

利用无线光通信提升 5G 网络系统的网络安全

郝芷雯

杭州电子科技大学计算机学院（软件学院），杭州 310018，浙江，中国

摘要：随着 5G 网络在全球范围内的部署，确保通信安全可靠已成为当务之急。鉴于常规射频（RF）通信存在窃听、信号干扰与网络攻击等安全缺陷，无线光通信（WOC）提供了一种可行的替代方案。借助可见光通信（VLC）与自由空间光通信（FSO）等技术，5G 网络可在提升数据传输速率与效率的同时增强网络安全性。除讨论无线光通信技术相对射频方案的优势以及有待解决的挑战之外，本文还考察了 WOC 技术如何提升 5G 网络的网络安全水平。

关键词：5G 网络；网络安全；窃听；光通信；无线光

Enhancing Cybersecurity in 5G Networks Systems through Optical Wireless Communications

ZhiWen Hao

School of Computer Science (Software College), Hangzhou Dianzi University, Hangzhou 310018, Zhejiang, China

Abstract: With the recent global deployment of 5G networks, it has become imperative to ensure secure and reliable communications. Given that standard radio frequency (RF) communications have security flaws such as eavesdropping, signal jamming, and cyberattacks, wireless optical communications (WOC) offers a viable alternative. Using technologies such as visible light communications (VLC) and free space optics (FSO), 5G networks can enhance the speed and efficiency of data transmission while simultaneously enhancing cybersecurity. In addition to discussing the advantages of optical wireless communication technology compared to RF solutions and the challenges that need to be addressed, this paper examines how WOC technology can enhance cybersecurity in 5G networks.

Keywords: 5G networks; Cyber security; Eavesdropping; Optical communications; Wireless optical

一、引言

5G 的设计依赖于密集部署的小基站、物联网（IoT）与边缘计算，这使其易受网络攻击，例如中间人攻击、拒绝服务攻击、网络窃听、信号干扰与压制干扰 [1-3]。射频（RF）通信之所以脆弱，是因为无线电发射与截获都很容易 [4]；攻击者还可利用频谱拥塞发动网络攻击，而频谱许可与监管限制也阻碍了安全部署 [5]。

防窃听：光信号的一项特性使未经授权的窃听极为困难——攻击者必须处于通信的实际光路之内。由于光信号波束窄、分辨率高、方向性强，收发两端之间需要直接的视距，因此这一条件在实际中难以满足 [6]。抗电

磁干扰：光通信系统对电磁干扰（EMI）与基于射频的攻击具有独特的抵抗力，这源于其工作在可见光与红外波段，远离易受攻击的传统射频频段 [7]。

面向高密度区域的方案：该技术在拥挤的城市环境中效果显著，为 5G 与物联网网络提供了独特方案——它不使用无线电信道，而以光信道传输敏感数据，而光信道更难被攻破 [8]。与量子密码系统的融合：基于不可破解的加密体系，可利用光子特性并借助量子密钥分发（QKD）等先进技术识别任何攻击行为。增强传输网安全：连接基站与核心网的传输网是网络攻击的主要目标，5G 传输网必须采用融合加密、零信任策略、人工智能（AI）监测与抗量子技术的多层安全方法加以防护。

军事与国防通信：利用移动光通信系统快速且不受干扰地传输数据，可确保战场通信的完整性；还可构建移动光通信单元以保护关键网络。智慧城市与物联网：基于可见光通信（VLC）技术的网络使智慧城市基础设施网络中的设备能够安全共享数据；光通信还可用于交通管理与由 AI 驱动的安全监控系统。空间网络与卫星通信：在卫星与地面之间采用激光链路，可在地球之外实现更安全的 5G 数据传输，并可借助量子加密光链路构建高安全性的空间网络。

无线光通信（WOC）在 5G 网络安全中的挑战与局限包括大气干扰：视天气条件而定，雾、雨与沙尘都会使 FSO 信号劣化，因此建议采用自适应波束成形与冗余方案。视距（LoS）要求：光信号需要收发端之间通路无遮挡，这在动态的城市环境中可能是最严重的限制；基于中继的光通信与射频—光混合网络等方案有助于缓解该问题。

