

doi:10.13756/j.gtxyj.2022.03.002

光通信系统与网络技术

一种基于混合光加密的物理层安全方法

巩小雪¹, 宣 冉¹, 张琦涵², 李 瑞¹

(1. 重庆邮电大学 通信与信息工程学院, 重庆 400065; 2. 东北大学 计算机科学与工程学院, 沈阳 110819)

摘要:针对目前光网络物理层面临的窃听安全问题, 文章提出了一种基于高非线性光纤(HNLF)和超结构光纤布拉格光栅(SSFBG)新的混合光加密方案。方案中采用简并四波混频(FWM)效应对用户信息进行加解密, 并采用光编码技术对密钥信息进行编解码, 编码的同时实现了密钥信号的隐匿传输。通过对比信道中传输的加密信号波形和原始发送信号波形衡量系统的安全性, 并通过系统接收端误码率来衡量系统的有效性。仿真结果表明, 使用了文章所提新的混合光加密方案后, 用户数据信息的频率和相位发生扰乱, 编码后的密钥信号光功率低至 -34.4 dBm, 因此窃听信道既无法得到有效数据信息, 也检测不到密钥信号, 从而实现了正交相移键控(QPSK)信号的安全传输。

关键词:光加密; 光编码; 隐匿传输; 高非线性光纤; 超结构光纤布拉格光栅

中图分类号: TN918.6

文献标志码: A

文章编号: 1005-8788(2022)03-0007-04

A Physical Layer Security Method based on Hybrid Optical Encryption

GONG Xiao-xue¹, XUAN Ran¹, ZHANG Qi-han², LI Rui¹

(1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; 2. School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China)

Abstract: Aiming at the current eavesdropping security issues in the physical layer of optical networks, a new hybrid optical encryption scheme based on Highly Nonlinear Fiber (HNLF) and Super Structured Fiber Bragg Grating (SSFBG) is proposed in this paper. In the scheme, degenerate Four Wave Mixing (FWM) is used to encrypt and decrypt user information, and optical coding technology is used to encode and decode the key information. Therefore, the encoding and secret transmission of the key signal can be realized simultaneously. The security of the system is measured by comparing the waveform of the encrypted signal transmitted in the channel with the waveform of the original transmitted signal, and the effectiveness of the system is measured by the bit error rate at the system receiver side. The simulation results show that the frequency and phase of the user data information are disturbed, and the optical power of the encoded key signal is as low as -34.4 dBm. Therefore, the eavesdropping channel cannot obtain effective data information nor detect the key signal, which demonstrates the safe transmission of Quadrature Phase Shift Keying (QPSK) signal.

Key words: optical encryption; optical coding; hidden transmission; HNLF; SSFBG

0 引 言

随着第五代移动通信(5th Generation Mobile Communication Technology, 5G)技术落地, 网络数据量急剧膨胀, 光纤通信的高容量特性使得光纤在成为承载大量数据主要载体的同时, 光纤中数据的传输也遭受了各种安全威胁^[1-3]。目前应用广泛的加密手段包括上层加密和物理层加密。上层加密技术缺乏对认证控制帧以及加密报头的保护, 同时存在复杂的密钥管理问题。光学系统的物理层加密(简称光层加密)利用光信号处理固有的高速和并行性, 不仅为上层数据提供了安全防护, 同时也为光纤上的透明传输数据提供了安全保护。

光层加密可以对全部数据进行加密, 同时避免了可监视的电磁特征。光层加密的方法主要包括基

于非线性四波混频(Four Wave Mixing, FWM)效应的光加密^[4-6]、光码分多址^[7-8](Optical Code Division Multiple Access, OCDMA)技术和混沌光加密^[9-10]。目前, 基于 FWM 效应的光加密方案主要通过半导体光放大器实现, FWM 加密效果并不理想。同时为了防止 FWM 效应中的泵浦波信号在信道中被窃听, 泵浦波信号需要一个单独的安全信道进行传输, 但是目前并没有通信协议指定标准的安全信道。

