Machine-Learning-Assisted Failure Prediction in Microwave Networks based on Equipment Alarms

Francesco Lateano*, Omran Ayoub†, Francesco Musumeci*, Massimo Tornatore*
*Politecnico di Milano, Milan, Italy. †Scuola Universitaria Professionale della Svizzera Italiana, Lugano, Switzerland.
‡Corresponding author: Francesco Lateano

***Abstract*—Modern microwave networks must cope with strict Quality of Services (QoS) requirements, such as low latency, high bandwidth and high availability. As network failures can affect service availability, failure management is crucial for service maintenance and, recently, application of Machine Learning (ML) for automated failure management is becoming pervasive. In particular, ML promises to deliver predictive maintenance capabilities, where failure occurrence is anticipated thanks to ML prediction capabilities. In this study we developed two workflows, based on a modular ML implementation, capable of short- and long-horizon failure predictions, while taking into consideration computational complexity constraint. As input data, we used real alarms coming from deployed equipment of a nation-wide microwave network. Our ML-based failure-prediction system learns from human experience through labelled data, performs alarms forecasting, detects future failure occurrence and identifies failure root causes. In our numerical results, we compare the prediction performance of different ML models in terms of various standard ML performance metrics. Overall accuracy over 95% is achieved in all prediction scenario simulated within an hour, suggesting that microwave network operators can gain actual operational benefits by deploying this framework in real-world infrastructures.**

***Index Terms*—Machine learning, microwave networks, alarms forecasting, failure identification and prediction, root-cause analysis**

I. Introduction

Today's microwave networks are installed with built-in monitoring capabilities, and generate a huge amount of monitored data, that can be stored and processed using new raising technologies, as network telemetry, SDN/NFV, edge computing, etc. Such progress in network monitoring makes Machine Learning (ML) a suitable methodology to automate microwave failure management [1].

Failure management plays a role of capital importance in communication networks to avoid service disruptions and to satisfy customers service level agreements (SLAs). Currently, failure management strongly depends on the ability of domain experts to perform manual troubleshooting of failures by observing monitored alarms and performance metrics. Considering the high amount of information to be treated in modern microwave networks and the stringent availability requirements of today's service, this time-consuming and human-error-prone process is not scalable. Novel Machine Learning (ML) techniques are currently being investigated as a solution towards automated failure management to reduce service unavailability by taking adequate countermeasures in a timely manner. Among the different aspects of failure management, future failure prediction is among the most important for network operators, as it may allow proactive decision making, such as network reconfiguration, traffic re-routing, in-field intervention, etc., and hence limit service unavailability.

The failures that can occur in a microwave link can be broadly classified either into failures related to radio signal propagation, such as channel interference and fading, or hardware failures, i.e., failures affecting the functioning of transmitting/receiving equipment. Microwave network operators can detect the failure the moment the link suffers from an unavailability (known as Unavailable Seconds, or UAS). Despite detecting the failure upon its occurrence, the forecast of future failures remains of utmost importance to network operators. In this study, we focus on automating failure management with the specific objective of forecasting failure occurrence and identifying failures causes of hardware failures leveraging alarm messages from network devices. More specifically, we develop a ML-based framework for future failure prediction in microwave networks that leverages field alarms collected from 1025 deployed microwave links. During the development, the prediction problem is designed with two alternative workflows differing in terms of time horizon and granularity. One achieves long-term predictions analyzing 15 minutes time intervals, while the other permits deeper inspection of data considering 1 second time intervals, but reaching a less forward-looking prediction in the future.

The proposed framework achieves promising results, measured in term of accuracy, precision, recall, with negligible execution time. We can summarize the contribution of this paper as follows:

- We propose a **short-term** proactive root-cause failure prediction using deep neural networks based on Long Short Term Memory cells, to forecast future alarm behaviour with a short-term time horizon (in the order of seconds); leveraging alarm forecast, joint failure detection and root-cause identification are performed using multiple ML classification models;
- We propose an alternative **long-term** ML-based prediction approach aiming at forecasting future failure causes considering only current alarms status and with no need for future alarms forecast.

