A Decentralized Federated Learning-Based Approach for Fault Detection in Optical Networks

Citation for the original published paper (version of record):
Ribeiro, A., Lobato, F., Silva, M. et al (2025). A Decentralized Federated Learning-Based Approach for Fault Detection in Optical Networks. Proceedings of the 29th International Conference on Optical Network Design and Modelling Ondm 2025.
http://dx.doi.org/10.23919/ONDM65745.2025.11029366

A Decentralized Federated Learning-Based Approach for Fault Detection in Optical Networks

Andrei N. Ribeiro*, Fabrício R. Lobato*, Moisés F. Silva†, Carlos Natalino‡,
Lena Wosinska‡, Luca Valcarenghi§, Andrea Sgambelluri§, João C. W. A. Costa*

*Federal University of Pará, Belém, Brazil
andrei.ribeiro@itec.ufpa.br, {frl, jweyl}@ufpa.br
†Los Alamos National Laboratory, Los Alamos, USA
mfelipe@lanl.gov
‡Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden
{carlos.natalino, wosinska}@chalmers.se
§Scuola Superiore Sant'Anna, Pisa, Italy
{luca.valcarenghi, andrea.sgambelluri}@sssup.it

***Abstract*—Optical networks offer an ultra-high transmission capacity and serve various online applications (e.g., 5G, IoT, AR/VR, telemedicine). Preventing faults that cause packet losses or even link interruption becomes vital to ensure the reliability of these networks and, consequently, access to vital online services. Moreover, as the volume of telemetry data rapidly increases, data processing is often done in the cloud, which can open up breaches of unauthorized data access and raise concerns about scalability. Therefore, this work proposes a decentralized federated learning (FL)-based approach that exploits the principal component analysis (PCA) to perform confidentiality-preserving fault detection in optical networks. Unlike centralized FL-based approaches, the PCA is split into several local PCAs trained with subsets of the entire telemetry dataset. Thereafter, each local model exchanges its parameters in a peer-to-peer manner to learn the information extracted from their local data. As local PCAs are trained with only normal data (i.e., without faults), these models become sensitive to data that indicate anomalies, enabling the detection of faults. Moreover, a scrambling technique is applied to shuffle the order of the dataset, hiding the structural dependency among samples from malicious agents. Combining decentralized FL with the scrambling technique can enhance data confidentiality and cope with network scalability, as the processing of the dataset will be distributed over several nodes, hindering the access of malicious agents. Results on a testbed-derived dataset show no penalties for adopting the proposed disaggregated solution, i.e., the performance is the same as that of the centralized solutions.**

***Index Terms*—Decentralized federated learning, PCA, Fault detection, Optical networks**

I. Introduction

Providing accurate and rapid fault detection is vital to guarantee the high reliability of optical networks and uninterrupted accessibility to online services [1]. Although effective fault management reduces service disruptions, the confidentiality of the telemetry data is often not taken into account [2]. As the volume of telemetry data increases due to emerging data-hungry applications, the network operators frequently utilize the cloud's computational power to process the vast amount of the control data (e.g., QoT parameters). In that scenario, once shared with the cloud, it is difficult for the operator to guarantee the confidentiality of the control data. Hence, the ultimate goal is effectively detecting network faults while preserving the data confidentiality.

As the complexity of optical networks grows rapidly, conventional fault management methods are limited by simplified operational methods that hinder their scalability and effectiveness [3]. Hence, machine learning (ML) techniques emerge as techniques that overcome these methods by enabling automated and cognitive networks to cope with a large number of system parameters [4]. However, most ML-based approaches are based on supervised learning (SL) algorithms that require a large volume of fault data for proper training, which limits their feasibility [3].

