工程技术发展
Engineering Technology Development
第 5 卷◆第 5 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

智慧水务行业的通信安全策略

周玉杰
浪潮数字企业技术有限公司
DOI:10.12238/etd.v5i5.9117

[摘　要] 随着智慧水务系统的广泛应用,其通信安全成为保障供水安全与稳定运行的关键。本文对智慧水务行业面临的通信安全挑战进行了分析,并提出一系列创新性的通信安全策略。通过构建多层次防御体系、强化数据加密与身份认证、以及实施安全管理与监控,本文为智慧水务行业的通信安全提供全面而有效的解决方案。这些策略不仅能够有效抵御外部攻击,还能确保内部通信的机密性、完整性和可用性,为智慧水务行业的可持续发展奠定坚实的基础。
[关键词] 智慧水务；通信安全；分析策略
中图分类号：TN918.91　**文献标识码：**A

Communication security strategy of smart water industry

Yujie Zhou
Inspur Digital Enterprise Technology Co., Ltd

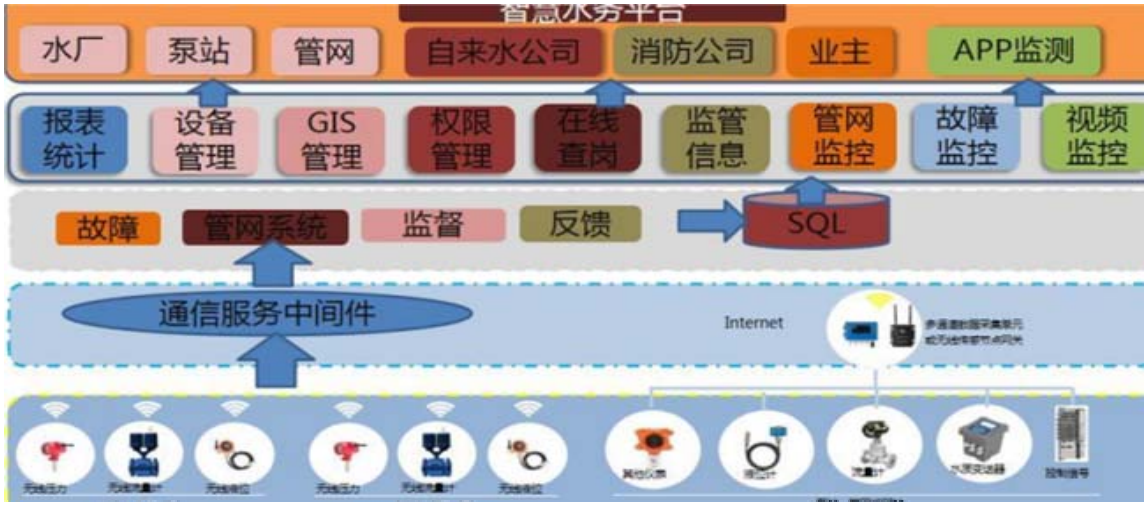
[Abstract] With the wide application of intelligent water system, its communication security has become the key to ensure the safety and stable operation of water supply. This paper analyzes the communication security challenges facing the smart water industry and proposes a series of innovative communication security strategies. By building a multi-level defense system, strengthening data encryption and identity authentication, and implementing security management and monitoring, this paper provides a comprehensive and effective solution for the communication security of the intelligent water industry. These strategies can not only effectively resist external attacks, but also ensure the confidentiality, integrity and availability of internal communications, laying a solid foundation for the sustainable development of the smart water industry.
[Key words] intelligent water; communication security; analysis strategy

引言

在数字化时代,智能水务系统因其高效率和智能化特性,正逐步成为城市水资源管理的关键组成部分。但随着系统结构变得日益复杂,数据量也急剧增长,通信安全问题也变得尤为突出。智能水务系统处理着众多关键信息,包括个人信息、水质测试数据、供水调度命令等。如果这些通信过程遭受攻击或信息泄露,可能会对供水的安全性、社会秩序甚至国家的安全造成严重威胁。因此,探索并确立一套科学且有效的通信安全措施,对于确保智能水务行业的稳定发展极为关键。

1 构建多层次防御体系

在智慧水务系统中构建多层次防御体系,是确保通信安全的基础。这一策略的核心在于通过多重安全机制,形成纵深防御,有效抵御各类网络威胁(图一)。首先,在系统边界部署新一代智能防火墙,不仅能够过滤网络流量,还可以深度检测应用层协议,识别和阻断恶意行为。同时,在网络内部实施微分段技术,将整个系统划分为多个独立的安全域,每个域之间通过严格的访问控制策略进行隔离。这样即使某一区域遭受攻击,也能将影响限制在局部范围内。在网络架构设计中,采用“蜂窝网络”模型,将关键系统节点置于多层保护之下。例如,核心数据中心可以设置物理隔离区、DMZ区和内网区,每个区域都配备独立的安全设备和策略。在终端设备管理方面,实施统一终端管理平台,对所有接入智慧水务网络的设备进行严格的准入控制。通过强制安装终端安全软件、定期漏洞扫描和补丁更新,确保每一个终端都成为防御体系中的坚固一环[1]。对于物联网设备,如智能水表和管网传感器,采用轻量级加密算法和专用安全芯片,在资源受限的情况下也能提供可靠的安全保护。此外,建立安全运营中心(SOC),集中管理和分析全网的安全日志和告警信息。利用人工智能和大数据分析技术,实现对潜在威胁的预警和快速响应。通过定期的红蓝对抗演练,持续评估和优化防御体系的有效性,确保多层次防御策略能够与时俱进,应对不断演化的网络威胁。除此之外,还可以考虑引入软件定义网络(SDN)技术,实现网络流量的动态调度和安全策略的灵活部署。通过SDN控制器,可以根



