第 51 卷 第 10 期：5090-5102 高电压技术 Vol.51, No.10: 5090-5102
2025 年 10 月 31 日 High Voltage Engineering October 31, 2025
DOI: 10.13336/j.1003-6520.hve.20250062

考虑灵活密钥资源调配和故障维修协同的量子电力通信网络快速恢复方法

钱雨琦，谢海鹏，钟　剑
（西安交通大学电气工程学院，西安 710049）

摘　要：量子密钥分发(quantum key distribution，QKD)技术能够有效满足新型电力系统不断增长的信息安全需求，其技术发展日趋成熟。然而，当前研究对基于 QKD 的量子电力通信网络弹性关注不足，尤其在 QKD 网络故障后的量子密钥供应恢复方面缺乏系统研究。该文通过挖掘量子设备生成密钥资源的灵活性，结合配电网信息流重构与通信元件修复过程，提出了一种协同灵活资源调配和故障维修的量子电力通信网络快速恢复方法。首先，构建了融合物理与辅助量子链路的弹性量子电力通信网络架构，刻画考虑灵活资源参与的弹性量子电力通信网恢复过程；其次，提出了以最大化量子通信恢复价值为目标的混合整数线性规划模型：在利用无人机调配密钥资源快速恢复关键业务的同时协同优化维修人员修复元件顺序，逐步恢复网络的量子密钥供应能力；最后，在改进的 IEEE 33 节点配电系统中验证了所提方法的有效性，算例结果表明充分利用密钥资源的灵活性及两种恢复手段的互补性，可显著提高量子电力通信网络的灾后恢复效率，并有效降低配电网失负荷风险。

关键词：量子密钥分发；灵活资源；配电网弹性；信息安全；灾后恢复

Rapid Recovery Method for Quantum Power Communication Networks Considering the Coordination of Flexible Key Resource Allocation and Fault Repair

QIAN Yuqi, XIE Haipeng, ZHONG Jian
(School of Electrical Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: Quantum key distribution (QKD) technology can effectively meet the growing information security demands of modern power systems, and its technical development is becoming increasingly mature. However, current research lacks sufficient focus on the resilience of QKD-based quantum power communication networks, especially in terms of systematic studies on the recovery of quantum key supply after QKD network failures. This paper proposes a rapid recovery method for quantum power communication networks that integrates flexible resource allocation with fault repair. First, a resilient quantum power communication network architecture is constructed, incorporating both physical and auxiliary quantum links, to characterize the recovery process of the resilient quantum power communication network involving flexible resources. Second, a mixed-integer linear programming (MILP) model is proposed with the objective of maximizing the recovery value of quantum communication, namely, critical services are rapidly restored by utilizing drones to deploy key resources while simultaneously optimizing the repair sequence of maintenance personnel to gradually recover the quantum key supply capability of the network. Finally, the effectiveness of the proposed method is validated using a modified IEEE 33-bus distribution system. The case study results demonstrate that fully utilizing the flexibility of key resources and the complementarity of the two recovery approaches can significantly enhance the post-disaster recovery efficiency of quantum power communication networks and effectively reduce the risk of load loss in power systems.

Key words: quantum key distribution (QKD); flexible resources; distribution network resilience; information security; post-disaster recovery

0　引言

随着新型电力系统的快速发展，电力通信网络已成为现代电力系统中不可或缺的核心组成部分，承担着关键控制信息和数据的传输任务[1-3]。然而，随着电力通信网络复杂性和信息化程度的提升，系统面临的网络安全威胁也日益严峻。一方面，电动汽车、分布式电源、虚拟电厂等智能化主体的广泛

基金资助项目：国家重点研发计划(2021YFB2401300)。
Project supported by National Key R&D Program of China (2021YFB2401300).

应用，导致电力系统中点对点通信业务的快速增长，从而加大了网络信息泄露风险[4-5]；另一方面，随着高效解密算法[6-8]以及协同信息攻击[9-10]等复杂攻击手段的出现，传统加密算法的安全性遭遇前所未有的挑战。特别是在量子计算技术的冲击下，基于计算复杂度的传统加密算法(如 RSA 等)安全性大幅降低，对电力通信网络安全构成极大威胁。因此，为有效应对这些新型网络攻击和信息安全风险，减小通信网络故障对电力系统的影响，确保电力系统的安全与稳定，迫切需要引入先进的通信加密技术，以提升电力通信系统的安全防护能力。

量子通信作为一种能够实现安全信息传输并完善现有加密体系的技术手段，正逐步在电力系统中试点应用并取得了积极的应用成效。通过结合量子力学原理与密码学加密方法，量子通信能够依赖量子力学的基本特性保障信息传输在物理层面上的无条件安全[11]。其中，量子密钥分发(quantum key distribution，QKD)技术作为当前最成熟、应用最广泛的量子通信形式，能够在发送方和接收方之间建立绝对安全的密钥对[12]。目前，已有若干学术研究和实践探索将 QKD 技术应用于电力系统中并取得良好效果。美国石溪大学的 P. Zhang 教授建立了基于 QKD 的量子安全微电网[13]；美国橡树岭国家实验室则在智能电网数控系统中开展了基于 QKD 的安全认证实验[14]。国家电网公司和南方电网公司近年来也逐步加快了量子通信建设的步伐，在北京、安徽、浙江等地建立了一系列量子电力通信示范项目，面向调度控制、状态感知和综合能源系统等多个场景开展基于 QKD 技术的量子通信应用探索[15-17]，验证了 QKD 技术在电力系统中的可行性。

然而，QKD 系统在实际应用中仍面临诸多挑战，特别是在工程实施过程中其脆弱性不可忽视。量子信道中的光信号对环境扰动、光纤非线性效应以及窄带噪声等物理攻击高度敏感[18-19]。攻击者可以通过注入窄带噪声或利用光纤旁路注入干扰信号，故意降低量子比特的信噪比，从而影响密钥生成过程[20-22]。一旦 QKD 系统遭遇破坏，失去量子密钥的安全保护，电力通信业务将直接暴露在各种攻击威胁下。攻击者可通过窃听、虚假数据注入(fault data injection，FDI)、伪装第三方等手段窃取或篡改传输的信息，进而引发用户信息泄露、交易数据篡改等安全事件。更为严重的是，攻击还可能通过干扰电力系统的调度与控制信息，直接造成电力负荷失调，甚至导致大规模停电，进而带来巨大的经济损失和社会影响。因此，如何在 QKD 系统遭遇攻击或设备故障后迅速恢复其密钥分发能力，并缩短通信业务暴露于潜在攻击的时间窗口，已成为提升电力系统量子安全性及信息安全韧性的关键问题。

目前围绕 QKD 系统的研究大多集中在灾前的规划和资源调度方面[23-25]，关于 QKD 系统在遭遇攻击或设备故障后的恢复研究相对较少。现有恢复方法主要包括基于重路由的资源分配和依赖人工的设备修复两种。基于重路由的资源分配策略[26-28]通过在故障发生后调整路由方案，重新分配未受故障影响的通信资源(如带宽、频段)，以满足部分业务的通信需求。这种方法在一定程度上具有灵活性，能够短期内缓解灾后通信压力，减少系统损失。然而，在量子电力通信系统中，由于电力通信网络的固定拓扑结构以及量子设备高昂的安装成本，安全通信路径通常是预先设定且固定的，这使得在故障场景中灵活调整路径变得困难。因此，该策略在实际应用中的效果受到较大限制。传统的修复手段则依赖现场维修人员对受损设备或通信线路进行直接修复[29-30]。这种方法虽然能够彻底恢复通信功能，但由于需要派遣人员到现场、诊断故障并完成修复，整个过程耗时较长。在突发事件中，修复时间过长可能导致关键业务在故障期间失去安全保护，从而对电网的信息安全带来严重隐患。因此，亟需提出一种能够有效适应量子通信结构特性、灵活保障关键业务通信安全的快速恢复方法，从而增强量子电力通信网的弹性，全面提升电力系统的安全性与可靠性。

为解决上述问题，本文提出了一种基于无人机与维修人员综合调度的量子电力通信网络快速恢复方法。本文的主要贡献如下：

1）提出了一种基于物理和辅助量子链路的电力量子通信网络架构。在正常运行时，通过光纤信道建立物理量子链路生成量子密钥；在物理链路发生故障时，通过链路两端节点的量子密钥池构建辅助量子链路。该架构能够提高量子设备利用效率并增强网络应对设备故障和信息攻击时的恢复能力。

2）构建了以最大化量子通信恢复价值为目标的量子电力通信网络恢复模型，旨在最小化重要电力业务失去量子通信保护时间。通过求解该优化模型，生成考虑电力业务信息流动态重构过程的量子电力通信网快速恢复策略：一方面，利用无人机灵

活调配系统中的可用密钥资源，构建辅助量子链路以快速恢复部分关键业务的量子安全通信；另一方面，优化维修人员对受损元件维修的调派顺序，逐步恢复网络的量子密钥生成能力。通过无人机调派与维修人员协同调派，为量子通信网络提供快速高效的恢复方案。

3）通过改进的 IEEE 33 节点系统中验证了所提方法的有效性。仿真结果表明，该方法能够显著缩短信息攻击后量子安全通信中断时间，增强量子电力通信网络的恢复能力，为关键电力业务信息的安全保障提供了有效支撑。