Principal component analysis (PCA) is a widely known unsupervised algorithm commonly used for anomaly detection, making it suitable for optical fault detection. For instance, authors in [5] exploited a PCA-based semi-supervised approach to perform soft failure detection in optical networks and introduced data scrambling to ensure data confidentiality in a homomorphic computation scheme (i.e., computation is performed directly on the encrypted data). This is only possible due to the PCA rotation invariant property, which was leveraged by shuffling telemetry data to preserve the information contained in the data. Note that this property enables PCA to work with shuffled data without changing the results. Similarly, [6] shows different dimensionality reduction methods combined with a privacy-preserving approach. Only PCA and singular value decomposition (SVD) maintain the exact performance with and without data scrambling.

Although efficient, all the aforementioned works are based on third-party centralized PCA, which does not cope with data confidentiality as all data is shared in one location.

This work was supported in part by the National Council for Scientific and Technological Development (CNPq) and by the project CLEVER (Project ID 101097560), which is supported by the Key Digital Technologies Joint Undertaking and its members (including top-up funding by Italian Ministry of University and Research — MUR).

978-3-903176-67-6 © 2025 IFIP

Moreover, considering the rapid increase in the volume of telemetry data, data processing scalability becomes a challenge as more data needs to be processed, consuming resources and computational power. In that regard, in [7] we proposed a semi-supervised disaggregated PCA approach to detect faults in optical networks while preserving data confidentiality and coping with network scalability. Inspired by the federated learning (FL) scheme, this approach splits the data through several computation nodes to partially solve the global PCA problem. The global solution is then computed from these partial results without direct access to the original datasets at a single location. Moreover, to improve data confidentiality, each portion of data shared among the several computation nodes is randomly scrambled following the approach proposed in [5], and [6].

Although working in a centralized FL manner (i.e., with a global PCA) improves data confidentiality, it still relies on a central server. Hence, in this work, we leverage a distinct federated configuration denominated decentralized FL [8], which adopts a peer-to-peer (P2P) topology. Consequently, there is no central server, as each local PCA conducts local model training based on its local data and exchanges or fuses its model characteristics in a P2P manner. Following a semi-supervised approach, each local PCA is trained using only data from the network's normal operation conditions, disregarding data from fault conditions, which is scarce and difficult to collect in practical scenarios. This decentralized FL approach eases model aggregation and updates without relying on a central server, thereby mitigating the presence of untrusted servers. In addition, the proposed approach achieves the same fault detection performance as the centralized FL and traditional centralized approaches.

II. Related Work

In recent years, several ML algorithms to manage faults in optical networks have been developed, encompassing fault detection, identification, and localization. For instance, the authors in [9] proposed two different finite state ML algorithms to detect and identify the causes of several faults that degrade the bit error rate (BER) in optical connections. Leveraging similar fault scenarios, the same authors also investigated ML-aided algorithms for soft failure localization [10]. Moreover, [11] compared several ML algorithms regarding complexity and accuracy to detect and identify equipment faults in optical networks. They achieved approximately 98% accuracy in identifying the equipment faults using BER traces.

In addition to BER, several approaches use different optical parameters for the same task. The authors in [12] used a neural network-based algorithm fed with experimental data from optical power measurement under diverse fault modes to perform fault detection. Moreover, the authors in [13] proposed a soft failure localization technique based on a supervised neural network applied over telemetry data from Software-defined Networks (SDN) streams of network parameters. Similarly, [14] proposed a soft-failure identification and localization approach based on optical spectrum captured by optical spectrum analyzers (OSA). Although the aforementioned works performed well for failure management, the ML techniques employed follow a supervised manner, i.e., they require a large amount of data from fault conditions to be adequately trained. However, obtaining data from fault conditions in real-world optical networks is unfeasible since the design of optical links tends to be conservative and over-engineered. In this scenario, data representing fault conditions are rare in practical systems, while data under normal conditions are abundant.

