Accepted for presentation in: IEEE International Symposium on Measurements and Networking (M&N), Rome, Italy, July 2024

AI-based Anomaly Detection for Industrial 5G Networks by Distributed SDR Measurements

Kevin-Ismet Šabanović, Christian Arendt, Steffen Fricke, Melina Geis, Stefan Böcker and Christian Wietfeld
Communication Networks Institute, TU Dortmund University, 44227 Dortmund, Germany
e-mail: {Kevin.Sabanovic, Christian.Arendt, Steffen.Fricke, Melina.Geis, Stefan.Boecker, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—The analysis of the physical layer in the frequency spectrum is subject to vigorous research in the last couple of years. From localization tasks to anomaly detection, the research is starting to incorporate more artificial intelligence-based solutions. In case of anomaly detection, the looming problem is that there are many different and unquantifiable types of anomalous effects. Hence trying to find a model that predicts anomaly itself is not feasible. Therefore, we propose an approach of successfully detecting all known signals in a given signal range, which implicitly leads to finding possible anomalies. This is done by collecting Power Spectral Density waterfall diagrams and segmenting them with a Convolutional Neural Network named U-Net. The results are compared against a knowledge base of the scanned bandwidth and an informed decision on the validity of the observed signal is made. We are able to provide a working concept for the distributed monitoring and stress test system STING for detecting anomalies in private 5G networks. The system is able to achieve an accuracy up to 90%, while providing a false negative rate of 2.37%. We aim to supply full coverage of a given industrial workplace, through the distribution of software defined radios over the STING-system itself and thus are able to detect anomalies over the complete industrial facility in the future.**

***Index Terms*—Anomaly Detection, Convolutional Neural Network (CNN), Software Defined Radio (SDR), 5G**

I. Introduction

With the increasing usage of private mobile and traditional wireless networks in industrial settings [1], detection of unwanted or malicious activity, such as wrongly tuned, overlapping networks or accidentally produced signals that interfere with the used infrastructure, is needed to guarantee a frictionless work environment. Due to the possible freedom in deployment, there has to be a flexible form of detection. While Key Performance Indicators (KPIs) like throughput and latency can give good insights into a given network on a higher level, they can not provide identification of the root cause of potential problems. In contrast, for example a Software Defined Radio (SDR) can be used to analyze a given frequency range on the physical layer [2]. Granted that the SDR is sufficiently sensitive enough, every external anomaly or a signal disrupting worker can be recorded. Additionally, different types of communication technologies provide distinct and recognizable signatures.

The overarching problem is that being able to recognize every possible anomaly is not practically possible. This leads to suggesting the inverse approach: If a system is able to detect every known distinct signal, which are then excluded from the detection, all remaining found signals by the system are expected to be anomalous.

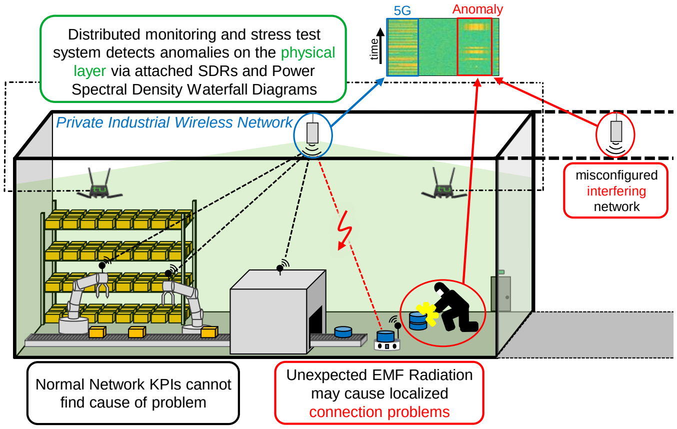
5G
Anomaly
time
Distributed monitoring and stress test system detects anomalies on the physical layer via attached SDRs and Power Spectral Density Waterfall Diagrams
Private Industrial Wireless Network
misconfigured interfering network
Normal Network KPIs cannot find cause of problem
Unexpected EMF Radiation may cause localized connection problems

Fig. 1. System implementation inside a production setting with present electromagnetic interference caused by a welding process. A nearby STING with installed SDR detects the interference and reports the anomaly.

