POLITECNICO DI TORINO
Repository ISTITUZIONALE

Multi-Threat Detection in Optical Networks Using Deep Neural Networks

Original
Multi-Threat Detection in Optical Networks Using Deep Neural Networks / Malik, G., Masood, M.U., Ali, A., Cheruvakkadu Mohamed, M., Straullu, S., Kishore Bhyri, S., Maria Galimberti, G., Pedro, J., Napoli, A., Wakim, W., Curri, V.. - (In corso di stampa). (IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN) Abu Dhabi (UAE) 8 - 11 June 2026).

Availability:
This version is available at: 11583/3015256 since: 2026-09-07T09:16:29Z

Publisher:
IEEE

Published
DOI:

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
IEEE postprint/Author's Accepted Manuscript

©9999 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

21 November 2026

Multi-Threat Detection in Optical Networks Using Deep Neural Networks

Gulmina Malik
Politecnico di Torino, Italy
gulmina.malik@polito.it

Muhammad Umar Masood
Politecnico di Torino, Italy
muhammad.masood@polito.it

Ahtisham Ali
Politecnico di Torino, Italy
ahtisham.ali@polito.it

Mashboob Cheruvakkadu Mohamed
Politecnico di Torino, Italy
mashboob.cheruvakkadu@polito.it

Stefano Straullu
Links Foundation, Italy
stefano.straullu@linksfoundation.com

Sai Kishore Bhyri
Nokia, Optical Networks
sai.bhyri@nokia.com

Gabriele Maria Galimberti
Nokia, Optical Networks
gabriele.galimberti@nokia.com

João Pedro
Nokia, Optical Networks
joao.pedro@nokia.com

Antonio Napoli
Nokia, Optical Networks
antonio.napoli@nokia.com

Walid Wakim
Nokia, Optical Networks
walid.wakim@nokia.com

Vittorio Curri
Politecnico di Torino, Italy
vittorio.curri@polito.it

***Abstract*—This paper investigates deep-learning-based multi-threat detection in optical fiber networks using state-of-polarization (SOP) monitoring. Mechanical disturbances such as shaking, tapping, and fiber manipulation introduce characteristic variations in the stokes parameters, which were captured through a high-speed polarimeter in a controlled robotic-arm testbed. Eight polarization fingerprints, representing both normal and critical events, were collected to emulate realistic physical-layer disturbances. Three neural network models - CNN, LSTM, and GRU - were trained to classify these events, and their performance was evaluated using test accuracy, training time, inference time, memory usage, and CPU consumption. A computational load index (CLI) was defined to quantify the overall computational cost based on normalized training time, inference latency, CPU load, and memory usage. The results show that GRU provides the highest accuracy, LSTM offers the best balance between accuracy and complexity, and CNN yields the lowest computational load for lightweight deployment. The combined accuracy–complexity assessment demonstrates that SOP-based sensing integrated with deep-learning models can support fast and reliable detection of physical-layer threats in optical transport networks, enabling proactive protection and improved system resilience.**

***Index Terms*—Neural networks, deep learning, state-of-polarization, CNN, LSTM, GRU, multi-threat detection.**

I. Introduction

Optical transport networks are the backbone of modern communication infrastructures, enabling ultra-high-capacity, low latency connectivity, and long reach data transmission. The low attenuation, wide optical bandwidth, and high linearity of standard single-mode fiber (SMF) enable long-haul signal propagation with minimal regeneration, making fiber the most reliable physical medium for high-bit-rate transmission. However, despite these intrinsic advantages, fiber infrastructures remain exposed to a variety of physical-layer impairments that can jeopardize network availability. Mechanical disturbances, including accidental dig-ups (leading to fiber cuts), cable deformation, unauthorized access attempts, or deliberate tapping, can induce abrupt polarization fluctuations, power excursions, or complete signal interruption [1]. Catastrophic failures such as fiber cuts represent a dominant cause of network outages in the field [2], typically triggered by construction activities, external mechanical impacts, or targeted intrusion events aimed at compromising confidentiality by extracting optical power from the transmission line [3].

