 DOI: https://doi.org/10.12349/iser.v7i3.9472

Analysis of Electronic Communication Security Technology Based on Optical Fiber Communication Technology

Haiwei Zhao

Shenyang Branch of China United Network Communications Co., Ltd., Shenyang, Liaoning, 110001, China

Abstract

Optical fiber communication, with its significant advantages such as wide bandwidth, low loss, and excellent anti-interference ability, has become the core support of modern communication networks. However, it must be pointed out that in many aspects such as link establishment, signal transmission, equipment node operation, and data storage, optical fiber communication is gradually revealing a series of security risks, posing a serious threat to information security. This paper analyzes the basic principles of optical fiber communication and discusses the security protection technologies for electronic communication from multiple dimensions including physical links, optical signals, data transmission and storage, and network architecture.

Keywords

Optical Fiber Communication; Electronic Communication Security; Network Architecture Optimization

基于光纤通信技术下的电子通信安全技术分析

赵海伟

中国联合网络通信有限公司沈阳市分公司，中国 · 辽宁 沈阳 110001

摘　要

光纤通信凭借其带宽宽广、损耗低微以及抗干扰能力卓越等显著优势，已然成为现代通信网络的核心支撑。然而，必须指出的是，光纤通信在链路搭建、信号传输、设备节点运行以及数据存储等诸多环节，正逐渐暴露出一系列安全隐患，对信息安全构成严重威胁。本文分析了光纤通信的基本原理，从物理链路、光信号、数据传输与存储以及网络架构等多个维度，探讨了电子通信的安全防护技术。

关键词

光纤通信；电子通信安全；网络架构优化

1 引言

通信作为社会运行的关键基础设施，在信息传递和经济发展中发挥着重要作用。光纤通信凭借其高速率、大容量和低损耗等突出优势，已成为现代信息传输体系的核心 [1]。但是，光纤网络在实际部署和运行过程中，也暴露出一系列不容忽视的安全隐患。由于光纤线缆铺设范围广泛，部分区段长期暴露于野外或公共场所，容易遭到蓄意破坏或恶意攻击，影响通信的连续性和可靠性。信号在传输过程中可能面临被窃听、篡改的威胁，敏感数据在存储和转发环节也存在泄露的风险 [2]。此外，设备自身的安全漏洞、网络架构设计不合理以及运维管理措施不到位，进一步导致整个通信系统的安全风险增加。本文从光纤通信技术基础入手，梳理现有安全防护措施，为后续研究提供支持和参考。

【作者简介】赵海伟（1996–），男，中国内蒙古通辽人，硕士，从事通信研究。

2 光纤通信技术核心基础

2.1 光纤通信技术原理

光纤通信是一种利用光传递信息的技术，光纤可以看作是“光传播的通道”。光纤通信是将光电信号与电光信号转换完成信号传输和接收。在信息发送端，用激光器等设备将电信号转变为携带信息的光信号，光信号沿光纤依靠“全反射”原理反射前行，能量损耗小，可实现远距离传输。在接收端，用光电二极管将光信号转换为电信号，处理后解读信息。

光纤有三层结构：最内层纤芯是光传播主要路径，由高纯度二氧化硅制成，折射率高使光不易外泄；中间层包层将光约束在纤芯内传播；最外层涂覆层起到了保护作用，增强耐用性。在通信过程中，光信号的传播速度和距离与光纤材料、光源性能及调制解调技术等存在直接关系。

2.2 光纤通信技术的主流类型

当前，光纤通信类型非常多，根据传输模式、信号类型以及用途的不同进行划分。每一种分类都意味着光纤通信

在不同场景下的技术特点和功能定位，共同构成了现代通信技术。

按照传输模式划分，可以分为为单模和多模两类。单模光纤的线芯极为纤细，直径大约在 8 至 10μm，仅允许一种光信号通过。其优势在于损耗较小、传输距离较远且容量较大，适合应用在长距离传输中。按照传输模式划分，可以分为为单模和多模两类。单模光纤的线芯极为纤细，直径大约在 8 至 10μm，仅允许一种光信号通过。其优势在于损耗较小、传输距离较远且容量较大，适合应用在长距离传输中。多模光纤的线芯相对较粗，通常为 50μm 或 62.5μm，所以可以同时传输许多的光模式，但是传输距离比较短，带宽有限，但是成本低且易于安装，所以适合应用在局域网、近距离接入网 [3]。

按照信号调制方式划分，可以分为数字光纤通信与模拟光纤通信。其中，数字光纤通信采用数字信号，通过对光信号的幅度或频移键控进行调制来传输信息。其优势体现在抗干扰能力强、信号还原度高，且便于进行加密处理。目前，大部分通信应用使用数字光纤通信 [4]。模拟光纤通信则运用模拟信号，调制光信号的幅度或频率，具有较高的传输效率，但是信号失真风险比较高、抗干扰能力较差，所以仅应用于少数的通信场景。

