信息化背景下智能建筑通信网络安全防护策略分析

张 涛
中国铁塔股份有限公司嘉兴市分公司 浙江 嘉兴 314000

摘 要：智能建筑作为现代城市发展的重要组成部分，其通信网络的安全性对建筑系统的稳定运行至关重要。随着信息化进程的推进，智能建筑的通信网络面临多重安全威胁，诸如设备漏洞、数据泄露、外部攻击等问题不断加剧。为了有效应对这些风险，本文提出了一系列网络安全防护策略，包括基于角色的权限管理、网络入侵检测与防御技术、数据加密技术等，同时探讨了多层次访问控制体系在智能建筑安全管理中的应用。通过完善的安全管理体系和技术保障措施，可以大幅提高智能建筑通信网络的安全性，降低潜在的网络安全隐患。随着技术的发展，智能建筑的网络安全防护将不断优化，逐步迈向更加智能化、动态化的管理模式。

关键词：智能建筑；通信网络；安全防护；入侵检测；权限管理

引言

智能建筑利用先进的通信技术实现各系统的自动化管理，提升了建筑的运营效率和智能化水平。智能建筑通信网络的复杂性和多样性使其面临诸多安全挑战，尤其是在设备互联和数据传输的过程中，网络安全问题日益严重。攻击手段的不断演化、外部黑客的入侵风险、以及内部数据泄露的隐患，均可能对建筑系统造成严重影响。确保智能建筑通信网络的安全性，已成为建筑管理领域亟待解决的核心问题。本研究旨在分析智能建筑网络安全面临的主要问题，提出有效的安全防护策略，并探讨如何通过技术手段和管理机制实现对网络安全的全方位保障，确保智能建筑系统的长期稳定运行。

1 智能建筑通信网络面临的主要安全问题与挑战

1.1 智能建筑通信网络的复杂性与多样性

智能建筑通信网络通常由多种不同的设备、系统和技术构成，这使得其结构变得异常复杂。在智能建筑中，传统的建筑控制系统（如照明、暖通空调、安防系统）已经通过互联网协议（IP）与各种智能设备相连接，形成了一个跨越多个层次、多个系统的数据传输网络。这些设备不仅需要实时传输大量的数据，还要支持高度集成的自动化控制功能。智能建筑的通信网络涉及到传感器、执行器、控制器以及数据分析平台等多个环节，各个环节之间通过不同的通信协议进行信息交互，包括但不限于Zigbee、Wi-Fi、蓝牙、LoRaWAN等技术。这种多样性使得系统难以统一管理和维护，也使得网络的安全防护面临更多挑战。由于设备种类繁多、协议差异化和系统开放性较强，导致通信网络在设计和实施过程中容易出现安全漏洞，进而增加了整个建筑系统遭受网络攻击的风险。

1.2 当前智能建筑网络安全面临的主要风险

智能建筑通信网络所面临的安全风险主要体现在几个方面。由于智能建筑系统通常涉及大量的传感器和控制设备，这些设备若未能充分考虑安全性，极易成为攻击的目标。许多智能设备的硬件和软件安全性较差，缺乏必要的加密和认证机制，使得恶意攻击者可以通过物理接触或远程方式获得控制权限。智能建筑中的通信网络通常依赖于开放的通信协议，这些协议在设计时可能未能充分考虑到信息的加密和保护问题，导致传输的数据容易被拦截和篡改[1]。基于Wi-Fi或Zigbee的通信设备若没有有效的加密手段，信息在网络中传递时容易受到中间人攻击。由于智能建筑系统通常与外部网络进行连接，特别是当系统与云端进行数据交互时，可能导致云服务提供商或第三方服务商的安全性成为潜在的威胁源。一旦云平台出现安全漏洞或遭到攻击，建筑内部的数据和控制信息可能被泄露或篡改，导致建筑系统的全面瘫痪。

2 信息化背景下智能建筑通信网络安全防护的必要性与紧迫性

2.1 智能建筑系统的高度集成化与安全需求

智能建筑技术的快速发展使得各类设备和系统之间的深度集成成为常态。通过中央控制平台，智能建筑实现了对照明、暖通空调、安防、能源管理等多个子系统的协同控制。这种系统集成的复杂性促使设备之间的数据交互频繁，虽然带来了管理和操作上的便利，但也使网络安全面临巨大挑战。集成化的智能系统通常涉及多种终端设备和技术平台，存在潜在的安全漏洞，若某一环节被攻击，可能导致系统的全局性故障或敏感数据泄露[2]。不同厂商提供的软硬件平台常常存在不同的安