In this paper, we propose an SDR-supported system, which is able to periodically scan the environment in a production facility and detect anomalies. This approach is added to the *Spatially distributed Traffic and Interference Generation (STING)* system, as depicted in Fig. 1. STING is a decentralized system enabling technology independent, systematic network performance testing and monitoring introduced in [3] and [4]. In our approach, learning to detect a given technology signature like 5G is accomplished using an image-based Neural Network structure called U-Net [5]. This CNN is used to discern patterns within a given matrix, which are in this case Power Spectral Density (PSD) waterfall diagrams. However, to achieve comprehensive signal recognition, the model necessitates exposure to all possible signature that may appear in a given communication network. Therefore, an online learning process with live networks is imperative to generate all potential signals per given type. As a proof of concept, experiments involving a single worker within a 5G network were conducted, focusing on a bandwidth of 50 MHz centered around 3.775 GHz.

The remainder of the paper is structured as follows. After discussing the related work in Sec. II, the integration into the STING-system is presented in Sec. III, as well as the collection of data, the training of the CNN the and detection workflow. Afterwards, detailed results are provided and discussed in Sec. IV before a conclusion is drawn in Sec. V.

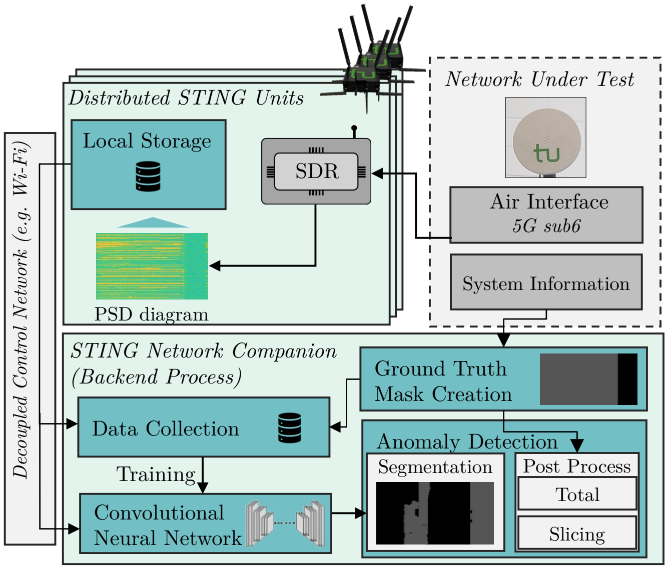

Fig. 2. STING-system with integrated SDR-STING units for data collection as PSD waterfall diagrams used centralized in Training. Anomaly detection is performed in the backend with the *Ground Truth* mask, created from known system information and a *Segmentation* produced from the CNN.

II. Related Work

The detection of anomalies has become increasingly important in recent years. While an anomaly can appear in many different ways and research fields, the need of early and reliable detection is often the biggest priority for the user. How an anomaly might manifest is highly dependent on the underlying type of data that is supplied. The authors in [6] describe their data as series of multi-modal sensory output. They convert this data into a spectrogram and utilize a CNN for the feature extraction and an auto-encoder to translate those into a user readable output. Several papers have recently been published on spectrum sensing, which are outlined and compared in [7]. The combination of so-called cognitive radios and deep learning is able to dynamically allocate the wireless spectrum. Therefore, different deep learning strategies are discussed to provide an overview over the current research in this field. The use of Machine Learning (ML) in the detection of signals is steadily increasing, as shown in [8]. The authors use an SDR-based approach called DeepSweep to sweep over a given frequency range and are able to recognize and sense signals of the wireless spectrum. They implement ML in the form of a CNN to identify signals like 5G or Wi-Fi with a high accuracy in real-time. [9] introduces an anomaly detection system for Software-defined Networking (SDN), which combines Security Information and Event Management (SIEM) with ML. They discuss the performance of various ML algorithms and show that they accurately categorize network traffic to identify anomalies or dynamically adapt to different scenarios. [10] presents a recurrent neural network-based method for detecting radio anomalies, enhancing anomaly detection in complex radio bands. By using Long Short-Term Memory (LSTM) networks, it accurately predicts radio signal behavior and effectively identifies anomalies across different communication bands. The system's performance demonstrates its potential for applications in spectrum monitoring and communications security. [11] uses an adversarial autoencoder (AAE)-based anomaly detector for wireless spectrum, achieving over 80% accuracy in identifying anomalies with a 1% false alarm rate. While providing real-time analysis of potential anomalies, it is also able to identify signal characteristics in a semi-supervised fashion and provides compression of PSD data.