One of the key challenges in optical network operations is the timely detection and localization of physical layer failures. Hard failures such as fiber cuts or extensive mechanical damage may lead to immediate service disruption, while soft failures evolve gradually and degrade network performance over time as a consequence of component aging, environmental stress, or physical layer attacks [4, 5]. Both hard and soft failures require continuous monitoring to maintain network resilience, protect the network infrastructure, and avoid large-scale service outages. These operational demands have motivated the development of advanced fault management frameworks that integrate autonomous analysis, adaptive learning mechanisms, and cognitive decision making [6]. Conventional fault-detection mechanisms, including threshold-based systems and optical time-domain reflectometry (OTDR), remain effective for detecting major disruptions and localizing them, but they exhibit limited sensitivity to subtle or transient physical disturbances [7]. In this context, state-of-polarization (SOP) monitoring has emerged as a promising way for fiber sensing due to its high sensitivity to any mechanical disturbances or manipulations

This work has received funding from the project PNRR-NGEU (MUR–DM117/2023), and from the EU's Horizon Europe research and innovation program under GA No. 101092766 (ALLEGRO Project), and EWOC GA No. 101073265.

in the fiber [8]. Owing to its high sensitivity, we have employed SOP in our analysis, which will be discussed in detail in section II. However, due to the inherent nature of SOP evolution, and environmental noise, this is non-trivial to interpret, especially in real-world metro networks. These challenges motivate intelligent, data-driven approaches with the capability to learn complex temporal and spatial patterns embedded in the polarization measurements.

With the recent advancements in machine learning (ML) and deep learning (DL), the fault identification has gained significant attention for its ability to automate the threat detection and classification. In our prior work [9, 10], we used basic classification approaches that required minimal computational resources. However, in real-world networks, environmental noise has a major impact on model training and validation, which is generally overlooked. Neural networks outperform standard ML techniques in noisy, complicated, and high-dimensional SOP data [11], making classical models subject to overfitting. Hybrid DL techniques have already demonstrated potential for fiber fault detection [12].

Building on our previous works, we have used SOP data as a critical feature within our neural network-based detection model. By learning normal and critical polarization patterns, the sensing model enhances its ability to identify and differentiate between various optical threats in real-time, with minimal impact on the underlying transmission quality. We investigate the ability of DL models, such as convolutional neural networks (CNNs), long short term memory (LSTM), and gated recurrent units (GRUs), to effectively categorize polarization signs in real-time while optimizing computational resources. Our research provides a thorough examination of the trade-offs between accuracy, computational resources, and model complexity, ultimately envisioning the development of a resilient and efficient self-healing fault detection systems for optical networks.

II. Polarization State Analysis

The SOP of an optical signal characterizes the orientation of the electric field vector as it propagates through an optical fiber. It can be circular, elliptical, or linear, describing the different ways the electric field can be oriented. In dynamic optical environments, the SOP can fluctuate due to physical disturbances, stress, wind, temperature variations, or intentional intrusions, compromising security. Observing the trajectory of the polarization state on the Poincaré sphere, facilitates the study of the SOP to identify subtle birefringence variations induced by external mechanical disturbances (e.g., drilling vibrations).

Due to sensitive nature of SOP, we developed a framework that continuously monitors the fiber variations, from telemetry data, allowing for early detection of damage or anomalies. The four stokes parameters $\{S_0, S_1, S_2, \text{and } S_3\}$ represent the polarization state of electromagnetic waves, or light. The total intensity or strength of the optical beam or light is represented by S_0, whereas the other three components, $\{S_1, S_2, \text{and } S_3\}$, correspond to different positions in the Poincaré sphere's geometry.