1 含灵活密钥资源的弹性量子电力通信网

1.1 基于中继的量子保密通信过程

量子保密通信的安全性源于量子叠加和纠缠特性所衍生的量子力学基本原理。测量塌缩理论表明，对系统的测量会破坏量子态；海森堡测不准原理则指出，量子系统的对偶性质无法同时被精确测量。因此，任何窃听行为都会扰动量子态，导致通信双方的测量出现误差，从而使窃听者无法在不被察觉的情况下窃取信息。此外，量子不可克隆原理确保了量子信息无法被未经授权的第三方准确复制。

基于 QKD 的量子保密通信包括密钥生成和密文传递两个阶段，涉及经典和量子两条信道。量子信道与经典信道可以通过波分复用方式在光纤中共存[31]，无需额外铺设新的设备，在电力系统中具备良好的应用基础。在密钥生成阶段，通过量子信道传输量子态信息、经典信道传输测量信息，通信双方可以生成安全的量子密钥对并存储。在密文传递阶段，发信方利用所获的量子密钥对传输信息明文进行加密，并通过经典信道将密文传递至收信方；收信方随后利用相应的量子密钥将收到的密文解密，完成密文传递，从而实现量子保密通信。

由于 QKD 的密钥生成率与信息传输距离成反比，直接在电力用户之间建立量子通信链路的密钥生成率较低，无法满足电力业务的加密需求。因此，需采用中继方案构建量子电力通信网。基于中继的 QKD 量子保密通信的具体流程如图 1 所示。

在基于中继的 QKD 方案中，中继节点 TR 的接收设备与发信方 A 的发射端相连，发射端与收信方 B 的接收端相连，从而分别与通信双方建立量子链接，并生成密钥 K_{AT} 和 K_{TB}。随后，中继节点对这两组密钥进行异或操作，即计算 $K_{AT}\oplus K_{TB}$，并将结果发送给收信方 B。收信方 B 再对其存储的密钥 K_{TB} 与 $K_{AT}\oplus K_{TB}$ 进行异或处理，得到$(K_{AT}\oplus K_{TB})\oplus K_{TB}=K_{AT}$。通过上述对量子信号的收发机制和对密钥的异或操作，发信方与收信方之间通过终结点成功共享一组量子密钥对 K_{AT}。目前这种基于中继的光纤 QKD 方案已经在京沪量子保密通信干线等典型量子通信网络中投入实际工程应用。

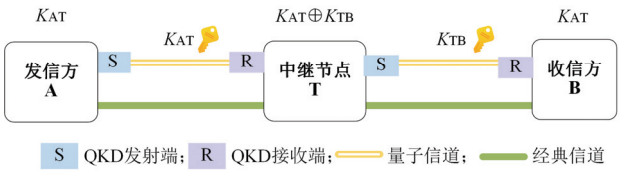


图 1 基于中继的 QKD 量子保密通信过程

Fig.1 Relay-based QKD secure communication process

1.2 考虑密钥池的灵活密钥资源生成与网络弹性提升

1.2.1 量子电力通信网中的灵活密钥资源

密钥池是量子通信系统中的关键设备，用于存储并管理 QKD 模块生成的量子密钥。在当前的量子系统中，密钥池通常用于储存相邻节点之间冗余的量子密钥，以便在实时密钥生成速率不足时进行补充，从而缓解密钥生成速率低的瓶颈问题。然而，在电力通信系统的背景下，由于地理跨度大、业务流量高，密钥生成速率通常较低，且通信业务消耗量大，因此相邻节点间的冗余密钥资源十分有限。多数情况下，电力通信网络依赖于实时生成并消耗密钥资源。

QKD 模块通常具备多个固定端口，能够建立多条量子链路。然而，由于电力通信网络结构的限制，每个节点与相邻节点的光纤连接已经确定，这使得部分节点的 QKD 模块存在冗余端口，未能充分发挥其密钥生成能力。此外，在新型电力系统中，电力业务种类繁多，信息流分布广泛，每个电力用户都可能充当双向信息流的中继节点。因此，每个节点的 QKD 模块通常都具备接收端和发射端设备。在这种情况下，具备冗余收发设备的节点能够使用 QKD 模块在日常运行时可以通过建立自发自收的量子链路生成安全密钥对，并将其储存在本节点中，作为备用量子密钥，为应急通信提供备用资源。在上述备用资源节点中，备用密钥待需要时通过移动载体将其传送至目标节点，辅助建立安全通信路径。

本文所提的灵活资源指的是上述过程中由节点 QKD 模块的冗余端口生成，并在节点密钥池中

成对储存、可通过移动载体快速分配的量子密钥。这些灵活密钥资源主要用于量子电力通信网络的应急快速恢复。通过密钥资源的灵活调派，不仅能够提高量子设备的利用率，还能提升量子链路的快速故障恢复能力，增强网络的抗攻击能力，从而提高量子电力通信网络的整体弹性。

值得注意的是，量子密钥的安全性随着时间推移而逐渐降低[32]。尽管量子密钥的生成过程具备固有的安全性，但一旦密钥生成后，它仍然面临潜在的恶意攻击风险，特别是在存储和分发至用户之前。因此，必须实施额外的安全防护措施，确保密钥在其生命周期内始终保持安全性。为了降低潜在的安全漏洞，应定期重新生成并储存新的量子密钥，从而确保备用密钥资源的持续有效性和安全性。

1.2.2　基于灵活密钥资源的量子电力通信网恢复示例

量子电力通信网络通过 QKD 技术生成量子密钥作为核心可用资源，并由此构建两类功能互补的量子链路，实现电力通信主体之间的安全通信。两种量子链路的特点如表 1 所示。

其中，物理量子链路依托相邻节点间的 QKD 设备进行，通过光纤中的量子信道传输量子态，并结合经典信道完成信息协商，生成的密钥对分别储存于通信双方，直接用于高实时性电力业务的加密通信。辅助量子链路则突破传统双节点限制，通过节点内部冗余的 QKD 端口进行自发自收，即在同一节点内完成量子信号的发射与接收，生成密钥对并预先存储于本地密钥池。当物理链路因故障中断时，这些预存密钥可通过移动载体快速分发至目标节点，在无需重建物理通道的条件下恢复安全通信。这两类链路在 QKD 技术的支撑下形成协同机制：物理链路保障日常业务的安全实时运行，辅助链路则通过密钥备用与灵活调度，快速实现灾后应急量子通信重构，从而形成具备攻击抵御能力的弹性量子电力通信网络。

考虑灵活密钥资源参与构建辅助量子链路的弹性量子电力通信网灾后恢复过程如图 2 所示。

假设网络在失效前存在一个安全通信请求(节点 1 与节点 3 之间的请求，速率为 20 kb/s)。故障发生时刻，量子信道 1-2 和 2-3 断开，由于没有其他可用路径，节点对之间的量子安全信息流终端。在恢复阶段，维修人员前往故障元件处进行维修。在时刻 1，维修人员前往链路(1-2)被修复，建立起物理量子链路生成量子密钥；而无人机前往资源节点

表 1　两种量子链路的特性分析

Table 1　Characteristics of two types of quantum links

链路类型	密钥来源	建立方式	应用场景	特性
物理链路	相邻节点间实时生成	光纤信道	日常运行	高可靠、低延迟
辅助链路	节点预先生成后分配	移动载体	灾后恢复	灵活性、时空解耦

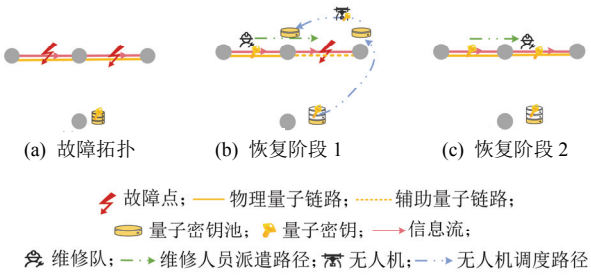


图 2　弹性量子电力通信网的灾后恢复过程

Fig.2　Post-disaster recovery process of the resilient quantum power communication network

4 充注密钥对并分别前往节点 2、节点 3 将密钥对分别分配给向节点密钥池，形成辅助链路。此刻节点 1 与节点 3 之间形成了一条物理链路与辅助链路组成的完整量子通信路径，故量子信息流重新流通，节点 1 和 3 的负荷恢复安全防护。但是此时链路 2-3 仍处于故障状态，只能消耗充注密钥临时恢复通信，如果密钥消耗完，辅助链路就会再次断开在时刻 2，维修人员继续元件修复工作，移动到节点 3 处进行修复，只有当两端节点设备和中间信道都恢复可用，比如此处的节点 2、节点 3 和链路 2-3 都可用，才能重新建立起物理量子链路，恢复网络的密钥生成能力元件维修完毕、全部故障处都重新建立起量子连接，重新恢复密钥生成，利用光纤建立起的量子链路生成密钥并实时分配给加密电力业务。

上述过程表明，考虑灵活密钥资源以建立辅助链路能够加速 QKD 网络的恢复过程。因此，将其纳入恢复序列，对恢复方案进行综合规划，可以有效降低攻击对电力通信业务的影响，确保关键负荷业务的安全性。

1.3　量子电力通信网中的网络攻击及其影响分析

量子电力通信网在信息化程度逐渐提升的新型电力系统中承担着对关键业务的通信安全保障，面临日益增长的物理攻击和信息攻击威胁。随着电力系统中新兴业务类型的逐渐增多[33](如分布式电源接入、负荷聚合、电动汽车充放电管理等)，对量

