PIM Detection in Wireless Networks as an Anomaly Detection Problem

Gokcan Cantali[†], Eren Deniz[*§], Ozcan Ozay[*], Onur Yildirim[*], Gürkan Gür[‡], and Fatih Alagoz[†]

[*] Yupana Inc., Walnut Creek, USA, name.surname@yupanatech.com
[†] Dept. of Computer Eng., Bogazici University, İstanbul, Turkey, name.surname@boun.edu.tr
[‡] Zurich University of Applied Sciences (ZHAW), Switzerland, gurkan.gur@zhaw.ch
[§] Dept. of Computer Eng., Ege University, İzmir, Turkey, eren.deniz@mail.ege.edu.tr

***Abstract*—As the number of base stations keeps increasing due to ever-growing wireless services and pervasive connectivity, the cost of operation for network service providers rises proportionally. In addition, with the evolution of wireless technology and development of next generation networks such as 5G and 6G, network operators are expected to encounter more complex challenges soon. One such network issue is the Passive Intermodulation (PIM) problem that is observed in both 4G and 5G networks. Although there is a significant body of work regarding PIM detection and cancellation methods, majority of such studies depend on hardware solutions and manual investigation by network engineers, which is costly in terms of time and labor. In this paper, we propose a time-series based anomaly detection method, for identifying PIM problems in network sites. The proposed solution utilizes a set of Key Performance Indicator (KPI) data of base stations, obtained from network management systems for a significantly long time interval, and detects possible PIM problems in a site without the need for a human-in-the-loop. We measure the performance of our solution, with the guidance of experienced network engineers, on our collected dataset.**

I. Introduction

With the constant evolution of wireless technologies, next generation networks such as 5G have become popular and widely used around the globe. As a consequence, mobile network providers are in constant need for increasing the number of their base stations, to provide an adequate network coverage and service quality for all of their customers. However, the increasing number of base stations also implies more labor work for maintaining network sites. Due to complex nature of technology used in these sites, network problems nowadays have also become more complicated compared to those in the past. On top of emerging network problems, older issues that were prominent in 4G networks, such as Passive Intermodulation (PIM), still pose a significant threat to network coverage and signal quality in today's wireless networks.

PIM is a network problem that stems from the nonlinearity of RF antennas or passive network elements such as connectors and cables, and cause serious decrease in signal quality and might even result in connection drops [1]. Such nonlinearity, when caused by a slow degradation of network equipment over time, is called *Internal PIM* [2]. Sometimes, the root cause of the PIM is not the internal components, but an external factor unrelated to the site network itself. This type of PIM, named *External PIM*, can be encountered when there are metallic objects such as a fence or barn roof nearby. Unlike Internal PIM that shows its symptoms slowly over time, External PIM causes sudden drop in signal quality and overall network performance.

Current PIM detection and cancellation methods typically depend on manual work and lead to further operational cost such as artificially loading a Radio Access Network (RAN) cell to identify the problem [3]. Therefore, remote solutions relying on processing of network monitoring data are actively investigated in the technical community. Those schemes may employ a variety of approaches such as machine learning and statistical analysis. In that regard, anomaly detection [4] is promising for PIM detection since PIM emerges as a performance anomaly and thus impacts related network metrics.

Anomaly detection is already a critical component of monitoring and maintaining the performance of mobile networks. The rapid growth in the number of mobile devices and the multiplying complexity of mobile network architectures have made it increasingly difficult to identify and troubleshoot issues in a timely manner. Anomaly detection methods use statistical models and machine learning techniques [5], [6] to automatically identify abnormal behavior in the network, including PIM issues. By detecting anomalies in a timely manner, network operators can take proactive measures to prevent or mitigate problems, improving the overall reliability and performance of the network for end users. As such, anomaly detection is an essential tool for ensuring efficient and secure operation of mobile networks.

