A Machine Learning Driven Methodology for Alarm Prediction Towards Self-Healing in Wireless Networks

Luís Mata[1,2,3,4] and Marco Sousa[1,2]
[1]CELFINET, A Cyient Company
Lisbon, Portugal
luis.mata@tecnico.ulisboa.pt,
marco.sousa@cyient.com

P. Vieira[2,3]
[2]Instituto Superior de Engenharia de Lisboa (ISEL)
Lisbon, Portugal
pedro.vieira@isel.pt

M. P. Queluz[3,4] and A. Rodrigues[3,4]
[3]Instituto de Telecomunicações (IT)
Lisbon, Portugal
[4]Instituto Superior Técnico
Lisbon, Portugal
paula.queluz@lx.it.pt, ar@lx.it.pt

2024 Wireless Telecommunications Symposium (WTS) | 979-8-3503-1788-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/WTS60164.2024.10536674

***Abstract*—Although Artificial Intelligence (AI) is already used by 5^{th} Generation (5G) to support specific network functions, the increased complexity of 6^{th} Generation (6G) will demand the adoption of extended AI capabilities to enhance network efficiency. Moreover, high network performance and availability at a sustainable cost will be crucial to emerging applications, such as autonomous vehicles and smart cities. In this context, operators are expected to implement Self-Healing Operations (SHOs) to transition from reactive handling of network faults to a preventive approach, relying on statistical learning of network data. This paper proposes a Machine Learning (ML)-driven methodology to predict network faults using generic Fault Management (FM) data, enabling the implementation of preventive actions to avoid service degradation or failure. The evaluation of this methodology using live network data revealed statistical associations among certain network faults, considering both time and root-cause factors. Therefore, FM data and two ML models, namely Logistic Regression (LR) and Light Gradient Boosting Model (LGBM), were used to predict network faults, achieving a 93% success rate within a 60-minute anticipation period.**

***Index Terms*—Mobile Networks, Self-Healing Operations, Predictive Fault Management, Machine Learning.**

I. Introduction

On the road to transitioning to 6^{th} Generation (6G) networks, Mobile Network Operators (MNOs) are faced with the challenge of enhancing the operational efficiency of current and future wireless networks, ensuring high network performance and availability. To address this challenge, a paradigm shift is required where Machine Learning (ML)-driven methodologies are used to increase automation across the different network domains, such as Fault Management (FM) and Performance Management (PM), devising intelligent, self-organising, and cost-effective strategies to reduce operating expenses. Regarding the FM domain, there is a shift from the traditional reactive approach to a predictive one, allowing for the implementation of Self-Healing Operations (SHOs) [1–5].

Considering the importance of reliable mobile networks in the adoption of new services, the integration of SHOs in evolving wireless networks is paramount for enabling MNOs to meet growing demands, while maintaining performance and sustainability. The traditional life cycle of network operations encompasses monitoring, detecting, and correcting network failures. Typically, these failures are identified through the activation of network alarms, prompting a reactive FM process that aims to restore the network to its normal state [6].

The paradigm shift of SHOs aims at implementing methodologies for alarm prediction and their root causes identification (*e.g.,* transmission failures in a mobile Base Station (BS)), with the objective of identifying and rectifying potential issues before they escalate into service disruptions. The adoption of preventive measures reduces the likelihood of critical failures and optimises network performance over the long term. Moreover, addressing issues early reduces costs in emergency repairs and increases customer satisfaction by minimising network downtime. Research on predictive approaches is undergoing, as in [7], where the authors proposed a model for predictive anomaly detection using Key Performance Indicators (KPIs), for a 4^{th} Generation (4G) network. The authors reported that linear ML models provided good accuracy in anomaly detection, although the accuracy notably declined for time intervals exceeding 15 minutes. In [8], the authors extended predictive FM to 5^{th} Generation (5G) core networks using traffic time series analytics to predict system failures relying on ML algorithms, validated through a 5G simulation platform. Additionally, in [9], the authors proposed an Artificial Intelligence (AI)-based framework called "openFM" for end-to-end autonomous FM of 5G and Beyond 5^{th} Generation (B5G) networks. Despite these advancements, existing methodologies for predictive FM often rely on limited data or focus on specific alarms,

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.

leaving a gap in the literature for a more comprehensive exploration of FM alarms, including their periodicity and predictability, while leveraging data from live networks.