按照复用技术进行分类，主要存在两种技术，分别为波分复用与时分复用。其中，波分复用是将不同波长的光信号整合至同一根光纤中进行传输，大大提升单根光纤的传输容量。时分复用是把时间划分为多个小段，将多个电信号在不同的时间段内整合为一个光信号进行传输，适合应用在中短距离的通信领域。而将波分复用结合时分复用技术，能够提升通信网络的传输效率。

2.3 光纤通信技术的优势与局限

与传统电缆和无线通信相比，光纤通信技术有优势也有局限性。在优势方面，首先，光纤通信技术的带宽大、具有更高的传输速率。单模光纤可传输高达几百 THz 的数据，能够满足高清视频、大文件传输以及语音通话等各种需求。当前常用光纤的传输速度已达 100Gbps，部分地区甚至能超过 1Tbps，完全满足当前数字时代的发展需求 [5]。其次，信号衰减程度低且传输距离长。光在光纤内传播时，能量损耗极小，并且不需要频繁设置中继器，也可以进行远距离不间断传输。最后，具备抗干扰能力。光纤为绝缘材质，不导电且不发射电磁波，尤其适用于工厂、军事等存在强干扰的环境，能够稳定运行，避免信号串扰或受到外界干扰。

光纤通信存在的局限性中，首先是物理层面防护难度较高。光纤线路铺设范围广泛，部分地段如管道外部、电线杆上悬挂的线路均暴露于露天环境，容易遭受人为蓄意破坏受自然灾害损毁，一旦受损通信立即中断。此外，当下私自接入光纤的手段也非常简单，使得物理安全问题更加严重 [6]。其次，光信号容易被不法分子攻击。当前的窃听技术不断发展，利用分光耦合或者光纤弯曲等途径，能够非法截取光信号，并且基本难以察觉。

3 基于光纤通信的电子通信安全技术

3.1 物理链路安全防护技术

3.1.1 线路防护与监测技术

户外光纤线路要想避免自然灾害或者人为破坏，需要将线路埋设至一定深度，或添加管道进行保护；如果是架空线路，则应加装防护套。同时，还需安装光纤监测系统，对光纤的光功率、损耗状况、偏振状态等参数进行实时监测。一旦发现线路出现断裂、弯折，或存在非法接线的情况，系统将立即发出警报，以便维修人员及时进行处理 .

3.1.2 非法接入防护技术

采用加密连接头与防拆接头等零件，防止他人随意拔插光纤或私自接入分光设备。针对重要区域的光纤线路，将其锁入封闭机柜，并安排专人进行监管，非相关人员不得触碰 [7]。此外，为每段光纤添加独一无二的专属加密标记，一旦发现未经授权的标记接入，系统将立即中断通信，从根本上杜绝非法接入的可能性。

3.1.3 信号泄漏防护技术

在进行光纤布线作业时，应当避免光纤出现过度弯曲的情况，防止发生信号泄漏。在传输重要信息的场景中，选用具备不易发生信号泄漏特性的光纤，降低信号泄漏的程度。必须在光纤的两端安装防护罩，既可以抵御外部信号的干扰，又能够防止他人窃取泄漏的信号。

3.2 光信号安全防护技术

3.2.1 光信号加密技术

通信加密存在两种方式：一为链路层加密，二是端到端加密。链路层加密指的是在光纤传输光信号时，直接对光进行加密处理。这一加密方式会变更光的强度、波的相位或者偏振方向等参数，即使中途企图窃取信息者截获信号也无法理解其内容。常见的技术包括光相位加密、光偏振加密，以及当下极为先进的量子密钥分发。该技术运用量子力学原理生成绝对安全的密钥，用于光信号的加密与解密，完全不需要担心被他人窃听。即便密钥被盗用，也无法解开密文。目前，政府、银行等对保密要求极高的领域均已采用链路层加密技术。端到端加密则有所不同。它是先对电信号进行加密，再将其转换为光信号进行传输，接收方收到光信号后，先将其转换回电信号，再进行解密 [8]。这种方法在传输过程中不需要过多关注中间环节的密钥，适合应用在需要经过多个节点的通信场景。

3.2.2 光信号监测与篡改检测技术

安装光信号监测系统，实时检测光信号的功率、波长、相位等。一旦发现信号出现突发异常变化，判断是否存在他人窃听或篡改信息的情况。同时，采用光信号指纹识别技术，为每一路信号生成唯一的指纹。接收端在接收到信号后，首

先核对指纹，指纹不匹配代表信号被篡改，立即停止接收，以防止虚假信息混入。

3.3 数据传输与存储安全技术

光纤通信主要用在数据传输领域，所以必须要具有高速、稳定的传输性能，同时保障数据安全。安全防护工作应贯穿数据从开始传输直至存储完成后的全过程，其核心在于确保数据不泄露、不被篡改且随时可用。

