CHALMERS
UNIVERSITY OF TECHNOLOGY

ML-based State of Polarization Analysis to Detect Emerging Threats to Optical Fiber Security

Citation for the original published paper (version of record):
Sadighi, L., Karlsson, S., Natalino Da Silva, C. et al (2025). ML-based State of Polarization Analysis to Detect Emerging Threats to Optical Fiber Security. IEEE Transactions on Network and Service Management, In Press. http://dx.doi.org/10.1109/TNSM.2025.3607022

(article starts on next page)

ML-based State of Polarization Analysis to Detect Emerging Threats to Optical Fiber Security

Leyla Sadighi, Stefan Karlsson, Carlos Natalino, Marija Furdek

***Abstract*—As the foundation of global communication networks, optical fibers are vulnerable to various disruptive events, including mechanical damage, such as cuts, and malicious physical layer breaches, such as eavesdropping via fiber bending. Traditional monitoring methods often fail to identify subtle or novel anomalies, stimulating the proliferation of Machine Learning (ML) techniques for detection of threats before they cause significant harm. In this paper, we evaluate the performance of Semi-Supervised Learning (SSL) and Unsupervised Learning (USL) approaches for detecting various abnormal events, such as fiber bending and vibrations, by analyzing polarization signatures with minimal reliance on labeled data. We experimentally collect thirteen polarization signatures on three different types of fiber cable and process them using One-Class Support Vector Machine (OCSVM) as an SSL, and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) as a USL algorithm for anomaly detection. We introduce tailored evaluation metrics designed to guide hyper-parameter tuning and capture generalization over different anomaly types, detection consistency, and robustness to false positives, enabling practical deployment of OCSVM and DBSCAN in optical fiber security. Our findings demonstrate DBSCAN as a strong contender to detect previously unseen threats in scenarios where labeled data are not available, despite some variability in performance between different scenarios, with F1 score values between 0.615 and 0.995. In contrast, OCSVM, trained on normal operating conditions, maintains high F1 scores of 0.98 to 0.998, demonstrating accurate detection of complex anomalies in optical networks.**

***Index Terms*—State of Polarization (SOP) variations, Machine Learning (ML), anomaly detection, Semi-Supervised Learning (SSL), Unsupervised Learning (USL), One-Class Support Vector Machine (OCSVM), Density-Based Spatial Clustering of Applications with Noise (DBSCAN).**

I. Introduction

FIBER optic networks form the foundation of modern telecommunications, enabling high-speed, long-distance, and reliable data transmission with minimal signal loss. In addition to backbone and long-haul networks, fibers are also deployed in the access segment, forming, e.g., Passive Optical Networks (PONs) that deliver broadband connectivity to end users. They connect regions and nations, supporting global connectivity and critical systems such as the Internet, government, financial, and healthcare networks.

Optical networks are vulnerable to physical threats such as fiber cuts, reportedly causing up to 60% of failures [1], [2]. A leading cause of fiber cuts are construction works, where the operation of heavy excavator machinery induces vibrations as a cut predecessor [3]. Fibers are also exposed to covert security risks from evanescent coupling and fiber bending [4], [5], which can compromise data confidentiality via eavesdropping, without affecting signal quality. Another security vulnerability arises from unauthorized signal access through unused or improperly secured ports, such as monitoring outputs or unused branches of optical splitters [6]. These access points, often overlooked during installation or maintenance, can be exploited by malicious actors to tap into the optical signal without introducing noticeable attenuation or disrupting service.

Quick detection and response to a range of anomalies is critical for safeguarding fiber optic networks. Techniques like Optical Time Domain Reflectometry (OTDR), based on Rayleigh backscattering, aid fault detection and localization of large-scale physical faults, such as sharp bends or fiber breaks [7], [8], [9], but face scalability and cost challenges [10], and exhibit limited sensitivity to detect subtle disturbances, such as minor mechanical vibrations and small-radius bends. Alternative methods such as Distributed Fiber Optic Sensing (DFOS) for intrusion detection [11] are effective yet complex and expensive, requiring high-speed lasers, diplexers, and advanced backscattering analysis.

Recent advancements rely on the existing optical fiber infrastructure for environmental sensing [12], successfully detecting natural and human-induced activities [13], [14]. A key enabler for such sensing is the State of Polarization (SOP), which is highly sensitive to mechanical disturbances. SOP is characterized by the Stokes parameters, organized into a four-element Stokes vector, $\mathbf{S} = [S_0, S_1, S_2, S_3]$, and represented on the Poincaré sphere for visual interpretation [2]. Mechanical stress, temperature changes, bending, and vibrations impact fiber birefringence, altering polarized light transmission and modifying the SOP [2]. SOP-based sensing is cost-effective, as modern Polarization-Multiplexed Quadrature Amplitude Modulation (PM-QAM) coherent receivers inherently track SOP for signal demodulation, eliminating the need for additional hardware [15]. SOP-based analysis leverages the inherent sensitivity of polarization to both benign and malicious disturbances, including covert eavesdropping attempts, and is capable of detecting subtle, short-duration, or overlapping events without relying on backscatter or reflection signatures. Thus, SOP-based monitoring simplifies the detection process, avoiding the complexity and cost of DFOS or OTDR.

Effective monitoring of polarization changes is essential to identify disturbances and maintain network integrity. However, SOP-based monitoring systems that rely on fixed rules and

L. Sadighi, C. Natalino, and M. Furdek are with the Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden.
S. Karlsson is with Micropol Fiberoptics AB, Stockholm, Sweden.

This work was supported by the Swedish Research Council (2023–05249) and the European Commission's Digital Europe Programme (101127973) through the 5G-TACTIC project.

thresholds struggle to handle evolving threats [16], especially those that induce complex changes in the SOP. To overcome these limitations and enable scalable, automated, and adaptive analysis of polarization signatures, recent research has shifted toward data-driven approaches that leverage Machine Learning (ML) as a critical monitoring technique in SOP-based fiber sensing, enabling models to learn and distinguish complex disturbance patterns from polarization data.

In the context of anomaly detection, polarization signatures can be defined as a sequence of the magnitude of polarization variations in a specific time and frequency, derived after processing the SOP variations data [17]. The derived polarization signatures are plotted in a waterfall diagram. These plots, unique for each event, help differentiate legitimate actions from eavesdropping, offering a cost-effective solution to security challenges. However, the method relies on manual interpretation by technicians, which requires expertise, time, and does not scale. Instead of focusing on image and vision-based analysis of SOP, our prior research [18], [19], [20], [21] employed sampling techniques and Fast Fourier Transform (FFT) processing on SOP and calculated the numerical value of changes in SOP to derive an SOP signature for each event type.

While Supervised Learning (SL) techniques show remarkable potential for the detection and classification of polarization signatures, their reliance on labeled datasets may be limiting for real-world applications. Labeling polarization events, especially in large-scale optical networks, is often labor-intensive, costly, time-consuming, and requires domain expertise, making it impractical for network-wide monitoring and timely anomaly detection. To overcome these challenges, this work investigates the potential of Semi-Supervised Learning (SSL) and Unsupervised Learning (USL) techniques to efficiently analyze and detect optical fiber events with minimal or no reliance on labeled training sets. By leveraging the intrinsic patterns within the data, SSL methods can learn from a small set of normal labeled data, while USL techniques such as clustering can identify patterns and outliers without any prior label knowledge. This shift towards more flexible and scalable ML techniques is essential to improve the robustness and effectiveness of fiber optic network monitoring, particularly in complex and dynamic environments where manual labeling is not feasible, or new threats, previously untrained for, may emerge. In this paper, we consider One-Class Support Vector Machine (OCSVM) as an SSL technique and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) as a USL method to tackle the challenge of anomaly detection in fiber optic sensing, where labeled data is scarce or costly to obtain. We apply these methods to the thirteen experimental scenarios described in [18], covering an extensive spectrum of events possibly affecting fiber optic installations across three cable types.

The rest of the paper is structured as follows. Section II overviews recent advancements in ML-based anomaly detection for optical networks. Section III describes the experimental setup and the data collection process for generating polarization signatures under various conditions. Section IV details the employed ML methodology, focusing on the data pre-processing and hyper-parameter tuning of OCSVM and DBSCAN. Section V analyzes experimental results, and Section VI concludes the paper.

