A High-Resolution Intrusion Detection Framework for Fiber Optic Networks Using Improved OLCR and LSTM-Based Temporal Analysis

Bo Zhang
Communication Engineering College, Luoyang normal university, Luoyang 471934, China
E-mail: z63895880@126.com

Keywords: improved OLCR, fiber optic secure communication, multi-dimensional feature fusion, LSTM, intrusion detection

Received: October 17, 2025

With the increasing demand for data transmission, fiber-optic communication systems face growing challenges in security and real-time monitoring. To address limitations in spatial resolution and weak anomaly detection, this study proposes a high-resolution intrusion detection framework integrating enhanced Optical Low-Coherence Reflectometry (OLCR) and Long Short-Term Memory (LSTM) networks. At the link layer, high-resolution interferometric signal detection and anomaly localization are achieved through spectral shaping, polarization stabilization, and optical path difference modulation. At the system layer, LSTM enables multi-dimensional feature fusion and temporal pattern recognition for intelligent intrusion classification and adaptive defense. Experiments on a 10-km fiber link simulate typical anomalies including breaks, splice faults, and bending eavesdropping, using NSL-KDD and Polarization Mode Dispersion datasets for training and validation. Measured parameters cover reflectivity, phase shift, and polarization angular velocity. Results demonstrate a spatial resolution of 11.15 μm at 100 m, detection accuracy of 96.40%, and intrusion recognition rate of 95.60%, outperforming existing methods. The fusion of improved OLCR and LSTM proves effective for high-precision detection and dynamic protection in complex environments, offering a scalable intelligent solution for secure fiber-optic systems.

Povzetek: Študija predstavi visoko natančen sistem, ki z izboljšano metodo OLCR in LSTM omogoča učinkovito zaznavanje in klasifikacijo anomalij v optičnih vlaknih.

1 Introduction

Global data traffic is growing exponentially, making information technology and network communication essential infrastructure across all aspects of daily life [1]. As the backbone of modern information networks, optical fiber communication supports key applications such as the Internet, 5G, and data centers with advantages like high bandwidth, low loss, and long-distance transmission [2]. However, despite its superior transmission performance, optical fiber remains vulnerable in physical security. Traditional encryption protects only data content and cannot prevent physical intrusions, which may lead to data leakage or service interruption without being detected in real time by upper-layer security mechanisms [3-4]. Meanwhile, existing physical layer monitoring techniques can locate faults but lack sufficient real-time performance, sensitivity to weak disturbances, and precise localization, falling short of high-security requirements [5]. Moreover, current fiber security solutions still lack an integrated approach combining high-precision detection, accurate localization, and anomaly identification [6]. To address these gaps, this study proposes a high-resolution intrusion detection framework for optical networks based on enhanced Optical Low-Coherence Reflectometry (OLCR) and Long Short-Term Memory (LSTM) networks. At the link layer, OLCR is optimized through spectral shaping, polarization stabilization, and optical path difference modulation to achieve high-resolution detection and localization of anomalies such as splice defects and covert eavesdropping. At the system layer, LSTM-based temporal modeling enables intelligent identification and classification of various intrusion types. The research aims to establish a physical-layer security system integrating high-precision detection, intelligent recognition, and dynamic protection, providing technical support for next-generation high-security optical fiber communication.

To systematically address key challenges in detection accuracy and system-level protection in optical fiber communication, the study formulates the following research questions: RQ1: Can the improved OLCR technique achieve sub-resolution anomaly detection and precise localization in long-distance fiber links? RQ2: Can multi-dimensional feature fusion and LSTM-based temporal modeling effectively enhance recognition accuracy and real-time response capability for diverse intrusion events?

2 Related work

With the rapid advancement of information technology and network communications, data security and privacy

Table 1: Current research progress and limitations of optical communication security methods.

Research	Methods	Application scenarios	Detection accuracy (%)	Spatial resolution (μm)	Advantages	limitation
[8]	Secure optical communication system based on RC4 cryptographic algorithm	Long-distance encrypted transmission	90.5	-	Excellent encryption performance and long transmission distance	Unable to perform physical layer anomaly detection
[9]	Light chaos encryption and information hiding	Hybrid free space/fiber optic communication	92.1	-	Strong anti-interference ability and high privacy	The detection speed is slow and the positioning accuracy is low
[10]	Data privacy protection scheme based on homomorphic encryption	Internet of Things and cloud data transmission	94.0	-	High data security and improved storage efficiency	High encryption overhead and poor real-time performance
[11]	Physical layer security scheme based on digital signal processing	Coherent optical communication system	90.0	30	Low cost and high physical layer security	Insufficient ability to recognize weak reflection events
[12]	Optimization of free-space optical communication channels	Atmospheric disturbance environment	91.8	50	Improve the signal-to-noise ratio and link stability	It is difficult to detect weak link intrusions
[13]	Unmanned aerial vehicle-assisted hybrid fiber-wireless communication system	Integrated communication between air, space, land and sea	89.7	>80	Dynamically optimize the beam divergence Angle and have a large capacity	Low detection sensitivity and slow response
[14]	Full-duplex free-space optical transceiver + intelligent lens stabilization technology	Optical fiber - free-space hybrid communication	93.3	45	Enhance link capacity and directional stability	The structure is complex and the cost is relatively high
[15]	Optical network routing and wavelength assignment based on reinforcement learning	Fixed grid optical network	95.2	-	Strong generalization ability in learning and high scheduling efficiency	It does not have the physical layer detection capability

protection have become core research areas [7]. Mohammed S H et al. proposed an RC4 cipher-based secure optical communication system using dispersion-compensating fiber to achieve long-distance secure message transmission while addressing range limitations [8]. Fadil E A et al. developed a hybrid secure system employing optical chaos to overcome traditional encryption limitations and signal degradation in chaotic encryption [9]. Alqahtani A S et al. introduced a homomorphic encryption technique focused on data owner, fog server, and consumer privacy, enhancing security during storage operations and reducing encryption length [10]. He J et al. designed a digital signal processing-based physical layer security scheme using two dispersion elements and a key-driven phase modulator for low-cost, efficient, and high-level security in coherent optical communication [11].

Additionally, Lema G G proposed a free-space optical communication method to maximize visibility and minimize bit error rate, improving link reliability under various atmospheric conditions [12]. Singh P et al. presented a unmanned aerial vehicle-assisted integrated fiber-wireless system using a cognitive divergence angle tracking algorithm to dynamically optimize beam divergence and overcome traditional RF limitations [13]. Bekkali A et al. developed a full-duplex, all-optical free-space transceiver to enhance capacity and reliability against atmospheric turbulence and pointing errors [14]. Nevin J W et al. applied reinforcement learning with invalid action masking and novel training to improve routing and wavelength assignment efficiency in fixed-grid optical networks [15].

In summary, significant progress has been made in data/physical layer security, transmission optimization, and intelligent management. However, real-time high-precision intrusion detection and localization at the optical fiber physical layer remain insufficient, as summarized in Table 1.