The rest of the paper is organized as follows. In Sec. II relevant existing work is discussed. Sec. III formulates the problem, while Sec. IV discusses the proposed framework. Sec. V discusses the numerical results obtained using real monitored data labelled by domain experts. In Sec. VI we

draw our conclusion.

II. Related Work

The problem of automated failure management in communication networks has gained lot of traction lately, with ML technologies enabling and pushing towards this automation [2]. Data collected from networks as alarms are used for either supervised-ML frameworks for failure detection [3], [4] and failure-cause identification [5], [6], or unsupervised ML frameworks for anomaly detection and identification [7], [8] when labelled data is scarce. Furthermore Ref. [9] shows time series prediction method based on variant LSTM recurrent neural network. In microwave (and, more generically, radio) networks, Refs. [10] and [11] are among the earliest works focusing on failure root-causes analysis. In Ref. [10] authors applied correlation techniques based on causality graphs and associate failure root-causes to alarm sequences. Similarly, Ref. [11] adopts artificial neural networks to correlate the presence of different alarms in mobile network equipment to an initial cause generating the alarms sequence. Authors in Ref. [12] designed a framework for automatic anomaly detection and root-cause identification in mobile networks, based on alarms and employing a decision process which emulates the human reasoning. In Ref. [5], microwave link failure detection based on LSTM was employed assuming sequential link features that describe the signal strength and power, and error states of nodes and links. Meanwhile, in Ref. [13] explainable artificial intelligence is used for failure identification. So, our works propose a new way to foresee failure root-cause using detection and identification technologies.

III. Problem Statement

The main goal of our study is to predict failure root cause by monitoring alarm data coming from microwave equipment. Given as input data the status of alarms (with a time granularity that can go down to one alarm instance per second), we aim to forecast the root cause (among a set of possible predefined root cause classes) of future failures with its relative probability.

To this end, we jointly solve the following three subproblems:

- **Alarm Forecasting**. Given current and past status of alarms, we predict future status (on or off) of all alarms. The alarm forecasting is modeled using a LSTM model.
- **Failure Detection**. Leveraging the prediction of the status of all alarms, we perform "incoming failure" detection, that is modeled as a supervised binary classification problem.
- **Failure Identification**. Once an incoming failure is detected, we identify the root-cause of this failure by classifying it into one of the root-cause classes. The failure root-cause identification is modeled as a supervised multiclass classification problem.

Timestamp	Alarm name	Change in alarm status	Link ID	Site ID

TABLE I: Alarm message structure

IV. Machine-Learning Failure Prediction Framework

The overall framework for failure prediction is summarized in Fig. 1. Details regarding each phase are reported in the next subsections.

A. Data Collection

Data regarding alarms and performance metrics are collected over a real nation-wide microwave network. Alarm messages are collected from 1025 links in period spanning seven consecutive days. Based on type of equipment installed, a total of 231 alarms exist. A centralized server collects alarm messages arriving from any link in the network, which represent the raw data. The alarm message format is shown in Table I.

B. Data Preprocessing

The alarm messages of each link are elaborated considering *site id* and *link id*, and, based on the change in alarm status, a sequence of bits (1 or 0) is constructed where each bit of the sequence indicates if an alarm is on or off in a given second. That is, for each alarm at a given site and at a given link, the alarm status at each second is reported, constructing what we refer to as *alarm bit sequence*. In total, for each alarm on a given site, 604800 seconds, referring to the whole duration of seven days, are constructed representing alarm status. Starting from the *bit sequence* dataset, we construct another dataset of 15-minute granularity windows considering i) the number of seconds an alarm is on (this value ranges between 0 and 900 in a 15-minute window) and ii) the number of times an alarms goes on in a window (ranges from 0 to 450). We refer to this dataset as *15-min window*. The *15-min window* dataset consists of 787200 data points of which 49899 with failure and 737301 without. In summary, two datasets are used in our analysis:

- **Alarm bit sequence**: contains, for each link, a row of bits representing the binary alarm status at each second.
- **15-min window**: aggregates bit sequences in windows of 15 minutes, counting for each alarm and each window the number of seconds the alarm is on and the number of times the alarm activates.

