) and current (b) from DGs under RIMVC; (c) DGs input voltage source, (d) CPLs Profile [Paper E].

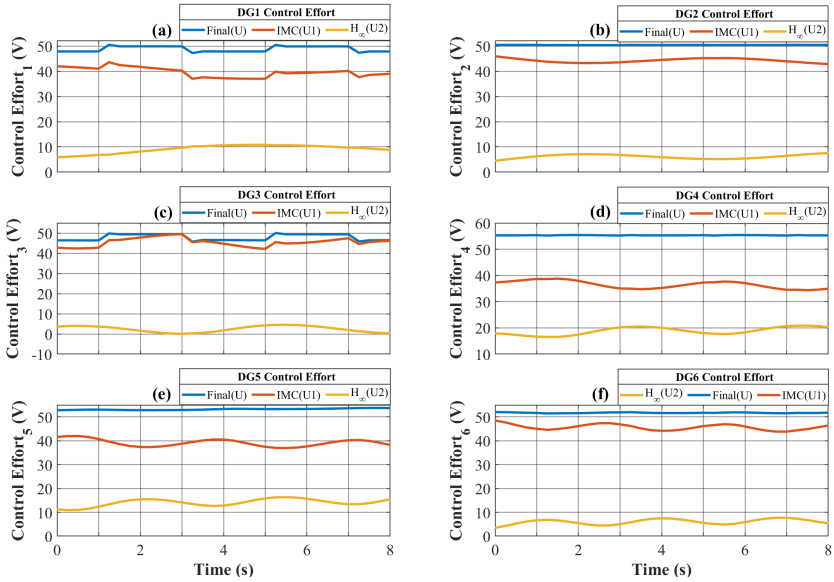

Fig. 5.11: All DGs' control effort signal: (a) DG 1, (b) DG 2, (c) DG 3, (d) DG 4, (e) DG 5, (f) DG 6 [Paper E].

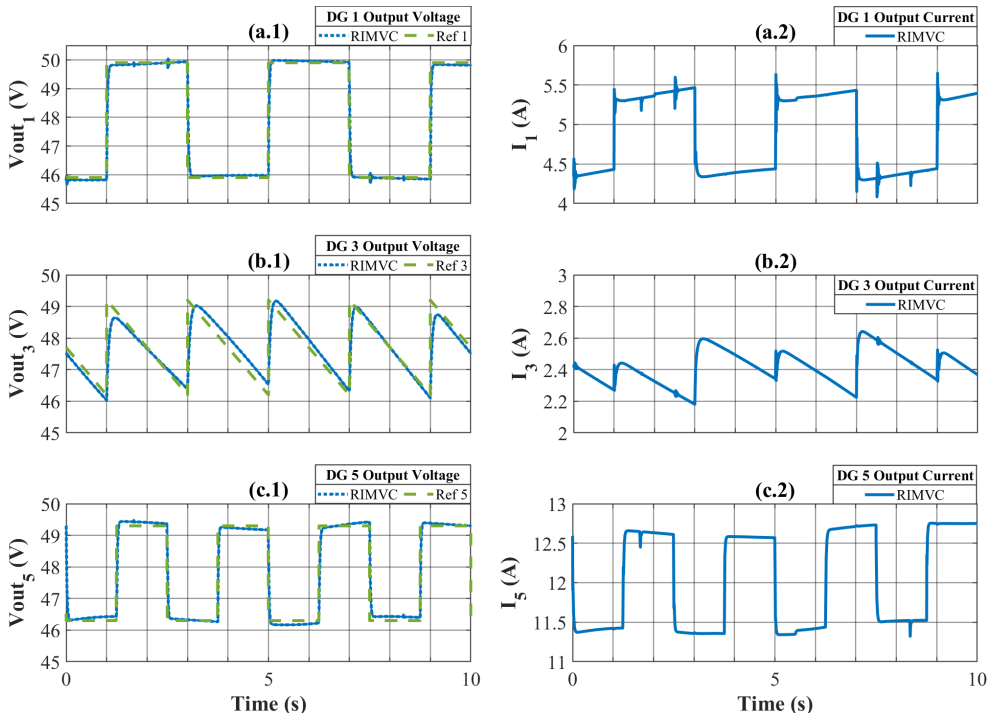

Fig. 5.12: Examination of the DC-DC boost converters' effect on the DCMG system's performance in DGs 3 and 5: (a.1) DG 1 Output Voltage; (a.2) DG 1 Output Current; (b.1) DG 3 Output Voltage; (b.2) DG 3 Output Current; (c.1) DG 5 Output Voltage; (c.2) DG 5 Output Current [Paper E].