Compared to the mentioned methods for anomaly detection that use, for example, multi-modal data or methods specialized for signal processing, our approach utilizes a well-established, general-purpose model validated in fields such as medicine. We chose to use real signal data for training and validation to ensure applicability in real-world environments. Additionally, our system can be integrated into the distributed monitoring framework (STING) to ensure comprehensive coverage of industrial facilities. By comparing segmented results against a predefined knowledge base, we enhance the reliability of anomaly detection in private 5G networks. This strategy not only achieves high accuracy but also ensures robust detection of anomalies across industrial facilities, providing a flexible and scalable solution tailored to the needs of modern industrial settings.

III. Anomaly Detection Approach

Our approach uses SDRs to sense wireless signals and implements deep learning in the from of a CNN to classify 5G signals similar to [8]. Additionally, we employ post-processing in order to compare the CNN output with a target status and report anomalies based on their difference. The underlying system architecture is shown in Fig. 2. As a prerequisite for implementing anomaly detection in the STING-system, every STING unit is required to have an integrated SDR. Due to the existing workload of each STING, the detection itself is

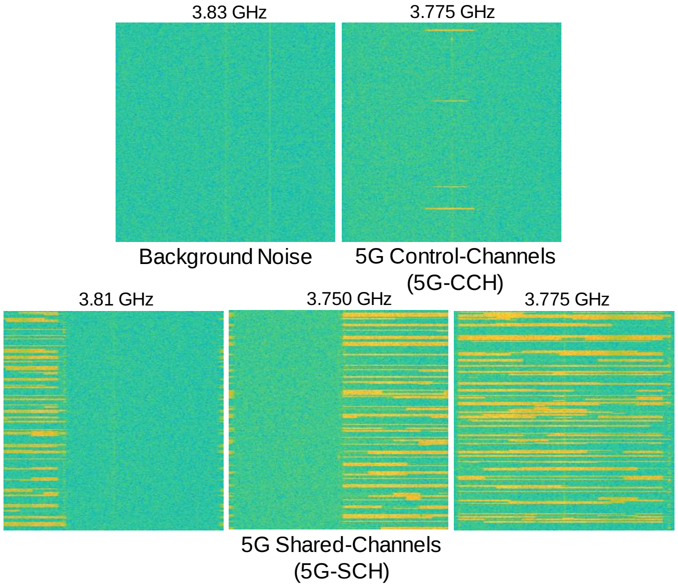

Fig. 3. Snapshots of PSD waterfall diagram of the training data, for each image type. 5G-DC includes a 50 MHz wide 5G active communication channel at differing center frequencies.

