

doi:10.13756/j.gtxyj.2025.250314.

专题:纪念创刊50周年

安跃华,唐斌,刘江伟,等. 电光反馈混沌保密系统时延标签特征隐藏研究[J]. 光通信研究, 2025(6): 250314.

An Y H, Tang B, Liu J W, et al. Research on the Time Delay Signature Concealment of Electro-Optic Feedback Chaotic Communication System [J]. Study on Optical Communications, 2025(6): 250314.

电光反馈混沌保密系统时延标签特征隐藏研究

安跃华¹,唐斌²,刘江伟¹,高震森²

(1. 广东技术师范大学 光电工程学院,广州 510665; 2. 广东工业大学 信息工程学院 通感融合光子技术教育部重点实验室,广州 510006)

摘要:【目的】混沌激光保密通信通过硬件加密,具有高速率、长距离和与经典光纤信道相兼容的优势,可为高速光纤通信系统提供物理层安全保障。针对传统电光反馈混沌加密系统中环路时延泄露而导致的安全性问题,文章提出了一种可隐藏电光反馈时延标签(TDS)特征的混沌保密光通信系统。【方法】通过耦合外部余弦信号进入电光反馈环路进行相位调制,利用余弦信号在自相关和延时互信息曲线中的周期性来掩盖原有电光反馈环路的TDS特征,避免环路时延物理参数被窃听者破解,进而充分保障了电光反馈加密结构的物理层安全。【结果】文章详细分析并对比了有无外部耦合信号及不同耦合比例和调制深度等关键物理参数对TDS特征隐藏的物理规律,仿真验证了一种28 Gbit/s 开关键控调制信号经过电光反馈混沌保密通信系统的物理层加密和解密性能,并探明了收发端电光反馈环路时延失谐对混沌同步和系统通信性能的影响。在几种典型的窃听场景下,通过仅有余弦相位解密、色散补偿、或联合使用相位解密和色散补偿的窃听方式,探究了系统的抗窃听攻击性能。【结论】文章所提方法可有效隐藏电光反馈混沌加密系统的TDS特征,防止反馈环路时延泄露,抵抗窃听者的非法攻击,为未来基于电光混沌保密通信系统的设计提供了一种新思路。

关键词:保密通信;混沌激光;电光混沌;时延标签

中图分类号:TN918

文献标志码:A

Research on the Time Delay Signature Concealment of Electro-Optic Feedback Chaotic Communication System

AN Yuehua¹, TANG Bin², LIU Jiangwei¹, GAO Zhensen²

(1. School of Optoelectronic Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China; 2. Key Laboratory of Photonic Technology for Integrated Sensing and Communication, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: 【Objective】Chaotic laser secure communication exhibits the advantages of high speed, long distance, and compatibility with classical optical fiber channels due to hardware encryption, which can provide physical layer security for high-speed optical fiber communication systems. In order to solve the physical security problem of feedback time delay leakage in conventional electro-optical feedback chaotic encryption systems, this paper proposes a secure optical communication system that can hide the characteristics of electro-optic feedback Time Delay Signature (TDS). 【Methods】By coupling an external cosine signal into the electro-optic feedback loop for feedback modulation, the periodicity of the cosine signal in the autocorrelation or mutual delay information curve is employed to mask the TDS of the original electro-optical feedback loop, so as to guarantee the physical layer security of the electro-optical feedback encryption structure. 【Results】The influence of key parameters such as the presence or absence of external coupling signals, coupling ratio, and modulation depth on TDS feature hiding is analyzed and compared in detail. The security and communication performances of a 28 Gbit/s on-off-keying modulated secure communication system are simulated and verified. The influence of feedback delay time detuning of the feedback loop on the synchronization and communication performance is also investigated. In several typical eavesdropping scenarios, the anti-eavesdropping attack performance is explored by cosine phase decryption, dispersion compensation or joint phase decryption and dispersion compensation eavesdropping. 【Conclusion】The results show that the proposed method can effectively conceal the TDS characteristics of the electro-optic feedback encryption system, prevent the leakage of feedback loop delay time, and resist against various illegal eavesdropping attacks, which provides a new solution for the design of electro-optic chaotic encryption systems in future.