In this context, this paper introduces a ML-driven methodology designed to predict network alarms by harnessing generic FM data. This methodology is founded on the observation that, in a mobile network, FM alarms often exhibit interdependent occurrence patterns, as evidenced by a comprehensive analysis using FM data collected from a live network. The advantages of the proposed methodology are twofold. Firstly, it is data-oriented and agnostic to the Radio Access Technology (RAT). Secondly, it is highly parametrizable, enabling flexible customization to suit specific use cases.

In summary, the main contributions of the paper are:

- Analysis of statistical associations between alarms in a live mobile network, taking into account their root causes and their network impact.
- Proposal of a ML-driven methodology to assist SHOs in predicting network alarms exclusively from historical alarm data, offering flexibility for customization to suit specific use cases.
- Evaluation of the methodology by applying distinct ML models with data from a real network.

This paper is organized as follows: Section I introduces the problem and covers related work. Section II analyses live network FM data and shows the statistical association between alarms. Section III introduces the proposed predictive FM methodology, while Section IV evaluates the methodology with various ML models. Section V concludes and outlines future work.

II. FM Data Analysis

This section analyses the FM dataset, Γ, used in this paper and highlights ten representative alarms to illustrate the application of the proposed methodology.

A. Dataset Overview

Due to the scarcity of historical FM data available for recent 5G networks, this study employed a 4G FM dataset as a practical demonstration of the proposed methodology. This decision was grounded in the similarity of FM data and the method's versatile applicability to any RAT. This dataset encompasses 135 distinct FM alarms recorded over a span of 35 calendar days, where ~692 000 alarm occurrences were registered across 1652 BSs. These FM alarms can be categorised based on their severity levels, which indicate the degree of urgency or criticality, and their root-cause typification, pinpointing the underlying reasons for the alarms. Tables I and II provide a breakdown of the observed FM alarm types, grouping them respectively by severity level and by their diverse root-cause factors, as presented in the vendor specifications [10]. Moreover, a succinct description for each alarm type is included, notably considering the network impact and handling policy of each alarm level.

Table I: Severity level of the FM alarms.

Alarm Level	Impact on Services	Handling Policy	Distinct Alarms (#)
Critical	Very high	Immediate action	3
Major	High	To be handled in time	77
Minor	Low	Check-up required	41
Warning	None	Dependent on status	14
			135

Table II: Root-cause typification of the FM alarms.

Alarm Type	Description	Distinct Alarms (#)
Communication	Inter device link failure	5
Environment	Environmental faults	14
Hardware	Physical resource faults	41
Power	Power supply faults	4
QoS	Service quality	1
Running	Transfer information status	33
Security	Security issues detected	4
Signalling	Signalling failures	16
Software	Processing errors	4
Trunk	Transmission links failures	13
		135

The occurrence patterns between the 135 unique observed alarm types are visualised in Figure 1. The severity level for each alarm type, as outlined in Table I, is presented on the left side of the diagram. Conversely, the typification of the root-causes, as described in Table II, is displayed on the right side.

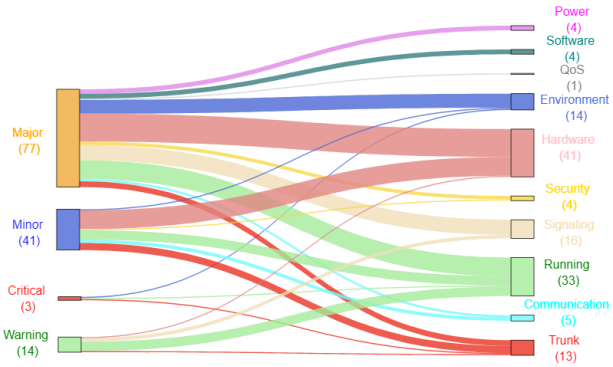

Fig. 1: Occurrence patterns of FM alarms considering their severity and root-cause typification.

It is evident that "Critical" alarms, which have the most significant impact, span across three distinct categories: "Trunk," "Running," and "Environment." Additionally, it is noteworthy that the same root-cause typification can

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.

result in varying severity levels of alarm occurrences based on the context.