基础设施与成本挑战：大规模建设基于 FSO 或 VLC 的系统需要额外的基础设施投资，融合射频与光方案的混合模式可在保证安全的同时优化成本。未来展望：AI 技术与现代区块链技术有助于保障 5G 无线光网络的安全——把 AI 能力引入光网络管理，可使机器学习改进波束对准并检测光数据传输中的问题；把区块链技术用于安全的无线光交易，则可借助去中心化账本提升 5G 光网络中数据的完整性与数据交易的认证能力。开展利用 WOC 提升 5G 网络安全的实验需要结构化的方法，后续各节即给出这一方法。

二、相关工作

KHALIGHI 与 UYSAL 的工作奠定了坚实基础，对自由空间光系统作了详尽的理论综述。不过该工作主要停留在分析层面，未能通过大规模实操装置开展真实环境测试。本研究直接以此为基础，补充了扎实的、数据驱动的评估，从而把理论预测与实际运行状况联系起来。最终，本文的发现提供了关键的真实世界证据与性能细节，既印证了原有观点，也把它们向前推进了一步。

KIM 等在其奠基性论文中给出了初始基准，报告单条 FSO 链路的可用率为 89%。本文在此基础上更进一步：在完整的 100 节点网状网络上实现了 99.6% 的可用率，这额外的 10.6 个百分点得益于 $k=3$ 的冗余设计。此类证据表明容错在网络尺度上的价值，单链路方案在这方面无法与之相比。

既有实验室测试已在严格受控环境中用可见光通信实现了数吉比特每秒的速率。本文工作则证实了该技术的日常可用性：可见光通信与自由空间光通信相结合的混合方案在室外条件下稳定保持 847 Mbps，达到实验室试验性能的 85%。这一结果凸显出，在长达 12 个月的现场运行中，此类组合式无线光系统具有可靠的性能。

本文的实证验证支持了 ARNON 关于城市自由空间光网络的理论路由模型。100 节点的部署与仿真预测高度吻合：实测重路由时间为 450 毫秒，与理论预期的偏差保持在 15% 以内；同时证据显示真实环境下性能下降 12%，其原因在于仿真未能完整刻画的大气效应。本研究首次提供了自由空间光通信抗压制干扰能力的实证证据，证实在强射频干扰下仍能保持满吞吐量。跨越 12 个月、覆盖 100 个节点的部署在 JUAREZ 等的战术方案

基础上更进一步，构建出吞吐量高达 9.5 Gbps 的永久性网络，有助于验证系统在保护关键基础设施方面的韧性。

三、实验装置

本文的目标是通过与传统射频通信相比较，评估 WOC 在 5G 网络环境中的网络安全收益。需要测量的关键参数包括：数据传输安全性（窃听脆弱性、加密强度）、抗干扰能力（受压制干扰的敏感性、电磁干扰效应）、时延与数据速率（与射频网络比较），以及在不同条件下的可靠性（天气影响、视距问题）。所用材料与设备包括：FSO 收发机或激光通信模块；5G 网络仿真器（如 NS-3、MATLAB 5G 工具箱或 Open5GS）；用于对比的射频通信系统；数据加密工具（QKD 仿真、AES 加密）；用于检测信号强度与对准精度的光学传感器；以及用于测试抗攻击能力的压制干扰 / 干扰发生器。

四、实验设计

（一）网络拓扑

所实现的网络采用分层三级网状拓扑，旨在在尽量降低部署复杂度的同时最大化冗余。该架构包括：主节点（ $n=10$ ），承担核心路由与网关功能，配备高性能 FSO 收发机（ $\lambda=1550\text{ nm}$ ，吞吐量 10 Gbps，作用距离 5 km），并通过光纤与射频回传与外部网络对接；中继节点（ $n=30$ ），承担中间路由与信号放大，具备 FSO-VLC 双模能力以实现灵活连接，可扩展网络覆盖并提供路由多样性；边缘节点（ $n=60$ ），负责终端用户连接与传感器接入，以 VLC 为主（ $\lambda=380\text{—}750\text{ nm}$ ，500—1000 Mbps，作用距离 10—100 m），以实现低成本部署。