TABLE I: Categorization of Collected Polarization Signatures

Abbr.	Event Type	Description
bl	Baseline	No impact on fiber integrity.
s_1	Shaking (1 Hz)	Normal; ambient environmental noise.
s_3	Shaking (3 Hz)	Normal; minor disturbances.
s_5	Shaking (5 Hz)	Normal; sustained mechanical stress.
c_7	Shaking (7 Hz)	Critical; possible fiber cut.
c_10	Shaking (10 Hz)	Critical; possible fiber cut.
sh_1	Small Hit (1 tap/s)	Normal; localized impact.
sh_2	Small Hit (2 tap/s)	Critical; repeated striking to damage the fiber.

In the context of multi-threat detection, SOP variations are particularly valuable as certain physical-layer attacks, such as fiber bending, tapping, fiber cut, shaking, or intrusion attempts, can induce abrupt or characteristic changes in polarization. For example, tapping may slightly perturb the fiber, that creates measurable deviations in SOP. These subtle changes remain undetectable through traditional signal metrics such as power or bit error rate, but does exploit the SOP due to its exceptional sensitivity. Such intrinsic properties of SOP have led us to use it as an early warning metric to detect any unforeseen or upcoming anomaly, in order to protect from large-scale disruption. To enable SOP monitoring, a polarimeter is typically deployed at the receiver or intermediate points, continuously recording stokes parameters on the Poincaré sphere. These measurements, when sampled over time, form temporal polarization fingerprints that are fed into a neural networks for classification and anomaly detection.

A. Data Collection

The data was collected in a controlled lab environment, using an Arduino-controlled robotic arm, to generate various events. Each event generates a unique signature of polarization. This paper provides an overview of the experimental setup for identifying anomalies in optical fibers, which was previously outlined in our research on real-time anomaly detection using AI/ML approach [9]. Our experimental testbed consists of a continuous wave (CW) laser source that emits unmodulated light at 1530 nm, with a power of 6 dBm. We have two G.652 SMF, 8 km and 5 km long, acting as sensors. These are connected to a third SMF segment which is manipulated by a robotic arm for event generation.

At the receiving end, a polarimeter (Novoptel PM1000) is connected, which captures the temporal evolution of the stokes parameters. The robotic arm manipulates the fiber to induce some anomalous mechanical events, as outlined in Table I, such as shaking and tapping. The data is collected from the polarimeter, in the form of stokes parameters S_1, S_2, S_3 with a sampling rate of 3.1 kHz, fulfilling the Nyquist theorem. S_0 was removed from our analysis, since it describes the total output power and is unaffected by SOP

variations. We collected eight fingerprints with the sampling time of 0.3 ms. Each event was captured for a period of 11.5 minutes. However, we collected 2,139,000 data points for each individual event. These stoke parameters were then normalized and standardized to remove any ambiguity and ensure consistency across the data. This data was then fed into our deep learning models as input, which is discussed in detail in Section V

B. Polarimetric Fingerprints

Every event has an unique polarization pattern or signature due to the sensitive nature of SOP. We collected eight unique fingerprints, each serving as an anomaly with different severity levels. The main purpose is to detect harmful or critical mechanical events on the installed fiber infrastructure and take preventive measures, ensuring network integrity. The concise overview of different events and their potential impact on fiber integrity are described in Table I, where "*bl*" refers to those that have no effect on the integrity of the fiber. Shaking events (*s_1*, *s_3*, *s_5*, *sh_1*) correlate to various frequencies of ambient or mechanical vibrations, ranging from low-frequency ambient noise to moderate disturbances that may result in minor stress. Critical events like (*s_7*, *s_10*, *sh_2*), indicate potential fiber damage like cuts or intrusions.

All these fingerprints were collected as stokes parameters from the polarimeter. These parameters quantify SOP of the light beam, emerging from the experimental setup. Each value corresponds to one of the normalized stokes parameters, indicating linear and circular polarization components. During the events [*s_1: s_5*], the robotic arm moves up and down with frequencies varying from 1-5 Hz and a deviation angle of $60°$. For the critical shaking (*s_7*, *s_10*), the fiber shakes at the frequencies of 7 and 10 Hz. This behavior suggests that at this shaking frequency, the light's polarization state is only slightly altered. The amplitude of the oscillations is substantially reduced at higher frequencies than at lower shaking frequencies (for example, 7 Hz), indicating a damping or filtering effect. *sh_1* and *sh_2* refer to small mechanical taps or hit on the fiber, with frequencies of 1 and 2 tap per second and angle of deviation $40°$.