In this study, we propose an anomaly detection solution for detecting possible PIM occurrences in RAN. Our solution utilizes a set of Key Performance Indicator (KPI) data, obtained from the site base station in a time-series format. Therefore, the solution does not require manual input for determining when the site starts to display effects of PIM. We measure the performance of our proposal on a collected KPI dataset of base station cells in a region and compare it to a baseline PIM detection technique.

The rest of the paper is organized as follows. In Section II, we discuss the related work on digital solutions for PIM detection in the literature. Section III provides background on

DOI: 10.1109/BalkanCom58402.2023.10167980

anomaly detection techniques and explains our methodology for data collection and preparation. We introduce our proposed time-series anomaly detection model and describe the design details in Section IV. In Section V, we present the performance results of our solution on the collected dataset. We discuss some identified research challenges in Section VI. Finally, Section VII concludes the paper and addresses future work.

II. Related Work

The current research works elaborate on different aspects of the PIM detection problem. A study by Chen et al. [7] focuses on the PIM problem caused by the antenna design, and suggests a method for improving the stability of the PIM in the design phase. Lampu et al. propose a promising model for canceling out specifically air-induced PIM problems [8], which is a special case of the *rusty bolt* PIM issue. Another PIM canceller, specifically targeting PIM problems on frequency-division duplexing (FDD) based 4G and 5G sites, is proposed by Waheed et al. in [9]. The same authors, along with other colleagues, present a detailed compilation of similar PIM cancellation methods in another study [10]. Although these works provide feasible detection mechanisms and solutions for some real-life PIM problems, detection of Internal PIM issues that are caused by gradual degradation of passive components need different approaches. There are already well-established techniques for gradual PIM detection as well, e.g., the Air-Interface Load Generator (AILG) test. Although these tests are highly accurate, generating such load on the network site causes a drop in service quality and, in some cases, even shuts down entire network site, preventing end users from getting service coverage. There is also a logistic cost for this solution, since a network site engineer may be required to visit the site physically to perform the test.

Some studies focus on utilizing Machine Learning (ML) models for detecting PIM problems automatically, without requiring manual labor. One such study by Jochems et al. [11] suggests using a newly developed ML method, called canonical system identification, for cancelling self-interference signals, which include the PIM problem. Mismar et al. propose an ML-based algorithm utilizing supervised learning for detecting PIM problems in Beyond 5G and 6G networks [12]. Another novel ML-based approach is presented by Liang et al. in [13], where a real-time recursion learning neural network is trained for detecting PIM in satellite networks. All of these studies provide accurate and novel approaches for PIM detection. However, they share an implicit assumption that a site either suffers from PIM from the beginning or PIM is never displayed on the site at all. The possibility that a healthy site might develop a PIM problem gradually over time is dismissed.

Anomaly detection techniques on time-series data are also used in some recent work regarding PIM detection. Banerjee et al. propose a forecasting approach using network KPIs and Fourier feature mapping to predict PIM issues in 4G/5G networks [14]. The proposed solution is demonstrated on four different applications, including a time-series forecasting and anomaly detection. A similar approach is adopted by Ranjani et al. in [15], where authors propose an ensemble technique consisting of time-series based ML, utilizing random forest models, and signal processing methods for automatically predicting PIM problems, for 4G and 5G networks sites in real-time. The proposed method also considers the KPIs of neighbor cells while determining whether a cell suffers from PIM, to improve the accuracy of PIM detection.

III. Anomaly Detection Techniques

Anomaly detection refers to identifying rare and unusual events whose characteristics are significantly different from majority of the data and normal behaviour of a procedure. From this regard, PIM problem can be seen as an anomaly in standard RAN operation. Therefore, we formulate PIM detection as an anomaly detection problem in this work.

Anomaly detection, especially for time-series data, is a long-studied topic in various domains in the technical literature [16]. In this work, we consider two anomaly detection techniques where the first one is an established technique serving as the baseline case, namely Isolation Forest, and the second one is our novel approach for PIM detection via time series analysis.