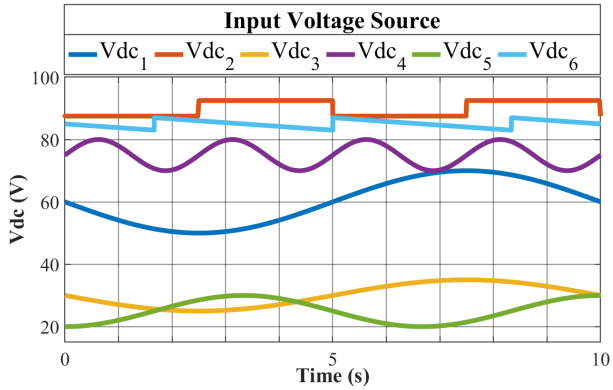

Fig. 5.13: All DGs' input voltage sources: (a) DG 1, (b) DG 2, (c) DG 3, (d) DG 4, (e) DG 5, (f) DG 6 [Paper E].

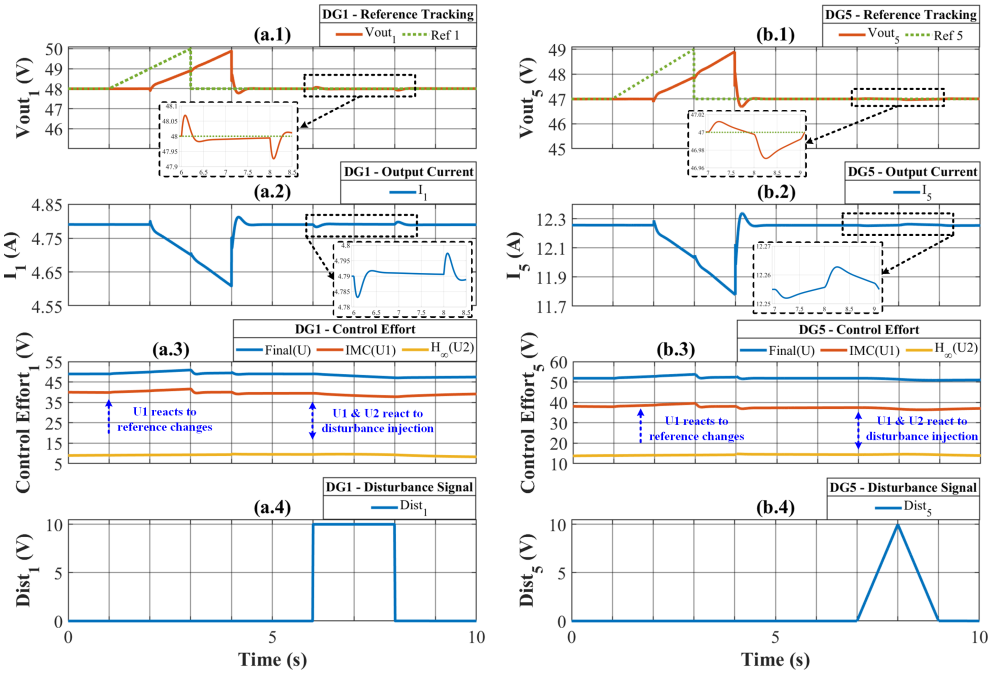

Fig. 5.14: Comparing the DG 1 and DG 5 in terms of 1 s time delay and voltage reference variations simultaneously: (a.1) The voltage at DG1's output, (a.2) The current at DG1's output, (a.3) DG1's controller effort, (a.4) External Disturbance Injection into DG 1, (b.1) DG5's output voltage, (b.2) DG5's output current, (b.3) DG5's controller effort, (b.4) External Disturbance Injection into DG 5 [Paper E].