Consequently, it was observed that, as the intensity of shaking increases, the fluctuation range in the stokes parameters diminishes. This decrease in the range of variation implies that the polarimetric response's variation band narrows as the shaking frequency rises because the stokes parameters become less sensitive to the changes. After being collected, these fingerprints are then processed like noise filtering, and normalized, before transmitting to an DL framework. DL promptly labels the low frequency vibrations as normal, and the high vibration as critical, indicative of a potentially malicious or damaging event such as nearby drilling, leading to a fiber cut.

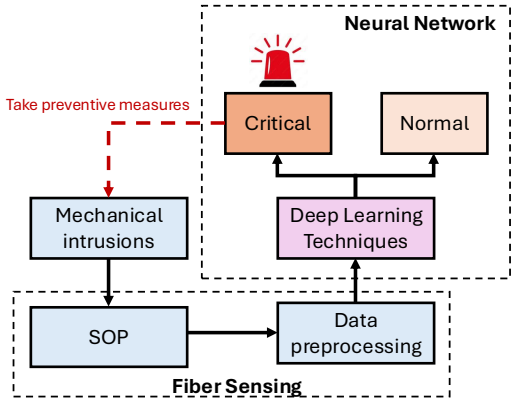


Fig. 1: Multi-threat proactive alarm system model.

III. Framework for SOP Sensing

In Fig. 1. we propose a proactive restoration approach based on real-time SOP monitoring. Our fiber sensing model continuously monitors any physical disturbance or intrusion in the optical fiber via collecting and processing SOP data. Particularly, the raw SOP data collected is passed to the preprocessing stage, where it is cleaned and scaled for further analysis. Once preprocessed, the data is fed into neural networks, where different deep learning techniques, namely CNN, and two types of recurrent neural network (RNN) – LSTM and GRU – are applied. The neural network based model has to be fast enough, not only to detect any critical anomalies in the installed fiber infrastructure, but also to trigger an alarm within the telemetry system [13]. If the model classifies any event as critical, indicating a hostile intrusion or fiber cut, the system triggers an alarm. As a countermeasure, preventive measures are taken based on the severity of the event, which may involve the controller rerouting the network traffic to a spare optical path or notifying the network operators. This intelligent system can promptly identify the potential threats and respond in time through continuous monitoring and analysis of SOP data, which ensures the reliability and security of optical communication networks. While the core idea is still in line with our earlier research, we have enriched our event classification spectrum and significantly expanded the dataset, enabling the application of DL techniques to evaluate their effectiveness. This study is a major step forward in terms of both scale and approach. In our previous study, we used a relatively small dataset and conventional ML approaches to show that proactive restoration is feasible for a restricted number of network event categories. The small event spectrum and the minimal complexity of the models used, affected the categorization capabilities, despite the encouraging results. In this work, we expanded the classification spectrum to encompass a greater range of real-world optical failures. Furthermore, by adding additional representative samples that more accurately reflect the noise and unpredictability found in operational situations, we have greatly expanded the size

and diversity of our dataset.

