分类号：TM76　　学校代码：10363
密　级：公开　　学　　号：2220310110

安徽工程大学
Anhui Polytechnic University

硕士学位论文

题目　混合网络攻击下的微电网分布式二次控制研究

论文作者　郭端娇
指导教师　葛愿　教授
学科（专业）　电气工程
研究方向　电力系统及其自动化

论文提交日期：2025 年 05 月 19 日

分类号：TM76　　单位代码：10363

密　级：公开　　学　　号：2220310110

题　　目　混合网络攻击下的微电网分布式二次控制研究

题　　目　RESEARCH ON DISTRIBUTED SECONDARY CONTROL OF MICROGRIDS UNDER HYBRID CYBER ATTACKS

学 生 姓 名 ：　郭 端 娇

校 内 导 师 ：　葛愿　教授

专 业 (领 域) ：　电 气 工 程

研究方向(领域)：　电力系统及其自动化

论 文 答 辩 日 期 ：　2025 年 05 月 11 日

安徽工程大学学位论文原创性声明

本人郑重声明：我恪守学术道德，崇尚严谨学风。所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已明确注明和引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品及成果的内容。论文为本人亲自撰写，我对所写的内容负责，并完全意识到本声明的法律后果由本人承担。

学位论文作者签名：郭端妍

日期：2025年 05月 19日

安徽工程大学学位论文版权使用授权书

学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅或借阅。本人授权安徽工程大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密 □，在 ____ 年解密后适用本版权书。

本学位论文属于

不保密 ☑。

学位论文作者签名：郭端妍　　指导教师签名：

日期：2025 年 05 月 19 日　　日期：2025 年 05 月 19 日

混合网络攻击下的微电网分布式二次控制研究

摘 要

新能源分布式发电技术发展推动直流微电网成为智能电网关键部分。其采用的分布式分层控制含一、二、三次控制，其中二次控制通信易受拒绝服务(Denial of Service, DoS)和虚假数据注入(False Data Injection, FDI)攻击，威胁系统安全运行。针对混合攻击下的电压偏差、均流误差与通信安全问题，本研究提出分阶段解决方案，经理论建模、策略创新与仿真验证，构建高可靠分布式控制体系。

（1）首先针对传统下垂控制导致的母线电压偏差与分布式电源(Distributed Generation, DG)输出电流比例失衡问题，本文中研究了一种分布式二次控制方法。通过构建基于下垂控制的一次控制层和包含通信系统的分布式二次控制层相结合的分层模型，用图论描述通信拓扑，推导微电网潮流动态方程。融合电压与电流误差反馈设计二次控制器，实现调压与均流。基于 Matlab/Simulink 建立直流微电网模型验证了该方案在负载突变等场景下，该方案可快速消除电压偏差，精准维持电流输出，与传统集中式方案相比显著提升了系统鲁棒性。

(2)其次针对开放通信环境下 FDI 和 DoS 混合攻击的协同干扰，研究建立了 FDI 攻击的信息篡改模型与 DoS 攻击的脉冲阻塞模型，揭示混合攻击对分布式控制的协同破坏机理。在此基础上，建立了一

种弹性事件触发控制架构。该架构由两个分别基于母线电压误差反馈和支路电流误差反馈的两个子控制器，以及事件触发管理器组成。管理器根据系统状态动态切换子控制器。同时，在二次控制器中引入补偿机制，以抵消存在 DoS 攻击下连续时间 FDI 攻击的影响。

(3)最后为进一步解决控制器在 DoS 攻击密集时段的潜在失效问题，并弥补不能重构 FDI 攻击信号的不足，设计了一种融合弹性周期采样与 FDI 攻击缓解层的策略。在二级控制层引入弹性周期采样，动态调整通信间隔减少数据丢失，同时降低通信资源消耗。增设基于神经网络的 FDI 攻击缓解层，对采样数据进行实时优化与虚假信息过滤，并结合攻击特征分析实现 FDI 攻击信号的重构。

本文为高安全直流微电网的设计提供了理论支撑与技术方案，具有显著的工程应用潜力。

关键词：直流微电网，调压均流，分布式二次控制，FDI 攻击，DoS 攻击

RESEARCH ON DISTRIBUTED SECONDARY CONTROL OF MICROGRIDS UNDER HYBRID CYBER ATTACKS

Abstract

The development of new distributed energy generation technology promotes DC microgrid as a key part of the smart grid. The distributed hierarchical control it adopts includes primary, secondary and tertiary control, where the secondary control communication is vulnerable to denial of service (DoS) and false data injection (FDI) attacks, which threaten the safe operation of the system. Aiming at the problems of voltage deviation, current sharing error and communication security under hybrid attacks, this study proposes a step-by-step solution to construct a highly reliable distributed control system through theoretical modelling, strategy innovation and simulation verification.

(1) First, to solve the problem of imbalance between bus voltage deviation and distributed generation (DG) output current ratio caused by traditional droop control, this study proposes a distributed secondary control method. By constructing a layered model combining the primary

control layer based on droop control and the distributed secondary control layer including the communication system, the communication topology is described by graph theory, and the dynamic equations of microgrid flow are derived. The secondary controller is designed by integrating voltage and current error feedback to achieve voltage recovery and proportional current sharing. Matlab/Simulink-based modelling of the DCMG verifies that the scheme can quickly eliminate voltage deviation and accurately maintain current output in scenarios such as sudden load changes, which significantly improves the system robustness compared with the traditional centralised scheme.

(2) Secondly, for the synergistic interference of FDI and DoS hybrid attacks in open communication environment, the study establishes the information tampering model of FDI attack and the impulse blocking model of DoS attack to reveal the synergistic damage mechanism of hybrid attacks on distributed control. On this basis, a hierarchical elastic event-triggered control architecture is proposed. The architecture consists of two sub-controllers based on bus voltage error feedback and branch current error feedback, respectively, and an event-triggered manager. The manager dynamically switches the sub-controllers according to the bus system state. Meanwhile, a compensation mechanism is introduced in the secondary controller to counteract the continuous-time FDI attack in the presence of DoS attacks.

(3) Finally, to further address the potential failure of the controller during the intensive period of the DoS attack and to compensate for the lack of active compensation for FDI attacks, a strategy that integrates elastic period sampling and attack reconfiguration is proposed. Elastic period sampling is introduced at the secondary control layer to dynamically adjust the communication interval to reduce data loss while reducing the consumption of communication resources. A neural network-based FDI attack mitigation layer is added to perform real-time optimisation and false information filtering on the sampled data, and combined with attack characterisation to achieve active estimation and compensation of FDI attacks.

This study provides theoretical support and technical solutions for the design of high-security DC microgrids with significant potential for engineering applications.

Duanjiao Guo (Electrical Engineering)

Supervised by Prof. Yuan Ge

KEYWORDS: DC Microgrid, Voltage Regulation and Current Sharing, Distributed Secondary Control, False Data Injection (FDI) Attack, Denial of Service (DoS) Attack

目录

第 1 章 绪论

1.1 研究背景及意义

各国政府与科研机构正在加速推进可再生能源开发，致力于构建低碳高效的分布式能源系统[1-3]。风力、光伏等新能源凭借清洁性与可再生性成为能源转型的核心方向，然而其发电特性与自然条件深度耦合，导致功率输出具有显著随机性和间歇性。这种不可控性在并网阶段易诱发电压波动、频率偏移及谐波污染等异常现象，不仅降低供电质量，还可能危及电力系统的安全稳定运行[4-5]。尤其在大规模新能源并网场景下，源荷双侧的不确定性叠加使得传统集中式电网架构的调节能力面临严峻挑战，亟需探索新型电力系统解决方案。

在此背景下，微电网技术作为分布式能源消纳的有效载体应运而生。通过构建“源-网-荷-储”协同运行的区域性能源网络，微电网实现了可再生能源的就地消纳与灵活调控，显著降低了新能源波动对主电网的冲击。相较于交流微电网，直流微电网在系统架构与控制策略方面展现出独特优势：首先，直流系统天然规避了交流电网中复杂的无功补偿问题，简化了变流器拓扑结构与控制逻辑；其次，直流母线无需考虑频率稳定性与相位同步，更适应新能源发电单元与储能装置的即插即用需求；此外，直流微电网在传输损耗、电能质量、故障隔离等方面具有显著优势，特别适用于数据中心、船舶电力、偏远地区供电等特定应用场景[6-8]。这些技术优势推动直流微电网成为智能配用电领域的重要研究方向，其控制策略的优化设计也成为学术界与工业界共同关注的焦点。

直流微电网控制系统普遍采用分层控制架构，其中二次控制层承担着电压恢复与电流分配的核心功能[9-10]。控制系统根据实施方式的不同，可分为三大类：集中式、分散式和分布式[11-12]。传统集中式控制依赖中央控制器实现全局信息处理，但存在系统扩展性与容错性的固有缺陷。分散式控制的特征是分布式电源(Distributed Generation, DG)单元各自控制器间无通讯通道，虽然结构简单，但灵活性和可靠性均较低。而随着微网的发展，其运行状态变得更加复杂，分散控制一般作为底层控制基础，与其他控制模式相配合。分布式控制策略通过相邻单元间的局部信息交互实现全局目标，不仅增强了系统冗余度与可靠性，还能更好地

契合微电网分布式电源的地理特性。分布式控制融合了集中式与分散式控制的优势，弥补了二者的不足，无需设置控制中心，也无需全局信息，实现微网的整体一致性协作[13-14]。基于一致性算法的分布式二次控制器通过设计合理的交互协议，能够在无需全局通信网络的情况下实现母线电压调节与输出电流的合理分配，有效提升了系统对拓扑变化的适应能力。然而，这种依赖于通信网络的信息交互机制也引入了新的安全隐患，使得网络攻击成为威胁直流微电网稳定运行的关键风险因素。

复杂网络环境中，分布式控制系统的通信链路面临较高的安全风险，极易受到恶意攻击者对信息完整性、可用性的破坏。其中最具代表性且防御难度较大的两种攻击类型分别是虚假数据注入(False Data Injection, FDI)和拒绝服务(Denial of Service, DoS)攻击[15-17]。FDI 攻击通过篡改节点间传输的电压、电流等关键状态信息，诱导控制器产生错误决策，导致电压失稳或电流分配失衡等问题。DoS 攻击则通过阻塞通信通道或耗尽网络资源，中断控制器间的正常信息交互，使系统退化为开环运行状态。这两类攻击具有隐蔽性强、破坏性大的特点，传统的基于固定阈值或静态模型的检测方法往往难以实时识别攻击特征[18-19]。更为严峻的是，孤岛运行的直流微电网缺乏大电网支撑，攻击引发的局部故障可能通过分布式控制协议快速扩散，引发级联失效甚至系统崩溃。现有研究多聚焦于理想通信条件下的控制器设计，对网络攻击下系统安全运行机制的探索仍存在理论上的不足，亟需构建具有主动防御能力的弹性控制体系。

面对能源转型与数字化转型的双重趋势，直流微电网既承载着提升可再生能源消纳能力的使命，也面临着网络安全威胁带来的全新挑战。针对 FDI 与 DoS 攻击设计具有强鲁棒性的分布式二次控制器，需要突破传统控制理论框架，在攻击检测、弹性控制、容错机制等维度开展系统性创新：在理论层面，需要建立网络攻击影响下系统动态特性的数学模型，揭示攻击传播路径与稳定性破坏机制；在方法层面，需要融合信息物理系统安全理论与自适应控制技术，设计具有攻击识别与补偿功能的协同控制策略；在工程层面，需要开发低时延、高可靠的通信机制，平衡控制性能与网络安全需求。相关研究不仅能够完善直流微电网安全控制理论体系，更可为实际工程中网络安全防护方案的制定提供技术支撑，对推动新型电力系统建设具有重要的学术价值与实践意义。

1.2 国内外研究现状

1.2.1 直流微电网安全概述

直流微电网作为未来能源体系的关键构成要素，依托其高效能量转换特性及对分布式可再生能源的良好适配性，在偏远区域供电保障、数据中心能源优化以及军事基地独立供能等场景中展现出显著的应用潜力。然而，其高度依赖电力电子接口与通信网络的特性，使得安全威胁从传统的物理故障向信息物理耦合攻击演变[20-21]。从物理架构分析，直流微电网的脆弱性主要体现在两方面：其一，系统惯性较低，缺乏交流电网的旋转备用容量，当遭遇功率突变或外部扰动时，母线电压的动态稳定性极易被破坏；其二，分布式控制依赖于稀疏通信网络，节点间的信息交互若被攻击者截获或篡改，可能导致全局控制失稳。如上所述，直流微电网在运行、控制与保护方面也面临独特的技术复杂性与缺陷。动态拓扑变化、双向功率流动、标准化缺失等问题，是交直流微电网的共性挑战[22-24]。但相较于交流微电网，直流微电网呈现显著差异化特征：其地理覆盖范围更小、配电线路更短，本质上属于阻性网络，物理惯性极低，在故障或扰动下更易失稳[25-26]。由于不存在无功功率流动，其电压稳定机制与交流系统截然不同——无法通过无功补偿调节电压，这使其电压控制更具挑战性[27]。

在直流微电网技术架构中，以功率变换器为核心的电力电子装置集群已成为实现电能精确调控与灵活分配的关键设备。这类装置不仅作为发电单元与负荷终端的能量接口，更深入地渗透至分布式电源接入、储能系统集成、配电网络重构及智能用电等各个层级，推动直流微电网向全电力电子化网络方向演进[28-30]。这种结构性变革在显著提升系统功率密度、传输效率和可控性的同时，也引发了多维度技术挑战：在装置层面，变换器内部复杂的开关调制特性与非线性控制特性相互耦合；在系统层面，多变换器间呈现多时间尺度动态交互特性，其与直流母线构成的网络化系统存在复杂的非线性耦合效应，导致系统稳定性机理与传统交流电网存在本质差异。更为严峻的是，高比例可再生能源的强随机性出力与多元化负荷的时变特性，迫使系统需要具备毫秒级动态响应能力与多目标协调控制能力[31-32]。这不仅涉及源、网、荷、储变换器的动态响应匹配、能量优化分配策略，还需解决故障工况下的协同保护机制等关键问题，由此衍生的多变量耦合建模、

多时间尺度控制、信息物理系统协同等难题，使得直流微电网的稳定运行与控制复杂度呈指数级增长。

1.2.2 分布式分层控制研究现状

如前所述，微电网既可以与主电网并网运行，也能够在脱离主网的情况下以孤岛模式独立运行。微电网的安全稳定与经济高效运行，依赖于对其实施科学合理的控制策略。微电网控制结构的主要作用是[33-35]：孤岛或并网运行下的电压和频率调节；协调分布式电源并适当分担负荷；调节微网与主网的同步运行；控制微网与主网之间的功率调节。这些需求具有不同的重要性和时间尺度，因此需要一个分层控制结构以在不同的控制层次上处理每个需求。

直流微电网的分层控制系统通常采用三层控制架构，分别为一次控制、二次控制和三次控制[36-38]。其中，一次控制的核心功能在于实现微电网内部的电流分配与电压调节，保障电力供需基本平衡及母线电压稳定；二次控制则起到补偿的作用，主要纠正一次控制可能引起的电压偏差，确保微电网的电压始终维持在合理的范围内；三次控制则主要针对微电网与主网的潮流协调控制，通过智能调度策略实现经济优化运行，优化电网与负荷之间的能量交互，进而提升系统整体运行效率与经济性。

直流微电网控制系统根据实施方式的不同，可分为三大类：分散式、集中式和分布式[39]。分散式控制的特征是 DG 各自控制器间无通信通道，由本地控制器独立操作，各本地控制器通过实时监测直流母线电压信号，实现对变换器的协调控制[40-41]。虽然结构简单，但灵活性和可靠性均较低。而随着微网的发展，其运行状态变得更加复杂，分散控制一般作为底层控制基础，与其他控制模式相配合使用。例如 Eyke Liegmann 等人提出一种基于分散式控制的方法，用于协调分布微电网中多个储能系统[42]。集中式控制是一种基于通讯网络的控制策略，通过一台中心控制器为主控单元，向全部直流电源传送信号。Che Liang 等人以及 Jin Chi 等人均提出过基于中央能源管理器的协调控制系统，增强单元间的数据收集实现调节目标[43-44]。然而，随着 DG 数量增加，当集中控制单元一旦发生故障，可能对整个微网系统造成严重影响甚至导致系统崩溃。上述两种控制策略都存着各自的不足，因此一种融合了集中式与分散式优势的分布式控制策略被提出。该策略

无需设置控制中心，也无需全局信息，通过在相邻 DG 之间建立了通信通道，利用局部信息并和相邻发电机组通信，有效避免单点故障。例如，Fanghong Guo 等人提出一种仅需要直流母线电压反馈的分布式二次控制方法，实现了母线电压调节与功率分配的目标[45]；Xiaokang Liu 等人研究了基于分布式监控的电压调节反馈与电流分配反馈灵活配置，克服了电压与电流调节回路线性组合可能产生的抵消效应[46]；Zhiyi Chen 等人提出基于事件触发的通讯策略，通过减少非必要通信显著节省了通信资源[47]。

1.2.3 FDI 和 DoS 攻击研究现状

为了实现分布式分层控制结构，需要在 DG 之间部署通信网络以实现局部信息交互。然而，通信网络的脆弱性可能对微电网控制系统的安全稳定运行构成严重威胁。恶意攻击者可通过破坏通信链路的完整性与可用性，导致控制指令传输出现延迟、丢包或篡改等异常情况，进而引发微电网系统失稳。其中最具代表性且防范难度较高的两种网络攻击类型分别是 FDI 攻击与 DoS 攻击[48-49]。FDI 攻击的技术特征表现为：攻击者通过非法接入 DG 二次控制传感器的通信通道，篡改实时监测数据，从而破坏控制系统的数据完整性。此类攻击利用二次控制层的数据交互特性，通过伪造或修改关键参数，可能导致微电网出现非预期的潮流分布或电压偏移。DoS 攻击则通过向通信网络注入海量无效数据，造成链路带宽资源耗尽，传输延迟显著增加。其技术实现通常通过分布式网络节点协同发起流量洪泛，使得合法控制指令无法正常传输。这种攻击方式尽管技术门槛相对较低，但可导致微电网控制中心与现场设备间的通信中断，进而使系统无法及时响应运行状态变化，严重时可能引发级联故障[50-51]。

现有研究表明，针对微电网通信系统面临的 FDI 和或 DoS 单一攻击场景，已有大量文献提出了相应的防护方案。针对 FDI 攻击的影响，已有研究提出了多种检测、隔离和缓解的策略。Subham Sahoo 等人与 Shan Zuo 等人的研究工作致力于通过分布式协同机制构建分层防御体系，突破传统单层防护的局限性。他们设计了跨控制层级的动态交互机制，通过增强不同控制层间的信息共享与协同决策能力，显著提升了对攻击行为的可观测性。在此基础上，提出了一种基于一致性算法的电压电流调节方案，该方案通过建立分布式节点间的共识机制，能够

