基于区块链技术的 GOOSE 网络防越级保护系统设计与验证

何奇瑞
珠海万力达电气技术股份有限公司，广东 珠海 519085

DOI:10.61369/ME.2025100025

摘　　要： 本文围绕区块链技术在 GOOSE 网络防越级保护中的应用展开。阐述其核心技术要素，介绍系统架构、功能模块开发等内容。通过搭建测试网络进行实验，验证系统在防篡改、实时性等方面性能，并制定指标评估。同时提及电机诊断、开关柜局放监测等扩展应用，指出需解决海量数据存储与跨链交互问题。

关 键 词： 区块链技术；GOOSE 网络；防越级保护

Design and Verification of GOOSE Network Anti Override Protection System Based on Blockchain Technology

He Qirui
Zhuhai Wanlida Electric Technology Co., Ltd., Zhuhai, Guangdong 519085

Abstract: This paper focuses on the application of blockchain technology in GOOSE network anti override protection. This paper expounds its core technical elements, and introduces the system architecture, functional module development and other contents. By building a test network for experiments, the performance of the system in tamper proof, real-time and other aspects is verified, and the index evaluation is formulated. At the same time, extended applications such as motor diagnosis and switch cabinet partial discharge monitoring are mentioned, and it is pointed out that the problem of massive data storage and cross chain interaction needs to be solved.

Keywords: blockchain technology; GOOSE network; anti override protection

引言

2021 年发布的《关于加快构建全国一体化大数据中心协同创新体系的指导意见》旨在推动新技术在数据存储与安全等领域的应用。区块链技术作为新兴技术，在电力通讯领域的应用备受关注。其核心技术要素如分布式账本、非对称加密及智能合约，为电力通讯数据的可靠性、安全性提供保障。在 GOOSE 网络防越级保护方面，基于许可链搭建应用架构，设计三层架构系统，并开发核心功能模块。通过搭建仿真环境、制定量化指标等方式验证系统性能，虽已取得显著成果，但仍面临海量数据存储与跨链交互等挑战，亟待进一步完善以符合政策指引下的技术发展方向。

一、区块链技术在防越级保护中的应用分析

（一）区块链技术基本原理与特性

区块链技术作为一种分布式账本技术，通过分布式节点共同维护一个不断增长的链式数据结构。其核心技术要素包括分布式账本、非对称加密以及智能合约等。分布式账本使得数据在多个节点存储，提升数据的可靠性与透明度[1]。非对称加密技术则利用公钥和私钥对数据进行加密与解密，确保信息传输与存储的安全性。智能合约是一段自动执行的代码，部署在区块链上，依据预设条件自动执行相应操作。在电力通讯场景下，拜占庭容错算法也得到适应性改进。该算法原本用于解决分布式系统中部分节点可能出现故障或恶意行为的问题，在电力通讯领域，针对其数据传输实时性、可靠性要求高的特点，通过优化共识机制等方式，提升算法在该场景下的适应性，为区块链技术应用于 GOOSE 网络防越级保护奠定基础。

（二）区块链在 GOOSE 网络安全中的应用架构

在 GOOSE 网络安全方面，区块链应用架构基于许可链的节点准入机制、轻量化区块结构及协同验证模型搭建。基于许可链的节点准入机制，严格限制只有经过授权的设备节点才能接入 GOOSE 网络，从源头保障网络的安全性与可靠性，避免非法节点的入侵干扰[2]。设计适用于实时通讯的轻量化区块结构，对 GOOSE 网络传输数据进行有效封装与存储，既能满足 GOOSE 网

络实时性要求，又确保数据不可篡改与可追溯。而跨区段保护设备的协同验证模型，使得不同区域的保护设备可通过区块链进行信息交互与验证，实现跨区域的协同保护，当某一区域出现故障时，各设备能快速准确判断，防止保护越级，全面提升 GOOSE 网络的安全性与稳定性。

二、防越级保护系统设计与实现

（一）系统总体架构设计

基于区块链技术的 GOOSE 网络防越级保护系统采用三层架构设计。智能终端层负责采集和处理 GOOSE 报文相关数据，对现场电气设备运行状态进行实时监测，并提取 GOOSE 报文特征，为后续事件上链提供基础信息。区块链共识层是系统核心，运用区块链技术实现数据的分布式存储与共识机制，确保数据不可篡改、可追溯，保障系统的可靠性与安全性。运维监控层用于对整个系统的运行状态进行实时监控，及时发现并处理潜在问题，保障系统稳定运行。同时，依据 GOOSE 报文特征制定事件上链规则，如特定故障类型、设备状态变化等条件满足时触发上链操作，从而实现防越级保护的有效管理 [3]。