Based on this, the study proposes a high-resolution intrusion detection framework for optical fiber networks using improved OLCR and LSTM temporal analysis. It innovatively integrates the physical layer detection capability of improved OLCR with deep learning-based temporal modeling. This approach not only improves sensitivity and localization accuracy for weak, concealed disturbances but also enables intelligent classification of

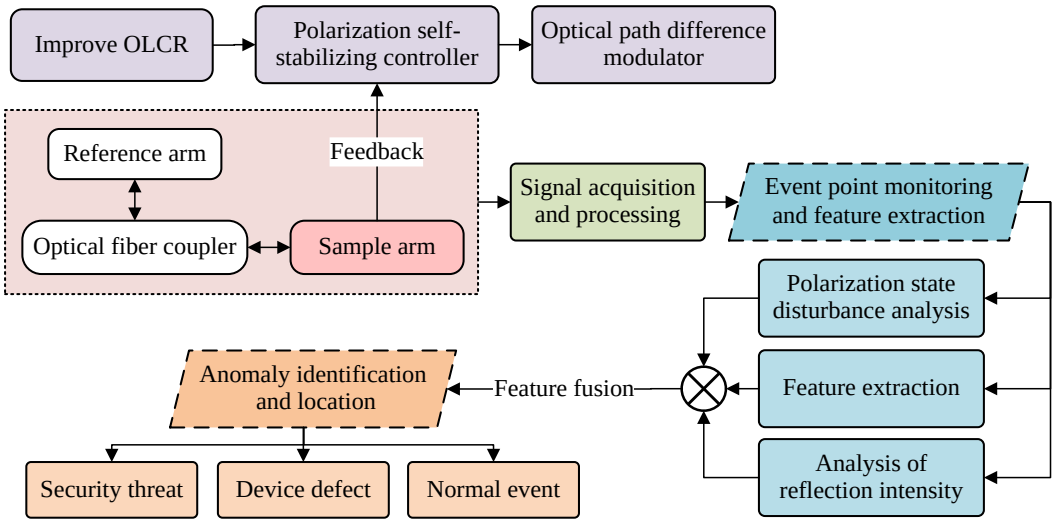


Figure 1: Optical fiber link anomaly detection and location technology based on improved OLCR.

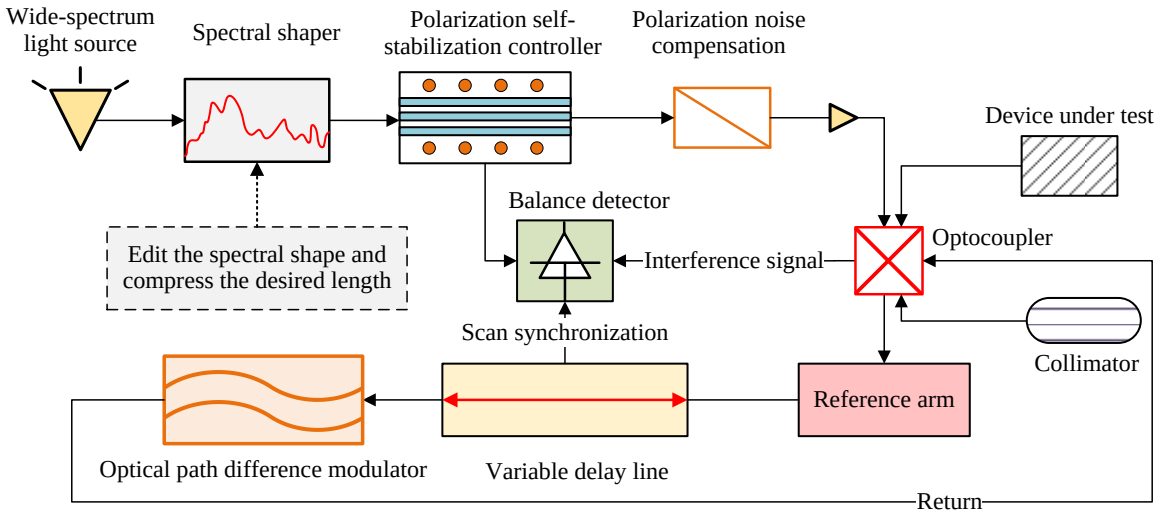


Figure 2: Improved OLCR system.

anomaly types and real-time response, establishing a comprehensive optical fiber security system that combines high-precision detection, intelligent identification, and dynamic protection.

3 Methods and materials

3.1 Fiber optic link anomaly detection and localization technology based on improved OLCR

To address the limitations of traditional OLCR systems in resolution, dynamic range, and weak anomaly detection, this study proposes an improved OLCR-based technique for optical fiber link anomaly detection and localization. By employing spectral shaping, polarization self-stabilization, and optical path difference modulation, the improved OLCR system achieves higher resolution and noise immunity. Combined with event point analysis for feature extraction and multi-event separation of interference signals, it enables precise identification and sub-resolution localization of link anomalies. The technical architecture is shown in Figure 1.

Figure 1 shows the fiber link anomaly detection and localization technology based on improved OLCR. Firstly, the traditional OLCR architecture is optimized, and improvements are made in spectral shaping, polarization self stabilization, and optical path difference modulation to construct a detection system with higher spatial resolution, larger dynamic range, and stronger stability. The improved OLCR system is shown in Figure 2.

Figure 2 shows an improved OLCR system that introduces a broad-spectrum light source with spectral shaping at the light source end, achieving sub ten micron

spatial resolution by compressing the self coherence length. The axial spatial resolution improvement is shown in equation (1) [16].

$$\Delta z \approx (\lambda_0^2/\Delta\lambda)\cdot(2\ln(2)/\pi n) \quad (1)$$

Equation (1) indicates that the resolution is directly proportional to the square of the center wavelength λ_0 of the light source, and inversely proportional to the full

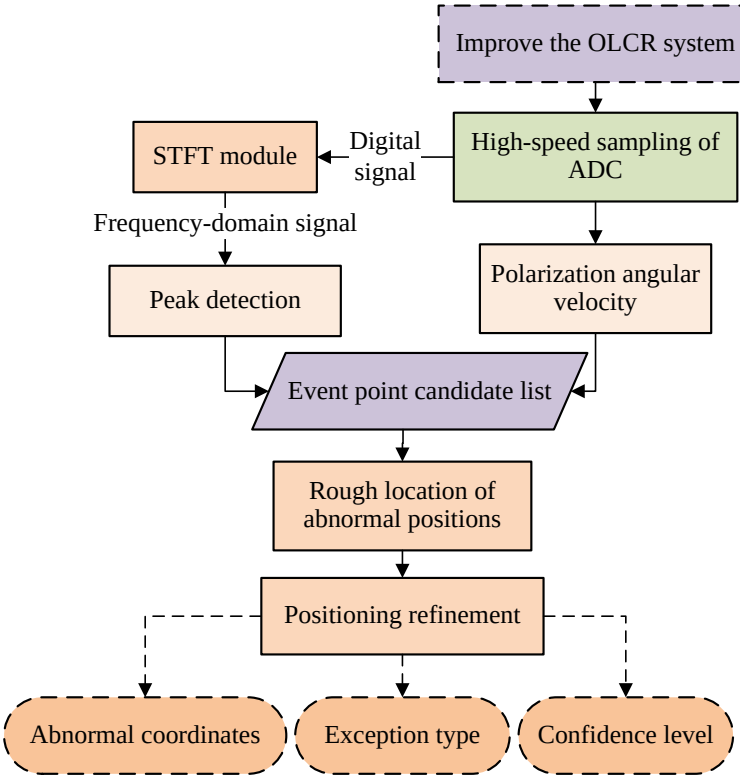


Figure 3: A link anomaly location method integrating optical path difference modulation and event point analysis.

width at half maximum spectral bandwidth $\Delta\lambda$ of the light source and the group refractive index n of the fiber. Among them, λ_0 and n are inherent parameters of the system, while $\Delta\lambda$ is a key variable that can be directly optimized through "spectral shaping" technology. Increasing $\Delta\lambda$ can effectively compress the coherence length of the light source, thereby achieving high-resolution detection at the sub ten micron level.