Recent studies have focused on semi-supervised learning approaches to make it viable to apply ML in scenarios with scarce data representing fault conditions. Hence, these models can address the challenge of obtaining data reported under fault conditions in practical optical network deployments. The authors in [15] proposed a semi-supervised approach based on generative adversarial networks (GAN) trained with electrical spectrum data to perform soft-failure detection and identification. Although the GAN model was trained using only normal samples for failure detection, the proposed approach utilized supervised algorithms trained with failure samples to perform failure identification. Similarly, in [16], authors proposed a hybrid unsupervised/supervised fault detection framework that combines density-based clustering techniques and deep neural networks. Like the previous approaches, this one still needs samples from failure conditions for deep neural network training. Despite their ability to work with only data from normal conditions, the previous semi-supervised approaches neglect concerns related to data confidentiality. Conversely, the authors in [5], [6] proposed dimensionality reduction-based approaches that perform semi-supervised fault detection while preserving the data confidentiality using the scramble technique. Although properly coping with data confidentiality, these works rely on third-party centralized approaches, which are less effective regarding confidentiality and not concerned with network scalability since all data are concentrated in one location.

Considering that scenario, in our previous work [7], we proposed a disaggregated confidentiality-preserving scheme that enables fault detection through several local models by sub-sampling the entire dataset into multiple subsets. This approach ensures data confidentiality and handles network scalability by avoiding the concentration of the entire telemetry data in a single central model but leveraging several local models that share their local data information through a global model. However, this approach still depends on a central server (the global model), which may be vulnerable to malicious attacks.

III. Decentralized Federated Learning Approach

Typically, PCA is used for dimensionality reduction and can also be applied in anomaly detection tasks. PCA refers to a method that replaces a set of m original variables with a set of d latent variables [17], where $|m| > |d|$. The set d is called principal components (PCs) and is obtained by multiplying the original data matrix by the eigenvectors of its covariance

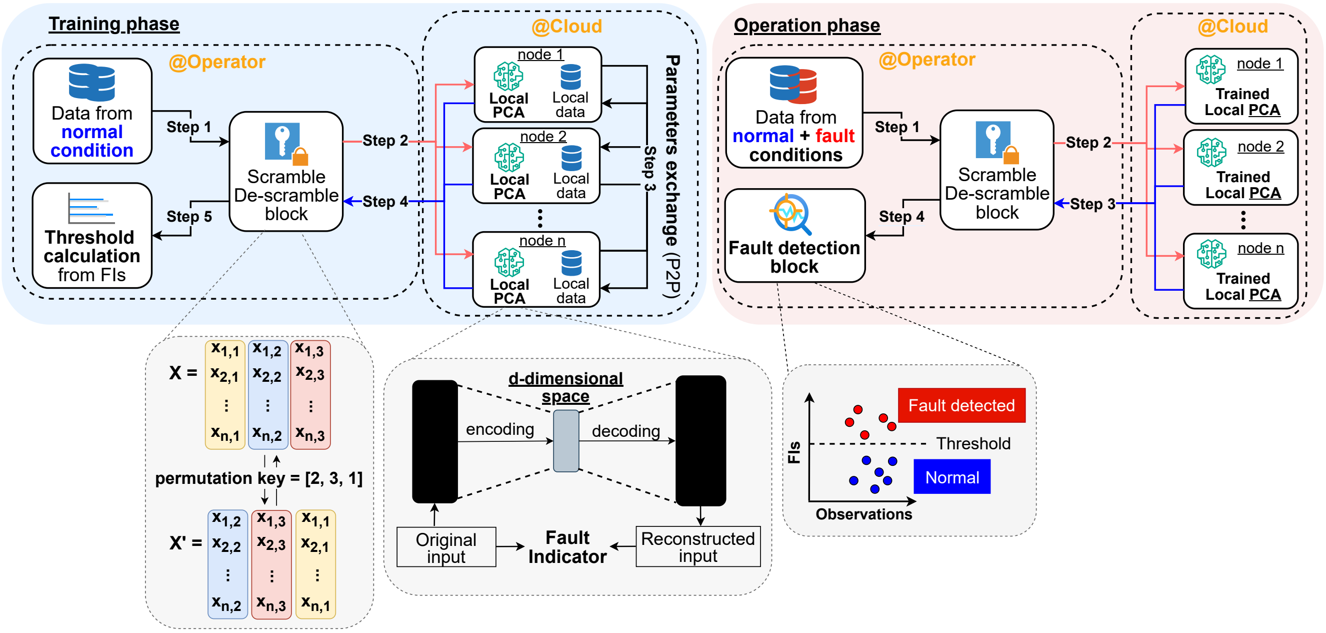


Fig. 1: Overview of the decentralized FL-based PCA approach for fault detection.