子电力通信网的网络攻击对电力系统的潜在影响变得更加复杂与严重。一方面，攻击能够从局部节点扩展至关键业务链条，例如针对分布式电源控制系统的攻击可能导致电源调节能力失效，进而引发区域电网的大规模供电中断甚至系统崩溃；另一方面，由于新型电力系统中多种业务类型高度耦合，攻击的连锁反应更加显著，例如在大规模可再生能源并网的场景下，攻击可能扰乱功率预测和调度，导致电力供应波动、负荷分配失衡，甚至引发系统级电网瘫痪。此外，攻击还可能显著延长多业务场景的恢复时间，进一步加剧对电网稳定运行的冲击。

1.3.1 物理攻击方式及其影响

量子信号相较于经典信号更加脆弱，易受外界干扰或破坏。尤其是当系统需要实时传输调度控制指令时，这将直接影响电力用户的信息安全和电网的稳定运行。以下两种物理攻击形式会造成量子密钥无法生成。

1）频段干扰：通过对量子信号频段进行噪声注入，阻断量子链路的建立，量子通信网络无法生成密钥。

2）设备破坏：直接破坏 QKD 模块使得节点的密钥生成能力完全丧失，进而影响所有相邻量子链路的建立。

1.3.2 信息攻击方式及其影响

信息攻击主要利用量子通信网络的逻辑漏洞，通过操纵数据流量或资源分配来削弱系统运行的稳定性。

1）拒绝服务攻击(denial of service, DoS)：通过伪造大量虚假业务请求，迅速耗尽量子密钥资源，使真实业务无法获得足够的密钥保护。

2）误码率提升：如果量子链路的误码率异常升高并超出设定阈值，通信双方会丢弃这部分无法用作密钥生成的量子数据，导致系统无可用安全密钥。

3）密钥资源窃取与篡改：通过新能源场站或第三方云平台的接入路径，窃取量子密钥资源或伪造密钥分发协议，造成电网业务节点通信失真。

综上所述，新型电力系统中的量子电力通信网中面临的攻击威胁更加多样化，且影响不再局限于单一业务节点，直接威胁电力侧稳定运行，让节点面临失负荷风险。因此，必须在遭受攻击后快速恢复量子电力通信网的安全通信支撑能力。

2 基于无人机和维修人员协同调配的量子电力通信网快速恢复策略

2.1 问题描述

建立量子电力通信网络 $G(V, E)$，其中 V 代表电力用户节点，承载不同的电力业务并具有对应的通信需求；E表示通信链路。在量子网络遭受攻击后，部分节点间的通信可能失去量子密钥的保护，从而使电力业务中的节点信息或控制指令面临被黑客窃取或篡改的风险。这种情况可能进一步导致节点失去负荷，从而威胁电力系统的稳定运行。因此，迅速恢复量子网络的密钥供应至关重要。

无人机与维修人员在通信网络恢复过程中各具优势。传统的通信网络修复方式主要依赖维修人员进行现场作业，如量子设备和光纤更换。然而，该过程受到地理环境及维修流程复杂性的限制，往往需要较长时间，难以满足突发情况下对通信的即时恢复需求。相比之下，无人机凭借高效的飞行能力和灵活的部署特性，在通信网络恢复中展现出显著优势。故障发生后，无人机能够迅速响应，快速抵达受损区域并调配密钥资源形成临时通信链路，从而在短时间内恢复安全通信，有效弥补传统维修方式的不足。因此，在通信网络的恢复过程中，无人机与维修人员协同配合，形成互补。无人机承担短期应急响应任务，而维修人员则负责网络密钥生成能力的恢复，两者共同作用保障量子电力通信网的全面恢复与稳定运行。

在网络因攻击而失效的瞬间，业务节点间可优先利用现有密钥池中的储备资源。然而，由于电网内不同节点之间的物理距离较远，密钥生成速率在满足电力业务需求后，剩余的可存储资源非常有限，仅能支持极短时间内的量子安全通信。因此，本方案在原有密钥资源耗尽后，启动恢复策略，具体措施包括：1）利用无人机的快速响应能力恢复关键故障链路，从可用资源节点充注并分发灵活密钥密钥至受影响的故障节点，建立辅助链路以维持一定时间的安全通信；2）派遣维修人员修复故障元件以恢复量子密钥持续生成，通过派遣维修人员修复受损设备或通信链路，重新利用光纤建立物理量子链路，逐步恢复网络正常的密钥生成能力，最终实现量子电力通信网的全面恢复。

由于每个时刻维修资源(包括灵活密钥资源、无人机和维修人员)有限，无法同时完成所有故障元件

的修复，因此量子电力网络在遭受攻击后的修复需要逐步推进。该过程需协同考虑上述两种恢复手段，优化元件修复计划，以最大限度地减少量子网络攻击对电力业务的影响，尽可能保障负荷节点的安全，从而确保电力系统的稳定运行。

2.2　目标函数

本文考虑在信息攻击下最小化系统失负荷风险，即以最大化受到量子密钥保护的安全负荷量为目标函数，其具体形式为：

$$\max \sum_{t\in T}\sum_{r\in R}\sum_{i\in V}\lambda_{i,t}^{r}\omega_i P_i \tag{1}$$

式中：T 为时刻组成的集合，为预计所有故障元件维修完成的时长；R 为电力业务集合，包括通信始末节点以及业务流量需求；$\lambda_{i,t}^{r}$ 为 t 时刻以节点 i 为始末节点的电力业务 r 是否受到量子密钥保护 0-1 决策变量，为 1 表示至少有一条量子信道构成的通信路径；ω_i 为节点 i 处负荷的重要程度；P_i 为节点 i 处的负荷量。

2.3　基于无人机的量子密钥快速调度

无人机飞行速度快、部署灵活，目前在电力系统的巡检与应急通信中已经取得广泛应用[34-36]。作为量子密钥移动储存介质的量子 U 盾体积小、重量轻，能够直接利用电力系统中已经部署的无人机进行运输[37-38]。一旦发生故障，无人机携带量子 U 盾去资源节点充注密钥，再分发至故障信道两端节点建立辅助量子链路，实现量子资源的快速响应。两端节点在注入密钥后通过经典信道传输量子加密后的业务信息，在充注密钥耗尽之间维持临时连接，减少安全通信中断的时间，从而减少节点失负荷的风险。

无人机从基站出发，作为灵活调配系统中可用量子资源的手段，飞行路径受到路径部署、飞行时间和量子密钥资源的约束。考虑到无人机续航能力，设置每个机巢覆盖一定范围，将整个系统划分为多个区域。若系统中包括 χ 个故障，其中故障光纤为 χ_{L}，故障光纤对应的故障节点为 χ_{LN}。使用 V_{FD}^{k} 代表区域 k 中无人机的部署点集合，包括 χ 个故障节点 χ_{LN}、ϕ 个具备可用资源节点以及 1 个无人机基站(机巢)，即 $V_{\mathrm{FD}}^{k}=V_{\chi_{\mathrm{LN}}}^{k}\cup V_{\phi}^{k}\cup V_{\mathrm{ds}}^{k}$。

2.3.1　路径选择约束

$$h_{i,i}^{m}=0,\forall i\in V_{\mathrm{FD}}^{k},m\in N_m \tag{2}$$

$$v_i^{\mathrm{S},m}=\sum_{j\in V_{FD}^{k}}h_{i,j}^{m},\forall i\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{3}$$

$$v_i^{\mathrm{D},m}=\sum_{j\in V_{FD}^{k}}h_{j,i}^{m},\forall i\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{4}$$

$$\sum_{m\in N_m}v_i^{\mathrm{S},m}=\sum_{m\in N_m}v_i^{\mathrm{D},m}=1,\forall i\in V_{\chi_{\mathrm{LN}}}^{k}\cup V_{\mathrm{ds}}^{k},\forall m\in N_m \tag{5}$$

$$\sum_{m\in N_m}v_i^{\mathrm{S},m}=\sum_{m\in N_m}v_i^{\mathrm{D},m}\le 1,\forall i\in V_{\phi}^{k},\forall m\in N_m \tag{6}$$

式中：$h_{i,j}^{m}$ 为 0-1 变量，表示无人机 m 是否选择了从节点 i 到节点 j 的路径，1 代表该路径被选择，0 代表未被选择；$v_i^{\mathrm{S},m}$ 和 $v_i^{\mathrm{D},m}$ 为 0-1 变量，表示无人机 m 是否选择离开和到达节点 i；$v_i^{\mathrm{S},m}$ 取值为 1、0 分别表示无人机 m 部署路径中包含、不包含节点 i 为起点的路径；$v_i^{\mathrm{D},m}$ 取值为 1、0 分别表示无人机 m 部署路径中包含、不包含节点 i 为终点的路径；N_m 为无人机集合。

式(2)表示不存在从自身出发回到自身的路径，避免自环；式(3)—(4)表示 $v_i^{\mathrm{S},m}$ 和 $v_i^{\mathrm{D},m}$ 与 $h_{i,j}^{m}$ 的关系；式(5)表示无人机在故障点和基站存在一次到达和离开的过程，即无人机从起降点出发经过所有故障点后回到起降点；式(6)表示无人机在资源点的到达次数等于离开次数，且可能不经过某些资源点。