II. Related Work

SL techniques, which rely on labeled data to train models for event detection and classification, have been proliferating in recent studies. In [22], a transfer learning strategy was proposed that leverages unrelated image datasets to improve SOP-based classification performance when labeled data are scarce. A follow-up work introduced a Vision Transformer framework for anomaly detection and localization using SOP time-series inputs, highlighting the effectiveness of deep attention mechanisms in optical monitoring [23]. Most recently, SOP spectrogram representations were combined with Vision Transformers to further enhance anomaly classification and localization accuracy in complex network scenarios [24]. Despite their advantages, SL techniques often struggle with complex scenarios involving overlapping effects, such as operational stress, harmful vibrations, and covert attacks, leading to reduced accuracy in distinguishing harmful from benign events in real-world deployments.

To address these challenges, our prior work combined robust SOP signature extraction with advanced SL models to improve accuracy in real-world conditions. In [18], polarization signatures from three cable types under thirteen scenarios were analyzed, with eXtreme Gradient Boosting (XGBoost) achieving 92.3% accuracy in classifying eavesdropping and other events. In [19], a polarization-based fiber sensor with supervised ML achieved 97.94% accuracy using Histogram Gradient Boosting (HGB) to distinguish harmful from non-harmful events on an indoor cable. In [20], we analyzed noisy SOP data from OpenIreland's live network [25] in Dublin, achieving 86.5% accuracy using the HGB classifier, demonstrating robustness in real-world conditions. In [21], we applied Deep Learning (DL) models to a broader, noisier dataset, improving accuracy to over 91%. The work in [26] presented a supervised Convolutional Neural Network (CNN)-based scheme for detecting fiber-bending eavesdropping at different bending radii (10.8 mm, 12.1 mm, 15 mm) in coherent optical systems based on the polarization data.

Despite the clear advantages of SSL and USL techniques for optical network monitoring and anomaly detection, to the best of our knowledge, no prior work has explored their application to polarization signature analysis for anomaly detection in optical fibers. The work in [27] proposed a combined USL and SL framework that utilized power spectral density and Signal-to-Noise Ratio (SNR) data to identify anomalies in optical networks. Recent studies, such as [15] and [28], have proposed advanced Digital Signal Processing (DSP)-based techniques for anomaly detection in polarization state, validated on metropolitan fiber links using mechanical shakers to introduce various vibration types. In contrast to these advanced DSP techniques, our study presents a new perspective on anomaly detection in optical fibers. While the work in [29] leveraged an USL approach using bisecting k-means clustering on Optical Performance Monitoring (OPM) data to detect and

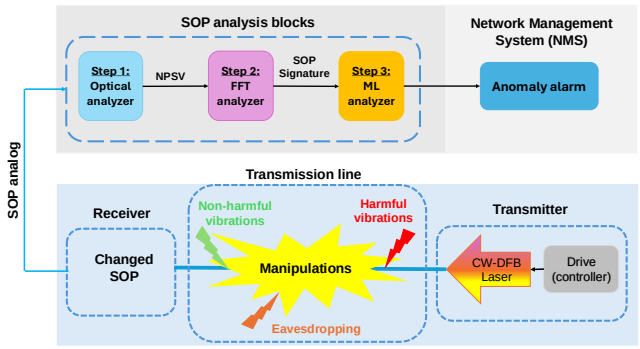


Fig. 1. A schematic of the system used to generate and analyze the SOP signatures.

localize eavesdropping in Wavelength Division Multiplexing (WDM) networks, our work analyzes SOP dynamics to detect a broader range of subtle anomalies, including those not evident through power-level changes. The work in [30] reported on an SOP-based system for detecting physical disturbances in optical fibers using SSL anomaly detection models, including thresholding and autoencoders. In this paper, we employ SSL and USL techniques to detect a wide range of anomalies in polarization signatures, including eavesdropping, harmful and non-harmful vibrations, and overlapping events directly from raw SOP data, eliminating the need for labeled data and enhancing adaptability to unknown threat types.

III. Testbed and Collected Signatures

The experimental configuration used to generate, record, and analyze polarization signature data is depicted in Fig. 1. It consists of a transmitter, transmission line, receiver with a polarization measurement system, and SOP processing units.

The transmitter includes a Continuous Wave Distributed Feedback (CW-DFB) laser emitting light at 1310 nm with polarization-maintaining properties. The laser is controlled by a driver that maintains a constant power level and temperature, ensuring stable operation. The optical signal is transmitted through a transmission line which is a serial structure of three different optical cables: Fiber Optical tactical Cable System (FOCS) cable, an indoor Single Mode (SM) cable, and a bare G.657.A SM bend-insensitive fiber. The CW-DFB laser is transmitting optical power occupying one of the available wavelengths in the O, E, S, C, or L-band of the network. In order to mimic real-world threat scenarios, we apply targeted manipulations to each cable type. These actions produce polarization signatures that characterize each specific event, crafted to simulate conditions typically linked to eavesdropping attempts, as well as both harmful and benign mechanical vibrations. The receiver obtains the transmitted signal and carries out the SOP analysis using the three steps described as follows.

Step 1: The optical analyzer is used to quantify changes in the SOP. The acquired optical SOP signal is mapped onto the Poincaré sphere to visualize and track polarization variations. To convert the analog signal into a digital format, a sampling mechanism is employed, which captures the SOP on the Poincaré sphere at intervals of 1 ms. This process is carried out over a 20-minute recording period, resulting in a total of 1.2 million samples per event. Subsequently, the numerical vectorial distance between the SOP at two consecutive sampling points is calculated using:

$$\text{NPSV}_t = \sqrt{(\Delta S_1(t))^2 + (\Delta S_2(t))^2 + (\Delta S_3(t))^2} \quad (1)$$

with $\Delta S_i = S_i(t) - S_i(t-1)$.

Step 2: The FFT analyzer further processes the data. FFT with hamming window [31] and 512 frequency bins is applied to concatenated 1-second Numerical Polarization State Variation (NPSV) data segments of 1,000 elements each. The result is a power spectrum data set of 1,200 samples (or rows, corresponding to time slots) and 512 samples (or columns, corresponding to frequency bins). The output of this step characterizes the polarization dynamics for each event type, referred to in this paper as *SOP signatures*.

Step 3: The collected signatures are analyzed by the ML analyzer. It applies techniques for detecting anomalies that may indicate harmful vibrations or eavesdropping attempts. The detected anomalies are communicated to the Network Management System (NMS), which oversees network health, raises alarms, and responds to potential threats. The considered approach is aimed at detecting the presence of anomalies at an affected fiber link, without providing the precise localization along the link.

Using the described experimental setup, we collect data from thirteen experimental scenarios, comprising normal and/or abnormal events. Normal considered events include the relaxed fiber without vibrations or eavesdropping (denoted as *rlx*) as well as non-harmful vibrations which might stem from equipment like fans, nearby traffic, or benign interactions with the network infrastructure. Since capturing all types of normal vibrations in real-life scenarios is complex, this study simulates normal vibrations using 130 Hz (denoted as *130vb*) and 155 Hz (denoted as *155vb*) frequencies, representing fans with speeds of approximately 7,000 and 9,000 Revolutions Per Minute (RPM). We deliberately selected frequencies close to each other in order to test the sensor system and ML models' ability to distinguish between similar vibration signatures. To generate these vibrations in our testbed, we attached a piezo electrical engine to the optical cable, powered by a sinusoidal 155/130 Hz vibration. This vibration is transferred by the inner layer of the cable and interacts with the optical fiber, inducing changes in the SOP.

