

# 安全光通信技术的发展趋势思考

## ——评《光编码安全光通信》

随着云计算、大数据、物联网等新兴技术的广泛应用,给信息社会带来了海量的数据传输需求。光通信是以光波为载波的通信方式,具有传输速度快、大容量、低损耗、抗干扰能力强等特点。由此可见,利用光通信技术可以较好地满足信息社会的数据传输需求。安全光通信技术的发展对于推动信息技术健康发展、保障国家网络空间安全具有重要意义,可促进相关产业链的升级和壮大,带动新技术、新应用的不断涌现,为经济社会可持续发展注入新的活力。然而,网络攻击手段的不断翻新和威胁类型的日益复杂多样,给光通信系统的安全性带来严峻挑战。

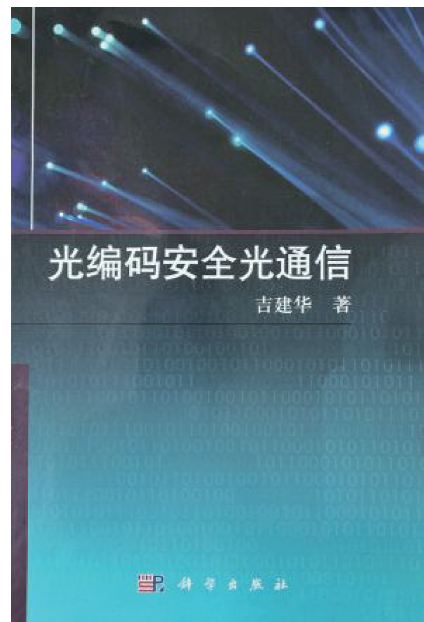
《光编码安全光通信》一书深入探讨了光通信系统中物理层安全性的前沿研究,特别是基于光编码技术的解决方案。作者通过分析光纤通信系统、自由空间光通信系统(FSO)以及混合光通信系统的物理层安全机制,为读者展现了光编码技术在保障光通信安全中的重要作用。该书首先概述了光网络面临的安全隐患及现有的物理层安全技术,详细阐述了基于光编码的物理层安全技术的原理与优势。通过引入信息论方法,科学评估了物理层安全性能,为后续深入讨论奠定了理论基础。然后,分别针对光纤光码分多址(OCDMA)系统、自由空间光-码分多址(FSO-CDMA)系统以及混合FSO光纤OCDMA系统,构建了搭线信道模型,并深入分析了这些系统在不同条件下的物理层安全性。特别是在FSO-CDMA系统中,探讨了多种调制技术,如开关键控、多进制脉冲位置调制下的物理层安全性能,并通过仿真验证了理论分析的正确性。最后,还创新性地提出了时间分集技术,进一步增强了FSO-CDMA系统的物理层安全性。全书内容丰富、结构严谨,既包含深入的理论分析,又涵盖详实的试验数据,颇具借鉴价值。

大数据、人工智能技术的日益成熟,使得安全光通信技术正逐步向智能化与自适应安全防护的方向转型,技术人员可利用先进的数据分析能力和机器学习算法,使光通信系统能够动态地识别、评估并应对各种网络威胁。传统的安全防护手段往往依赖于预设的规则和策略,对于新型攻击手段往往反应滞后,而智能化防护机制则能够通过持续学习网络流量模式、用户行为特征等大数据信息,自动识别和标记异常行为,实现威胁的即时预警和快速响应。面对复杂多变的网络环境,一个固定的安全防护方案往往难以全面应对各种挑战,而自适应防护策略则能够根据实时威胁情报、系统运行状态等因素,动态调整防护策略,确保系统始终保持在最佳的安全防护状态。通过不断引入新技术、新方法,优化算法模型,提升信息数据处理能力,安全光通信技术将不断突破传统界限,如可利用深度学习算法深度挖掘海量数据,发现潜在的安全隐患,或者采用分布式计算技术,提高系统的处理速度和扩展性。

云计算、边缘计算、物联网等技术的广泛应用,使得网络架构变得更加复杂和多样化。在此背景下,单纯依靠光通信系统自身的安全防护已经难以满足整体网络安全的需求。因此,推动光通信系统与网络架构的融合安全成为了安全光通信技术发展的必然趋势。融合安全要求光通信系统在设计之初就充分考虑了与网络架构的协同工作,要求光通信系统需要与网络中的其他组件(如路由器、交换机、防火墙等)实现无缝对接,共享安全策略、威胁情报等信息资源,形成统一的安全防护体系。融合安全强调从全局视角出发,构建多层次的安全防护策略,包括在网络架构的不同层次(如接入层、汇聚层、核心层等)部署相应的安全设备和服务,形成纵深防御体系;同时,在跨域通信、多协议交互等关键环节采取特殊的安全保护措施,确保数据在传输过程中的完整性和保密性。安全光通信技术还需要与网络架构中的其他组件紧密协作,共同构建具备冗余备份、故障切换等能力的安全体系。

总之,在云计算、大数据与物联网技术交织的当下,光通信作为信息传输的动脉,其安全性成为不容忽视的基石。智能化与自适应防护机制的兴起,以及光通信系统与网络架构融合安全的深化,正在加速构建一个安全、高效、韧性的网络空间,为信息社会的发展注入源源不断的动力与活力。

(赵佳伟/黄冈师范学院物理与电信学院)



书名:光编码安全光通信  
作者:吉建华  
出版社:科学出版社  
ISBN:9787030709080  
定价:98元  
出版时间:2022年3月