2.3.2　飞行时间约束

$$0\le t_i^{\mathrm{S},m}\le Mv_i^{\mathrm{S},m},\forall i\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{7}$$

$$0\le t_i^{\mathrm{D},m}\le Mv_i^{\mathrm{D},m},\forall i\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{8}$$

$$t_{V_{\mathrm{ds}}}^{\mathrm{S},m}=1,\forall m\in N_m \tag{9}$$

$$t_j^{\mathrm{D},m}\ge t_i^{\mathrm{S},m}+D_{ij}^{m}T^{\mathrm{tr},m}-M(1-h_{i,j}^{m}),\forall i,j\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{10}$$

$$t_j^{\mathrm{D},m}\le t_i^{\mathrm{S},m}+D_{ij}^{m}T^{\mathrm{tr},m}+M(1-h_{i,j}^{m}),\forall i,j\in V_{\mathrm{FD}}^{k},\forall m\in N_m \tag{11}$$

$$t_i^{\mathrm{S},m}\ge t_i^{\mathrm{D},m}+T^{\mathrm{op},m}-M(1-v_i^{\mathrm{S},m}),\ \forall i\in V_{\chi_{\mathrm{LN}}}^{k}\cup V_{\phi}^{k},\forall m\in N_m \tag{12}$$

$$t_i^{\mathrm{S},m}\le t_i^{\mathrm{D},m}+T^{\mathrm{op},m}+M(1-v_i^{\mathrm{S},m}),\ \forall i\in V_{\chi_{\mathrm{LN}}}^{k}\cup V_{\phi}^{k},\forall m\in N_m \tag{13}$$

式中：$t_i^{\mathrm{S},m}$ 和 $t_i^{\mathrm{D},m}$ 为连续变量，分别表示无人机 m 从节点 i 出发和到达时间；M 为一个大数常量；D_{ij}^{m} 为节点 i、j 之间的无人机飞行距离；$T^{\mathrm{tr},m}$ 为无人机每公里飞行耗时；$T^{\mathrm{op},m}$ 为无人机在节点进行密钥充放操作的耗时。

式(7)、(8)表示只有选定的节点才存在无人机的出发和到达时间；式(9)表示无人机从基站出发的初始时间为 1；式(10)、(11)表示无人机到达节点 j 的时间等于从节点 i 出发的时间加上飞行过程所耗时长；式(12)、(13)表示无人机从节点 i 出发的时间等于到达节点 i 的时间加上在节点进行量子密钥充放操作所耗时长。

2.3.3 量子密钥资源约束

$$0 \le k_i^{\mathrm{S},m} \le Q_{\max}^m v_i^{\mathrm{S},m}, \forall i \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{14}$$

$$0 \le k_i^{\mathrm{D},m} \le Q_{\max}^m v_i^{\mathrm{D},m}, \forall i \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{15}$$

$$k_{V_{\mathrm{ds}}}^{\mathrm{S},m} = 0, \forall m \in N_m \tag{16}$$

$$0 \le \sum_{m \in N_m} Q_i^{\mathrm{dis},m} \le Q_{i,\max}, \forall i \in V_{\chi_{\mathrm{LN}}}^k, \forall m \in N_m \tag{17}$$

$$0 \le \sum_{m \in N_m} Q_i^{\mathrm{fill},m} \le Q_{i,\mathrm{P}}, \forall i \in V_\phi \tag{18}$$

$$k_i^{\mathrm{S},m} = k_i^{\mathrm{D},m} + (Q_i^{\mathrm{fill},m} - Q_i^{\mathrm{dis},m}) v_i^{\mathrm{S},m}, \quad \forall i \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{19}$$

$$k_j^{\mathrm{D},m} \ge k_i^{\mathrm{S},m} - M(1 - h_{i,j}^m), \forall i,j \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{20}$$

$$k_j^{\mathrm{D},m} \le k_i^{\mathrm{S},m} + M(1 - h_{i,j}^m), \forall i,j \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{21}$$

$$k_i^{\mathrm{S},m} \ge Q_j^{\mathrm{dis},m} - M(1 - h_{i,j}^m), \forall i,j \in V_{\mathrm{FD}}^k, \forall m \in N_m \tag{22}$$

式中：$k_i^{\mathrm{S},m}$ 和 $k_i^{\mathrm{D},m}$ 为连续变量，分别表示无人机 m 从节点 i 出发和到达时携带的量子密钥数；$Q_{\max}^m$ 为无人机 m 携带密钥的容量上限；$Q_i^{\mathrm{dis},m}$ 为无人机 m 分配给节点 i 的密钥量；$Q_i^{\mathrm{fill},m}$ 为无人机 m 从节点 i 充注的密钥量；$Q_{i,\max}$ 为节点密钥储存的容量上限；$Q_{i,\mathrm{p}}$ 为故障发生时节点 i 密钥池中储存的可用密钥数。

式(14)、(15)表示只有选定的节点才存在无人机出发和到达时的密钥量；式(16)表示无人机从基站出发时初始密钥量为 0；式(17)表示无人机分配给故障点的密钥必须满足节点密钥储存容量约束；式(18)表示无人机从资源点充注的密钥量小于节点密钥池中的可用密钥量；式(19)表示无人机在节点 i 处密钥数量的变化；式(20)、(21)表示无人机从节点 i 移动到节点 j 时，无人机上的密钥数没有变化；式(22)表示只有无人机在节点 i 时有足够分配给节点 j 的量子才会移动。

2.3.4 故障元件状态约束

在无人机灵活调度资源的过程中，各故障链路的状态为：

$$t_l^m = \max(t_i^{\mathrm{S},m}, t_j^{\mathrm{S},m}), \forall i,j \in V_{\chi_{\mathrm{LN}}}, \forall l \in V_{\chi_{\mathrm{L}}}, \forall m \in N_m \tag{23}$$

$$\sum_{t \in T} \tau_{l,t} = 1, \forall i \in V_{\chi_{\mathrm{LN}}} \tag{24}$$

$$\sum_{t \in T} t\tau_{l,t} \ge \sum_{m \in N_m} t_l^m, \forall i,j \in V_{\chi_{\mathrm{LN}}}, \forall l \in V_{\chi_{\mathrm{L}}} \tag{25}$$

$$\sum_{t \in T} t\tau_{l,t} \le \sum_{m \in N_m} t_l^m + 1 - \varepsilon, \forall i,j \in V_{\chi_{\mathrm{LN}}}, \forall l \in V_{\chi_{\mathrm{L}}} \tag{26}$$

$$w_{l,t} = \sum_{t \in T} t\tau_{l,t}, \forall l \in V_{\chi_{\mathrm{L}}} \tag{27}$$

式中：t_l^m 为故障链路 l 的恢复时间；$\tau_{l,t}$ 为 0-1 变量，用于表征故障链路 l 在 t 时刻的恢复状态；ε 为一个小数常量；$w_{l,t}$ 为 0-1 变量，用于表征故障链路 l 上在 t 时刻是否由无人机建立起了量子链路。

式(23)表示只有链路两端的节点都充注了密钥，故障链路才能恢复；式(24)—(27)用于确定故障链路 l 上临时量子链路的可用状态。

2.4 维修人员派遣

在维修资源有限的条件下，需要制定合理的维修计划调度维修人员，实现通信恢复的价值最大化。维修人员需要到达现场修复损坏的 QKD 设备或光纤，逐步恢复物理量子链路的正常密钥生成能力。由于人工修复过程较久，且受到故障地理位置和天气条件等因素的制约，维修人员主要作用于量子通信网络中密钥能力的恢复，确保系统能够持续生成量子密钥并恢复长期安全通信。随着量子信道故障的逐步恢复，网络中的信道可用状态发生改变，需要对拓扑进行及时更新。因此，本文采取信息流重构与故障维修动态配合的策略，结合维修进度及时调整信息流分布。V_{FC} 为故障元件(光纤和节点)和维修站组成的集合，即 $V_{\mathrm{FC}}=V_\chi \cup V_{\mathrm{cs}}$。

2.4.1 路径选择约束

$$g_{i,i}^c = 0, \forall i \in V_{\mathrm{FC}}, c \in N_c \tag{28}$$

$$y_i^{\mathrm{S},m} = \sum_{j \in V_{\mathrm{FC}} \setminus \{i\}} g_{i,j}^c, \forall i \in V_{\mathrm{FC}}, \forall c \in N_c \tag{29}$$

$$y_i^{\mathrm{D},c} = \sum_{j \in V_{\mathrm{FC}} \setminus \{i\}} g_{j,i}^c, \forall i \in V_{\mathrm{FC}}, \forall c \in N_c \tag{30}$$

$$\sum_{c \in N_c} y_i^{\mathrm{S},c} = \sum_{c \in N_c} y_i^{\mathrm{D},c} = 1, \forall i \in V_{\mathrm{FC}}, \forall c \in N_c \tag{31}$$

式中：$g_{i,j}^c$ 为 0-1 变量，表示维修队 c 是否选择了从节点 i 到节点 j 的路径，1 代表该路径被选择，0 代表未被选择；$y_i^{\mathrm{S},c}$ 和 $y_i^{\mathrm{D},c}$ 为 0-1 变量，分别表示维修队 c 是否选择离开或到达节点 i；N_c 为维修队集合。

式(28)表示不存在从自身出发回到自身的路径，避免自环；式(29)—(31)表示每个故障元件都有一个维修队维修一次，并且维修队在修复完所有故障元件后回到维修站。

2.4.2 维修时间约束

$$0 \le t_i^{\mathrm{S},c} \le M y_i^{\mathrm{S},c}, \forall i \in V_{\mathrm{FC}}, \forall c \in N_c \tag{32}$$

$$0 \le t_i^{\mathrm{D},c} \le M y_i^{\mathrm{D},c}, \forall i \in V_{\mathrm{FC}}, \forall c \in N_c \tag{33}$$

$$t_{V_{\mathrm{cs}}}^{\mathrm{S},c} = 1, \forall c \in N_c \tag{34}$$

$$t_j^{\mathrm{D},c} \ge t_i^{\mathrm{S},c} + D_{ij}^c T^{\mathrm{tr},c} - M(1 - g_{i,j}^c), \quad \forall i,j \in V_{\mathrm{FC}}, \forall c \in N_c \tag{35}$$

$$t_j^{\mathrm{D},c} \le t_i^{\mathrm{S},c} + D_{ij}^c T^{\mathrm{tr},c} + M(1 - g_{i,j}^c), \quad \forall i,j \in V_{\mathrm{FC}}, \forall c \in N_c \tag{36}$$

$$t_i^{\mathrm{S},c} \ge t_i^{\mathrm{D},c} + T^{\mathrm{re},c} - M(1 - y_i^{\mathrm{S},c}), \quad \forall i \in V_{\mathrm{FC}} \setminus V_{\mathrm{cs}}, \forall c \in N_c \tag{37}$$

$$t_i^{\mathrm{S},c} \le t_i^{\mathrm{D},c} + T^{\mathrm{re},c} + M(1 - y_i^{\mathrm{S},c}), \quad \forall i \in V_{\mathrm{FC}} \setminus V_{\mathrm{cs}}, \forall c \in N_c \tag{38}$$

