电力通信网络敏感信息传输路由安全优化设计

崔淑涛
邯郸市睿智电力工程设计有限公司　河北邯郸　056000

摘　要：电力通信网络作为智能电网的“神经中枢”，承担着电力生产、调度、监控等核心业务的数据传输任务。随着电力系统数字化、智能化加速推进，敏感信息（如电网控制指令、用户用电数据）的传输安全已成为行业焦点。然而，当前网络架构存在路由协议易受攻击、动态拓扑适应性差、多维度威胁交织等风险，传统安全防护手段难以满足新型电力系统对“实时性、保密性、可靠性”的严苛要求，亟需从路由层构建安全防线。本文提出一种基于多目标优化模型的路由安全框架，结合加密技术、拓扑感知算法和动态风险评估，在保障传输效率的同时提升抗攻击能力。

关键词：电力通信网络；敏感信息传输；路由安全优化；设计

引言

电力通信网络的安全防护需超越传统“点状防御”模式，向“全局化、动态化”的安全体系演进。敏感信息传输路由的安全不仅需依赖加密算法的静态防护，更需融合动态拓扑感知、实时风险评估与智能路径规划，构建“安全－效率”双维度协同机制。通过软件定义网络（SDN）的集中控制能力，结合威胁情报驱动的动态路由决策，实现网络资源的最优分配与安全风险的主动规避，为电力通信提供“韧性、高效、可信”的传输保障。

一、电力通信网络敏感信息传输的安全威胁分析

1.路由协议与拓扑动态性引发的安全漏洞

电力通信网络依赖动态路由协议（如OSPF、BGP）实现数据转发，但其天然存在安全缺陷。传统协议缺乏对敏感信息的差异化保护机制，攻击者可利用协议漏洞（如伪造路由更新、篡改链路状态）实施路由劫持或欺骗，导致敏感数据流向非法节点。此外，电力网络拓扑随设备状态（如故障、检修）频繁变化，动态调整过程中易产生“中间状态暴露”，即临时路由路径未被加密或认证，攻击者可趁机窃听或篡改数据。更严峻的是，分布式能源（如光伏、风电）的接入加剧了网络复杂度，部分边缘设备可能因算力或协议兼容性问题，成为攻击跳板，进一步威胁核心通信链路安全。

2.物理层与网络层交织的复合攻击风险

电力通信网络需同时应对物理层与网络层的双重威胁。物理层方面，攻击者可利用电磁干扰、光纤窃听等手段直接截获或篡改传输信号，尤其针对光纤通信，通过“弯折光纤”或“注入光脉冲”即可窃取敏感数据。网络层方面，DDoS攻击、中间人攻击等传统威胁依然活跃，且攻击手段日益复杂化（如AI驱动的流量生成、零日漏洞利用）。更危险的是，复合攻击模式逐渐显现：攻击者先通过物理层干扰破坏通信稳定性，再利用网络层漏洞注入恶意指令，导致电网设备误动作。例如，针对变电站通信节点的攻击可能同时引发光纤信号衰减和路由协议篡改，造成区域性停电风险。

3.新型技术融合带来的未知威胁

电力通信网络向智能化、数字化演进过程中，新技术引入了新的安全风险。例如，软件定义网络（SDN）虽提升了网络灵活性，但集中式控制器的单点故障可能被攻击者利用，通过控制平面攻击瘫痪全网路由。此外，量子计算的发展对传统加密算法构成威胁，一旦攻击者利用量子计算机破解对称加密密钥，敏感信息将完全暴露。更值得警惕的是，电力物联网（IoT）设备的广泛部署导致攻击面指数级增长，部分设备因固件更新滞后或安全机制缺失，可能成为攻击者的“跳板机”，进而渗透至核心通信网络。例如，智能电表若被劫持，攻击者可通过伪造计量数据干扰电网调度，甚至触发保护装置误动。

二、由安全优化设计原则

1.分层防御与动态协同

传统路由安全依赖静态加密或单一防护机制，难以应对复杂多变的网络威胁。分层防御原则强调将安全功能解耦为“感知层、决策层、执行层”，通过多层次协同

提升整体韧性。例如，感知层利用软件定义网络（SDN）的集中控制能力，实时采集全网拓扑与流量数据；决策层基于威胁情报与风险评估模型，动态生成安全路由策略；执行层通过边缘设备快速响应策略调整，实现“秒级”切换。分层架构的动态协同可避免单点故障，例如，当某区域链路遭受攻击时，系统可自动隔离该区域，并通过备用路径重新规划路由，确保敏感信息不中断传输。此外，分层防御需与量子安全通信、零信任架构等前沿技术深度融合，构建“防御–检测–响应”的闭环体系。