Table 5.1: Examining the RIMVC's performance compared to the CC [Paper E]

Controller Type	Scenarios			
RIMVC	**Case Study 1**	**Case Study 2**	**Case Study 3**	**Case Study 4**
	DG1 → { IAE = 0.79, $\|u\|_2$ = 189.9 } DG3 → { IAE = 1.47, $\|u\|_2$ = 187.8 }	DG1 → { IAE = 0.87, $\|u\|_2$ = 178.4 } DG2 → { IAE = 1.03, $\|u\|_2$ = 179.8 } DG3 → { IAE = 1.17, $\|u\|_2$ = 181.1 }	DG4 → { IAE = 1.08, $\|u\|_2$ = 164.3 } DG5 → { IAE = 1.19, $\|u\|_2$ = 153.2 } DG6 → { IAE = 1.63, $\|u\|_2$ = 181.1 }	DG1 → { IAE = 0.67, $\|u\|_2$ = 213.2 } DG2 → { IAE = 0.41, $\|u\|_2$ = 196.5 } DG3 → { IAE = 0.84, $\|u\|_2$ = 187.6 }
	Case Study 5		**Case Study 6**	**Case Study 7**
	DG1 → { IAE = 7.597, $\|u\|_2$ = 189.2 } DG2 → { IAE = 5.604, $\|u\|_2$ = 195.4 } DG3 → { IAE = 7.406, $\|u\|_2$ = 185.6 }	DG4 → { IAE = 10.45, $\|u\|_2$ = 215.1 } DG5 → { IAE = 8.063, $\|u\|_2$ = 205.8 } DG6 → { IAE = 7.062, $\|u\|_2$ = 200.4 }	DG1 → { IAE = 1.03, $\|u\|_2$ = 189.9 } DG3 → { IAE = 5.646, $\|u\|_2$ = 187.5 } DG5 → { IAE = 2.256, $\|u\|_2$ = 205.5 }	DG1 → { IAE = 8.535, $\|u\|_2$ = 218.1 } DG5 → { IAE = 10.06, $\|u\|_2$ = 231.9 }
CC	**Case Study 1**	**Case Study 2**	**Case Study 3**	**Case Study 4**
	DG1 → { IAE = 6.42, $\|u\|_2$ = 199.9 } DG3 → { IAE = 6.21, $\|u\|_2$ = 198.7 }	DG1 → { IAE = 4.65, $\|u\|_2$ = 189.6 } DG2 → { IAE = 5.43, $\|u\|_2$ = 195.3 } DG3 → { IAE = 5.26, $\|u\|_2$ = 186.1 }	DG4 → { IAE = 5.85, $\|u\|_2$ = 200.3 } DG5 → { IAE = 4.37, $\|u\|_2$ = 187.2 } DG6 → { IAE = 4.61, $\|u\|_2$ = 233.1 }	DG1 → { IAE = Not Applicable, $\|u\|_2$ = Not Applicable } DG2 → { IAE = Not Applicable, $\|u\|_2$ = Not Applicable } DG3 → { IAE = Not Applicable, $\|u\|_2$ = Not Applicable }
	Case Study 5, 6, 7			
	Not Applicable			

5.5 Conclusions

For DCMGs, we employed a RIMVC using a 2-DoF IMC and H_∞ control methods. The simulation results proved that the RIMVC was capable of tracking the voltage setpoint, even with a wide range of disturbances. Deviations in load and voltage reference, unknown model parameters, and plug-and-play capabilities of each unit were all factored into the system's overall evaluation. The RIMVC is superior to the CC scheme in terms of performance when compared with schemes such as the one proposed in [44]. The study also shows that the proposed approach is effective at providing a fast-tracking response with a limited amount of control costs.

Chapter 6: Closing Remarks

The last section of this thesis presents a recap of the various topics covered in the earlier chapters, followed by an emphasis on the key findings of the research. Additionally, a brief mention of the future trends that are projected to advance this field of study will be included.

