无线传感器网络在电力系统自动化中的应用及安全性能分析

李蔚渠
广州海关技术中心，广东 广州 510000
DOI: 10.61369/TACS.2025060004

摘　　要： 本文研究了无线传感器网络在电力系统自动化中的应用及其安全性能。无线传感器网络凭借其部署灵活与成本低廉的优势，在电力设备状态监测、故障诊断及智能电网建设中发挥重要作用，提升了系统感知与响应能力。然而，其开放通信环境与受限节点资源也面临窃听、篡改、拒绝服务等多重安全威胁。研究从加密认证、容侵路由、入侵检测等方面提出轻量化安全机制，并通过形式化验证与仿真等手段评估防护效果，对增强电力系统自动化运行的可靠性与安全性具有重要意义。

关 键 词： 无线传感器网络；电力系统自动化；安全性能

Application and Security Performance Analysis of Wireless Sensor Networks in Power System Automation

Li Weiqu
Guangzhou Customs Technology Center, Guangzhou, Guangdong 510000

Abstract: This paper investigates the application of wireless sensor networks (WSNs) in power system automation and analyzes their security performance. Leveraging flexible deployment and low-cost advantages, WSNs play a key role in power-equipment condition monitoring, fault diagnosis, and smart-grid construction, thereby enhancing system perception and response capabilities. However, their open communication environment and resource-constrained nodes are exposed to multiple security threats such as eavesdropping, tampering, and denial-of-service attacks. The study proposes lightweight security mechanisms in the aspects of encryption and authentication, intrusion-tolerant routing, and intrusion detection, and evaluates the protection effectiveness through formal verification and simulation. The results are significant for improving the reliability and security of power system automation.

Keywords: wireless sensor networks; power system automation; security performance

引言

随着电力系统规模与复杂度的不断提升，传统监控手段已难以满足高可靠性及实时性要求。无线传感器网络以其灵活部署、低成本和实时感知等优势，为电力系统自动化提供了有效的技术支持，广泛应用于设备状态监测、故障诊断与智能电网建设。《“十四五”现代能源体系规划》（2022年）明确提出推动能源数字化转型与智能化升级，强化电力系统智能感知与安全调控能力。然而，无线通信开放性及节点资源受限也带来数据窃听、恶意攻击等安全威胁。因此，研究其在电力系统中的应用及安全性能，对保障系统稳定运行具有重要现实意义。

一、无线传感器网络的基本原理

无线传感器网络是一种由大量低功耗、微型化的传感器节点组成的新型信息获取与处理系统。传感器节点通常集成数据采集、信号处理和无线通信等功能，能够通过自组织方式构建多跳无线网络，实现对目标区域的连续监测与数据传输。其基本架构一般划分为感知层、网络层和应用层：感知层负责对环境参数或设备状态进行实时采集，网络层承担数据的传输与路由，应用层则对数据进行综合处理并为上层系统提供服务。

由于该网络依托 Ad Hoc 技术实现动态组网，节点之间无需固定基础设施即可进行通信，具备较强的灵活性与适应性[1]。然而，传感器节点本身计算能力、存储容量及能源供应均十分有限，这一特性决定了在协议设计、路由策略与系统优化过程中，必须把能量消耗和资源分配作为核心考量。如何在保证数据传输可靠性与实时性的同时延长网络寿命，成为无线传感器网络研究与应用中的关键问题。这一技术在环境监测、智能交通、医疗健康和国

防安全等领域均展现出广阔应用前景。

二、无线传感器网络在电力系统自动化中的应用

（一）远程监控与数据采集

无线传感器网络在电力系统自动化中的远程监控与数据采集环节发挥着至关重要的作用。通过在输电线路、变电站及配电环节广泛部署传感器节点，系统能够实时感知和获取电力设备的运行状态参数，包括电压、电流、温度以及负荷变化等关键信息。这些数据通过多跳自组织网络进行高效传输，最终汇聚至监控中心，实现对电网运行的全景感知与动态掌控。与传统依赖人工巡检的方式相比，该模式大幅提升了信息采集的实时性与完整性，显著降低人工投入和巡检成本[2]。