The abnormal events encompass potentially harmful vibrations and eavesdropping attempts. The harmful vibrations considered in this study include fiber vibrations at 80 Hz (denoted as *80vb*). An example of such malicious event is an excavator digging close to the installed fiber optical ground cable, which may result in an accidental or deliberate fiber cut, leading to a disruption in network traffic. A common excavator generally runs at 4,800 RPM. Since one minute equals 60 seconds, the fundamental tone of the excavator corresponds to a frequency of 80 Hz (4,800/60 = 80). While the full vibration spectrum includes a range of frequencies around 80 Hz, for detecting the presence of an excavator it is enough to detect the presence of the 80 Hz vibration. In commercial equipment,

TABLE I
COLLECTED SIGNATURES FOR BARE FIBER AND FOCS CABLE

Abbr.	Scenario	Justification
155vb_br	155 Hz vibration bare	Normal
155vb_fcs	155 Hz vibration FOCS	Normal
80vb_br	80 Hz vibration bare	Harmful; possible cut predecessor
80vb_fcs	80 Hz vibration FOCS	Harmful; possible cut predecessor
eav_br	Bending bare	Eavesdropping
eav_fcs	Bending FOCS	Eavesdropping

TABLE II
COLLECTED SIGNATURES FOR INDOOR CABLE

Abbr.	Description	Justification
rlx_idr	Relaxed fiber	Normal
155vb_idr	155 Hz vibration	Normal
80vb_idr	80 Hz vibration	Harmful; possible cut predec.
eav_130vb_idr	Bending + 130 Hz vibration	Eavesdropping + non-harmful
eav_80vb_idr	Bending + 80 Hz vibration	Eavesdropping + harmful
eav_80vb_130vb_idr	Bending + 80 Hz + 130 Hz vibrations	Eavesdropping + non-harmful + harmful
rlx_80vb_130vb_idr	Relaxed + 80 Hz + 130 Hz vibrations	Non-harmful + harmful

the entire bandwidth needs to be detected and analyzed in order to detect an excavator running with some other engine at different RPM. For the purpose of this paper, the main issue is to present a fiber optical sensor together with the ML model that can separate examples of malicious events from examples of normal events that can be experienced in a real-life fiber optical network. This vibration was simulated by a loudspeaker producing a sinusoidal tone of 80 Hz at 60 dBA volume (A-weighted sound level). The bare fiber was exposed to the tone at a distance of 5 cm from the membrane of the loudspeaker. The eavesdropping attack signatures (denoted as *eav*) are generated by bending the fiber over a 10 mm diameter rod. The bend radius is chosen to be 4 mm with a bend angle of 25 degrees.

To successfully perform eavesdropping, the eavesdropper must manipulate the fiber optic cable and expose the bare optical fiber that is protected within it. This process generates various signatures that can be detected. In our experiment, we considered three cable configurations: (i) bare (*br*) fiber, (ii) a standard indoor (*idr*) patch cable, and (iii) a military-grade FOCS (*fcs*) cable. These 3 cable types were deliberately selected to span a range of mechanical isolation levels. The bare optical fiber offers direct mechanical exposure and thus produces strong vibration signatures with high SNRs, serving as a baseline for unshielded conditions. The indoor patch cable, a commonly deployed fiber type, provides minimal isolation, allowing external vibrations to be readily coupled into the fiber and resulting in detectable signatures. In contrast, the FOCS tactical cable is designed for deployment in rugged environments, featuring a robust design that includes multiple protective layers. These layers provide substantial mechanical shielding, enabling the cable to withstand pulling forces up to 2,000 Newtons and resist damage from knotting. This construction significantly attenuates mechanical disturbances before they reach the fiber. As such, we expect the vibration signatures in the FOCS cable to have lower SNR.

For the bare and the FOCS cables, we consider one normal and two abnormal events, summarized in Table I. The normal event involves non-harmful vibrations at 155 Hz, denoted as *155vb_br* for the bare and *155vb_fcs* for the FOCS cable. The abnormal events include potentially harmful vibrations at 80 Hz, referred to as *80vb_br* and *80vb_fcs* for the two cables, as well as eavesdropping, denoted as *eav_br* and *eav_fcs*.

For the indoor cable, we consider two normal and five abnormal events, outlined in Table II. The normal events include a relaxed fiber without vibrations or eavesdropping (*rlx_idr*) and with vibrations at 155 Hz (*155vb_idr*). The abnormal events include potentially harmful vibrations at 80 Hz (*80vb_idr*) and a set of overlapping events: a combination of eavesdropping and non-harmful vibration at 130 Hz (*eav_130vb_idr*), a combination of eavesdropping and harmful vibration at 80 Hz (*eav_80vb_idr*), a combination of eavesdropping with dual-frequency vibrations at 80 Hz and 130 Hz (*eav_80vb_130vb_idr*), and a relaxed fiber subjected to both harmful and non-harmful frequency vibrations (*rlx_80vb_130vb_idr*). Overlapping events reflect real-world scenarios with fiber exposed to multiple simultaneous stressors, e.g., routine vibrations generated by fan ventilation or traffic, and intentional malicious activities, such as eavesdropping. They are specifically considered for the indoor cable because this environment is more likely to experience a variety of simultaneous disturbances, making it an ideal candidate to test the robustness of our anomaly detection models.

IV. ML-BASED ANOMALY DETECTION MODELS

To analyze the obtained SOP data, we use OCSVM as an SSL, and DBSCAN as an USL model. To evaluate the performance of our anomaly detection models, we use standard values derived from the confusion matrix: True Positives (TP), referring to correctly detected anomalies; False Positives (FP), referring to normal instances incorrectly flagged as anomalies; True Negatives (TN), referring to correctly identified normal instances; and False Negatives (FN), referring to anomalies that the model failed to detect. These values enable calculation of key evaluation metrics such as True Positive Rate (TPR) (also known as recall or sensitivity), measuring the proportion of actual anomalies correctly detected as TPR $= \frac{TP}{TP+FN}$; False Positive Rate (FPR) (FPR $= \frac{FP}{FP+TN}$), representing the fraction of normal data mistakenly flagged as anomalous; True Negative Rate (TNR) (also known as specificity), which measures the proportion of normal samples correctly identified (TNR $= \frac{TN}{TN+FP}$); and False Negative Rate (FNR), quantifying the proportion of anomalies that were missed by the model (FNR $= \frac{FN}{TP+FN}$). We also consider the Accuracy (acc), which measures the overall proportion of correctly detected instances (both normal and abnormal), and precision, defined as the ratio of correctly identified anomalies among all detected anomalies. The F1-score, computed as the harmonic mean of precision and recall, offers a balanced perspective on model performance by jointly considering false positives and false negatives. This makes it particularly relevant for

anomaly detection tasks, where both Type I (FP) and Type II (FN) errors are critical. In security-sensitive applications, FPR and FNR are especially critical: high FPR can overwhelm operators with false alerts, wasting resources, while high FNR may allow threats to go undetected, potentially leading to breaches or service disruptions. For clustering-based models like DBSCAN, we additionally use the Silhouette Score (SS) to assess the cohesion and separation of detected clusters, and the Adjusted Rand Score (ARS) to measure similarity between clustering results and ground truth labels while accounting for the possibility that some agreement may occur purely by random chance, rather than meaningful structure. Both OCSVM and DBSCAN models require careful data pre-processing of the collected SOP signatures and hyper-parameter tuning, detailed in the following.

A. One-Class Support Vector Machine (OCSVM)

OCSVM is a powerful ML algorithm widely used for anomaly detection, particularly in scenarios where the available data (predominantly) represents normal behavior, with the goal of detecting outliers or anomalies that deviate from this norm. OCSVM operates in a semi-supervised manner by learning the boundaries that encapsulates the majority of data points, assuming that they represent normal working conditions. The algorithm maps the input data into a high-dimensional feature space using a kernel function and then constructs a decision boundary that maximizes the separation between the origin and the data points in this feature space. Data points that fall outside of this boundary are detected as anomalies. The choice of kernel function and hyper-parameters, such as the kernel coefficient gamma (γ) and the regularization parameter (ν), is critical in determining the sensitivity of the model to outliers and its overall performance. During model inference, new data points are detected as normal if they fall within the boundary, and abnormal otherwise.

1) Data pre-processing for OCSVM: For each of the considered scenarios, the pre-processing phase begins by separating the dataset into subsets corresponding to normal operating conditions (referred to as normal scenario for brevity) and the malicious/harmful events (referred to as abnormal scenario). Table III summarizes the separation of training and test data for these scenarios. For each cable type, we created a training set of 900 samples from the normal condition and a test set of 1,500 samples, comprising 300 normal samples and 1,200 of the corresponding abnormal scenario samples. In the case§indoor cable, we considered two normal cases: relaxed fiber (case 1) and 155 Hz vibration (case 2). To assess the detector's behavior when exposed to all abnormal events, we introduced the *total* test sets that contain all respective abnormal events into a single evaluation case. This results in a larger test set comprising 300 normal samples and the cumulative 1,200-sample sets for each abnormal event (e.g., totaling 2,400 samples for bare and FOCS cables, and 6,000 samples for indoor cable cases). After data separation, we evaluated the impact of feature normalization on the performance of our OCSVM model. The results indicated that normalization did not confer any advantages; hence, normalization was not applied in the final analysis.