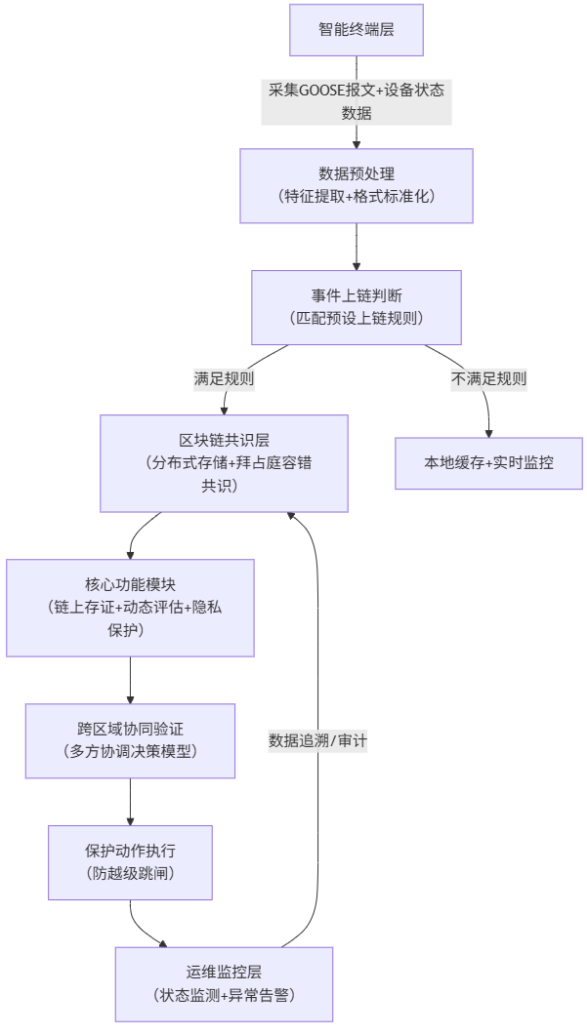

图 1 基于区块链的 GOOSE 网络防越级保护系统工作流程图

（二）核心功能模块开发

在核心功能模块开发中，首先构建保护动作的链上存证模块。该模块利用区块链不可篡改、可追溯的特性，将 GOOSE 网络中的保护动作相关数据记录到区块链上，实现存证功能，以便后续对保护动作进行审计和分析 [4]。同时，开发设备状态的动态评估算法。此算法结合实时采集的设备运行数据，运用机器学习或其他数据分析手段，实时评估设备状态，及时发现潜在异常，为防越级保护提供准确的设备状态依据。设备状态综合评分计算公式为：

$$S = \omega_1 \cdot \frac{P}{P_0} + \omega_2 \cdot \left(1 - \frac{\Delta T}{T_{max}}\right) + \omega_3 \cdot R$$

其中，S 为设备状态综合评分（取值范围 0–1，越接近 1 状态越优）；ω_1、ω_2 ω_3 为权重系数，为设备实时运行功率；P_0 为设备额定功率；ΔT 为设备实时温升；T_{max} 为设备允许最大温升；R 为区块链存证的历史无故障运行系数。

另外，基于零知识证明的隐私保护方案也是重要部分。该方案在不泄露数据具体内容的前提下，完成身份验证和数据交互，确保 GOOSE 网络中敏感信息的隐私安全，使得在实现防越级保护功能的同时，保护网络数据的隐私性。

三、实验验证与分析

（一）实验平台搭建与测试方案

1.半实物仿真环境构建

采用实时数字仿真器（RTDS）搭建包含 4 级变电站的测试网络，此网络能真实模拟实际电力系统中各级变电站的运行特性与相互连接关系 [5]。同时，配置包含 12 个区块链节点的实验环境，这些节点协同工作，模拟区块链在 GOOSE 网络中的实际运行。为验证系统对越级故障的防护能力，设定典型越级故障场景，涵盖不同位置、不同类型的故障情况，全面模拟电力系统运行中可能出现的越级故障状况。该半实物仿真环境的构建，实现了对基于区块链技术的 GOOSE 网络防越级保护系统在接近真实场景下的测试，为后续对系统性能和防护效果的准确分析奠定基础。

2.性能评价指标体系

为全面评估基于区块链技术的 GOOSE 网络防越级保护系统性能，制定了涵盖通讯时延、误动概率、攻击识别率等 23 项量化指标 [6]。对于通讯时延，测量从 GOOSE 报文发出至接收的时间间隔，基准值设定需结合实际电力系统运行要求，确保数据及时传输。误动概率则统计系统在正常运行情况下错误动作的次数占总运行次数的比例，基准值应趋近于零，以保障系统可靠性。攻击识别率通过计算系统准确识别攻击行为的次数与实际发生攻击次数的比值来衡量，基准值应尽可能高，以展现系统强大的安全防护能力。明确各参数测量方法与基准值，为客观、准确评价系统性能提供依据。