有效识别通信链路中的异常数据特征，从而实现对遭受 FDI 攻击的通信链路的精准检测与隔离[52-53]。Yihao Wan 等人与 Aquib Mustafa 等人在解决微电网通信系统 FDI 攻击问题时，提出了数据驱动的动态检测与自适应防御相结合的技术方案，构建了互补的协同防御体系。研究通过强化学习算法与概率统计模型的有机结合，建立了攻击行为特征数据库，并以此为基础为每个 DG 的邻域节点设定数据可信区间。这种基于数据特征分析的防御机制能够实时监测通信链路中的数据异常，通过动态调整信任边界，实现对遭受 FDI 攻击的异常数据的精准识别与隔离，从而保障微电网控制系统的信息完整性[54-55]。Chao Deng 与 Yun Liu 等人针对微电网分布式控制场景下的 FDI 攻击问题，提出了一种分层分布式弹性控制框架。该框架基于分布式共识协议构建双重防御机制：当攻击强度在预设阈值内时，通过鲁棒控制设计维持系统频率及电压稳定；若攻击超出阈值范围，则启动弹性响应机制，通过实时攻击检测算法定位受攻击节点，并实施节点隔离策略阻断攻击扩散，同时采用优化调度算法保障系统功率的公平分配。这种分阶段防御策略有效融合了鲁棒性与弹性控制理论，在提升系统抗攻击能力的同时，确保了微电网在异常工况下的稳定运行[56-57]。彭华晔等人与 Shankar Abhinav 等人针对 FDI 攻击场景，提出了一种基于链路状态监测的攻击识别方法，并构建了“检测-补偿-隔离”的递进式防御体系。该研究通过实时监测通信链路的异常数据特征，首先实现攻击行为的精准检测；继而采用动态补偿算法对受污染数据进行修正，维持微电网的频率稳定与运行状态鲁棒性；最终通过智能隔离策略切断受攻击链路的影响扩散。这种分阶段防御机制不仅在 FDI 攻击场景下展现出良好的稳定性维持能力，更为通信资源受限场景下的抗 FDI 攻击问题提供了普适性解决方案，为提升微电网信息物理系统的安全韧性提供了新的技术思路[58-59]。另一方面，为了应对 DoS 攻击的影响，Zhijie Lian 等人、Gang Xu 等人与 Junjie Ma 等人提出了一种事件触发机制驱动的二次控制策略。该策略的核心在于构建了动态化的通信激活机制，控制器通过实时监测系统运行状态，仅在满足预设事件触发条件时才向相邻节点发送本地状态信息。这种基于阈值驱动的通信模式能够有效减少冗余数据传输，相较于传统周期性通信方式，可显著降低不必要的通信频次，从而大幅节省网络带宽资源，提升系统整体运行效率。该控制方案通过动态优化数据传输的触发机制，在维持系统控制性能的前提下，实现了网络负载的有

效降低。其独特优势在于能够显著提升通信资源利用效率，适用于需要高效通信管理的分布式控制系统[60-62]。Weitao Yao 等人提出了一种创新性的弹性控制策略，该策略针对多样化的网络干扰场景，设计了具有自适应增益调节能力的弹性控制器，以保障系统在干扰环境下的稳定性。提出了一种新颖的量化指标，用于评估 DoS 攻击对系统的影响程度，并在此基础上结合攻击影响评估结果，开展了系统时域稳定性分析。这种将干扰场景适应性设计、攻击量化评估及时域稳定性验证相结合的技术路线，为提升微电网在复杂网络攻击下的鲁棒性提供了新的解决方案[51]。Songlin Hu 等人与 Chao Deng 等人的研究中，针对直流微电网在 DoS 攻击下面临的通信不确定性问题，研究提出动态时序调整策略以应对非周期性攻击，并构建切换式状态反馈控制算法，确保系统在 DoS 攻击下的稳定性[63-64]。

上述研究主要关注的是单一类型攻击对微电网的影响。然而，实际应用场景中，FDI 攻击和 DoS 攻击往往并存，此类混合攻击造成的影响远比单一 FDI 攻击或 DoS 攻击更严重。更为关键的是，混合攻击的隐蔽性使其检测难度显著增加，导致其被及时发现的概率较低。攻击者常通过同时实施 FDI 攻击与 DoS 攻击的策略，使系统的防御措施面临更大的挑战。为了更准确地描述这一复杂的攻击模式，本文将这种攻击方式统一称为混合攻击。已有部分研究涉及 FDI 和 DoS 攻击并存的场景。Xiaoli Chen 等人的研究中针对存在 FDI 攻击和 DoS 攻击的多区域负载频率控制系统，提出共同估计与弹性补偿控制框架，并首次推导了攻击下输出反馈多系统的指数稳定性判据[65]；Quan Zhou 等人则提出跨层控制策略以增强微电网对混合攻击的弹性，该策略的核心优势在于无需依赖网络攻击的实时检测与隔离机制[66]。然而这些研究未考虑 FDI 攻击的多样性，仅针对有界的 FDI 攻击展开分析。Zihao Cheng 等人与 Md Musabbir Hossain 等人针对微电网通信系统的混合攻击问题，提出动态通信节奏调节策略[67-68]：前者在 DoS 导致的切换残差拓扑中，通过模型相关平均停留时间结合负载频率控制与虚拟惯性控制协同控制抵御 FDI 攻击；后者设计误差驱动的带宽动态分配，借助事件触发机制打破网络攻击的攻击周期性依赖。尽管这些研究提出了应对混合攻击的策略，但仅能减轻 FDI 攻击的影响，无法实现攻击的重建或估计。Xiaokang Liu 等人提出了基于自适应增益的控制方案以应对间歇性 DoS 与脉冲式 FDI 攻击，但其策略在 DoS 攻击发生时强制将控制输入置零，可能影响系统正常运行[69-70]。

综上所述，分布式二次控制在直流微电网的性能调节方面展现出显著优势，但网络安全问题日益突出。攻击者可通过 FDI 与 DoS 破坏系统的功率分配与电压稳定，而现有研究多聚焦单一攻击类型，对 FDI 与 DoS 混合攻击的协同建模与防御机制仍存一些空白，因此，针对混合网络攻击下直流微电网的分布式二次控制的研究，对于提升系统的安全韧性与稳定运行能力具有重要的理论意义与实际应用价值。

1.3 主要研究内容

本文围绕孤岛直流微电网在 FDI 和 DoS 混合网络攻击下的分布式二次控制问题展开研究，针对传统下垂控制引发的电压偏差、均流误差以及通信网络存在恶意攻击等挑战，研究了一种分阶段递进的解决方案。研究内容主要包括以下三部分内容：

(1)基于母线电压和支路电流反馈的分布式二次控制器设计。直流微电网的孤岛运行依赖于下垂控制实现功率分配，但其固有的电压-电流下垂特性会导致母线电压偏差和分布式电源输出电流比例失衡。为此，本部分设计了一种基于局部通信的分布式二次控制策略，旨在同时实现电压恢复与比例均流目标。首先对直流微电网系统及分层控制结构进行建模，构建包含一次下垂控制层、分布式二次控制层和通信系统的模型，利用图论描述 DG 间的通信拓扑，并推导微电网的潮流动态方程。结合母线电压误差反馈与支路电流误差反馈，设计分布式二次控制器。在该控制器的作用下，直流微电网能够解决一次下垂控制所导致的电压偏差问题，将电压调节至目标值。与此同时，各个 DG 的输出电流能够按照所需比例进行输出。基于 Matlab/Simulink 平台构建包含 4 个 DG 单元的直流微电网仿真模型，对所提控制器的性能进行验证。仿真结果显示，该控制器在负载阶跃变化、电流分配比例突变等复杂工况下，均能有效实现电压调节与电流分配。

(2)FDI 和 DoS 混合网络攻击下的弹性事件触发分布式二次控制器设计。在开放通信环境下，直流微电网的分布式二次控制器易受 FDI 攻击和 DoS 攻击的协同干扰。现有研究多针对单一攻击类型，缺乏对混合攻击的适应性。为此，本部分提出一种分层弹性事件触发控制架构以抵御混合网络攻击。该控制器采用了独特的架构设计，主要由两个子控制器以及一个基于事件触发机制的管理器共同

构成。其中，第一个子控制器是基于母线电压误差反馈，通过实时监测母线电压的实际值与设定的目标值之间的误差，进行精确计算和调整，从而实现对母线电压的有效控制。第二个子控制器则是基于支路电流误差反馈，能够实时监测本单元支路电流与相邻单元支路电流之间的误差，进而对支路的电流进行精准调节。基于事件触发的管理器则根据系统当前的运行状况、母线电压误差、支路电流误差等多种关键因素，动态地选择合适的子控制器投入工作。并通过Matlab/Simulink 平台搭建包含 4 个 DG 单元的直流微电网仿真模型，对所提控制器的性能进行验证。仿真结果表明，该控制器在多种运行工况下均能有效实现电压调节与电流分配。

(3)FDI 和 DoS 混合网络攻击下的弹性周期采样与 FDI 攻击缓解的协同优化分布式二次控制器设计。尽管第二部分方案能够抵御混合攻击，但仍存在两点局限：一是依赖连续事件触发机制，在 DoS 攻击密集期可能失效；二是不能对 FDI 攻击信号进行重构。为此，本部分提出一种融合弹性周期采样与攻击重构的控制策略。该分布式分层弹性控制方案在二次控制层引入了弹性周期采样技术，根据系统实时状态和攻击情况，动态调整通信间隔，在保证系统性能的同时减少 DoS 攻击导致的数据丢失，降低通信资源消耗。为了进一步应对 FDI 攻击，该方案设置了基于神经网络的 FDI 攻击缓解层。当采样数据经过这一层时，会通过深度分析和甄别对数据进行优化处理，从而过滤虚假数据，有效减轻甚至消除 FDI 攻击对系统的影响。本章方案通过 FDI 攻击缓解层的设计，解决了上一章中无法对 FDI 攻击进行重建或估计的局限性，能够深入分析 FDI 攻击的特征和影响，为后续的防御和恢复工作提供有力支持。并通过 Matlab/Simulink 搭建含 4 个 DG 单元的直流微电网模型对该控制器进行验证，仿真结果表明其在多种场景下都能实现调压和均流。

1.4 论文组织结构

本文围绕直流微电网在混合网络攻击下的分布式二次控制问题，从基础控制框架构建、混合攻击防御到通信与攻击缓解协同优化展开递进式研究，全文共分为五章，各章节内容安排如下：

第 1 章为绪论。首先阐述直流微电网的研究背景与意义，分析传统下垂控制

导致的电压偏差问题，以及分布式控制面临的网络攻击威胁。随后从直流微电网安全概述、分布式分层控制技术、网络攻击防御技术等方面综述国内外研究进展，指出现有工作在混合攻击适应性、通信效率优化及攻击重构方面的不足。最后明确本文的研究目标与创新点，并概述全文结构框架，为后续章节提供逻辑引导。

第 2 章聚焦于孤岛直流微电网的基础建模与分布式二次控制器设计。从系统建模出发，构建包含分布式电源、直流母线和电力电子变换器的电气拓扑模型，分析一次下垂控制的电压-电流耦合特性及其固有缺陷。在此基础上，研究分层控制架构，结合网络图论原理设计通信拓扑，融合母线电压误差反馈与支路电流误差反馈机制，设计一种分布式二次控制策略。该策略通过动态一致性协议实现电压恢复与比例均流的双重目标，同时在仿真环境中验证控制器的有效性，为后续研究奠定基础。

第 3 章针对通信网络面临的 FDI 和 DoS 混合攻击问题，在第二章的控制框架上进一步优化。首先建立 FDI 攻击的信息篡改模型与 DoS 攻击的脉冲阻塞模型，揭示混合攻击对分布式控制的协同破坏机理。基于此，设计一种分层弹性事件触发控制器，通过解耦的设计调压子控制器与均流子控制器，并引入自适应的事件触发管理器动态切换控制模式。同时在仿真环境中验证控制器的有效性，为复杂攻击场景提供了可行的解决方案。

第 4 章针对第三章方案在通信连续性与攻击重构能力上的不足，提出弹性周期采样与攻击缓解协同优化策略。通过设计弹性周期通信机制，动态调整采样间隔以平衡通信效率与抗 DoS 攻击能力。进一步构建 FDI 攻击缓解层，针对每个单元设计局部估计器，助神经网络估计变换器的输出电流及母线电压。将神经网络的输出作为控制器的参考值，以去除其中的虚假信息，用处理后的无虚假信息的数值来替换原始采样信息，作为传输至相邻单元的信息。该方案在提升通信资源利用率的同时，解决了攻击重构难题。仿真结果表明，在高强度混合攻击下，系统仍能保持高精度调压与均流性能，且通信带宽需求显著降低。

第 5 章总结全文研究成果并展望未来方向。系统梳理了从基础控制设计到混合攻击防御、再到协同优化的递进式研究框架，归纳了双反馈控制架构、弹性事件触发机制及攻击缓解层等核心创新点。

第 2 章 直流微电网分布式二次控制策略

2.1 引言

与交流微电网相比，直流微电网具有效率高以及变流器控制简单的优点，同时，直流无需同步，消除了无功和谐波问题，这些优势使得直流微电网的研究受到广泛关注。分层控制作为一种高效的控制方法，已成为直流微网的优选控制策略。分层控制结构由一次二次和三次控制层组成。一次控制主要是基于下垂控制，作用是实现微电网的均流和调压目标；二次控制的作用是补偿由一次控制引起的电压偏差，分布式二次控制融合了集中式与分散式于控制的优势，无需设置控制中心，也无需全局信息，因而被广泛采用；三次控制则针对微网与主网之间的潮流进行管理，实现经济最优运行。

本章主要介绍直流微电网的系统建模、分层控制结构建模，简述了网络图论基本原理及控制系统的通信机制，介绍了一种基于母线电压误差反馈和支路电流误差反馈的分布式二次控制策略。该控制器能够解决一次下垂控制导致的电压偏差，将母线电压调节到目标值，同时确保各个 DG 输出电流按比例分配，从而实现调压与均流的双重目标。基于 Matlab/Simulink 建立仿真模型，验证了该控制器的有效性。

2.2 系统模型与问题描述

与传统大电网相比，直流微电网中广泛采用了电力电子变换装置。这些设备在 DG 与直流母线的接口设计、直流母线与负载的连接，以及微电网母线与主电网的交互中发挥着关键作用。本章将以连接 DG 与直流母线的双向 DC-DC 换流器为例，对微电网系统的建模及控制方式进行阐述。

直流微电网由多个分布式电源、负荷以及 DC-DC 变换器组成。文中考虑一个单母线微电网模型，其中包含 N 个分布式电源其集合为 $v=\{1,2,...N\}$ 和 M 个负荷其集合为 $C_L=\{1,2,...M\}$，如图 2.1[71]所示。在该模型中，分布式电源和线性负荷并联在公共母线上，变换器工作在电压模式下。系统中通过通信网络实现分布

式控制器之间的信息交互。

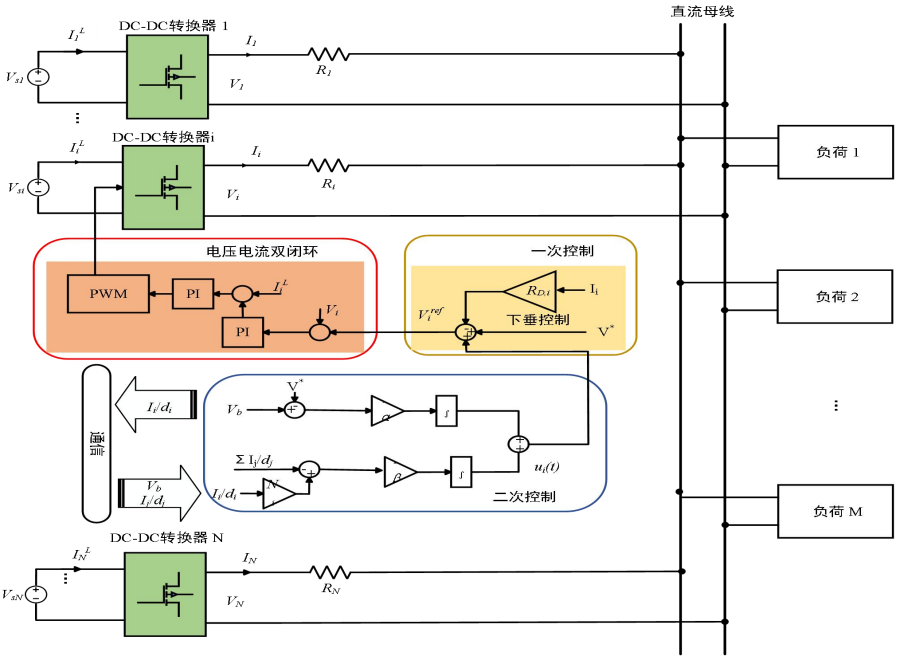


图 2.1 分布式二次控制下的直流微电网

2.2.1 直流微电网模型

在该模型中，微电网的变量定义如下：V_i为第 i 个变换器的输出电压，I_i为第 i 个变换器的输出电流，R_i为对应的线路阻抗，$R_{L.i}$为第 i 个负载的阻抗，V_b为母线的电压。基于上述变量定义，微电网的潮流方程可表示为：

$$\begin{cases} R_i I_i = V_i - V_b \\ \sum_{i \in v} I_i = V_b \sum_{i \in C_L} 1/R_{L.i} \end{cases} \tag{2-1}$$

当信息通信网络系统融入直流微电网后，直流微电网可被视作多节点协同通信的信息物理体系。在这一体系内，与 DC-DC 变换器关联的分布式控制器可视为通信系统中的节点单元。因此，借助代数图论的相关原理，能够以矩阵形式展现联合分布式控制器的网络通信架构，而针对其系统特征，可采用矩阵理论开展分析。

假设通信网络是无向图，通常采用通信图 $G=\{v,E\}$进行建模。其中v表示直流微电网中的分布式电源节点，$E \subseteq v*v$ 为连接这些节点的边。另外，$N_i = \{j \in v \mid v_i v_j \in E\}\}$表示第 i 个节点的所有邻居节点的集合，$A=[a_{ij}]_{N\times N}$为邻接

矩阵，$D_d=[d_{ij}]_{N\times N}$ 为度矩阵，$L=[l_{ij}]_{N\times N}$ 为图 G 的拉普拉斯矩阵。其中，如果 $v_i v_j \in E$，$a_{ij}=0$，否则 $a_{ij}=0$，且如果 $i=j$，$a_{ij}=0$。D_d 为对角矩阵，如果 $i=j$，$d_{ij}=\sum_{j=1}^{N} a_{ij}$，否则 $d_{ij}=0$，$L=D_d-A$。对无向网络拓扑，其拉普拉斯矩阵具有对称性，如果图 G 中任意两个节点之间存在一条路径，则称 G 为连通图。

2.2.2 直流微电网控制目标

直流微电网具有两大控制目标，分别是电压调节和电流比例分配，即调压和均流。其要求将母线电压维持在额定值的水平，并使输出电流达到预期的比例分配状态。从数学建模角度出发，设计相应的控制器，以实现对每个变换器的输出电压以及输出电流比例进行调节，并通过潮流公式(2-1)的解来对以下两个问题予以验证：

$$V_b = V^* \tag{2-2}$$

$$I_i(t)/d_i = I_j(t)/d_j \tag{2-3}$$

式中，d_i 是期望的比例参数，表示电力系统在考虑经济特性的情况下计算得出的最优分配比例。

2.3 微电网分布式分层控制策略

微电网的分层控制体系一般包含三个调控层级：一次控制层、二次控制层和三次能量优化层，分别在不同时间尺度上发挥作用。其中一次控制层作为分布式电源的初级控制单元，主要由本地电源控制器和负荷管理模块构成。该层级通过采集本地电压、电流等实时状态数据，采用下垂控制算法维持微电网的电压稳定，并实现电流的比例分配。在并网运行时，系统参考值由配电网络提供；切换至孤岛模式后，则由 DG 单元自主维持本地电能质量指标。但是，基于下垂特性的有差控制会导致系统电压存在稳态偏差。二次控制层作为二级调控机制，能够有效补偿一次控制产生的静态误差，提升系统的收敛性能。该层级通过引入额外的补偿信号，在保证电流精确分配的同时改善电能质量。能量优化层作为最高层级，主要负责根据市场需求和调度指令优化微电网的功率输出。在满足基本控制目标

的基础上，该层级通过动态调整能量流动路径，实现微电网运行的经济性最大化。本文主要考虑微电网在孤岛运行模式下的电压稳定及电流分配问题，即主要研究一次控制和二次控制策略。