A. Isolation Forest

Many anomaly detection algorithms construct a profile for normal behaviour which serves as a ground truth when deciding whether an event is an *anomaly*. However, Isolation Forest [17] takes a different route to isolate anomalies from normal events where isolation referring to separate an event from the rest. In its core, it takes advantage of anomalies being "few and different" and constructs a tree structure that enables identifying anomalies in its leaves.

Isolation Forest recursively generates partitions on the dataset by randomly selecting a feature and then randomly selecting a split value for that feature. Presumably, the anomalies need fewer random partitions to be isolated compared to normal points in the dataset, so the anomalies will be the points which have a smaller path length in the tree, path length being the number of edges traversed from the root node.

In the following, we provide step-by-step procedure of an Isolation Tree construction:

1) Given a dataset, a random sub-sample of the data is selected and assigned to a binary tree.
2) Branching of the tree starts by selecting a random feature of the input. Then, branching is applied on a randomly determined threshold value of the selected feature.
3) If the value of an input is less than the selected threshold, it goes to the left branch, else to the right.
4) This process is continued until each data point is completely isolated or maximum depth threshold is reached.

The foregoing steps are repeated to construct a number of random binary trees (i.e., a forest). After an ensemble of trees is created, model training is complete. During scoring, a data point is traversed through all the trees which were trained earlier. An 'anomaly score' is assigned based on the depth of the node that the data point reaches. The overall score is an

DOI: 10.1109/BalkanCom58402.2023.10167980

aggregation of the depth obtained from each of the trees in the trained model.

B. Temporal Analysis Based Anomaly Detection (TABAD)

We propose an anomaly detection technique that suits better for time series data in PIM use case. According to this technique, we analyze characteristics of previous data collected over time and compare current events against them. Isolation Forest handles data as separate and independent data points which includes anomalies of a certain ratio. In contrast, we consider a stream of data in which we check whether the current data behaves like an anomaly based on previous data. For this reason, we call our technique temporal analysis based anomaly detection (TABAD). We follow this approach, because even a completely healthy network site displays a considerable amount of variation in its KPI data, depending on the day and the hour of the measurement, or on the occurrence of a special occasion near the site. Therefore, we believe that considering a stream of past KPI data, while investigating a new data point, is necessary to make a healthier detection.

Algorithm 1: TABAD algorithm

Input: $hist, prb$: time-series like data
Output: $true$: anomaly, $false$: normal
Function *tabad(hist, prb: Array) : bool*
  $histIntr \leftarrow splitTimeIntervals(hist)$;
  $histChrc \leftarrow getChrcIndicators(histIntr)$;
  $baseAvg, baseVar \leftarrow normal(histChrc)$;
  $prbChrc \leftarrow getChrcIndicators(prb)$;
  return $ZTest(prbChrc, baseAvg, baseVar)$

We further divide the historical data into time intervals such as daily, weekly or monthly based on periodic characteristics of the time series data. For example, KPI signals retrieved from a downtown location completes a cycle in a week where the load is higher in weekdays and lower at weekends. This is more useful than considering each data point separately as it provides a more complete information regarding normal operation. In our proposed technique, we consider mean and variance of a KPI signal within a time interval as characteristics and we assume that those characteristic values normally distributes over the history. We check whether the current time interval's characteristic indicators come from this normal distribution to examine if it presents an anomaly.

Algorithm 1 outlines core steps of our approach. It takes an array of historical data that will be used to form a base for normal operation and another array of data which is under examination. The function starts with splitting the historical data into time intervals and inferring characteristics for each time interval of historical data. In the next step, we find the mean and the variance of calculated characteristics, which lets us define a normal data distribution establishing a ground truth for normal operation. Subsequently, we calculate characteristics of the data under examination and apply statistical test that checks whether given data is coming from the given distribution or not. The outcome of this test is simply the output of the function.