C. Building the Ground Truth: Clustering and Labeling

To build the ground truth for our framework, we labelled the observations belonging to failure classes in the *15-min window* dataset. Then, we performed clustering using k-means, assigning the same root-cause label to data points belonging to same cluster. Specifically, different numbers of clusters have been taken into consideration and to determine the best number of clusters, first we performed elbow analysis on inertia, then we had multiple interactions with domain experts

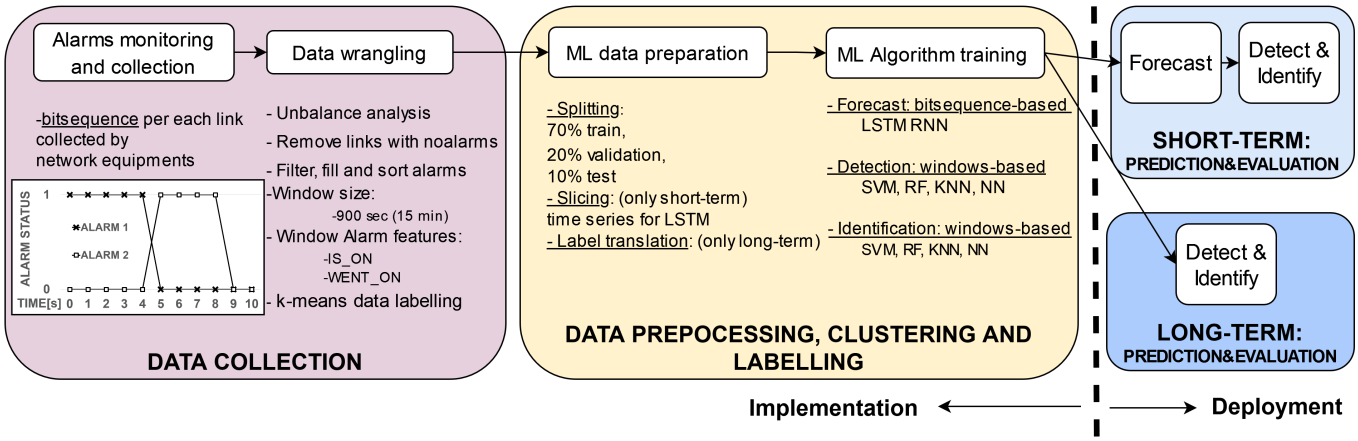

Fig. 1: Overall Prediction Diagram

who manually analyzed around 10% of the data points of each cluster for label assignment. At the end of this clustering and labelling process, we ended up with 35 clusters, assigned by domain experts to different failure root causes.

In the next two subsections we describe two different proposed approaches for failure prediction, namely, *Short-Term* Approach in Subsec. IV-D, and *Long-Term* Approach in Subsec. IV-E.

D. Short-Term Approach

The *short-term* approach consists of three components: *alarm forecaster*, responsible for predicting future status of alarms, *failure detector*, responsible for detecting failures, and the *fault identifier*, which, in case a failure is detected, is responsible to identify failure cause. Fig. 2 shows the overall workflow of the *short-term* approach. First, the bit sequence of each alarm is given as input to the *alarm forecaster*. Then, the *alarm forecaster* outputs the predicted status of all alarms for a given time horizon (1 or 0 for ON or OFF status, respectively). To forecast alarm status, we employ three different models, including two baseline algorithms used as benchmarks:

1) **Baseline**: as baseline approach we use a static probabilistic forecaster with fixed probability for ON and OFF status, based on the overall percentage of ON alarms in the whole dataset. For each alarm, its future status is selected with probability p_1 or p_0, for ON ('positive') or OFF ('negative') status according to the following formulas:

$$\begin{cases} p_1 = \dfrac{positive[all\ data]}{total[all\ data]}; & (1) \\ p_0 = 1 - p_1. & (2) \end{cases}$$

2) **Baseline Optimized**: here we consider a variable probabilistic forecaster, where ON and OFF probabilities p_0 and p_1 also depend on the alarm status during the preceding 'x' seconds. More specifically, we consider a moving window of x=10 seconds (that corresponds to the prediction interval, in our scenario) and use the following formulas for ON and OFF probabilities:

$$\begin{cases} p_1 = \alpha \dfrac{pos[all\ data]}{total[all\ data]} + \beta \dfrac{pos[mov\ win]}{total[mov\ win]}; & (3) \\ p_0 = 1 - p_1. & (4) \end{cases}$$

Parameters α and β could be set to optimize model performance, and for our work they have been set respectively to 0.5 and 0.1.

3) **LSTM** model with hyperparameters reported in Tab. II

Parameter	Value
Output layer	Dense, sigmoid
Loss function	Binary Cross Entropy
Optimizer	Adam
Overfitting	Earlystopping, patiente 10
Epoch	1, trained iteratively on links

TABLE II: Hyperparameters selected for LSTM algoritm

Based on the outcome of the *alarm forecaster*, 15-minute windows are constructed and are then fed as input to the *failure detector*. The *failure detector* detects whether failure occurs based on predicted status of alarms, and, in case of failure detection, the *fault identifier* classifies the 15-minute window into one of the failure classes. For failure detection and identification, we employed four different ML models, namely, Random Forest (RF), K-Nearest Neighbors (KNN), Support Vector Machine (SVM) and Artificial Neural Network (ANN) with hyperparameters reported in Tables III.

E. Long-Term Approach

The *long-term* approach also uses the *15-min window* dataset and it also consists of three cascaded components, namely, *failure detector*, *fault identifier* and *fault forecaster*. Fig. 3 shows the overall workflow of the *long-term* approach, detailed in the following. First, the *failure detector* takes the 15-min window observations in input and classifies them as either a failure or not. In case of failure, the *fault identifier* classifies the 15-min window observation in one of the

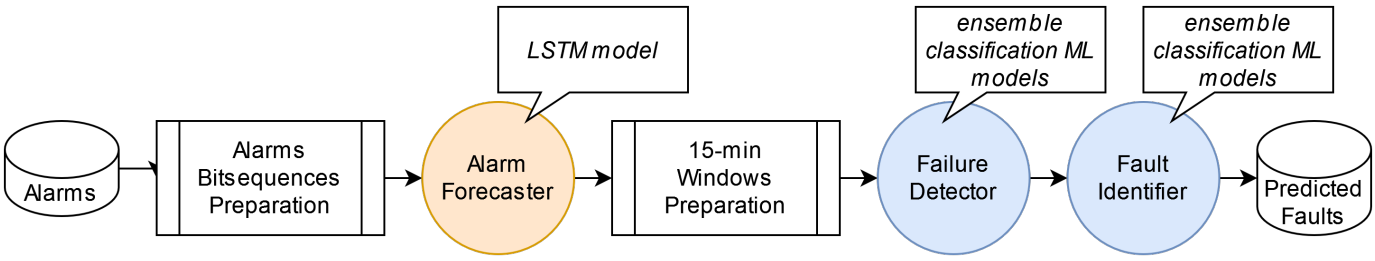

Fig. 2: Short-term Approach

Model	Parameter	Value
RF	Number of trees	10
	Maximum tree depth	10
	Minimum number of split	2
KNN	Number of neighbors	5
	Weight function	Distance
	Distance function	Manhattan
	Searching algorithm	Kd-tree
SVM	Regularization parameter	100
	Kernel	RBF
	Kernel coefficient	0.01
	Decision function	One-versus-rest
ANN	Number of hidden neuron	5
	Activation function	Linear