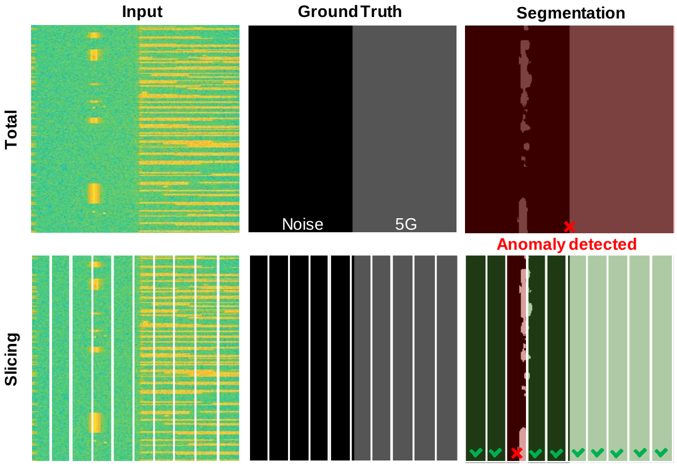

Fig. 4. Comparison between Ground Truth and Segmentation images resulting in anomaly detection with two different strategies. An anomaly is detected if a chosen pixel difference threshold is surpassed.

carried out on the centralized STING Network Companion. This server is able to analyze the incoming PSD waterfall diagrams from each STING and report a possible anomaly via the integrated GUI. Each part of the detection system is detailed below, starting with the data acquisition.

A. Reference Signal Data Collection

An *Ettus USRP B205mini-i* was utilized to collect training and test data. The setup involved an active private 5G network at a carrier frequency of 3.775 GHz and a bandwidth of 50 MHz with one User Equipment (UE) attached. Data collection occurred during either active communication (5G-Shared-Channels) or passive signaling channels (5G-Control-Channels). Samples were collected at a constant distance between the SDR, cell, and UE. IQ samples with 10,000 values and a sample rate of 50 MHz were collected, resulting in a bandwidth of 50 MHz and converted into a PSD via Fast Fourier Transformation (FFT) and collected over 256 ms to create a waterfall diagram. This was done with a lightweight custom software created for the mentioned SDR. For each waterfall diagram, a segmentation mask was generated. A mask consists of a matrix where each pixel is assigned a value: 0 for background noise and 1 for the 5G signal. Each mask is able to be created automatically due to the information presented by the private network. The center frequency as well as the bandwidth of the deployed 5G network are known at all times and can therefore be labeled in a given mask. 2,000 data pairs were collected with a diverse range of center frequencies containing active or passive 5G signals, as well as samples with no signal present, as visible in Fig. 3.

B. Segmentation Training

It was decided to use a CNN following the U-Net structure [5] because of its great success in medical applications and proven ability in diverse fields of research. PyTorch was used for the implementation and the initial learning rate was set to 0.0005. The ADAM optimizer was used and the CrossEntropyLoss was selected as loss function. The

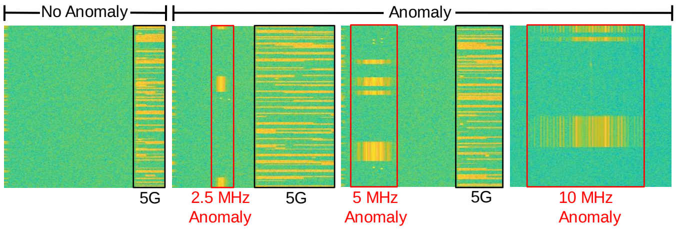

Fig. 5. Sample images of evaluation dataset. One sample without anomaly and three sinusoid anomalies with different bandwidths.

data collected in subsection III-A is split randomly in an 80/20 distribution for training and validation. Because of the similarity of background noise and 5G Control-Channels (5G-CCH) images (Fig. 3), two different models are trained: one with and one without 5G-CCH (see Fig. 7). Due to the similarity of the input data, the risk of overfitting increases, therefore augmentation is introduced to increase the robustness of the network. The images are randomly cropped and flipped 50% of the time to reduce the change of overfitting. For the same reason, early stopping is implemented in the form of a learning rate scheduler named ReduceLROnPlateau in case of a stagnating learning rate. In subsection IV-A, the results of the training are discussed.

