European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Confidentiality-preserving Machine Learning Scheme to Detect Soft-failures in Optical Communication Networks

Moisés Felipe Silva[(1)], Alessandro Pacini[(2)], Andrea Sgambelluri[(2)], Francesco Paolucci[(3)], Luca Valcarenghi[(2)]

[(1)] Los Alamos National Laboratory, Engineering Institute, USA, mfelipe@lanl.gov
[(2)] TeCIP Institute, Scuola Superiore Sant'Anna, Pisa, Italy
[(3)] CNIT, Pisa, Italy.

Abstract *We introduce a third-party confidentiality-preserving machine learning scheme for soft-failure detection leveraging the robustness of the principal components algorithm to the changes in the rotation of the data axis. We demonstrate that random scrambling of the data is effective to hide sensitive telemetry information.*

Introduction

With the increase of communication network complexity, intelligent monitoring systems play an important role in Network Management. In most approaches, machine learning (ML) algorithms are the first attempt to ensure high performance in evaluating the integrity of communication networks, which leads to the collection of an enormous volume of telemetry data, bringing concerns on the data security, privacy and confidentiality-preservation[1],[2],[3],[4].

In the context of optical communication, physical encryption have been seen as a means to ensure security of in-flight data in the transport layer[5]. Optical encryption, for instance, exploits the coherent nature of the laser beams. A common technique is based on the phase modulation of light beams using the direct superposition of phase masks containing the original data and an encrypting phase key[5]. Implemented as a service, optical encryption can be seen as a protocol agnostic solution which allows the configuration of several other protocols on the top of it running out-of-band without system overhead. Similarly, in the control and management plane, concerns may raise when data are elaborated by a third-party AI/ML algorithm provider. Indeed, optical network disaggregation may enable third-party telemetry-driven analytics services thanks to open YANG models[6]. In this specific case, network providers might not want to reveal their devices performance to preserve confidentiality.

For this purpose, based on the works described in[7],[8],[9], we propose a further step towards confidentiality-preserving failure detection models, implementing a steganography solution for applications of soft-failure detection in optical networks. Leveraging the linear properties of the widely-known principal component analysis technique (PCA)[10], we demonstrate how to transmit telemetry data from an optical system to untrusted third-party cloud computing resources for analysis, without revealing sensitive spatial geometry information contained in the data. This work will help reducing the security and confidentiality concerns that arise with the deployment of on-cloud processing solutions for network condition assessment and prognostics.

Background

Principal components analysis (PCA) is a classical multivariate statistical procedure that aims to estimate a linear static relationship between the data in its input space and a small unknown number of latent variables that retain most of the variance in the data[10]. Although PCA has been used for several different purposes, varying from feature extraction to manifold learning, here we apply the technique in a fashion for failure detection.

Assuming the training data matrix $\mathbf{X} \in \mathbb{R}^{n \times m}$ is composed of m telemetry parameters collected n times from several different network devices under normal working conditions, $\mathbf{X}$ can be decomposed into $\mathbf{X} = \mathbf{T}\mathbf{U}^T$, where $\mathbf{T}$ is called the scores matrix and $\mathbf{U}$ is a set of m orthogonal vectors, also called the loadings matrix (analogous to the eigenvectors). This method allows to perform an orthogonal transformation by retaining only the principal components d ($\leq m$), also known as the number of factors. Choosing only the first d eigenvectors, the final matrix can be rewritten without significant loss of information in the form of $\hat{\mathbf{X}} = \mathbf{T}_d\mathbf{U}_d^T + \mathbf{E}$, and therefore reconstructing the original input data matrix. In this case, $\mathbf{E}$ is the residual matrix resulting from the d factors.