IV. Anomaly-Based PIM Detection via RAN KPIs

For real-world PIM detection, we assume that real time streaming KPI data is available and consider a 4G LTE network. In principle, our approach is applicable to every individual KPI, however, in this work, we primarily investigate the changes in KPIs related to the RSSI (Received Signal Strength Indicator) of interference in the UL (Uplink) channels, PUCCH (Physical Uplink Control Channel) and PUSCH (Physical Uplink Shared Channel). We primarily choose these two KPIs based on the opinions of expert network engineers who specialize in PIM detection. In addition, a recent patent work regarding remote PIM detection utilizes these KPIs as well [18].

Figure 1 illustrates our general PIM detection scheme using TABAD. According to this, our system monitors streaming KPIs in real time and checks whether the values in current window present an anomaly or not. Our design allows monitoring multiple KPIs simultaneously and but decision is made separately for each KPI. Decisions for different KPIs can be aggregated in several ways. It is a new research problem on its own and requires careful analysis. In this work, we apply simple voting among multiple decisions.

We instantiate TABAD in two ways. In the first one, we choose characteristic indicator as mean value and in the second one we select it as variance. Both mean and variance are relevant indicators for different KPIs. For example, for PUCCH based KPIs mean value usually increases in cells with any PIM issue. For some other KPI, PIM might affect the variance rather than the mean value. We start with finding mean (or variance) of the KPI values collected over current time window of one-week duration. We also find mean (or variance) of values collected over previous weeks. We assume that those mean (or variation) values follow a normal distribution and we check whether the current week's mean (or variation) is drawn from that distribution.

A. Effects of Hyper-Parameters

TABAD approach utilizes the following three hyper-parameters:

- History Size (HS)
- Window Under Investigation (WUI)
- Flag Level Threshold (FLT)

HS determines the amount of past KPI data (in days) the algorithm considers when predicting anomaly. For instance, if *HS* is 10, the algorithm will use the KPI data of past 10 days, to decide whether the site currently suffers from a PIM problem. Increasing *HS* is likely, though not guaranteed, to increase the accuracy of the predictions. However, keeping it too long might result in missing latest trends in the data.

WUI tells the algorithm to treat a certain amount of KPI data (in days) as a whole, such that the algorithm considers this entire batch at once while determining whether there is a PIM problem. For instance, if *WUI* is 7, the algorithm considers the KPI data for the next 7 days, and either marks the entire 7 days as anomaly or does not mark any of these days. The most

DOI: 10.1109/BalkanCom58402.2023.10167980

effective way of choosing WUI is to determine the periodic behaviour of the KPI signal (e.g., weekly cyclic behavior).

The last hyper-parameter is basically the threshold value for the anomaly decision. TABAD algorithm determines that a KPI should only be marked as an anomaly if the probability of this KPI value appearing on a healthy site is less than the value defined by this threshold. Decreasing *FLT* makes the algorithm more conservative for predictions, thus decreasing the false PIM alarms but increases the potential misses. On the contrast, increasing *FLT* value makes the process more sensitive, increasing the correct predictions, but also causes more false alarms. We consider two levels of threshold for **red flag** and **orange flag**. Red flag alarms are more strict, thus indicate a *major* PIM problem, whereas orange flag alarms are less strict and indicate a *minor* PIM problem.