2) Tuning of OCSVM hyper-parameters: After data pre-processing, we tuned the main OCSVM hyper-parameters to improve OCSVM anomaly detection performance. This hyper-parameter tuning focused on exploring a grid of three parameters: the kernel type, ν, and γ. The γ parameter controls how much influence each training point has on the model. Smaller γ values produce smoother and more general decision boundaries, while larger values produce boundaries more close to the training samples. In our case, smaller values worked better. We also varied ν, which controls the fraction of data points in the training set allowed to be outliers. Our grid search considered a range of $[0.001, 0.5]$ for ν, $[10^{-7}, 0.5]$ for γ, and $\{\texttt{poly}, \texttt{rbf}, \texttt{sigmoid}\}$ for the kernel function.

For each hyper-parameter combination, we employed 5-fold cross-validation (CV), assessing the model performance across different training-validation splits. The mean and standard deviation (std) values obtained from the CV folds allows us to evaluate whether a certain hyper-parameter setting results in a model overly tailored to a specific data split. A key element of our model selection process is the use of a novel performance metric that we define in (2).

$$\textit{OCSVM\_perf} = avg\Big([TPR - FPR + \mathrm{CV}_{mean} - \mathrm{CV}_{std} - |\mathrm{acc}_{train} - \mathrm{acc}_{test}| + F1]\Big) \tag{2}$$

This metric was designed to balance the trade-offs between different evaluation criteria by averaging the TPR, FPR, CV_{mean}, CV_{std}, F1-score, acc, and the difference in accuracy between the training and the testing sets ($|acc_{train} - acc_{test}|$). After calculating the value of $OCSVM\_perf$ for each hyper-parameter combination, the models were ranked, and the model with the highest *OCSVM_perf* score was selected.

3) Results of hyper-parameter tuning for OCSVM: Tables IV and V summarize the selected hyper-parameters for each cable type and event scenario. The best hyper-parameter setting for each normal vs. abnormal scenario, as well as the *total* scenario are shown. The Radial Basis Function (RBF) kernel function consistently achieves the best result across all scenarios. For the bare fiber (Table IV, rows 1–3), the best selected hyper-parameters generally reflect a need for high sensitivity, as indicated by consistently low values of ν and γ, suitable for detecting subtle deviations in polarization caused by events like eavesdropping. In contrast, the FOCS cable (Table IV, rows 4–6), which offers greater insulation from environmental factors, exhibits a wider range of ν values across different scenarios, pointing to a more scenario-dependent sensitivity requirement. Nonetheless, the γ values for both cables remain within a relatively narrow band, reflecting the model's consistent preference for smoother decision boundaries. In *total* scenarios, moderate ν values were selected, indicating a balance between sensitivity and generalization across different types of disturbances.

For the indoor cable (Table V), where scenarios are more complex and involve overlapping events, ν values generally range from 0.001 to 0.02, with γ values tightly controlled between 1×10^{-5} and 3×10^{-5}. This configuration ensures that the model can effectively distinguish between normal and

TABLE III
SUMMARY OF THE CONSIDERED NORMAL AND ABNORMAL EVENTS FOR EACH CABLE TYPE, AND DATASET SEPARATION FOR OCSVM MODEL

Cable Type	**Normal event**	**Abnormal events**	**Training Set**	**Test Set**
Bare	*155vb_br*	*eav_br* *80vb_br* total (2 abnormal events)	900 of *155vb_br*	300 of *155vb_br* + 1,200 of *80vb_br* (1,500 Samples) + 1,200 of *eav_br* (1,500 Samples) + 2,400 of all abnormal events (2,700 Samples)
FOCS	*155vb_fcs*	*eav_fcs* *80vb_fcs* total (2 abnormal events)	900 of *155vb_fcs*	300 of *155vb_fcs* + 1,200 of *80vb_fcs* (1,500 Samples) + 1,200 of *eav_fcs* (1,500 Samples) + 2,400 of all abnormal events (2,700 Samples)
Indoor (Case 1)	*rlx_idr*	*80vb_idr* *eav_130vb_idr* *eav_80vb_idr* *eav_80vb_130vb_idr* *rlx_80vb_130vb_idr* total (5 abnormal events)	900 of *rlx_idr*	300 of *rlx_idr* + 1,200 of *80vb_idr* (1,500 Samples) + 1,200 of *eav_130vb_idr* (1,500 Samples) + 1,200 of *eav_80vb_idr* (1,500 Samples) + 1,200 of *eav_80vb_130vb_idr* (1,500 Samples) + 1,200 of *rlx_80vb_130vb_idr* (1,500 Samples) + 6,000 of all abnormal events (6,300 Samples)
Indoor (Case 2)	*155vb_idr*	*80vb_idr* *eav_130vb_idr* *eav_80vb_idr* *eav_80vb_130vb_idr* *rlx_80vb_130vb_idr* total (5 abnormal events)	900 of *155vb_idr*	300 of *155vb_idr* + 1,200 of *80vb_idr* (1,500 Samples) + 1,200 of *eav_130vb_idr* (1,500 Samples) + 1,200 of *eav_80vb_idr* (1,500 Samples) + 1,200 of *eav_80vb_130vb_idr* (1,500 Samples) + 1,200 of *rlx_80vb_130vb_idr* (1,500 Samples) + 6,000 of all abnormal events (6,300 Samples)

TABLE IV
TUNED HYPER-PARAMETERS OF OCSVM FOR BARE AND FOCS CABLES

Event type	Cable type	kernel	ν	γ
155vb vs *80vb*	Bare	rbf	0.001	1×10^{-5}
155vb vs *eav*	Bare	rbf	0.02	3×10^{-5}
155vb vs *total*	Bare	rbf	0.035	1×10^{-5}
155vb vs *80vb*	FOCS	rbf	0.2	8×10^{-5}
155vb vs *eav*	FOCS	rbf	0.001	1×10^{-4}
155vb vs *total*	FOCS	rbf	0.05	5×10^{-5}

TABLE V
TUNED HYPER-PARAMETERS OF OCSVM FOR INDOOR CABLE

Event type	kernel	ν	γ
155vb vs *80vb*	rbf	0.01	3×10^{-5}
rlx vs *80vb*	rbf	0.02	3×10^{-5}
155vb vs *eav_130vb*	rbf	0.01	1×10^{-5}
rlx vs *eav_130vb*	rbf	0.01	1×10^{-5}
155vb vs *eav_80vb*	rbf	0.02	3×10^{-5}
rlx vs *eav_80vb*	rbf	0.01	1×10^{-5}
155vb vs *eav_130vb_80vb*	rbf	0.01	1×10^{-5}
rlx vs *eav_130vb_80vb*	rbf	0.01	1×10^{-5}
155vb vs *rlx_130vb_80vb*	rbf	0.01	1×10^{-5}
rlx vs *rlx_130vb_80vb*	rbf	0.01	1×10^{-5}
155vb vs *total*	rbf	0.001	1×10^{-5}
rlx vs *total*	rbf	0.009	3×10^{-4}

various abnormal scenarios, including those involving multiple simultaneous vibrations and eavesdropping.

B. Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

The DBSCAN model is an unsupervised ML technique, chosen in this work for its robustness in detecting arbitrarily-shaped clusters and its effectiveness in isolating noise or outliers in unlabeled data. Since DBSCAN does not rely on a training process, it can be directly applied to a sequence of consecutive data points, making it particularly flexible and adaptable to various conditions. The DBSCAN algorithm operates by defining two key parameters: the radius of the neighborhood ϵ and the minimum number of points required to form a dense region $MinPts$. A sample is considered a core point if it has at least $MinPts$ neighbors within the radius ϵ. Clusters are formed by core points that are within ϵ of each other. Points that do not belong to any cluster and have fewer than $MinPts$ neighbors within ϵ are classified as noise or outliers (i.e., anomalies in our case). The choice of ϵ and $MinPts$ values significantly impacts the performance of DBSCAN. A small ϵ may result in classifying many data points as noise, while a large ϵ can lead to the formation of fewer clusters, with potential anomalies remaining undetected. Similarly, a small $MinPts$ value can cause the algorithm to detect too many small clusters, potentially labeling noise points as part of clusters, while a large $MinPts$ value may result in fewer clusters, with some anomalies being overlooked. Applying DBSCAN to detect anomalies in polarization signatures data, where abnormal patterns manifest as sparse or isolated points in the feature space requires careful tuning of these parameters.

1) Data pre-processing for DBSCAN: For data pre-processing and hyper-parameter tuning, we consider 1,200 data points for each cable type under normal operating conditions and 1,200 data points corresponding to each abnormal condition. The normal and the abnormal events are defined in the same way as stated in Table III. The dataset is then normalized through z-score standardization, ensuring that the feature values are consistent and properly scaled for effective application of the DBSCAN algorithm.