6.1 Summary

The introduction to this thesis provided an overview of deploying the local modern renewable energy-based MGs, including PV panels, wind turbines, energy storage systems, and other RESs. Then, the benefits of MG, DCMG in particular, for updating traditional power systems were also briefly discussed.
Distributed control systems are becoming increasingly popular for application in DCMG systems as a result of recent advances in communication technology. In this regard, different MG control architectures were introduced. The distributed control system faces cyber security issues due to its reliance on data transmission via communication links. Following a discussion of various types of DCMG control systems, particularly hierarchical control systems and their sublayers, namely primary, secondary, and tertiary layers, were introduced and a brief discussion of the communication system, which is more implemented for the MG systems was provided. DCMG's cyber vulnerabilities are then thoroughly discussed. Different types of cyber attacks that occur in DCMG systems were presented, emphasizing the need for a robust control system capable of dealing with these cyber attacks on the one hand and meeting the other technical and operational challenges on the other. To that end, through five research papers in the following chapter, this study attempted to provide affordable and appropriate solutions to the aforementioned challenges.

The second chapter introduced a comprehensive description of the system configuration as well as the mathematical model of the DCMG that was used in this thesis. Two different DCMG testbed models with varying system configurations and DG unit numbers were considered for the evaluation of the proposed control methods in the following chapters.

In Chapter 3, related to **Paper A**, a reliable estimator was proposed that uses ANFIS to detect and monitor malicious activities in real-time. This estimator is particularly useful for detecting FDI attacks in distributed control of DCMGs. By accurately estimating the output voltage and current of each DG unit, the proposed estimator can analyze the residual data between estimated and actual sensed signals to detect FDI attacks.

In **Paper B**, the proposed ANFIS-based estimator was used in a framework designed to detect and mitigate FDI attacks in DCMGs in real-time. The proposed framework relies on ANFIS as a supervised algorithm to accurately estimate the output voltage and current of all DG units. ANFIS was chosen for its efficiency, simplicity, and low computational burden. The proposed framework analyzes trends in the error signal generated by comparing estimated and actual sensed signals to detect and mitigate cyber-attacks. Using an OCPD method, the proposed framework makes it unnecessary to select a fixed threshold for residual analysis. Overall, the proposed framework provides an efficient and reliable solution to guarantee DCMG reliability and stability, as confirmed by the simulation analysis.

In Chapter 4, **Paper C** presented a solution for voltage consensus, current sharing, and reference voltage tracking in DCMGs with minimal reliance on neighboring units' information transmitted through communication links. The solution included a distributed secondary controller that leveraged physical relationships within the DCMG network, removing the need for local controllers to rely on voltage information from adjacent units. This was achieved by using local measurements of load and unit currents, along with line resistances, to achieve voltage consensus throughout the network. The control law for the unit responsible for tracking the reference voltage from an external tertiary controller was also modified to release it from all other responsibilities except for reference voltage tracking. Additionally, a saturation function on the secondary controller with an integrator anti-windup logic was suggested to maintain system stability.

In the fifth chapter, **Paper D** focused on the possibility of implementing an IMVC system for DCMGs. The biggest issue in voltage control of DC/DC converters is maintaining voltage reference tracking in the presence of unknown external disturbances and measurement noise while the load changes. To address this problem, a voltage control framework was proposed in **Paper D** that utilizes a model-based voltage controller for VSCs at the primary level. The effectiveness of this control scheme was evaluated by testing it against unknown external disturbances, rapid voltage reference changes, and load profile changes across multiple case study scenarios.

Moreover, in **Paper E**, an extended version of the IMVC for the DCMG system was proposed, with the aim of developing a robust version of the previously proposed IMVC to deal with challenges such as model parameter uncertainties. Voltage regulation in DC-DC converters of DCMGs is a difficult task because it requires accurately tracking

the voltage setpoints received from the secondary control, even when the noise in sensor measurements and system delays are present. In response to this challenge, **Paper E** proposes a PnP robust voltage control scheme by developing a voltage control scheme that can be utilized with various DC-DC converters, such as step-up and step-down converters.

6.2 Contribution

As an outcome of this Ph.D. study, several key contributions have been identified that set it apart from similar research endeavors. These contributions have been meticulously examined and analyzed to gain a comprehensive understanding of their potential value in the field. By presenting these findings in a detailed and organized manner, this study strives to contribute to the existing body of knowledge, ultimately benefiting the academic and practical communities.