Using only the principal components and adopting measurement collected under normal

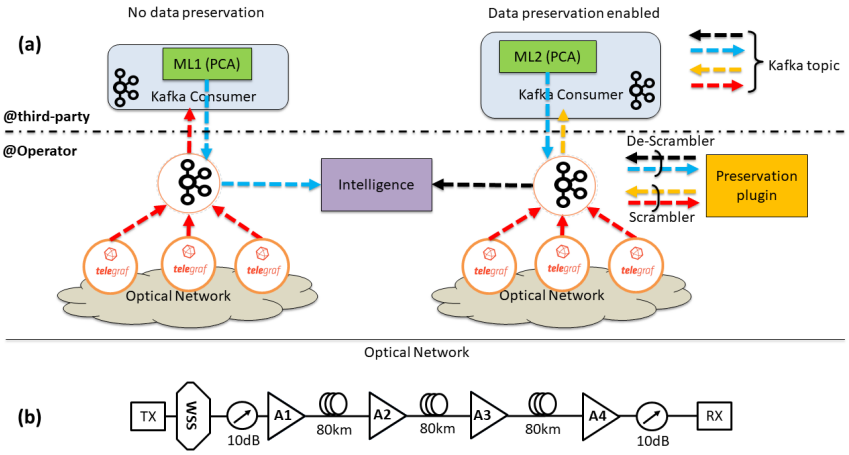

Fig. 1: (a) Reference scenario with and without data preservation; (b) Reference Optical Network Topology

or failure conditions, the analytic operations are performed using the main orthogonal vectors $\mathbf{U}_d$. Since the orthogonal vectors have been learned to map only telemetry data from normal working conditions, in the case of data under failure condition, the residual error will grow proportionally to the level of discrepancy between the failure condition and the normal state learned during training, allowing the direct detection of soft-failures.

Telemetry Data Confidentiality

Relying on a key property of PCA, we observed that the ordering of the measurement instances has no effect on the resulting calculation of the principle components and principle directions. This can be exploited to achieve confidentiality preservation, by reshuffling the telemetry data.

Finding the correct spatial ordering of a set of collected measurements is analogous to trying to correctly reassemble a common jigsaw puzzle. The work in[11] showed that this problem falls into the NP-complete class, and is therefore an unfeasible problem to be optimally solved computationally, with no efficient algorithm available up to this date. Thus, the scrambling order acts as a secret key that allows proper reconstruction of a dataset.

For a clear illustration, a simple scrambling operation over matrix $\mathbf{X}$ could involve the random swapping of its rows using a function $[\tilde{\mathbf{X}}_n, \mathrm{id}_n] = scramble\,(\mathbf{X}, n)$, where n indicates a random swapping of entire rows of the given matrix. A different but also effective operation could be the random swapping of columns using $[\tilde{\mathbf{X}}_m, \mathrm{id}_m] = scramble\,(\mathbf{X}, m)$, where m denotes the random swapping of entire columns. Apart from returning a scrambled version of the input dataset, this swapping function also keeps a vector id with the correct order of the data in the training matrix that works as an encryption key holded by the data owner or manager. Whenever necessary this unscrambling vector can be used to rearrange the matrix to its original form.

Applying the PCA technique over $\tilde{\mathbf{X}}_n$ or $\tilde{\mathbf{X}}_m$ results in the same manifold space but with different rotations. This further implies that a deployed monitoring system can send spatially-scrambled data to a third-party cloud service to perform failure detection via PCA without any concern for the spatial information associated with the structure being revealed. A similar result holds for shuffling the data using both approaches, whose difference still in the rotation of the learned manifold space.

Fig. 1 shows the reference scenario of application for the proposed solution. In particular, starting from the monitoring framework proposed in[12], two scenarios are considered: the case without data preservation (on the left) and the case with data preservation (on the right). In both cases the PCA algorithm runs in third-party location, different with the operator premises, where the telemetry data is collected. If no data preservation is applied, the telemetry data are sent transparently to the ML algorithm, subscribed to the monitoring topic. In the second case, the data preservation plugin is involved, applying the data scrambling and later the descrambling. In both cases, the intelligence block receives the failure detection information, being able to perform the proper operations in the network.