2) Tuning of DBSCAN hyper-parameters: To tune ϵ and $MinPts$, we adopted a controlled sampling strategy to simulate realistic yet varied conditions. We selected fixed-size windows of pre-processed data containing both normal and abnormal samples. The number of normal samples in each window (#N) ranged from 150 to 300, while the number of abnormal samples (#AN) was varied between 10 and 15 to

TABLE VI
TUNED HYPER-PARAMETERS OF DBSCAN FOR BARE AND FOCS CABLES AND THE SELECTED WINDOW SIZE OF NORMAL (#N) AND ABNORMAL (#AN) SAMPLES.

Event type	Cable type	ϵ	$MinPts$	# N	# AN
155vb vs *80vb*	Bare	19	53	220	11
155vb vs *eav*	Bare	20	78	220	11
155vb vs *total*	Bare	20	78	220	11
155vb vs *80vb*	FOCS	19	11	200	10
155vb vs *eav*	FOCS	15	80	200	10
155vb vs *total*	FOCS	19	11	200	10

TABLE VII
TUNED HYPER-PARAMETERS OF DBSCAN FOR INDOOR CABLE AND THE SELECTED WINDOW SIZE OF NORMAL (#N) AND ABNORMAL (#AN) SAMPLES.

Event type	ϵ	$MinPts$	# N	# AN
155vb vs *80vb*	24	50	150	10
rlx vs *80vb*	23	60	150	10
155vb vs *eav_130vb*	16	90	150	10
rlx vs *eav_130vb*	15	12	150	10
155vb vs *eav_80vb*	15	85	150	10
rlx vs *eav_80vb*	12	18	150	10
155vb vs *eav_130vb_80vb*	16	80	150	10
rlx vs *eav_130vb_80vb*	16	80	150	10
155vb vs *rlx_130vb_80vb*	21	20	150	10
rlx vs *rlx_130vb_80vb*	24	100	150	10
155vb vs *total*	16	90	150	10
rlx vs *total*	12	18	150	10

reflect realistic start of threat scenarios with low anomaly prevalence. For each combination of ϵ and $MinPts$, we randomly sampled such windows of consecutive samples and evaluated the detection performance across 20 independent iterations. To assess the effectiveness of a hyper-parameter combination (ϵ, $MinPts$) under varying data conditions, we introduced the metric *DBSCAN_perf*, defined in equation (3).

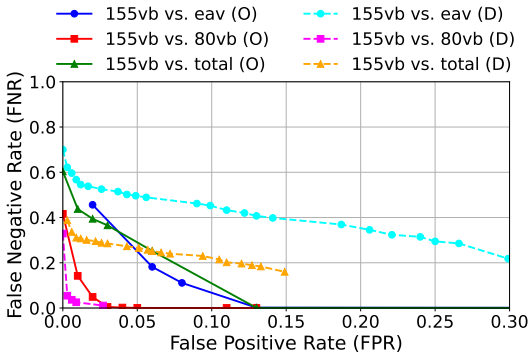
$$DBSCAN\_perf = avg(TPR - FPR + F1 + ARS + SS) \quad (3)$$

This metric aggregates five important evaluation criteria into a single scalar value, averaged over the sampling iterations. The rationale behind this formulation is to combine multiple complementary aspects of clustering performance. It combines TPR, F1-score, and FPR to reflect detection performance, while ARS and SS assess the quality of the resulting clusters. Together, *DBSCAN_perf* provides a balanced view of detection accuracy and cluster quality, guiding the selection of hyper-parameters that yield robust clustering performance across multiple randomized trials. After evaluating all possible hyper-parameter combinations, the results were sorted by their *DBSCAN_perf* value, and the hyper-parameter configuration that achieved the highest value was selected. The selected model was then subjected to 50 additional iterations over different sampled windows of normal and abnormal data for further validation, during which the final assessment metrics presented in the next section were calculated.

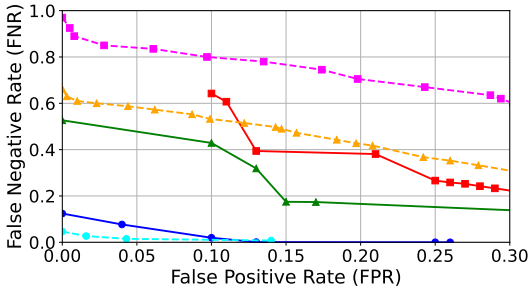
3) Results of hyper-parameter tuning for DBSCAN: Tables VI and VII summarize the tuned hyper-parameters used for the DBSCAN models across the three cable types for all considered events. For bare fiber (Table VI), due to the unshielded nature of the cable, moderate values of ϵ and $MinPts$ were selected to capture fine-grained distinctions between normal and abnormal behavior. In contrast, the FOCS cable (Table VI) required either more compact or more dispersed clusters depending on the event type, indicating a need to accommodate its more stable but insulated signal profile. The indoor cable (Table VII) presented the most diverse tuning requirements, with a wide spread in both ϵ and $MinPts$ values. This reflects the higher complexity of overlapping event scenarios. Interestingly, the eavesdropping scenario drove the selection of the total hyper-parameters for the bare cable, while 80vb drove the selection for the FOCS cable.

C. Hyper-parameter tuning overview

In this section, we summarize the results of the hyper-parameter tuning process by showing the trade-off between



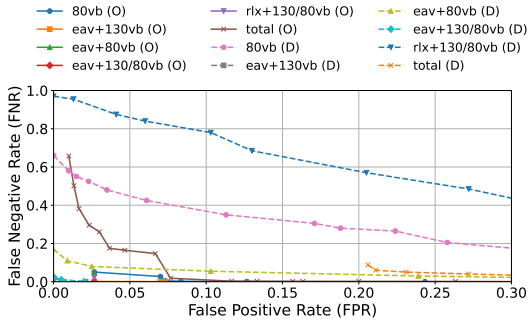
(a) Bare fiber



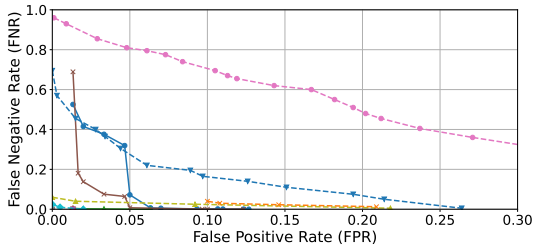
(b) FOCS cable

Fig. 2. Pareto frontier curves illustrating the trade-off between FNR and FPR during hyper-parameter tuning of OCSVM (O) and DBSCAN (D) for each scenario in (a) bare fiber and (b) FOCS cable.

FNR and FPR for all hyper-parameter settings tested. The trade-off is illustrated by selecting the hyper-parameter settings that show the best (i.e., the lowest) FPR for a given FNR (and vice-versa). Fig. 2 shows the Pareto frontier that indicates the trade-off between FPR and FNR for OCSVM and DBSCAN across three evaluation scenarios for bare and FOCS cables. For bare fiber (Fig. 2a), OCSVM consistently demonstrates more favorable detection performance, achieving lower FNR values at comparable or lower FPR across all hyper-parameter settings. OCSVM is particularly effective in the *155vb* vs. *80vb* case, nearly eliminating false negatives while maintaining minimal false positives. In contrast, DBSCAN exhibits higher FNR even at low FPR, especially in the *155vb* vs. *eav* and *155vb* vs. *total* scenarios. A similar trend is observed for



(a) *155vb_idr*



(b) *rlx_idr*

Fig. 3. Pareto frontier curves illustrating the FNR-FPR trade-off during hyper-parameter tuning of OCSVM (O) and DBSCAN (D) for the different indoor cable scenarios, considering (a) *155vb_idr* and (b) *rlx_idr* as the normal baseline.

the FOCS cable (Fig. 2b). OCSVM continues to outperform DBSCAN across all scenarios, maintaining lower FNR values for the same or lower FPR. In particular, for *155vb* vs. *eav*, it exhibits a near perfect separation with negligible false positives and minimal missed detections. Even in the *155vb* vs. *total* scenario, OCSVM exhibits strong generalization capability. In contrast, DBSCAN exhibits consistently higher FNR values across the same range of FPR levels. Notably, in the *155vb* vs. *80vb* and *155vb* vs. *total* scenarios, DBSCAN fails to reach the same low FNR levels as OCSVM, underscoring its limited adaptability when handling heterogeneous data from multiple abnormal events.