Key words: secure optical communication; chaotic laser; electro-optic chaos; TDS

收稿日期:2025-09-22; 修回日期:2025-10-20; 纸质出版日期:2025-12-10

基金项目:国家自然科学基金资助项目(62375055);广东省自然科学基金资助项目(2023B1515020088);广东技术师范大学科研启动项目(2022SDKYA013)

作者简介:安跃华(1984-),女,山西忻州人。讲师,博士,主要研究方向为光通信器件和系统。

通信作者:高震森,教授。E-mail: gaozhensen@gdut.edu.cn

© Editorial Office of *Study on Optical Communications*. This is an open access article under the CC BY-NC-ND license.

宽限制效应可等效于二阶带通滤波器从 f_L 到 f_H 的频率范围,参数 $\theta=1/(2\pi f_L)$ 和 $\tau=1/(2\pi f_H)$ 分别为带通滤波器的低频响应时间和高频响应时间。通过控制环路增益参数,使得电光反馈系统输出信号的李雅普诺夫指数 >0 时,加密系统即可进入混沌状态。电光反馈环路中的关键物理参数设置如表 1 所示。在本系统中,仅以开关键控调制信号为例进行研究,但可进一步拓展到相位调制以及更高阶的调制信号中。

加密信号经过 50 km 的单模光纤进行传输,并通过掺铒光纤放大器补偿其传输损耗。放大器引入的噪声对解密影响不大,而传输色散则影响较大。为了降低传输色散对加解密造成的影响,利用另一段色散补偿光纤来补偿传输链路的色散。在接收端,通过使用与发送端硬件参数高度匹配的解密结构来实现信息恢复。首先利用色散模块 D_3 补偿 D_2 的色散,对加密信号进行色散解扰,随后利用电光解密装置进行相位解密。该解密装置由 FC_2 将输入信号分为两部分,一部分进入 PM_2 ,另一部分经过 MZI_2 、 TDL_2 、 PD_2 和 EA_2 之后加载到 PM_2 上。解密部分需耦合与发送端同频同相的余弦信号驱动 PM_2 ,且当解密电光反馈环路时延 DT_2 等于加密反馈环路时延 DT_1 、 PM_2 的 MD 等于 PM_1 但符号相反时,解密装置即可完成相位解密。最后 PM_2 的输出信号经过色散模块 D_4 ,补偿 D_1 对信号的色散扰乱,并通过 ESA 即可获得最终的原始信息。最后采用商用软件 VPI 与 Matlab 进行联合系统仿真,仿真所采用的参数如表 1 所示。

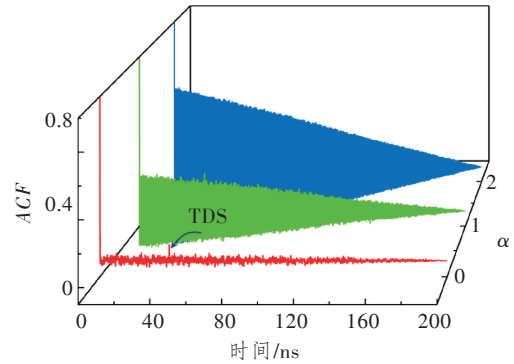
表 1 系统仿真参数

参数	术语名称	参考值
$R/\text{Gbit/s}$	信息传输速率	28
f_0/THz	激光器中心频率	193.1
$DT_1,DT_2/\text{ns}$	电光反馈环路时延	40
α	余弦信号与反馈信号耦合比例	2
MD	相位 MD	1.05
f_w/GHz	余弦信号频率	5
$\Delta T/\text{ps}$	MZI 延迟时间	35.71
BW/GHz	带通滤波器带宽	9.999 97
f_c/GHz	带通滤波器中心频率	5.000 02
f_L, f_H	带通滤波器上、下截止频率	32 kHz, 10 GHz
θ, τ	低频/高频响应时间	5 μs , 16 ps
$D_1, D_2/\text{ps/nm}$	色散模块 D_1, D_2 的色散值	540, 720
$D_3, D_4/\text{ps/nm}$	色散模块 D_3, D_4 的色散值	-720, -540