传统的分布式分层控制框架如图 2.1 所示，该框架由一个内部双环 PI 控制器、一个一次控制器以及一个二次控制器组成。其中，双环 PI 控制用于产生 PWM 控制信号，并保证输出电压 V_i 能够在快速时间尺度上紧紧跟随参考电压 V_i^{ref}。此外，将分布式发电机组建模为电压控制源后，可推导出如下公式：

$$V_i(t) = V_i^{ref}(t) \tag{2-4}$$

电压V_i^{ref}为直流微电网潮流调节参考电压，由一次控制和二次控制产生，则：

$$V_i^{ref}(t) = V^* - R_{D,i} I_i(t) + u_i(t) \tag{2-5}$$

式中，V^*为直流母线的额定电压，$R_{D,i}$为下垂系数，$u_i(t)$为二次控制信号。如果(2-2)和(2-3)成立，则直流微电网实现了调压和均流。

2.3.1 一次控制

在微电网孤岛运行场景中，需根据负载变化实时调节各 DG 的输出电流分配即有功功率分配。作为分层控制体系的核心组成部分，一次控制通过维持母线电压稳定，实现各 DG 单元的电流协调分配。微电网的一次控制层级多采用下垂控制技术，该技术属于典型的无通信分散控制方式。该策略通过自调节机制，在系统发生波动时无需依赖 DG 间的信息交互，即可快速实现调节目标的实时匹配。

直流微电网中第 i 个 DG 一次控制的下垂方程可表示为:

$$V_i^{ref}(t) = V^* - R_{D,i} I_i(t) \tag{2-6}$$

由式(2-4)结合潮流方程(2-1)和式(2-6)可得：

$$V_b(t) = V^* - (R_i + R_{D,i}) I_i(t) \tag{2-7}$$

由(2-7)可知，电流分配比与线路电阻 R_i 与下垂增益系数 $R_{D,i}$ 之和成反比，即:

$$\frac{I_i(t)}{I_j(t)} = \frac{R_j + R_{D,j}}{R_i + R_{D,i}},\ i, j = 1, 2, ..., N \tag{2-8}$$

当选取的下垂系数 $R_{D,i}$ 远大于传输线电阻 R_i 时，即 $R_{D,i} \gg R_i$，则电流分配精度仅与下垂系数有关，即：

$$\frac{I_i(t)}{I_j(t)} = \frac{R_j + R_{D,j}}{R_i + R_{D,i}} \approx \frac{R_{D,j}}{R_{D,i}},\ i, j = 1, 2, ..., N \tag{2-9}$$

由式(2-9)可得，增大下垂系数 $R_{D,i}$，可提升电流分配精度。然而由式(2-7)可知，该系数增大会导致母线电压偏离标称值的程度更加显著。因此，在传统的下垂控制中需要合理选取 $R_{D,i}$，在保证电流分配精度的同时，尽量降低电压偏差。

2.3.2 二次控制

通过上述对基于下垂控制的一次控制的分析可知，经一次控制调节的微电网系统电压无法达到参考值，这表明一次控制属于有差调节。为了进一步解决母线电压偏差的问题，在初级控制的基础上引入了二次控制。

分布式二次控制不需要全局信息，只需要直流母线电压和各支路电流的测量和反馈，从而使设计的控制器更易于实施且运行可靠，有效避免单点故障的发生。因此，采用分布式二次控制器能够补偿电压降，同时保证电流输出按比例分配。

将母线电压误差 $e_V(t)$ 定义为：

$$e_V(t) = V_b(t) - V^* \tag{2-10}$$

DGi 的控制器的电流误差 $e_{I,i}(t)$ 定义为：

$$e_{I,i}(t) = \frac{1}{d_i} \sum_{j \in N_i} (I_i(t)/d_i - I_j(t)/d_j) \tag{2-11}$$

基于直流微电网的两个调节目标和上述两个误差，分布式二次控制器形式如下[45]：

$$\begin{cases} u_i(t) = \delta_i(t) \\ \dot{\delta}_i(t) = -\alpha e_V(t) - \beta e_{I,i}(t) \end{cases} \tag{2-12}$$

式中，δ_i 表示控制器的内部状态；正参数α和β分别为电压和电流的增益。

由式(2-10)(2-11)(2-12)可知，为实现调压和均流，分布式控制器需要测量母线电压，也需要通讯网络来交换各个分布式控制器的输出电流信息。

2.4 闭环系统与稳定性分析

定义 $I=\mathrm{col}[I_1,...,I_N]$，$V=\mathrm{col}[V_1,...,V_N]$，$e_I=\mathrm{col}[e_{I,1},...,e_{I,N}]$，$\delta=\mathrm{col}[\delta_1,...,\delta_N]$，$K=\mathrm{diag}[k_1,...,k_N]$，$D=\mathrm{diag}[d_1,...,d_N]$，由潮流方程(2-1)以及(2-6)(2-7)可得对 I_i 求导为：

$$\dot{I}_i=\frac{1}{R_i+R_{D,i}}(\dot{\delta}_i-\dot{V}_b)=k_i(\dot{\delta}_i-\dot{V}_b) \tag{2-13}$$

式中，$k_i=\dfrac{1}{R_i+R_{D,i}}$。

由潮流方程(2-1)以及(2-13)可得 V_b 的导数为：

$$\dot{V}_b=\frac{\sum_{i\in v}k_i\dot{\delta}_i}{\sum_{i\in v}k_i+\sum_{i\in C_L}\dfrac{1}{R_{L,i}}}=\frac{1}{\eta}\sum_{i\in v}k_i\dot{\delta}_i \tag{2-14}$$

式中，$\eta=\sum_{i\in v}k_i+\sum_{i\in C_L}\dfrac{1}{R_{L,i}}$。

将(2-14)带入(2-13)可得：

$$\dot{I}_i=k_i(\dot{\delta}_i-\frac{1}{\eta}\sum_{i\in v}k_i\dot{\delta}_i) \tag{2-15}$$

向量形式为 $\dot{I}=K(I_N-\dfrac{1}{\eta}1_N1_N^TK)\dot{\delta}$，$1_N$ 为所有元素都为 1 的列向量，则有

$$\dot{e}_V=\dot{V}_b=\frac{1}{\eta}1_N1_N^TK\dot{\delta} \tag{2-16}$$

$$\dot{e}_I=D^{-1}LD^{-1}\dot{I}=D^{-1}LD^{-1}K(I_N-\frac{1}{\eta}1_N1_N^TK)\dot{\delta}=D^{-1}LD^{-1}K\Gamma\dot{\delta} \tag{2-17}$$

式中，L 为通信网络的拉普拉斯矩阵，$\Gamma=I_N-\dfrac{1}{\eta}1_N1_N^TK$。

定义组合误差为：

$$\varphi_i=\alpha e_V(t)+\beta e_{I,i}(t) \tag{2-18}$$

令 $\varphi(t)=\mathrm{col}(\varphi_1(t),...,\varphi_N(t))$ 对(2-18)求导则有

$$\dot{\varphi}(t)=\alpha\dot{e}_V(t)+\beta\dot{e}_I(t)=(\alpha\frac{1}{\eta}1_N1_N^TK+\beta D^{-1}LD^{-1}K\Gamma)\dot{\delta}=\Phi\dot{\delta} \tag{2-19}$$

式中，Φ 为闭环系统动态矩阵，$\Phi=\alpha\frac{1}{\eta}1_N1_N^TK+\beta D^{-1}LD^{-1}K\Gamma$。

由特征向量分析可知 $K\Gamma$ 是一个正定矩阵，若α>0 且β> 0，则 Φ 的特征值都是正的。那么，存在一个唯一的正定矩阵 P，使得下面的李雅普诺夫方程成立

$$P\Phi+\Phi^TP=1_{N\times N} \tag{2-20}$$

$1_{N\times N}$是一个 N 维矩阵。

令 Lyapunov 函数为：

$$W(t)=\varphi(t)^TP\varphi(t) \tag{2-21}$$

对(2-21)求导，由(2-18)-(2-20)可得

$$\begin{aligned}\dot{W}(t)&=\varphi(t)^T(P\Phi+\Phi^TP)\dot{\delta}(t)\\&=\varphi(t)^T\dot{\delta}(t)\end{aligned} \tag{2-22}$$

则有：

$$\begin{aligned}\dot{W}(t)&=\sum_{i\in v}(\alpha e_V(t)+\beta e_{I,i}(t))(-\alpha e_V(t)-\beta e_{I,i}(t))\\&=-\sum_{i\in v}((\alpha e_V(t)+\beta e_{I,i}(t))^2\le 0\end{aligned} \tag{2-23}$$

综上可知当控制增益参数满足α>0 且β>0 时，闭环系统动态矩阵的特征值均具有正实部，从而保证了系统的全局渐近稳定性。这一理论结果验证了分布式二次控制器在动态调节过程中能够有效抑制母线电压偏差，同时确保电流分配的精确性。

2.5 算例及仿真结果分析

为了验证上述分布式控制方案的有效性，本节基于 Matlab/Simulink 建立模型，对所设计的控制器性能进行验证。仿真中使用的直流微电网模型如图 2.2 所示，该模型包含 4 个 DG 及其对应的控制器。详细参数见表 2.1，母线参考电压

设定为 100V。

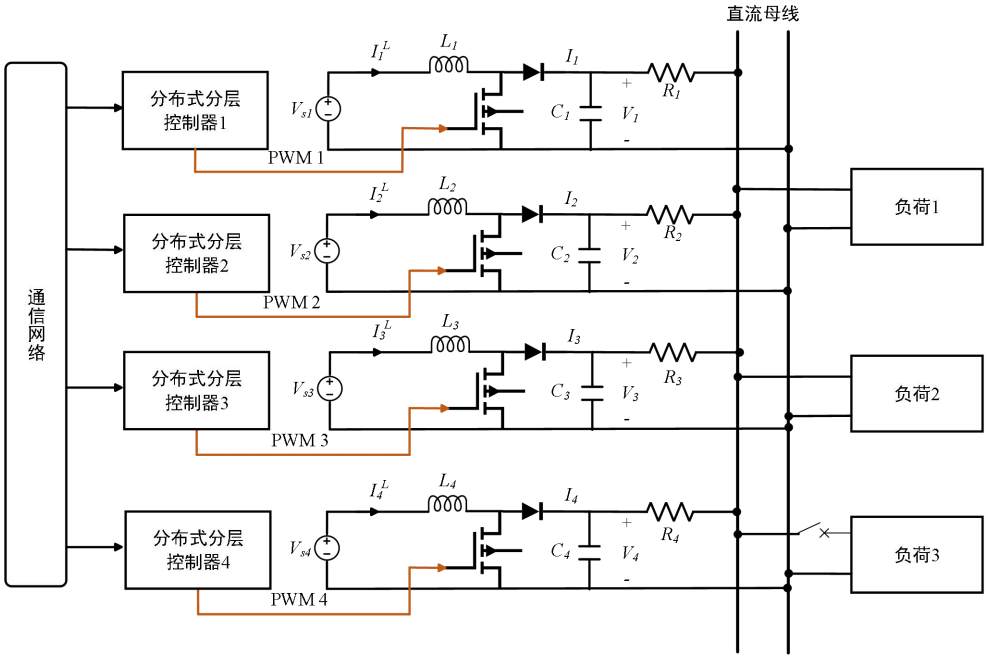


图 2.2 直流微电网 simulink 仿真模型

表 2.1 直流微电网系统参数

直流微电网参数	
DC 电源	V_{si}=50V，i=1，2，3，4
LC 滤波	L_i=2mH，C_i=470μF，i=1，2，3，4
线路电阻	R_1=0.2Ω，R_2=0.4Ω，R_3=0.5Ω，R_4=0.3Ω
负荷	$R_{L,1}$=50Ω，$R_{L,2}$=100Ω，$R_{L,3}$=100Ω
一次控制参数	
电压环	K_{VPi}=0.2，K_{VIi}=16，i=1，2，3，4
电流环	K_{IPi}=1.5，K_{IIi}=0.1，i=1，2，3，4
下垂增益	$R_{D,1}$=1.8，$R_{D,2}$=1.6，$R_{D,3}$=1.5，$R_{D,4}$=1.7
二次控制参数	
增益参数	α=10，β=10

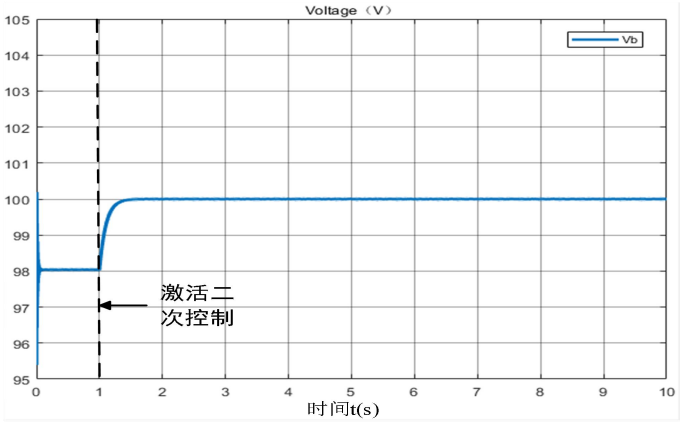
2.5.1 调压和均流测试

首先验证所设计的控制器是否能实现调压和均流的目标。DG 的变换器输出电流的期望比例参数是电力系统在考虑经济特性的情况下计算得出的最优分配

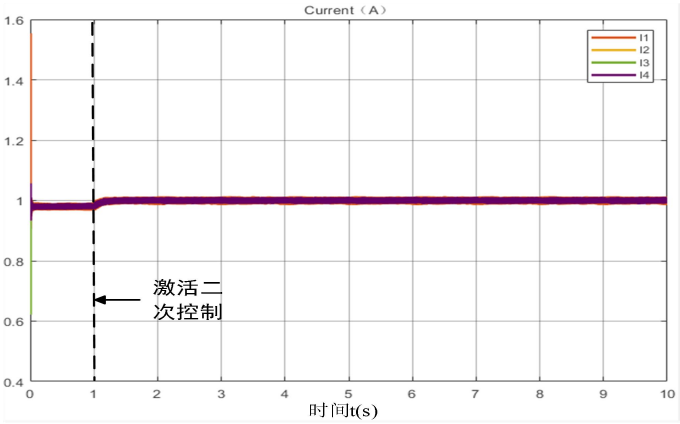
比例。在本案例中测试所设计的控制器是否能实现按设定目标值调节电压并按任意所需比例输出电流。

(1)仿真时间设置为 10s，在 t∈[0,2)s 时，二次控制器未投入工作，仅一次控制器工作；在 t=2s 时，激活二次控制器。设置电流分配比例参数设置为 d_1：d_2：d_3：d_4=1：1：1：1，即输出电流为 I_1：I_2：I_3：I_4=1：1：1：1。

如图 2.3 所示，当二次控制器未激活，仅一次控制器工作时，系统完全依赖下垂控制策略维持运行，由于其固有的电压调节特性，导致母线电压调节存在误差。



(a)调压



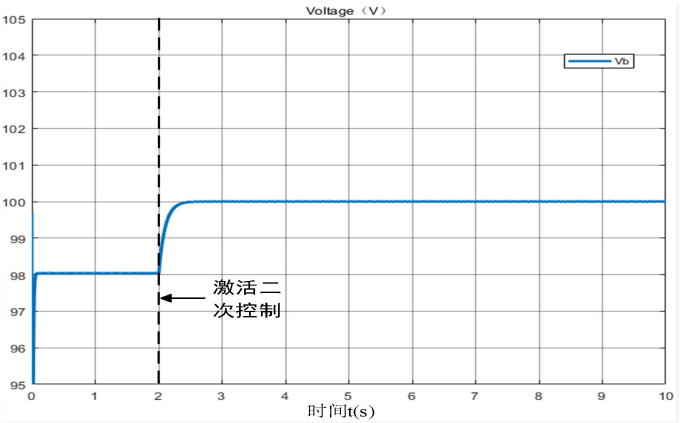
(b)均流

图 2.3 分布式控制器性能测试(d_1：d_2：d_3：d_4：=1：1：1：1)

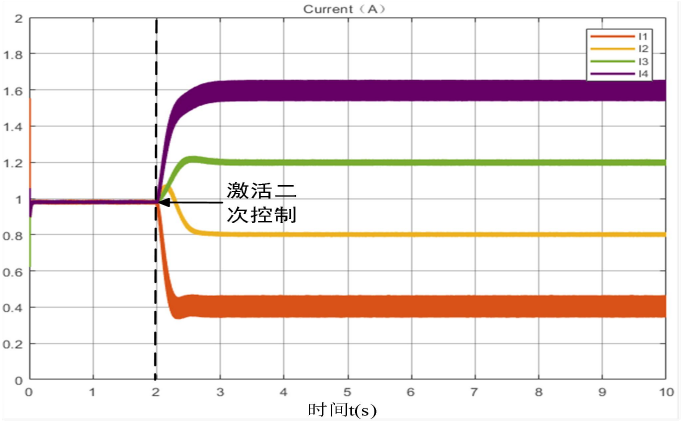
受下垂控制影响，母线电压出现明显下降，实测值降至 98V，与设定的 100V 参考值存在 2V 的偏差，这一结果显示了单纯依靠一次控制器与下垂控制在电压调节方面的局限性。当 t=2s 时，二次控制器被激活，母线电压迅速恢复到参考值 100V，并且输出电流按照设定比例分配。

(2)仿真时间设置为 10s，在 t∈[0,2)s 时，二次控制器未激活，仅一次控制器工作，在 t=2s 时，激活二次控制器。设置电流分配比例参数设置为 d_1：d_2：d_3：d_4=1：2：3：4，即输出电流为 I_1：I_2：I_3：I_4=1：2：3：4。

如图 2.4 所示，当二次控制器未激活，只有一次控制器工作时，受下垂控制影响，母线电压下降到 98V，未达到设定的 100V。当 t=2s 时，二次控制器被激活，母线电压迅速恢复到参考值 100V，并且输出电流按照设定比例分配。



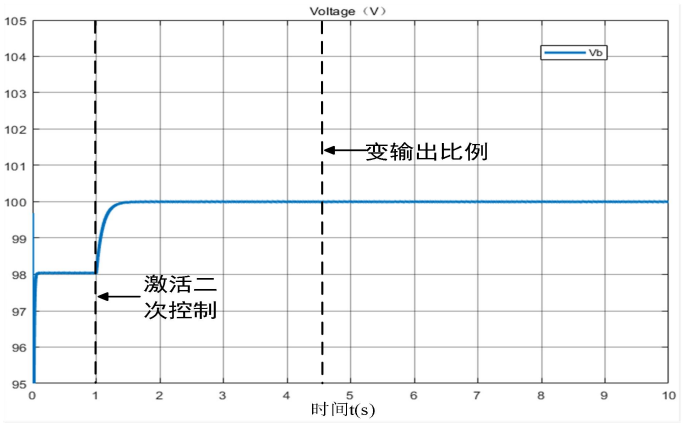
(a)调压



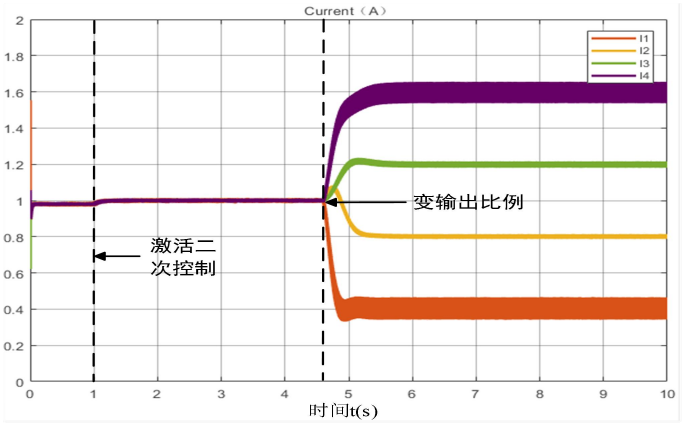
(b)均流

图 2.4 分布式控制器性能测试(d_1：d_2：d_3：d_4：=1：2：3：4)