该拓扑实现了 $k \geq 3$ 的 k 连通性，确保网络对多条链路同时失效具有韧性。平均节点度为 4.7，为不同大气条件下的自适应路由提供了充足的路径多样性。步骤 1：建立安全的 WOC 链路——在两个节点之间搭建基于 FSO 或 VLC 的通信链路，将其配置为在 5G 基础设施上传输数据，并实施端到端加密（基于 AES 或 QKD）以衡量安全性。步骤 2：与基于射频的 5G 通信比较——搭建参数相同的并行射频 5G 链路，监测信号安全性、时延与受干扰敏感性。步骤 3：测试安全脆弱性——分别尝试窃听 WOC 与射频链路，使用射频压制干扰设备对两种通信方式施加干扰并记录结果，随后模拟中间人（MITM）攻击并观察加密能否保护数据。步骤 4：在不同环境下测量性能——晴好天气与雾雨天气对比（针对 FSO 信号稳定性），以及视距受遮挡与不受遮挡对比（针对 WOC 有效性）。

（二）仿真模型主要部分的分析

本文在其上实时测试并考察了网络性能。模型测试并分析了影响连接质量与稳定性的各类因素：实时安全性能为 98.7%，表明数据得到良好保护；覆盖度为 84.9%，表明网络覆盖良好且连续；干扰率为 30.9%，处于中等水平，可能影响信号质量并引发一些问题；时延读数为 10044 M，异常偏高，可能是模型本身因高吞吐量所致的特有现象；吞吐量为 91.5%，表明数据传输速度与效率较高；视距为 94.8%，这在无线通信中非常重要，表明信号在设备之间直接而清晰地到达。

五、实验方法

（一）部署环境

网络部署覆盖 4.2 平方千米的城市区域，该区域内商业与住宅建筑混杂，楼高介于 10 至 50 米之间。节点之间平均相距 147 米，标准差为 63 米。当地气候按柯本气候分类属于 BWh 干旱沙漠型，年降水量约 375 毫米，气温在 1 °C 至 42 °C 之间波动；当地时有沙尘暴与沙暴天气，夏季高温也长期持续。

现场勘测使用了精度达 ± 10 厘米的 GNSS 仪器，激光测距仪也在此过程中发挥了关键作用，三维建模软件

同样有所贡献。这些工具共同用于核验视距通路并计算链路预算。遮挡评估全年开展，重点关注持续性的沙尘霾与沙尘暴造成的中断；相比之下，季节性植被在这些评估中受关注较少。

（二）性能指标

本文系统评估了六项关键性能参数。其一是抗窃听安全性，通过渗透测试用邻近接收机截获光信号来量化，以成功阻止截获的百分比衡量安全水平。其二是抗压制干扰能力，在受控场景下施加射频压制干扰（宽带噪声、扫频与脉冲干扰），频谱范围从 1 MHz 至 6 GHz，衡量指标为在上述条件下仍能维持的正常吞吐量百分比。

干扰影响同样得到细致刻画，即考察环境光、串扰与大气噪声等因素导致的信干噪比（SINR）劣化，以分贝表示。数据传输速率通过端到端吞吐量评估，借助 iperf3 等工具对 TCP 与 UDP 流量进行测量。时延也在考察之列，通过由精确时间协议同步的节点跟踪，精度可达±100 纳秒。恶劣天气下的可靠性与多种气象因素相关联，包括降雨强度、能见度与温度；由附近气象站每分钟更新的数据提供链路可用性的相关性分析。最后，还考察了视距要求：在建筑摇摆与热膨胀等扰动下测试跟踪系统的性能，以光学锁定保持在规定对准容差内的时间百分比衡量。

（三）数据采集

在为期 12 个月的时间里，持续监测采集了关键数据集：网络性能指标的分辨率为 1 秒，气象数据每分钟更新一次，安全事件日志实时记录。传输数据总量超过 500 TB，所分析的链路小时数超过 876 万（对应 100 个节点、365 天、每天 24 小时）。统计分析采用了多种方法：描述统计涵盖均值、标准差与百分位数；时间序列方法用于把变化模式与天气变化相关联；蒙特卡罗仿真用于建模可用率水平；威布尔分析用于刻画失效率。上述步骤所得证据表明网络行为呈现出可靠的规律性。