B. Statistical Relation Between Alarms

The development of a supervised ML-based alarm prediction methodology, relying on previous occurrences of alarms, is grounded in the assumption that alarms are interrelated, reinforcing prediction confidence through their collective contributions. To explore this assumption, a correlation analysis was conducted providing the average correlation of each alarm with all other alarms. Additionally, given the diverse range of alarms in the FM dataset it is important to examine their distribution of occurrences. Hence, a scatter analysis between the average correlation of each alarm with the remaining ones (x-axis), and the total number of occurrences (y-axis) is presented in Fig. 2. Each point denotes an alarm, whose size represents the distinct number of BSs with occurrences, where the colour depicts its root-cause typification. Considering the diverse occurrences of alarms, a logarithmic scale was implemented on the y-axis. At the peak of this scale, a singular alarm from the "Trunk" category stands out, with over 5×10^6 instances recorded over the 35-day time-frame. This equates to an alarm being triggered approximately every 11 minutes.

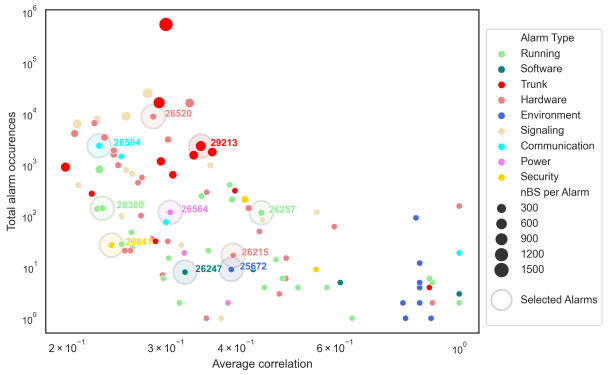

Fig. 2: FM alarms distribution and the selected 10 target alarms.

As observed, FM alarms display significant statistical correlations, further supporting the hypothesis that statistical learning can be used to predict the likelihood of a specific alarm occurrence based on the prior occurrence of other alarms. For instance, a critical alarm may be preceded by specific patterns of minor alarms, potentially serving as informative cues for predicting the former and facilitating the implementation of preventive measures. Moreover, due to the impracticality of evaluating the proposed methodology with every alarm type present in the FM dataset, a shorter list of ten representative alarms is defined for evaluation purposes. These alarms were chosen using inclusion criteria considering occurrence frequency, severity levels, root causes, and inter-alarm correlations, ensuring the representation of diverse distribution segments. The target alarms are indicated in Fig. 2 by greyed circles surrounding the corresponding FM alarms, with the displayed number representing the alarm designation per the vendor's specifications (*e.g.,* alarm "29213"). In Table III, the selected alarm list is detailed, with additional descriptive information.

Table III: List of representative target alarms.

Alarm ID	Alarm Type	Alarm Level	Brief Description
25672	Environment	Critical	Burglar Alarm
26215	Hardware	Major	Inter-Board Link Failure
26247	Software	Minor	Configuration Failure
26257	Running	Warning	SW download ended
26504	Communication	Minor	RF Unit CPRI Error
26520	Hardware	Major	TX Gain Out of Range
26564	Power	Major	Input Power Failure
26841	Security	Major	Certificate Invalid
28380	Hardware	Major	NE Shutdown
29213	Trunk	Critical	eNB S1 Interruption

III. Predictive FM Methodology

This section introduces the ML-based methodology for alarm prediction using FM data and provides an illustrative example of its implementation.

The FM dataset, referred to as Γ, introduced in Section II, exhibits an irregular structure that contains alarm occurrences based on internal identification codes but lacks associated labels. As a result, employing a supervised learning approach with ML models is not feasible. Therefore, given the statistical relationships between alarms, the goal is to generate a modified dataset, denoted as $D = f(\Gamma)$, suitable for application with general ML models. These models will predict alarm occurrences based on the historical patterns of prior alarms. As a result, the proposed methodology is centred on three core objectives.