2 仿真结果与分析

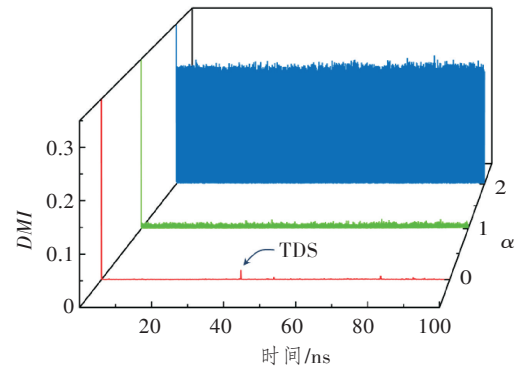
2.1 TDS 特征隐藏

采用自相关函数 (Autocorrelation Function, ACF) 和延时互信息 (Delay Mutual Information, DMI) 来表征系统的时延特征。图 2 所示为耦合比例 α 对 TDS 的影响。当 $\alpha=0$ 时,ACF 和 DMI 在反馈环路时延为 40 ns 处都能观察到明显的 TDS,表明环路时延可被窃取;当 $\alpha=1$ 时,ACF 和 DMI 曲线会整体抬升,此时 TDS 没有 $\alpha=0$ 时那么明显,但在 40 ns 处的 TDS 峰值略高于两侧。随着耦合比例 α 的增加,余弦信号所占比重增多,即使环路反馈信号存在自相性,但仍会被余弦信号的自相关所掩盖;在 $\alpha=2$ 时,不管 ACF 还是 DMI 均已无法观察到明显的 TDS,实现了 TDS 隐藏。



(a) 加密信号 ACF 分布

(a) ACF of the encrypted signal



(b) 加密信号 DMI 分布

(b) DMI of the encrypted signal

图 2 不同耦合比例 α 下加密信号的 ACF 和 DMI 曲线Figure 2 The ACF and DMI curves of encrypted signal for different coupling ratios α

为了更清晰地表征 TDS 特征,引入残差进一步分析。残差 e_i 定义为实际值 y_i 与回归模型拟合值 \hat{y}_i 之间的差,即 $e_i = y_i - \hat{y}_i$, i 为不同的时间序列。图 3(a)~图 3(d)和图 3(e)~图 3(h)分别为 $\alpha=1$ 和

2时 ACF、DMI 的峰值及残差 ACF、DMI 值。当 $\alpha=1$ 时,在 ACF 和 DMI 的峰值及残差图中,均能在反馈时延为 40 ns 处观察到 TDS 峰,残差 ACF 和 DMI 则更加明显,分别接近 0.10 和 0.04, 仍有被窃听者截获破解的可能。随着 α 的增加,当 $\alpha=2$

时,更多的余弦信号成分体现在 ACF 和 DMI 之中,ACF 峰值更陡,DMI 大幅抬升,此时在残差-ACF 和残差-DMI 图中完全无法观察到 TDS 峰的存在,表明引入外部余弦信号耦合调控可有效防止 TDS 特征暴露。