Fig. 3 presents the Pareto frontier curves obtained during hyper-parameter tuning of OCSVM and DBSCAN, where each curve corresponds to one evaluated indoor attack scenario. The plots highlight the parameter settings which achieve the most favorable balance between the FPR and FNR. There is a pronounced advantage of OCSVM over DBSCAN, particularly in handling diverse and overlapping abnormal conditions. In both baseline configurations, i.e., *155vb_idr* (Fig. 3a) and *rlx_idr* (Fig. 3b), OCSVM maintains low FNR values across all tested scenarios. The decision boundary learned from normal conditions generalizes well, allowing the model to reject a wide range of abnormal patterns without significantly increasing false alarms. In contrast, DBSCAN exhibits inconsistent behavior in the same scenarios.

V. Results

We first analyze the performance of the two ML models for each fiber type, followed by an assessment of the overall performance across all fiber types. The performance is measured in terms of the TPR, FNR, FPR, and TNR.

TABLE VIII
Results for Bare Fiber Scenarios (Normal vs Abnormal) using the OCSVM (O) and DBSCAN (D) Models (M) in terms of True Positive Rate (TPR), False Negative Rate (FNR), False Positive Rate (FPR), and True Negative Rate (TNR), in %.

Scenario	M	TPR	FNR	FPR	TNR
155vb vs *80vb*	O	99.92	0.08	3.33	96.67
155vb vs *80vb*	D	94.55	5.45	0.63	99.37
155vb vs *eav*	O	99.75	0.25	10.67	89.33
155vb vs *eav*	D	46.55	53.45	1.16	98.84
155vb vs *total*	O	97.50	2.50	5.00	95.00
155vb vs *total*	D	69.14	30.86	0.89	99.11

TABLE IX
Results for FOCS Cable Scenarios (Normal vs Abnormal) using the OCSVM (O) and DBSCAN (D) Models (M) in terms of True Positive Rate (TPR), False Negative Rate (FNR), False Positive Rate (FPR), and True Negative Rate (TNR), in %.

Scenario	M	TPR	FNR	FPR	TNR
155vb vs *80vb*	O	79.67	20.33	32.33	67.67
155vb vs *80vb*	D	80.4	19.6	67.36	32.64
155vb vs *eav*	O	99.83	0.17	2	98
155vb vs *eav*	D	92	8	0.47	99.53
155vb vs *total*	O	98.33	1.67	2.00	98.00
155vb vs *total*	D	73.00	27.00	33.40	66.60

A. Results for bare fiber

Table VIII depicts the performance of the OCSVM and DBSCAN models in distinguishing between three types of events for the bare fiber model. We examine the effectiveness in differentiating harmful vibration at 80 Hz (*80vb*), eavesdropping (*eav*), as well as the combined abnormal scenario (*total*) that includes both types of attacks from normal vibration at 155 Hz (*155vb*). The results show that OCSVM achieves below 1% FNR for individual events, but higher FPR of up to 10%. For the combined dataset, OCSVM achieves a high performance, with 97.5% TPR and 95% TNR. The DBSCAN model achieves good results for the *80vb* scenario, but has poor FNR performance for eavesdropping, which also affects the results for the combined dataset. Although DBSCAN achieved an FPR below 1%, demonstrating good ability in detecting the anomalies, its 30.86% FNR means that nearly one-third of actual anomalies were not detected, which reflects a high risk of undetected threats, and indicates the need for further improvements. In practical terms, OCSVM achieves superior performance in detecting harmful vibrations for bare fiber, making it a more reliable choice for environments where the primary concern is preventing physical damage to the fiber.

B. Results for FOCS cable

Table IX presents the performance of the OCSVM and DBSCAN models in distinguishing the three abnormal scenarios, i.e., *80vb*, *eav*, and the combined abnormal scenario (*total*), from the normal scenario (*155vb*) in the FOCS cable.

Based on the multi-layered protection property, we can expect that distinguishing between the signatures of *80vb_fcs* and *155vb_fcs* will be a more challenging task than in other cable types. This is confirmed in Table IX where the performance for *155vb* vs. *80vb* drops substantially for both models compared to bare fiber (Table VIII). Surprisingly, the eavesdropping

detection performance is better than the one observed for bare fiber. This indicates that the protective layers of FOCS cables, while detrimental to the detection of vibrations, may better reveal the effects of the eavesdropping procedures, facilitating its detection by ML models. When considering all anomalous scenarios (*total*), OCSVM shows a strong performance with 98% in both TPR and TNR. However, DBSCAN does not achieve a good performance, with high false negative (27%) and positive (33%) rates.

C. Results for indoor cable

The performance of OCSVM and DBSCAN for the indoor cable scenarios is shown in Tables X and XI. Different from the two previously considered fiber types where the normal scenario featured 155 Hz vibrations, for the indoor cable we consider two normal scenarios: the 155 Hz vibrations *155vb_idr*, and relaxed fiber *rlx_idr*. In both cases, all other signatures, i.e., *80vb_idr*, *eav_130vb_idr*, *eav_80vb_idr*, *eav_80vb_130vb_idr*, *rlx_80vb_130vb_idr*, and *total* (a comprehensive set of anomalies encompassing all the abnormal scenarios), are considered abnormal. We focus on the ability of the two models to distinguish *(i)* harmful vibrations at 80 Hz, *(ii)* overlapping frequency vibrations at 80 Hz, 130 Hz and *(iii)* eavesdropping combined with single or dual frequency vibrations at 80 Hz and 130 Hz, and *(iv) total* from the two normal cases.

1) Detection of harmful 80 Hz vibrations: When distinguishing the abnormal 80 Hz vibrations from the normal 155 Hz vibration, as depicted in the first two rows of Table X, the OCSVM model demonstrates excellent performance, correctly detecting 99.58% of the abnormal instances with a minimal FNR of 0.42%. However, the model obtains an FPR of 7.33%, which suggests that environments with frequent, benign disturbances might generate unnecessary alerts. In comparison, the DBSCAN model presents a high FNR (35.2%) and FPR (9.08%). Similar observations can be made when the relaxed fiber is considered as baseline, as shown in the first two rows of the Table XI. Overall, results show that OCSVM achieves good performance with more than 90% true positive and negative rates in all scenarios. DBSCAN, in contrast, shows a large performance gap. This performance gap in comparison to OCSVM indicates that, while DBSCAN is capable of detecting harmful vibrations, it may not be as effective in distinguishing between closely related vibration patterns in indoor cable.

2) Detection of eavesdropping overlapping with single and dual-frequency vibrations: The central rows of Tables X and XI (rows 3-8) assess the ability of the models to distinguish scenarios with overlapping events involving eavesdropping and single- or dual-frequency vibrations from two baseline normal conditions: *155vb_idr* and *rlx_idr*. Across these overlapping-event scenarios, both OCSVM and DBSCAN demonstrate high detection capabilities, with OCSVM generally offering stronger abnormal detection due to its training-based nature. OCSVM's performance remains consistently high regardless of the combination of harmful or non-harmful vibrations, with TPR higher than 97% and TNR higher than 92% in all scenarios. DBSCAN, except for one scenario, shows good performance with false rates below 10%. However, in the *80vb* scenario, its performance is substantially lower than that of OCSVM. In general, these findings are consistent with the previous one, showing that OCSVM has strong capabilities, while DBSCAN may need further enhancements to be suitable for real-world applications.

TABLE X
RESULTS FOR INDOOR CABLE SCENARIOS (NORMAL VS ABNORMAL) CONSIDERING *155vb* AS THE NORMAL CLASS USING THE OCSVM (O) AND DBSCAN (D) MODELS (M) IN TERMS OF TRUE POSITIVE RATE (TPR), FALSE NEGATIVE RATE (FNR), FALSE POSITIVE RATE (FPR), AND TRUE NEGATIVE RATE (TNR), IN %.