2.风险驱动的智能路由

传统路由算法以“最短路径”为唯一目标，忽视链路安全性与业务优先级差异。风险驱动原则要求将安全风险量化为路由决策的输入参数，实现“安全–效率”的智能平衡。例如，通过实时监测链路的丢包率、延迟波动、物理干扰等指标，结合机器学习算法预测潜在威胁，动态调整路由权重。对于高优先级业务（如电网控制指令），系统可自动选择冗余路径并启用端到端加密；对于低优先级业务（如监测数据），则采用轻量级加密与负载均衡策略。风险驱动的智能路由还可通过模拟攻击测试验证策略有效性，例如，主动注入虚假流量触发路由切换，评估系统在极端情况下的抗攻击能力。

3.弹性自适应与持续演进

电力通信网络拓扑随设备状态（如故障、检修）频繁变化，传统路由策略难以快速适应。弹性自适应原则强调通过自动化与自愈机制，实现路由的“无感切换”与“自我修复”。例如，当某条链路因物理攻击失效时，系统可基于拓扑感知快速生成替代路径，并通过数字孪生技术验证路径可行性，避免人工干预导致的延迟。持续演进则要求路由安全框架具备“学习–优化”能力，例如，通过历史攻击数据训练风险评估模型，不断优化路由策略；或结合区块链技术实现安全策略的分布式共识，防止单一机构篡改。弹性自适应与持续演进还需与行业合规标准（如《网络安全法》《关键信息基础设施保护条例》）深度绑定，确保技术方案始终符合最新安全要求。

三、安全路由优化设计关键技术

1.动态信任评估与路径选择机制

动态信任评估作为安全路由优化的核心基石，依托于对网络节点行为的实时感知与量化分析，构建具备自适应能力的可信路由路径。评估模型需融合多维信任因子，包括节点历史通信的完整性（如丢包率、时延稳定性）、数据转发的可靠性（如成功交付率、重传次数）以及安全事件响应的时效性（如漏洞修复速度、攻击阻断效率），通过动态加权评分算法（如时间衰减加权法）实时更新节点信任值。对于信任值低于预设阈值的节点，系统将自动触发隔离机制（如物理隔离或逻辑降权），确保路由路径仅由高可信节点组成，从而阻断恶意节点的渗透路径。路径选择阶段引入多目标决策理论，将信任值、链路质量与负载均衡纳入统一评价体系，通过模糊逻辑或熵权法计算最优路径。该机制能够有效抵御恶意节点渗透，同时避免传统静态路由策略的僵化问题，提升网络整体安全性。

2.分层加密与轻量级密钥管理

敏感信息传输需在协议栈各层实施差异化加密策略，以平衡安全性与计算资源消耗。物理层采用基于国密算法的帧级加密技术，直接对链路层数据帧进行封装，确保底层传输的机密性；网络层则通过动态密钥分发协议（如基于身份的密钥协商协议，IBKE）实现路由控制信息的端到端保护，避免传统公钥基础设施（PKI）中证书交换的复杂开销。密钥管理方案需与网络拓扑动态性联动：当节点移动或链路状态变化时，系统自动触发密钥更新机制，并引入前向安全性（Forward Secrecy）与后向安全性（Backward Secrecy）约束，防止长期密钥泄露导致的回溯攻击。例如，采用基于椭圆曲线密码（ECC）的轻量级密钥协商协议，可显著降低计算开销，同时满足电力通信网络对低延迟（如<50ms）与高安全性的双重需求。

3.自适应抗攻击路由协议

传统路由协议在面对主动攻击时存在响应滞后、防御手段单一的问题，需设计具备自适应特性的抗攻击路由协议。该协议通过集成软件定义网络（SDN）的集中控制逻辑，实现全局视角下的实时威胁感知与路径重构。具体而言，系统持续监测网络流量特征（如丢包率、延迟抖动、路由表更新频率），利用机器学习算法识别异常行为（如洪泛攻击、路由表篡改），并触发动态路径切换机制。例如，当检测到某条链路遭受DDoS攻击时，SDN控制器可快速隔离攻击流量，并通过备用路径（如多路径冗余传输）恢复通信。协议核心在于平衡安全性与可用性：采用概率性路由通告验证（如基于区块链的路由签名）防止伪造路由消息，同时通过多路径分流降低单点故障风险。此外，协议支持策略动态加载，根据攻击类型（如DoS、窃听、中间人攻击）自动切换防御模式（如速率限制、强化加密、身份验证），形成“检测–响应–恢复”的闭环安全防护体系。