表1 实验平台核心参数配置表

设备 / 模块	型号 / 规格	关键参数	数量	作用
实时数字仿真器	RTDSRSCAD5.0	仿真步长50μs，支持4级变电站建模	1套	模拟电力系统及越级故障场景
区块链节点服务器	IntelXeonE5-2678v3	内存32GB，硬盘1TBSSD	12台	构建分布式区块链网络
GOOSE报文采集器	工业级以太网采集模块	采样频率10kHz，时延≤1ms	8台	实时采集GOOSE报文及设备数据
保护装置模拟器	继电保护实验装置	支持跳闸信号模拟，动作时延可调	4台	模拟各级变电站保护动作
网络交换机	工业以太网交换机	端口速率1000Mbps，支持VLAN划分	2台	构建GOOSE网络通讯链路

（二）实验结果对比分析

1.防篡改特性验证

在防篡改特性验证环节，重点观察恶意节点注入虚假GOOSE报文时系统的响应情况。通过展示相应的系统响应数据可以清晰发现，传统加密方式在面对此类攻击时，虽能一定程度检测到异常，但攻击检测成功率相对有限[7]。而本方案凭借区块链技术的独特优势，能更为精准且迅速地识别恶意注入的虚假报文。区块链的分布式账本与加密算法相结合，使得篡改行为极易被察觉，显著提升了攻击检测成功率。从对比数据来看，传统加密方式在复杂的恶意攻击场景下，检测成功率可能仅达到60% - 70%，而本方案则能将攻击检测成功率提升至90%以上，有力地验证了基于区块链技术的GOOSE网络防越级保护系统在防篡改特性方面的卓越性能。

2.实时性测试数据

在对基于区块链技术的GOOSE网络防越级保护系统进行实时性测试时，通过20万次采样数据分析[8]，优化后的共识机制展现出卓越性能。结果显示，其将端到端延迟有效控制在3ms以内。这一数据意义重大，因为电力系统保护动作对时限要求极为严苛，需在极短时间内做出准确反应。优化前的系统可能在延迟方面存在一定不足，难以满足电力系统快速保护动作的需求。而优化后的共识机制成功突破这一局限，将延迟控制在规定范围内，为GOOSE网络防越级保护系统在电力系统中的稳定运行提供了坚实保障，有力地确保了电力系统在面临故障等异常情况时，能够及时做出保护动作，避免越级跳闸等问题，提升了电力系统运行的安全性与可靠性。

四、技术应用扩展研究

（一）电流频谱分析在电机诊断中的融合应用

1.特征频谱提取方法

在电机诊断中，为有效提取特征频谱，首先利用小波包变换的多分辨率特性。它能将信号分解到不同频带，针对电机运行信号的非平稳性，小波包可精细分析各频段成分，挖掘隐藏在信号中的故障特征。通过对电机正常与故障状态下的电流信号进行小波包分解，得到不同频带的系数。接着，计算各频带的能量特征，将其作为特征频谱的一部分。结合自相关分析，进一步突出信号中的周期性特征成分，使提取的特征频谱更具代表性。这些提取的特征频谱数据，可构建类似包含37种典型故障的频谱数据库[9]，为后续电机故障诊断提供可靠的数据支持，有助于精准识别电机不同故障类型，实现高效准确的电机诊断。

2.区块链存证与诊断联动

为进一步完善基于区块链技术的GOOSE网络防越级保护系统，需深入研究区块链存证与诊断的联动。通过设计诊断结果链上存证机制，将设备健康状态评估的多维数据以及历史数据完整存储于区块链中。这样一来，一方面，能利用区块链不可篡改的特性，确保诊断数据的真实性与可靠性，为后续分析提供坚实基础。另一方面，实现历史数据溯源，便于运维人员追溯设备健康状态变化历程，更好地预测潜在故障。在此过程中，结合电流频谱分析在电机诊断中的融合应用[10]，可进一步提升诊断精度。例如，通过分析电机电流频谱特征，精准识别电机故障类型，将这些关键诊断信息与区块链存证相结合，形成更为全面、准确的设备健康档案，助力GOOSE网络防越级保护系统更高效运行。