Adding a polarization self stabilization module to the interference arm effectively reduces the impact of polarization state fluctuations on the interference signal and improves the long-term stability of the system operation. The interference signal strength is shown in equation (2) [17].

$$I_t \propto R(z)\cdot\cos(2k\Delta l)\cdot\exp\left[-(2\Delta l / L_c)^2\right] \quad (2)$$

Equation (2) reveals the detection mechanism of the OLCR system, whose amplitude is determined by the reflectivity $R(z)$ of the reflection point, and the cosine term $\cos(2k\Delta l)$ contains the phase interference information caused by the optical path difference Δl, where k is the wavenumber. The exponential envelope term $\exp\left[-(2\Delta l / L_c)^2\right]$ ensures that the effective interference signal only exists within a range of coherence length L_c near zero optical path difference. Equation (2) indicates that by demodulating this signal and extracting the envelope, the reflectance distribution $R(z)$ curve of the fiber optic link can be inverted.

By configuring a variable optical path delay line and an optical path difference modulator in the reference arm, combined with frequency domain analysis methods, not only is the measurement dynamic range expanded, but the masking of weak reflection event points by baseband noise is also suppressed. The receiving end adopts balanced detection and high-speed sampling, combined with real-time digital signal processing, to extract the envelope of the interference signal and separate multiple event points. The event location is shown in equation (3).

$$z = \Delta l / (2n) \quad (3)$$

Equation (3) establishes a direct correspondence between the optical path difference Δl and the physical position z. The core of equation (3) lies in the denominator $2n$, which reflects the physical essence of light undergoing "round-trip" propagation at the event point. By accurately scanning and measuring the optical path difference Δl when interference occurs, the system can calculate the precise location of the reflection event based on equation (3).

Through the above improvements, the system can achieve stable detection and feature output of fiber optic link anomalies while ensuring high resolution, providing reliable data support for subsequent event point analysis and anomaly localization.

Subsequently, in response to possible device defects, connection point losses, and bending eavesdropping anomalies in the link, the study combined optical path

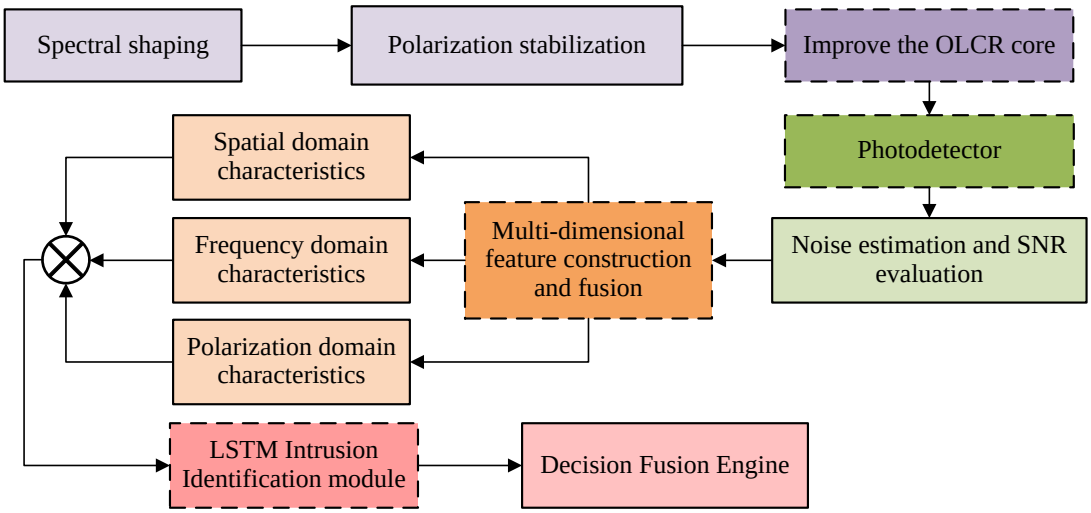


Figure 4: Optimal design of optical fiber secure communication system based on improved OLCR and LSTM.

difference modulation with event point analysis to perform multi-event detection and feature extraction on low coherence interference signals, extracting parameters such as reflection intensity, phase shift, and polarization disturbance, and achieving high-precision identification of abnormal behavior. The link anomaly localization method that integrates optical path difference modulation and event point analysis is shown in Figure 3.

Figure 3 shows a link anomaly localization method that combines optical path difference modulation and event point analysis. The system maps spatial reflection information in the fiber link to the frequency domain by introducing small amplitude optical path difference modulation in the reference arm, and effectively suppresses baseband noise by combining short-time Fourier transform (STFT) and frequency domain filtering, thereby enhancing the detection ability of weak reflection events. The optical path difference modulation function is shown in equation (4).

$$\Delta l(t) = l_0 + A_m \sin(2\pi f_m t) \quad (4)$$

Equation (4) defines the dynamic variation of the reference arm optical path, where l_0 is the basic optical path difference set by the variable delay line, responsible for large-scale scanning. A_m is a small modulation amplitude, much smaller than the coherence length to ensure that the interference signal is not lost, and f_m is the modulation frequency. This modulation linearly maps spatial reflection information to the high-frequency band, effectively avoiding the low-frequency noise region of the baseband, laying the core foundation for subsequent frequency domain filtering and signal-to-noise ratio improvement.

Subsequently, envelope extraction and multi event analysis are performed on the interference signal to achieve high-precision identification of event points through peak detection, interpolation positioning, and phase separation. The abnormal location is determined by combining time delay distance conversion. By utilizing polarization perturbation and amplitude phase information, different types of anomalies can be distinguished. Finally, multi-resolution localization is achieved through multi event correlation and local refinement algorithms, outputting the location, type, and confidence of anomalies, providing support for fiber optic link safety monitoring and intelligent recognition. The polarization disturbance discrimination factor is shown in equation (5).

$$P_d = \frac{1}{N}\sum_{i=1}^{N}\left|d\theta_s(i)/dt\right| \quad (5)$$

Equation (5) quantifies the jitter intensity of the polarization state at the event point by calculating the average absolute value of the polarization azimuth angle change rate $d\theta_s(i)/dt$ of N sampling points within the time window. This factor can effectively distinguish between stable device faults (low P_d values) and dynamic micro bending eavesdropping behavior (high P_d values).

Through the design of "Improved System-Anomaly Detection and Localization", high-resolution monitoring and precise localization of physical layer anomalies in fiber optic links are achieved, providing a solid foundation for subsequent optimization of secure communication.