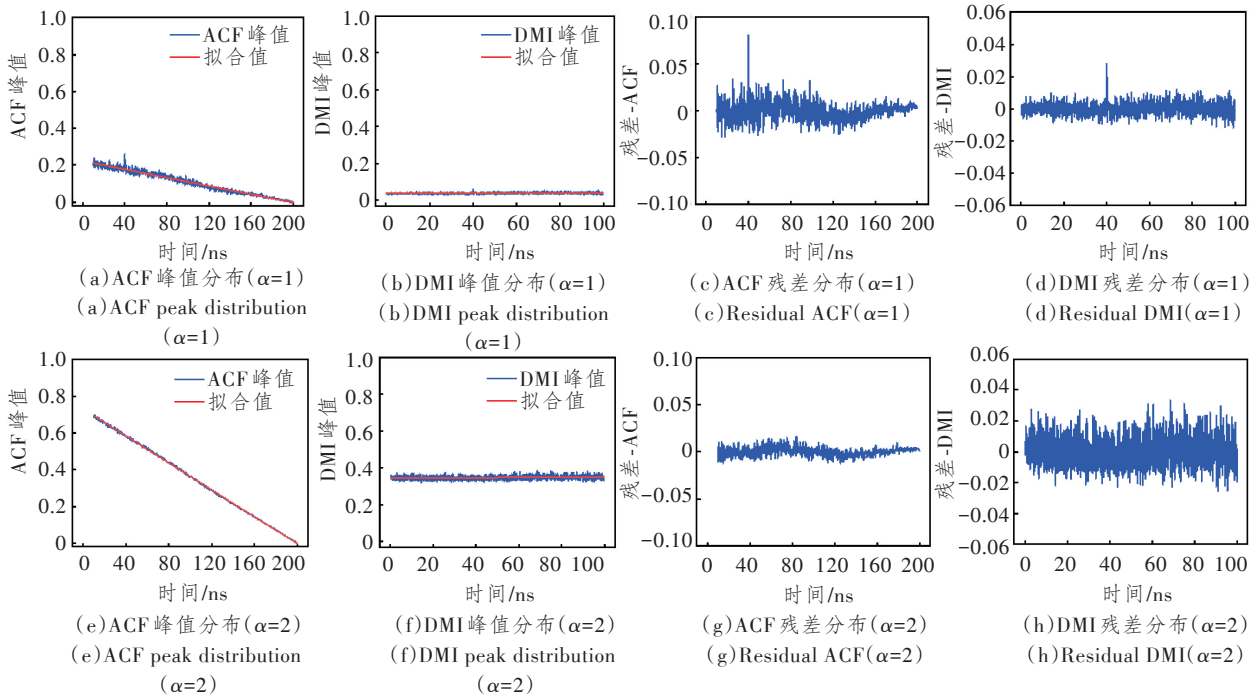


图3 不同耦合比例 α 下 ACF 和 DMI 及其残差分布示意图

Figure 3 ACF/DMI peak and residual ACF/DMI distributions for different coupling ratios α

本文进一步定量分析了残差-ACF 和残差-DMI 的 TDS 峰值随耦合比例 α 的变化规律,如图 4 所示。随着 α 的增加,残差-ACF 呈现下降趋势,当 α 达到 1.5 之后,残差-ACF 下降至背景-ACF 以下,意味着 TDS 被有效隐藏。残差-DMI 则随 α 呈现增加的趋势,但背景-DMI 上升速度快于信号残差-DMI,在 α 增大至 2 时,残差-DMI 处于背景-

DMI 之下,表明 DMI 中的 TDS 被隐藏。因此, α 应不小于 2,以保证 ACF 和 DMI 的 TDS 特征均能有效隐藏。

2.2 物理层加解密性能

图 5 所示为一种 28 Gbit/s 开关键控信号的物理层加解密性能。图 5(a)~图 5(d)和图 5(e)~图 5(h) 分别表示原始信号、加密信号、非法窃听信号、解密信号的波形和相应的眼图。由图可知,经过电光反馈混沌加密后,信号波形呈混乱状态,眼图呈现闭合状态,窃听者由于缺乏硬件解密装置,无法窃取保密信号。而合法接收端经过解密装置后,可有效恢复信号波形和眼图,解密波形跟原始波形高度匹配,眼图清晰地张开,实现了物理层的加密和解密。

图 6 所示为加解密信号的同步系数(Correlation Coefficient, CC)和误码率(Bit Error Rate, BER)随环路反馈时延失谐量的变化。由图可知, MD 越大,时延失谐容忍范围越小。在本系统中,相位 MD 是通过余弦信号与反馈信号的合路信号计算获得。在 $MD=1.05$ 时,环路反馈时延失谐容忍度约为 ± 12 ps,以满足 CC 在 0.9 之上和 BER 在前