TABLE III: Hyperparameters selected for ML algorithms

Window #	Fault	New Fault Prediction: 2
1	RC_1	RC_3
2	RC_2	RC_4
3	RC_3	RC_5
4	RC_4	RC_6

TABLE IV: Windows labelling considering 2-windows prediction time horizon

35 classes of failures. The failure root cause identified by *fault identifier* is then given as an input, along with failure root causes identified for x previous windows, to the *fault forecaster*. The *fault forecaster*, which now has a vector representing the failure root causes of the previous x windows on the link, predicts the failure root causes of the next x 15-min windows (i.e., for the next 30 minutes if $x = 2$). To perform failure detection and identification, we use the same four different ML models, namely, RF, KNN, SVM and ANN, used in the *short-term* approach.

V. Numerical Results

We now evaluate the performance of the two prediction approaches. In Subsec. V-A, we focus on the *short-term* approach and in Sec. V-B on the *long-term* approach. In all our evaluations, datasets are divided considering 70% for training set, 20% for validation and 10% for testing. All the results are cross-validated using 10-fold cross-validation method.

A. Short-Term Approach

Alarm Status Prediction: We evaluated the alarm-status prediction model considering different forecasting time horizons ranging from 2 to 120 seconds. Specifically, we consider a forecasting time horizon of 2, 10, 30, 60 and 120 seconds[1]. In all cases, we use 10 seconds of alarm status as input. Figure 4 shows the performance of our developed LSTM approach in terms of accuracy, precision and recall for varying forecasting horizon. Results show that the model achieves its best performance for a 2-seconds (1 for accuracy and precision, and 0.94 for recall). Performance in terms of all the three metrics slightly decreases as the forecasting horizon increases to 10 seconds, but performance does not decreases further as forecasting time horizon increases further to reach 120 seconds. In these cases, the model achieves an accuracy close to 1, precision near 0.94 and recall near 0.86. We now compare the performance of the LSTM approach to two baseline scenarios. Figure 5 shows the performance in terms of accuracy, precision and recall of the LSTM approach with respect to the baseline approaches for a forecasting time horizon of 120 seconds. Results show that LSTM approach significantly outperforms the baseline approaches.

Failure Detection: We now compare the performance of the various models for failure detection. Figure 6 shows the accuracy, precision and recall of RF, SVM, KNN and NN considering windows formed with a forecasting time horizon of 10 seconds and 120 seconds. Results show that all models have an accuracy and precision of around 1 and around 0.95 when windows are formed considering 10 and 120 seconds of forecasting time horizon, respectively. In terms of recall, the models show a performance of around 1 in case of 10-seconds forecasting time horizon, significantly higher than that for 120-seconds forecasting time horizon which shows a recall of 0.82. There are not relevant differences between models. As expected, since the prediction for a longer time into the future is more prone to error, the performance considering a length of 120-second forecasting time horizon is lower than that of 10 seconds. Yet, performance of various models can be considered acceptable, being higher than 0.8.

[1]Note that we limit this analysis to a maximum of 120 seconds as forecasting time horizon due to limitations in the random access memory required to manage all ML model weights needed during the training phase.