全标准和漏洞修复机制，增加了安全防护的难度。如果其中某一部分被攻破，可能会引发整个建筑系统的安全风险。随着集成化程度的提升，智能建筑对安全性的要求愈加迫切，必须从设计阶段起就把安全性纳入核心考量，确保各子系统的协调和防护得到有效保障。

2.2 网络安全事件频发对建筑安全管理的影响

随着信息化和物联网技术的广泛应用，网络安全事件频发已成为智能建筑面临的重要问题。网络攻击不仅使建筑系统的正常运行受到威胁，还可能带来不可预估的经济损失和声誉影响。某些网络攻击可能导致建筑的自动化控制系统被入侵，从而造成空调、电梯等关键设施的停止运转，甚至会直接影响到建筑内人员的生命安全和财产安全。攻击者通过网络漏洞获取建筑中的敏感数据，如人员进出记录、财务信息或设备状态等，可能使建筑业主和住户面临隐私泄露和安全威胁。而随着智能建筑对外联网程度的加深，数据在互联网上流通频繁，也增加了外部攻击的机会。网络安全事件的频发使得建筑安全管理面临更多挑战，传统的安全管理方式已经难以应对现代智能建筑的复杂性和规模。在这种背景下，智能建筑的安全管理需要更加注重网络安全防护，综合运用各种技术手段加强网络监控、威胁检测和应急响应机制，确保建筑的整体安全与稳定运行。

3 智能建筑通信网络安全防护策略的核心技术与方法

3.1 网络入侵检测与防御技术

智能建筑通信网络面临的安全威胁多种多样，入侵检测与防御技术成为保障网络安全的重要手段。入侵检测系统（IDS）通过监测网络流量、分析通信数据包，能够及时识别异常行为和潜在攻击，如拒绝服务攻击（DDoS）、恶意软件入侵等。这些系统结合基于签名的检测与行为分析的方式，提高了对未知攻击的识别能力。入侵防御技术（IPS）能够在攻击发生前主动拦截和防御，通过实时分析和响应，有效避免了潜在的安全事件[3]。为了提升智能建筑网络的防护能力，除了部署传统的防火墙、IDS和IPS之外，还需要整合人工智能与机器学习算法，通过对大规模数据的分析，实时调整防护策略，提高防御的准确性和反应速度。这些技术的结合可以显著降低网络攻击的风险，确保建筑设备的安全与稳定。

3.2 数据加密技术与信息传输安全保障

随着智能建筑中数据流动频率的增加，数据加密技术成为确保信息传输安全的关键手段。通过加密技术对通信过程中的敏感信息进行保护，防止信息在传输过程中被窃取或篡改。在数据传输过程中采用的对称加密和非对称加密技术，通过复杂的算法加密数据内容，使得未经授权的用户无法读取或修改数据。SSL/TLS协议常用于保护传输层的数据安全，确保网络通信的私密性和完整性。智能建筑系统中的终端设备与控制系统之间的通信需要采用安全的加密协议，如AES（高级加密标准），保证数据在无线网络环境中的传输安全。随着云计算和物联网技术的发展，数据加密不仅局限于局部设备，还应延伸至云平台和远程控制端，确保整个智能建筑生态系统的网络安全，防止数据泄露及远程控制风险。

4 智能建筑通信网络安全防护中的权限管理与访问控制机制

4.1 基于角色的权限管理模型

基于角色的权限管理（RBAC）模型在智能建筑通信网络中具有重要的应用价值。通过定义不同的角色（如管理员、操作员、维护人员、访客等），可以合理地控制不同用户对系统资源的访问权限。每个角色拥有特定的权限集合，确保用户仅能访问与其职责相关的系统功能，避免不必要的权限泄露或滥用。管理员角色可能拥有系统配置、用户管理和设备控制的全部权限，而普通操作员则只能够进行实时数据查看和设备状态监控[4]。该模型的优势在于简化了权限管理，减少了人为错误和不当权限分配的风险。随着智能建筑中设备和人员的多样化，基于角色的权限管理还可以与身份验证系统相结合，通过生物识别、智能卡等方式进一步增强安全性。角色权限模型的灵活性和可扩展性，使其成为管理智能建筑复杂系统中安全控制的有效工具。