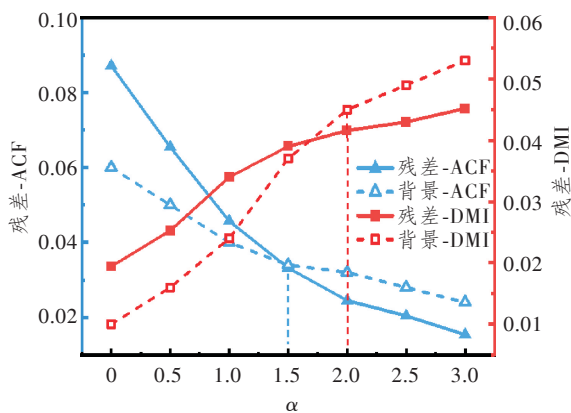


图4 耦合比例 α 对 ACF 和 DMI 残差分布的影响
Figure 4 The effect of coupling ratio α on the ACF and DMI distributions

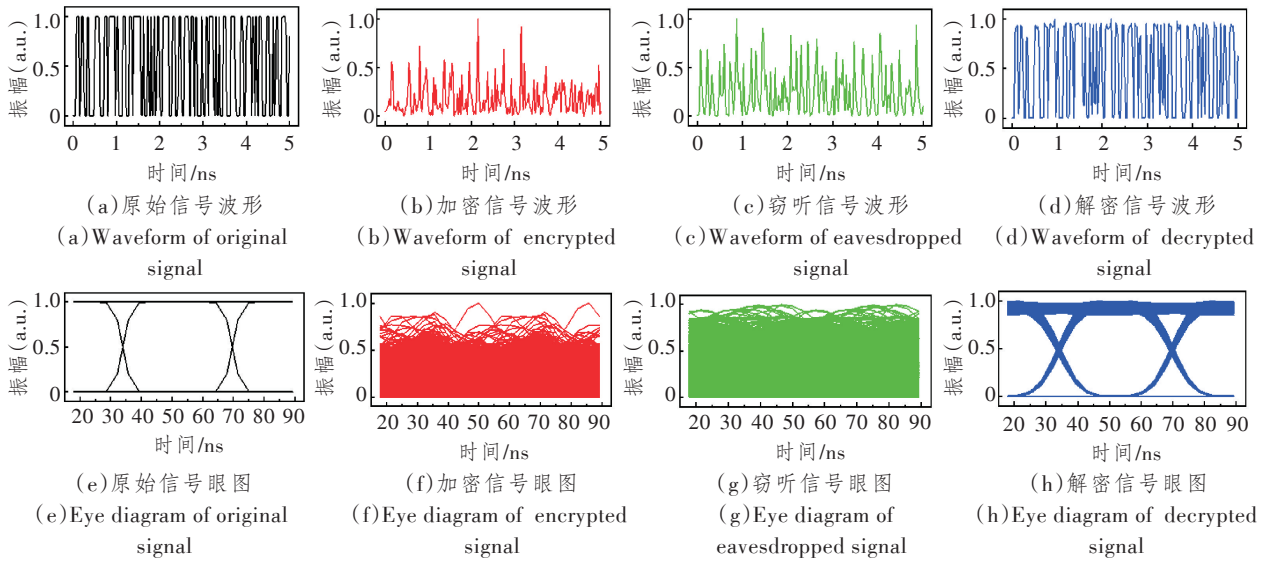


图5 原始信号、加密信号、窃听信号和解密信号的波形及眼图

Figure 5 Waveforms and eye diagrams of original, encrypted, eavesdropped and decrypted signals