3.2 Design of a high-resolution intrusion detection framework for fiber optic networks based on improved OLCR and LSTM time series analysis

The improved OLCR technique achieves high-resolution detection and localization of anomalies such as breaks,

splice faults, and bending eavesdropping. To address challenges in modeling multi-dimensional anomalies, strong intrusion concealment, and lack of adaptive protection in optical fiber systems, this study proposes a high-resolution intrusion detection framework combining improved OLCR and LSTM. It fuses multi-dimensional features from OLCR with LSTM's temporal modeling capability for intelligent anomaly classification. Result

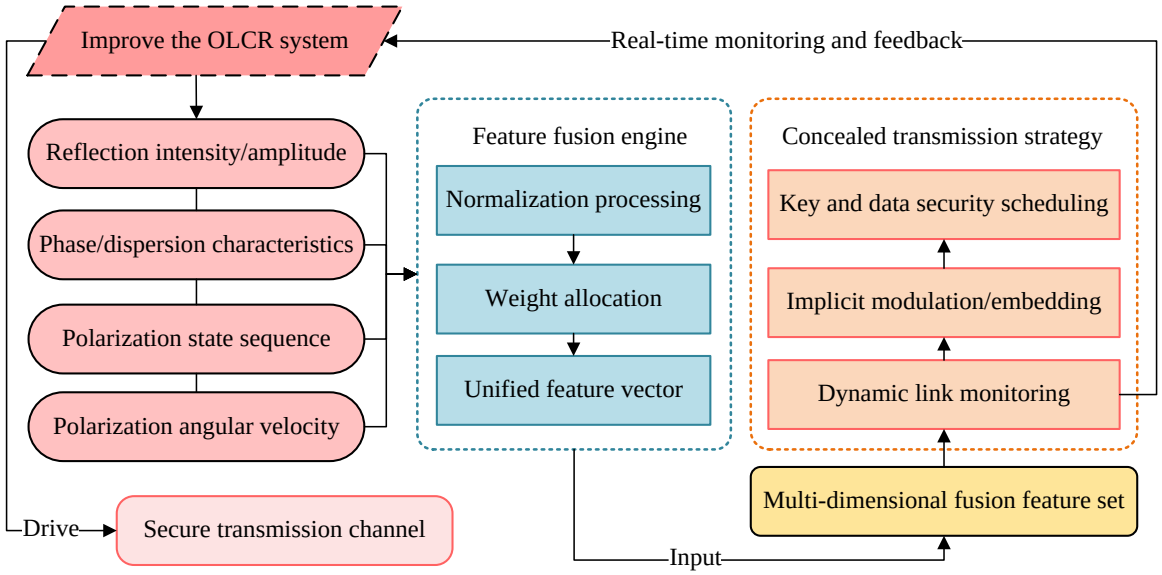


Figure 5: Multi-dimensional feature fusion and concealed transmission strategy based on improved OLCR.

feedback drives adaptive adjustment of transmission scheduling and OLCR scanning, establishing a closed-loop mechanism integrating physical layer detection and system protection. The intrusion detection framework is shown in Figure 4.

Figure 4 presents the high-resolution intrusion detection framework integrating improved OLCR and LSTM temporal analysis. Using improved OLCR as the core sensing unit, it outputs high-resolution multidimensional features including reflection intensity, phase shift, and polarization angular velocity. These features are normalized and fused into unified vectors for the deep learning model. The multidimensional feature fusion and covert transmission strategy based on improved OLCR are shown in Figure 5.

Figure 5 illustrates the multidimensional feature fusion and covert transmission strategy using improved OLCR. The system first acquires multi-dimensional link characteristics in real time. To improve LSTM recognition accuracy, six features are selected as inputs: reflection intensity, phase shift, polarization angular velocity, power spectral density, noise energy distribution, and delay gradient, covering major physical disturbances in optical links. Correlation analysis shows an average feature redundancy of only 0.21, ensuring input independence and validity. A confidence-weighted fusion mechanism is employed, where initial weights are set based on feature-label correlations and dynamically adjusted during training via gradient feedback to maximize validation accuracy. The weighted fusion vector is given by equation (6) [18].

$$F_{fused} = \sum_{i=1}^{N} w_i \cdot \frac{F_i - \mu_{F_i}}{\sigma_{F_i}} \qquad (6)$$

Equation (6) normalizes the i th original feature F_i using Z-score, subtracts the mean μ_{F_i} and divides it by the standard deviation σ_{F_i} to eliminate dimensional differences, multiplies it by its corresponding confidence level w_i, and finally sums up all weighted standard features to generate a comprehensive fused feature value.

Building on this, a covert transmission strategy is proposed. Utilizing a physical layer perturbation embedding mechanism, it dynamically senses link state changes and maps them to feature perturbations, employing controlled phase shifts and polarization variations as steganographic carriers for secure implicit transmission of data and keys. The transmitter embeds perturbation information through synchronized spectral shaping and phase modulation control, while the receiver recovers it via polarization reference signals and phase correction channels. This enhances transmission stealth and anti-eavesdropping capability while maintaining data integrity and interference resistance. The perturbation mapping function for covert transmission is given by equation (7) [19].

$$\Delta P = G \cdot \left(\frac{1}{1 + e^{-k \cdot (F_{fused} - T)}} \right) \cdot M(t)] \qquad (7)$$

Equation (7) uses a Sigmoid function to convert the comparison result between the fused feature value F_{fused} and threshold T into a smooth adjustment coefficient between 0 and 1. This coefficient is then multiplied by the disturbance amplitude gain G and the covert message $M(t)$ to generate the final physical layer parameter disturbance value ΔP. To ensure scientific and reproducible threshold T selection, the study employed ROC curve analysis. Extensive baseline data was

collected from a 10km test link under normal operation, alongside simulated intrusion signals including microbending, vibration, and connector disturbances. Analysis determined that setting the threshold at 0.82 maximizes the Youden index, achieving an optimal balance with 98.80% detection rate while maintaining a 2.10% false alarm rate.

The LSTM-based temporal recognition module effectively captures dynamic patterns in link characteristics over time. Combined with polarization

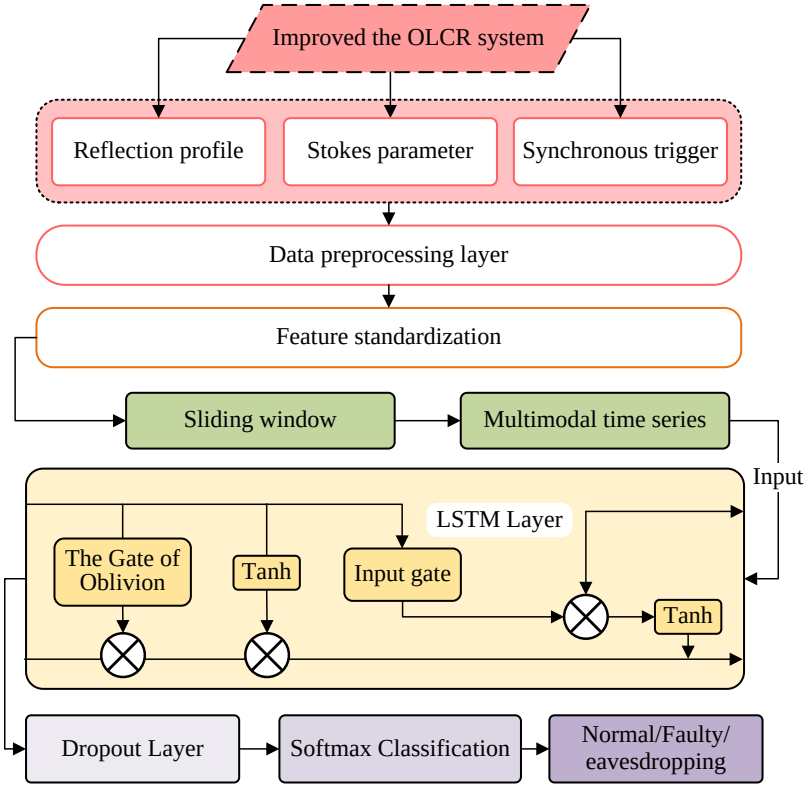


Figure 6: Intelligent intrusion recognition method combining polarization state angular velocity and LSTM.