(3)仿真时间设置为 10s，在 t=1s 时，激活二次控制器。t∈[1,4.6)s 时，电流分配比例参数设置为 d_i=1，i=1，2，3，4；t∈[4.6,10)s 时，电流分配比例参数设置为 d_1：d_2：d_3：d_4=1：2：3：4。如图 2.5 所示，在二次控制器激活后，电压能维持在目标值 100V，输出电流按照预定的比例分配。



(a)调压



(b)均流

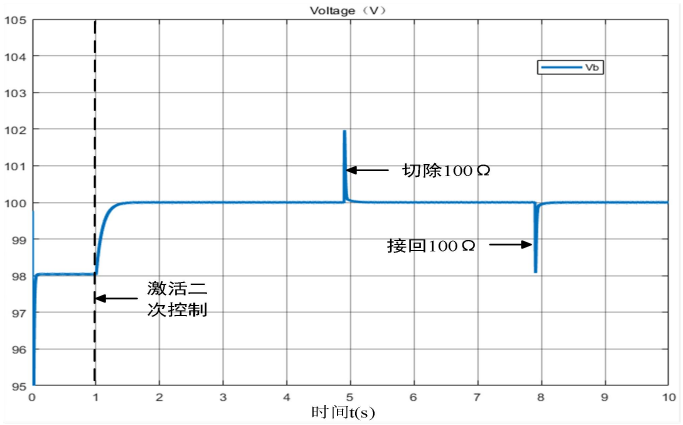
图 2.5 分布式控制器的变输出比例测试

2.5.1 负荷突变测试

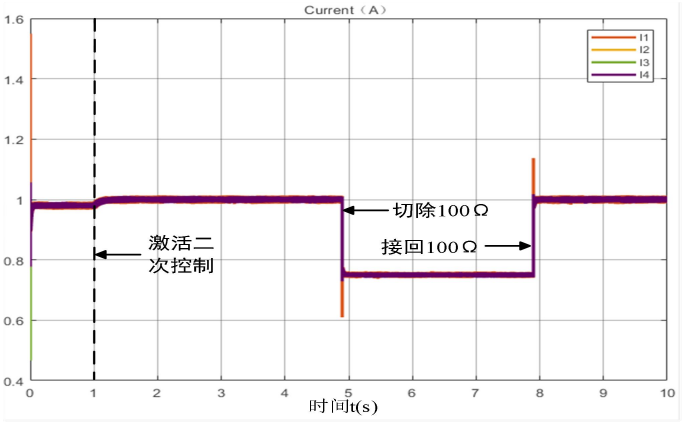
本例中，仍将仿真时间设置为 10s，电流比例参数设置为 d_i=1，i=1，2，3，4。测试所设计的控制器的负荷阶跃性能。在 t=1s 时，激活二次控制器。当仿真进行到 t=4.9s 时，切除 100Ω的负荷。这一负荷切除瞬间，系统功率平衡被打破，母线电压与各变流器输出电流随即产生剧烈波动。在 t=7.9s 时，重新将 100Ω负荷连接入回路，再次引发系统负荷的阶跃变化。这两次负荷的动态调整，模拟了实际电力系统中常见的负荷投切场景，为检验控制器性能提供了极具挑战性的测试条件。

如图 2.6 所示的实验结果曲线来看，在整个负荷阶跃过程中，尽管负荷的突变不可避免地引发了显著的瞬态偏差，但凭借分布式二次控制器中先进的控制算

法与快速响应机制，稳态母线电压都能在短时间内恢复到 100V。这一结果充分彰显了二次控制器在抑制电压波动、加速系统稳态恢复方面的卓越效能。



(a)调压



(b)均流

图 2.6 分布式控制器的负载阶跃性能仿真结果

上述测试结果表明，该分布式二次控制器能够有效补偿由下垂控制引起的母线电压偏差，并且能够使各个变流器输出电流按照设定比例分配。

2.6 本章小结

本章围绕直流微电网及分布式二次控制展开研究。首先，建立了直流微电网的电气拓扑模型，接着分析了微电网分层控制结构的基本原理。其次，在此基础上阐述了一次控制层基于下垂控制的运行特性，并重点构建了分布式二次控制架构，研究了一种能够实现微电网电压调节和电流比例分配的分布式二次控制策略。最后，在 Matlab/Simulink 中建立模型，对分布式控制器的调压和均流性能进行

了测试，同时测试了其在负荷突变场景下的动态响应能力。仿真结果表明，所提出的分布式策略不仅满足电压调节与电流分配的控制目标，还能有效保障微电网系统的稳定运行。

第 3 章 混合网络攻击下基于事件触发的微电网分布式二次控制策略

3.1 引言

在第 2 章中介绍了直流微电网的模型和分层控制结构，并设计了一种融合集中式和分散式控制优点的分布式控制策略，以解决下垂控制带来的电压偏差，同时实现电流比例分配，保障微电网系统的稳定运行。为了实现分布式分层控制策略，需要在 DG 之间部署通信网络，以实现局部信息交互。然而，通信网络极易受到网络攻击，破坏控制器的正常工作，进而造成微电网系统失稳。最典型也最具挑战性的两种网络攻击：FDI 和 DoS 攻击。FDI 攻击的主要目标是通过访问 DG 二次控制传感器之间的交互信息，篡改数据，破坏微电网控制系统中数据的真实性。DoS 攻击是通过发送大量无效信息来阻断正常信息的通信。

攻击者经常同时使用 FDI 攻击和 DoS 攻击以破坏微电网的稳定运行，文中将这种攻击方式称为混合攻击。本章针对分布式二次控制的通信系统存在混合攻击的情况展开研究。为了保证直流微电网系统在混合攻击下仍能保持安全稳定运行，设计了一种分布式分层弹性事件触发控制器。该控制器由两个子控制器和一个基于事件触发的管理器组成。两个子控制器分别是基于母线电压误差反馈和支路电流误差反馈，由管理器根据系统状态选择控制器。并在二次控制器中设计一个补偿机制，以抵消存在 DoS 攻击下连续时间 FDI 攻击的影响。在 Matlab/Simulink 环境搭建直流微电网测试系统，验证了设计的控制器的有效性。

3.2 微电网及控制系统模型

3.2.1 微电网系统

以典型的基于直流变换器的微电网为研究对象，考虑有 N 个 DC 电源其集合为 $C_v=\{1,2,...N\}$ 和 M 个负荷其集合为 $C_L=\{1,2,...M\}$ 的 DCMG 模型。在该模型中，分布式发电机组和负荷并联在公共母线上，如图 3.1[71]所示。

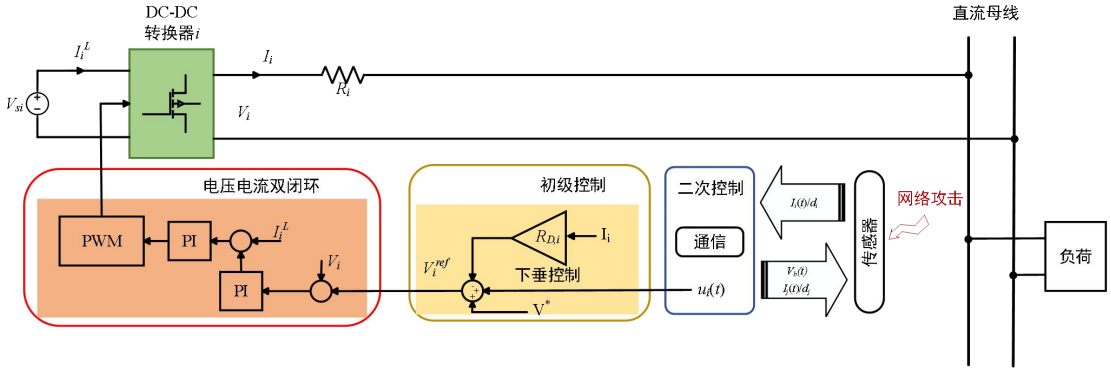


图 3.1 分布式二次控制下的直流微电网

在该模型中，微电网的变量定义如下：V_i 为第 i 个变换器的输出电压，I_i、R_i 分别为对应的输出电流和线路阻抗，$R_{L.i}$ 为第 i 个负载的阻抗，V_b 为母线的电压。其潮流方程为：

$$\begin{cases} R_i I_i = V_i - V_b \\ \sum_{i \in v} I_i = V_b \sum_{i \in C_L} 1/R_{L,i} \end{cases} \tag{3-1}$$

假设通信网络是无向图，其可以用通信图 $G=\{v,E\}$ 表示。其中 v 表示直流微电网中的分布式节点，$E \subseteq v \times v$ 为连接这些节点的边。另外，$N_i=\{j \in v \mid (v_i v_j \in E)\}$ 表示第 i 个节点的所有邻居节点的集合，$A=[a_{ij}]_{N\times N}$ 为邻接矩阵，$D_d=[d_{ij}]_{N\times N}$ 为度矩阵，$L=[l_{ij}]_{N\times N}$ 为图 G 的拉普拉斯矩阵。其中，如果 $v_i v_j \in E$，$a_{ij}=0$，否则 $a_{ij}=0$，且如果 $i=j$，$a_{ij}=0$。D_d 为对角矩阵，如果 $i=j$，$d_{ij}=\sum_{j=1}^{N} a_{ij}$，否则 $d_{ij}=0$，$L=D_d-A$，如果图 G 中任意两个节点之间存在一条路径，则称 G 为连通图。

均流和调压是直流微电网的两大控制目标。这两大目标要求将母线电压维持在额定值水平，并使输出电流实现预期的比例分配。从数学建模的角度出发，需设计控制器以调节每个变换器的输出电压，并通过潮流方程(3-1)的解对以下两个问题进行验证。

$$\frac{I_i(t)}{d_i} = \frac{I_j(t)}{d_j} \tag{3-2}$$

$$V_b = V^* \tag{3-3}$$

式中，d_i 是期望的比例参数。

第 i 个控制器的电压和电流误差分别定义为以下形式。

$$e_V(t) = V_b(t) - V^* \tag{3-4}$$

$$e_{I,i} = \frac{1}{d_i}\sum_{j\in N_i}\left(\frac{I_i(t)}{d_i} - \frac{I_j(t)}{d_j}\right) \tag{3-5}$$

3.2.2 分层控制系统

图 3.1 展示了传统的分布式分层控制框架，该框架由一个内部双环 PI 控制器、一个一次控制器和一个二次控制器组成，一次控制器采用下垂控制技术。双环 PI 控制负责产生 PWM 控制信号，并确保输出电压 V_i 在快速时间尺度上紧跟参考电压 V_i^{ref}。将分布式发电机组建模为电压控制源，可推导出如下公式：

$$V_i(t) = V_i^{ref}(t) \tag{3-6}$$

参考电压 V_i^{ref} 的形式为：

$$V_i^{ref}(t) = V^* - R_{D,i}I_i(t) + u_i(t) \tag{3-7}$$

式中，V^* 为直流母线的额定电压，$R_{D,i}$ 为下垂系数，$u_i(t)$ 为二次控制信号。

3.3 以二次控制器为目标的混合网络攻击模型

二次控制作为直流微电网的核心调控环节，主要实现电流精确分配、母线电压恢复及系统稳定性调节等关键功能。当遭受 DoS 和 FDI 攻击时，传统二次控制策略可能失效，导致系统电压偏差、功率分配失衡甚至运行崩溃。为解决混合攻击引发的控制性能退化问题，需要构建准确的网络攻击模型，分析攻击的作用机理与影响规律，从而为防御策略设计提供理论支撑。在本小节中，对混合网络攻击进行建模。

3.3.1 DoS 攻击模型

直流微电网中 DG 的控制器通过通信网络进行邻居间的信息交互，在这个通讯过程中可能会遭受到 DoS 攻击。DoS 攻击通过阻塞通道来影响信息的的传输，

它在每个变换器与其邻居节点通信时起作用，导致控制器无法接收到相邻单元的信息。为了对 DoS 攻击进行数学建模，需要两个时间序列：$\theta_D=\{s_1,s_2,...,s_k,...\}$ 和 $\theta_I=\{\varsigma_1,\varsigma_2,...,\varsigma_k,...\}$ 分别描述它发生的时刻和持续时间。Π_D(s,t)为攻击者在[s,t]时间间隔内阻断的通信网络的集合，Π_N(s,t)为在[s,t]上不受 DoS 攻击的通信网络的集合，如图 3.2 所示。

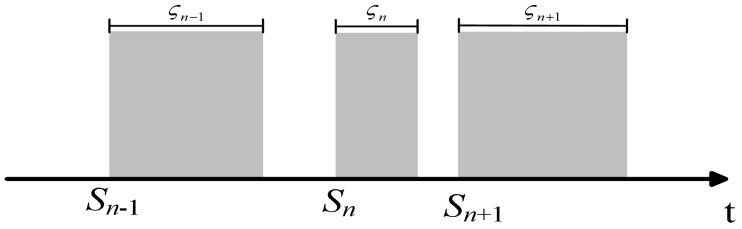


图 3.2 随机 DoS 攻击序列示意图

则通信网络的状态描述为：

$$p(t)=\begin{cases}0, & t\in\Pi_D\\ 1, & t\in\Pi_N\end{cases} \tag{3-8}$$

假设存在一个常数 0< ρ <1，使得

$$\left|\Pi_N(0,t)\right|\geq\rho t \tag{3-9}$$

式中，$\left|\Pi_N(0,t)\right|$为$\Pi_N(0,t)$的长度。

3.3.2 FDI 攻击模型

FDI 攻击可以通过篡改传感器测量的有效信息对直流微电网产生显著影响。FDI 攻击在微电网控制系统中的作用的原理如下：攻击者利用系统数据验证机制缺陷，在信息采集、传输或处理环节植入伪造数据，通过篡改真实状态参数破坏系统正常运行。由于分布式控制系统采用局部通信机制，各节点仅与相邻节点进行数据交互，缺乏全局信息感知能力，因此当特定节点或通信链路遭受攻击时，系统难以有效识别数据异常性。在二次控制环节中，所有与通信和计算相关的组件(包括传感器、控制器及通信链路)均可能成为 FDI 攻击的目标。

本章关注的是发生在控制器上的 FDI 攻击，而非直接操纵电流和电压等物理量，此类攻击通过修改二次控制器的输出信号实现。对于连续无界 FDI 攻击，

这些信号表示为函数 $\omega_i^z(t)$，则有：

$$u_i^a(t)=u_i(t)+\omega_i^z(t) \tag{3-10}$$

式中，$u_i^a(t)$为受到 FDI 攻击后的包含虚假数据的二次控制信号，$u_i(t)$为系统真实的二次控制信号。

3.4 基于事件触发的二次控制器设计

分布式分层弹性事件触发控制器在第 2 章中所介绍的传统分布式二次控制器的基础上集成了一个基于事件触发的管理器，通过事件触发来提高控制器性能，如图 3.3 所示。管理器根据传感器收集的信息判断哪个部分更需要配置，在两个子控制器信号之间切换。

在第 2 章中的分布式二次控制器采用同步实现直流母线电压调节与电流分配的线性叠加控制策略。该线性叠加策略在有向通信网络环境下可能引发控制性能耦合问题。具体而言，电流误差反馈环节旨在实现比例分配电流，而电压误差反馈环节则负责维持母线电压稳定。由于控制输入维数小于被控对象阶数，两个控制通道可能产生相互干扰。基于这一特性，在本节中设计一种具有动态调节能力的管理架构，以优化直流微电网的控制参数配置。

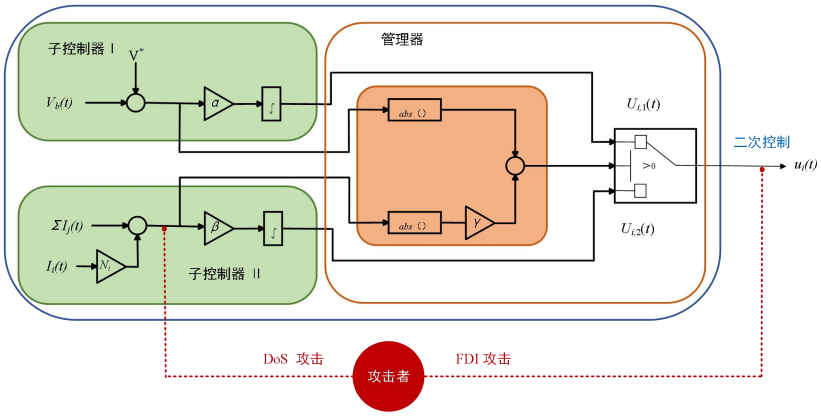


图 3.3 分布式事件触发二次控制

基于直流微电网的调压和均流两个调节目标和控制器 i 的电压和电流误差，该二次控制器的设计两个相应的子次级控制器 u_{i,σ_i}，$\sigma_i=\{1,2\}$。详细设计如下所示。

第一个子控制器是基于母线电压误差反馈。母线电压作为直流微电网中至关

重要的运行参数，其稳定性直接关系到整个系统的正常运行。该子控制器通过实时监测母线电压的实际值与设定的目标值之间的误差，并根据该误差进行精确计算和调整，从而实现对母线电压的有效控制。

子控制器I：

$$\begin{cases} u_{i,1}(t)=\delta_{i,1}(t) \\ \dot{\delta}_{i,1}(t)=-\alpha e_V(t) \end{cases} \tag{3-11}$$

第二个子控制器则是基于支路电流误差反馈。支路电流同样是直流微电网运行中的关键参数，不同的 DG 在输出功率时会通过各自的支路输送电流。该子控制器能够实时监测各支路电流的实际值与预期值之间的误差，进而对各支路的电流进行精准调节，以实现系统电流的合理分配。

子控制器II：

$$\begin{cases} u_{i,2}(t)=\delta_{i,2}(t) \\ \dot{\delta}_{i,2}(t)=-\beta e_{I,i}(t) \end{cases} \tag{3-12}$$

式中，$u_{i,1}$和$u_{i,2}$是两个子控制器；$\delta_{i,1}$和$\delta_{i,2}$表示控制器的内部状态；α和β需要设计的正参数。

分布式控制器二级控制框架中的管理器根据触发条件来负责协调子控制器之间的切换。

$$u_i(t)=\begin{cases} u_{i,1}(t), & \text{if} \quad f(e_V,e_{I,i})>0 \\ u_{i,2}(t), & \text{if} \quad f(e_V,e_{I,i})\le 0 \end{cases} \tag{3-13}$$

基于事件触发的管理器在整个控制器中起到了智能调度的核心作用。它会实时对系统的状态进行全面监测和分析，根据系统当前的运行状况、母线电压误差、支路电流误差等多种关键因素，动态地选择合适的子控制器投入工作。这种智能化的选择机制使得控制器根据系统的实际需求灵活调整控制策略，有效提高了控制的精准性和效率。

触发条件 $f(e_V,e_{I,i})$ 为：

$$f(e_V,e_{I,i})=\left|e_V\right|-\gamma\left|e_{I,i}\right| \tag{3-14}$$

式中，$\gamma=\dfrac{\beta}{\alpha}$。

由公式(3-4)、(3-5)、(3-11)以及(3-12)可知，子控制器I需要通过通讯网络获

得母线电压信息，子控制器II需要通过通讯网络获得相邻节点电流信息。

在混合攻击的持续冲击下，在二级控制器中设计一个补偿 $\Delta_{i,\sigma}(t)$，$\sigma=\{1,2\}$，来抵消存在 DoS 攻击时连续时间 FDI 攻击，使直流微电网在允许的偏差范围内实现电流的分配和电压的调节。