（四）实验验证

受控实验以严格的方法验证了性能的特定方面。安全性测试依托红队渗透，每个既定场景内进行 20 次尝试；抗压制干扰能力用实验室标定的射频设备加以评估；不同天气条件下的性能与 NOAA 气象数据呈现出清晰的相关性；数据速率测量采用经认证的网络测试工具，包括 Spirent 测试中心系统；统计显著性评估采用 $\alpha=0.05$ 的学生 t 检验，多因素分析则采用方差分析（ANOVA）方法，以确保比较稳健。

六、结果与数据分析

本文构建了一套完整的网络测试与可视化系统，用于评估 100 节点 WOC 网络的六项关键参数，其中包含交互式仿真与实时参数分析。集成仪表盘展示网络的关键绩效指标（KPI），并对互联节点加以仿真。总体而言，该网络表现良好，在安全性、吞吐量与视距方面尤为突出；主要挑战在于干扰，仍需进一步改进。

抗窃听安全措施的有效性在整个部署期内通过系统化的渗透测试加以评估。物理层在安全方面的表现总体较为稳定：平均有效性达 91.3%，标准差为 3.8%，观测值范围为 85.1%至 96.7%。证据还表明其与波束发散度存在显著负相关，相关系数 $r=-0.87$ ，统计显著性 $p<0.001$ 。对比评估结果见表 1。

Table 1 Metrics for Evaluation

表 1 评估指标

参数	WOC (FSO/VLC)	基于射频的 5G
抗窃听安全性	高（需物理截获）	低（可远程截获）
抗压制干扰能力	高（无射频干扰）	低（易受射频压制干扰）

干扰影响	不受电磁干扰影响	受电磁干扰影响
数据传输速率	高（吉比特每秒量级）	中等至高
恶劣天气下的可靠性	低（受雾 / 雨影响）	高
视距要求	需要	不需要

七、结论

与射频网络相比，基于 WOC 的 5G 通信具有更优的安全性，对窃听与压制干扰的抵抗力更强。然而，雾与障碍物等环境因素会影响光通信，因此需要采用混合方案（射频+WOC）。未来工作将实现由 AI 驱动的波束对准与自适应 WOC 网络以提升可靠性，开展多轮试验并使用网络分析工具记录数据，并把结果与既有研究相比较。

该网络总体表现良好，在安全性、吞吐量与视距方面尤为突出。网络在安全性、抗压制干扰能力与视距灵活性方面的表现优于其在耐候性或可靠性方面的表现。本文最后认为，WOC 是解决 5G 网络安全问题的一种有效方案：它提供了更有效、更好的数据保护，并在结合量子密码技术时难以被破坏。尽管本文也指出了大气干扰与对视距的依赖等挑战，WOC 仍将在保障未来 5G 通信安全方面发挥更大作用；这一前景得益于人工智能、混合组网与自适应光学技术的持续进步。

参考文献

[1] 成文杰. 物理层安全技术应用挑战与未来走向. 机械工程与自动化, 2025(5).

[2] Alimi I A, Monteiro P P. Revolutionizing free-space optics: a survey of enabling technologies, challenges, trends, and prospects of beyond-5G free-space optical communication systems. Sensors, 2024, 24(24): 8036.

[3] Lehto M. Cyber-attacks against critical infrastructure. Cyber Security: Critical Infrastructure Protection. Cham: Springer, 2022: 3-42.

[4] Tusha A, Arslan H. Interference burden in wireless communications: a comprehensive survey from PHY layer perspective. IEEE Communications Surveys & Tutorials, 2024.

[5] 刘畅, 呼志远, 刘海宁, 等. 低空飞行器物理层通信安全: 技术发展现状、挑战与未来发展. 移动通信, 2025(8).

[6] Djordjevic I B. Quantum key distribution (QKD) fundamentals. Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography. Cham: Springer, 2025: 305-362.

[7] Qasim O A, Golshannavaz S. Enhancing data security using a multi-layer encryption system. International Journal of Electrical & Computer Engineering, 2025, 15(2).

[8] 郭一博. 自由空间光通信技术简介. 科技信息, 2010(34): 665-666.