Detecting Anomalies in the Optical Layer Using Unsupervised Machine Learning

Sandra Aladin[1,2], **Lena Wosinska**[2] **and Christine Tremblay**[1]
[1]*École de technologie supérieure, 1100 Notre-Dame W., Montréal, H3C 1K3 Canada*
[2]*Chalmers University of Technology, Chalmersplatsen 4, 412 96 Göteborg, Sweden*
sandra.aladin.1@ens.etsmtl.ca

Abstract: We propose an unsupervised machine learning (ML) approach using field data for the detection of optical layer anomalies. We show how multivariate ML models can forecast hard failures by detecting soft failures. © 2024 The Author(s)

1. Introduction

The rapid development of emerging technologies and online services, such as real-time video and cloud services, leads to the drastically increasing capacity demand and infrastructure complexity as well as a need for high network flexibility. In such a context, any network failure can lead to massive loss of data and customers churn due to non-compliance with the service level agreements. It is thus particularly important to ensure high quality of service (QoS) for all applications requiring high bandwidth and/or ultra-low latency and jitter.

Machine learning (ML) has been proposed to enable proactive fault management in optical networks. Network faults can be categorized into hard failures linked to immediate service disruptions, and soft failures which are linked to gradual quality of transmission (QoT) degradations in optical networks. The main objective of an effective ML-based fault management system is to detect, identify and localize soft failures in order to prevent them from deteriorating to hard failures. In [1], the authors proposed a hybrid unsupervised and supervised ML approach for anomaly detection in optical networks. Their framework analyzes patterns of experimental optical performance monitoring (OPM) data using an unsupervised data clustering module. Then, the learned patterns are fed to a supervised data regression and classification module for online anomaly detection. The authors in [2, 3], similarly to aforementioned authors, used experimental imbalanced data with a semi-supervised approach to detect failures in optical networks, and synthetically generated data with encoder-decoder long short-term memory (ED-LSTM) to model and predict the evolution of soft failures for several days with the aim to trigger proactive maintenance and component replacement actions before hard failures occur. In [4, 5], the authors used optical performance monitoring data gathered from production networks. The first study showed that it was possible to use ML techniques to predict the loss of signal with good precision 1 to 7 days before they occur. Similarly, the second study presents an ML-based model to detect performance degradations in optical networks. In both studies, the authors used a supervised learning approach to detect QoT degradations in the OPM data, which required a labeling phase to perform loss of signal forecast and anomaly detection tasks.

In this study, we propose the use of three unsupervised learning techniques to detect anomalies from the OPM data. Then we use the labeling principles based on the alarm parameters in the dataset as in [4], to visualize and compare the results of the ML-based anomaly detection models.

2. Methodology

2.1 Anomalies in OPM data

Fig.1 shows the OPM metrics for one lightpath with the anomalies defined from alarms over 4 years. In the context of this study, anomalies represent instances of OPM parameters that do not conform to the majority of values recorded over a collection period. Point anomalies are single data points that are significantly different from the rest of the data. Contextual anomalies are instances that deviate from the other data points in a particular context, while being

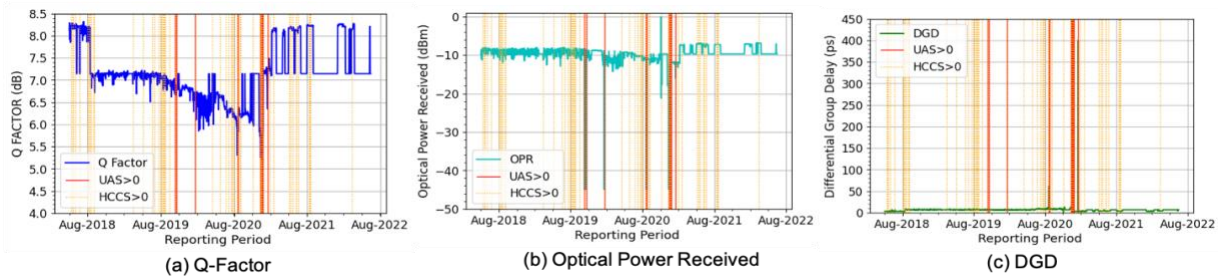

Fig. 1. Anomalies observed in the OPM metrics for one lightpath during 4 years. UAS: unavailable seconds; HCCS: high correction count seconds; OPR: optical power received; DGD: differential group delay

considered normal in a different context. A group of data points which, taken individually may be considered normal, but deviate considerably from the rest of the data points when gathered together, represent the collective anomalies [6]. A point-anomaly detection approach was adopted for the algorithms implementation as opposed to a collective or a contextual anomaly detection approach.