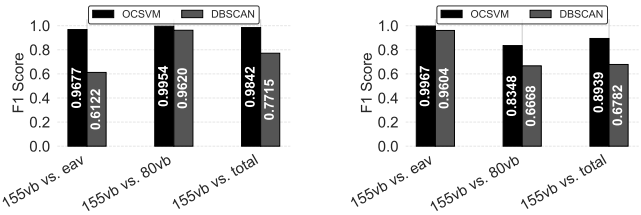
Scenario	M	TPR	FNR	FPR	TNR
155vb / 80vb	O	99.58	0.42	7.33	92.67
155vb / 80vb	D	64.80	35.20	9.08	90.92
155vb / eav_130vb	O	99.83	0.17	2.67	97.33
155vb / eav_130vb	D	97.20	2.80	0.04	99.96
155vb / eav_80vb	O	98.17	1.83	7.00	93.00
155vb / eav_80vb	D	91.80	8.20	0.49	99.51
155vb / eav_80vb_130vb	O	99.92	0.08	2.67	97.33
155vb / eav_80vb_130vb	D	96.40	3.60	0.05	99.95
155vb / rlx_80vb_130vb	O	98.17	1.83	7.00	93.00
155vb / rlx_80vb_130vb	D	91.00	9.00	49.96	50.04
155vb vs *total*	O	97.90	2.10	2.00	98.00
155vb vs *total*	D	96.92	3.08	41.18	58.82

TABLE XI
RESULTS FOR INDOOR CABLE SCENARIOS (NORMAL VS ABNORMAL) CONSIDERING *rlx* AS THE NORMAL CLASS USING THE OCSVM (O) AND DBSCAN (D) MODELS (M) IN TERMS OF TRUE POSITIVE RATE (TPR), FALSE NEGATIVE RATE (FNR), FALSE POSITIVE RATE (FPR), AND TRUE NEGATIVE RATE (TNR), IN %.

Scenario	M	TPR	FNR	FPR	TNR
rlx / 80vb	O	98.83	1.17	5.00	95.00
rlx / 80vb	D	81.60	18.40	40.89	59.11
rlx / eav_130vb	O	100.00	0.00	1.33	98.67
rlx / eav_130vb	D	99.20	0.80	0.00	100.00
rlx / eav_80vb	O	99.58	0.42	1.33	98.67
rlx / eav_80vb	D	97.20	2.80	0.03	99.97
rlx / eav_80vb_130vb	O	100.00	0.00	1.33	98.67
rlx / eav_80vb_130vb	D	98.40	1.60	0.00	100.00
rlx / rlx_80vb_130vb	O	100.00	0.00	1.33	98.67
rlx / rlx_80vb_130vb	D	76.20	23.80	6.91	93.09
rlx vs *total*	O	99.77	0.23	5.00	95.00
rlx vs *total*	D	98.00	2.00	20.02	79.98

3) Detection of dual-frequency 80 Hz and 130 Hz vibrations: When detecting dual-frequency vibrations in the indoor cable (rows 9-10 of Tables X and XI), the OCSVM model consistently shows robust performance. It maintains high sensitivity to anomalies while keeping false positives low across both evaluated baselines. In contrast, the performance of DBSCAN becomes less reliable under the same conditions. Specifically, it exhibits greater difficulty in separating complex overlapping anomalies from normal behavior, especially when the relaxed fiber scenario is used as the baseline. This is evident in the increased misclassification of normal samples and reduced anomaly sensitivity compared to OCSVM. These trends confirm that, while DBSCAN may handle certain overlapping patterns well, OCSVM is more effective in consistently detecting subtle dual-frequency vibration events in more challenging and realistic baseline conditions.

4) Detection of combined abnormal events: The last two rows in Tables X and XI present the performance of the



(a) Bare fiber (b) FOCS cable

Fig. 4. F1-scores for the two abnormal scenarios in bare fiber and FOCS cable.

OCSVM and DBSCAN models in detecting the *total* scenarios. Both models achieve high TPR, but OCSVM consistently offers superior performance, particularly in minimizing false positives and maximizing true negatives. This advantage is more evident when the relaxed fiber scenario is used as the baseline, highlighting the robustness of OCSVM to background variation. In contrast, while DBSCAN maintains strong sensitivity, its performance is limited by higher FPRs. These trends underscore the suitability of OCSVM for comprehensive anomaly detection in indoor fiber environments.

D. Overall assessment

We compare the anomaly detection performance of the considered models and scenarios in terms of F1-score values. In practical terms, a high F1-score means that the model not only accurately identifies anomalies (high precision) but also captures the majority of them (high recall).

Fig. 4 shows the F1-scores obtained by OCSVM and DBSCAN when detecting the three abnormal scenarios in bare and FOCS fibers. For bare fiber (Fig. 4a), OCSVM achieves F1-scores of 0.9677, 0.9954, and 0.9842 for detecting eavesdropping, harmful vibrations, and total anomalies, respectively. DBSCAN is comparatively effective in detecting harmful vibrations with an F1-score of 0.9620, but attains values of only 0.6122 and 0.7715 for eavesdropping and total anomalies, indicating weaker performance in these scenarios. OCSVM demonstrate a strong overall anomaly detection performance for the FOCS cable (Fig. 4b), achieving an excellent F1-score of 0.9967 for eavesdropping detection. It also performs well in the combined anomaly scenario with an F1-score of 0.8939, and maintains a solid score of 0.8348 when detecting harmful vibrations. DBSCAN, while exhibiting greater variability, achieves an F1-score of 0.9604 for eavesdropping detection, but its performance declines in the *total* and harmful vibration scenarios, with scores of 0.6782 and 0.6668, respectively. These results further highlight the stronger generalization capability of OCSVM. The diminished performance of DBSCAN, particularly for harmful vibrations, is likely influenced by the FOCS cable's multi-layered protective structure, which dampens the physical effects that would otherwise be reflected in polarization changes.

Results for the more complex indoor cable scenarios with overlapping events are presented in Fig. 5. These results reinforce the consistent high performance of the OCSVM model across all scenarios. Regardless of whether the normal baseline is set to the relaxed fiber (*rlx_idr*) or the 155Hz

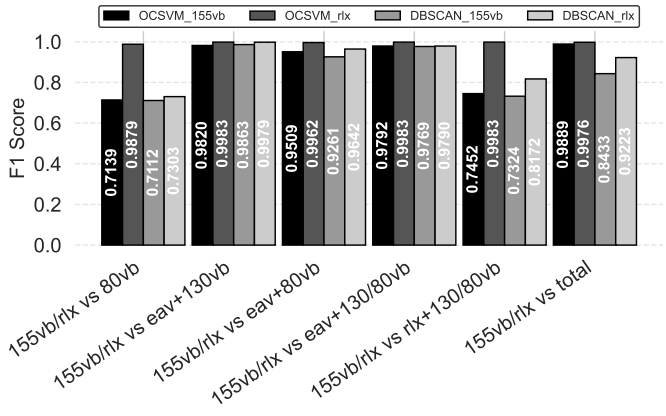


Fig. 5. F1-score comparison of OCSVM and DBSCAN performance for the abnormal scenarios in indoor cable considering *155vb_idr*/*rlx_idr* as normal scenarios.

vibration (*155vb_idr*), OCSVM maintains F1-scores above 0.97 in most scenarios, with peak values reaching 0.9983 in scenarios that involve combined eavesdropping and multi-frequency vibrations. Even in the most challenging *total* anomaly scenario, it achieves F1-scores of 0.9889 (*155vb*) and 0.9976 (*rlx*), demonstrating excellent generalization across diverse threat types. DBSCAN, in contrast, shows greater variability depending on the scenario and baseline condition. It achieves competitive performance in certain scenarios with clear separability, such as eavesdropping combined with dual-frequency vibration, where it attains F1-scores as high as 0.9979. However, its performance degrades for detecting harmful vibrations, where F1-score drops to 0.7112 (*155vb*) and 0.7303 (*rlx*). In the *total* anomaly scenario, DBSCAN achieves moderate to good results, with F1-score of 0.8433 for the *155vb* and 0.9223 for the *rlx* baseline.

VI. Conclusion

In this study, we presented a comprehensive analysis of ML-based anomaly detection in optical fiber networks through the collection and processing of SOP data. We evaluated the performance of SSL and USL techniques, specifically OCSVM and DBSCAN. Our goal was to detect various abnormal events, such as eavesdropping and harmful vibrations, by analyzing polarization signatures of three different cable types: bare fiber, FOCS, and indoor cable. Thirteen polarization signatures were collected under controlled experimental conditions, and careful hyper-parameter tuning was performed. Our findings indicate superior performance of OCSVM in detecting anomalies, with F1-score values exceeding 0.98 in most scenarios. Despite achieving high accuracy in some scenarios, DBSCAN exhibited greater variability in performance and poor performance in complex scenarios with overlapping events. While OCSVM consistently demonstrated high accuracy across most scenarios when trained on well-characterized normal data, our analysis highlights that DBSCAN retains significant value in deployment contexts where such baseline data is scarce or difficult to obtain. In such cases, DBSCAN's unsupervised nature enables it to detect clusters and anomalies

without requiring prior labeling, making it a practical alternative when semi-supervised or supervised learning is infeasible. The results suggest a strong potential for the SSL and USL models to aid human security engineers in the process of detecting events in optical networks, although their performance still shows a non-negligible amount of false positives and false negatives. By using the ML techniques investigated in this paper, human effort can be limited to the analysis of detected anomalies, rather than periodically analyzing the data. This can contribute to more cost-effective security solutions and more sustainable optical network operation. These findings underscore that the choice between SSL and USL techniques should be guided by the availability of training data and the specific operational constraints of the deployment scenario. Moreover, our results suggest that the performance of USL approaches like DBSCAN could be improved through additional post-processing steps, such as window-based temporal analysis of detection outputs. Exploring such enhancements to reduce the performance gap between USL and SSL models represents a promising direction for future research.