matrix. The dimensionality of d is defined by the number of eigenvectors used. Each PC retains a part of the variance of the original data. The quality of the d set approximation can be measured by the sum of the variances associated with the retained PCs. The eigenvectors of the covariance matrix of m can be computed using SVD. Applying SVD to m leads $m = UKV^\top$, from which the covariance matrix can be written as $m^\top m = VK^2V^\top$, where V are the eigenvectors and K^2 the eigenvalues associated with the eigenvectors. The original data matrix can be reconstructed by applying $\hat{m} = QV^\top + E$, where E is the error matrix. Training the PCA model using only normal data results in a reconstruction model where errors for data from faulty conditions increase, depending on the level of fault.

All the concepts mentioned above are based on a centralized approach. However, in this paper, leveraging our previous work [7], we propose a decentralized FL-based PCA approach for fault detection. The main difference between the centralized and the proposed here decentralized FL-based approaches lies in the model aggregation architecture. In the centralized approach, all the local PCAs share their model information through a global PCA. On the other hand, in the decentralized one, all the local PCAs exchange their model information directly with each other, following a P2P fashion.

The main idea within this distributed PCA-based approach is to calculate the principal components (PCs) over partitioned data. The entire dataset is firstly partitioned into several subsets (local data). Then, local PCs are calculated for each subset of data, and instead of communicating with a central server as made in [7], these local PCs are exchanged between all local PCAs. Then, each local PCA, now containing information about all the other ones, estimates a global covariance matrix. Correspondingly, this matrix is used to obtain the global PCs. In the end, all local data is projected into these global parameters. By splitting the entire dataset into several local nodes, unauthorized access to the data by a potentially malicious third-party actor may be prevented, as it does not have access to the entire dataset.

Additionally, as made in [7], we leverage the advantages of distributed learning and homomorphic encryption by integrating the decentralized FL-based PCA with the data scrambling technique proposed in [5]. This technique modifies the order of the features of the dataset, i.e., it changes the order of the optical parameters in the dataset, making it less intelligible in the event of a data breach attack (e.g., the man in the middle [18]), adding an extra layer of protection to this decentralized learning scheme. Since PCA is rotationally invariant, it does not depend on the actual order of the data. We can train the PCA model over the scrambled data in a homomorphic fashion without performance degradation or losing generality [5].

In that regard, the proposed decentralized FL-based PCA approach takes some procedures to perform fault detection, as shown in Fig. 1. This scheme comprises an operator and cloud components. The operator side is composed of homomorphic encryption and decision-making components. The cloud side comprises the ML components. The training and operation phases are described below:

Training phase:

Step 1: As the proposed approach works in a semi-supervised manner, only telemetry data from normal conditions are sent to the scramble/de-scramble block, where the data is scrambled and zero-centered following a permutation key.

Step 2: The scrambled data is split and distributed with the cloud-located local PCAs. Then, each local model calculates its respective PCs using its local data.

Step 3: Every local PCA exchanges its respective local PCs with the others. Then, the global PCs are calculated and saved by each local PCA. Using these global PCs, the reconstruction errors can be computed. These errors represent the difference between the original data and the reconstructed data and can be used as Fault Indicators (FIs). One can expect these FIs to present small values for data under normal conditions, as only data from such conditions were used for model training. The training of models is finished in this step, as every local PCA has been trained and got their global PCs.

Step 4: The training-derived FIs are sent to the scramble/de-scramble block, which reorders the dataset into its original form using the permutation key.

Step 5: Finally, a threshold is computed based on a specific percentile of the FIs, i.e., all the FIs are ordered, and the value from a particular percentile of position is chosen as the threshold.