式中：$t_i^{\mathrm{S},c}$ 和 $t_i^{\mathrm{D},c}$ 为连续变量，分别表示维修队 c 从节点 i 出发和到达时间；D_{ij}^c 为节点 i、j 之间的维修人员行进距离；$T^{\mathrm{tr},c}$ 为维修队每公里行进耗时；$T^{\mathrm{re},c}$ 为维修队修复故障元件的耗时。

式(32)、(33)表示维修队经过节点才有离开和到达时间；式(34)表示无人机从基站出发的初始时间为 1；式(35)、(36)表示维修队到达节点 j 的时间等于从节点 i 出发的时间加上飞行过程所耗时长；式(37)、(38)表示维修队从节点 i 出发的时间等于到达节点 i 的时间加上在节点进行维修操作所耗时长。

2.4.3　故障元件状态约束

在维修队维修过程中，故障元件的状态如下：

$$\sum_{t\in T}\sigma_{i,t}=1,\forall i\in V_{\chi} \tag{39}$$

$$\sum_{t\in T}t\sigma_{i,t}\geq\sum_{c\in N_c}t_i^c,\forall i\in V_{\chi} \tag{40}$$

$$\sum_{t\in T}t\sigma_{i,t}\leq\sum_{c\in N_c}t_i^c+1-\varepsilon,\forall i\in V_{\chi} \tag{41}$$

$$s_{i,t}=\sum_{t\in T}t\sigma_{i,t},\forall i\in V_{\chi_{\mathrm{LN}}} \tag{42}$$

$$s_{l,t}=\sum_{t\in T}t\sigma_{i,t},\forall l\in V_{\chi_{\mathrm{L}}} \tag{43}$$

式中：t_i^c 为故障元件 i 的恢复时间；$\sigma_{i,t}$ 为 0-1 变量，用于表征故障元件 i 在 t 时刻的恢复状态；$s_{i,t}$、$s_{l,t}$ 为 0-1 变量，分别用于表征故障节点 i 和故障链路 l 在 t 时刻是否被维修人员修复。

式(39)表示故障元件状态变化的时刻，呈现阶跃特性；式(40)—(43)用于确定故障节点 i 和故障链路 l 的可用状态。

2.5　量子加密信息流重构过程

综合考虑无人机灵活密钥资源调度行为、维修人员维修行为以及量子电力通信网实时的网络重路由行为，则量子加密信息流约束表述如下：

$$\sum_{j\in V}x_{ij,t}^r-\sum_{j\in V}x_{ji,t}^r=\begin{cases}1-\eta_t^{1,r}, & i=V_{\mathrm{s}}^r\\ -1+\eta_t^{1,r}, & i=V_{\mathrm{d}}^r\\ 0, & \text{其他}\end{cases},\forall r\in R,t\in T \tag{44}$$

$$\lambda_{i,t}^r\leq(1-\eta_t^{1,r})(1-\eta_t^{2,r}),\forall i\in V_{\mathrm{s}}^r\cup V_{\mathrm{d}}^r,\forall r\in R \tag{45}$$

$$x_{ij,t}^r=q_{ij,t}^r\vee p_{ij,t}^r,\forall i,j\in V,r\in R,t\in T \tag{46}$$

$$p_{ij,t}^r\leq w_{l,t} \tag{47}$$

$$\sum_{t\in T}\sum_{r\in R}F^r(p_{ij,t}^r+p_{ji,t}^r)\leq\sum_{m\in N_m}Q_i^{\mathrm{dis},m},\forall i\in V_{\chi_{\mathrm{LN}}} \tag{48}$$

$$q_{ij,t}^r\leq s_{l,t}\cdot s_{i,t}\cdot s_{j,t} \tag{49}$$

$$\sum_{j\in V}\sum_{r\in R}q_{ij,t}^r\leq O_{\max},\forall i\in V \tag{50}$$

$$\sum_{r\in R}F^r\cdot(q_{ij,t}^r+q_{ji,t}^r)\leq\gamma_l(l),\forall i,j\in V,\forall l(i,j)\in L \tag{51}$$

式中：$x_{ij,t}^r$ 为量子信道(i,j)上通信业务 r 信息流动方向的状态变量，若信息由节点 i 流向节点 j，则 $x_{ij,t}^r=1$，若信息由节点 j 流向节点 i，则 $x_{ji,t}^r=1$；$\eta_t^{1,r}$、$\eta_t^{2,r}$ 为引入的松弛 0-1 变量；V_{s}^r 为通信业务 r 的起点；V_{d}^r 为通信业务 r 的终点；$p_{ij,t}^r$ 为无人机调配量子密钥资源形成的临时量子信道；F^r 为通信业务 r 的流量速率；$q_{ij,t}^r$ 为维修人员维修完成后通过光纤建立的物理量子信道；$O_{\max}$ 为量子节点量子端口的数量；$\gamma_l(l)$ 为光纤信道的量子密钥生成率，与信道长度成反比，具体计算过程和参数见附录 A。

式(44)表示通信节点对之间信息流平衡，如果节点 i 是通信节点对 r 的起始点，那么信息流之差为 1，意味着信息从节点 i 流出；如果节点 i 是通信节点对 r 的终点，那么信息流之差为−1，意味着信息从节点 i 流出；对于中继节点，流入等于流出；式(45)为表示通信节点对之间是否存在可行量子信道路径的 0-1；式(46)表示通过光纤建立的物理链路或者通过无人机分发密钥资源建立的辅助链路都可以作为量子信道支撑量子安全通信；式(47)表示临时量子连接受到无人机修复故障链路状态的约束；式(48)表示恢复过程中临时量子链路上通信业务 r 流量消耗量总和小于节点被分配的量子密钥数；式(49)表示物理量子连接受到维修队修复故障链路和链路两端故障节点状态的约束；式(50)表示节点建立起的物理连接小于节点的端口数；式(51)表示信息传输物理量子链路上所有电力业务的信息流量总和小于链路上的密钥生成速率。由于在密钥生成阶段所占用的带宽相较于电力光纤的总带宽极小，不会成为主要限制，因此不考虑密钥生成时量子信道和经典信道占用的带宽。

2.6　线性化处理

本文提出的量子电力通信网灾后快速恢复模型是一个非线性混合整数模型(mixed-integer programming，MIP)，传统的方法难以求解，因此对模型中非线性部分做线性化处理。

采用线性方法[39]、Big-M 方法[40-41]和 McCormick 方法[42]将非线性约束式(19)、(23)、(45)和(49)转化为线性形式。其中，式(19)包含两个双线性项之差，因此引入辅助变量 $z_i^{\mathrm{fill},m}$、$z_i^{\mathrm{dis},m}$ 分别表示这两个双线性项，并通过 McCormick 松弛进行线性化处理，从而将其转化为线性约束；式(23)引入

一个大数 M，通过 Big-M 方法将取最大值的操作转换为一系列线性不等式；z_l为辅助变量；式(45)和(49)分别是两个和 3 个二元变量的乘积，因此分别引入 z_t^r 和 $z_{l,i,j,t}^r$ 辅助变量并添加相关约束将乘积项转化为线性形式。线性化后得到的约束如下：

$$\begin{cases} z_i^{\mathrm{fill},m} \le M v_i^{\mathrm{S},m}, z_i^{\mathrm{dis},m} \le M v_i^{\mathrm{S},m} \\ z_i^{\mathrm{fill},m} \le Q_i^{\mathrm{fill},m}, z_i^{\mathrm{dis},m} \le Q_i^{\mathrm{dis},m} \\ z_i^{\mathrm{fill},m} \ge Q_i^{\mathrm{fill},m} - M(1-v_i^{\mathrm{S},m}) \\ z_i^{\mathrm{dis},m} \ge Q_i^{\mathrm{dis},m} - M(1-v_i^{\mathrm{S},m}) \\ z_i^{\mathrm{fill},m} \ge 0, z_i^{\mathrm{dis},m} \ge 0 \end{cases} \tag{52}$$

$$k_i^{\mathrm{S},m} = k_i^{\mathrm{D},m} + z_i^{\mathrm{fill},m} - z_i^{\mathrm{dis},m} \tag{53}$$

$$\begin{cases} t_l^m \ge t_i^{\mathrm{D},m} \\ t_l^m \ge t_j^{\mathrm{D},m} \\ t_l^m \le t_i^{\mathrm{D},m} + M z_l \\ t_l^m \le t_i^{\mathrm{D},m} + M(1-z_l) \end{cases} \tag{54}$$

$$\begin{cases} z_t^r \le 1-\eta_t^{1,r} \\ z_t^r \le 1-\eta_t^{2,r} \\ z_t^r \ge (1-\eta_t^{1,r}) + (1-\eta_t^{2,r}) - 1 \end{cases} \tag{55}$$

$$0 \le \lambda_{i,t}^r \le z_t^r \tag{56}$$

$$\begin{cases} z_{l,i,j,t}^r \le s_{l,t} \\ z_{l,i,j,t}^r \le s_{i,t} \\ z_{l,i,j,t}^r \le s_{j,t} \\ z_{l,i,j,t}^r \ge s_{l,t} + s_{i,t} + s_{j,t} - 2 \end{cases} \tag{57}$$

$$q_{ij,t}^r \le z_{l,i,j,t}^r \tag{58}$$

以上目标函数和约束条件，共同组成了线性化处理后的基于无人机灵活资源和维修人员综合调度的量子电力通信网快速恢复模型。该模型为混合整数线性规划问题(mixed-integer linear programming, MILP)，利用商业求解器进行求解可得到最优的综合恢复策略。