子控制器I：

$$\begin{cases} u_{i,1}(t)=\delta_{i,1}(t) \\ \dot{\delta}_{i,1}(t)=p(t)(-\alpha e_V(t)+\omega_i^z(t)+\Delta_{i,1}(t)) \\ \dot{\Delta}_{i,1}(t)=-p(t)\alpha e_V(t) \end{cases} \tag{3-15}$$

子控制器II：

$$\begin{cases} u_{i,2}(t)=\delta_{i,2}(t) \\ \dot{\delta}_{i,2}(t)=p(t)(-\beta e_{I,i}(t)+\omega_i^z(t)+\Delta_{i,2}(t)) \\ \dot{\Delta}_{i,2}(t)=-p(t)\beta e_{I,i}(t) \end{cases} \tag{3-16}$$

二次控制：

$$u_i(t)=\begin{cases} u_{i,1}(t), & \text{if} \quad f(e_V,e_{I,i})>0 \\ u_{i,2}(t), & \text{if} \quad f(e_V,e_{I,i})\le 0 \end{cases} \tag{3-17}$$

触发条件：

$$f(e_V,e_{I,i})=\left|e_V(t)\right|-\gamma\left|e_{I,i}(t)\right| \tag{3-18}$$

式中，$\Delta_{i,\sigma}(t)$ FDI 攻击的补偿项，$p(t)$ 是 DoS 攻击函数(3-8)。$p(t)\omega_i^z(t)$ 项表明当 DoS 攻击阻断通信网络时，FDI 攻击信号不能通过网络发挥作用。

3.5 闭环系统

定义 $I=\mathrm{col}[I_1,...,I_N]$，$V=\mathrm{col}[V_1,...,V_N]$，$e_I=\mathrm{col}[e_{I,1},...,e_{I,N}]$，$\delta=\mathrm{col}[\delta_{1,\sigma_1},...,\delta_{N,\sigma_N}]$，$K=\mathrm{diag}[k_1,...,k_N]$，$D=\mathrm{diag}[d_1,...,d_N]$，由潮流方程(3-1)以及(3-6)(3-7)可得对 I_i 求导为：

$$\dot{I}_i=\frac{1}{R_i+R_{D,i}}(\dot{\delta}_{i,\sigma_i}-\dot{V}_b)=k_i(\dot{\delta}_{i,\sigma_i}-\dot{V}_b) \tag{3-19}$$

式中，$k_i=\dfrac{1}{R_i+R_{D,i}}$

由潮流方程(3-1)以及(3-19)可得V_b的导数为：

$$\dot{V}_b=\frac{\sum_{i\in v}k_i\dot{\delta}_{i,\sigma_i}}{\sum_{i\in v}k_i+\sum_{i\in C_L}\frac{1}{R_{L,i}}}=\frac{1}{\eta}\sum_{i\in v}k_i\dot{\delta}_{i,\sigma_i} \tag{3-20}$$

式中，$\eta=\sum_{i\in v}k_i+\sum_{i\in C_L}\frac{1}{R_{L,i}}$。

将(3-20)带入(3-19)可得：

$$\dot{I}_i=k_i(\dot{\delta}_{i,\sigma_i}-\frac{1}{\eta}\sum_{i\in v}k_i\dot{\delta}_{i,\sigma_i}) \tag{3-21}$$

向量形式为$\dot{I}=K(I_N-\frac{1}{\eta}1_N1_N^TK)\dot{\delta}$，$1_N$为所有元素都为1的列向量，则有

$$\dot{e}_V=\dot{V}_b=\frac{1}{\eta}1_N1_N^TK\dot{\delta} \tag{3-21}$$

$$\dot{e}_I=D^{-1}LD^{-1}\dot{I}=D^{-1}LD^{-1}K(I_N-\frac{1}{\eta}1_N1_N^TK)\dot{\delta}=D^{-1}LD^{-1}K\Gamma\dot{\delta} \tag{3-23}$$

L为通信网络的拉普拉斯矩阵，$\Gamma=I_N-\frac{1}{\eta}1_N1_N^TK$。

定义组合误差为：

$$\varphi_i=\alpha e_V(t)+\beta e_{I,i}(t) \tag{3-24}$$

$$\varphi_{i,1}=\alpha e_V \tag{3-25}$$

$$\varphi_{i,2}=\beta e_{I,i} \tag{3-26}$$

令 $\varphi(t)=\mathrm{col}(\varphi_1(t),...,\varphi_N(t))$，$\Delta(t)=\mathrm{col}(\Delta_{1,\sigma_1}(t),...,\Delta_{N,\sigma_N}(t))$，$\varphi_{i,\sigma_i}(t)=\mathrm{col}(\varphi_{1,\sigma_1}(t),...,\varphi_{N,\sigma_N}(t))$对(3-24)求导则有

$$\dot{\varphi}(t)=\alpha\dot{e}_V(t)+\beta\dot{e}_I(t)=(\alpha\frac{1}{\eta}1_N1_N^TK+\beta D^{-1}LD^{-1}K\Gamma)\dot{\delta}=\Phi\dot{\delta} \tag{3-27}$$

式中，Φ 为闭环系统动态矩阵，$\Phi=\alpha\frac{1}{\eta}1_N1_N^TK+\beta D^{-1}LD^{-1}K\Gamma$ 。

令 $\tilde{\Delta}(t)=\omega_i^z(t)+\Delta(t)$，由(3-15)(3-16)和(3-27)可得闭环系统为

$$\begin{bmatrix}\dot{\varphi}(t)\\ \dot{\tilde{\Delta}}(t)\end{bmatrix}=\begin{bmatrix}-\Phi & \Phi\\ -I_N & 0\end{bmatrix}\begin{bmatrix}\varphi_{i,\sigma_i}(t)\\ \tilde{\Delta}(t)\end{bmatrix}+\begin{bmatrix}0\\ \dot{\omega}_i^z(t)\end{bmatrix} \tag{3-28}$$

3.6 算例及仿真结果分析

在本节中，基于 Matlab/Simulink 建立模型，验证所设计的控制器的有效性。仿真中使用的直流微电网模型如图 3.4 所示，该模型由 4 个 DG 及其相对应的控制器组成。详细参数见表 3.1，母线参考电压为 100V。本节中的 DoS 攻击是一个周期为 0.1 的方波信号，正常通信时间为 0.07s，取 ρ=0.7。

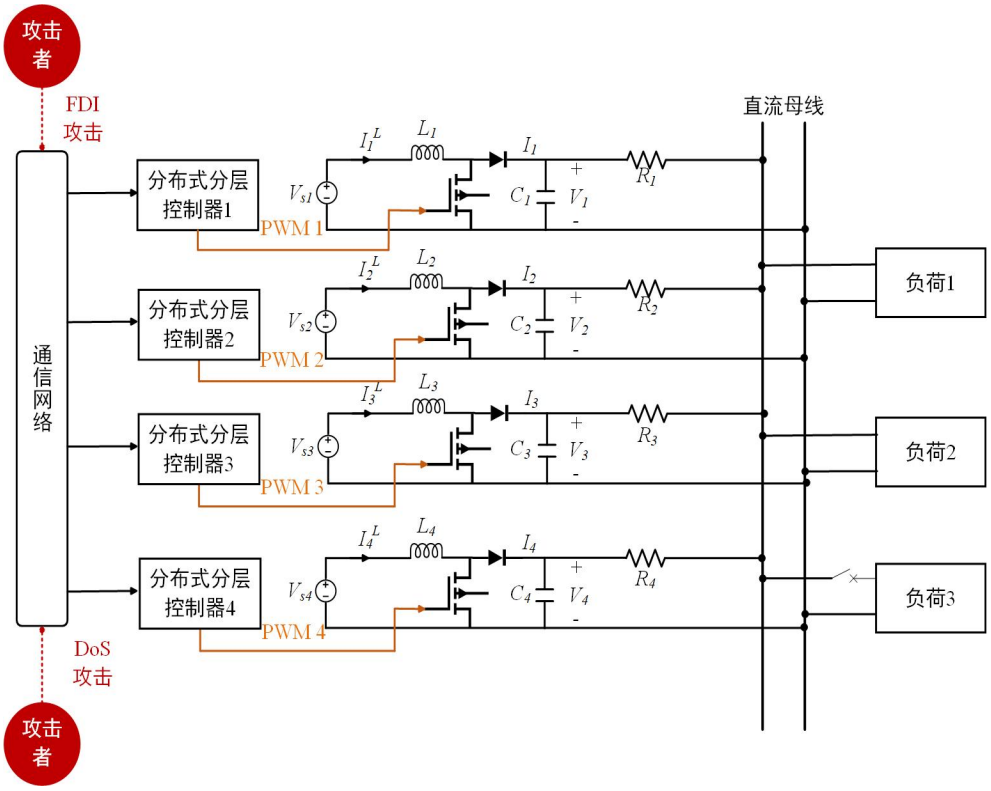


图 3.4 直流微电网 simulink 仿真模型

表 3.1 直流微电网系统参数

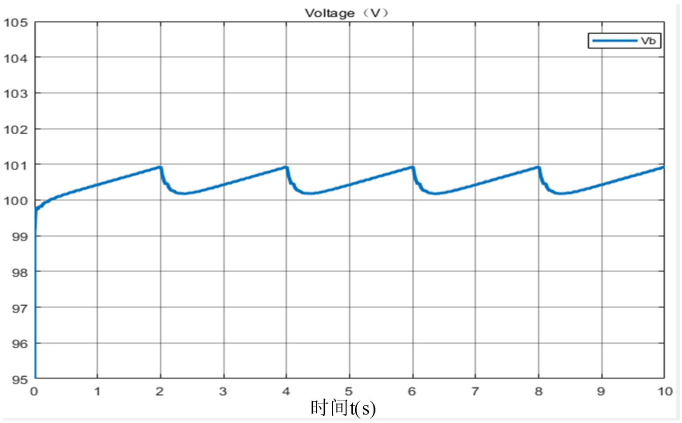
直流微电网参数	
DC 电源	V_{si}=50V，i=1，2，3，4
LC 滤波	L_i=2mH，C_i=470μF，i=1，2，3，4
线路电阻	R_1=0.2Ω，R_2=0.4Ω，R_3=0.5Ω，R_4=0.3Ω
负荷	$R_{L,1}$=50Ω，$R_{L,2}$=100Ω，$R_{L,3}$=100Ω
一次控制参数	
电压环	K_{VPi}=0.2，K_{VIi}=16，i=1，2，3，4
电流环	K_{IPi}=1.5，K_{IIi}=0.1，i=1，2，3，4
下垂增益	$R_{D,1}$=1.8，$R_{D,2}$=1.6，$R_{D,3}$=1.5，$R_{D,4}$=1.7
二次控制参数	
增益参数	α=10，β=10，γ=1

3.6.1 调压和均流测试

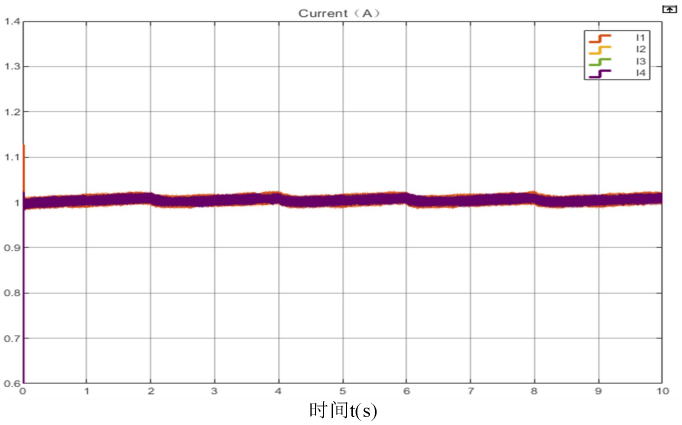
本节验证所设计的控制器是否能实现调压和均流的目标，仿真时间设置为10s。在本案例中测试所设计的控制器是否能实现按设定目标值调节电压并按任意所需比例输出电流。将所设计的控制器(3-15)-(3-18)与传统控制器(3-11)-(3-14)进行比较。仿真时间设置为 10s，电流比例参数设置为 d_i=1，i=1，2，3，4，即输出电流为 I_1：I_2：I_3：I_4=1：1：1：1。

(1)周期性锯齿信号注入

仿真时间设置为10s，向通信系统注入DoS和周期性锯齿信号FDI混合攻击。由于通讯系统中存在混合网络攻击，如图 3.5 所示的传统分布式控制器(3-11)-(3-14)因缺乏有效的攻击防御和数据校验机制，无法准确获取系统真实状态信息。这导致其控制指令出现偏差，难以维持电压稳定，母线电压呈现出锯齿状周期震荡，各分布式变换器输出电流也随之产生周期性波动。这种不稳定的运行状态，不仅严重影响系统供电质量，还可能引发设备过载、寿命缩短等一系列问题。



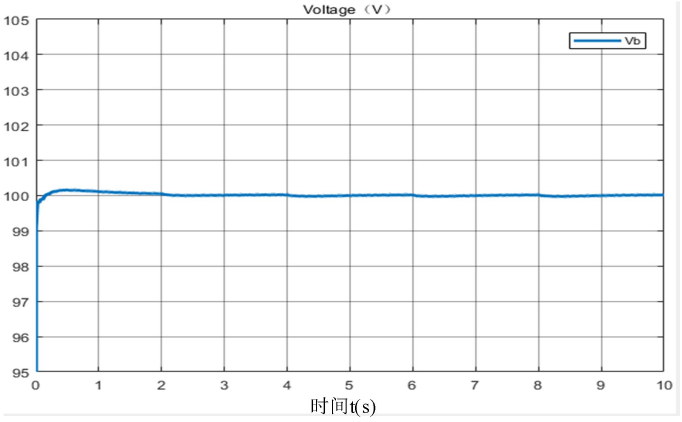
(a)调压



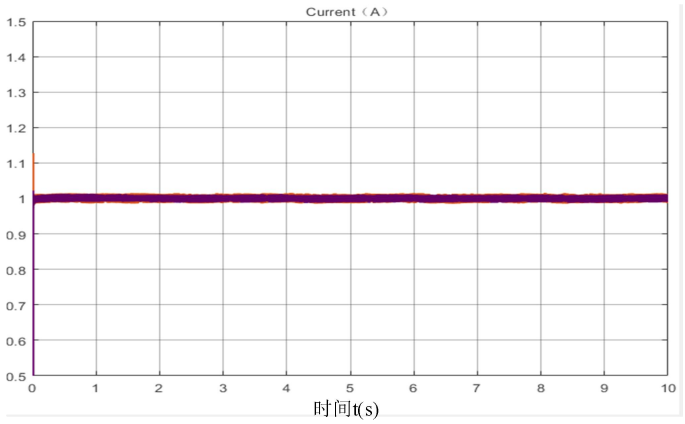
(b)均流

图 3.5 传统分布式控制器锯齿攻击信号性能

相比之下，从图 3.6 中可以看出，文中所设计的弹性分布式控制器在在周期性 FDI 攻击和 DoS 攻击的双重压力下，它依然能够保持精准的电压调节能力，将母线电压稳定在设定范围内，同时通过优化的电流分配算法，确保各分布式变换器输出电流按照预定比例稳定分配。



(a)调压



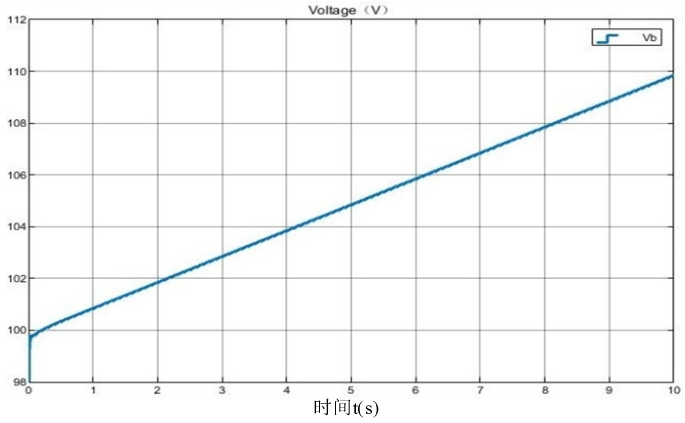
(b)均流

图 3.6 弹性布式控制器锯齿攻击信号性能

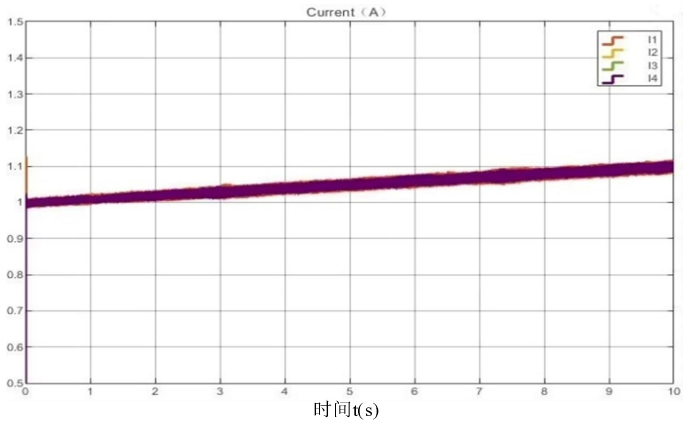
(2)无界时变信号注入

仿真时间设置为 10s，向通信系统注入 DoS 和无界时变 FDI 混合攻击，取 $\omega_i^z(t)=10t$ 。

由于通讯系统中存在混合网络攻击，如图 3.7 所示，在传统分布式控制器(3-11)-(3-14)的情况下，母线电压在网络攻击下持续升高，电流也不断增加，这说明其在受到攻击时无法实现控制目标。电压与电流的异常攀升，不仅使系统偏离正常运行状态，更可能触发过压、过流保护机制，引发设备损坏甚至系统崩溃，充分印证其在遭受攻击时无法实现维持系统稳定运行的核心控制目标。



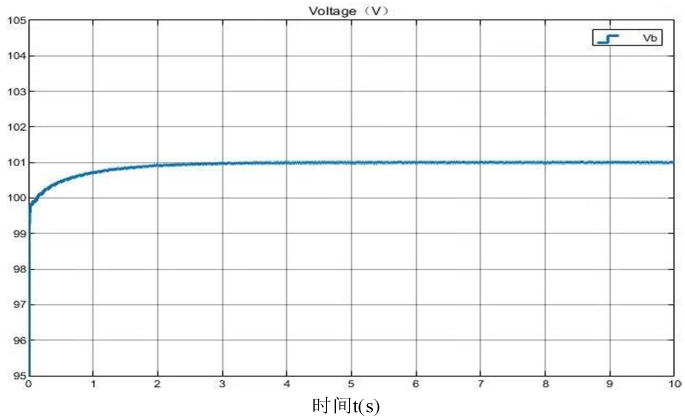
(a)调压



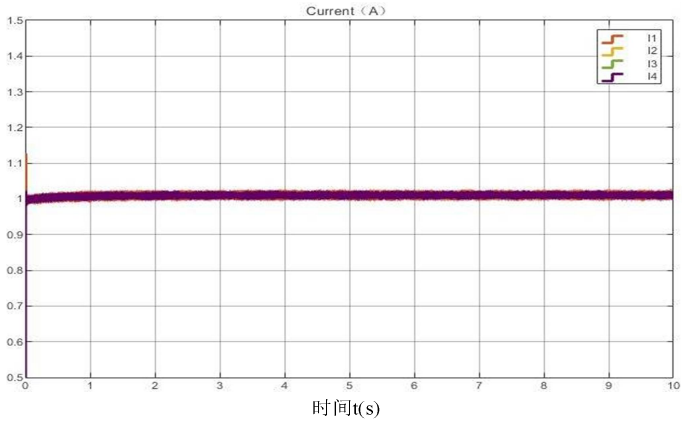
(b)均流

图 3.7 传统分布式控制器无界时变攻击信号性能

相比之下，从图 3.8 中可以看出，文中所设计的弹性分布式控制器在持续存在无界 FDI 攻击和 DoS 攻击的情况下，能够将母线电压维持在额定值附近的稳定水平，也能保证电流的合理分配。