针对系统安全性不足的问题, 本文提出了一种基于高非线性光纤(Highly Nonlinear Fiber, HNLF)简并 FWM 效应进行用户信息加密, 同时也基于超结构光纤布拉格光栅(Super Structured Fiber Bragg Grating, SSFBG)对密钥进行编码的混合光加密方案。

收稿日期: 2021-10-07

基金项目: 国家自然科学基金资助项目(62075024, 61801105); 重庆市自然科学基金资助项目(cstc2019jcyj-msxmX0615)

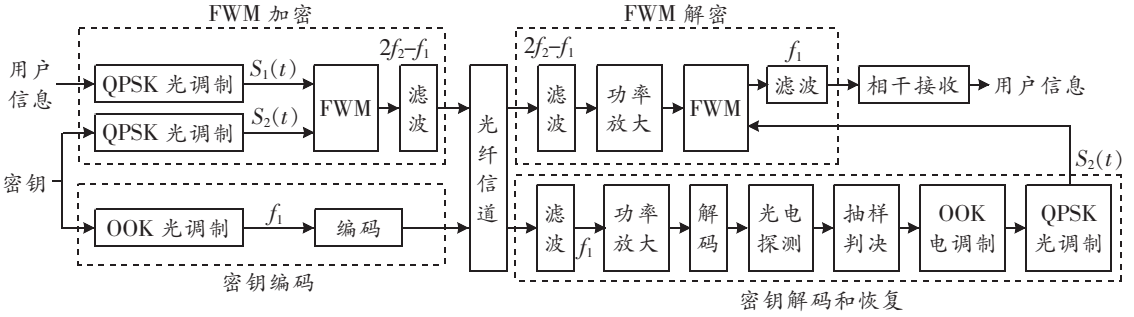
作者简介: 巩小雪(1988—), 女, 辽宁沈阳人。副教授, 博士, 主要研究方向为光接入网信号损伤补偿技术、高速安全光传输理论及技术、数字信号处理算法设计与实现。

通信作者: 宣冉, 硕士。E-mail: xuanran0108@foxmail.com

1 混合光加密原理分析

正交相移键控 (Quadrature Phase Shift Keying, QPSK) 信号的混合光加密方案主要由两个部

分组成,分别为 QPSK 信号加解密和密钥的隐匿传输。图 1 所示为本文所提 QPSK 信号的混合光加密系统原理结构图。



注: $S_1(t)$ 为用户 QPSK 光信号; $S_2(t)$ 为密钥 QPSK 光信号; t 为时间; f_1 为用户 QPSK 光信号的频率; f_2 为密钥 QPSK 光信号的频率; OOK 为开关键控。

图 1 QPSK 信号的混合光加密系统原理结构图

为提升 QPSK 信号光传输系统的加解密效果,本文考虑使用简并形式非线性 FWM 效应对 QPSK 信号进行加密。用户数据信息存在于 QPSK 信号的相位 θ_1 中,信号 $S_1(t) = \exp(j2\pi f_1 t + \theta_1)$,其中 j 为复数虚部单位,相位 $\theta_1 \in \{\pi/4, 3\pi/4, -\pi/4, -3\pi/4\}$ 。同样,经过 QPSK 调制的密钥 $S_2(t) = \exp(j2\pi f_2 t + \theta_2)$,相位 $\theta_2 \in \{\pi/4, 3\pi/4, -\pi/4, -3\pi/4\}$ 。图 2 所示为 FWM 加解密过程,图 2(a) 所示为 FWM 加密过程。承载用户信息的 QPSK 信号波与承载密钥信息的 QPSK 泵浦波在 HNLF 上发生简并 FWM 效应,会产生频率为 $f_3 = 2f_2 - f_1$ 、相位为 $\theta_3 = 2\theta_2 - \theta_1$ 的闲频波。这是由于纤芯中光功率密度过高,诱导了光纤材料的非线性极化,导致脉冲之间发生了能量转移,从而产生新的频率信号。FWM 效应是属于光纤的非线性极化所引起的一种光纤非线性效应。满足相位失配条件,即波矢和频率的匹配,则 $\Delta k = 2\beta_2 - \beta_1 - \beta_3 = 0, \omega_3 = 2\omega_2 - \omega_1$,且对应 $\theta_3 = 2\theta_2 - \theta_1$ 。式中: Δk 为相位失配条件; ω_2 为泵浦波角频率; ω_1 为信号波角频率; ω_3 为 FWM 产生的闲频波角频率; β_j 为角频率为 ω_j 的光信号传播常数; θ_j 为角频率为 ω_j 的光信号的相位。FWM 解密过程如图 2(b) 所示。加密信号作为信号波与承载密钥信息的 QPSK 泵浦波在 HNLF 上再次发生简并 FWM 效应,生成频率 f_1 、相位 θ_1 的闲频波,恢复用户信息。