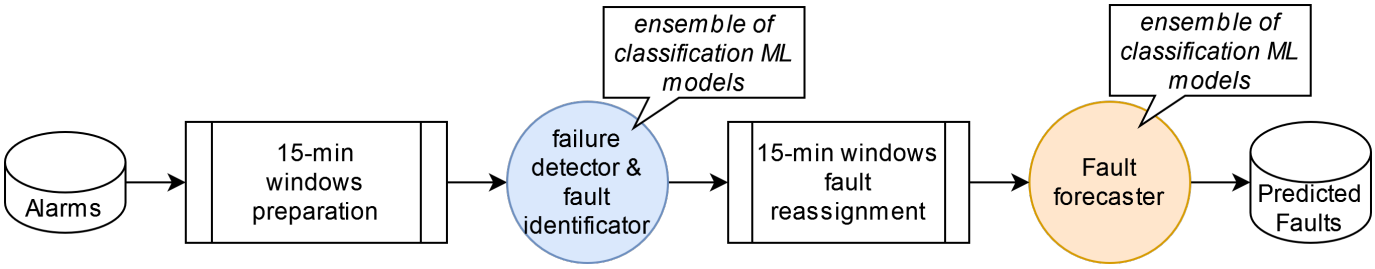

Fig. 3: Long-term Approach

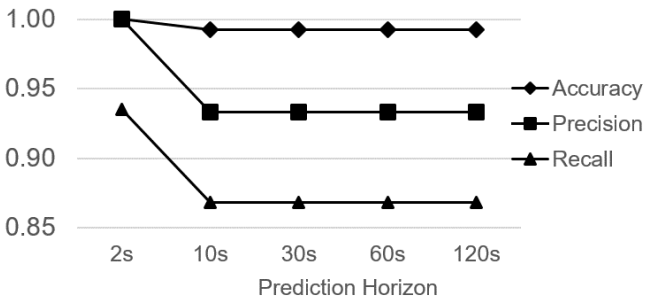

Fig. 4: LSTM performance varying prediction horizon

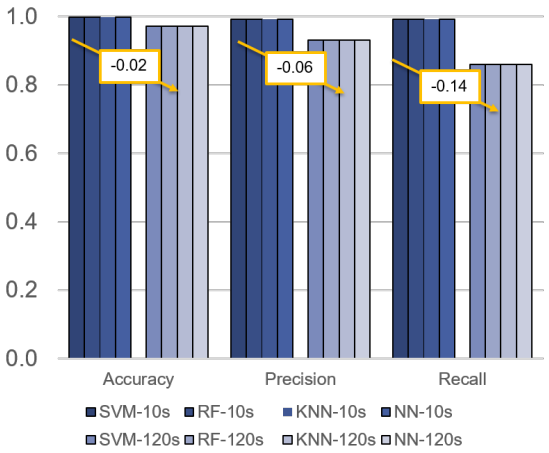

Fig. 6: Short-Term Failure Detection Performance

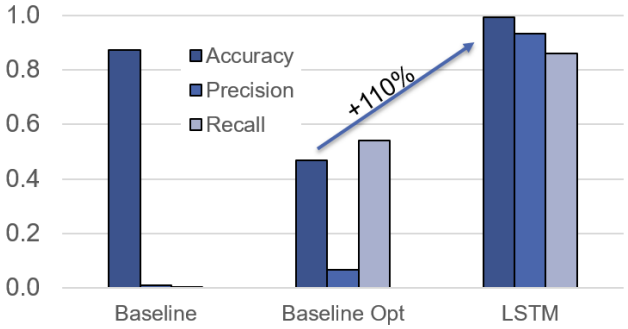

Fig. 5: Alarms Forecast Performance Comparison

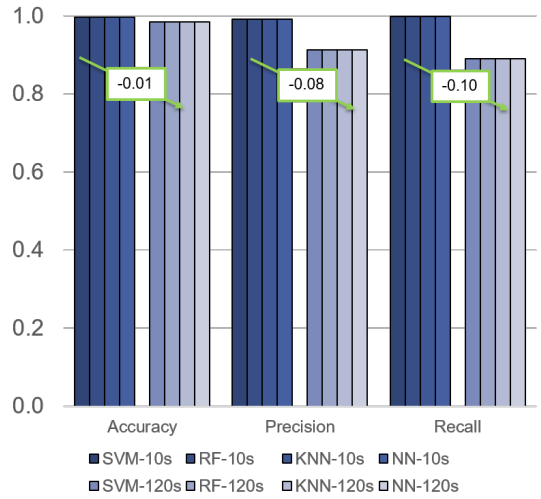

Fig. 7: Short-Term Failure Identification Performance

Failure Identification: We now compare the performance of the different developed models for failure identification. Fig. 7 shows the accuracy, precision and recall considering 10- and 120-second-length forecasting time horizon. Similar to the case of failure detection, results show that models perform better considering a forecasting time horizon of 10 seconds with respect to the case of 120 seconds.

B. Long-Term Approach

We consider three prediction scenarios for the *long-term* approach that differ in terms of the prediction time horizon which is set at either 1, 24 or 48 hours. Figures 8, 9, 10 plot the accuracy, precision and recall, respectively. Results show a general trend inversely proportional to time horizon, with a similar pattern appearing for all metrics in all scenarios,

	PRO	CON
Short-term (seconds)	More accurate	Prediction horizon limited by computational constraint
Long-term (hours)	Longer prediction horizon	Short-term prediction not possible

TABLE V: Prediction approach comparison

except for KNN which shows an unacceptable performance for a prediction interval of 48 hours. Comparing long-term and short-term we note a decrease in long-term performance as expected due to increase in prediction time horizon. An overall comparison between the two approaches is shown in Tab. V.