- Introduction of a regular time scale, which can be customised to suit specific use cases.
- Creation of labels to support a multi-class classification, where each class denotes a customisable time interval until the next occurrence of a given target alarm.
- Creation of features relying on the elapsed time between the selected target alarm and all the remaining ones.

Formally, the FM dataset is denoted by $\Gamma = \{v_i, o_i\}_{i=0}^{m}$, where $v_i \in V$ (set of possible alarms) and $o_i \in O$ (timestamps of alarm occurrences) are respectively the identification and occurrence time of the i^{th} alarm, and m is the number of alarm occurrences. Considering the irregular time occurrence of network alarms, the

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.

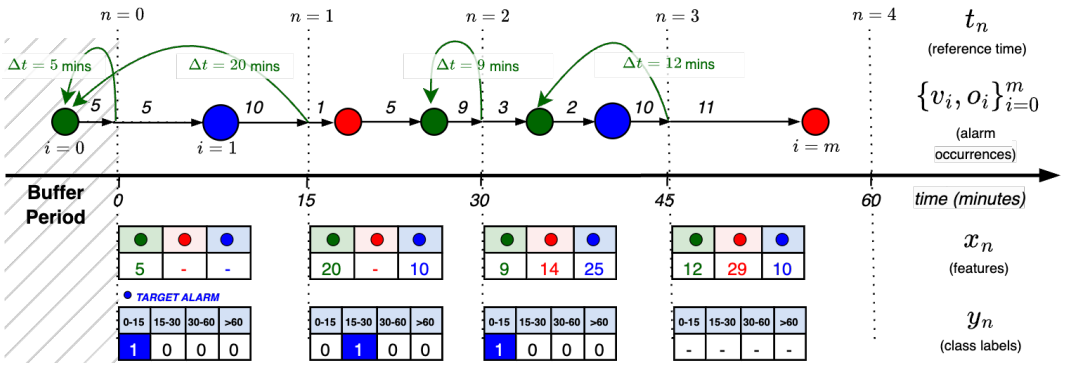

Fig. 3: Exemplification of the proposed methodology for the generation of the dataset, $D = \{x_n, y_n\}_{n=0}^{3}$, from FM alarm occurrences, $\Gamma = \{v_i, o_i\}_{i=0}^{m}$, considering the "blue" alarm as the target alarm, and using $\delta = 15$ minutes and $K = 4$.

proposed methodology starts by creating a new dataset, D, with a regular time-scale, T, where, for each $t_n \in T$, a feature vector, $x_n \in \mathbb{R}^P$, reflects the elapsed time since the last occurrence of each alarm, $v_i \in V$, up to t_n. Here, $P = \mathbf{card}(V)$ indicates the number of possible FM alarm types. Moreover, a set of target alarms, $A \subset V$, is defined for developing ML-based prediction models. Therefore, for each x_n, a label vector, $y_n \in \mathbb{R}^C$, is generated, where $C = \mathbf{card}(A)$ represents the number of target FM alarms. Subsequently, for each target alarm $a \in A$ a label $y_n^a \in [0, K-1]$ is assigned, through a multi-class classification with K categories. These categories correspond to the time intervals for the next alarm occurrence after t_n, where the first time interval is given by $I_0 = [t_n, t_n + \delta[$, with t_n being the reference time instance and δ representing the minimum interval length in minutes. Subsequently, the following k^{th} time intervals increase according to a geometric progression of δ, defined as $I_k = [t_n + \delta \times 2^{(k-1)}, t_n + \delta \times 2^{(k)}[$ for $k = 1, 2, ..., K-2$. The last interval is given by $I_{(K-1)} = [t_n + \delta \times 2^{(K-2)}, \infty[$, with an infinite length.