本方案中,为了防止密钥在信道中被窃听,采用 6 码字相移型 SSFBG 作为编码器对密钥信号进行编解码,同时实现密钥的隐匿。图 3 所示为一个码字为 $\pi 0 \pi \pi 0 0$ 相移型 SSFBG 折射率的变化图样。

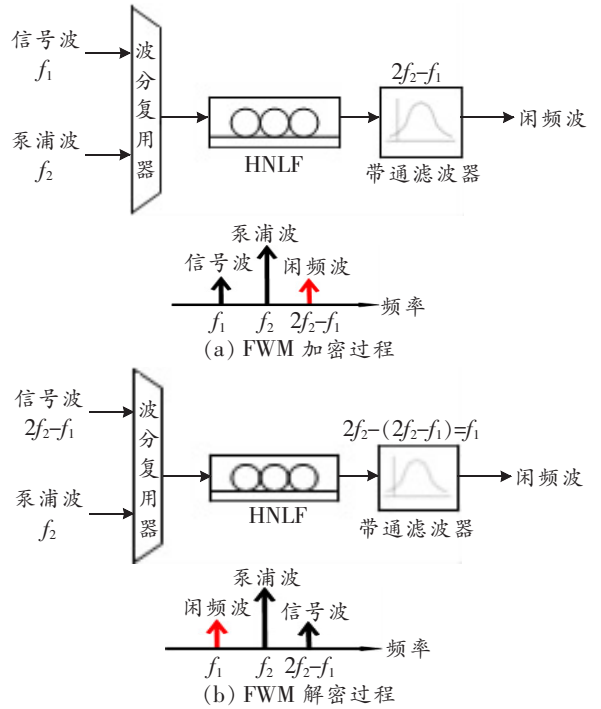
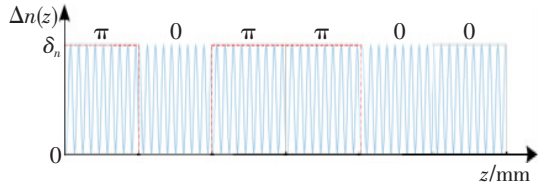