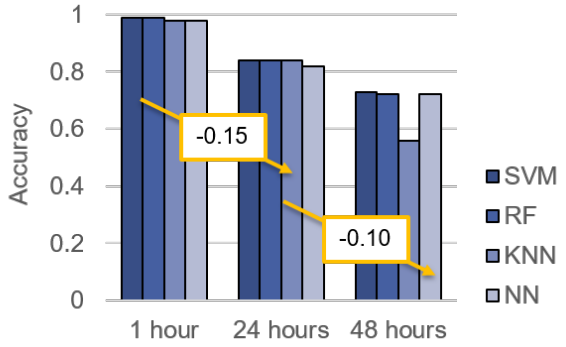

Fig. 8: Long-Term Performance: Accuracy

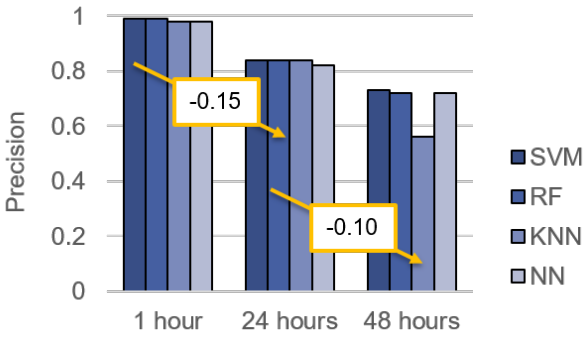

Fig. 9: Long-Term Performance: Precision

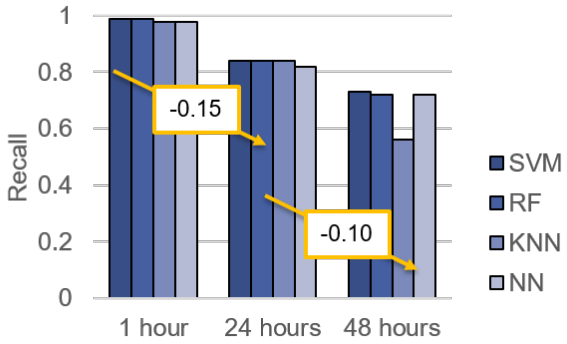

Fig. 10: Long-Term Performance: Recall

VI. Conclusion

We designed a ML-based framework for failure root-cause prediction on microwave links based on equipment alarms from real data. We proposed two different workflows, one for long-term time horizons and the other one for short-term. Each step of the process is measured with performance metrics: accuracy, precision, recall. Overall, considering prediction time horizons, the framework results in very high system performance, with metrics above 95% within an hour, while for longer horizons we lose 20% each 24 hours. Models performs the same for the considered scenario expect for KNN losing reliability at long prediction interval. Execution times are in terms of seconds and are negligible related to the prediction time horizon order of magnitude. These results suggest that our proposed approaches, both short-term and long-term, are suitable to solve this problem. As future work, short-term prediction horizon could be extended and compared directly with long-term approach, by using more powerful computing machines. In addition, future works may focus on the integration of a graph neural network for fault identification and localization.

Acknowledgements

The authors would like to thank colleagues from SIAE Microelettronica S.p.A. (Italy) for providing data on microwave network failures and guidance on the equipment functioning and settings.

References

[1] F. Musumeci, L. Magni, O. Ayoub, R. Rubino, M. Capacchione, G. Rigamonti, M. Milano, C. Passera, and M. Tornatore, "Supervised and semi-supervised learning for failure identification in microwave networks", IEEE Transactions on Network and Service Management, 2020.

[2] X. Chen, B. Li, M. Shamsabardeh, R. Proietti, Z. Zhu, and S. Yoo, "On real-time and self-taught anomaly detection in optical networks using hybrid unsupervised/supervised learning," in 2018 European Conference on Optical Communication (ECOC). IEEE, 2018, pp. 1–3.