Evaluation and results

Fig. 2 shows the performance of the proposed approach in terms of data reconstruction and failure detection while Fig. 3 shows with the confusion matrix for both baseline and scrambled data. The dataset is a smaller version of the one introduced

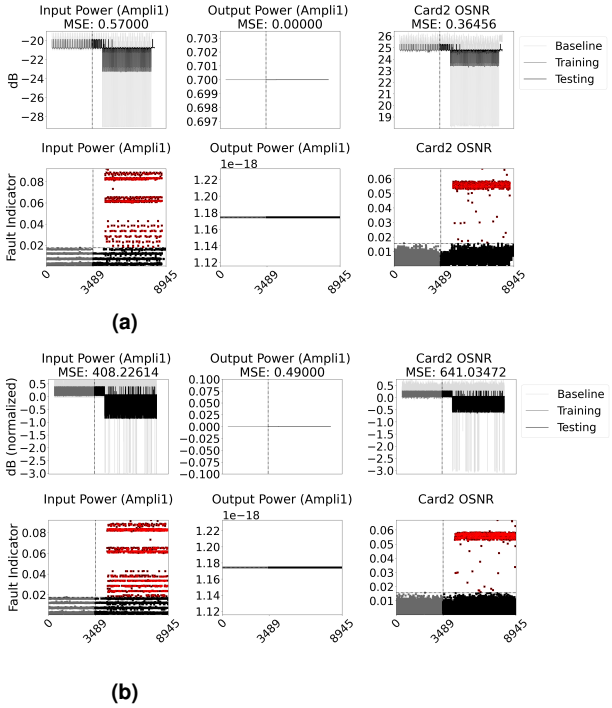

Fig. 2: Model reconstruction and failure detection for the baseline (a) and scrambled (b) data.

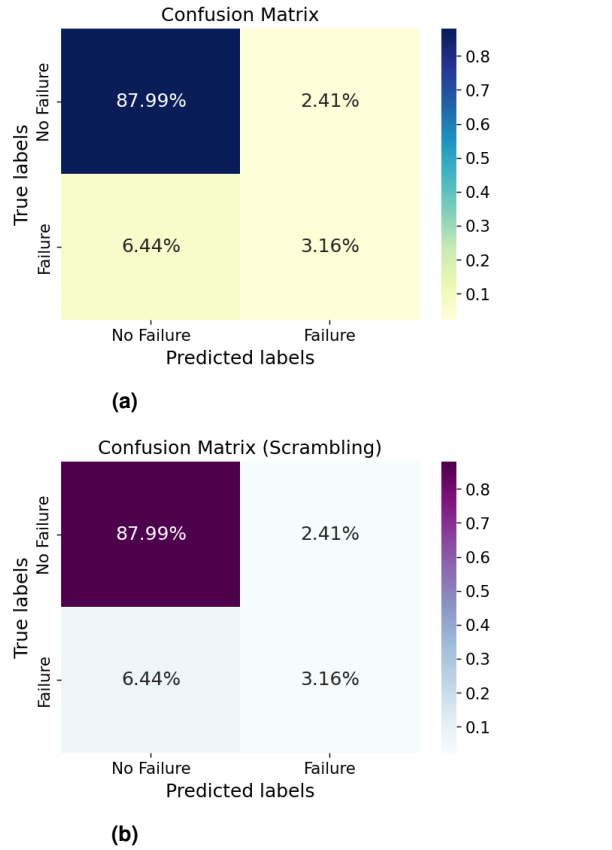

Fig. 3: Confusion matrix: baseline (a), scrambled (b) data.

in[7]. It has been collected from the multi-span link topology shown in Fig. 1b and includes the metrics related to the traversed devices (input and output power levels of the amplifiers and the coherent data at the RX). The ingress WSS is used to variate the power level entering in the transmission system. The dataset consists of two phases. In the training phase (portion of data before the vertical line in Fig. 2) the key parameters are observed in normal conditions, with no failures. The second phase (portion of data after the vertical line in Fig. 2) introduces soft failures, obtained by adding 10dB attenuation at the WSS, impacting the input power of Ampli1 (A1 in Fig. 1b). All the EDFA present a mute power of 0.4dBm, thus the input power variation is observed only at A1. By considering the training part in the top row of Fig. 2a, the model adequately reproduces the normal pattern of the system, which is corroborated by the small values of the mean squared error for the training data. In the test data, the model does not reach the same performance level in reconstruction for the part of data related to soft failures. At the bottom line of Fig. 2a the failure indicators are shown with red circles indicating the samples collected under failure conditions. In Fig. 2b, the same behavior for the reconstructed data and the failure indicators is applied together with the data confidentiality, where the samples are randomly scrambled and normalized.

