Machine Learning-Based Polarization Signature Analysis for Detection and Categorization of Eavesdropping and Harmful Events

Machine Learning-Based Polarization Signature Analysis for Detection and Categorization of Eavesdropping and Harmful Events

Leyla Sadighi[1,*], Stefan Karlsson[2], Carlos Natalino[1], and Marija Furdek[1]

[1] *Department of Electrical Engineering, Chalmers University of Technology, 412 96 Gothenburg, Sweden.*
[2] *Swedish Defense Material Administration, 586 63 Linköping, Sweden.*

[*] *sadighi@chalmers.se*

Abstract: We propose a methodology that uses polarization state changes and machine learning to detect and classify eavesdropping, harmful, and non-harmful events in the optical fiber network. Our solution achieves 92.3% accuracy over 13 experimental scenarios.

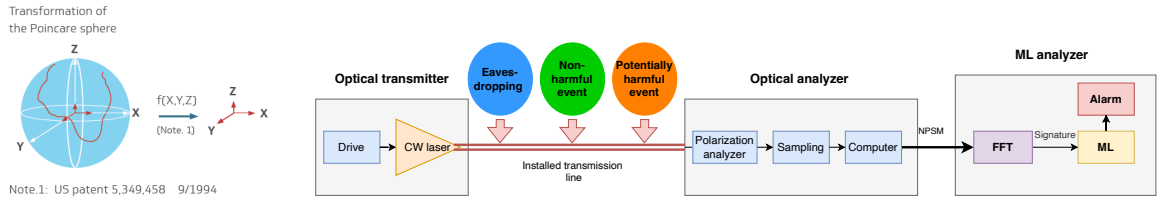
1. Introduction

Optical fiber infrastructures are critical for handling a broad range of sensitive data, from military intelligence to personal information, across diverse environments such as expansive duct-based installations, submarine routes, and localized indoor networks. Recent years have marked an increase in sabotage attempts on these systems, alongside the ever-present risk of unauthorized data interception, which is exacerbated by advances in quantum computing [1, 2]. Optical fibers are particularly vulnerable to eavesdropping attacks, wherein unauthorized light coupling techniques such as evanescent coupling, V-groove cut, and micro/macro bending [3, 4] can be used to intercept data. While monitoring optical power levels is one way to detect eavesdropping attacks, it may not be applicable against those attacks that cause minimal or undetectable power level drops [5]. A more sophisticated technique than optical power tracking involves monitoring of polarization state changes at the receiver to distinguish normal system variations from eavesdropping attempts. Early work [6] introduced a system using distributed fiber optical sensing (DFOS) that could detect signatures from touching or manipulating a fence with installed fiber optical cables. However, reliance on Rayleigh and Brillouin backscattering due to fiber impurities made this solution complex. Furthermore, the need for high-speed pulsing lasers to determine the position of a breach based on backscattering pulse delays, coupled with the requirement for diplexers to filter amplified spontaneous noise, contributes to its high costs. The work in [7] investigated polarization signatures of different fiber events as sequences of polarization changes over a specific time and frequency window, derived by processing the polarization state in the Poincaré sphere (refer to Fig. 1a). The signatures generated from eavesdropping and harmful events are visualized in a unique plot, referred to as a waterfall, allowing a human security operator to visually distinguish between legitimate and unauthorized activities. This is a simpler and more cost-effective approach to malicious activity detection than the method from [6]. Nevertheless, the visualization-based technique has limited applicability and scalability due to the need of a human specialist analyzing the waterfall plots.

To overcome the scalability and cost limitations of existing human-dependent solutions, we introduce a novel methodology using Machine Learning (ML) algorithms to analyze polarization signatures. This paper is the first to experimentally collect and analyze a dataset containing eavesdropping attacks and other potentially harmful and non-harmful events for three cable types. Our methodology automates the process of analyzing and categorizing eavesdropping and potentially harmful events from normal operating conditions and non-harmful events, allowing for potential large-scale optical network deployments. The presented methodology successfully segregates signatures with an accuracy of 92.3%.

2. Data Collection and Proposed Methodology

In the act of unauthorized data interception from fiber optic cables, eavesdroppers physically manipulate the cables. These malicious acts generate unique polarization signatures that can be identified using ML techniques. In this study, ML algorithms analyze the signatures derived from Polarization State Movements (PSM) data generated from experiments mimicking real-world conditions over fiber optic installations, including the risk of cable severance from nearby excavations and eavesdropping by manipulating exposed fibers. The proposed workflow is depicted in Fig. 1b. For data collection, a continuous wave distributed feedback (DFB) laser with a polarization-maintaining fiber generates optical power at a specific wavelength. The laser is regulated by a driver that maintains



(a) (b)