图一　智慧水务监测系统建设方案

图二　智慧水务管理系统可视化

据实时网络状况和安全威胁情报，快速调整网络拓扑和安全规则，提高系统的整体防御能力。最后，可以利用区块链技术构建去中心化的安全日志存储系统，确保日志数据的完整性和不可篡改性，为事后追溯和取证提供可靠依据。

2 强化数据加密与身份认证

在智慧水务系统中，数据的安全传输和可靠身份认证是保障通信安全的关键环节。强化这两个方面不仅能有效防止数据泄露和篡改，还能确保系统操作的合法性和可追溯性。首先，在数据加密方面，采用端到端加密技术，确保数据从生成到处理的全生命周期安全。对于传感器采集的原始数据，在源头就进行加密处理，使用轻量级但高强度的加密算法，如ChaCha20-Poly1305，既保证了安全性，又不会过多占用传感器的计算资源。在数据传输过程中，采用国密算法SM4进行加密，并结合SM3哈希算法确保数据完整性。对于存储在云端或本地数据中心的敏感信息，如用户个人信息、水质检测结果等，使用高级加密标准(AES)的256位加密，并实施数据分片存储，将关键数据分散存储在不同的物理位置，降低大规模数据泄露的风险。在身份认证方面，实施基于零信任架构的动态身份验证机制。每次访问系统资源时，都需要进行身份验证，不再依赖传统的边界安全模型[2]。具体而言，可以采用多因素认证(MFA)技术，结合密码、硬件令牌和生物特征等多种方式进行身份验证。对于高级管理员账户，引入基于行为分析的持续认证技术，通过实时监控用户的操作行为，如键盘敲击模式、鼠标移动轨迹等，持续验证操作者的身份，一旦发现异常，立即中断操作并要求重新认证。为了应对日益复杂的网络攻击，智慧水务系统还可以引入基于区块链的分布式身份认证系统。通过将用户身份信息和访问权限记录在区块链上，实现

身份信息的去中心化存储和不可篡改性。同时,利用同态加密技术,在保护用户隐私的前提下,实现对加密数据的直接处理和分析,进一步增强了系统的安全性和功能性。此外,为了进一步提升数据加密的安全性,可以考虑引入量子密钥分发(QKD)技术。QKD利用量子力学原理,实现理论上无法被破解的密钥交换,为智慧水务系统提供最高级别的加密保护。在身份认证方面,可以探索利用区块链技术构建去中心化身份管理系统(DID),赋予用户对个人身份信息的完全控制权,同时提高身份验证的可信度和效率。针对物联网设备的特殊需求,可以开发轻量级的Post-Quantum密码算法,为未来可能出现的量子计算攻击做好准备。

3 实施安全管理与监控

在智慧水务行业中,实施全面的安全管理与监控机制是确保通信安全的重要保障。首先,建立专门的信息安全管理团队,负责制定和执行安全策略。这个团队应该由具备水务行业背景和信息安全专业知识的复合型人才组成,确保安全措施既符合行业特点,又能满足技术要求。同时,实施分级授权管理制度。根据员工的职责和权限需求,将系统访问权限细分为多个等级,如只读、基础操作、高级管理等。对于核心系统的操作,实行双人双密码制度,即任何重要操作都需要两名授权人员同时在场并输入各自的密码才能执行,有效防止单点风险。此外,在日常运营中,部署智能安全态势感知平台,实时监控网络流量、系统日志和用户行为(图二)。利用机器学习算法,建立正常行为基线模型,快速识别异常活动。例如,检测到异常的数据访问模式或频繁的失败登录尝试时,系统会自动触发警报并采取相应的防护措施。另外,定期开展安全审计和风险评估,不仅包括技术层面的漏洞扫描和渗透测试,还应涵盖管理流程和人员操作的合规性检查[3]。建立动态的风险评估模型,根据新出现的威胁和系统变更及时调整安全策略。同时,制定详细的应急响应预案,定期进行演练,确保在发生安全事件时能够快速、有序地进行处置。

4 结语

在智能水务领域,确保通信安全是维护供水安全和系统顺畅运作的关键。通过实施一系列策略,如构建多级防护架构、加强数据的加密处理和用户身份验证、执行安全管理和监控措施,可以显著提高智能水务系统的安全性。这些措施不仅能够防范外部威胁和内部信息泄露,还能为行业的长期发展提供稳固的支持。展望未来,随着技术的持续进步和安全标准的逐步完善,智能水务系统的通信安全将变得更加稳固和高效。

[参考文献]

[1]王万鹏.智慧水务运行监测系统的设计与实现[D].山东科技大学,2019.

[2]李宏伟,闵乐乐.数字化转型下智慧水务应用安全建设[J].现代信息科技,2022,6(22):101-104.

[3]铁瀛.基于大数据的智慧水务信息共享数据中心的构建分析[J].无线互联科技,2022,19(23):24-26.

作者简介：

周玉杰(1988--),男,汉族,山东高密人,全日制本科,从事电子信息/大数据分析应用研究。