Algorithm 2: Anomaly Alarm Decision

Input: $zScore : prob., fltRed : prob., fltOrange : prob.$

Output: $major$: Major PIM, $minor$: Minor PIM, $none$: No PIM

Function *decidePIMAlarm(zScore: float, fltRed: float, fltOrange: float)* → *pimAlarm: string*

```
pimAlarm ← null;
if zScore <= fltRed then
    pimAlarm ← "major";
else if fltRed < zScore <= fltOrange then
    pimAlarm ← "minor";
else
    pimAlarm ← "none";
return pimAlarm
```

Due to the gradual progression of PIM problems, the major PIM issues occur less frequently than minor ones. Therefore, we always have a lower threshold level for red alarms compared to orange alarms. If the gap between two threshold levels widens, the number of minor PIM alarm increases. On the other hand, if this gap narrows, the number of minor PIM alarms decreases. The reason is that, only the KPI values that fall between the two threshold levels trigger a minor PIM alarm, as one can deduce from Algorithm 2. Consequently, both red *FLT* and orange *FLT* affect the number of minor PIM alarms, whereas major PIM alarms are not affected by orange *FLT* at all. During the simulation phase, we only consider red flags, as an attempt to keep the evaluation simpler. Therefore, the term *FLT* hereafter refers to the red *FLT*.

V. Evaluation

A. Benchmark

We have collected KPI values of 37 4G RAN cells over a 18 months period. Our aggregated data contains more than 40 KPIs. However, in this work we consider PUCCH and PUSCH based KPIs as noted in Section IV. Although our data set contains relatively a small number of cells in a zone, they were monitored over a very long period. This is necessary because PIM usually occurs over such long periods of time.

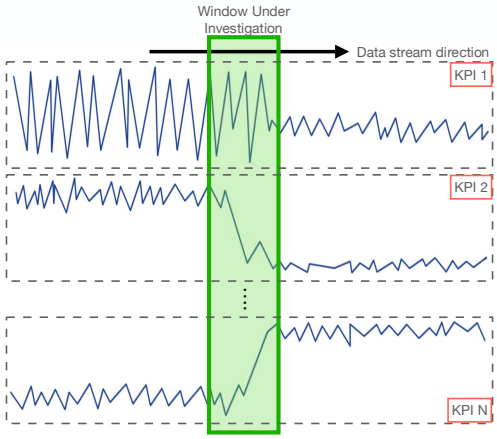

Fig. 1: Real time PIM analysis with TABAD.

All of our 37 cells are known to have PIM problem at some point within these 18 months. In addition to this, these cells were physically visited by field teams to fix their PIM problem after its occurrence as part of RAN maintenance work.

B. Experimental Design

Unfortunately, it is not always possible to identify at which point PIM emerges exactly even with expert view from maintenance teams with comprehensive hands-on experience. On the other hand, we have cell visit time information that corresponds to the point where PIM is fixed. Our history-based anomaly detection technique is sensitive to any change irregardless of PIM occurrence or PIM fix. For this reason, we consider visit dates as ground truth anomalies (i.e., PIM fix events) and we check whether our technique can identify them or not. We report True Positive (TP), False negative (FN), precision and recall as performance metrics.

C. Results

In this section we present our quantitative and qualitative findings for the following research questions:

1) **Performance:** *What is the performance of our algorithm in detecting anomalies in KPI signals?*
2) **Comparison:** *How well does our algorithm perform compared to a baseline anomaly detection method?*
3) **Hyperparameters:** *How does the performance of our algorithm get affected by changes in hyper-parameters (i.e., configuration)?*

1) RQ1 - Performance: For our study, as described in Section V-A, the expert RAN engineers from the field teams provided us a data set of 37 network sites, which used to suffer from a PIM problem before a site visit. According to the explanation by experts, 25 of these sites show improvements on their KPIs after a site visit. However, 12 of them do not display an apparent change in their KPIs due to being located in a sparsely populated area, hence receiving low traffic demand all the time. Therefore, we are advised to exclude these 12 sites from our experiment, to avoid having corrupted/biased data impacting the results.