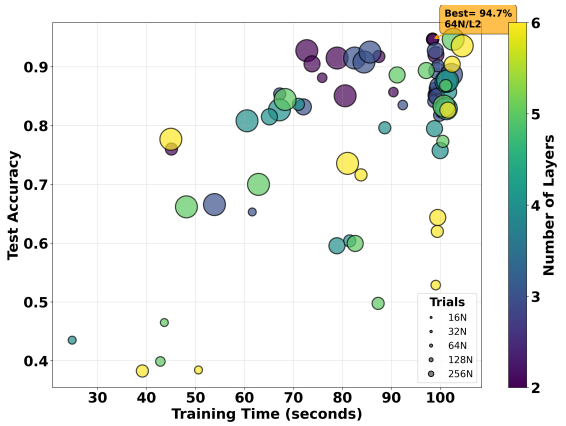
IV. Neural Network/Deep Learning Models for Multi-Threat Analysis

We analyzed a number of DL models, including CNNs, RNNs, such as LSTM networks, and GRUs, to precisely identify various physical-layer threats in optical transport networks. These architectures are selected based on their ability to capture temporal, spatial, and structured data patterns; these attributes are in line with the SOP time-dependent variations and other optical signal metrics. Our goal is to create a framework that responds proactively to possible threats, particularly those involving external activities such as drilling or fiber hitting, which could jeopardize network integrity. These models' capacity to discern between benign environmental factors and malicious or critical events makes them essential to assure the security and dependability of optical transport networks. We split the dataset into 70% for training and validation and reserve 30% for testing. Following that, we introduced some noise to emulate real-world environment, which includes environmental factors commonly observed in deployed optical networks. By training these models on labeled datasets representing normal and critical states, we evaluated their effectiveness in multi-threat classification and anomaly detection tasks.

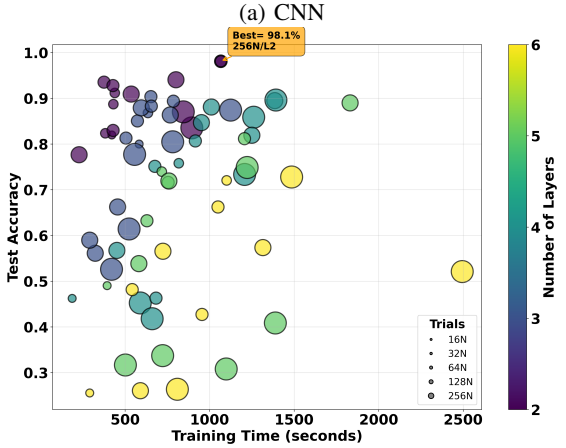
A. Model Descriptions

CNNs are an implementation of deep neural networks [14], which are utilized for their strength in extracting spatial features, information and local patterns from raw data derived from SOP signals and power variations. They don't require any manual feature engineering. This ability to learn and automatically discover the polarization trends from the raw stokes parameters, provides a substantial advantage over the traditional classification techniques. In our CNN model, we have used a sequence length of 500 and a batch size of 64. We have trained the model using AdamW optimizer and cross-entropy loss, which makes it suitable for classification tasks. CNN learns the complex patterns of the data at each layer of the network, in a hierarchical manner.

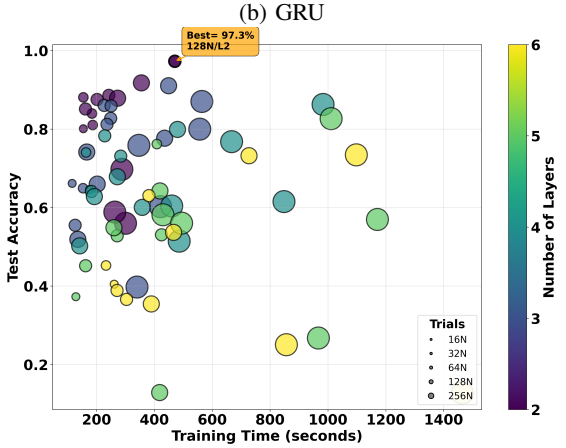
RNNs, along with their gated variants LSTM and GRU, are deployed to model the temporal dynamics inherent in optical signal data. RNNs have specifically been tailored to process sequential data, where the output is dependent of the previous data. This characteristic makes them suitable for our time-series analysis of the SOP, as it learns long-term dependencies, making them suitable for detecting threats that evolve gradually or exhibit temporal signatures like critical events. LSTMs are well-suited to our data's time-series structure because they successfully capture the long-term dependencies and temporal dynamics required to recognize polarization state changes caused by external factors [15]. GRU is also used to analyze sequential data, using the gating mechanism to control information flow and identify