2.2 Dataset Description and Preprocessing

For this study, we used a dataset of daily binned PMs collected from equipment in the production network of a North American Service Provider over 4 years. The PM metrics are pulled from specific ports of these devices linked to specific facilities. We gathered instances for the optical transport module services among others (Ethernet, OC-n, …), encapsulated by the optical transport network. Amongst these parameters, the Q-Factor for the signal quality, the optical power received (OPR) and the differential group delay (DGD) were the ones used to build our anomaly detection models. Moreover, the high correction count seconds (HCCS) and the unavailable seconds (UAS) alarm parameters were used to identify ground truth anomalies in the OPM time series [4,7,8]. While the equipment's unavailability duration in seconds is reported as UAS, the duration in seconds where the number of errors to be corrected by forward error correction exceeds some threshold is referred to as HCCS. We structured the data as multivariate time series, using the collection date of each record. Missing data was replaced using a moving average using a 7-day sliding window. Then we normalized the data using the preprocessing module in scikit learn [9]. A correlation analysis using the *stats* module from the *scipy* library revealed that the correlation between the OPR and DGD parameters with the Q-Factor is statistically significant. The Pearson coefficients calculated for the OPR and DGD parameters with regards to the Q-Factor were 0.48 and -0.18, respectively.

2.3 Unsupervised learning-based anomaly detection

We implemented three anomaly detection models utilizing the density-based spatial clustering of applications with noise (DBSCAN), one-class support vector machine (OCSVM) and isolation forest (IF) techniques. Three performance metrics commonly used with clustering techniques have been used to compare the three models. The silhouette score (SS) allows to validate consistency within clusters of data. It ranges from -1 to +1, with higher values indicating a well-matched instance to its own cluster. The Calinski-Harabasz index (CH), also known as the variance ratio criterion, is the ratio of the sum of the dispersion between-clusters and within-cluster for all clusters (where dispersion is defined as the sum of distances squared). Higher CH index means well-separated clusters. The Davies-Bouldin index (DB) measures the average similarity between clusters. The lower the index value the better the separation between clusters [9].

The DBSCAN algorithm is an unsupervised learning technique that can find arbitrary shaped clusters and clusters with noise. It uses the number of samples in a neighborhood for a point to be considered as a core point (*min_samples*) and the maximum distance between two samples for one to be considered as in the neighborhood of the other (*eps*). The unsupervised learning algorithm OCSVM is a variation of the regular SVM. It can learn the boundary for normal data points where instances outside the boundary are considered to be anomalies. The isolation forest technique uses a repeated recursive process to randomly select a feature from the dataset and create partitions of the data based on a split value, until anomalies are isolated. The OCSVM and the IF models use the parameters "*nu*" and *contamination*, respectively. These parameters correspond to the proportion of outliers in the data set.

3. Results and comparative analysis

We used the Silhouette score to find the optimal *min_samples* and *eps* parameters for the DBSCAN model within value ranges [5-80] and [0.05-0.9] respectively. And the proportion of outliers was set to 4% for the OCSVM and IF

Table 1. Performance scores for the anomaly detection models

	DBSCAN	OCSVM	IF
Precision	**0.54**	0.26	0.32
Recall	0.18	0.23	**0.28**
F1-score	0.27	0.24	**0.30**
SS	**0.82**	0.69	0.68
CH	**363.65**	78.61	201.82
DB	**1.10**	2.71	1.49

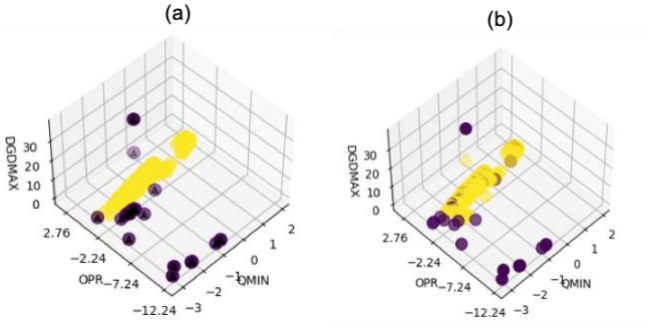

Fig. 2. (a) Detected anomalies by DBSCAN; (b) Labeled anomalies

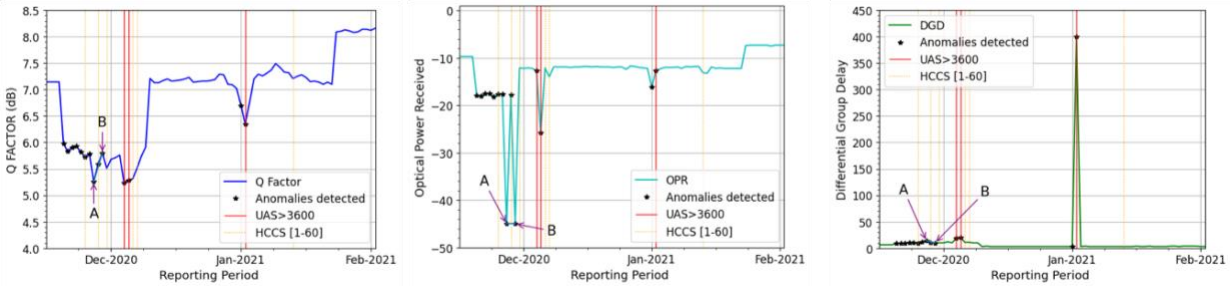

Fig. 3. Anomalies detected on the 3 PM metrics (Q-Factor, OPR and DGD) by DBSCAN

algorithms as per the ratio obtained by dividing the number of instances with HCCS > 0 or UAS > 0 by the total number of instances in the data set. Table 1 shows how well the DBSCAN model outperformed the OCSVM and IF models, based on the *Precision* score as well as the unsupervised learning performance metrics as in [10,11]. The low *Recall* score might be explained by the fact that the dataset is highly imbalanced in terms of anomalies compared to normal instances. Moreover, the training time for IF, OCSVM and DBSCAN on a 12.7 GB RAM Virtual Machine with Nvidia's T4 GPUs was 0.37 s, 0.02 s and 0.05 s, respectively, with OCSVM slightly faster than DBSCAN.