- A DD framework has been developed that can monitor and detect malicious system activities in DCMGs in real-time. This framework can not only detect cyber-attacks but also identify the exact location of intrusion in either the current or voltage sensors of each DG unit, simplifying the mitigation process.
- An OCPD technique has been proposed which makes it unnecessary to select a fixed threshold for residual analysis
- An online attack mitigation mechanism has been proposed that can keep the system performance within acceptable limits without the need for unplugging attacked units during intrusions.
- Detecting cyber-attacks can be challenging due to the similar effects caused by FDIAs and regular load shifts on sensor measurements. The proposed framework for attack detection and mitigation addresses this issue by effectively minimizing false alarms.
- A secondary control scheme for DCMGs has been developed that relies less on cyber layer data and enables the reference unit to be followed more precisely by the tertiary controller. The system voltages are kept in a safe range by including lower and upper limits on the reference voltages, along with an anti-windup logic that enhances the stability and performance of the secondary controller.
- A fully decentralized robust voltage regulation control scheme has been proposed that provides PnP functionality for all DG units and can scale up to a high number of units.

- A RIMVC scheme has been developed to accurately track the voltage setpoints received from the secondary control, even in the presence of noise in the sensor measurements and system delays.

6.3 Future work

The field of MG security is still in the early stages of development, with numerous methods and techniques yet to be developed and implemented in a variety of applications. The following research areas are recommended for future studies based on the studies carried out in this Ph.D. thesis.

- In real-world scenarios, cyber-attacks can compromise data from sensors or data transfer links at the same time, especially in MG networks with a large number of sensors. As a result, detecting multi-attacks presents significant challenges and necessitates additional research.
- While various centralized and distributed cyber-attack detection strategies have been proposed, the majority of them are centered on false data injection attacks. Hackers with access to system information, on the other hand, may devise a covert attack that is difficult to detect. As a result, detecting covert attacks necessitates extensive research.
- It is important to note that current research focuses solely on detecting cyber-attacks and is incapable of eradicating attacks or restoring the system. As a result, developing a coordinated attack detection and mitigation and resilient control system is critical to ensuring the MGs' safe and stable operation and protecting it from physical destruction in the event of an attack.
- The current research is solely concerned with DCMG systems. However, because ACMG systems continue to play an important role in power systems, future research will focus on developing analysis and attack detection methods for both DC and ACMGs. ACMGs have more complex operational characteristics than DCMGs, making the design of attack detection more difficult.
- Finally, as the emphasis on decarbonization grows, more distributed MGs will emerge, and the penetration of renewable energy resources will continue growing. MG clusters will take the place of traditional power systems. As a result, investigating efficient attack detection and mitigation strategies for MG cluster systems is critical.

Chapter 7: References

References

[1] A. A. Bajwa, H. Mokhlis, S. Mekhilef, and M. Mubin, "Enhancing power system resilience leveraging microgrids: A review," *Journal of Renewable and Sustainable Energy*, vol. 11, no. 3, p. 035503, 2019.

[2] A. Maknouninejad, Z. Qu, F. L. Lewis, and A. Davoudi, "Optimal, nonlinear, and distributed designs of droop controls for dc microgrids," *IEEE Transactions on smart grid*, vol. 5, no. 5, pp. 2508–2516, 2014.

[3] A. Basati, M. B. Menhaj, and A. Fakharian, "Ga-based optimal droop control approach to improve voltage regulation and equal power sharing for islanded dc microgrids," in *2016 Electric Power Quality and Supply Reliability (PQ)*. IEEE, 2016, pp. 145–150.

[4] N. Ertugrul and D. Abbott, "Dc is the future [point of view]," *Proceedings of the IEEE*, vol. 108, no. 5, pp. 615–624, 2020.

[5] E. Shahradfar and A. Fakharian, "Optimal controller design for dc microgrid based on state-dependent riccati equation (sdre) approach," *Cyber-Physical Systems*, vol. 7, no. 1, pp. 41–72, 2021.

[6] A. Basati, A. Fakharian, and J. M. Guererro, "An intelligent droop control for improving voltage regulation and equal power sharing in islanded dc microgrids," in *2017 5th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, 2017, pp. 190–195.

[7] L. Xing, Q. Xu, F. Guo, Z.-G. Wu, and M. Liu, "Distributed secondary control for dc microgrid with event-triggered signal transmissions," *IEEE Transactions on Sustainable Energy*, vol. 12, no. 3, pp. 1801–1810, 2021.