4.2 多层次访问控制体系在安全防护中的应用

在智能建筑中，信息安全不仅仅依赖于单一的访问控制机制，而是需要多层次的保护措施。多层次访问控制体系通过将安全策略划分为多个层次，从物理层、网络层到应用层进行全面的安全防护。物理层的安全控制通过身份验证、门禁系统等手段确保只有授权人员能够接触关键设备；网络层通过防火墙、入侵检测和虚拟专用网络（VPN）等技术隔离敏感数据与外部网络，确保信息在传输过程中的安全；而应用层的访问控制则根据用户身份、权限角色等细化管理，确保用户只能访问特定的系统功能。不同层次的安全措施相互配合、相互加强，提供了更为强大的防护能力。尤其是在云计算和远程控制的背景下，多层次访问控制体系可以有效地防止来自外部的网络攻击，同时保护建筑内部网络和设备免受内部人员的不当访问或误操作。通过综合利用多层次访问控制，可以在保障智能建筑信息安全的提高系统运行的稳定性与可靠性。

表1：国内智能建筑网络安全防护技术市场规模及发展趋势（单位：亿元）

年份	网络入侵检测与防御技术	数据加密技术	访问控制与身份认证技术	安全监控与响应技术	总体市场规模
2020年	18.5	22.3	15.8	9.6	66.2
2021年	21.0	25.1	17.6	12.3	76.0
2022年	24.3	28.0	20.5	15.1	87.9
2023年	27.1	31.0	23.1	18.4	99.6
2024年(预测)	30.5	34.5	25.8	22.0	112.8

数据来源：

1. 中国建筑安全与信息技术协会《智能建筑安全技术市场研究报告》2023年

2. 中国网络安全产业联盟《2023年中国网络安全市场发展与趋势报告》

5 智能建筑通信网络安全防护策略的实施与优化路径

5.1 安全防护策略的落实与技术保障

智能建筑的安全防护策略不仅需要理论上的设计，还需要在实践中得到有效落实。这要求各类安全技术在建筑的网络中深入部署，从物理设备到数据传输层面都必须具备可靠的防护措施。在技术保障方面，网络防火墙、入侵检测系统（IDS）和加密算法等技术的应用至关重要。通过部署多层次的安全防护体系，可以从不同角度确保智能建筑网络的安全[5]。在传输层加强数据加密和身份验证，在网络层进行实时流量监控与异常行为检测，在应用层进行精细化的权限控制。防护策略的落实还需要与建筑管理系统的运维同步，包括定期的安全检查、漏洞修补和应急响应演练。确保技术保障体系的持续性与可维护性，使其能够在不断变化的网络环境中有效抵御潜在威胁。

5.2 智能建筑网络安全管理体系的优化与发展方向

随着智能建筑网络安全形势的日益严峻，传统的安全管理方式已无法应对复杂的网络威胁。智能建筑网络安全管理体系的优化成为必然趋势。安全管理体系需要更加注重跨部门协作和信息共享，尤其是在网络运维、建筑管理与信息安全之间建立有效的沟通机制。基于大数据和人工智能技术的安全监控与自动化响应能力将成为未来的主要发展方向。这些技术可以帮助系统实时检测和预测潜在风险，快速应对并修复安全漏洞。智能建筑安全管理体系还应与国际先进的安全标准接轨，如ISO27001信息安全管理体系等，提升整体安全管理的规范性和国际化水平。随着智能建筑技术的不断进步，未来的网络安全管理体系将更加智能化、动态化和自动化。

结语

智能建筑的快速发展使得其通信网络的安全性成为一个亟待解决的关键问题。随着系统集成度的提升和技术复杂性的增加，建筑网络面临的安全威胁愈加多样化和复杂化。通过实施多层次的安全防护策略，包括权限管理、入侵检测、数据加密等技术手段，可以有效降低潜在的安全风险，确保智能建筑系统的稳定运行。随着人工智能和大数据技术的应用，未来智能建筑的网络安全将逐步向智能化、自动化发展，实现更加精准和高效的安全防护。在这一过程中，智能建筑安全管理体系的优化也至关重要，需通过持续的技术创新和管理提升，确保建筑信息和设备的长期安全，推动智慧城市建设向更加安全、可持续的方向发展。

参考文献

[1]刘敏.财会信息化背景下智能财税的发展趋势与挑战[J].中国会展,2024,(21):234-236.

[2]王东海,薛楠,赵学梅,等.智能信息化背景下高校会计专业学科融合研究[J].商业会计,2024,(11):118-121.

[3]任江峰,费建国.农业信息化背景下智能农机的发展与研究[J].河北农机,2024,(02):57-59.

[4]沙乘风,王茂清.信息化背景下高校智能后勤建设与服务路径[J].中国高校科技,2023,(12):97.

[5]孙梦迪.信息化背景下企业人力资源管理模式创新研究[J].中国市场,2023,(34):134-137.