图 2 FWM 加解密过程



注: $\Delta n(z)$ 为 SSFBG 的折射率变化函数; z 为光栅长度; δ_n 为平均折射率变化。

图 3 码字为 $\pi 0 \pi \pi 0 0$ 相移型 SSFBG 折射率变化图样

在 SSFBG 满足弱耦合近似时,结合耦合模式理论^[11]分析可知,光栅的反射谱 ρ 满足

$$\rho = i \int \kappa(z) e^{i2\pi\chi z} dz,$$

式中: i 为复数虚部单位; $\chi = 2n_{\text{eff}}(f - f_B)/c$, n_{eff} 为光纤有效折射率, f 为光栅入射信号的频率, f_B 为布拉格频率, $f - f_B$ 为光电场频率相对光栅布拉格频率的偏移量, c 为光速; 耦合系数 $\kappa(z) = \pi f_B \Delta n(z)/c$, $\Delta n(z) = \sum_{j=1}^6 \delta_n \cos(2\pi z/\Lambda + \varphi_j(z))$ 为相移 SSFBG 的折射率变化函数, Λ 为光栅的布拉格周期, $\varphi_{1,3,4} = \pi$, $\varphi_{2,5,6} = 0$ 。分析可知, 光纤布拉格光栅的折射率结构与其反射频响之间满足傅里叶变换关系。密钥信号的编解码过程中, 发送端 OOK 信号经过相移 SSFBG 时, 反射出的编码信号相当于入射信号经过系统响应 $h(t) = |2n_{\text{eff}}/c| \kappa(2tn_{\text{eff}}/c)$ 作用后的信号; 接收端经过匹配的光栅解码器, 密钥可以恢复出来, 并且因为光栅的平均折射率变化系数 δ_n 很小, 光栅频响特性 $h(t)$ 的峰值很小, 这将导致经过 SSFBG 后的编码信号功率远低于 FWM 加密信号的光功率。相移 SSFBG 不仅实现了对密钥的编解码, 还降低了编码后信号的光功率。因此, SSFBG 编码器提高了密钥的隐匿传输能力和安全性。

2 仿真设置与结果分析

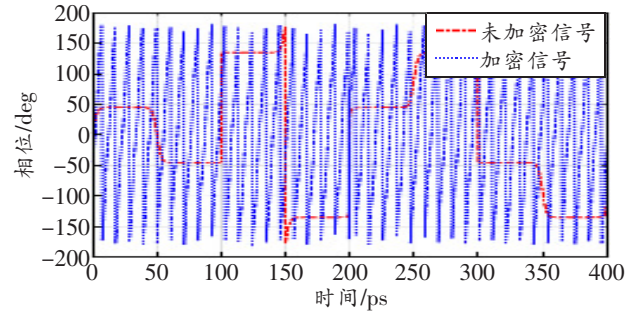
本文使用 VPI Transmission Maker 9.5 仿真验证所提系统方案的性能。基本组件的仿真参数设置如表 1 所示。

表 1 基本组件的仿真参数

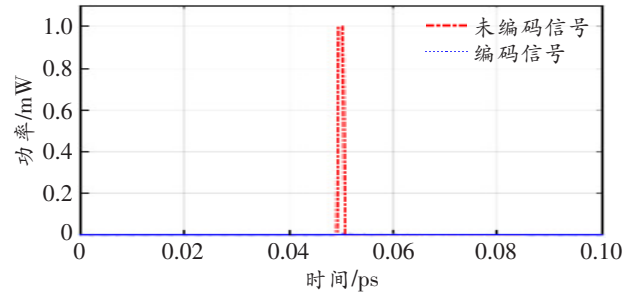
组件	变量	变量
1 激光器	频率 1: 193.389 5 THz	光功率 1: 1 mW
	频率 2: 193.576 8 THz	光功率 2: 30 mW
2 HNLF	长度: 200 m	非线性系数: 326.4e-22 m ² /W
3 SSFBG	布拉格周期: 533.912 3 nm	有效折射率: 1.450 9
	长度: 3.6 mm	码字: $\pi 0 \pi \pi 0 0$
4 标准单模光纤	长度: 50e3 m	衰减: 0.2 dB/km
5 掺铒光纤放大器	色散: 16e-6 s/m ²	色散斜率: 80 s/m ³
	增益控制时	功率控制时输出
	增益: 30 dB	光功率: 1 mW

图 4 所示为混合光加密方案的仿真结果。图 4(a) 所示为 FWM 加密前后信号的相位谱。由图可知, 已经无法直接从加密后相位谱中恢复出原始信号的相位信息。图 4(b) 所示为密钥信号编码前后的波形。编码后, 信号在时域上有规律的展宽, 同时功率下降, 低至 -34.4 dBm。编码前后的功率差有利于信号的隐藏, 当信道遭到非法用户窃听时, 小功