(a) CNN



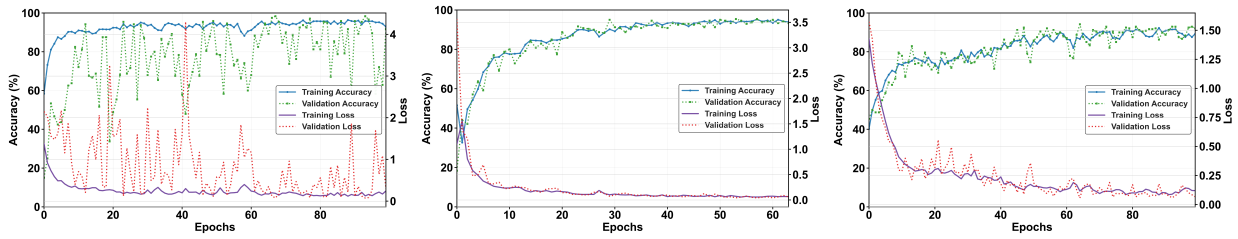
(b) GRU



(c) LSTM

Fig. 2: Performance comparison of CNN, LSTM and GRU models for different layer depth and neurons/layer.

long-term SOP variations [16]. It improves the performance of standard RNNs, that is, the vanishing gradient problem, which results in difficulties in learning long-term variations of the data. It consists of two gates, update gate and reset gate. The update gate decides on which part of the previous memory should remain, allowing the network to remember crucial SOP fluctuations over rather long sequences, whereas the reset gate selects what information should be dropped,



(a) CNN (b) GRU (c) LSTM

Fig. 3: Convergence behavior of the three considered models: Training and Validation accuracy/loss across epochs

thus discarding data or features that add minimal value to the classification problem. However, to manage class imbalance, both LSTM and GRU are trained with AdamW optimization and focal loss across 100 epochs. We also used an early-stopping mechanism, in which if validation accuracy does not improve after 20 epochs, training is terminated early. GRU also incorporated an attention mechanism, to improve the model performance for long-term variations. This memory mechanism makes the GRUs very suitable for applications with significant SOP fluctuations, such as detecting the tiny and progressive perturbations in optical networks (e.g., leading to fiber cuts). The comparative performance analysis reported in the next section helps to identify the most suitable architecture for real-time deployment in optical transport monitoring systems.

V. Results and Discussion

In this section, we discuss the performance analysis for all three DL models trained over the multi-threat dataset. We initially assessed how model depth and neuron count influence accuracy, loss convergence, and training behavior. We then analyzed the best-performing configurations of each model through training and validation curves. Finally, we concluded by evaluating the performance in terms of computational aspects, such as memory, inference time, CPU consumption, and overall load to determine which model provides the optimal balance for real-network deployment.

To evaluate the challenges faced by the DL models, we have trained them using various number of hidden layers [2-6]. For each trial (number of layers), we experimented with different ranges of neurons [32, 64, 128, 256] to better highlight the performance for the three considered models, as shown in Fig. 2. Each bubble corresponds to each trial of a model, with the bubble size representing the number of neurons and the color representing the number of layers in each neural network model. Fig. 2a. displays the performance of CNN with varying the layers of each configuration. It relates the training duration of each trial to the test accuracy [17, 18] (the proportion of properly identified samples out of the total number of samples). We altered the amount of hidden layers and neurons, with each trial represented by a circle. The top-performing trial was a 2-layer model with an accuracy of 94.7% in 98.42 seconds of training time. This demonstrates that a 2-layer (64 neurons) CNN model surpasses the other trials by striking the best balance of accuracy and efficiency. The analysis also reveals that the majority of the trials had training times of more than 80 seconds.