Operation phase:

Step 1: Both data from normal and failure conditions are sent to the scramble/de-scramble block.

Step 2: The scrambled data is split and distributed with the trained cloud-located local PCAs. Each local model computes the FI for each sample from its respective local test data. No parameter information is exchanged in the testing phase, as all the local PCAs have been trained.

Step 3: The computed FIs are sent to the scramble/de-scramble block, which reorders the dataset into its original form using the permutation key.

Step 4: Finally, the operator receives the FIs in the original order, and the decision-making process is then carried out by comparing the FIs against the threshold. Samples with FIs lower than the threshold are classified as samples from normal condition samples. Otherwise, samples with FIs higher than the threshold are classified as fault-condition samples.

IV. Results

A. Experimental Setup and Data Acquisition

The telemetry dataset described in [19] is leveraged to evaluate the proposed approach. The considered testbed includes two Ericsson Special Purpose Outlet (SPO) 1400 devices, one Wavelength Selective Switch (WSS), and four EDFA amplifiers. At the end of the WSS, a 10 dB attenuator is installed to simulate attenuation or failures, as shown in Fig. 2. The dataset is collected during 10 hours. In the first 8 hours, two normal operation conditions were simulated: a stationary normal behavior during the first 6 hours, and a noisy normal behavior in the remaining 2 hours by randomly changing the attenuation at the range from 0 to 18 dB. In the remaining 2 hours, the same behavior as during the last 8 hours is simulated, but a 25dB attenuation is added every 40 seconds, putting the network in a failure condition for 10 seconds. After that, the WSS is reconfigured so that the network starts working correctly again.

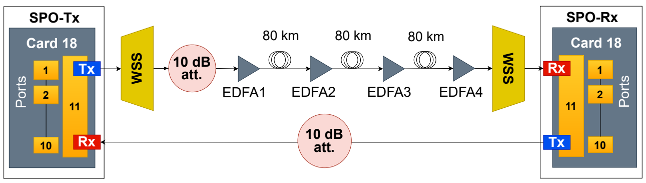


Fig. 2: Optical network testbed.

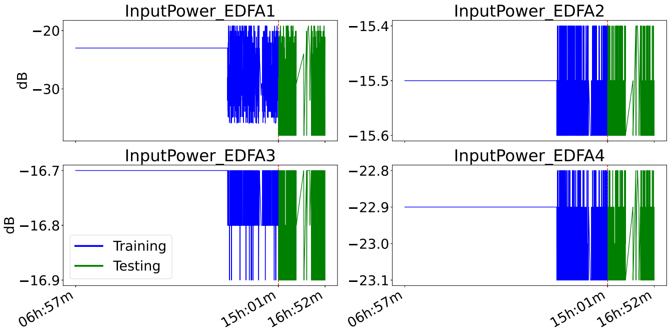


Fig. 3: Optical dataset split into training and testing sets. Approximately the first 8 hours of data are used for training, and the remaining 2 hours for testing.

The optical connection comprised three 80 km spans between the SPO-TX and SPO-RX. The data is collected every 3.5 seconds and consists of 4 features corresponding to the input power at each of the 4 EDFAs. An interpolation technique was employed due to missing values in the original data set generated at the end of 13,948 samples. Among the samples, the first 80% of data are used for training, and the following 20% are for testing. Notably, failure conditions were exclusively part of the test phase data. The decentralized FL-based scheme configuration is shown in Fig. 1, which in our study has four local PCA nodes, and each of them is trained with 25% of the training dataset (approximately 2,789 samples). Similarly, in the testing phase, 25% of the testing dataset is used for each node (approximately 697 samples). The linear threshold is defined as the value corresponding to the 99th percentile position computed from the training FIs. This value is chosen by looking for a good trade-off between