率密钥信号会极大增加窃听合法信息的难度, 保证数据安全性。



(a) FWM 加密前后信号的相位谱



(b) 密钥信号编码前后的波形

图 4 混合光加密方案的仿真结果

图 5 所示为接收端误码率仿真结果。接收端, 要恢复用户数据, 首先需要恢复密钥。通过提高解码信号接收光功率 (Received Optical Power, ROP) 和改变抽样判决阈值, 系统可以实现用户数据的无误码传输。由图可知, 随着解码信号 ROP 的上升, 接收端误码率呈下降趋势。当解码后抽样判决阈值为 5.8×10^{-6} 时, 解码信号 ROP 接近 -25.5 dBm, 就可以实现系统的无误码传输。由图中曲线对比分析可知, 当解码后抽样判决阈值降低 0.8×10^{-6} , 解码信号 ROP 降低约 0.4 dBm 也可以实现系统的无误码传输。

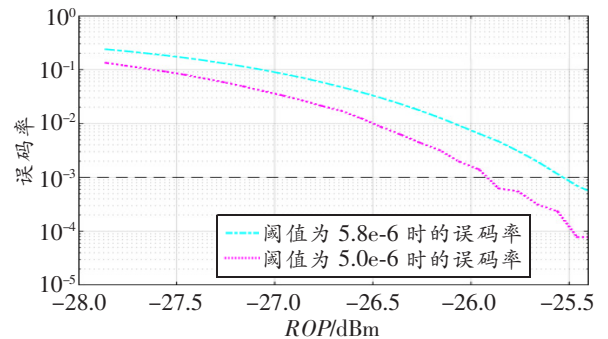


图 5 接收端误码率

3 结束语

本文提出了一种针对物理层数据安全问题的混合光加密方案。该方案不仅可以为物理层数据提供

加密防护,还可以有效防止信道窃听。然而,对于高密度波分多路复用技术来讲,更多的信道意味着信道之间干扰更加严重,这对于密钥的恢复将是一个重要挑战,需要选择合适的码型和码字长度,这也是未来需要继续研究的内容。

参考文献:

[1] Gong X,Zhang Q,Zhang X,et al. Security Issues and Possible Solutions of Future-Oriented Optical Access Networks for 5G and Beyond[J]. IEEE Communications Magazine, 2021, 59(6):112—118.

[2] Fok M P, Wang Z, Deng Y, et al. Optical Layer Security in Fiber-optic Networks[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 725—736.

[3] Shaneman K,Gray S. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection & Prevention[C]//IEEE MIL-COM 2004. Monterey,CA,USA:IEEE,2004,2:711—716.

[4] Zhang Q, Gong X, Guo L. All-optical Pattern Recognition of QPSK Signals for High Speed Optoelectronic Firewalls [C]//Asia Communications and Photonics Conference. Beijing, China: Optical Society of America, 2020:M4A. 199.

[5] 杨玮. 基于 SOA-FWM 的 DQPSK 光信号加/解密方案[J]. 北京信息科技大学学报(自然科学版), 2018,

33(2):60—65.

[6] Zhang M, Cui Y, Zhan Y, et al. Optical Encryption/Decryption of 8PSK Signal Using FWM-based Modified XOR[J]. Applied Optics, 2015, 54(25):7813—7819.

[7] Li P, Wang Y, Lan Z, et al. Research on the Coding and Decoding Technology of the OCDMA System [C]//Sixth International Conference on Electronics and Information Engineering. Dalian, China: International Society for Optics and Photonics, 2015, 9794: 97940U.

[8] Liu X, Wang L. Chaotic OCDMA System based on Superstructure Fiber Bragg Grating[J]. Journal of Optoelectronics Laser, 2014 (5):876—880.

[9] Li X, Pan W, Luo B, et al. Mismatch Robustness and Security of Chaotic Optical Communications based on Injection-locking Chaos Synchronization [J]. IEEE Journal of Quantum Electronics, 2006, 42(9):953—960.

[10] Rontani D, Locquet A, Sciamanna M, et al. Multiple-access Optical Chaos-based Communications using Optoelectronic Systems [C]//Conference on Lasers and Electro-Optics. San Jose, California ,USA: Optical Society of America, 2010:CFC5.

[11] Erdogan T. Fiber Grating Spectra [J]. Journal of Lightwave Technology, 1997, 15(8):1277—1294.