3 算例分析

3.1 算例说明

为验证本文所提出的灾后量子电力通信综合恢复策略的有效性，本文基于图 3 所示改进 IEEE 33 节点配电网进行仿真验证[43]。本文测试算例在 MATLAB2024b 中建立模型。采用 YALMIP 工具箱集合 Gurobi11.0.1 求解器对模型进行求解。

由于电力通信专网中光纤与电力线路具有一一对应关系[44-45]，且本文采用了基于光纤介质的 QKD 方案，因此本算例中参考电力网络设置对应通

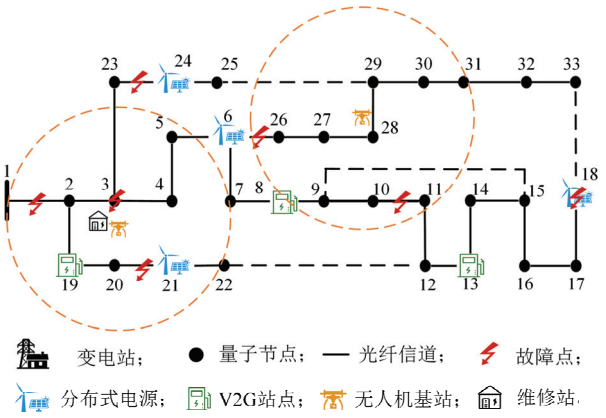


图 3 改进 IEEE 33 节点系统示意图

Fig.3 Diagram of modified IEEE 33-bus system

信网络拓扑，每条光纤容量为 1 Gb/s。该算例设定配电网控制中心位于母线 1 处。配电网中包含 4 个分布式电源，分别位于母线 6、18、21 和 24；3 个电动汽车充电站，分别位于母线 8、13 和 19。设定配电网一、二、三级负荷的权重系数分别为 1.0、0.4 与 0.2[46]。配电网母线节点坐标与节点负载、负载比例权重系数均在附录 B1、B2 表格分别所示。所有节点均装设一组收发 QKD 设备，能够发送和接收量子信号。因此，用户既可以作为发信方或收信方，也可以作为中继节点，成为量子安全通信路径的一部分。其中，节点 1 由于同时负责和上级电网之间的连接，故不做本配电网系统中的备用资源点。对于剩余节点，不与其他节点建立量子信道的空闲 QKD 设备端口通过 2 m 光纤连接，密钥生成率为 372.64 kb/s，在设备运行期间持续生成备用量子密钥资源，每两小时更新一次，节点密钥储存容量为 1 GB。

该算例中，配电网中配置 2 个无人机基站和 1 个维修站。考虑到无人机的电池续航限制，每个无人机基站以 30 km 的范围覆盖线路，每条线路只有两端节点都在覆盖范围内才算被无人机区域覆盖，每条线路最多只被一个无人机区域包含，形成了两块独立区域。无人机基站和维修站的具体信息见附录表 B3。每个基站包含 1 架无人机，无人机飞行速度为 80 km/h，在节点进行量子密钥充放操作耗时为 5 min。无人机携带的量子 U 盾密钥储存容量为 512 MB。故障点维修站包含 2 支维修队，分别从维修站出发并维修好所有的故障元件后返回站点。维修队的移动速度为 50 km/h，单个故障元件的维修时间为 45 min。无人机的移动路径根据不同地点(包

含故障点和基站)之间的最短直线距离进行设置[34]，以确保快速、高效的响应；而维修队的移动路径则沿电力网络拓扑设置[47]，以确保维修工作能够覆盖到电网中的关键节点，并与电力设施保持一致，从而提高修复工作的有效性和系统的整体恢复效率。

由于分布式发电、电动汽车充电站和主动负荷的接入，配电网中存在传统电力业务和新兴业务，产生了多组点对点的安全通信需求。本算例考虑控制中心和分布式发电之间的调度控制、主动负荷节点参与的能量交易以及电动汽车相关业务(vehicle-to-grid，V2G)，根据不同节点类型构建配电网中电力通信需求场景，给出了各通信节点对之间的电力业务流量的估计值[48]，具体业务通信需求设置见附录表 B4，通信需求均采用一次一密模式，即消耗的量子密钥数等于业务流量。

假设遭遇网络攻击后，系统中光纤(1-2)、(6-26)、(10-11)、(20-21)、(23-24)和节点 3、18 故障，失去量子密钥生成能力。具体的故障位置见附录表 B5。

3.2　结果分析

为说明灵活调度密钥资源以及无人机和维修人员协同优化对于量子电力通信网恢复的影响，本节采用 3 种不同方案恢复网络攻击场景下配电网中的量子安全负荷并对其效果进行对比分析，具体如下所述。

1）方案 1：仅派遣维修人员前往故障点修复故障元件，负荷在承载对应电力业务的路径上所有元件修好后恢复安全。

2）方案 2：分别调度无人机并派遣维修人员，即两种恢复手段之间不进行协同优化。负荷可通过建立起的辅助链路和物理链路恢复安全通信。

3）方案 3：采用本文所提恢复方法进行综合调度，即无人机灵活资源调度和维修人员故障维修协调配合以实现量子电力通信网快速恢复。

3.2.1　各方案恢复效果对比

该子算例对上述 3 中方案进行对比实验，结果如图 4 所示。

在量子网络受到攻击后，多处量子信道和量子节点出现故障，量子链路中断，电力业务缺乏密钥供给，导致对应的电力负荷失去安全保护。仅有部分电力业务通过重构，由未中断的量子链路支撑，整个系统处于严重的信息安全风险之中。

通过对比量子安全恢复负荷曲线可知：方案 2 和方案 3 通过调配系统中的密钥资源能够在前期显

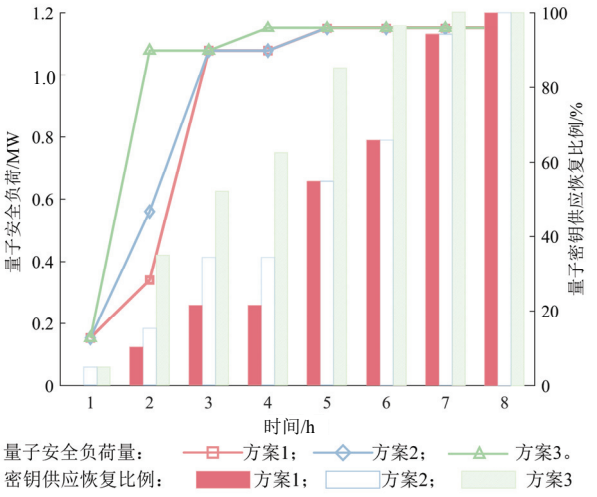


图 4　3 种方案的量子安全负荷和密钥供应能力对比

Fig.4　Comparison of quantum-safe load recovery and quantum key supply capability of three schemes

著提升负荷恢复速度，这是因为无人机作为运输载体能快速调配可用灵活资源，在故障信道两端充注密钥，从而建立辅助链路恢复量子链路，使得更多业务能够通过重构信息流恢复安全通信。方案 3 相比方案 2 具有更高的负荷恢复量，表明协同优化无人机和维修人员能够进一步提升系统恢复效果。一方面，若无人机和维修人员独立调度，无人机会选择历经多个资源点以提升分发给故障节点的密钥数量，从而延长辅助链路的支撑时间，这导致其到达故障节点并恢复安全通信的时间延后；另一方面，恢复目标促使无人机和维修人员优先处理承载关键电力业务的故障点，其部署路径存在较大重叠。在这种情况下，维修人员到达故障点进行修复工作的时刻与无人机完成密钥充注的时刻接近，导致辅助链路的支撑作用无法充分发挥。通过有序协同优化无人机和维修人员，可调整故障元件的优先级顺序，推迟对已建立辅助链路的故障信道的维修，又能在无人机建立辅助链路失效之前完成维修任务。这样不仅能够充分发挥辅助链路的作用，还能在同一时刻建立更多的量子链路，提升恢复资源的利用率。

通过对比量子密钥供应恢复比例可知：在恢复初期，无人机运输的灵活资源是密钥供应恢复的主要来源。然而，由于备用资源节点的量子密钥数量有限，这些资源无法长期维持并满足电力业务实时通信的安全需求，因此系统的密钥供应能力没有大幅提升。随着故障节点和信道的修复，网络中的物理量子链路重新建立并逐步恢复密钥供应能力。这

表明两种恢复手段具有互补性：无人机调度灵活资源速度快，但所能承载的安全负荷量较少；故障维修速度慢，但能够恢复密钥生成能力以承载较多的安全负荷。需要注意的是，尽管前期的恢复已能够支撑大部分电力业务，但若不继续维修故障元件，辅助链路的密钥耗尽后，电力负荷将再次失去安全保障。因此，前期灵活资源的快速响应与后期故障维修的稳步推进相结合，才能实现系统全面恢复。