Fig. 2b., showing the results obtained with GRU, highlights that with increasing the number of layers, the accuracy in predicting the events can be increased by the expense of augmented complexity. The standout trial is a 2-layer GRU model (with 256 neurons), achieving an accuracy of 98.1%. However, as it can be observed, training this model requires an extended training period (1065.9 seconds). The worst performance trial is the 6-layer model (with 16 neurons), indicating that increasing the number of layers does not necessarily improve model performance. It can be seen that, in contrast to CNN, which achieves peak performance faster, GRU requires extensive computational resources to acquire a better level of accuracy.

In Fig. 2c., the best trial for LSTM is a 2-layer model (with 128 neurons), which achieves an accuracy of 97.3% with a moderate training time of 470.54 seconds. It shows that a moderately complex LSTM model performs better, offering a trade-off between accuracy and computational cost, for real-time multi-threat detection in optical transport networks. The evaluation in Fig. 2. demonstrates that the most complex models do not necessarily provide the highest accuracy. Interestingly, the computational resources also play a vital role in characterizing the performance of a model for deployment in real-networks. Among the three DL models, GRU achieved the peak accuracy (98.1%), but at the cost of high training overhead. However, LSTM is an interesting alternative because it requires less computational resources, making it a practical candidate for deployment in live optical network monitoring environments.

After evaluating several configurations, we picked the optimum trial for each model and analyzed their training and validation accuracy and losses, as shown in Fig. 3.. For instance, Fig. 3c. and Fig. 3b. exhibit consistent learning behavior as both their training and validation curves are closely aligned to each other. This indicates that both recurrent models (LSTM and GRU) capture the temporal dependencies of SOP more effectively, and generalize adequately to the unseen data.

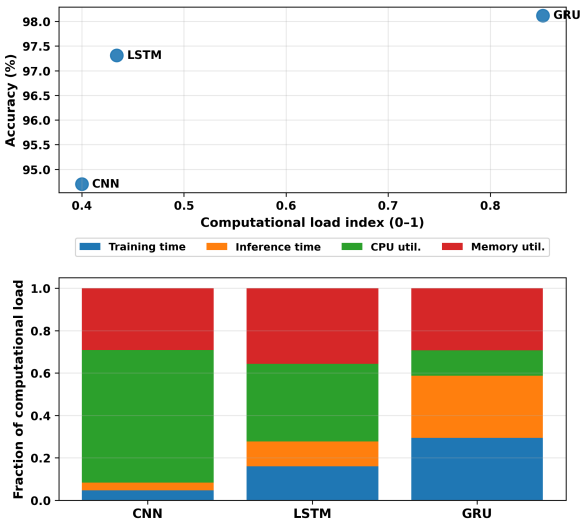


Fig. 4: Comparative accuracy and load distribution across CNN, LSTM, and GRU.

Conversely, Fig. 3a. depicts a large discrepancy between the training and validation trends, which shows that the model extracts the spatial features, and not long-term temporal fluctuations in the data. The critical events such as {*c_7*, *c_10* and *sh_2*} have subtle polarization changes and because CNN doesn't have memory (like RNNs), it is unable to model and memorize these variations in the unseen data, which leads to poor validation consistency. This results in overfitting the data in the training set SOP patterns, compromising its ability to correctly identify unseen polarization signatures and resulting in lower validation stability. In contrary, both LSTM and GRU show a stable convergence between accuracy and loss, due to their ability to capture long-term temporal SOP dependencies. GRU converges significantly quicker, although with slightly higher variance in validation loss due to its reduced gating method, while still achieving strong generalization.

Fig. 4. compares the three DL models in terms of test accuracy and computational cost. The top plot shows accuracy versus the computational load index (CLI). The CLI is computed by normalizing training time, inference time, average CPU usage, and average memory usage, and combining them with equal weights. This results in a normalized score (0–1) that reflects the relative computational load of each model. The results show that CNN has the lowest load but also the lowest accuracy, LSTM provides a balanced trade-off, and GRU achieves the highest accuracy but with the highest computational load. The normalized bottom plot decomposes the CLI into its four components, showing the contribution of each metric to the overall load. The breakdown also highlights how inference time contributes to the total computational load, with CNN showing the lowest inference time, LSTM moderate values, and GRU the highest. The overall breakdown highlights that GRU's improved accuracy comes at the cost of higher inference latency and memory usage, which is important when selecting a model for real-time detection in operational optical networks.