其一，数据传输过程中需进行加密处理。不仅要对信号本身加密，还应对数据采用多种方式进行多层加密。例如，可运用对称加密或非对称加密对数据进行加密，即使数据在传输途中被截取，截取者也无法解读数据内容。而数据需要跨网络、跨地区传输时，可以采用 VPN 技术，借助光纤带宽大的优势搭建一条加密的“专属通道”，将其与外部网络隔离开来，从而提升数据传输的安全性。

其二，需验证数据是否被篡改。例如，可运用哈希算法（如 SHA - 256）为传输的数据计算一个“验证码”，接收方也重新计算该“验证码”并进行比对。当比对结果不一致时，代表数据在传输中途被篡改，需要立即要求重新传输，以确保数据的完整性。此外，还可采用数字签名技术，由发送方对数据进行签名，接收方验证该签名，这样即可以避免数据被伪造、篡改，又能确认发送方身份的真实性 [9]。

其三，数据存储时也需要做好安全防护。光纤网络中存储的数据，如中继节点或核心设备中的数据，必须要加密存储。当设备被盗或遭受黑客攻击，也不会发生数据泄露风险。同时，应部署备份系统，定期对核心数据进行备份，最好将备份数据存储于不同地点。当发生天灾或设备故障，数据也不会丢失，可以随时恢复。此外，还应做好权限管理工作，为不同人员分配不同的访问权限，防止有人随意查看、篡改其无权访问的数据。

3.4 网络架构安全优化技术

良好的网络架构可以增强光纤通信的抗攻击能力，降低安全风险。具体而言，主要有以下几种举措：

其一，做好备份设计。例如，采用两条线路、两套设备，为重要的通信线路及核心设备均准备备用方案。当主线路或主设备出现故障时，系统能够立即切换至备用部分，确保通信不中断，避免因一处损坏而致使整个网络瘫痪。

其二，对网络进行分区隔离。根据业务类型和数据的敏感程度，将整个通信网络划分为不同的安全区域，如核心区、业务区和接入区。运用防火墙、隔离设备将这些区域分隔开，对相互访问进行控制。这样即使某个区域被攻破，攻击也不会蔓延至整个网络。针对特别敏感的数据，还可以采用专门的线路进行传输，不与普通业务混合，以提升安全性。

其三，强化路由安全。选择安全程度更高的路由协议，例如具备防篡改功能、带有安全认证的 OSPFv3 或 BGP 扩展版，防止路由被欺骗或劫持。同时，设置路由监控系统，实时监测路由信息是否存在异常变化，及时发现问题情况，阻止非法路由接入。合理规划数据传输路径，减少中转次数，也能够使数据传输更加稳定、安全 [10]。

其四，部署入侵检测和防御系统。利用专门的 IDS 和 IPS 设备实时监测网络流量和数据传输行为，识别端口扫描、数据篡改、非法接入等恶意攻击，及时报警并进行拦截。再结合大数据和人工智能技术，对异常行为进行分析和预测，使网络能够更主动地进行防御，提前抵御可能出现的安全威胁。

4 结语

光纤通信技术的核心在于使信息借助光在光纤中实现高速传输。本文对其工作原理、常见类型以及优缺点进行了分析，并且探究了电子通信安全的保护策略。所以，从光纤线路、光信号、数据存储传输以及网络结构等方面，构建了一套全面的安全保护方案。各项技术协同配合，能够有效防范各类安全风险，增强整个通信网络的安全性。保障物理线路安全是基础，对光信号进行加密与监控是核心，确保数据安全是关键，优化网络结构则是支撑。只有各个环节落实到位，才可以确保光纤通信安全且稳定地运行。

参考文献

[1] 谢丽君,彭建军.基于光纤通信的车载电子通信安全技术分析[J].数字技术与应用,2024,42(10):51-53.

[2] 仲伟.光纤通信技术在基层电子信息工程中的应用[J].移动信息,2025,47(8):481-483.

[3] 王梦琪.工程电子信息中光纤通信高速率传输技术探索[J].漫科学(科技应用),2025(6):25-27.

[4] 王慧龙,吴新.基于光纤通信技术的车载电子通信安全技术[J].通信电源技术,2023,40(2):155-157+161.

[5] 史慧玲.基于光纤通信技术的车载电子通信安全技术研究[J].移动信息,2023,45(8):28-30.

[6] 欧阳李亮,陈白昀.基于光纤通信技术的车载电子通信安全技术研究分析[J].通信电源技术,2022,39(2):151-153.

[7] 裴雅,李亚珂.数据加密技术在计算机网络通信安全中的应用探究[J].信息记录材料,2025,26(4):87-89.

[8] 黄秋艳,夏靖,王号,孟凡森,宋海涛.光缆线路故障告警技术在光纤通信工程中的应用[J].移动信息,2025,47(5):81-83.

[9] 索国杰,王宇雁.量子秘钥分发的光纤通信安全技术研究[J].高科技与产业化,2024,30(8):34-35.

[10] 彭晓黎.基于光纤通信技术的车载电子通信安全技术[J].电子技术与软件工程,2019(3):19-19.