[8] A. Basati, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, and S. Golestan, "A data-driven framework for fdi attack detection and mitigation in dc microgrids," *Energies*, vol. 15, no. 22, p. 8539, 2022.

[9] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple dc microgrid clusters," *Applied Energy*, vol. 310, p. 118425, 2022.

[10] N. M. Dehkordi, N. Sadati, and M. Hamzeh, "Distributed robust finite-time secondary voltage and frequency control of islanded microgrids," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3648–3659, 2017.

[11] B. Ning, Q.-L. Han, and L. Ding, "Distributed secondary control of ac microgrids with external disturbances and directed communication topologies: A full-order sliding-mode approach," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 3, pp. 554–564, 2021.

[12] J. M. Guerrero, M. Chandorkar, T.-L. Lee, and P. C. Loh, "Advanced control architectures for intelligent microgrids—part i: Decentralized and hierarchical control," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1254–1262, 2012.

[13] M. Faisal, M. A. Hannan, P. J. Ker, A. Hussain, M. B. Mansor, and F. Blaabjerg, "Review of energy storage system technologies in microgrid applications: Issues and challenges," *Ieee Access*, vol. 6, pp. 35 143–35 164, 2018.

[14] A. M. Jadhav, N. R. Patne, and J. M. Guerrero, "A novel approach to neighborhood fair energy trading in a distribution network of multiple microgrid clusters," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1520–1531, 2019.

[15] D. Mihailova, "Redefining business models for the energy transition: Social innovation and sustainable value creation in the european energy system," *Energy Research & Social Science*, vol. 100, p. 103114, 2023.

[16] B. Jones, R. J. Elliott, and V. Nguyen-Tien, "The ev revolution: The road ahead for critical raw materials demand," *Applied Energy*, vol. 280, p. 115072, 2020.

[17] R. M. Elavarasan, R. Pugazhendhi, M. Irfan, L. Mihet-Popa, I. A. Khan, and P. E. Campana, "State-of-the-art sustainable approaches for deeper decarbonization in europe–an endowment to climate neutral vision," *Renewable and Sustainable Energy Reviews*, vol. 159, p. 112204, 2022.

[18] M. J. Burke and J. C. Stephens, "Political power and renewable energy futures: A critical review," *Energy research & social science*, vol. 35, pp. 78–93, 2018.

[19] O. Dag and B. Mirafzal, "On stability of islanded low-inertia microgrids," in *2016 Clemson University Power Systems Conference (PSC)*. IEEE, 2016, pp. 1–7.

[20] N. Ertugrul and D. Abbott, "Dc is the future [point of view]," *Proceedings of the IEEE*, vol. 108, no. 5, pp. 615–624, 2020.

[21] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, "Ac-microgrids versus dc-microgrids with distributed energy resources: A review," *Renewable and sustainable energy reviews*, vol. 24, pp. 387–405, 2013.

[22] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, 2014.

[23] Q. Shafiee, T. Dragičević, J. C. Vasquez, and J. M. Guerrero, "Hierarchical control for multiple dc-microgrids clusters," *IEEE transactions on energy conversion*, vol. 29, no. 4, pp. 922–933, 2014.

[24] J. Ma, L. Yuan, Z. Zhao, and F. He, "Transmission loss optimization-based optimal power flow strategy by hierarchical control for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 32, no. 3, pp. 1952–1963, 2016.

[25] S. Islam, S. Agarwal, A. Shyam, A. Ingle, S. Thomas, S. Anand, and S. R. Sahoo, "Ideal current-based distributed control to compensate line impedance in dc microgrid," *IET Power Electronics*, vol. 11, no. 7, pp. 1178–1186, 2018.

[26] F. Guo, Q. Xu, C. Wen, L. Wang, and P. Wang, "Distributed secondary control for power allocation and voltage restoration in islanded dc microgrids," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 4, pp. 1857–1869, 2018.

[27] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, 2014.

[28] S. Peyghami, H. Mokhtari, P. Davari, P. C. Loh, and F. Blaabjerg, "On secondary control approaches for voltage regulation in dc microgrids," *IEEE Transactions on Industry Applications*, vol. 53, no. 5, pp. 4855–4862, 2017.