Fig. 2 a) shows the clusters created by the DBSCAN algorithm. The yellow cluster represents normal instances while the dark purple points with triangles are the anomalies detected by the model. Fig. 2 b) displays a 3D scatter of the normal data in yellow with the labeled anomalies in dark purple.

Fig. 3 presents a 60-day period where the system was unavailable for more than 1 hour (December 19th, 20th 2020 and January 16th 2021), with the detected anomalies displayed for the different features used. The orange vertical lines represent the HCCS within [1, 60] s (transient loss of signal (LOS)) and the red vertical lines are days when UAS > 3600 s (imminent loss of signal (ILOS)) as in [4]. We can see that the DBSCAN model detected 14 anomaly points including the 3 ILOS events for the period, but did not detect 4 LOS events (Dec 15th, 21st, 22nd 2020 and January 27th 2021). These undetected cases may be related to alarms raised for events not linked to the PM metrics considered in this study. On the other hand, 9 days during which anomalies were detected by the DBSCAN model don't have any alarms recorded. On December 12th, 14th 2020 for example, there were two occurrences of Q-Factor degradation, with very low (-45 dBm) OPR values (indicated by A and B), while the DGD remained stable for both days. This shows that the model can find combinations of PMs abnormal, while PMs might not all be anomalies when taken one by one.

4. Conclusion

We propose an unsupervised ML approach for anomaly detection. Our study demonstrates the benefits of unsupervised learning's ability to process unlabeled data and create clusters, thus allowing anomaly detection in multivariate time series without time consuming hand-labeling task on the data. In future work, we will develop a strategy allowing to capture gradual degradations in lightpath QoT considering multiple parameters simultaneously.

Acknowledgements: This work was supported by the National Sciences and Engineering Research Council of Canada (RGPIN 2019-03972), the ÉTS Program for the Development of International Research Collaborations and the EUREKA cluster CELTIC-NEXT project AI-NET PROTECT funded by the Swedish Innovation Agency.

5. References

[1] X. Chen et al., "Self-Taught Anomaly Detection with Hybrid Unsupervised/Supervised Machine Learning in Optical Networks," in Journal of Lightwave Technology, vol. 37, no. 7, pp. 1742-1749, 1 April1, 2019, doi: 10.1109/JLT.2019.2902487.
[2] S. Liu et al., "Semi-supervised Anomaly Detection with Imbalanced Data for Failure Detection in Optical Networks," 2021 Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA, USA, 2021, pp. 1-3.
[3] S. Behera et al., "Machine learning framework for timely soft-failure detection and localization in elastic optical networks," in Journal of Optical Communications and Networking, vol. 15, no. 10, pp. E74-E85, October 2023, doi: 10.1364/JOCN.490008
[4] W. Du et al., "Forecasting loss of signal in optical networks with machine learning," in Journal of Optical Communications and Networking, vol. 13, no. 10, pp. E109-E121, October 2021, doi: 10.1364/JOCN.423667.
[5] S. Allogba et al., "Extraction and Early Detection of Anomalies in Lightpath SNR Using Machine Learning Models," in Journal of Lightwave Technology, vol. 40, no. 7, pp. 1864-1872, 1 April1, 2022, doi: 10.1109/JLT.2021.3134098.
[6] M. Nesryne, et al. "Unsupervised Anomaly Detection in Time-series: An Extensive Evaluation and Analysis of State-of-the-art Methods." arXiv preprint arXiv:2212.03637 (2022).
[7] C. Tremblay et al., "Detection and Root Cause Analysis of Performance Degradation in Optical Networks Using Machine Learning," 2023 European Conference on Optical Communication (ECOC), Glasgow, Scotland, 2023, M.B.7.2.
[8] Y. Pei, et al., "Identifying root causes of network service degradation," U.S. Patent 11,477,070, October 18, 2022.
[9] https://scikit-learn.org/stable/modules/clustering.html#clustering
[10] Y. Wan et al., "Anomaly Detection Based on Correlative Prediction for Elastic Optical Network," 2021 Opto-Electronics and Communications Conference (OECC), Hong Kong, Hong Kong, 2021, pp. 1-3, doi: 10.1364/OECC.2021.T2A.7.
[11] R. K. Chouhan et al., "An Unsupervised Attack Detection Approach for Software Defined Networks," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2022, pp. 1025-1030, doi: 10.1109/ICAISS55157.2022.10010577.