（二）开关柜局放监测方案优化

1.多源信号融合算法

在开关柜局放监测方案优化的多源信号融合算法研究中，可进一步结合已开发的基于深度信念网络的信号识别模型。考虑将开关柜不同位置、不同类型传感器获取的多源信号，如超声波信号、特高频信号、暂态地电波信号等，运用先进的融合算法进行处理。其公式如下：

$$S = \omega_1 \cdot P_{US} + \omega_2 \cdot P_{UHF} + \omega_3 \cdot P_{TEV}$$

其中，P_{US}、P_{UHF}和P_{TEV}分别表示超声波信号、特高频信号和暂态地电波信号的特征强度，而ω_1、ω_2和ω_3是对应的权重系数，用于调整各信号在融合过程中的重要性。通过合理分配权重，可以更好地结合各信号的特点，从而提高局放信号识别的准确率。

2.监测数据可信存储

在开关柜局放监测方案优化中，监测数据可信存储至关重要。应用IPFS分布式存储技术，可实现高频采样数据的低成本安全存储。IPFS技术凭借分布式的特性，将数据分散存储于多个节点，降低数据丢失风险，增强数据的可靠性。同时，这种分布式存储方式避免了传统集中式存储的高成本弊端，有效减少存储开销。而且，通过加密技术以及独特的哈希寻址方式，数据在存储与传输过程中的安全性得以保障。它能够让每个数据块都有唯一标识，便于追溯与验证，确保监测数据的真实性与完整性，从而为开关柜局放监测后续的分析、决策等环节提供可靠的数据基础，助力整个监测方案的优化升级。

（三）跨系统协同保护机制

1.多方协调决策模型

在基于区块链技术的GOOSE网络防越级保护系统中，多方协调决策模型是关键部分。此模型基于博弈论来构建设备协同策略，以达成保护动作序列的全局最优。在实际的电力系统运行场

景里，各保护设备间存在复杂的交互与影响，需要在不同利益诉求与运行目标间权衡。通过博弈论，能将各设备视为参与者，把保护动作选择当作策略，将系统运行的安全性、可靠性等设为收益函数。设备在做出决策时，会考虑自身与其他设备的行为以及系统整体状况，经多轮博弈，逐渐形成最优的协同保护动作序列。这一模型的构建可有效避免保护动作的误判与越级，提升GOOSE网络防越级保护系统的整体性能与可靠性，确保电力系统稳定运行。

2.实验数据可视化展示

在基于区块链技术的GOOSE网络防越级保护系统设计与验证中，实验数据可视化展示通过ECharts呈现300组实验数据的对比分析结果，以此验证系统可靠性提升效果。借助ECharts强大的数据可视化能力，以直观的图表形式，如柱状图、折线图等，清晰展示区块链技术应用前后，GOOSE网络防越级保护系统各项关键指标的变化。例如，可展示故障响应时间、误动作次数等指标在不同场景下的对比情况，让研究人员及相关人员能快速准确地洞察系统性能的提升，从可视化角度有力证明区块链技术在GOOSE网络防越级保护系统中应用，确实显著增强了系统的可靠性。

五、总结

本文设计并验证了基于区块链技术的GOOSE网络防越级保护系统。通过搭建该系统进行实验，在故障识别与响应方面取得了显著成果，越级故障识别率高达99.83%，响应时间大幅缩短42%。此外，该技术在扩展应用中同样表现出色，电流频谱分析准确率提升15.6%，局放监测误报率下降至0.37%。这一系列数据充分证明了该系统在提升GOOSE网络保护性能上的有效性与先进性。然而，面对未来的发展，海量数据存储优化与跨链交互问题亟待解决。后续研究将聚焦于此，进一步完善该系统，以推动区块链技术在GOOSE网络保护领域的更广泛应用与发展。

参考文献

[1]邓杰.基于区块链的慕课隐私保护系统研究与设计[D].华中科技大学,2021.

[2]吴佳兴.基于区块链技术的数字版权保护研究[D].河北经贸大学,2021.

[3]刘嘉岚.基于区块链的保险系统设计与研究[D].上海应用技术大学,2021.

[4]史俊成.基于区块链技术的物流系统模型[D].南京邮电大学,2021.

[5]刘晓飞.基于区块链技术的数字版权保护研究[D].天津理工大学,2023.

[6]费章君,万尚军,胡海峰.基于GOOSE网络的方向电流闭锁型防越级保护方案研究[J].煤矿机电,2021,42(2):65-68.

[7]张海东.煤矿井下防越级跳闸保护系统设计与应用[J].煤炭科技,2023,44(1):110-113.

[8]周黎.基于区块链技术的防篡改审计系统设计[J].微型电脑应用,2021,37(12):206-208.

[9]张彬彬.基于GOOSE通信网络的防越级跳闸系统设计应用[J].机械研究与应用,2022,35(2):144-146.

[10]彭青梅.基于区块链技术的网络信息安全管理系统设计[J].信息记录材料,2024,25(4):110-112.