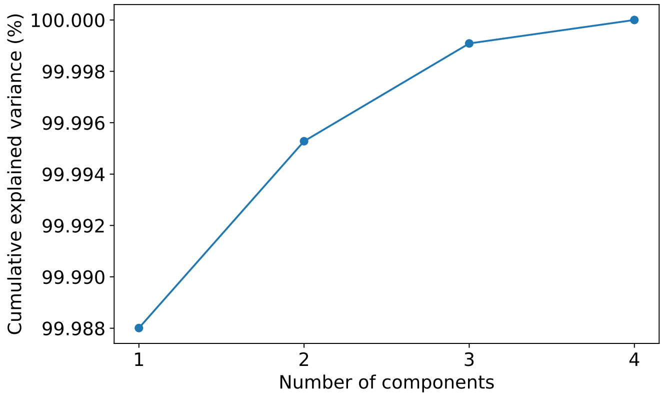
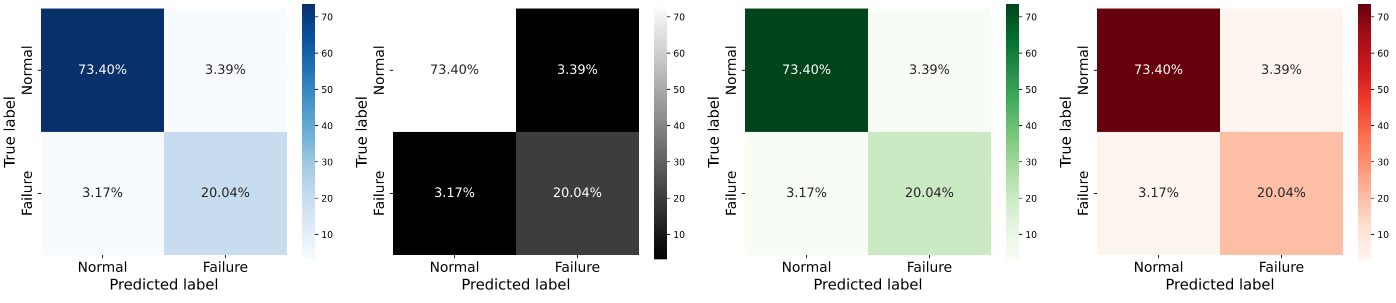


Fig. 4: Cumulative explained variance per number of components for PCA.



(a) Traditional PCA

(b) Traditional PCA + Scramble

(c) Cent. FL-based PCA + Scramble

(d) Dec. FL-based PCA + Scramble

Fig. 5: Confusion matrices of the compared scenarios. The diagonal elements represent the percentage of points for which the predicted label is equal to the true label, while off-diagonal elements are those that are mislabeled by the model, i.e., the Type I and Type II errors.

false-positive and false-negative errors in the operation phase. To promote clear visualization of the dataset, Fig. 3 presents the four used features, partitioned into training and testing sets.

As expected among the EDFA features, only the input power of EDFA1 presents variations in the testing set, as the 10 dB attenuator is placed at the link between WSS and EDFA1. Moreover, within the training set, two distinct distributions can be observed across all features. The first 6 hours are composed of data under stationary normal conditions, while the remaining 2 hours contain data under normal conditions with typical variations to simulate real-world traffic. These variations are included to improve model generalization, as they provide information about regular network traffic conditions, distinct from the initial stationary period.

Furthermore, the performance of PCA depends on the number of PCs chosen to reduce the dimensionality of the data. The ultimate goal is to find a number that can reduce the dimensionality while retaining the maximum variance. In that sense, different values of PCs were evaluated, as shown in Fig. 4.

Note that when PCA reduces the dimensionality of the data to one single dimension, more than 99.98% of the entire data variance is retained. Therefore, the PCA model compressed a 4-dimensional original space into a 1-dimensional space with minimum loss of information.