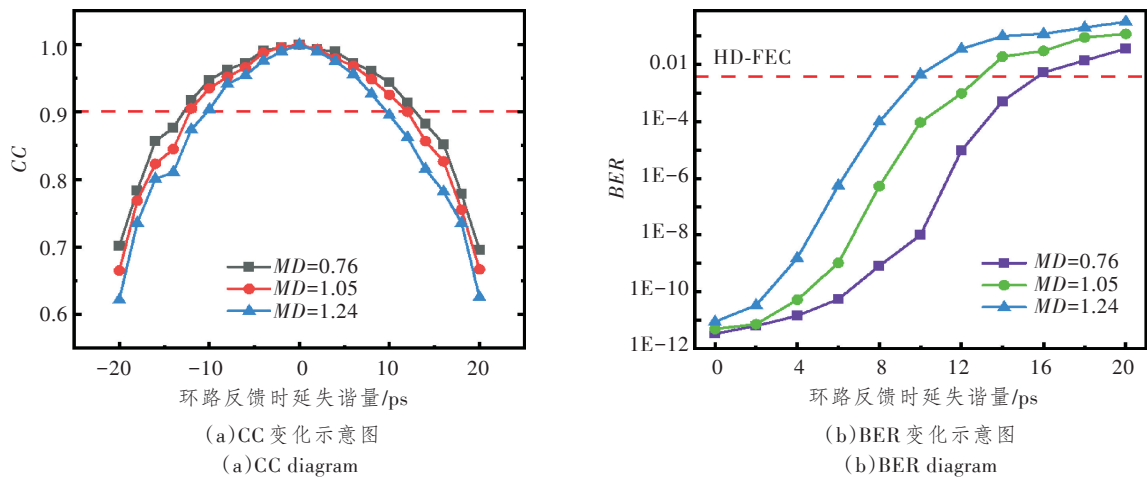


图6 环路反馈时延失谐对CC和BER的影响

Figure 6 CC and BER for different feedback time delay mismatch

向纠错硬判决(Hard-Decision Forward Error Correction, HD-FEC)门限之下。在实际系统中,可以采用高精度 TDL 进行控制,以保证系统的解密和通信性能。

2.3 抵抗窃听攻击性能

最后,本文模拟了3种可能的窃听场景,包括:
 ①只有余弦相位解密;②可调色散补偿模块+余弦相位解密;③补偿 D_2 色散+余弦相位解密+补偿 D_1 色散,以探究系统能否抵御潜在的非攻击,如图7所示。在第1种场景下,窃听者仅可调节窃听的相位MD。随着MD的变化,窃听BER始终大于HD-FEC,窃听结果如图7(a)所示;在第2种场景

下,窃听者使用可调色散补偿模块(Tunable Dispersion Compensator, TDC)扫描,之后再进行余弦解密,但还是无法窃取任何信息,BER在HD-FEC之上,如图7(b)所示;在第3种极端场景下,假设窃听者已知发送端的加密色散 D_1 和 D_2 ,仅有TDS信息,MD未知。当发射端 $MD < 1$ 时,随着窃听余弦信号MD的增加,出现BER小于HD-FEC的情况,说明此时电光反馈混沌加密作用不大,窃听者仅通过余弦信号就可完成解密,安全性不足;但当 $MD=1.05$ 及 1.24 时,窃听BER始终高于HD-FEC,表明发射端加密的MD需不小于1,以抵抗非法窃听,如图7(c)所示。