VI. Conclusion

This work demonstrated that SOP-based sensing combined with deep-learning models can reliably detect physical-layer disturbances in optical fibers. Among the evaluated models, GRU achieved the highest accuracy, LSTM provided the best accuracy-to-complexity trade-off, and CNN offered the lowest computational load. The CLI enabled a unified comparison of model costs. Overall, the results show that lightweight DL models can support real-time disturbance detection for improved monitoring and protection in optical transport networks. In future, we will incorporate a diverse dataset and integrate with autonomous network systems for proactive restoration and improved physical-layer security.

References

[1] F. Boitier *et al.*, "Proactive fiber damage detection in real-time coherent receiver," 09 2017, pp. 1–3.

[2] M. Hoffman, "Cable cuts." [Online]. Available: http://all.net/CID/Attack/papers/CableCuts.html

[3] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection prevention," in *IEEE MILCOM 2004. Military Communications Conference, 2004.*, vol. 2, 2004, pp. 711–716 Vol. 2.

[4] A. P. Vela *et al.*, "Ber degradation detection and failure identification in elastic optical networks," *Journal of Lightwave Technology*, vol. 35, no. 21, pp. 4595–4604, 2017.

[5] C. Natalino *et al.*, "Root cause analysis for autonomous optical networks: A physical layer security use case," in *2020 European Conference on Optical Communications (ECOC)*, 2020, pp. 1–4.

[6] X. Chen *et al.*, "Automating optical network fault management with machine learning," *IEEE Communications Magazine*, vol. 60, no. 12, pp. 88–94, 2022.

[7] K. Abdelli *et al.*, "Machine-learning-based anomaly detection in optical fiber monitoring," *JOCN*, vol. 14, no. 5, pp. 365–375, 2022.

[8] G. Malik *et al.*, "Machine learning for predictive multi-event detection in fiber optic systems," in *International Conference on Machine Learning and Communication Networks (ICMLCN)*, 2025.

[9] ——, "Sop-based anomaly detection leveraging machine learning for proactive optical restoration," *Optical Newtork Design and Modeling (ONDM)*, 2025.

[10] ——, "Resilient anomaly detection in fiber-optic networks: A machine learning framework for multi-threat identification using state-of-polarization monitoring," *AI*, vol. 6, no. 7, 2025.

[11] J. E. D. Albuquerque Filho *et al.*, "A review of neural networks for anomaly detection," *IEEE Access*, vol. 10, pp. 112 342–112 367, 2022.

[12] K. K. Soothar *et al.*, "Optimizing optical fiber faults detection: A comparative analysis of advanced machine learning approaches," *Computers, Materials and Continua*, vol. 79, no. 2, pp. 2697–2721, 2024.

[13] G. Malik *et al.*, "Ai-driven fault prediction and restoration leveraging real-time sop monitoring," in *2025 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2025, pp. 1–6.

[14] T. Tanimura *et al.*, "Data-analytics-based optical performance monitoring technique for optical transport networks," in *OFC Conference*. Optica Publishing Group, 2018, p. Tu3E.3.

[15] S. Cruzes, "Failure management overview in optical networks," *IEEE Access*, vol. 12, pp. 169 170–169 193, 2024.

[16] Z. Yi *et al.*, "A signal detection method based on bigru for fso communications with atmospheric turbulence," *Photonics*, vol. 12, no. 10, 2025.

[17] "Support vector regression to predict power consumption,university of new mexico," 2024.

[18] "Classification assessment methods, applied computing and informatics," vol. 17, no. 1, 2021.