B. Fault Detection Results

In this subsection, fault detection performance results are presented. We compare our proposed approach with three different scenarios: Traditional PCA, Traditional PCA+Scramble, and Centralized FL-based PCA+Scramble. Typically, two evaluation metrics are used for anomaly detection approaches: Type I and Type II errors (also known as false positive and false negative errors, respectively). In that regard, there are important considerations. In our scenario, which focuses on optical network fault management, reducing Type II errors is more critical than reducing Type I errors, i.e., it is more important to correctly classify an actual fault than to misclassify a normal sample as from a fault condition, as the consequences of these two types of misclassification differ significantly. While Type I errors refer to false alarms leading to time and money waste, Type II errors refer to real failures in the network that are missed by the model and directly affect network QoT, leading to several SLA violations until the network operator manually notices it. In that regard, Fig. 5 condenses the failure detection results (Type I/II errors) for the four tested scenarios. Firstly, Fig. 5a refers to the most common application of PCA for anomaly detection. On the other hand, Fig. 5b presents the PCA combined with the data scrambling technique. As shown in the work [6], this approach does not change the result compared to the traditional PCA due to its rotation invariant property. Moreover, Fig. 5c shows the results of our previous work that leverages a centralized FL-based PCA approach with scrambling. One can note that, although the dataset is distributed following the configuration of four local nodes and one global node, the results do not change compared to the two previous traditional PCA approaches. Fig. 5d presents the results of the decentralized FL-based approach. One can note that even working in a fully distributed manner (i.e. no global node was used), this proposed approach achieved the same results as the other compared scenarios: 93.44% accuracy, 3.39% Type I error, and 3.17% Type II error. That fact is significantly desired, as we increased the data confidentially in terms of the absence of a central server, meanwhile providing the same failure detection accuracy.

Fig. 6 highlights the fault detection performance of the proposed approach. The black dots, representing the baseline condition (BC) training samples, are primarily located below

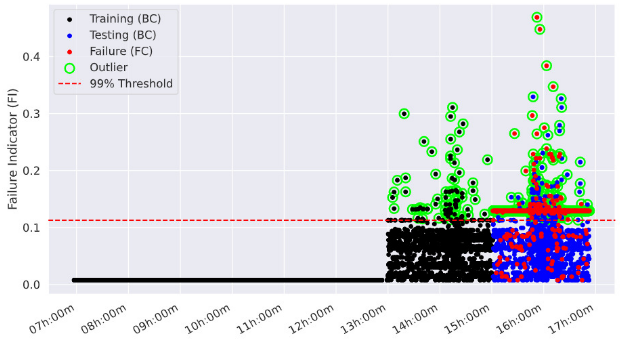


Fig. 6: Fault detection performance over time when in operation mode.

the threshold line, as this parameter was derived from those respective training samples. Note that some black dots are above the threshold line due to the 99th percentile position, which allows for up to 1% of Type I errors in the training phase. In the testing phase, most of the actual samples from fault conditions (FC) represented by red dots are presented above the threshold line, indicating the correct failure detection by the model. In addition, the aforementioned values of Type I and Type II errors in Fig. 5d can be noted as the few blue dots above the threshold line (Type I errors) and the few red dots below the threshold line (Type II errors), respectively.

V. Conclusion

This work employed a decentralized federated learning-based approach that leverages a principal component analysis model to detect faults in optical networks. Three scenarios were compared to the proposed approach, showing that although the approach operates in a decentralized manner to improve data confidentiality, it achieves the same fault detection performance as centralized approaches. Having a detection accuracy of 93.44%, the decentralized FL-based PCA approach exhibits satisfactory fault detection performance while improving data confidentiality and decreasing the risk of malicious attacks by functioning in a peer-to-peer architecture.

References

[1] X. Chen et al., “Flexible availability-aware differentiated protection in software-defined elastic optical networks,” J. Lightw. Technol., vol. 33, no. 18, pp. 3872–3882, Sep. 2015.

[2] M. Furdek, C. Natalino, A. D. Giglio, and M. Schiano, “Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats,” J. Opt. Commun. Netw., vol. 13, no. 2, pp. A144–A155, Feb. 2021.

[3] F. Musumeci, C. Rottondi, G. Corani, S. Shahkarami, F. Cugini, and M. Tornatore, “A tutorial on machine learning for failure management in optical networks,” J. Lightw. Technol., vol. 37, no. 16, pp. 4125–4139, Aug. 15, 2019.