(a)调压



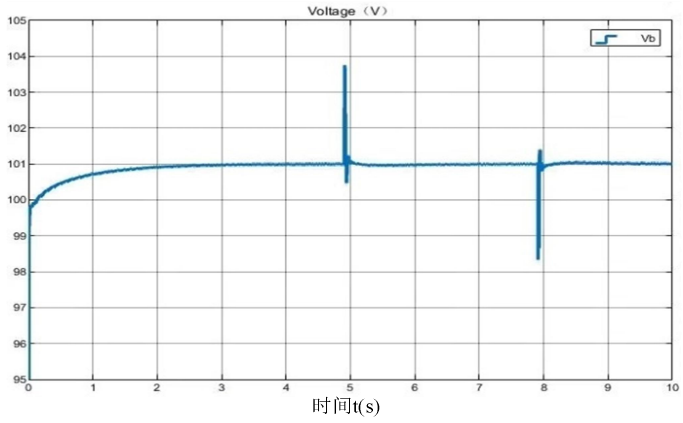
(b)均流

图 3.8 弹性布式控制器无界时变攻击信号性能

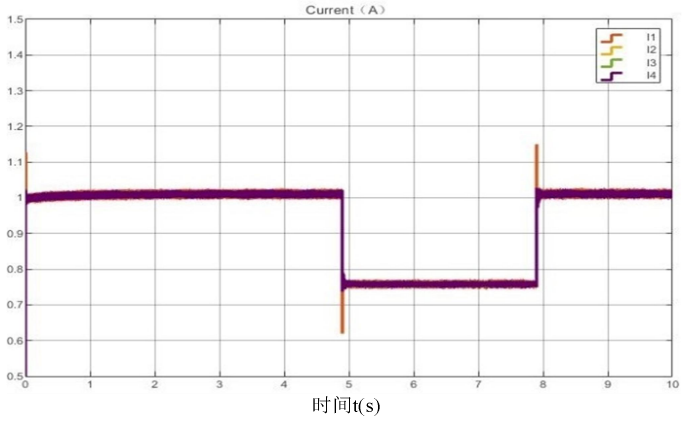
3.6.2 负荷突变测试

本例中，仍将仿真时间设置为 10s，电流比例参数设置为 d_i=1，i=1，2，3，4。本次实验的核心目标是测试本文所设计的控制器在负荷阶跃工况下的性能。实验过程中，以 100Ω负荷作为阶跃负载，通过模拟其断开与重新连接的操作，人为制造系统负荷的剧烈变化。在 t=4.9s 时，切除 100Ω的负荷，t=7.9s 时重新将负荷连接入回路。

如图 3.9 所示实验结果曲线来看，在整个负荷阶跃过程中，尽管由于负荷的突变不可避免地产生了瞬态偏差，但凭借控制器先进的控制算法与快速响应机制，稳态母线电压都能够在极短时间内恢复至 100V。



(a)调压



(b)均流

图 3.9 分布式控制器的负载阶跃性能仿真结果

结果充分表明，本文所设计的控制器具备优异的负荷阶跃性能，不仅能够有效抑制负荷变化带来的电压波动，还能在瞬态过程结束后迅速实现系统的稳定运

行。在通讯网络存在混合网络攻击的情况下，控制器展现出良好的动态调节能力与稳态精度，为实际电力系统的稳定运行提供了可靠的技术保障。

3.7 本章小结

本章设计了一种适用于单母线直流微电网系统的分布式分层弹性事件触发控制器设计，旨在混合网络攻击下实现调压与均流控制目标。该控制器是基于传统二次控制的电压和电流反馈回路设计了两个子控制器，通过反馈回路中引入补偿项以抵消 FDI 信号，并通过事件触发环节动态选择子控制器。最后以孤岛微电网为仿真对象，在 Matlab/Simulink 中搭建模型，对分布式控制器的调压和均流性能进行了测试，仿真结果表明了该控制器的有效性，同时也验证了该控制器在负载突变的情况下仍能快速实现调节目标。

第 4 章 混合网络攻击下基于攻击缓解层的微电网分布式二次控制策略

4.1 引言

在前两章中，针对直流微电网的分布式二次控制展开了研究，构建了直流微电网模型和分布式分层控制结构。由于分布式二次控制需要依赖于通讯网络，而通讯网络面临网络攻击的安全隐患，因此在第 3 章中提出了一种在连续通讯情况下能够应对 FDI 和 DoS 混合攻击的分布式二次控制器。然而，分析表明，采用周期采样通讯可以大大减少通讯信息，从而有效降低通信和计算资源的浪费。

基于此，本章中提出一种集成弹性周期采样机制与基于神经网络 FDI 攻击缓解层的分布式分层弹性控制方案。该方案在二级控制层采用弹性周期采样，通过减少因 DoS 攻击而丢失的采样数据，降低了 DoS 攻击对直流微电网通信系统的影响，使通信系统能够获取更有效的信息，进而提升通信效率与系统性能。FDI 攻击缓解层利用神经网络估计系统状态，能够过滤虚假数据、修复优化真实数据，以减轻甚至消除 FDI 攻击的影响，同时也解决了上一章设计方案不能重建或估计 FDI 攻击的问题。在 Matlab/Simulink 环境搭建直流微电网测试系统，验证了设计的控制器的有效性。

4.2 系统模型

4.2.1 微电网与控制系统

沿用第 3 章中的直流微电网系统，如图 3.1 所示，其模型与第 3 章公式(3-1)一致，即：

$$\begin{cases} R_i I_i = V_i - V_b \\ \sum_{i \in v} I_i = V_b \sum_{i \in C_L} \dfrac{1}{R_{L,i}} \end{cases} \tag{4-1}$$

式中，式中各项含义皆与公式(3-1)相同。

同时，仍采用分布式分层控制结构，即：

$$V_i^{ref}(t)=V^*-R_{D,i}I_i(t)+u_i(t) \tag{4-2}$$

式中，V^*为直流母线的额定电压，$R_{D,i}$为下垂系数，$u_i(t)$为二次控制信号。

4.2.2 二次控制模型

将母线电压误差和第 i 个控制器的电流误差分别定义为以下形式：

$$e_V(t)=V_b(t)-V^* \tag{4-3}$$

$$e_{I,i}=\frac{1}{d_i}\sum_{j\in N_i}(I_i(t)/d_i-I_j(t)/d_j) \tag{4-4}$$

基于直流微电网的调压和均流目标和上述两个误差，传统分布式二次控制器形式如下：

$$\begin{cases}u_i(t)=\delta_i(t)\\ \dot{\delta}_i(t)=-\alpha e_V(t)-\beta e_{I,i}(t)\end{cases} \tag{4-5}$$

δ_i表示控制器的内部状态；正参数α和β分别为电压和电流的增益。

由式(4-3)、(4-4)和(4-5)可知，为实现调压和均流，该控制器需要各个 DG 之间的通信，需要通过通讯网络获得母线电压信息，与相邻节点电流信息。

然而通信过程极易遭受网络攻击。当攻击者通过 DoS 攻击阻断通信通道或是使用 FDI 攻击篡改交互数据时，该控制器将不能完成相应的控制目标，甚至将影响到系统的稳定性。针对上述网络攻击引起的问题，对二次控制器(4-5)进行改进，引入一种弹性采样机制以减轻 DoS 攻击的影响，并对采样结果进行检测与修正。

4.3 以节点为目标的混合网络攻击模型

4.3.1 DoS 攻击模型

攻击者利用 DoS 攻击来阻断通信信道，阻断信息的传递。在这种情况下，DoS 攻击将对系统的性能、数据的传递产生很大的影响，导致数据的丢失，从而

导致控制系统的失效。根据攻击对象的不同，DoS 攻击可分为两类：1)以节点为目标的 DoS 攻击，旨在防止某一节点向任意邻居发送信息。2)以通信链路为目标的 DoS 攻击，旨在破坏邻近节点间的通讯通道。DoS 攻击通过阻塞通道来影响直流微电网的性能，它在每个转换器与其邻居节点通信时起作用。相较于对通信链路的攻击，对节点攻击可以导致更为严重的影响，甚至导致系统崩溃。鉴于此，本章将重点研究节点目标型 DoS 攻击，即当 DG 受到 DoS 攻击时，其采样数据都会被阻塞，不能向所有邻近节点传送。

对 DoS 攻击进行数学建模，需要两个时间序列：$\theta_D=\{s_1,s_2,...,s_k,...\}$ 和 $\theta_I=\{\varsigma_1,\varsigma_2,...,\varsigma_k,...\}$，分别描述 DoS 攻击发生的时刻和相应持续的时间。即第 k 次 DoS 攻击开始于 s_k，并持续到 $s_k+\zeta_k$，并且 $s_k+\zeta_k<s_{k+1}$，使得攻击区间不会发生重叠。$\Pi_D(t_1,t_2)$为攻击者在$[t_1,t_2]$时间间隔内阻断的通信网络的集合，$\Pi_N(t_1,t_2)$为在$[t_1,t_2]$上不受 DoS 攻击的通信网络的集合，t_1，t_2 为任意正数且满足 $t_1<t_2$。

假设 1[72]：存在常数 $v\geq 0$，$\tau_D>0$，DoS 发生频率条件满足：

$$\left|n(t_1,t_2)\right|\leq v+\frac{t_2-t_1}{\tau_D},\forall t_2>t_1 \tag{4-5}$$

式中，$\left|n(t_1,t_2)\right|$表示在区间$[t_1,t_2]$内发生 DoS 的次数。

假设 2[72]：存在常数 T>1，DoS 持续时间条件满足:

$$\left|\Pi_D(t_1,t_2)\right|\leq \varsigma+\frac{t_2-t_1}{T},\forall t_2>t_1 \tag{4-6}$$

式中，$\left|\Pi_D(t_1,t_2)\right|$为$\Pi_D(t_1,t_2)$的长度。

4.3.2 FDI 攻击模型

FDI 攻击是通过对有效信息的篡改来影响系统。在本文中，所考虑的 FDI 攻击模型是将虚假数据添加到真实采样数据中。若未受到攻击的真实数据为 $x(t)$，其中 $x(t)$表示通信网络中进行传输的变换器输出电流 $I_i(t)$或是母线电压 $V_b(t)$，攻击网络的虚假数据为$\omega^z(t)$，则有：

$$x^a(t)=x(t)+\omega^z(t) \tag{4-7}$$

式中，$x^a(t)$为受到 FDI 攻击后采样的包含虚假数据的采样值，该值通过通信网络传输给相邻单元的二次控制；$x(t)$为系统真实数据。

4.4 分布式二次控制器设计

本章将在上文所述的分布式分层控制的基础上，针对 DoS 和 FDI 混合攻击下对数据传输过程的影响，构建网络攻击模型，并引入弹性周期采样机制和基于神经网络的 FDI 攻击缓解层，以检测并保障数据的稳定、正确传输，从而保障控制器的稳定运行，相应的整体控制框图如图 4.1 所示。

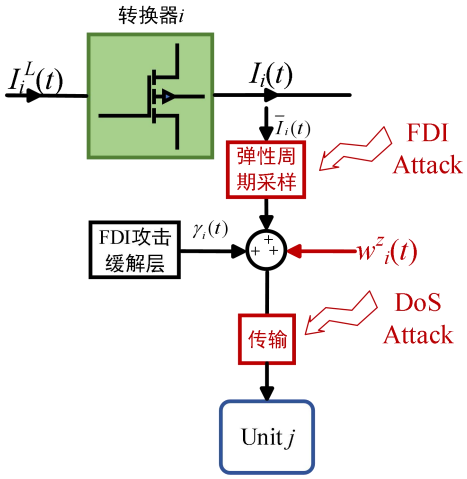


图 4.1 混合网络攻击下的数据通信

4.4.1 弹性周期采样

在 DG 中，每个二级控制器都有一个采样周期 $h>0$，在采样时刻 $S_n=nh(n=0,1,2,\ldots)$将实时信息传输给相邻控制器。但在 DoS 攻击的影响下，如果采样数据 $x(t)$在采样时刻 S_n 时通信链路受到攻击，则该数据无法传输。

以图 4.2(a)所示情况为例，在采样时刻 $S_n=nh$ 存在 DoS 攻击，因此 $x(S_n)$无法传输，直到 $t=S_{n+1}$，$x(S_{n+1})$才能正常传输。因此在 $t\in(S_n,S_{n+1})$内，系统的性能会受到影响。为了减轻 DoS 攻击对系统的影响，加入一种弹性周期采样机制，如果在采样瞬间 S_n 的采样数据不能顺利传输则在 $t\in[nh,(n+1)h)$区间内以一个较小的采样周期$\mathcal{E}(\mathcal{E}<h)$进行第二轮采样，直到 $S'_n=nh+l\mathcal{E}(l=1,2,\ldots,\mathcal{E}/h)$，采样数据能够顺利传输时停止，直到 $t=(n+1)h$，恢复以 h 为周期采样。

在$[S_n, S_{n+1})$期间，$x(S_n)$无法传输，其相邻 DG 信息不能及时更新，只能继续

保持在 S_n 时接收到的数据，直到 $S'_n=n'h$ 时，通信恢复，数据立即更新到 $x(S'_n)$。以 DG 的输出电流 I_i 为例，$t\in[t_k,t_{k+1})$其相邻 DG 接收到的信息为：

$$\bar{I}_i(t)=\begin{cases} I_i(S_{n-1}), & t\in[nh,n'h) \\ I_i(S'_n), & t\in[n'h,(n+1)h) \end{cases} \tag{4-8}$$

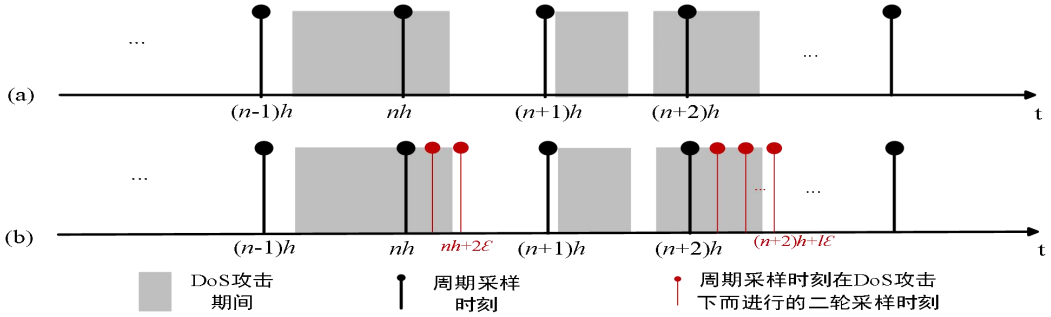


图 4.2 弹性周期采样(a)DoS 攻击下定周期采样；(b)DoS 攻击下弹性周期采样

4.4.2 基于神经网络 FDI 攻击缓解层

1、FDI 攻击缓解层

FDI 攻击会使采样数据偏离真实值，进而影响到控制器的正常运行，向传感器或通信链路注入 FDI 攻击均会引发系统状态扰动。具体而言，当 DG 的传感器遭受攻击时，该 DG 将向所有相邻节点发送错误数据；而通信链路攻击仅会影响通过该链路进行通信的特定邻居节点。由于针对 DG 传感器的 FDI 攻击等价于同时破坏该 DG 与所有邻居的通信链路。因此与第 3 章中考虑在控制器中注入 FDI 攻击不同的是，本章重点研究针对传感器的 FDI 攻击这种更具破坏性的攻击场景。主要的目的是检测通信网络的采样数据，减轻 FDI 攻击对控制系统的影响。采用的策略是使用基于神经网络的参考跟踪应用程序，以去除虚假数据$\omega^z(t)$，减少 FDI 攻击的影响。在这项工作中，为每个单元设计了一个局部估计器，使用神经网络估计变换器的输出电流和母线电压。将神经网络的输出做 PI 控制器的参考，然后用 PI 控制器的输出添加到变换器输出电流中以去除虚假信息$\omega^z(t)$，替换 $x^a(t)$作为传输到相邻单元的数值。

在图 4.3 中，以 DG 变换器 i 输出电流 $I_i(t)$为例，说明了该方法的实现过程。当分布式电源存在以神经网络单元和 PI 控制器构成的 FDI 攻击缓解层时，传输到相邻单元的变换器输出电流 $I_i(t)$替换为 $I_i^{'}(t)$，即：

$$I_i^{'}(t) = I_i(t) + \omega_i^z(t) + \gamma_i(t) \tag{4-9}$$

式中，$\omega_i^z(t)$为注入在 $I_i(t)$上的假数据，$\gamma_i(t)$为 PI 控制器的输出。

神经网络正常运行下，经 PI 控制器可以得出理想的估计值，即：

$$\lim_{t\to\infty} \omega_i^z(t) + \gamma_i(t) = 0 \tag{4-10}$$

也就是：

$$\lim_{t\to\infty} \gamma_i(t) = -\omega_i^z(t) \tag{4-11}$$

由式(4-11)可知，如果 $\lim_{t\to\infty} \gamma_i(t) \neq 0$，则表示该单元受到 FDI 攻击；如果 $\lim_{t\to\infty} \gamma_i(t) = 0$，则表示该单元未受到 FDI 攻击。因此，可以通过检测每个单元中的 $\gamma_i(t)$，可以判断该单元是否受到攻击，以及重构 FDI 攻击的虚假数据值。

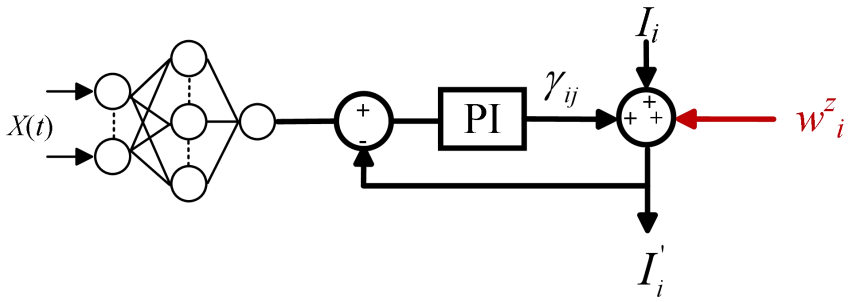


图 4.3 FDI 攻击缓解层

2、神经网络

在如图 4.3 所示的 FDI 攻击缓解策略中，攻击缓解层的输出 $I_i^{'}$ 应该接近真实数据 I_i，并且具有较高的精度和较小的误差。在这项工作中，神经网络作为估计器具有重要的作用，它应该准确地估计出变换器输出电流，并且误差小。前馈神经网络具有较好的估计和预测变换器输出电流的能力，因此，考虑到结果的可接受性及降低参考预测层的复杂性，选择前馈神经网络作为本工作的方案。

前馈神经网络由一个输入层、一个隐藏层和一个输出层组成。每一层由多个神经元组成，数据从一层的神经元传播到另一层[73]。用数学公示描述该映射关系如下：

$$\bar{y}(t) = f\left(\begin{bmatrix} x_1(t-1) & \cdots & x_1(t-D) \\ \cdots & \cdots & \cdots \\ x_n(t-1) & \cdots & x_n(t-D) \end{bmatrix}_{n\times D}\right) \tag{4-12}$$