Fig. 1: (a) Changes in the Poincaré sphere (b) Proposed methodology for extracting signatures and ML analyzer

a consistent power level and temperature. Subsequently, the laser emits polarized light into an installed transmission line at a wavelength occupying one channel in the O, E, S, C, or L-band. All other types of optical transmission could occupy the remaining free spectrum. Each external event produces a unique effect on the PSM that can be recorded by the optical analyzer employing the Poincaré sphere analysis technique in the polarization analyzer block (Fig. 1b). The sampling block generates samples of each polarization state on the Poincaré sphere every 1 ms (fulfilling the Nyquist theorem) over a 20-minute recording period, resulting in 1.2 million samples over the entire recording time for each event. The numerical value of the distance between two consecutive polarization states, referred to as NPSM (Numerical PSM). We partition the NPSM data into 1200 time slots of 1000 elements each, and apply a Fast Fourier Transform (FFT) analysis with 512 frequency bins, utilizing a Hamming window [8].The resulting signature for each specific event is power spectrum data of 1200 rows (corresponding to time slots) and 512 columns (corresponding to frequency bins). ML methods then analyze the data to detect the specific signatures and generate an alarm if an eavesdropping attempts or a threat to the installed transmission is identified (Fig. 1b). Our ML analysis uses data from 13 experimental scenarios, summarized in Table 1, aiming to distinguish between normal operational signatures and those from eavesdropping or harmful events. In our test bed, we use 1310 nm signal over a 2 km transmission line that consists of a series of military fiber optical tactical cable systems (FOCS; *fc*), indoor cables (*id*), and bare single-mode G.675 bend-insensitive fiber (*bf*). The normal events include the relaxed (*rlx*) fiber without vibrations or eavesdropping, as well as vibrations at 155 Hz and 130 Hz (*n-v*) frequency (the two different values are used for diversity). The considered harmful events include fiber vibrations at 80 Hz (*an-v*), which corresponds to an excavator with an engine running at 4,800 rpm digging close to the cable installation, threatening to cut the cable. We also consider the case of dual vibrations (*dl-v*) at 80 and 130 Hz. The considered eavesdropping attacks are characterized by fiber bending (*b*) over a 10 mm diameter rod. We also consider the case without bending and with dual vibrations (*wb-dl-v*). The collected dataset was randomly

Table 1: The considered experimental scenarios

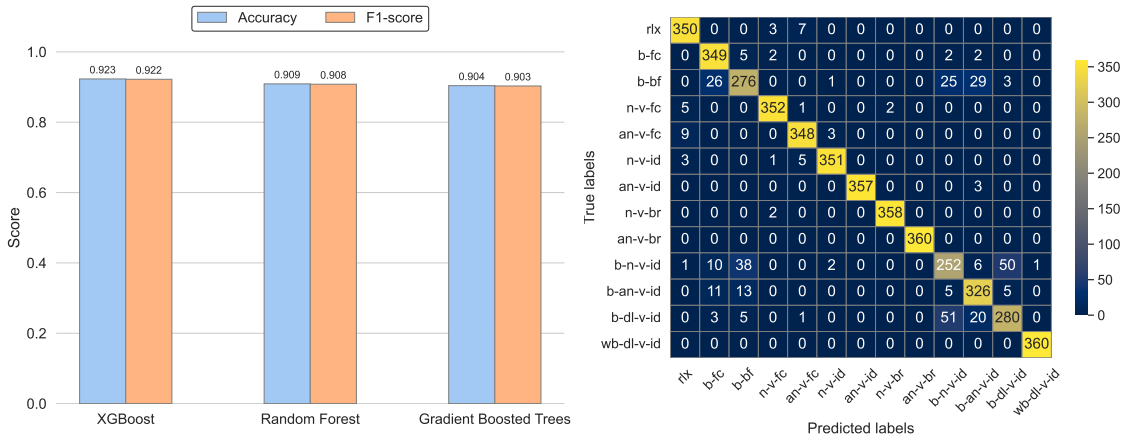
Abbr.	Scenario description	Justification
rlx	Relaxed fiber	Baseline; normal operating conditions
b-fc	FOCS cable bending	Eavesdropping
b-bf	Bare fiber bending	Eavesdropping
n-v-fc	FOCS cable + 155 Hz vibration	Normal operating conditions (non-harmful vibr.)
an-v-fc	FOCS cable + 80 Hz vibration	Harmful; possible cut predecessor
n-v-id	Indoor cable + 155 Hz vibration	Normal operating conditions (non-harmful vibr.)
an-v-id	Indoor cable + 80 Hz vibration	Harmful; possible cut predecessor
n-v-bf	Bare fiber + 155 Hz vibration	Normal operating conditions (non-harmful vibr.)
an-v-bf	Bare fiber + 80 Hz vibration	Harmful; possible cut predecessor
b-n-v-id	Indoor cable bending + 130 Hz vibration	Eavesdropping + non-harmful vibration
b-an-v-id	Indoor cable bending + 80 Hz vibration	Eavesdropping + harmful vibration
b-dl-v-id	Indoor cable bending + 80/130 Hz vib.	Eavesdropping + non-harmful and harmful vibrations
wb-dl-v-id	Indoor cable + 80/130 Hz vibrations	Non-harmful and harmful vibrations

divided into a 70% training (840 points) and a 30% testing subset (360 points), each with equal representation of the 13 scenarios. This led to a training dataset comprising 10,920 samples and a testing set of 4,680 samples. The labeled dataset with 13 distinct classes frames our analysis as a supervised ML problem (classification).