DOI: 10.1109/BalkanCom58402.2023.10167980

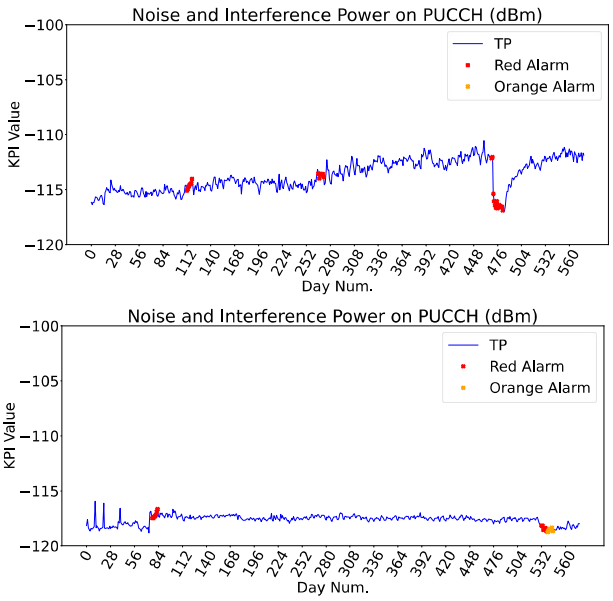

Fig. 2: TABAD method marks anomalies in PUCCH signals in two different cells. Experts confirm that the first mark corresponds to the point where PIM starts. Also, the last mark is where the PIM is solved by field teams.

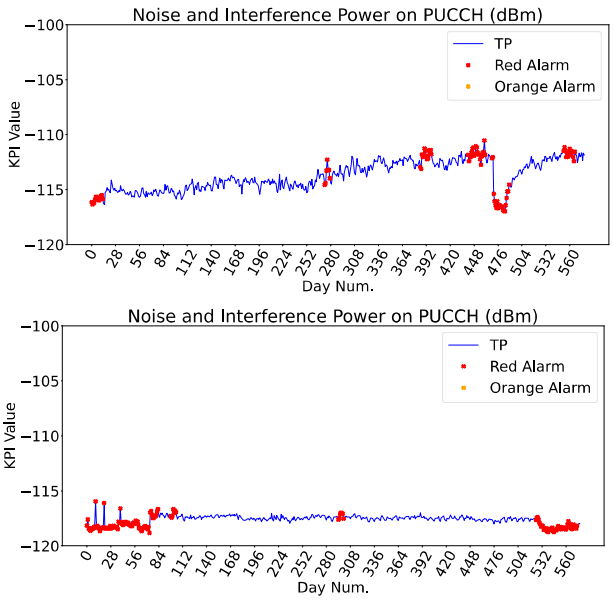

Fig. 3: Isolation Forest anomaly detection method marks anomalies in PUCCH signals in two different cells. It marks a lot of unrelated points in addition to the correct anomaly points which greatly reduces its practical usage.

TABLE I: Performance Metrics

	Isolation Forest	TABAD
Precision	< 0.05	0.33
Recall	0.56	0.80

We measure the performance of our method by checking whether an abnormal change occurs right after a site visit. We consider an alarm raised right after that visit an anomaly detection. If there are any other alarms besides the site visit date, it is considered a false alarm. Similarly, if the algorithm misses the alarm at the visit date, it is considered a false negative.

Based on the simulation results conducted for 25 network cells, our method correctly identifies 20 of the 25 site visits, while 5 of site visits are missed. Therefore, we have 20 true positives and 5 false negatives. On the other hand, our method triggers 40 false alarms irrelevant to site visit dates. Computing true negatives in this setup is a tricky task, because the data is almost always considered normal except the site visit date. Therefore, we omit this metric here. Using the formulas, our approach achieves a recall of 80% and a precision of 33.3% precision.

2) RQ2 - Comparison: When we simulate the same setup with Isolation Forest method, we obtain 14 correctly identified and 11 missed sites, which has a recall of 56%. However, Isolation Forest produces more than 300 false alarms for the tested 25 sites. Therefore, the precision value of the method is less than 5%. One can observe from the results displayed in Table I that our method performs significantly better for both precision and recall compared to the Isolation Forest method.