angular velocity, it enables precise identification and classification of various anomalies including device defects, environmental disturbances, and eavesdropping attacks, while outputting anomaly types and confidence levels. The intelligent intrusion recognition architecture integrating polarization angular velocity with LSTM is shown in Figure 6.

Figure 6 shows the intelligent intrusion recognition method combining polarization angular velocity and LSTM. By utilizing an improved OLCR system to simultaneously acquire link reflection amplitude-phase and polarization state timing data, the polarization state angular velocity characteristics are extracted through first-order differential calculation of the Stokes vector. This approach sensitively detects intrusive behaviors such as micro-bending and local perturbations. The angular velocity of its polarization state is shown in equation (8) [20].

$$w_s(t) = \frac{d}{dt}\left(\frac{1}{2}\arctan\left(\frac{S_2(t)}{S_1(t)}\right)\right) \quad (8)$$

Equation (8) quantifies the instantaneous jitter intensity of the polarization state in the fiber by calculating the rate of change $\frac{d}{dt}$ of the polarization azimuth angle over time defined by the normalized Stokes parameters $S_1(t)$ and $S_2(t)$. This physical quantity is highly sensitive to mechanical disturbances such as micro bending and compression, and can effectively amplify and capture weak intrusion signals that are difficult to detect by static parameters.

Subsequently, the angular velocity is fused with features such as reflection intensity and phase shift, and a sliding window is used to construct a time-series sequence for input into LSTM, capturing the dynamic patterns of intrusion events and achieving accurate identification of normal fluctuations, device failures, and eavesdropping attacks. The LSTM status update is shown in equation (9).

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (9)$$

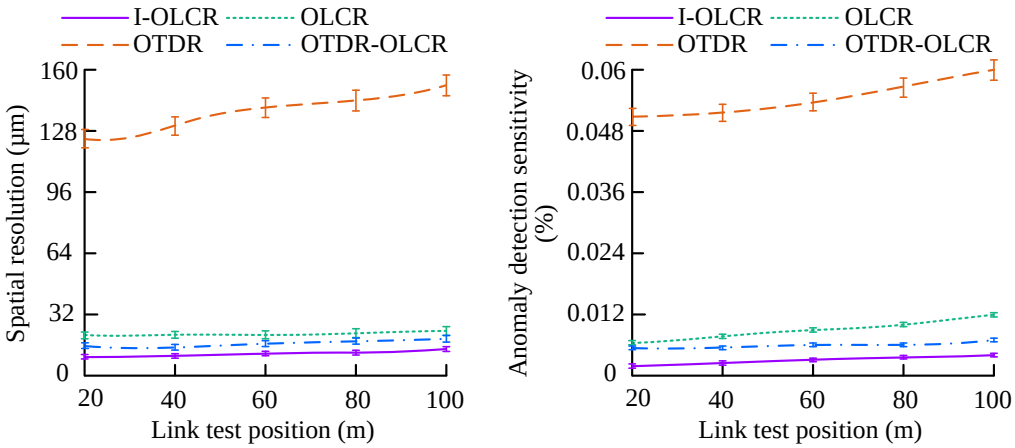
Equation (9) achieves precise regulation of long-term memory c_t through the forget gate f_t (controlling the degree of retention of the previous state c_{t-1}), input gate i_t (controlling the degree of writing of candidate state $\tilde{c}_t$), and their element wise multiplication.

The recognition results are output to the system monitoring and security scheduling module after threshold determination and confidence correction, which can provide real-time alarms and drive OLCR scanning and adaptive adjustment of transmission parameters, thus forming a closed loop between physical layer detection and intelligent analysis, and improving system security.

The output of multi-category abnormal decisions is shown in equation (10).

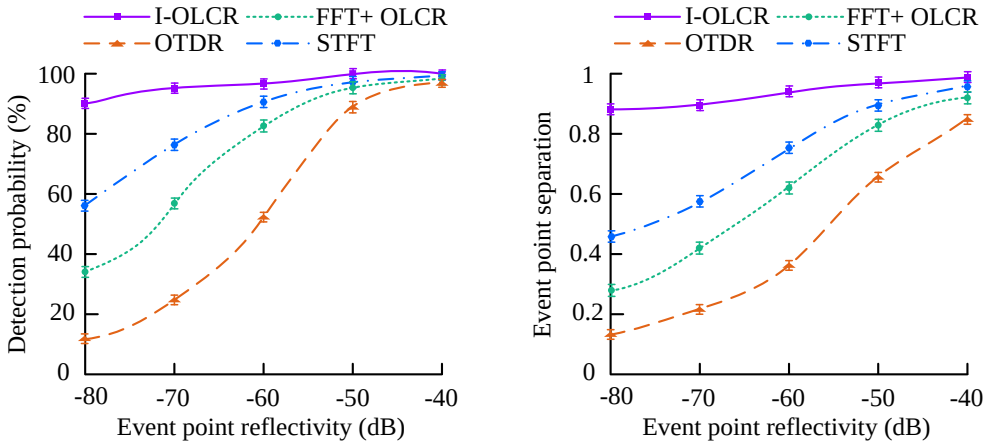
$$P(y=k \mid X)=e^{z_k} \Big/ \sum_{j=1}^{K} e^{z_j} \tag{10}$$

Equation (10) converts the original score z_k output by the LSTM network into the probability distribution of category k (such as normal, faulty, eavesdropping) using the Softmax function. Equation (10) normalizes the scores of k categories exponentially, so that the total output probability is 1, thereby intuitively representing the confidence of the model in the anomaly type to which the input sequence k belongs.



(a) Spatial resolution comparison (b) Detection sensitivity comparison

Figure 7: Link anomaly detection performance comparison.



(a) Detection probability comparison (b) Comparison of event point separation

Figure 8: Comparison of event point positioning and noise suppression performance.