[29] L. Meng, Q. Shafiee, G. F. Trecate, H. Karimi, D. Fulwani, X. Lu, and J. M. Guerrero, "Review on control of dc microgrids and multiple microgrid clusters," *IEEE journal of emerging and selected topics in power electronics*, vol. 5, no. 3, pp. 928–948, 2017.

[30] C. Papadimitriou, E. Zountouridou, and N. Hatziargyriou, "Review of hierarchical control in dc microgrids," *Electric Power Systems Research*, vol. 122, pp. 159–167, 2015.

[31] A. Basati, J. Wu, J. M. Guerrero, and J. C. Vasquez, "Internal model-based voltage control for dc microgrids under unknown external disturbances," in *2022 International Conference on Smart Energy Systems and Technologies (SEST)*, 2022, pp. 1–6.

[32] M. Kermani, B. Adelmanesh, E. Shirdare, C. A. Sima, D. L. Carnì, and L. Martirano, "Intelligent energy management based on scada system in a real microgrid for smart building applications," *Renewable Energy*, vol. 171, pp. 1115–1127, 2021.

[33] I. Friedberg, D. Laverty, K. McLaughlin, and P. Smith, "A cyber-physical security analysis of synchronous-islanded microgrid operation," in *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3*, 2015, pp. 52–62.

[34] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[35] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[36] S. Hu, P. Yuan, D. Yue, C. Dou, Z. Cheng, and Y. Zhang, "Attack-resilient event-triggered controller design of dc microgrids under dos attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 2, pp. 699–710, 2019.

[37] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragičević, "Distributed screening of hijacking attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 7, pp. 7574–7582, 2019.

[38] T. Irita and T. Namerikawa, "Detection of replay attack on smart grid with code signal and bargaining game," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 2112–2117.

[39] Y. Yang, X. Wei, R. Xu, L. Peng, L. Zhang, and L. Ge, "Man-in-the-middle attack detection and localization based on cross-layer location consistency," *IEEE Access*, vol. 8, pp. 103 860–103 874, 2020.

[40] M. Ahmed and A.-S. K. Pathan, "False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, pp. 1–14, 2020.

[41] K. Paridari, N. O'Mahony, A. El-Din Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 113–128, 2018.

[42] C. Jin, P. Wang, J. Xiao, Y. Tang, and F. H. Choo, "Implementation of hierarchical control in dc microgrids," *IEEE transactions on industrial electronics*, vol. 61, no. 8, pp. 4032–4042, 2013.

[43] F. Gao, R. Kang, J. Cao, and T. Yang, "Primary and secondary control in dc microgrids: a review," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 2, pp. 227–242, 2019.

[44] M. Tucci, S. Riverso, J. C. Vasquez, J. M. Guerrero, and G. Ferrari-Trecate, "A decentralized scalable approach to voltage control of dc islanded microgrids," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 6, pp. 1965–1979, 2016.

[45] V. Venkatasubramanian, H. Schattler, and J. Zaborszky, "Fast time-varying phasor analysis in the balanced three-phase large electric power system," *IEEE Transactions on Automatic Control*, vol. 40, no. 11, pp. 1975–1982, 1995.

[46] T. Glad and L. Ljung, *Control theory*. CRC press, 2000.

[47] J.-S. Jang, "Anfis: adaptive-network-based fuzzy inference system," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 23, no. 3, pp. 665–685, 1993.

[48] A. Basati, N. Bazmohammadi, J. M. Guerrero, and J. C. Vasquez, "Real-time estimation in cyber attack detection and mitigation framework for dc microgrids," in *2023 23rd International Scientific Conference on Electric Power Engineering (EPE)*, 2023, pp. 1–6.

[49] S. Aminikhanghahi and D. J. Cook, "A survey of methods for time series change point detection," *Knowledge and information systems*, vol. 51, no. 2, pp. 339–367, 2017.

[50] S. Sahoo and S. Mishra, "A distributed finite-time secondary average voltage regulation and current sharing controller for dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 282–292, 2017.