3) RQ3 - Hyperparameters: During our simulation, we used various values for our hyper-parameters, *HS*, *WUI* and *FLT*. After a parameter space search via multiple trials, we observe that our algorithm performs best when the hyper-parameters are set to values provided in Table II. These values achieve a precision of 33% and a recall of 80%, as mentioned before.

TABLE II: Optimal Values for Hyper-Parameters

Hyper-Parameter	Optimal Value
HS	10 weeks
WUI	1 week
FLT	0.01

When we increase the value of *HS*, we observe that the number of false positives decreases significantly, at the expense of increasing false negatives. Surprisingly, using a *HS* value lower than the optimum causes an increase in both false positives and false negatives. Examples of different *HS* values are given in Table III, along with corresponding performance results, where other hyper-parameters are set to their optimum values.

When we use a *WUI* higher than the optimum value, the number of false negatives increases while the number of false positives decreases in a drastic manner. Using a *WUI* lower than the optimum value, increases both false negatives and false positives. A pair of different *WUI* values and the resulting performance results are given in Table IV. Again, other hyper-parameters are set to their optimum values during

TABLE III: Different Values for Hyper-Parameter HS

HS Value	TP	FN	FP	Precision	Recall
5 weeks	12	13	120	0.09	0.48
15 weeks	8	17	20	0.28	0.32

DOI: 10.1109/BalkanCom58402.2023.10167980

TABLE IV: Different Values for Hyper-Parameter WUI

WUI Value	TP	FN	FP	Precision	Recall
3 days	14	11	150	0.08	0.56
2 weeks	12	13	10	0.54	0.48

TABLE V: Different Values for Hyper-Parameter FLT

FLT Value	TP	FN	FP	Precision	Recall
0.005	13	12	30	0.30	0.52
0.025	21	4	60	0.26	0.84

these experiments.

Since *FLT* parameter directly acts as a threshold, we expect an increase in false negatives and a decrease in false positives when *FLT* becomes more strict. Similarly, when *FLT* is loosened, an increase in false positives and a decrease in false negatives is expected. The results of our trials suggest that our expectations are correct, as one can observe from Table V, where other hyper-parameters are set to their optimum values.

VI. Discussion and Research Challenges

PIM analysis and detection via remote and data analytics based techniques is a multifaceted research problem. In our investigation, we have run into various challenges regarding the data collection and analysis aspects for PIM detection, which we highlight in this section:

– Data Dimension: Data collection for PIM detection is a labor-intensive and human-driven process. Considering the data composition, the collected datasets typically contain more non-PIM sites than PIM sites, thus creating a bias for non-PIM sites, which results in more false negatives. We have exploited the expert provided knowledge and PIM labeling to address these challenges to the extent possible. Moreover, not every obtained dataset contains the same set of KPIs (i.e., features) for the monitored cells. We have addressed this issue via using an offline data pipeline where the experiments are run on stored but time labelled data.

– Selection of right performance metrics: Although, other metrics, e.g., F1 score, may be better to quantify the detection performance, we have adopted Precision and Recall since they are widely used in the literature and more convenient for comparison with existing works.

VII. Conclusion

In this work, we have proposed a novel PIM detection technique based on anomaly detection and compared it to a baseline method. The proposed approach was tested on a KPI data set collected over a long time period from operational cells. The experimental results show that our approach has high performance in terms of Precision and Recall metrics and outperforms the baseline approach. The main challenges including data dimensioning, data gathering and performance metrics were also identified in Section VI.

Future research includes the testing of our techniques with a more comprehensive data set, in terms of time and cell coverage. Another important research direction is the investigation of additional ML techniques for PIM detection purposes.

Acknowledgment

The authors would like to thank H. Ferit Eniser from MPI-SWS, Germany for his valuable comments and insights.

References

[1] Z. Cai, L. Liu, F. de Paulis, and Y. Qi, "Passive intermodulation measurement: Challenges and solutions," *Engineering*, vol. 14, pp. 181–191, 2022.