4 Results

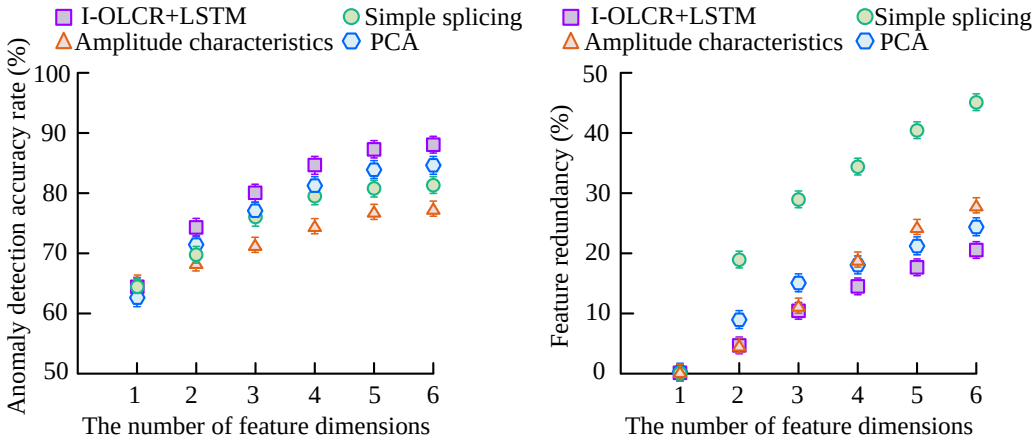
4.1 Link detection and localization performance verification of the improved OLCR

To validate the improved OLCR's link detection and localization performance, an experimental platform was constructed containing a broadband source, spectral shaper, polarization stabilizer, optical path difference modulator, variable delay line, coupler, reference/test fibers, balanced detector, and high-speed acquisition card. Using 10 km SMF-28 fiber (0.2 dB/km attenuation) at 25 ±1°C with vibration isolation, anomalies included breaks (-40 dB reflection), splice defects (0.3-0.5 dB loss), and microbending eavesdropping (2-5 mm radius). The broadband signal was spectrally shaped and split into interferometer arms. Polarization stabilization suppressed fluctuations while the reference arm enabled dynamic scanning. Interference signals were captured, processed for envelope extraction, event point separation, and noise suppression, ultimately extracting multidimensional features (reflectivity, phase shift, polarization disturbance) for sub-resolution localization. Comparative experiments against conventional OTDR, basic OLCR, and hybrid OTDR-OLCR used 10 repeated trials. The experimental results are shown in Figure 7.

As shown in Figure 7, the improved OLCR achieved a spatial resolution of 11.15 ± 0.36 μm (95% CI: 10.88-11.42) at 100m, improving approximately 11μm over basic OLCR's 22.30 ± 1.07 μm (CI: 21.53-23.07). Detection sensitivity reached 0.0022 ± 0.0002% (CI: 0.0021-0.0023) versus basic OLCR's 0.012 ± 0.0011%

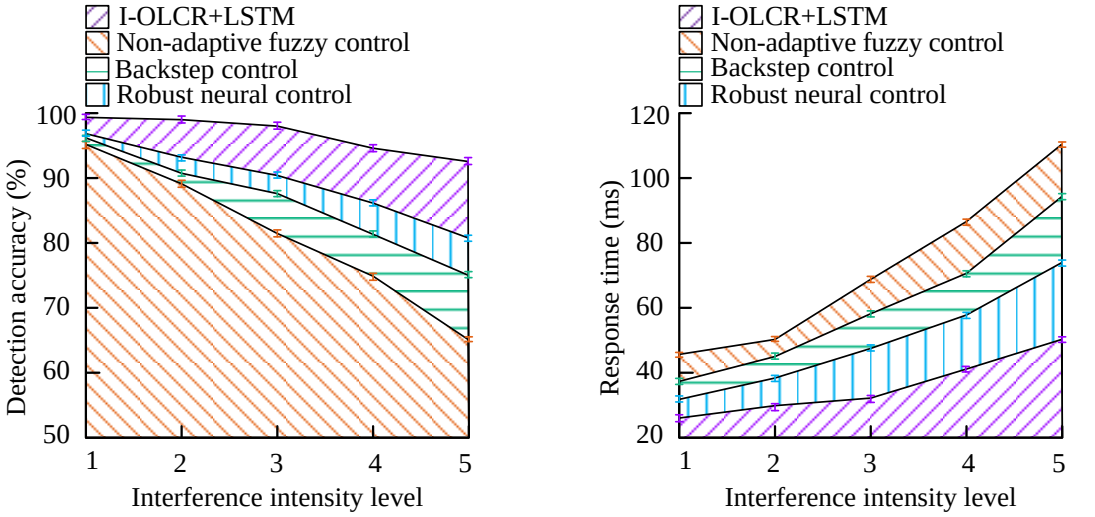
(CI: 0.011-0.013), demonstrating about 0.01% improvement. All comparisons showed $p<0.01$, confirming statistical significance. Subsequent event localization and noise suppression tests compared basic OLCR, frequency-domain OLCR, and STFT methods using 10 repeated trials, with results shown in Figure 8.

Figure 8 shows the improved OLCR achieved a detection probability of 92.70% ± 2.78% (95% CI: 90.77-94.63) for -80dB weak events, outperforming unmodulated OLCR, FFT-processed, and STFT methods



(a) Comparison of anomaly detection accuracy (b) Comparison of feature redundancy

Figure 9: Performance testing of multi-dimensional feature fusion recognition.



(a) Comparison of robustness test results (b) Comparison of sensitivity test results

Figure 10: Robustness and sensitivity testing of research methods under environmental changes/link interference.

by approximately 80.20%, 57.50%, and 33.80% respectively. Its event separation degree reached 0.88 ± 0.04 (CI: 0.85-0.91), significantly surpassing other methods. One-way ANOVA confirmed $p<0.01$ for all comparisons, validating the effectiveness of improved OLCR in improving weak event detection and localization precision.

4.2 Validation of the effectiveness of the improved OLCR and LSTM time-series analysis framework for high-resolution intrusion detection in fiber optic networks

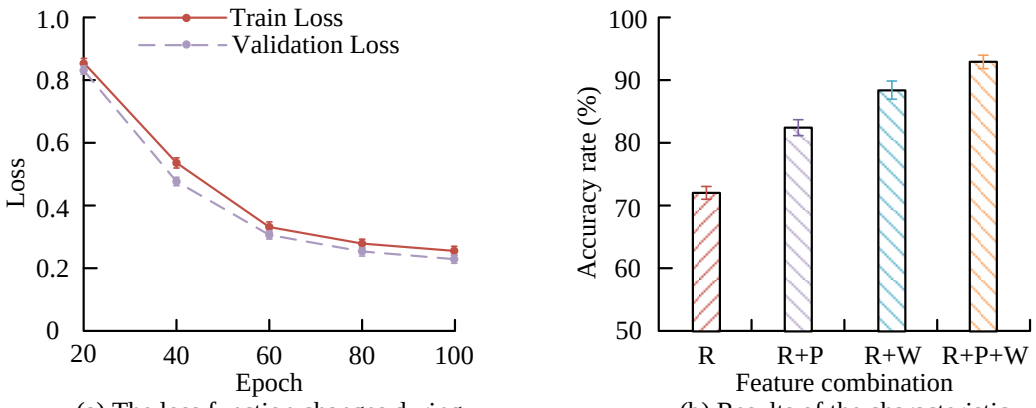
Following OLCR validation, a simulation platform was established to evaluate the integrated OLCR-LSTM intrusion detection framework. The environment used NVIDIA RTX 3080 GPU, Python with TensorFlow 2.0, Adam optimizer (learning rate 1 × 10-3), 10 km fiber length, 1 GS/s sampling rate, -80 dB to -30 dB noise, 2-layer LSTM (64 units/layer), and 100 maximum iterations. Datasets included NSL-KDD and Polarization Mode Dispersion with characterized network connections and fiber parameters. Tests on multidimensional feature fusion compared amplitude-only characteristics and simple splicing using 10 repeated trials, with results shown in Figure 9.