[4] R. Gu, Z. Yang, and Y. Ji, “Machine learning for intelligent optical networks: A comprehensive survey,” J. Netw. Comput. Appl., vol. 157, May 2020, Art. no. 102576.

[5] M. F. Silva et al., “Confidentiality-preserving Machine Learning Scheme to Detect Soft-failures in Optical Communication Networks,” 2022 European Conference on Optical Communication (ECOC), Basel, Switzerland, 2022.

[6] M. F. Silva et al., “Confidentiality-preserving machine learning algorithms for soft-failure detection in optical communication networks,” J. Opt. Commun. Netw., vol. 15, no. 8, pp. C212-C222, August 2023, doi: 10.1364/JOCN.481690.

[7] R. Sales, A. Ribeiro, M. Silva, F. Lobato, A. Sbambelluri, L. Valcarenghi, and J. Costa, “Disaggregated confidentiality-preserving scheme for fault detection in optical networks,” in 2024 Optical Fiber Communications Conference and Exhibition (OFC), 2024, pp. 1–3.

[8] X. Zhou et al., “Decentralized P2P federated learning for privacy-preserving and resilient mobile robotic systems,” IEEE Wireless Commun., vol. 30, no. 2, pp. 82–89, Apr. 2023.

[9] A. Vela, B. Shariati, M. Ruiz, F. Cugini, A. Castro, H. Lu, R. Proietti, J. Comellas, P. Castoldi, S. J. B. Yoo, and L. Velasco, “Soft failure localization during commissioning testing and lightpath operation,” J. Opt. Commun. Netw., vol. 10, no. 1, pp. A27–A36, Jan. 2018.

[10] A. Vela, M. Ruiz, F. Fresi, N. Sambo, F. Cugini, G. Meloni, L. Poti, L. Velasco, and P. Castoldi, “BER degradation detection and failure identification in elastic optical networks,” J. Lightw. Technol., vol. 35, no. 21, pp. 4595–4604, Nov. 2017.

[11] S. Shahkarami, F. Musumeci, F. Cugini, and M. Tornatore, “Machine-learning-based soft-failure detection and identification in optical networks,” in Optical Fiber Communication Conf. (OFC), Mar. 2018, pp. 1–3.

[12] D. Rafique, T. Szyrkowiec, H. Grießer, A. Autenrieth, and J. Elbers, “Cognitive assurance architecture for optical network fault management,” J. Lightw. Technol., vol. 36, no. 7, pp. 1443–1450, Apr. 2018.

[13] K. Mayer, J. Soares, R. Pinto, C. Rothenberg, D. Arantes, and D. Mello, “Machine-learning-based soft-failure localization with partial software-defined networking telemetry,” J. Opt. Commun. Netw., vol. 13, no. 10, pp. E122–E131, 2021, doi: 10.1364/JOCN.424654.

[14] L. Velasco, B. Shariati, A. Vela, J. Comellas, and M. Ruiz, “Learning from the optical spectrum: soft-failure identification and localization,” in Optical Fiber Communication Conf. (OFC), Mar. 2018, p. W1G.1.

[15] H. Lun, M. Fu, Y. Zhang, H. Jiang, L. Yi, W. Hu, and Q. Zhuge, “A GAN based soft failure detection and identification framework for long-haul coherent optical communication systems,” J. Lightw. Technol., vol. 41, pp. 2312–2322, 2023.

[16] 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,” J. Lightw. Technol., vol. 37, no. 7, pp. 1742–1749, Apr. 2019

[17] Jolliffe, Ian T., and Jorge Cadima, “Principal component analysis: a review and recent developments,” Philosophical transactions of the royal society A: Mathematical, Physical and Engineering Sciences 374.2065 (2016): 20150202.

[18] A. S. Bhadouria, “Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World’s Biggest Data Breaches,” Int. J. Sci. Res. Publ (2022).

[19] InRete Lab, “Optical Failure Dataset,” Scuola Superiore Sant’Anna. 2021. [Online].
https://github.com/Network-And-Services/optical-failure-dataset