[2] YUPANA Inc., "Passive inter-modulation sources and cancellation methods." https://yupanatech.com/media/uploads/PIM_YUPANA.pdf, 2022. YUPANA White Paper.

[3] H. M. Karaca, "Passive inter-modulation sources and cancellation methods," *The European Journal of Research and Development*, vol. 2, p. 75–91, Jun. 2022.

[4] G. Muruti, F. A. Rahim, and Z.-A. bin Ibrahim, "A survey on anomalies detection techniques and measurement methods," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, pp. 81–86, 2018.

[5] A. Toshniwal, K. Mahesh, and R. Jayashree, "Overview of anomaly detection techniques in machine learning," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 808–815, 2020.

[6] S. Wang, J. F. Balarezo Serrano, K. Sithamparanathan, A. Al-Hourani, K. Gomez Chavez, and B. Rubinstein, "Machine learning in network anomaly detection: A survey," *IEEE Access*, vol. PP, pp. 1–1, 11 2021.

[7] C. Chen and Y. Gu, "A mechanical modelling and simulation method for resolving PIM problems in antennas," *Sensors*, vol. 22, no. 1, 2022.

[8] V. Lampu, L. Anttila, M. Turunen, M. Fleischer, J. Hellmann, and M. Valkama, "Air-induced passive intermodulation in FDD networks: Modeling, cancellation and measurements," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*, pp. 983–988, 2021.

[9] M. Z. Waheed, D. Korpi, A. Kiayani, L. Anttila, and M. Valkama, "Digital cancellation of passive intermodulation: Method, complexity and measurements," in *2019 IEEE MTT-S International Microwave Conference on Hardware and Systems for 5G and Beyond (IMC-5G)*, pp. 1–3, 2019.

[10] M. Z. Waheed, D. Korpi, L. Anttila, A. Kiayani, M. Kosunen, K. Stadius, P. P. Campo, M. Turunen, M. Allén, J. Ryynänen, and M. Valkama, "Passive intermodulation in simultaneous transmit–receive systems: Modeling and digital cancellation methods," *IEEE Transactions on Microwave Theory and Techniques*, vol. 68, no. 9, pp. 3633–3652, 2020.

[11] F. Jochems and A. Balatsoukas-Stimming, "Non-linear self-interference cancellation via tensor completion," *arXiv e-prints*, p. arXiv:2010.01868, Oct. 2020.

[12] F. B. Mismar, "Intermodulation interference detection in 6G networks: A machine learning approach," *arXiv e-prints*, p. arXiv:2111.00524, Oct. 2021.

[13] B. Liang, X. Bu, M. Li, P. Guo, and C. Liu, "A novel RTRLNN model for passive intermodulation cancellation in satellite communications," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 18–23, 2018.

[14] S. Banerjee, R. R. Martin, and A. Pardo, "Frequency-aware time series forecasting, anomaly detection, classification and granger causality," in *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 217–221, 2022.

[15] H. Ranjani, S. P. Puthennurakel, A. Brisebois, S. Banerjee, and V. Umaashankar, "Time series based approach for detecting passive intermodulation occurrences in cellular network," in *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 630–638, 2022.

[16] A. Blázquez-García, A. Conde, U. Mori, and J. A. Lozano, "A review on outlier/anomaly detection in time series data," *ACM Comput. Surv.*, vol. 54, apr 2021.

[17] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *International Conference on Data Mining*, pp. 413–422, 2008.

[18] H. Evircan, E. K. Ulusoy, and M. M. Dalan, "*Remote Detection and Analysis of Passive Intermodulation Problems in Radio Base Stations*." US10009784, Jun 26, 2018, https://patentscope.wipo.int/search/en/detail.jsf?docId=US221793731, Accessed on: May 5, 2023.

DOI: 10.1109/BalkanCom58402.2023.10167980