模型求解用时方面，方案 1 模型求解耗时 98.32 s，方案 2 模型求解耗时 279.25 s，方案 3 模型求解耗时 401.95 s。方案 3 中更多的变量和约束条件导致模型求解时间增加，但提升了模型针对量子电力通信网灾后恢复问题的适用性，使得负荷在网络攻击下能更加快速的恢复安全通信和量子密钥供应。此外，方案计算时长与故障发生后数小时的恢复周期相比较短，故认为其满足恢复决策的时限要求。

上述结果表明：通过考虑无人机的快速响应能力，能够在维修人员抵达并完成故障修复之前显著缩短关键电力业务失保护时长，充分挖掘了系统中灵活资源的弹性潜力；通过无人机和维修人员协同调度，能够调整元件维修计划以优化网络恢复的整体表现。方案 3 中，量子电力通信网的总恢复时间和风险负荷量均有所降低，验证了所提方案的有效性。

3.2.2 方案 3 结果分析

该子算例对于方案 3 系统资源调度和逐步恢复情况进行展示。图 5 展示了在网络故障发生后本文所提方案与不考虑协同方案的元件维修计划。

区域 1 的无人机基站覆盖故障线路 1-2 和 20-21，区域 2 的无人机基站覆盖故障线路 10-11。在故障发生后，区域 1 的无人机从基站出发，路径为 DS1-20-2-1。无人机首先从覆盖范围内的资源节点 20 充注密钥后，依次前往节点 2 和节点 1 进行分配，临时建立量子链路 1-2。整个过程耗时 48 min，快速恢复了链路 1-2 的量子安全通信。区域 2 的无人机则沿路径 DS2-11-10 行动。由于故障线路 10-11 两侧的节点储备了足够的密钥资源，无人机直接从节点 11 取密钥运往节点 10，整个过程耗时 25 min，快速建立了临时链路 10-11 的量子通信能力。维修人员在无人机建立起临时链路后分别于 109 min 和 237 min 到达故障线路 1-2 和 10-11 处，并完成设备修复，恢复了量子链路的密钥生成能力。在此期间，灵活资源的调度确保临时量子链路的持续运行。相比不协同调度的方案，该方案优先利用临时链路支撑通信，因此能够推迟对某些线路的维修。然而，灵活量子密钥资源是有限的，如果链路承载的电力业务对信息流至关重要，则必须在密钥耗尽、链接可能再次中断之前完成修复，以保障重要业务的稳定运行。对于故障线路 20-21，由于无人机完成对线路 1-2 的密钥分配后密钥资源不足，需前往其他资源点补充密钥，再到达线路 20-21 的时间已较晚。与此同时，维修队在故障发生后 105 min 已抵达并完成修复，因此无人机未参与恢复线路 20-21。

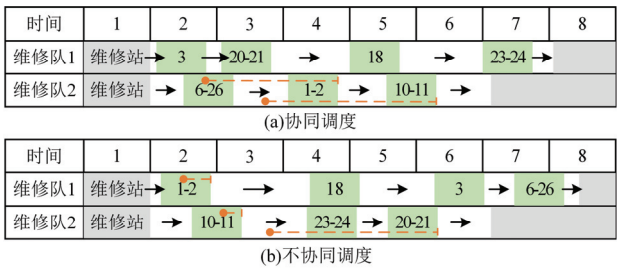


图 5 网络攻击后元件维修计划

Fig.5 Post-cyberattack component repair plan

综上所述，本文提出的综合无人机灵活调度与维修人员派遣的方案，充分利用了两种恢复手段的协同优势，发挥了系统中资源节点生成备用密钥的价值，能够在灾后快速恢复电力业务的安全通信，有效提升系统的恢复效率与可靠性。

4 结论

本文提出了一种考虑灵活密钥资源调配与故障维修协同的量子电力通信网络快速恢复方法。该方法通过协同调度无人机与维修人员实施故障恢复，旨在提升灾后量子密钥供应的恢复效率和网络弹性。研究结果验证了该方法在灾后恢复中的有效性，并为新型电力系统中量子技术的实际应用提供了参考。主要结论如下：

1）构建融合物理链路与辅助链路的网络架构能够提高量子设备利用效率，增强量子电力通信网络在设备故障和信息攻击下的恢复能力。

2）利用无人机灵活调配系统中的可用密钥资源，能够构建辅助量子链路以快速恢复部分关键业务的量子安全通信；而优化维修人员对受损元件的维修顺序，能够逐步恢复网络的量子密钥供给能力。

3）协同调派无人机与维修人员能够显著缩短信息攻击后量子安全通信中断时间，增强量子电力通信网络的恢复能力，为保障电力信息安全提供有

效支撑。

此外，本文没有考虑故障元件修复过程受交通状况、维修时长不确定性等因素的影响。后续可综合考虑上述因素，并通过启发式算法进一步研究分析，以增强该方法在更大规模电网应用中的鲁棒性和适用性。

附录见本刊网络版(http://hve.epri.sgcc.com.cn)。

参考文献　References

[1] 赵俊华，文福拴，薛禹胜，等. 电力 CPS 的架构及其实现技术与挑战[J]. 电力系统自动化，2010，34(16)：1-7.
ZHAO Junhua, WEN Fushuan, XUE Yusheng, et al. Cyber physical power systems: architecture, implementation techniques and challenges[J]. Automation of Electric Power Systems, 2010, 34(16): 1-7.

[2] 江秀臣，许永鹏，李曜丞，等. 新型电力系统背景下的输变电数字化转型[J]. 高电压技术，2022，48(1)：1-10.
JIANG Xiuchen, XU Yongpeng, LI Yaocheng, et al. Digitalization transformation of power transmission and transformation under the background of new power system[J]. High Voltage Engineering, 2022, 48(1): 1-10.

[3] 盛戈皞，钱　勇，罗林根，等. 面向新型电力系统的数字化电力设备关键技术及其发展趋势[J]. 高电压技术，2023，49(5)：1765-1778.
SHENG Gehao, QIAN Yong, LUO Lin'gen, et al. Key technologies and development trends of digital power equipment for new type power system[J]. High Voltage Engineering, 2023, 49(5): 1765-1778.

[4] 杨　挺，翟　峰，赵英杰，等. 泛在电力物联网释义与研究展望[J]. 电力系统自动化，2019，43(13)：9-20，53.
YANG Ting, ZHAI Feng, ZHAO Yingjie, et al. Explanation and prospect of ubiquitous electric power internet of things[J]. Automation of Electric Power Systems, 2019, 43(13): 9-20, 53.

[5] 盛万兴，刘科研，李　昭，等. 新型配电系统形态演化与安全高效运行方法综述[J]. 高电压技术，2024，50(1)：1-18.
SHENG Wanxing, LIU Keyan, LI Zhao, et al. Review of basic theory and methods of morphological evolution and safe & efficient operation of new distribution system[J]. High Voltage Engineering, 2024, 50(1): 1-18.

[6] BOYER M, BRASSARD G, HØYER P, et al. Tight bounds on quantum searching[J]. Fortschritte Der Physik, 1998, 46(4/5): 493-505.

[7] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, USA: IEEE, 1994: 124-134.

[8] HARROW A W, HASSIDIM A, LLOYD S. Quantum algorithm for linear systems of equations[J]. Physical Review Letters, 2009, 103(15): 150502.

[9] 刘　念，余星火，张建华. 网络协同攻击：乌克兰停电事件的推演与启示[J]. 电力系统自动化，2016，40(6)：144-147.
LIU Nian, YU Xinghuo, ZHANG Jianhua. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147.

[10] 汤　奕，陈　倩，李梦雅，等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化，2016，40(17)：59-69.
TANG Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(17): 59-69.

[11] BENENTI G, CASATI G, STRINI G. Principles of quantum computation and information[M]. Hackensack, USA: World Scientific, 2004.

[12] LO H K, CHAU H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[13] TANG Z F, QIN Y Y, JIANG Z M, et al. Quantum-secure microgrid[J]. IEEE Transactions on Power Systems, 2021, 36(2): 1250-1263.

[14] Trustworthy cyber infrastructure for the power grid[EB/OL]. [2022-10-03]. http://www.tcipg.org/about-us. html.

[15] 冯　宝，李国春，俞学豪，等. 量子保密通信电网应用情况及研究进展[J]. 信息通信技术与政策，2021，47(7)：39-45.
FENG Bao, LI Guochun, YU Xuehao, et al. Application and research progress of quantum secure communication in power grid[J]. Information and Communications Technology and Policy, 2021, 47(7): 39-45.

[16] 郝国文，徐　青，杨烨，等. 基于网络水印技术的水电智能终端安全通信方法研究［J］. 电力信息与通信技术，2024，22(6)：52-58.
HAO Guowen, XU Qing, YANG Ye, et al. Research on secure communication for intelligent terminals in hydropower plant aided by network watermark［J］. Electric Power Information and Communication Technology, 2024, 22(6): 52-58.

[17] 闫龙川，陈智雨，俞学豪，等. 基于量子密钥分发的新型城镇电力业务安全交互架构[J]. 电力系统自动化，2020，44(8)：28-35.
YAN Longchuan, CHEN Zhiyu, YU Xuehao, et al. Security interaction framework for electricity service in new-type town based on quantum key distribution[J]. Automation of Electric Power Systems, 2020, 44(8): 28-35.