4. 智能威胁感知与动态防护体系

构建基于深度学习的网络异常检测模型，通过分析流量特征（如数据包大小、传输频率、协议类型）和行为模式（如设备连接规律、用户操作习惯）实现攻击行为的早期预警。系统采用分布式探针采集网络状态信息，运用图神经网络（GNN）和时序分析技术（如LSTM）挖掘潜在威胁关联性。例如，当检测到某区域设备频繁发起异常连接请求时，系统可结合拓扑信息推断攻击路径，并触发防御响应。设计动态安全策略引擎，根据威胁等级（如低危、高危、紧急）自动调整防护强度（如流量清洗、访问控制、隔离阻断），实现从被动防御到主动防护的转变。引入SDN的集中控制架构，通过全局视图统一监控全网安全状态，并利用意图驱动网络（IBN）技术快速下发安全策略。例如，当检测到高级持续性威胁（APT）时，系统可自动启动“沙箱隔离+流量溯源”模式，阻断攻击链。建立安全防护闭环系统，将检测结果实时反馈至路由决策模块（如调整路径优先级、隔离受攻击节点），形成“感知–分析–决策–执行”的持续优化机制。

四、未来研究方向

1. 量子通信技术与电力专用加密体系融合

量子密钥分发技术在电力通信网络中的应用将突破传统加密技术的安全瓶颈。研究重点在于开发适用于电力系统特殊环境的量子通信设备，解决长距离传输和复杂电磁干扰下的稳定性问题。需要构建电力专用量子密钥分发协议，优化现有网络架构实现经典与量子信道的协同传输。同时探索抗量子计算攻击的新型密码算法，设计面向智能电网的混合加密体系。该方向的发展将显著提升电力敏感信息传输的前向安全性，为构建下一代电力通信网络安全基础设施提供技术支撑。

2. 人工智能驱动的自主安全防御系统

基于深度强化学习的网络安全自主决策系统将成为未来研究热点。重点突破方向包括构建电力通信网络数字孪生平台，通过仿真环境训练智能体应对各类攻击场景。研究多智能体协同防御机制，实现分布式节点的自主安全联动。开发轻量级神经网络模型，使其能够部署在各类电力终端设备上实时监测异常行为。探索可解释AI技术在安全决策中的应用，提升系统透明度和运维人员信任度。该方向的发展将推动电力网络安全防御从规则驱动向智能自主演进，大幅提升对新型威胁的实时应对能力。

3. 基于区块链的分布式安全认证机制

探索区块链技术在电力通信网络身份认证与访问控制中的创新应用，构建去中心化的信任基石。针对电力设备算力资源受限的挑战，重点研发轻量级共识算法（如分层共识、边缘计算辅助共识），在保障安全性的同时降低计算开销。通过优化区块链存储结构（如分片存储、链上链下协同），突破海量终端接入的性能瓶颈。开发基于智能合约的动态权限管理系统，实现“按需授权、实时审计”的细粒度控制，例如，通过链上规则自动执行权限变更，并记录全流程操作日志。该机制可彻底消除传统集中式认证系统的单点故障风险，显著提升电力通信网络的抗攻击能力和可追溯性，为智能电网构建可信的数字身份底座。

结束语

本文提出的电力通信网络敏感信息传输路由安全优化设计，通过动态信任评估、分层加密、多路径冗余和智能威胁感知等关键技术，构建了全方位安全防护体系。研究成果为提升电力系统通信网络安全性和可靠性提供了有效解决方案，对保障关键基础设施安全运行具有重要意义，具有广阔的应用前景。

参考文献

[1] 杨波. 电力通信网络敏感信息传输路由安全优化设计 [J]. 电子设计工程，2024，32（24）：32-35+41.

[2] 龚喜，张旭，杨飞朋，等. 一种无线通信网络信息敏感密文数据差错恢复方法 [J]. 自动化技术与应用，2024，43（07）：107-110+162.

[3] 曹康宁. 基于深度强化学习的战术通信网络路径智能优选算法研究 [D]. 南京信息工程大学，2024.

[4] 杜玉昌. 基于局部差分隐私的通信网络敏感数据安全传输控制 [J]. 高师理科学刊，2024，44（05）：46-49+55.

[5] 胡人卓，黄立勤. 电力通信网络中的安全问题及其解决方案研究 [J]. 信息系统工程，2023，（08）：80-83.

[6] 黄徐川. 面向电力时延敏感类业务的数据转发机制的设计与实现 [D]. 北京邮电大学，2022.