传感器节点不仅具备基本的数据采集功能，还能够进行本地化的数据处理与压缩，有效减轻通信负担，降低网络能耗，从而延长系统整体运行寿命。远程监控系统的应用为电力系统调度与运行维护提供了强有力的数据支撑，也为故障预警和应急响应创造了条件。在此基础上，电力企业能够进一步发展智能控制和自主决策功能，推动电力系统向更加智能化和可靠化的方向演进。

（二）故障检测与诊断

无线传感器网络在电力系统的故障检测与诊断中发挥着不可替代的作用。通过在输电线路、变电站和关键设备处部署大量智能传感器节点，系统能够实时采集电压、电流、频率、温度等多维度运行参数，并依托自组织多跳网络高效传输至中央处理单元进行分析。基于连续的数据流，监测系统能够在极短时间内识别异常运行状态与潜在隐患，对线路短路、设备过载或过热等典型故障实现快速定位与精确诊断[3]。

结合机器学习与大数据分析方法，不仅能够对历史与实时数据进行深度挖掘，还能优化故障分类与预测模型，提升诊断的准确性和前瞻性。部分数据处理任务可在边缘节点完成，从而减少大规模数据传输带来的通信压力，缩短延迟并提升整体响应速度。这一技术应用显著增强了电力系统的自愈能力与运行可靠性，在降低停电损失、缩短恢复时间及提高电网安全性方面具有重要意义，同时也为实现更加智能化的电网管理提供了坚实支撑。

（三）智能电网的实现

无线传感器网络为智能电网的实现提供了关键技术支撑，尤其在提升电网智能化与互动化水平方面作用显著。该系统通过广泛分布的传感器节点实时监测发电、输电、配电及用电各环节的运行状态，实现对电网全景信息的精准感知与高效集成。借助于多跳自组织网络，各类监测数据能够可靠传输至主站系统，为智能调度与能源管理提供实时、准确的数据基础[4]。

在用电侧，无线传感器网络支持智能电表与家用能源网关之间的双向通信，实现用电信息的自动采集与用户侧需求响应。在配电网中，依托传感器网络对分布式能源接入点的监测与控制，提升了电网对风电、光伏等间歇性能源的接纳能力与运行稳定性。此外，通过将边缘计算与传感节点相结合，可在本地完成部分数据处理与决策，降低上行通信压力，提高控制指令的响应速度与可靠性。无线传感器网络所赋能的智能电网，显著增强了系统的自适应能力、能源利用效率与供电可靠性，为实现电网智能化转型奠定了坚实基础。

三、无线传感器网络的安全性能分析

（一）安全威胁与挑战

无线传感器网络在电力系统自动化应用中面临多重安全威胁，其开放式的无线通信环境与资源受限的节点特性加剧了系统的脆弱性。主要威胁包括数据窃听、信息篡改、恶意节点注入及拒绝服务攻击等。攻击者可利用信道广播特性截获敏感数据，破坏监测信息的机密性；通过篡改传输中的报文内容，干扰系统对设备状态的准确判断，甚至诱发错误控制动作[5]。

传感器节点常部署于无人值守区域，易遭受物理捕获或伪装，攻击者可通过复制、伪造节点注入虚假数据，扰乱系统运行状态。拒绝服务攻击通过消耗节点有限的计算、存储与通信资源，致使网络服务中断，影响电力监控的实时性与连续性。此外，无线传感器网络多采用多跳自组织传输，路由协议自身的安全缺陷可能被利用，造成路径误导或网络分区[6]。这些安全挑战若未有效应对，将直接威胁电力系统的可靠运行与供电安全，因此构建兼顾轻量化与高强度的安全防护体系尤为迫切。

（二）安全机制与策略

为应对无线传感器网络在电力系统中所面临的安全威胁，需构建多层次、轻量化且适应资源约束的安全机制。在数据安全方面，采用轻量级加密算法（如轻量级分组密码与椭圆曲线密码）保障数据传输机密性与完整性，结合高效消息认证码防止数据篡改与重放攻击。身份认证机制通过双向身份校验与轻量化数字签名，有效识别并排除恶意节点，防止非法设备接入[7]。