Figure 3 depicts the methodology to create the labelled dataset, D for an example considering three alarm types, V = [RED, GREEN, BLUE], with a single target alarm to be classified; A = [BLUE]. In this example, the model is parameterised with $K = 4$ and $\delta = 15$, which results in the following four intervals: 0-15, 15-30, 30-60, and >60 minutes. The four classification classes were chosen such that they present actionable time intervals that enable MNOs to deploy preventive actions to avoid network faults or, at least, mitigate their effects. In this paper, the choice of a geometric progression for the K time intervals is driven by the recognition that fine time granularity is crucial for short-term predictions, but less vital for longer-term scenarios where preventive actions are limited. However, these intervals can be easily customised for specific use cases. As seen in Figure 3, new dataset entries are created at each time reference t_n, capturing the elapsed time since the last occurrence of all other alarms (e.g., Δt for the GREEN alarm). The corresponding class is determined based on the time elapsed from t_n until the next occurrence of the target alarm. Given that the proposed methodology depends on the time intervals between alarms and on the reference times for feature creation (x_n), an initial buffer period was considered in the dataset to include the first occurrence of each possible alarm $v_i \in V$, whenever feasible. The data within this buffer period was not used for model training and evaluation; its sole purpose was feature initialisation.

IV. Experimental Study

In this section, the proposed methodology is applied to the FM dataset presented in Section II, considering the list of ten target alarms. Additionally, the proposed methodology is tested with two ML models also considering a feature selection process for the input features in the FM predictive models.

A. Feature Selection and Implementation

A two-step feature selection process was executed to exclude non-informative features (alarm types). In the initial step, alarms displaying an average correlation with the remaining alarms below 10% were removed, as they represent independent events with limited value for the prediction. Subsequently, alarms exhibiting pairwise correlations surpassing 95% were randomly eliminated to mitigate the impact of multicollinearity. This resulted in a final feature set of 57 alarm types.

As referred in Section III, the proposed methodology is rooted in the creation of a dataset, D, which is suitable for the application of a supervised learning approach using generic ML models. Hence, in this section two ML algorithms were employed as an example for predictive FM modelling, starting with a simple Logistic Regression (LR) and then adding more complexity with

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.

a Light Gradient Boosting Model (LGBM). However, the methodology is agnostic and can be applied with any generic ML algorithm. Each algorithm was trained on 70% of the total dataset using the negative log-likelihood loss function. The hyperparameter tuning was performed on 20% of the data using a standard optimisation framework [11]. Finally, the models' results were subsequently assessed on the test set, for the remaining 10% of the dataset.

B. Experimental Results

The proposed methodology was evaluated in eight experiments employing the considered ML algorithms to predict the occurrence of the ten pre-selected target alarms. A multi-class classification approach with four time intervals for the occurrence of the next alarm (0-15, 15-30, 30-60, and >60 minutes) was considered and the F1-Score was used as the accuracy metric for the classification. The experiments were conducted as follows: in the 1^{st} and 2^{nd} experiments, all the alarms were used as features and default hyperparameters were applied ("$\_ALL$"). For the 3^{rd} and 4^{th}, optimizations were considered; a Lasso regularization in the case of the LR ("$\_ALL\text{-}REG$"), and hyperparameter tuning was performed in the case of LGBM ("$\_ALL\text{-}T$"). The Lasso regularisation, or L1 regularisation, was chosen due to its capability to drive the weights of less important features to zero, resulting in a simpler model with improved interpretability. The same experiments were subsequently replicated with the reduced set of alarm types ("$\_FS$"). In Fig. 4 the experiments' results, using both ML models, are illustrated, providing a breakdown of the model predictions for each class (time interval for next alarm occurrence). Primarily, it stands out that only three target alarm types have more than 100 examples comprised within the first three classification classes. Therefore, the result analysis is focused on the target alarms "26520," "29213," and "26504". The highest F1-Score, surpassing 80%, was attained with alarm "29213" (eNodeB S1 Interruption). Furthermore, the LR model consistently lags behind the LGBM, highlighting the presence of non-linear relationships between the model's features and the alarm occurrence intervals (the median value observed is approximately 5 days between alarm occurrences). The LGBM can capture such non-linear relationships between the occurrence of an alarm and the prior occurrence of other alarms, resulting in superior accuracy compared to the LR. Regarding the remaining alarms, either the employed classes for the time intervals do not align with their occurrence patterns, or they may be independent events that are challenging to predict based on previous alarms.