[18] SHARMA V. Effect of noise on practical quantum communication systems[J]. Defence Science Journal, 2016, 66(2): 186.

[19] 马国明，王思涵，张晓星，等. 变电设备状态信息光纤/光学传感研究[J]. 高电压技术，2024，50(8)：3354-3386.
MA Guoming, WANG Sihan, ZHANG Xiaoxing, et al. Research on optical fiber/optical sensing for state information of transformer equipment[J]. High Voltage Engineering, 2024, 50(8): 3354-3386.

[20] SATOH T, NAGAYAMA S, SUZUKI S, et al. Attacking the quantum internet[J]. IEEE Transactions on Quantum Engineering, 2021, 2: 4102617.

[21] BOUCHARD F, ENGLAND D, BUSTARD P J, et al. Achieving ultimate noise tolerance in quantum communication[EB/OL]. (2021-02-09)[2024-11-18]. http: //arxiv. org/abs/2102.05098.

[22] PONOSOVA A, RUZHITSKAYA D, CHAIWONGKHOT P, et al. Protecting fiber-optic quantum key distribution sources against light-injection attacks[J]. PRX Quantum, 2022, 3(4): 040307.

[23] JABIR M V, ANNAFIANTO N F R, BURENKOV I A, et al. Energy and bandwidth efficiency optimization of quantum-enabled optical communication channels[J]. Npj Quantum Information, 2022, 8(1): 63.

[24] YAN R D, WANG Y, DAI J H, et al. Quantum-key-distribution-based microgrid control for cybersecurity enhancement[J]. IEEE Transactions on Industry Applications, 2022, 58(3): 3076-3086.

[25] ZHAO Y L, CAO Y, WANG W, et al. Resource allocation in optical networks secured by quantum key distribution[J]. IEEE Communications Magazine, 2018, 56(8): 130-137.

[26] ZHU Q C, ZHAO Y L, YU X S, et al. Collaborative resilience in hybrid quantum-classical networks[C]//2022 IEEE 14th International Conference on Advanced Infocomm Technology (ICAIT). Chongqing, China: IEEE, 2022: 116-119.

[27] YANG L, ZHAO Y M, XU H L, et al. Dynamic entanglement routing based on stream processing for quantum networks[J]. IEEE Transactions on Networking, 2025, 33(1): 382-397.

[28] ALSHOWKAN M, LUKENS J M, LU H H, et al. Resilient entanglement distribution in a multihop quantum network[EB/OL]. (2024-07-29)[2024-11-18]. http://arxiv.org/abs/2407.20443.

[29] LI M Y, ZHANG Q L, GATTO A, et al. DRL-based progressive recovery for quantum-key-distribution networks[J]. Journal of Optical Communications and Networking, 2024, 16(9): E36-E47.

[30] 徐 岩，郭佳睿，马天祥. 考虑韧性提升的配电网故障恢复与抢修协调优化[J]. 高电压技术，2024，50(12)：5516-5528.
XU Yan, GUO Jiarui, MA Tianxiang. Coordinated optimization of fault recovery and emergency repair for distribution network considering resilience improvement[J]. High Voltage Engineering, 2024, 50(12): 5516-5528.

[31] PATEL K A, DYNES J F, CHOI I, et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber[J]. Physical Review X, 2012, 2(4): 041010.

[32] PIRONIO S, MASANES L, LEVERRIER A, et al. Security of device-independent quantum key distribution in the bounded-quantum-storage model[J]. Physical Review X, 2013, 3(3): 031007.

[33] 刘丽军，陈 昌，胡 鑫，等. 基于“车-路-站-网”信息耦合的电动汽车有序充电策略[J]. 高电压技术，2024，50(2)：693-703.
LIU Lijun, CHEN Chang, HU Xin, et al. Ordered charging strategy for electric vehicles based on the information coupling of vehicle-road-station-grid[J]. High Voltage Engineering, 2024, 50(2): 693-703.

[34] 刘瑞环，陈 晨，叶志刚，等. 基于无人机应急通信的配电网灾后信息物理协同恢复策略[J]. 电网技术，2023，47(3)：1218-1229.
LIU Ruihuan, CHEN Chen, YE Zhigang, et al. Cooperative cyber-physical distribution system restoration with UAV-based emergency communication UAV after disasters[J]. Power System Technology, 2023, 47(3): 1218-1229.

[35] 钟 剑，陈 晨，张昊辰，等. 极端天气下配电网信息物理耦合故障快速恢复策略[J/OL]. 电力系统自动化，1-23[2025-09-03]. https://link. cnki. net/urlid/32.1180. tp. 20241008.1649.004.
ZHONG Jian, CHEN Chen, ZHANG Haochen, et al. Rapid restoration strategy for cyber-physical integrated failures in distribution systems under extreme weather conditions[J/OL]. Automation of Electric Power Systems, 1-23[2025-09-03]. https://link.cnki.net/urlid/32.1180.tp.20241008.1649.004.

[36] 蔡焕青，付 晶，杨 宁，等. 500 kV 变电站无人机巡检作业安全距离[J]. 高电压技术，2024，50(7)：3199-3208.
CAI Huanqing, FU Jing, YANG Ning, et al. Safe distance of inspection operation by unmanned aerial vehicles in 500 kV substation[J]. High Voltage Engineering, 2024, 50(7): 3199-3208.

[37] 深圳市大疆创新科技有限公司. 大疆创新[EB/OL]. [2025-02-07]. https://www. dji. com/.
Shenzhen DJI Innovations Technology Co., Ltd. DJI innovations[EB/OL].[2025-02-07]. Available: https://www.dji.com.

[38] 科大国盾量子技术股份有限公司. 国盾量子[EB/OL]. [2023-02-07]. https://www. quantum-info. com/.
Quantum CTek Co., Ltd. Quantum CTek[EB/OL]. [2023-02-07]. https://www. quantum-info. com/.

[39] ZHAO L, ZENG B. An exact algorithm for two-stage robust optimization with mixed integer recourse problems[EB/OL]. [2025-01-15]. https://optimization-online.org/wp-content/uploads/2012/01/3310. pdf.

[40] HU B Q, WU L. Robust SCUC considering continuous/discrete uncertainties and quick-start units: a two-stage robust optimization with mixed-integer recourse[J]. IEEE Transactions on Power Systems, 2016, 31(2): 1407-1419.

[41] FORTUNY-AMAT J, MCCARL B. A representation and economic interpretation of a two-level programming problem[J]. Journal of the Operational Research Society, 1981, 32(9): 783-792.

[42] MCCORMICK G P. Computability of global solutions to factorable nonconvex programs: part I-convex underestimating problems[J]. Mathematical Programming, 1976, 10(1): 147-175.

[43] DOLATABADI S H, GHORBANIAN M, SIANO P, et al. An enhanced IEEE 33 bus benchmark test system for distribution system studies[J]. IEEE Transactions on Power Systems, 2021, 36(3): 2565-2572.

[44] 许 珞，郭庆来，刘新展，等. 提升电力信息物理系统韧性的通信网鲁棒优化方法[J]. 电力系统自动化，2021，45(3)：68-75.
XU Luo, GUO Qinglai, LIU Xinzhan, et al. Robust optimization method of communication network to improve resilience of cyber-physical power system[J]. Automation of Electric Power Systems, 2021, 45(3): 68-75.

[45] 蔡 晔，汤 丽，唐夏菲，等. 基于 NSGA-Ⅱ的电力信息物理系统骨干网络辨识[J]. 电力系统自动化，2023，47(12)：38-46.
CAI Ye，TANG Li，TANG Xiafei，et al. Backbone network identification of cyber-physical power system based on non-dominated sorting genetic algorithm-Ⅱ[J]. Automation of Electric Power Systems，2023，47(12)：38-46.

[46] 中华人民共和国住房和城乡建设部. 供配电系统设计规范：GB 50052—2009[S]. 北京：中国计划出版社，2010.
Ministry of Housing and Urban Rural Development of the People’s Republic of China. Code for design electric power supply systems: GB 50052—2009[S]. Beijing, China: China Planning Press, 2010.

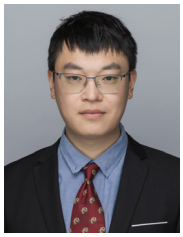
[47] 臧天磊，刘云飞，王世俊，等. 计及故障传播效应的配电信息物理系统多时段维修-恢复协同策略[J]. 电力自动化设备，2024，44(12)：247-256.
ZANG Tianlei, LIU Yunfei, WANG Shijun, et al. Multi-period maintenance and restoration collaborative strategy for cyber physical distribution system considering fault propagation effect[J]. Electric Power Automation Equipment, 2024, 44(12): 247-256.

[48] 何清素，曾令康，欧清海，等. 配电通信网业务断面流量分析方法[J]. 电力系统自动化，2014，38(23)：91-95.
HE Qingsu, ZENG Lingkang, OU Qinghai, et al. An analysis method for business sectional flow of distribution communication network[J]. Automation of Electric Power Systems, 2014, 38(23): 91-95.



钱雨琦
2000—，女，博士生
主要从事量子通信在电力系统的应用和弹性电力系统研究
E-mail: qianyuqi77@stu.xjtu.edu.cn

QIAN Yuqi
Ph.D. candidate



谢海鹏(通信作者)
1989—，男，博士，副教授，博导
主要从事电力系统可靠性、能源互联网弹性和量子信息学在电力系统的应用研究
E-mail: haipengxie@mail.xjtu.edu.cn

XIE Haipeng
Ph.D.
Associate professor
Corresponding author

收稿日期 2025-01-15 修回日期 2025-09-24 编辑 陈 蔓