Although the data is scrambled, the goal is to maintain the same failure detection accuracy as for the dataset without data confidentiality. To check the correspondence between a detected soft failure and the actual condition of the system the confusion matrix is presented in Fig. 3. Comparing the values at the main diagonal of the confusion matrix for both baseline and scrambled datasets (which is the global accuracy of the model) one can verify that the performance is exactly, with a solid 91.15% of accuracy in the predictions which confirms that our approach ensure the same level of performance as for the baseline data.

Conclusions

This work introduced an extended confidentaility-preserving unsupervised ML approach capable to detect soft failures in optical networks with high accuracy. The technique aims at performing simple scrambling operations in the collected data and extrapolate inner properties of a well-known ML technique to reach the same level of accuracy as in the using the original dataset without any scrambling. The proposed solution, when applied to large datasets, ensures data confidentiality for the data owner allowing the data usage by third-party cloud services.

Acknowledgements

Funding received from the ECSEL JU project BRAINE (grant agreement No 876967). The JU receives support from the EU Horizon 2020 research and innovation programme and the Italian Ministry of University, and Research (MUR).

References

[1] S. Belikovetsky, Y. A. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Digital audio signature for 3d printing integrity", *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1127–1141, 2019. DOI: 10.1109/TIFS.2018.2851584.

[2] G. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging", *Nature Machine Intelligence*, vol. 2, pp. 305–311, 2020.

[3] F. Zerka, S. Barakat, S. Walsh, *et al.*, "Systematic review of privacy-preserving distributed machine learning from federated databases in health care", *JCO Clinical Cancer Informatics*, no. 4, pp. 184–200, 2020. DOI: 10.1200/CCI.19.00047.

[4] A. Vizitiu, C. I. Nita, A. Puiu, C. Suciu, and L. M. Itu, "Towards privacy-preserving deep learning based medical imaging applications", *2019 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, pp. 1–6, 2019.

[5] "Optical encryption and decryption", in *Generalized Phase Contrast*. Dordrecht: Springer Netherlands, 2009, pp. 273–298, ISBN: 978-90-481-2839-6. DOI: 10.1007/978-90-481-2839-6_11.

[6] A. Sgambelluri, J.-L. Izquierdo-Zaragoza, A. Giorgetti, *et al.*, "Fully disaggregated ROADM white box with NETCONF/YANG control, telemetry, and machine learning-based monitoring", in *2018 Optical Fiber Communications Conference and Exposition (OFC)*, 2018.

[7] M. F. Silva, A. Pacini, A. Sgambelluri, and L. Valcarenghi, "Learning long-and short-term temporal patterns for ML-driven fault management in optical communication networks", *IEEE Transactions on Network and Service Management*, pp. 1–1, 2022. DOI: 10.1109/TNSM.2022.3146869.

[8] M. F. Silva, A. Pacini, A. Sgambelluri, L. Valcarenghi, and F. Paolucci, "Bringing disaggregated telemetry and ML to the transceiver for autonomic signal adaptation", in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, 2022, pp. 1–3.

[9] D. Mascarenas, A. Green, M. Silva, and B. Martinez, "Privacy-preserving structural dynamics", in *Data Science in Engineering, Volume 9*, R. Madarshahian and F. Hemez, Eds., Cham: Springer International Publishing, 2022, pp. 237–240, ISBN: 978-3-030-76004-5.

[10] I. Jolliffe, *Principal Component Analysis*. 2nd Edition. Springer, 2002.

[11] E. D. Demaine and M. L. Demaine, "Jigsaw puzzles, edge matching, and polyomino packing: Connections and complexity", *Graph. Comb.*, vol. 23, no. 1, pp. 195–208, Feb. 2007, ISSN: 0911-0119. DOI: 10.1007/s00373-007-0713-4.

[12] A. Sgambelluri, A. Pacini, F. Paolucci, P. Castoldi, and L. Valcarenghi, "Reliable and scalable kafka-based framework for optical network telemetry", *Journal of Optical Communications and Networking*, vol. 13, no. 10, E42–E52, 2021. DOI: 10.1364/JOCN.424639.