REFERENCES

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

[2] J. Pesic, E. Le Rouzic, N. Brochier, and L. Dupont, "Proactive restoration of optical links based on the classification of events," in *ONDM Conf.* IEEE, 2011, pp. 1–6.

[3] Urbint, "Telecom fiber cuts: Causes, consequences, and prevention," https://www.urbint.com/blog/telecom-fiber-cuts-consequences.

[4] A. Harris and P. Castle, "Bend loss measurements on high numerical aperture single-mode fibers as a function of wavelength and bend radius," *Journal of Lightwave Technology*, vol. 4, no. 1, pp. 34–40, 1986.

[5] M. Zafar Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," in *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, 2011, pp. 164–168.

[6] D. Dahan and U. Mahlab, "Security threats and protection procedures for optical networks," *IET Optoelectronics*, vol. 11, no. 5, pp. 186–200, 2017.

[7] W. Lee, S. I. Myong, J. C. Lee, and S. Lee, "Identification method of non-reflective faults based on index distribution of optical fibers," *Optics express*, vol. 22, no. 1, pp. 325–337, 2014.

[8] K. Abdelli, H. Grießer, C. Tropschug, and S. Pachnicke, "Optical fiber fault detection and localization in a noisy OTDR trace based on denoising convolutional autoencoder and bidirectional long short-term memory," *IEEE Journal of Lightwave Technology*, vol. 40, no. 8, pp. 2254–2264, 2021.

[9] K. Abdelli, J. Y. Cho, F. Azendorf, H. Griesser, C. Tropschug, and S. Pachnicke, "Machine-learning-based anomaly detection in optical fiber monitoring," *Journal of optical communications and networking*, vol. 14, no. 5, pp. 365–375, 2022.

[10] B. Steinar, "Locating disturbances in optical fibres," U.S. Patent WO2 022 185 075A1, Sep 9, 2022, international Patent Application.

[11] Y. Aono, E. Ip, and P. Ji, "More than communications: environment monitoring using existing optical fiber network infrastructure," in *OFC Conf.* Optica Publishing Group, 2020, pp. W3G–1.

[12] G. Marra, D. Fairweather, V. Kamalov, P. Gaynor, M. Cantono, S. Mulholland, B. Baptie, J. Castellanos, G. Vagenas, J.-O. Gaudron *et al.*, "Optical interferometry–based array of seafloor environmental sensors using a transoceanic submarine cable," *Science*, vol. 376, no. 6595, pp. 874–879, 2022.

[13] A. Mecozzi, C. Antonelli, M. Mazur, N. Fontaine, H. Chen, L. Dallachiesa, and R. Ryf, "Use of optical coherent detection for environmental sensing," *Journal of Lightwave Technology*, vol. 41, no. 11, pp. 3350–3357, 2023.

[14] M. Cantono, J. C. Castellanos, V. Kamalov, A. Mecozzi, R. Muller, S. Yin, and Z. Zhan, "Seismic sensing in submarine fiber cables," in *ECOC Conf.* IEEE, 2021, pp. 1–3.

[15] S. Pellegrini, L. Minelli, L. Andrenacci, D. Pilori, G. Bosco, B. Koch, R. Noé, C. Crognale, S. Piciaccia, and R. Gaudino, "Real-time demonstration of anomalous vibrations detection in a metro-like environment using a SOP-based algorithm," in *OFC Conf.*, 2024, pp. 1–3.

[16] D. Rafique, T. Szyrkowiec, H. Grießer, A. Autenrieth, and J.-P. Elbers, "Cognitive assurance architecture for optical network fault management," *Journal of Lightwave Technology*, vol. 36, no. 7, pp. 1443–1450, 2018.

[17] S. Karlsson, M. Andersson, R. Lin, L. Wosinska, and P. Monti, "Detection of abnormal activities on a SM or MM fiber," in *OFC Conf.* Optica Publishing Group, 2023, p. M3Z.6.

[18] L. Sadighi, S. Karlsson, C. Natalino, and M. Furdek, "Machine learning-based polarization signature analysis for detection and categorization of eavesdropping and harmful events," in *OFC Conf.*, 2024, pp. 1–3.

[19] L. Sadighi, S. Karlsson, L. Wosinska, and M. Furdek, "Machine learning analysis of polarization signatures for distinguishing harmful from non-harmful fiber events," in *ICTON Conf.*, 2024, pp. 1–5.

[20] L. Sadighi, S. Karlsson, C. Natalino, L. Wosinska, M. Ruffini, and M. Furdek, "Detection and classification of eavesdropping and mechanical vibrations in fiber optical networks by analyzing polarization signatures over a noisy environment," in *ECOC 2024; 50th European Conference on Optical Communication*, 2024, pp. 527–530.

[21] ——, "Deep learning for detection of harmful events in real-world, noisy optical fiber deployments," *Journal of Lightwave Technology*, pp. 1–9, 2025.

[22] K. Abdelli, M. Lonardi, J. Gripp, S. Olsson, F. Boitier, and P. Layec, "Breaking boundaries: harnessing unrelated image data for robust risky event classification with scarce state of polarization data," in *ECOC Conf.*, vol. 2023. IET, 2023, pp. 924–927.

[23] K. Abdelli, M. Lonardi, J. Gripp, D. Correa, S. Olsson, F. Boitier, and P. Layec, "Anomaly detection and localization in optical networks using vision transformer and SOP monitoring," in *OFC Conf.*, 2024, pp. 1–3.

[24] K. Abdelli, M. Lonardi, F. Boitier, D. Correa, J. Gripp, S. Olsson, and P. Layec, "Vision transformers for anomaly classification and localization in optical networks using sop spectrograms," *Journal of Lightwave Technology*, vol. 43, no. 4, pp. 1902–1913, 2025.

[25] Open Ireland Testbed, "Launch of Open Ireland: €2 million open networking testbed," https://connectcentre.ie/news/launch-of-open-ireland-e2-million-open-networking-testbed/.

[26] W. Qin, Q. Zhang, W. Hou, X. Zhang, and X. Gong, "Convolutional neural networks for fiber-bending eavesdropping attacks detection in coherent optical communication systems," in *2024 International Conference on Ubiquitous Communication (Ucom)*. IEEE, 2024, pp. 342–345.

[27] X. Chen, B. Li, R. Proietti, Z. Zhu, and S. J. B. Yoo, "Self-taught anomaly detection with hybrid unsupervised/supervised machine learning in optical networks," *Journal of Lightwave Technology*, vol. 37, no. 7, pp. 1742–1749, 2019.

[28] L. Minelli, S. Pellegrini, L. Andrenacci, D. Pilori, G. Bosco, L. D. Chiesa, A. Tanzi, C. Crognale, and R. Gaudino, "SOP-based DSP blind anomaly detection for sensing on deployed metropolitan fibers," in *ECOC Conf.*, vol. 2023, 2023, pp. 519–522.

[29] H. Song, R. Lin, L. Wosinska, P. Monti, Y. Li, and J. Zhang, "Eavesdropping detection and localization in WDM optical system," in *2023 IEEE Future Networks World Forum (FNWF)*, 2023, pp. 1–5.

[30] A. Tomasov, P. Dejdar, P. Munster, T. Horvath, P. Barcik, and F. Da Ros, "Enhancing fiber security using a simple state of polarization analyzer and machine learning," *Optics & Laser Technology*, vol. 167, p. 109668, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030399223005613

[31] P. Podder, T. Z. Khan, M. H. Khan, and M. M. Rahman, "Comparative performance analysis of hamming, hanning and blackman window," *International Journal of Computer Applications*, vol. 96, pp. 1–7, 2014.