Despite the positive outcomes observed in these experiments using multi-class classification to predict alarm occurrence time intervals, notably with alarms "26520," "29213," and "26504", their applicability in real network operations scenarios, considering only the F1-Score analysis, may present challenges in terms of interpretability. A simplified approach, with a binary classification for each class, offers clearer insights, making it more accessible for MNOs to measure the model's impact for SHO. Therefore, Receiver Operating Characteristic (ROC) curve analysis [12] can be used to showcase the model's classification accuracy for each class against all others. The performance of the model for each specific class can be further evaluated using the Area Under the Curve (AUC), indicating the probability of the model assigning a higher score to a random positive example than to a random negative one. Hence, in Fig. 5, the ROC curve analysis is presented to supplement the evaluation of the classification performance for the alarm "29213".

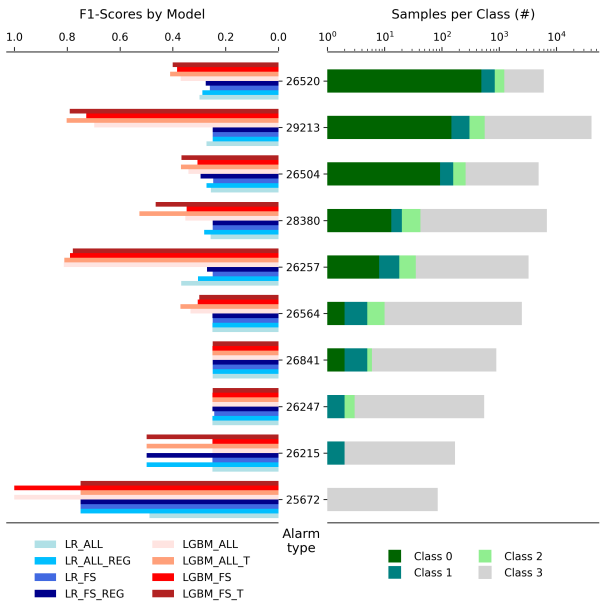

Fig. 4: F1-Score obtained for the list of target alarms and the respective number of test set examples.

The analysis of the ROC curves for alarm "29213" reveals AUC values higher than 97% across all prediction classes. Notably, when considering the first three classes representing predictions up to 60 minutes, a combined probability of 93% is achieved. Therefore, within a 60-minute anticipatory window, there is a 93% likelihood of accurately predicting alarm "29213". Considering this alarm's "critical" severity, this is an encouraging result that could pave the way for implementing preventive measures to mitigate, or avert, its impact on the network. Not only it can lead to the enhancement of network management efficiency, but it also contributes to a seamless

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.

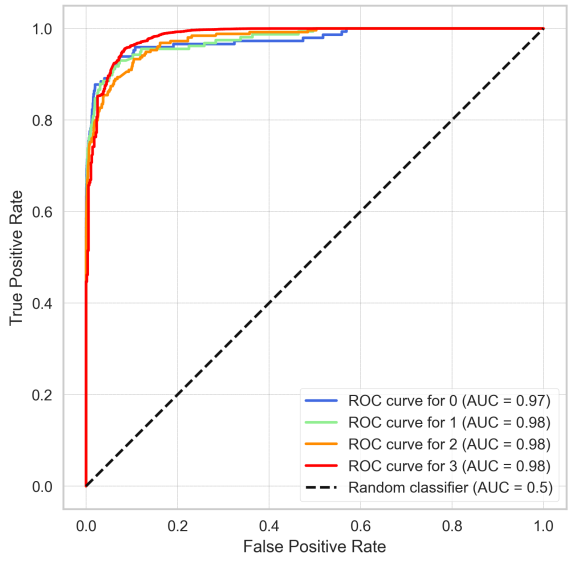

Fig. 5: ROC curves for the alarm 29213 (eNB S1 Interruption).

and uninterrupted experience for end-users.

In summary, the proposed methodology offers two key advantages. Firstly, it remains agnostic to the RAT, relying solely on the occurrence time of generic FM events. Secondly, it is adaptable to diverse use cases, permitting a scalable and incremental analysis of results by tailoring the prediction intervals.