式中，$\bar{y}(t)$ 表示神经网络输出，$x_n(t)$表示神经网络输入，$f(.)$表示一个非线性函数，D 为正数，表示输入存储顺序。

对于前馈神经网络的实现，需要两个步骤。第一步，对神经网络进行离线训练，得到一个训练后的神经网络；第二步，利用训练好的前馈神经网络对变换器输出的直流电流和母线电压进行监测和估计。首先，对具有一个隐藏层的前馈神经网络进行离线训练，然后对其进行检查，以估计不同情况下输出结果。在已有结果的基础上，在避免复杂性的前提下，考虑了一种单隐层的神经网络。具有一个隐藏层和一个输出的前馈神经网络的数学描述如下:

$$\bar{y} = f_{out}(f_{hid}(XW^{hid} + b^{hid})W^{out} + b^{out}) \tag{4-13}$$

式中 f_{hid} 和 f_{out} 别为隐藏层和输出层神经元的激活函数，b^{hid} 和 b^{out} 为隐藏层和输出层偏执权值，W^{hid} 和 W^{out} 为隐藏层和输出层权值矩阵。X 是有 n 个输入的神经网络的输入向量，定义如下:

$$X = (x_1, x_2, ..., x_k) \tag{4-14}$$

前馈神经网络离线训练的目的是找到 W^{hid}, W^{out}, b^{hid}，b^{out} 的最优值，并得到一个神经网络来正确估计输出。为了离线训练神经网络，需要准备一组输入数据和相应的输出，用于训练过程中对前馈神经网络的参数进行优化。进行离线训练的主要原因是，防御者可以确定训练所收集的数据来自非攻击条件，因此它们是真实值。

为了估计每个单元的输出电流 I_i，将第 i 个单元 DC/DC 转换器的输入电流 I^L_i 和输出电压 V_i 作为神经网络的输入，则由式(4-12)可得单元 i 的估计输出电流作为神经网络的输出有：

$$\bar{I}_i(t) = f_i\left(\begin{bmatrix} I_i^L(t-1) & ... & I_i^L(t-D) \\ V_i(t-1) & ... & V_i(t-D) \end{bmatrix}_{2\times D}\right) \tag{4-15}$$

式中，$\bar{I}_i(t)$ 为神经网络输出的估计值 $f_i(.)$为单元 i 的非线性函数。

与变换器输出电流一样，为估计母线电压 V_b 将各个单元变换器输出电压 V_i 作为神经网络的输入，则估计母线电压作为神经网络的输出有：

$$\bar{V}_b(t)=f_b\left(\begin{bmatrix} V_1(t-1) & \ldots & V_1(t-D) \\ V_2(t-1) & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ V_N(t-1) & \ldots & V_N(t-D) \end{bmatrix}_{N\times D}\right) \tag{4-16}$$

式中，$\bar{V}_b(t)$为神经网络输出的估计值$f_b(.)$母线电压的非线性函数。

4.5 算例及仿真结果分析

在本节中，在 Matlab/Simulink 中建立模型，验证所设计的控制器的有效性。仿真中使用的直流微电网模型如图 4.4 所示，该模型由 4 个分布式发电机和相应的控制器组成。一次控制经 PI 双环，通过 PWM 产生控制信号，二次控制接收来自通信链路的的信息，即母线电压和相邻系统电流。选取采样周期 h=0.06s，二轮采样周期$\mathcal{E}$=0.006s。微电网和控制系统的详细参数见表 4.1，母线参考电压为 100V。网络攻击：DoS 攻击每 0.1s 发生一次，每次持续 0.03s，FDI 攻击信号$\omega^z(t)$=-2t。

表 4.1 直流微电网系统参数

直流微电网参数	
DC 电源	V_{si}=50V，i=1，2，3，4
LC 滤波	L_i=2mH，C_i=470μF，i=1，2，3，4
线路电阻	R_1=0.2Ω，R_2=0.4Ω，R_3=0.5Ω，R_4=0.3Ω
负荷	$R_{L,1}$=50Ω，$R_{L,2}$=100Ω，$R_{L,3}$=100Ω
一次控制参数	
电压环	K_{VPi}=0.2，K_{VIi}=16，i=1，2，3，4
电流环	K_{IPi}=1.5，K_{IIi}=0.1，i=1，2，3，4
下垂增益	$R_{D,1}$=1.8，$R_{D,2}$=1.6，$R_{D,3}$=1.5，$R_{D,4}$=1.7
二次控制参数	
增益参数	α=10，β=10

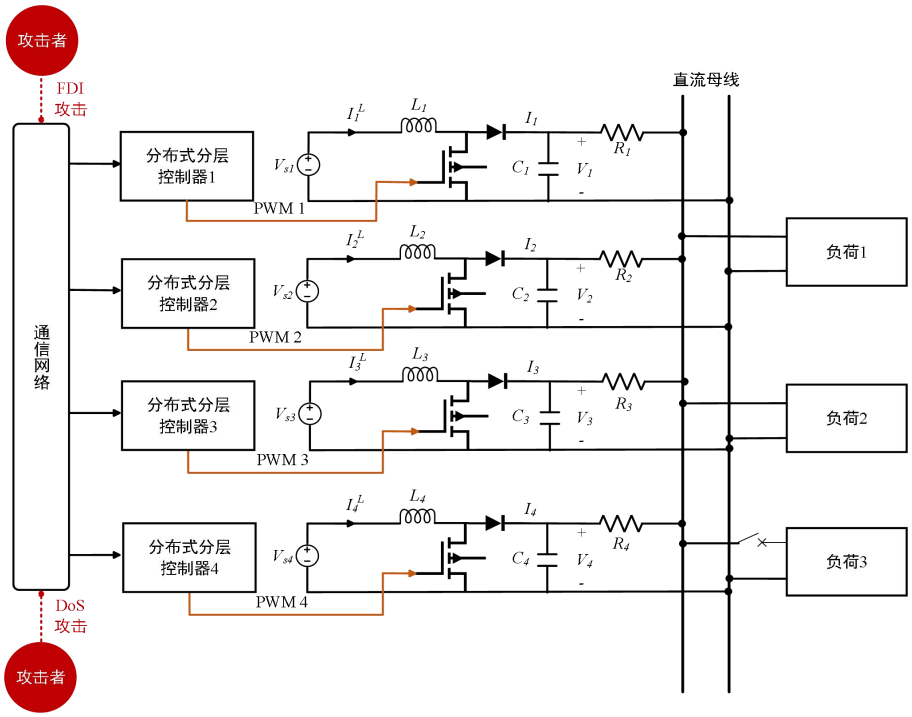
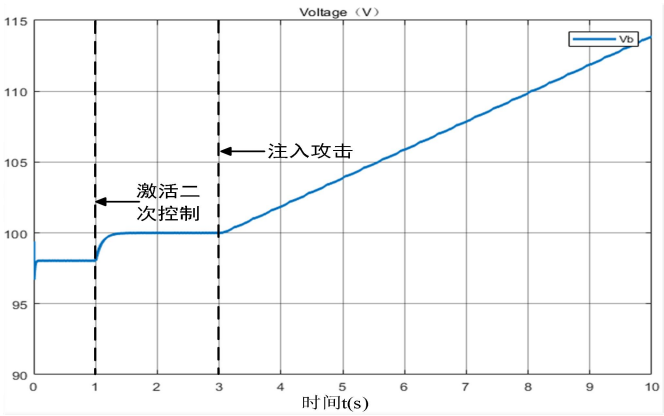


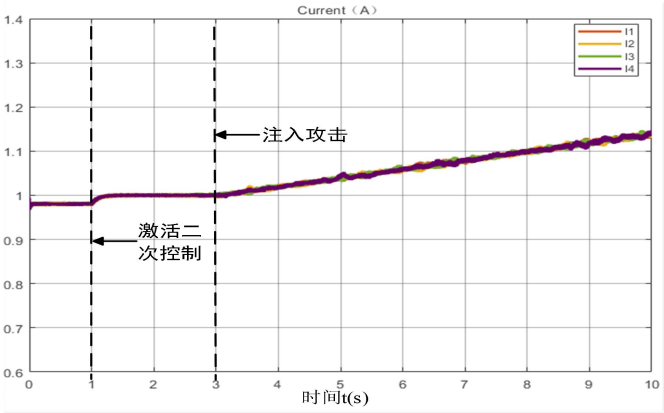
图 4.4 直流微电网 simulink 仿真模型

4.5.1 调压和均流测试

首先验证所设计的控制器在 FDI 和 DoS 混合攻击下仍能实现调压和均流的目标，并将其与传统的分布式二次控制器(4-5)在相同的攻击下进行比较。仿真时间设置为 10s，在 t∈[0,1)s 时，二次控制器未激活，只有一次控制器工作，在 t=1s 时，激活二次控制器。在 t=3s 时，向通信系统注入 FDI 和 DoS 混合攻击。本案例中，电流分配比例参数设置为 d_i=1，i=1，2，3，4。



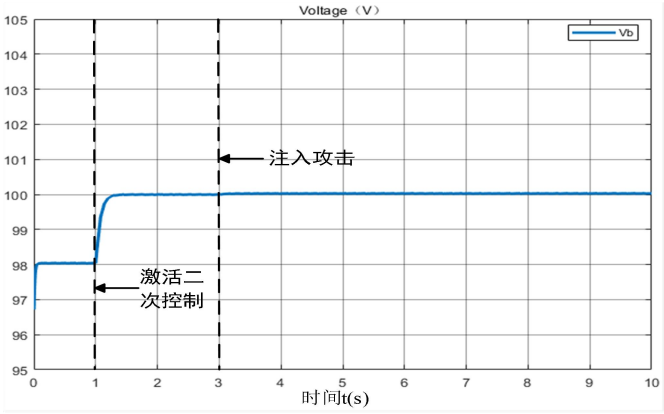
(a)调压



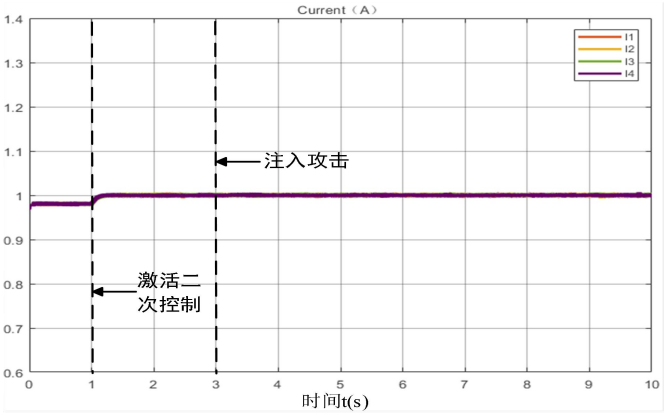
(b)均流

图 4.5 传统的分布式二次控制器(4-5)

在图 4.5 和 4.6 中，二次控制被激活后，二次控制解决了一次控制造成的母线电压偏差问题。在图 4.5 中，在通信系统中注入混合网络攻击后，母线电压继续升高，DG 的变换器输出电流也随之增大，这说明传统控制器(4-5)在受到攻击时无法实现控制目标。相比之下，从图 4.6 中可以看出，本章中所设计的控制器，在存在混合网络攻击的情况下仍能实现调压和均流。



(a)调压

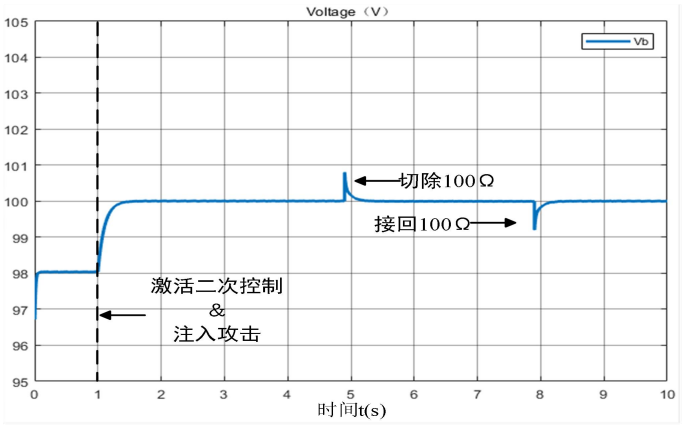


(b)均流

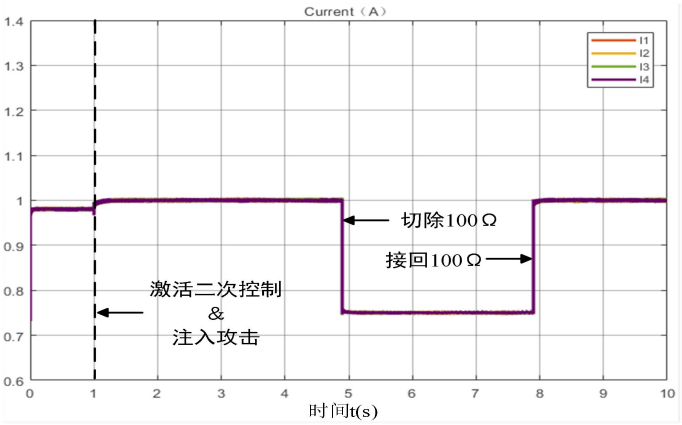
图 4.6 本章所设计分布式二次控制器

4.5.2 负荷突变测试

在本案例中测试所设计的控制器在混合攻击下的负荷阶跃性能。仿真时间设置为 10s，在 t=1s 时，激活二次控制器并向通信系统注入混合攻击。本案例中，电流分配比例参数设置为 d_i=1，i=1，2，3，4。在 t=4.9s 时，切除 100Ω的负荷，t=7.9s 时重新将负荷接入回路。如图 4.7 所示，无论是断开还是重新连接这 100Ω的负荷，都可以快速实现调压和并维持输出电流按预期比例分配。



(a)调压



(b)均流

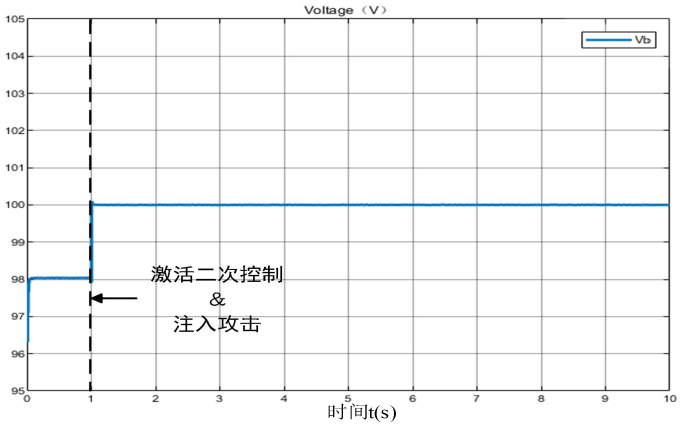
图 4.7 控制器在混合网络攻击下的负载阶跃性能测试

4.5.3 变输出电流分配比例参数测试

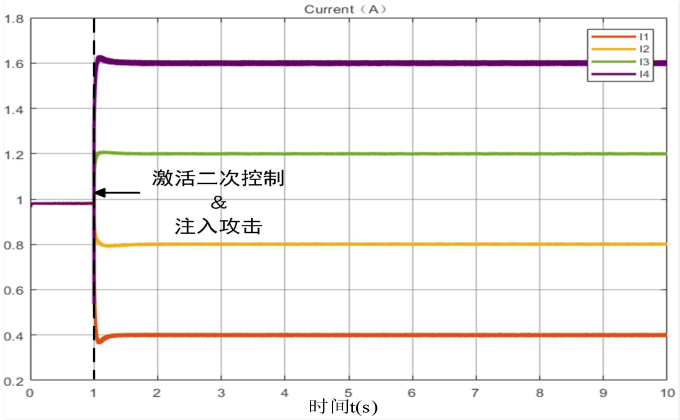
DG 的变换器输出电流的期望比例参数是电力系统在考虑经济特性的情况下计算得出的最优分配比例。在本案例中测试所设计的控制器在混合攻击下能实现

按任意所需比例输出电流。

(1)仿真时间设置为 10s，在 t=1s 时，激活二次控制器并向通信系统注入 FDI 和 DoS 混合攻击。设置电流分配比例参数设置为 d_1：d_2：d_3：d_4=1：2：3：4，即输出电流为 I_1：I_2：I_3：I_4=1：2：3：4。如图 4.8 所示，电压能维持在目标值 100V，输出电流按照预定的比例分配。



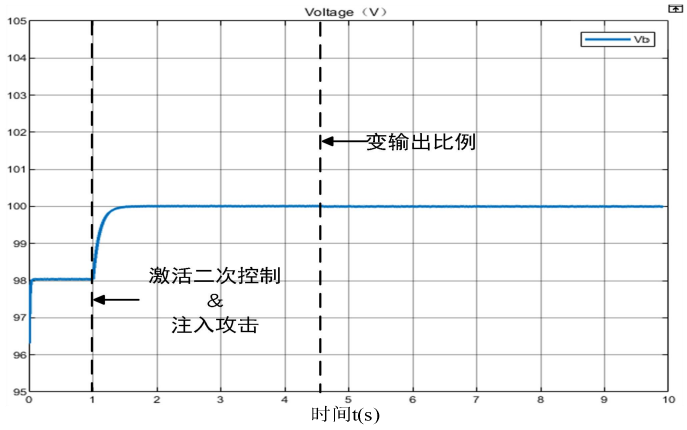
(a)调压



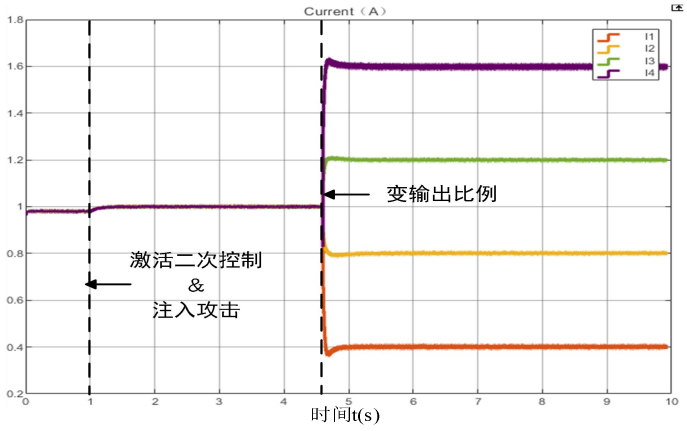
(b)均流

图 4.8 控制器在混合网络攻击下的性能测试(d_1：d_2：d_3：d_4：=1：2：3：4)

(2)仿真时间设置为 10s，在 t=1s 时，激活二次控制器并向通信系统注入 FDI 和 DoS 混合攻击。t∈[1,4.6)s 时，电流分配比例参数设置为 d_i=1，i=1，2，3，4；t∈[4.6,10)s 时，电流分配比例参数设置为 d_1：d_2：d_3：d_4=1：2：3：4。如图 4.9 所示，电压能维持在目标值 100V，输出电流按照预定的比例分配。



(a)调压



(b)均流

图 4.9 控制器在混合网络攻击下的变输出测试

4.6 本章小结

本章提出了一种适用于单母线直流微电网系统的分布式分层弹性控制器设计，旨在混合网络攻击下实现调压与均流控制目标。该控制器是基于传统二次控制的电压和电流反馈回路的基础上设计的，具体来说，在该控制器在二级控制层采用弹性周期采样以解决 DoS 攻击下数据丢失的问题，并将采样数据经 FDI 攻击缓解层进行优化，以减轻甚至消除 FDI 攻击的影响。最后在 Matlab/Simulink 中建立孤岛微电网为仿真对象，对分布式控制器的调压和均流性能进行了测试，同时也开展了对负荷突变场景的动态响应测试。仿真结果表明了该控制器的有效性，同时也验证了该控制器在各种不同的工作情况下仍能快速实现调节目标。

第 5 章 结论与展望

5.1 结论

本文围绕孤岛直流微电网分布式二次控制在网络攻击下的电压偏差、均流误差和通信安全问题，提出递进式解决方案，构建了理论与工程兼具的控制体系。

在研究初期，针对传统下垂控制缺陷，融合母线电压与支路电流误差反馈，设计分布式二次控制器。该控制器有效消除电压偏差，实现电源电流按比例输出。仿真结果表明，该策略在多种场景下都能实现调节目标，验证了基础控制框架的鲁棒性。然而，这一阶段的研究未考虑通信网络的安全威胁。

随着研究深入，通信链路的脆弱性成为新的焦点。面对 FDI 与 DoS 混合攻击的协同破坏，提出了分层弹性事件触发控制架构。解耦设计调压与均流子控制器。配合事件触发管理器动态调度，并引入补偿机制，以抵消存在 DoS 攻击下连续时间 FDI 攻击的影响，确保直流微电网在允许的偏差范围内实现电压和电流的稳定调节。但此方案仍受限于连续通信模式与攻击信号不可观测的缺陷，需进一步优化。

为突破上述局限，研究提出弹性周期采样机制与基于神经网络 FDI 攻击缓解层。前者依据系统实时状态和遭受攻击的情况，动态调整通信间隔。减少了因 DoS 攻击造成的数据丢失，降低了通信资源的消耗；后者利用神经网络估计系统状态，能够过滤虚假数据、修复优化真实数据，可减轻或消除 FDI 攻击影响，还能重建 FDI 攻击，实现通信与安全协同优化。

5.2 展望

尽管本文在网络攻击防御、通信优化等方面取得一定成果，但直流微电网的分布式控制仍面临诸多挑战。未来研究可在以下方向深化探索：

(1)非线性模型控制。本文研究基于线性模型，而实际直流微电网因电力电子变换器和负载呈非线性。未来需构建攻击感知的鲁棒控制框架，解决非线性误差补偿与攻击抵御双重难题。

(2)通讯故障的多样性分析。研究中仅关注恶意攻击，而器件故障、通信延

迟等非攻击因素也会影响通信。后续需建立融合故障辨识的安全控制框架，增强系统对复杂通信扰动的适应性。

(3)实物平台验证。当前研究仅通过仿真验证算法，未考虑实物平台的真实扰动对控制性能的影响，在仿真中被简化的因素可能导致理论设计与实际运行出现偏差。未来需搭建硬件在环半实物测试平台，完成从数字仿真到实际应用的闭环优化，提升控制策略的工程可靠性。

参考文献

[1] Peter N, Gupta P and Goel N. Intelligent Strategies for Microgrid Protection: A Comprehensive Review[J]. Applied Energy, 2025, 379: 124901-124939.