3. Results and Conclusion

We conducted experiments over a number of ML algorithms to select the most appropriate classifier for this 13-class classification problem. Our evaluation included the following classifiers from the Scikit-Learn library:

XGBoost, Random Forest, Gradient Boosted Trees, Bagging with Decision Trees, Decision Tree, Support Vector Machines (SVM), Linear Discriminant Analysis, k-Nearest Neighbors (k-NN), Multi-Layer Perceptron (MLP) Neural Network, and Logistic Regression. The classifiers were evaluated based on their accuracy and F1-score over the testing dataset. The final result is summarized in Fig. 2a. XGBoost performed the best, achieving an accuracy of 92.3% and an F1-score of 0.92, indicating a balanced performance in terms of false positives and false negatives. Random Forest and Gradient Boosted Trees closely follow the XGBoost performance.



(a) (b)

Fig. 2: (a) Accuracy and F1 score for the top 3 classifiers (b) Confusion matrix of XGBoost for the test dataset .

As illustrated in Fig. 2b, the confusion matrix validates the good performance of the XGBoost classifier. The classifier not only demonstrated proficiency in categorizing the relaxed one (*rlx*) and the scenarios without bending combined with dual frequency vibrations for indoor cables (*wb-dl-v-id*), but it also exhibited robust discrimination between harmful vibration events across the three cable types. This achievement is particularly significant in enhancing optical network security as the designed classifier effectively distinguishes between typical signal behaviors and those altered due to harmful events and eavesdropping. However, discerning among bending data for bare fiber (*b-bf*), bending and 155 Hz vibration for indoor cable (*b-n-v-id*), and bending and vibrations in two frequencies for indoor cable (*b-dl-v-id*) presented some challenges with evident misclassifications.

In conclusion, this study underscores the critical importance of bolstering security within optical networks, particularly given the escalating vulnerabilities to covert eavesdropping and harmful events. Through an analysis of PSM data signatures from optical devices, we successfully employed ML techniques, specifically the XGBoost classifier, to detect and categorize eavesdropping and harmful events with a high accuracy. To the best of our knowledge, this is the first study that applies ML techniques to detect and categorize harmful and non-harmful events in optical networks with this category of polarization state changes data.

Acknowledgment: This work was supported by Sweden's innovation agency VINNOVA (2020-03506) within the framework of the EUREKA cluster CELTIC-NEXT project AI-NET-PROTECT and the Swedish Research Council 2019-05008.

References

1. https://securethegrid.com/attacks-on-fiber-networks-in-california-baffle-fbi/
2. https://www.defensenews.com/naval/2022/07/14/italian-navy-telecom-provider-team-up-to-deter-attacks-on-undersea-cables/
3. A. Harris and P. Castle. *Bend loss measurements on high numerical aperture single-mode fibers as a function of wavelength and bend radius*, in *J. Lightw. Technol.*, vol. 4, no. 1, pp. 34–40, 1986. DOI: 10.1109/JLT.1986.1074626.
4. M. Z. Iqbal, *et al. Optical fiber tapping: Methods and precautions*, in *International Conference on High-Capacity Optical Networks and Emerging Technologies*, pp. 164–168, 2011. DOI: 10.1109/HONET.2011.6149809.
5. S. Karlsson, *et al. Eavesdropping G. 652 vs. G. 657 fibres: a performance comparison*, in *International Conference on Optical Network Design and Modeling (ONDM)*, 2022. DOI: 10.23919/ONDM54585.2022.9782849.
6. Y. Aono, *et al. More than communications: environment monitoring using existing optical fiber network infrastructure*, in *Optical Fiber Communication Conference (OFC)*, W3G.1, 2020. DOI: 10.1364/OFC.2020.W3G.1.
7. S. Karlsson, *et al. Detection of abnormal activities on a SM or MM fiber*, in *OFC 2023*, pp. M3Z.6, 2023. DOI: 10.1364/OFC.2023.M3Z.6.
8. P. Podder, *et al. Comparative performance analysis of hamming, hanning and blackman window*, in *International Journal of Computer Applications*, Vol. 96, No. 18, pp. 1–7, 2014. DOI: 10.5120/16891-6927.