V. Conclusion and Future Work

Considering the complexity of future 6G networks, MNOs are expected to adopt SHO as a new operative model for FM, aiming at enhancing operational efficiency and reducing operating costs. A possible SHO-based approach relies on using ML-driven methodologies to predict network faults, allowing the implementation of preventive actions to avoid network performance degradation. This paper proposes a new methodology for predicting the occurrence of network faults, relying only on generic FM data. Hence, it can be applied to current and evolving wireless networks towards 6G. By applying the proposed methodology, a FM dataset is generated to support the development of predictive models for the occurrence of a target alarm across multiple time intervals, given the occurrence of previous alarms. The proposed methodology was evaluated with FM data from a live 4G network due to data availability constraints. For the methodology evaluation, two ML models were used: LR and LGBM. An F1-Score of 80% was achieved in classifying a critical alarm, whose occurrence can be predicted with a joint probability of 93% with up to 60 minutes antecedence.

For future work, it is envisaged to evaluate this methodology with more complex ML algorithms, notably with spatial-temporal graph networks and applying 5G data.

Acknowledgment

This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020.

References

[1] M. Cilínio, D. Duarte, P. Vieira, M. P. Queluz, and A. Rodrigues. Root cause analysis of low throughput situations using boosting algorithms and the treeshap analysis. In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, pages 1–5, 2022. DOI:0.1109/VTC2022-Spring54318.2022.9860734.

[2] Chao Zhang. Intelligent Internet of Things Service Based on Artificial Intelligence Technology. *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pages 731–734, 2021. DOI: 10.1109/ICBAIE52039.2021.9390061.

[3] Muhammad Zeeshan Asghar, Furqan Ahmed, and Jyri Hämäläinen. Artificial intelligence enabled self-healing for mobile network automation. *2021 IEEE Globecom Workshops*, pages 1–6, 2021. DOI:10.1109/GCWkshps52748.2021.9681937.

[4] Muhammad Sajid Riaz, Haneya Naeem Qureshi, Usama Masood, Ali Rizwan, Adnan Abu-Dayya, and Ali Imran. Deep learning-based framework for multi-fault diagnosis in self-healing cellular networks. *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 746–751, 2022. DOI:10.1109/WCNC51071.2022.9771947.

[5] Tao Zhang, Kun Zhu, and Ekram Hossain. Data-driven machine learning techniques for self-healing in cellular wireless networks: Challenges and solutions. *Intelligent Computing*, 2022, 2022. DOI:10.34133/2022/9758169.

[6] Cherrared, Sihem and Imadali, Sofiane and Fabre, Eric and Gössler, Gregor and Yahia, Imen Grida Ben. A Survey of Fault Management in Network Virtualization Environments: Challenges and Solutions. *IEEE Transactions on Network and Service Management*, 16(4):1537–1551, 2019. DOI:10.1109/TNSM.2019.2948420.

[7] Hadj-Kacem, Imed and Jemaa, Sana Ben and Allio, Sylvain and Slimen, Yosra Ben. Anomaly prediction in mobile networks: A data driven approach for machine learning algorithm selection. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–7, 2020. DOI:10.1109/NOMS47738.2020.9110429.

[8] Pousali Chakraborty and Marius Corici and Thomas Magedanz. System Failure Prediction within Software 5G Core Networks using Time Series Forecasting. *IEEE International Conference on Communications Workshops, ICC Workshops 2021, Montreal, QC, Canada, June 14-23, 2021*, pages 1–7, 2021. DOI:10.1109/ICCWorkshops50388.2021.9473530.

[9] Mukherjee, Shubhabrata and Coudert, Oliver and Beard, Cory. An open approach to autonomous ran fault management. *IEEE Wireless Communications*, 30(1):96–102, 2023. DOI:10.1109/MWC.004.2200244.

[10] Huawei. Overview of alarms: eSight 20.1 Operation Guide 12, 2023. URL https://support.huawei.com/enterprise/br/doc/EDOC1100192873/9bf87a75/overview-of-alarms. Accessed: 2023-09-14.

[11] Takuya Akiba, Shotaro Sano, Toshihiko Yanase, Takeru Ohta, and Masanori Koyama. Optuna: A Next-generation Hyperparameter Optimization Framework. *25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 2623–2631, 2019. DOI:10.1145/3292500.3330701.

[12] Andrew P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. *Pattern Recognition*, 30(7):1145–1159, 1997. DOI:0.1016/S0031-3203(96)00142-2.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on November 06,2024 at 08:38:22 UTC from IEEE Xplore. Restrictions apply.