[3] L. Pan, J. Zhang, P. P. Lee, M. Kalander, J. Ye, and P. Wang, "Proactive microwave link anomaly detection in cellular data networks," Computer Networks, vol. 167, p. 106969, 2020.

[4] P. Casas, P. Fiadino, and A. D'Alconzo, "Machine-learning based approaches for anomaly detection and classification in cellular networks." in TMA, 2016, pp. 1–8.

[5] Z. Ruan, S. Yang, L. Pan, X. Ma, W. Luo, and M. Grobler, "Microwave link failures prediction via lstm-based feature fusion network," in 2021 International Joint Conference on Neural Networks (IJCNN), pp. 1–8, IEEE, 2021.

[6] P. Casas, P. Fiadino, and A. D'Alconzo, "Machine-learning based approaches for anomaly detection and classification in cellular networks.," in TMA, 2016.

[7] S. Varughese, D. Lippiatt, T. Richter, S. Tibuleac, and S. E. Ralph, "Identification of soft failures in optical links using low complexity anomaly detection," in Optical Fiber Communication Conference. Optical Society of America, 2019, pp. W2A–46.

[8] X. Chen, B. Li, R. Proietti, Z. Zhu, and S. B. Yoo, "Self-taught anomaly detection with hybrid unsupervised/supervised machine learning in optical networks," Journal of Lightwave Technology, vol. 37, no. 7, pp. 1742–1749, 2019.

[9] X.Wang, Y. Zhang, and M. Zhang, "Time series prediction method based on variant lstm recurrent neural network," Neural Processing Letters, vol. 52, no. 2, pp. 1485–1500, 2020.

[10] Kliger, Shmuel, et al. "A coding approach to event correlation." International Symposium on Integrated Network Management. Springer, Boston, MA, 1995.

[11] Wietgrefe, Hermann, et al. "Using neural networks for alarm correlation in cellular phone networks." International Workshop on Applications of Neural Networks to Telecommunications (IWANNT). Stockholm, Sweeden: Citeseer, 1997.

[12] Szilágyi, Péter, and Szabolcs Nováczki. "An automatic detection and diagnosis framework for mobile communication systems." IEEE transactions on Network and Service Management 9.2 (2012): 184-197.

[13] O. Ayoub, F. Musumeci, F. Ezzeddine, C. Passera, and M. Tornatore, "On using explainable artificial intelligence for failure identification in microwave networks," in 2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN), pp. 48–55, IEEE, 2022.