Figure 9 shows that the improved OLCR-LSTM with 6-dimensional features achieved 96.40%±1.93% anomaly detection accuracy (95% CI: 94.37-98.43), outperforming amplitude-only characteristics, simple splicing, and PCA by approximately 11.30%, 9.20%, and 5.30% respectively. Its feature redundancy was 20.50%±2.05% (CI: 19.08-21.92), significantly lower than other methods. Statistical tests confirmed $p<0.01$ for all comparisons, validating both improved accuracy and controlled redundancy. Subsequent robustness tests under environmental/link variations compared non-adaptive fuzzy control, backstep control, and robust neural control using 10 repeated trials, with results shown in Figure 10.

Table 2: Generates the music quality assessment data table.

Evaluation dimension	Traditional Encryption	I-OLCR	LSTM	I-OLCR+LSTM
Detection Rate (%)	-	92.50 ± 2.78 CI: [90.77, 94.23]	85.30 ± 3.41 CI: [82.93, 87.67] p < 0.01	98.80 ± 0.99** CI: [98.10, 99.50]
False Positive Rate (%)	-	8.70 ± 0.87 CI: [8.09, 9.31]	6.20 ± 0.62 CI: [5.77, 6.63]	2.10 ± 0.21** CI: [1.95, 2.25]
Response Delay (ms)	-	85.50 ± 6.84 CI: [80.76, 90.24]	72.30 ± 5.78 CI: [68.28, 76.32]	35.20 ± 2.82** CI: [33.24, 37.16]
System Throughput Retention Rate (%)	100.00 ± 0.00 CI: [100.00, 100.00]	88.90 ± 3.56 CI: [86.34, 91.46]	91.50 ± 3.66 CI: [88.84, 94.16]	96.80 ± 1.94** CI: [95.43, 98.17]

Note: The symbol "**" indicates that this indicator is statistically due to other models ($p < 0.01$)



(a) The loss function changes during the training process

(b) Results of the characteristic ablation experiment

Figure 11: The results of LSTM model training process loss and feature ablation experiments.

As shown in Figure 10, under interference level 5 (± 5°C temperature fluctuation + strong EMI), the proposed method achieved 93.50% ± 2.81% detection accuracy (95% CI: 91.50-95.50), surpassing non-adaptive fuzzy control, backstep control, and robust neural control by 27.70%, 16.60%, and 12.30% respectively. Its response time was 52.90±3.17 ms (CI: 50.70-55.10), outperforming the others by 59.60 ms, 42.40 ms, and 23.90 ms. All comparisons showed $p<0.01$, confirming robust performance under extreme interference. Subsequent system-level validation compared traditional encryption, improved OLCR, and LSTM alone using metrics including Detection Rate (true intrusions detected), False Positive Rate (false alarms), Response Delay (detection-to-response time), and Throughput Retention Rate (protected vs. baseline throughput). Results from 10 repeated trials are shown in Table 2.

Table 2 shows the improved OLCR+LSTM closed-loop system achieved a detection rate of 98.80%±0.99% (95% CI: 98.10-99.50), surpassing physical-layer-only and intelligence-only methods by 6.30% and 13.50% respectively. Its false positive rate was 2.10%±0.21% (CI: 1.95-2.25), reduced by 6.60% and 4.10%, with a response delay of 35.20±2.82 ms (CI: 33.24-37.16) and throughput retention of 96.80% ± 1.94% (CI: 95.43-98.17). All comparisons showed $p<0.01$, confirming superior

detection, security, and communication performance. Finally, LSTM training loss and feature ablation studies were conducted using 70%/15%/15% data splits, Random Search optimization (Batch Size=64, Dropout=0.2). Incremental ablation used reflection/amplitude (R-group) as baseline, adding phase/dispersion (P-group) for R+P, polarization/temporal (W-group) for R+W, and full features (R+P+W), with results in Figure 11.

Figure 11(a) shows the LSTM's training loss decreased from 0.85 ± 0.043 (95% CI: 0.824-0.876) at Epoch 20 to 0.25 ± 0.013 (CI: 0.242-0.258) at Epoch 100, with validation loss dropping correspondingly from 0.82 ± 0.041 (CI: 0.795-0.845) to 0.24 ± 0.012 (CI: 0.233-0.247). The overfitting ratio remained stable at 1.04-1.09. In Figure 11(b), full feature fusion (R+P+W) achieved 95.63% ± 1.91% accuracy (CI: 94.31-96.95), outperforming reflection-only characteristics ($71.35\% \pm 2.14\%$, CI: 69.84-72.86) by $24.28\% \pm 1.21\%$ (CI: 23.48-25.08). All improvements were statistically significant ($p<0.001$), confirming stable training without overfitting and the effectiveness of multi-feature fusion.

5 Discussion

The proposed fiber-optic security system integrating improved OLCR (with spectral shaping, polarization stabilization, and path difference modulation) and LSTM achieved high-resolution detection and intelligent intrusion recognition. He J et al. [11] used DSP and phase modulation for security but showed limited weak reflection detection, whereas our method achieved 98.80% detection rate at 100m with improved sensitivity. Lema G G [12] optimized SNR for link stability but had >50 μm spatial resolution. Our approach-maintained stability while enhancing detection of subtle anomalies. Singh P et al. [13] demonstrated excellent link capacity in unmanned aerial vehicle-assisted systems, yet their detection sensitivity remained below 0.01%. Our LSTM-based fusion strategy significantly improved sensitivity and robustness.

However, the method requires balancing performance and computational efficiency. The LSTM introduces ≈ 15% additional computational load, with notable GPU and training time demands for long sequences. High hardware precision is essential, potentially needing compensation in extreme conditions. Future work could explore lightweight temporal networks or attention mechanisms to reduce computational cost while maintaining detection performance.

6 Conclusion

This study proposes an improved OLCR and LSTM-based high-resolution intrusion detection method for optical fiber networks, addressing limitations in real-time performance, detection accuracy, and intrusion identification. The approach innovatively improves OLCR through spectral shaping to compress coherence length and enhance spatial resolution, integrates polarization stabilization to suppress interference noise, and combines optical path difference modulation with event point analysis to strengthen response to weak anomalies. Simultaneously, LSTM is introduced to model time-varying features, establishing closed-loop protection from the physical to system layers. Results demonstrate a spatial resolution of 11.15 μm and a detection rate of 98.80% at 100m, with only 2.10% false alarm rate, outperforming conventional OLCR and other compared methods. The proposed method achieves a 92.70% detection probability for extremely weak events (-80dB), an 80.20% improvement over the original OLCR (12.50%). This confirms that the deep integration of physical layer sensing and intelligent algorithms effectively balances detection precision, response speed, and system efficiency. To address nonlinear and dynamic disturbances in high-security communications, future work could incorporate adaptive control, chaotic control, and optimal control strategies to enhance environmental adaptability and robustness. Furthermore, the method shows promise for quantum communications, defense networks, and data centers, potentially enabling integrated fiber security systems encompassing detection, protection, and scheduling.