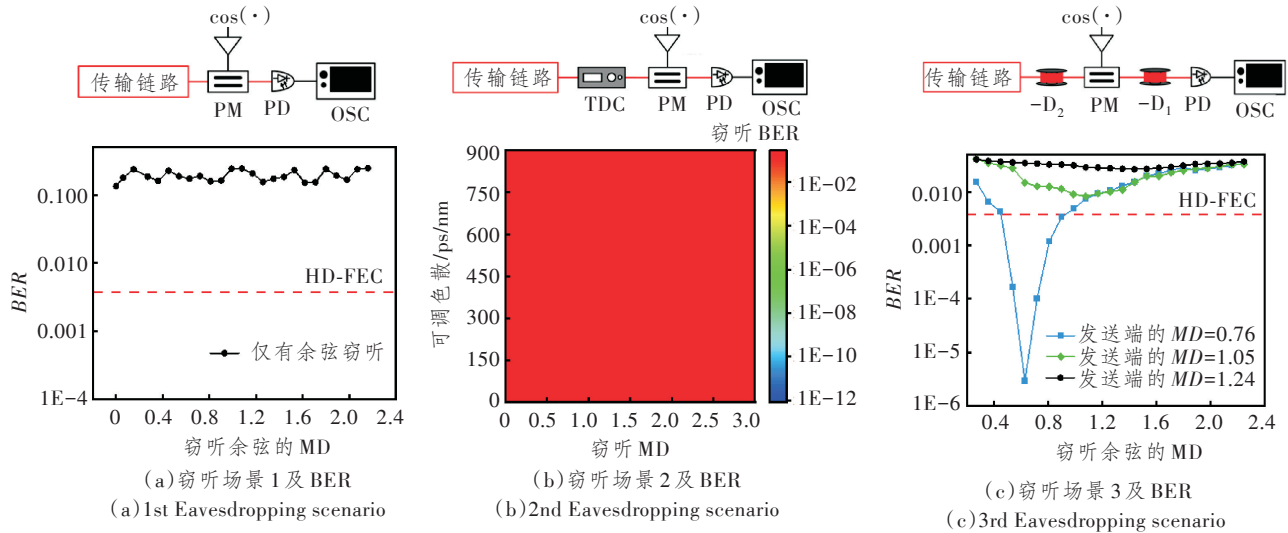


图7 不同窃听场景下,窃听者获得的 BER 变化趋势
Figure 7 The trend of eavesdropped BER for different eavesdropping scenarios

3 结束语

本文提出了一种隐藏电光反馈 TDS 特征进而实现高速保密光通信的解决方案。通过外部余弦信号耦合调制电光反馈环路,利用余弦信号周期性的自相关特性来掩盖原有电光反馈信号的 TDS 特征。系统分析了 TDS 隐藏的物理规律,并仿真验证了一种 28 Gbit/s 保密通信系统的物理层加解密性能,模拟了几种典型的窃听场景和抗攻击性能。结果表明,在电光反馈混沌加密结构中引入外部余弦信号耦合调制可以有效隐藏 TDS 特征,防止环路时延泄漏,提高系统的安全性,为未来基于电光反馈混沌加密系统的设计提供了一种新思路。

参考文献:

- [1] Niu Z, Xie Y, Xu G, et al. Experimental Demonstration of Integrated Encryption and Communication over Optical Fiber[J]. National Science Review, 2025, 12(7): nwaf112.
- [2] 王识, 邢甜甜, 王俊华, 等. 光纤通信物理层抗截获技术综述[J]. 光通信技术, 2018, 42(12): 10-14.
Wang S, Xing T T, Wang J H, et al. Overview of Anti-Interception Techniques for Physical Layer of Optical Fiber Communication [J]. Optical Communication Technology, 2018, 42(12): 10-14.
- [3] 高欣, 李苗, 张燕玲. 基于混沌映射的光纤通信物理层抗截获方法[J]. 光通信研究, 2023(2): 29-33.
Gao X, Li M, Zhang Y L. Anti-Interception Method of Optical Fiber Communication Physical Layer based

on Chaotic Mapping[J]. Study on Optical Communications, 2023(2): 29-33.

- [4] Xie Y, Yang Z, Shi M, et al. Signal-to-Noise Ratio Degradation Analysis for Optoelectronic Feedback-based Chaotic Optical Communication Systems[J]. Optics Letters, 2023, 48(19): 5005-5008.
- [5] Lu Y, Wang H, Ji Y. A Time-Delay Signature Elimination and Broadband Electro-Optic Chaotic System with Enhanced Nonlinearity by Deep Learning[J]. Optics Express, 2022, 30(11): 17698-17712.
- [6] Zhang L, Huang W, Tang B, et al. Strategy for Attacking the Key Parameters of Electro-Optic Self-Feedback Phase Encryption System [J]. Photonics, 2023, 10(4): 356.
- [7] Lu Y, Wang H, Ji Y, et al. Security-Enhanced Electro-Optic Chaotic Communication System based on the Logistic Map Feedback and Dynamic Key [J]. JOSA B, 2023, 40(5): 1131-1140.
- [8] Bai J, Wang H, Ji Y. Time-Delay Signature Concealing Electro-Optic Chaotic System with Multiply Feedback Nonlinear Loops[J]. Optics Express, 2021, 29(2): 706-718.
- [9] Huang H, Li Z, Gao X, et al. An Enhanced Electro-Optic Chaos Secure Communication System Immune to Time Delay Signature Extraction [J]. IEEE Photonics Journal, 2022, 14(1): 7209407.
- [10] Gu W, Gao X, An Y, et al. Security-Enhanced Electro-Optic Mutual Injection Secure Communication Scheme with Time-Delay Signature Suppressing [J]. IEEE Photonics Journal, 2023, 15(3): 7201208.