在网络层面，设计具有容侵能力的安全路由协议，可抵御选择性转发、黑洞攻击等路由欺骗行为，维护多跳传输路径可靠。入侵检测系统部署于汇聚节点或区域管理器，通过异常流量分析与行为监控识别恶意活动，实现攻击早期预警。

密钥管理是安全基础，可采用分簇式或基于身份的密钥管理方案，平衡安全强度与通信开销。同时，引入信任管理模型，通过节点行为评价动态调整其信任值，增强网络动态安全防御能力[8]。这些策略协同实施，可显著提升无线传感器网络在电力自动化环境中的鲁棒性与安全性

（三）安全性能评估方法

无线传感器网络的安全性能评估需结合其应用场景与资源约束特性，采用多维度、定量化的分析方法。评估指标体系通常涵盖机密性、完整性、可用性及抗攻击能力等方面，通过建模与实验手段综合评价安全机制的有效性[9]。在机密性方面，可通过分析加密算法强度与密钥管理机制的抗破解能力，评估数据防窃听水平；完整性可通过误码率、篡改检测率等指标衡量认证机制的有效性。

典型评估方法包括形式化验证、仿真实验与实测分析。形式

化方法运用逻辑与数学工具验证安全协议的正确性与完备性；仿真平台（如 NS2、OMNeT++）可模拟多种攻击场景，测试网络在不同威胁下的存活率、数据包投递率及能耗变化。实测评估则依托真实网络环境，注入典型攻击流，观测系统响应与性能退化情况，评估安全机制的实际部署效果[10]。此外，可引入韧性评估概念，衡量系统在遭受攻击后维持关键功能及自我恢复的能力，从而全面反映无线传感器网络在电力自动化环境中的安全性能。

四、结论

无线传感器网络凭借其部署灵活、成本低廉及实时监测等优势，已成为提升电力系统自动化水平的关键技术。其在远程监控、故障诊断与智能电网构建等方面的应用，显著提高了电力系统的感知能力、响应速度与运行可靠性。然而，无线通信开放性及节点资源受限等特点，也引入了数据窃听、恶意攻击、路由欺骗等多类安全威胁，对电力系统稳定运行构成潜在风险。

针对上述安全问题，需构建轻量化、多层级的安全防护体系，结合加密认证、容侵路由、入侵检测与信任管理等机制，提升网络抗攻击与自恢复能力。安全性能应通过形式化验证、仿真与实测等方法进行系统评估，以保证其在实际电力环境中的有效性。未来研究应进一步聚焦于兼顾低开销与高强度的安全方案设计，以推动无线传感器网络在电力系统自动化中更可靠、更广泛的应用。

参考文献

[1] 刘文利 . 试述无线传感器网络在楼宇自动控制中的应用 [J]. 黑龙江科技信息 ,2015,(24):34.

[2] 王瀚 . 配电网自动化通信网络的安全管理分析 [J]. 集成电路应用 ,2022,39(5):182-183.

[3] 张思伟 . 配电网自动化通信网络的安全管理分析 [J]. 电声技术 ,2022,46(11):83-85.

[4] 张忠林 . 无线电子通信技术的应用安全分析 [J]. 科学与信息化 ,2024(1):90-92.

[5] 李霞婷 , 陈杰建 . 基于无线传感器网络技术的智能物联施工安全防护系统设计 [J]. 现代信息科技 ,2024,8(03):159-163.

[6] 占亚波 , 涂潜 , 李俊 , 等 . 大规模输电线路状态监测传感器网络的周期性低功耗通信技术方案 [J]. 电信科学 ,2023,39(2):83-91.

[7] 苏博 . 无线传感器网络容量与安全性研究 [D]. 西安电子科技大学 ,2013.

[8] 洪勇 , 李平 . 基于无线传感器网络相关性的信息安全防御机制 [J]. 计算机应用 ,2013,33(02):423-425+467.

[9] 王亨友 , 彭木根 , 王文博 . 基于网络编码技术的无线传感器网络安全机制 [J]. 中国电子科学研究院学报 ,2010,005(6):616-620.

[10] 何明 , 董强 , 袁黎苗 , 裘杭萍 , 曾晓光 . 无线传感器网络的可靠性评估模型 [J]. 陆军工程大学学报 ,2010,11(4):392-39.