7 Funding

The research is supported by: Research and Practice Project on Vocational Education Teaching Reform in Henan Province, Exploratory Study on Implementing Curriculum-based Ideological and Political Education in Secondary Vocational Schools from the Perspective of 'Three Teachings' Reform (No. Yu Jiao [2023] 89739).

References

[1] Danshi Wang, Yuchen Song, Yao Zhang, Xiaotian Jiang, Jiawei Dong, Faisal Nadeem Khan, Takeo Sasai, Shanguo Huang, Alan Pak Tao Lau, Massimo Tornatore, and Min Zhang. Digital twin of optical networks: a review of recent advances and future trends. Journal of Lightwave Technology, 42(12):4233-4259, 2024. https://doi.org/10.1109/JLT.2024.3401419.

[2] Ebrahim E. Elsayed. Investigations on OFDM UAV-based free-space optical transmission system with scintillation mitigation for optical wireless communication-to-ground links in atmospheric turbulence. Optical and Quantum Electronics, 56(5):837-838, 2024. https://doi.org/10.1007/s11082-024-06692-1.

[3] Riyaz Saiyyed, Manoj Sindhwani, Neeraj Kumar Mishra, Hunny Pahuja, Shippu Sachdeva, and Manoj Kumar Shukla. Synergizing intelligent signal processing with wavelength-division multiplexing for enhanced efficiency and speed in photonic network communications. Journal of Optical Communications, 46(3):591-606, 2025. https://doi.org/10.1515/joc-2024-0139.

[4] Ahmed W. Abdulwahhab, A. K. Abass, Mohammed A. Saleh, and Fareed F. Rashid. Enhancing performance of optical chaotic-based secure fiber-

optic communication system. Optical and Quantum Electronics, 55(5):468-469, 2023. https://doi.org/10.1007/s11082-023-04757-1.

[5] Anqi Hu, Lu Gan, Lei Guo, Hao Yan, and Junfan Hu. Convex optimization-based high-speed and security joint optimization scheme in optical access networks. Optics Express, 32(4):6748-6764, 2024. https://doi.org/10.1364/OE.512191.

[6] Sergio Hernandez, Christophe Peucheret, Francesco Da Ros, and Darko Zibar. End-to-end optimization of optical communication systems based on directly modulated lasers. Journal of Optical Communications and Networking, 16(8):D29-D43, 2024. https://doi.org/10.1364/JOCN.522761.

[7] Senaa H. Mohammed, A. K. Abass, M. H. Ali, and Fareed F. Rashid. Design and simulation of secure fiber optic communication system utilizing hill cipher algorithm. Journal of optics, 53(2):1499-1507, 2024. https://doi.org/10.1007/s12596-023-01313-8.

[8] Senaa H. Mohammed, M. H. Ali, A. K. Abass, and Waleed Khalid Al-Azzawi. Design and implementation of cipher algorithm based secure optical communication system. Optical and Quantum Electronics, 55(1):86-87.10, 2023. https://doi.org/1007/s11082-022-04354-8.

[9] E. A. Fadil, A. K. Abass, and S. R. Tahhan. Design and simulation of optical chaotic-based secure hybrid optical communication system. Journal of Optics, 52(4):1887-1896, 2023. https://doi.org/10.1007/s12596-023-01143-8.

[10] Abdulrahman Saad Alqahtani, Youssef Trabelsi, P. Ezhilarasi, R. Krishnamoorthy, S. Lakshmisridevi, and S. Shargunam. Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication. Optical and Quantum Electronics, 56(3):487-488, 2024. https://doi.org/10.1007/s11082-023-06098-5.

[11] Jiaxiang He, Roger Giddings, Wei Jin, and Jianming Tang. DSP-based physical layer security for coherent optical communication systems. IEEE Photonics Journal, 14(5):1-11, 2022. https://doi.org/10.1109/JPHOT.2022.3202433.

[12] Gebrehiwet Gebrekrstos Lema. Free space optics communication system design using iterative optimization. Journal of Optical Communications, 44(1):s1205-s1216, 2024. https://doi.org/10.1515/joc-2020-0007.

[13] Priyanka Singh, Vivek Ashok Bohara, and Anand Srivastava. On the optimization of integrated terrestrial-air-underwater architecture using optical wireless communication for future 6G network. IEEE Photonics Journal, 14(6):1-12, 2022. https://doi.org/10.1109/JPHOT.2022.3210481.

[14] Abdelmoula Bekkali, Hideo Fujita, and Michikazu Hattori. New generation free-space optical communication systems with advanced optical beam stabilizer. Journal of Lightwave Technology, 40(5):1509-1518, 2022. https://doi.org/10.1109/JLT.2022.3146252.

[15] Josh W. Nevin, Sam Nallaperuma, Nikita A. Shevchenko, Zacharaya Shabka, Georgios Zervas, and Seb J. Savory. Techniques for applying reinforcement learning to routing and wavelength assignment problems in optical fiber communication networks. Journal of Optical Communications and Networking, 14(9):733-748, 2022. https://doi.org/10.1364/JOCN.460629.

[16] Saravanan Pandiaraj, R. Krishnamoorthy, S. Ushasukhanya, Janjhyam Venkata Naga Ramesh, Rakan A. Alsowail, and Shitharth Selvarajan. Optimization of IoT circuit for flexible optical network system with high-speed utilization. Optical and Quantum Electronics, 55(13):1206-1207, 2023. https://doi.org/10.1007/s11082-023-05452-x.

[17] Mahmoud M. A. Eid, Vishal Sorathiya, Sunil Lavadiya, Eslam Shehata, and Ahmed Nabih Zaki Rashed. Free space and wired optics communication systems performance improvement for short-range applications with the signal power optimization. Journal of Optical Communications, 45(1):s327-s335, 2025. https://doi.org/10.1515/joc-2020-0304.

[18] Salman A. AlQahtani, Mohamed E. M. Alngar, Reham M. A. Shohib, and Abdulaziz M. Alawwad. Enhancing the performance and efficiency of optical communications through soliton solutions in birefringent fibers. Journal of Optics, 53(4):3581-3591, 2024. https://doi.org/10.1007/s12596-023-01490-6.

[19] Fangyuan Xing, Shibo He, Victor C. M. Leung, and Hongxi Yin. Energy efficiency optimization for rate-splitting multiple access-based indoor visible light communication networks. IEEE Journal on Selected Areas in Communications, 40(5):1706-1720, 2022. https://doi.org/10.1109/JSAC.2022.3145818.

[20] Yanyi Wang, Dongju Du, Yingxiong Song, Zhengxuan Li, Nan Ye, Qianwu Zhang, Junjie Zhang, Jian Chen, and Bingyao Cao. Photonics-based integrated radar jamming and secure communication system at Ka-band. Journal of Lightwave Technology, 42(10):3621-3630, 2024. https://doi.org/10.1109/JLT.2024.3362254.