[51] A. Basati, S. Bashash, J. M. Guerrero, and J. C. Vasquez, "Distributed finite-time secondary control for dc microgrids with reduced internetwork data transmission dependency," in *2023 International Conference on Future Energy Solutions (FES2023)*, 2023, pp. 1–6.

[52] J. C. Smith, G. Hensley, and L. Ray, "Ieee recommended practice for monitoring electric power quality," *IEEE std*, pp. 1159–1995, 1995.

[53] IEEE, "Ieee standard for dc microgrids for rural and remote electricity access applications," *IEEE Std 2030.10-2021*, pp. 1–47, 2021.

[54] A. Basati, J. M. Guerrero, J. C. Vasquez, A. Fakharian, K. H. Johansson, and S. Golestan, "Robust internal model-based voltage control for dc microgrids: An lmi based h_∞ control," *Sustainable Energy, Grids and Networks*, vol. 35, p. 101094, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352467723001029

[55] Y. Wang, Z. H. Xiong, and H. Ding, "Robust internal model control with feedforward controller for a high-speed motion platform," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2005, pp. 187–192.

[56] C. E. Garcia and M. Morari, "Internal model control. a unifying review and some new results," *Industrial & Engineering Chemistry Process Design and Development*, vol. 21, no. 2, pp. 308–323, 1982.

[57] J. Doyle, K. Glover, P. Khargonekar, and B. Francis, "State-space solutions to standard h/sub 2/ and h/sub infinity / control problems," *IEEE Transactions on Automatic Control*, vol. 34, no. 8, pp. 831–847, 1989.

[58] S. Skogestad and I. Postlethwaite, *Multivariable feedback control: analysis and design*. Citeseer, 2007, vol. 2.

[59] C. Scherer, P. Gahinet, and M. Chilali, "Multiobjective output-feedback control via lmi optimization," *IEEE Transactions on Automatic Control*, vol. 42, no. 7, pp. 896–911, 1997.

[60] K. J. Åström, T. Hägglund, and K. J. Astrom, *Advanced PID control*. ISA-The Instrumentation, Systems, and Automation Society Research Triangle Park, 2006, vol. 461.

Part II

Papers

Paper A

Real-Time Estimation in Cyber Attack Detection and Mitigation Framework for DC Microgrids

Amir Basati, Najmeh Bazmohammadi, Josep M. Guerrero, and Juan C. Vasquez

The paper has been published in the
Proceedings International Scientific Conference on Electric Power Engineering (EPE 2023), Brno, Czech Republic, 2023.

The layout has been revised.

Paper B

A Data-Driven Framework for FDI Attack Detection and Mitigation in DC Microgrids

Amir Basati, Josep M Guerrero, Juan C Vasquez, Najmeh Bazmohammadi and Saeed Golestan

The paper has been published in the
Journal, Energies 2022, 15(22), 8539. https://doi.org/10.3390/en15228539.

The layout has been revised.

Paper C

Distributed Finite-Time Secondary Control for DC Microgrids with Reduced Internetwork Data Transmission Dependency

Amir Basati, Saeid Bashash, Josep M Guerrero, and Juan C Vasquez

The paper has been published in the
Proceedings International Conference on Future Energy Solutions (FES2023), Vaasa, Finland, 2023.

The layout has been revised.

Paper D

Internal Model-based Voltage Control for DC Microgrids Under Unknown External Disturbances

Amir Basati, Jingxuan Wu, Josep M Guerrero, and Juan C Vasquez

The paper has been published in the
*Proceedings*2022 International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, Netherlands, 2022, pp. 1-6.
https://doi.org/10.1109/SEST53650.2022.9898430.

The layout has been revised.

Paper E

Robust Internal Model-based Voltage Control for DC Microgrids: An LMI Based H_∞ Control

Amir Basati, Josep M Guerrero, Juan C Vasquez, Ahmad Fakharian, Karl Henrik Johansson, and Saeed Golestan

The paper has been published in the
*Journal*Sustainable Energy, Grids and Networks (SEGAN) - Elsevier, Vol. 35, p. 101094, 2023.
https://www.sciencedirect.com/science/article/pii/S2352467723001029.

The layout has been revised.

ISSN (online): 2446-1636
ISBN (online): 978-87-7573-676-8

AALBORG UNIVERSITY PRESS