[2] 陈晓华, 王志平, 吴杰康, 等. 微电网技术研究综述[J]. 黑龙江电力, 2023, 45(06): 471-480.

[3] 雷基林, 余林兴, 别玉, 等. 孤岛微电网能量管理系统研究综述[J]. 发电技术, 2025, 46(02): 370-385.

[4] Hamanah W M, Hossain M I, Shafiullah M, et al. AC Microgrid Protection Schemes: A Comprehensive Review[J]. IEEE Access, 2023, 11: 76842-76868.

[5] Dahane S A and Sharma B R. Hybrid AC-DC Microgrid Coordinated Control Strategies: A Systematic Review and Future Prospect[J]. Renewable Energy Focus, 2024, 49: 100553-100567.

[6] Gu Y, Li W and He X. Frequency-Coordinating Virtual Impedance for Autonomous Power Management of DC Microgrid[J]. IEEE Transactions on Power Electronics, 2015, 30(4): 2328-2337.

[7] Xia Y, Wei W, Peng Y, et al. Decentralized Coordination Control for Parallel Bidirectional Power Converters in a Grid-Connected DC Microgrid[J]. IEEE Transactions on Smart Grid, 2018, 9(6): 6850-6861.

[8] 张译铎, 刘尚博, 孟晓芳. 交直流混合微电网运行控制策略研究[J]. 东北电力技术, 2024, 45(12): 26-31.

[9] Majid M, Mojtaba H and Fariborz S Z. An Overview on Consensus-Based Distributed Secondary Control Schemes in DC Microgrids[J]. Electric Power Systems Research, 2023, 225: 109870-109885.

[10] Papadimitriou C, Zountouridou E and Hatziargyriou N. Review of Hierarchical Control in DC Microgrids[J]. Electric Power Systems Research, 2015, 122: 159-167.

[11] Han Y, Ning X, Yang P, et al. Review of Power Sharing, Voltage Restoration and Stabilization Techniques in Hierarchical Controlled DC Microgrids[J]. IEEE

Access, 2019, 7: 202-223.

[12]JANG Enyu, ZHAO Jikang, Ml Yang, et al. Control Strategy of Reactive Power Sharing of Microgrid Based on Fuzzy Adaptive Virtual Impedance[J]. Southern Power System Technology, 2019, 13(05): 37-43.

[13]Gururaj M V and Padhy N P. A Novel Decentralized Coordinated Voltage Control Scheme for Distribution System with DC Microgrid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(5): 1962-1973.

[14]Ali N, Shen X, Armghan H, et al. Hierarchical Control Combined with Higher Order Sliding Mode Control for Integrating Wind/Tidal/Battery/Hydrogen Powered DC Offshore Microgrid[J]. Journal of Energy Storage, 2024, 82: 110521-110534.

[15]Sahoo S, Mishra S, Peng H, et al. A Stealth Cyber Attack Detection Strategy for DC Microgrids[J]. IEEE Transactions on Power Electronics, 2019, 34(8): 8162-8174.

[16]Chen Y, Qi D, Dong H, et al. A FDI Attack Resilient Distributed Secondary Control Strategy for Islanded Microgrids[J]. IEEE Transactions on Smart Grid, 2021, 12(3): 1929-1938.

[17]Ma Yong sheng, Che Wei wei and Deng chao. Event-Triggered Control of DC Microgrids With DoS Attacks[J]. Control Theory and Technology, 2022, 39(10): 1907-1914.

[18]Abianeh A J, Wan Y, Ferdowsi F, et al. Vulnerability Identification and Remediation of FDI Attacks in Islanded DC Microgrids Using Multiagent Reinforcement Learning[J] IEEE Transactions on Power Electronics, 2022, 37(6): 6359-6370.

[19]Hu S, Yuan P, Yue D, et al. Attack Resilient Event-Triggered Controller Design of DC Microgrids under DoS Attacks[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(2): 699-710.

[20]曹善康, 魏繁荣, 林湘宁, 等. 网侧电压跌落下计及无功支撑效能的直流微电网多目标优化策略[J]. 中国电机工程学报, 2023, 43(15): 5759-5772.

[21]Lejla A and Mustafa M. Comprehensive Review of Trends in Microgrid Control[J]. Renewable Energy Focus, 2021, 38: 84-96.

[22]Manohar M, Bhaskar P, Monalisa B, et al. A Systematic Review on DC-Microgrid Protection and Grounding Techniques: Issues, Challenges and Future Perspective[J]. Applied Energy, 2022, 313: 8010-8035.

[23]Srivastava C and Tripathy M. Novel Grounding and Protection Strategy for DC Microgrid Restraining Fault Current[J]. IEEE Transactions on Power Delivery, 2024, 39(4): 2182-2193.

[24]Kamal K and Hari O G. DC Microgrid: A Comprehensive Review on Protection Challenges and Schemes[J]. IETE Technical Review, 2023, 40(4): 574-590.

[25]Joshua, Mary A, Vittal, et al. Incremental Transient Power-Based Protection Scheme for a DC Microgrid[J]. Electrical Engineering, 2022, 104(4): 1-12.

[26]刘海媛. 直流微电网稳定与协调控制关键技术研究[D]. 中国矿业大学, 2019.

[27]邢晓敏, 潘尧坤, 李贻涛. 动态直流微电网故障分析及保护方案研究[J]. 电网与清洁能源, 2024, 40(11): 22-30.

[28]Pan P, Mandal K R, Manohar M, et al. An Intelligent Protection Scheme for DC Microgrid Using Hilbert-Huang Transform with Robustness Against PV Intermittency and DER Outage[J]. Electrical Engineering, 2024,106(5): 5967-5985.

[29]舒薇. 智能微电网保护和控制技术研究[J]. 智能建筑与智慧城市, 2021, 10: 148-150.

[30]申艳红, 庞科伟, 黄浩然. 多端直流输电与直流电网技术[J]. 电子技术与软件工程, 2018, 05: 173-173.

[31]刘进军. 电能系统未来发展趋势及其对电力电子技术的挑战[J]. 南方电网技术, 2016, 3(13): 78-81.

[32]Ikhide M, Tennakoon B S, Griffiths L A, et al. A Novel Time Domain Protection Technique for Multi-Terminal HVDC Networks Utilising Travelling Wave Energy[J]. Sustainable Energy, Grids and Networks, 2018, 16: 300-314.

[33]Kunya B A, Mundu M M, Babangida A, et al. MPC Based Frequency Control of an Autonomous Microgrid Integrated with Electric Vehicles[J]. Results in Engineering, 2025, 26: 104727-104738.

[34]Yang Y, Yandong C, An L, et al. Second Ripple Current Suppression by Two Bandpass Filters and Current Sharing Method for Energy Storage Converters in DC

Microgrid[J]. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2017, 5(3): 1031-1044.

[35] Yuen C, Oudalov A, and Timbus A. The Provision of Frequency Control Reserves from Multiple Microgrids[J]. IEEE Transactions on Industrial Electronics, 2011, 58: 173-183.

[36] Igyso Z, Ionela P and Laurent L. A Hierarchical Control Approach for Power Loss Minimization and Optimal Power Flow within a Meshed DC Microgrid[J]. Energies, 2021, 14(16): 4846-4895.

[37] Xie C, Wei M, Luo D, et al. Energy Balancing Strategy for the Multi-Storage Islanded DC Microgrid Based on Hierarchical Cooperative Control[J]. Frontiers in Energy Research, 2024, 12: 1390621-1390635.

[38] Y. Zeng, Q. Zhang, Y. Liu, et al. Hierarchical Cooperative Control Strategy for Battery Storage System in Islanded DC Microgrid[J]. IEEE Transactions on Power Systems, 2022, 37(5): 4028-4039.

[39] 姜海阳. DoS 攻击下基于边沿事件触发的直流微电网分布式控制[D]. 哈尔滨工业大学, 2023.

[40] Dragičević T, Lu X, Vasquez J C, et al. DC Microgrids—Part II: A Review of Power Architectures, Applications, and Standardization Issues[J]. IEEE Transactions on Power Electronics, 2016, 31(5): 3528-3549.

[41] Gavriluta C, Candela J I, Citro C, et al. Decentralized Primary Control of MTDC Networks with Energy Storage and Distributed Generation[J]. IEEE Transactions on Industry Applications, 2014, 50(6): 4122-4131.

[42] Liegmann E and Majumdre R. An Efficient Method of Multiple Storage Control in Microgrids[J]. IEEE Transactions on Power Systems, 2015, 30(6): 3437-3444.

[43] Liegmann E and Majumder R. An Efficient Method of Multiple Storage Control in Microgrids[J]. IEEE Transactions on Power Systems, 2015, 30(6): 3437-3444.

[44] Chi J, Peng W, Xiao J, et al. Implementation of Hierarchical Control in DC Microgrids[J]. IEEE Transactions on Industrial Electronics, 2014, 61(8): 4032-4042.

[45] Guo F, Xu Q, Wen C, et al. Distributed Secondary Control for Power Allocation

and Voltage Restoration in Islanded DC Microgrids[J]. IEEE Transactions on Sustainable Energy, 2018, 9(4): 1857-1869.

[46] Liu X K, Wang Y W, Lin P, et al. Distributed Supervisory Secondary Control for a DC Microgrid[J]. IEEE Transactions on Energy Conversion, 2020, 35(4): 1736-1746.

[47] Chen Z, Yu X, Xu W, et al. Modeling and Control of Islanded DC Microgrid Clusters with Hierarchical Event-Triggered Consensus Algorithm[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68(1): 376-386.

[48] Beg O A, Johnson T T and Davoudi A. Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5), 2693-2703.

[49] Ding D, Han Q L, Xiang Y, et al. A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems[J]. Neurocomputing, 2018, 275: 1674-1683.

[50] Liu J, Lu X and Wang J. Resilience Analysis of DC Microgrids under Denial of Service Threats[J]. IEEE Transactions on Power Systems, 2019, 34(4): 3199-3208.

[51] Yao W, Wang Y, Xu Y, et al. Cyber-Resilient Control of an Islanded Microgrid Under Latency Attacks and Random DoS Attacks[J]. IEEE Transactions on Industrial Informatics, 2023, 14(9): 5858-5869.

[52] Sahoo S, Mishra S, Peng J, et al. A Stealth Cyber-Attack Detection Strategy for DC Microgrids[J]. IEEE Trans Power Electron, 2018, 34(8): 8162-8174.

[53] Zuo S, Altun T, Lewis F L, et al. Distributed Resilient Secondary Control of DC Microgrids Against Unbounded Attacks[J]. IEEE Trans Smart Grid, 2020; 11(5): 3850-3859.

[54] Wan Y and Dragicevi T. Data-Driven Cyber-Attack Detection of Intelligent Attacks in Islanded DC Microgrids[J]. IEEE Transactions on Industrial Electronics, 2023, 70(4): 4293-4299.

[55] Mustafa A, Poudel B, Bidram A, et al. Detection and Mitigation of Data Manipulation Attacks in AC Microgrids[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2588-2603.

[56]Deng C, Wang Y, Wen C, et al. Distributed Resilient Control for Energy Storage Systems in Cyber–Physical Microgrids. IEEE Transactions on Industrial Informatics, 2021, 17(2): 1331-1341.

[57]Liu Y, Li Y, Wang Y, et al. Robust and Resilient Distributed Optimal Frequency Control for Microgrids Against Cyber Attacks[J]. IEEE Transactions on Industrial Informatics, 2022; 18(1): 375-386.

[58]彭华晔, 彭晨, 孙洪涛, 等. 微电网在虚假数据注入攻击下的增量检测机制[J]. 信息与控制, 2019, 48(05): 522-527.

[59]Abhinav S, Modares H, Lewis F, et al. Synchrony in Networked Microgrids under Attacks[J]. IEEE Transactions on Smart Grid, 2017, 9(6): 6731-6741.

[60]]Lian Z, Guo F, Wen C, et al. Distributed Resilient Optimal Current Sharing Control for an Islanded DC Microgrid under DoS Attacks[J]. IEEE Transactions on Smart Grid, 2021, 12 (5): 4494-4505.

[61]Xu G and Ma L. Resilient Self-Triggered Control for Voltage Restoration and Reactive Power Sharing in Islanded Microgrids under Denial-of-Service Attacks[J]. Applied Sciences, 2020, 10(11): 3780-3804.

[62]Ma J, Zhou T and Wang H. Distributed Dynamic Event-Triggered Secondary Control Scheme Based on Sampled-Data for Islanded Microgrids[J]. Journal of Power Electronics, 2024, 25(2): 1-12.

[63]Songlin Hu, Fuyi Yang, Sergey Gorbachev, et al. Resilient Control Design for Networked DC Microgrids under Time-Constrained DoS Attacks[J]. ISA Transactions, 2022, 127: 197-205.

[64]Deng C, Guo F, Wen C, et al. Distributed Resilient Secondary Control for DC Microgrids Against Heterogeneous Communication Delays and DoS Attacks[J] IEEE Transactions on Industrial Electronics, 2022, 69(11): 11560-11568.

[65]Chen X, Hu S, Li Y, et al. Co-Estimation of State and FDI Attacks and Attack Compensation Control for Multi-Area Load Frequency Control Systems under FDI and DoS Attacks[J]. IEEE Transactions on Smart Grid, 2022, 13(3): 2357-2368.

[66]Zhou Q, Shahidehpour M, Alabdulwahab A, et al. Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids[J]. IEEE Transactions on Smart

Grid, 2021, 12(5): 3705-3717.

[67] Cheng Z, Hu S, Yue D, et al. Resilient Distributed Coordination Control of Multiarea Power Systems under Hybrid Attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(1): 7-18.

[68] Hossain M M, Peng C, Sun H T, et al. Bandwidth Allocation-Based Distributed Event-Triggered LFC for Smart Grids under Hybrid Attacks[J]. IEEE Transactions on Smart Grid, 2022, 13(1): 820-830.

[69] Liu X K, Wen C, Xu Q, et al. Resilient Control and Analysis for DC Microgrid System under DoS and Impulsive FDI Attacks[J]. IEEE Transactions on Smart Grid, 2021, 12(5): 3742-3754.

[70] Liu X K, Wang S Q, Chi M, et al. Resilient Secondary Control and Stability Analysis for DC Microgrids under Mixed Cyber Attacks[J]. IEEE Transactions on Industrial Electronics, 2024, 71(2): 1938-1947.

[71] Guo D J, Wang H X, Ge Y, et al. Distributed Hierarchical Resilient Event-Triggering Control for DC Microgrids Under Mixed Cyber Attacks[C]. 2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2), 2023, 2902-2907.

[72] An L and Yang G H. Decentralized Adaptive Fuzzy Secure Control for Nonlinear Uncertain Interconnected Systems Against Intermittent DoS Attacks[J]. IEEE Transactions on Cybernetics, 2019, 49(3): 827-838.

[73] Habibi M R, Sahoo S, Rivera S, et al. Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks[J]. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9(4): 4629-4638.

攻读学位期间发表的学术论文目录

[1] Guo D J, Wang H X, Y. Ge, et al. Distributed Hierarchical Resilient Event-Triggering Control for DC Microgrids Under Mixed Cyber Attacks[C]. 2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2), Hangzhou, China, 2023, 2902-2907.

[2] Guo D J, Sun Y P and Wang D D. Optimization of Time-of-Use Electricity Price of Electric Vehicles Charging Load Based on Spatial-temporal Distribution[C]. 2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2), Hangzhou, China, 2023, 3217-3222.

致谢

时光如梭，在安工程的七年求学时光转瞬即逝。回望论文创作的历程，既有突破难关的喜悦，也有陷入困境的迷茫，而心中最深处满是对师长、同窗及亲友的感恩。值此论文完成之际，谨以最真挚的文字，向所有给予我支持、陪伴与指引的人致以最衷心的感谢。

首先，我要向我的导师葛愿教授致以最诚挚的谢意。在学位论文的撰写过程中，您始终给予我悉心指导和无微不至的支持。您渊博的学识、严谨的治学态度和对科研的热忱始终激励着我。每当我在研究中陷入困惑，您总能耐心为我剖析问题，指引解决方向。在三年的研究生学习中，您不仅传授我专业知识，更培养了我科学的研究思维，教导我如何剖析问题、解决难题，并在探索中持续提升自我。

其次，我要感谢实验室的师兄师姐，同届以及师弟师妹们还有我的室友们。在研究过程中，你们不仅为我提供了宝贵的支持，更在生活与学习中给予我细致的关心。当我在研究中遇到瓶颈时，你们与我共同查阅资料、攻克难关；当我对职业规划感到困惑时，你们为我提供建议；当我在生活中面临挑战时，你们亦给予我支持与帮助。

此外，我要衷心感谢我的家人。在我求学的道路上，你们始终给予我坚定的支持与鼓励。每当我遭遇困难与挫折时，你们总是给予我耐心的安慰与激励。正是你们的理解与包容，让我能够心无旁骛地投身学术研究。家人的无私付出，是我在学术旅程中坚定信念、逐一克服挑战的坚实后盾。

最后，感谢所有在我学术旅程中给予过我帮助的朋友们，感谢你们无私的分享与支持。每一份帮助，都是我成长的动力。在今后的研究和工作中，我将继续努力，不断追求学术的卓越，以回报社会与所有关心与支持我的人。

尚德教学　唯实惟新