C. Anomaly Detection Workflow

When a PSD waterfall diagram is sent to the server, the images are segmented by the CNN. Additionally, the current system information (see Fig. 2), namely bandwidth and center frequency, is gathered and used to create a *Ground Truth* mask of where the network should be located in a given image. The *Segmentation* is then compared against the *Ground Truth* (see Fig. 4). The next step is to decide whether there is an anomaly present. For this purpose, the following two comparison strategies are considered:

1) **Total**: Calculating the percentage of differing pixels over the full image. Example Fig. 4: In order to detect an anomaly a pixel difference threshold of 2.5% is needed.

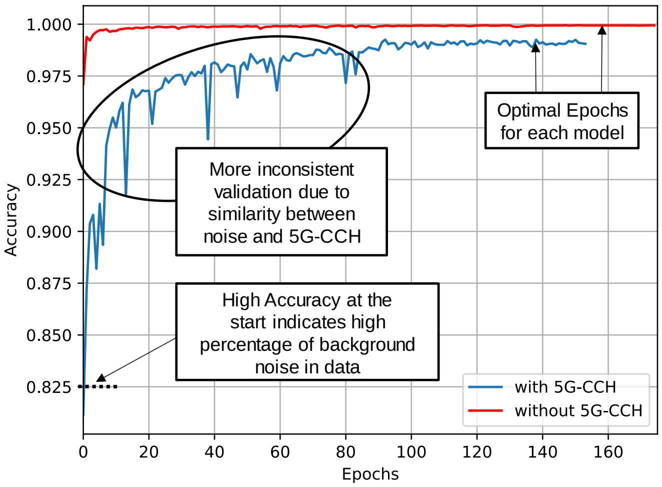

Fig. 6. Validation performance of the Segmentation Algorithm over the number of epochs with 5G-CCH (red) and without 5G-CCH (blue).

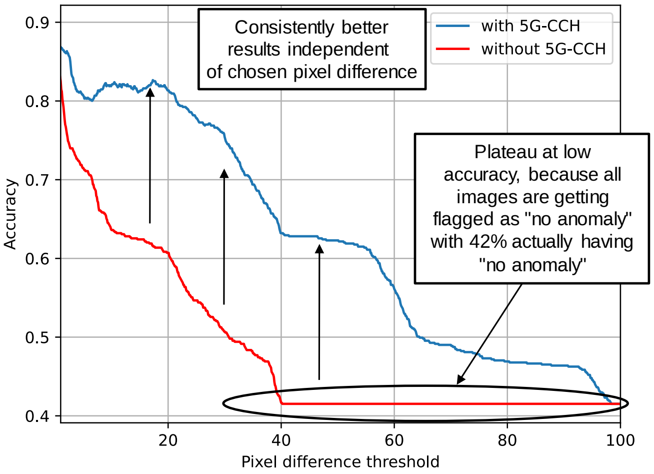

Fig. 7. Comparison of both trained models, over all possible pixel differences (Red: Model with 5G-CC, Blue: Model without 5G-CC)

2) **Slicing**: Splitting the image into multiple slices and calculating the pixel difference for each slice. Example Fig. 4: For the detection o an anomaly, a pixel difference threshold of 20% for at least one slice in required.

In the case of **Total**, an anomaly is detected if the pixel difference percentage for the image is exceeding a chosen threshold. For **Slicing**, every slice is checked for an anomaly, and as soon as one slice has a pixel difference too high, an anomaly is reported. This ensures that smaller differences in pixels are not overshadowed by big areas that do not contain an anomaly. It has to be noted, that the pixel difference threshold also needs to be optimized, which is explored in IV-C.

IV. Detection Precision Results

A test dataset was created for the evaluation, consisting of 800 images of three different synthetic anomaly types, each with its own bandwidth and random pattern. These anomalies are positioned at random frequencies, while the 5G cell remains at the same position in the spectrum for this test. The SDR collected images at different center frequencies. Samples of the resulting dataset can be seen in Fig. 5. The first step is to compare the different trained models with each other to decide which model is more suitable for the remaining evaluation. Next, the optimal number of slices for **Slicing** is presented and lastly the two post-processing algorithms are discussed, the optimal pixel difference percentage is shown and evaluated.

A. Convolutional Neural Network Segmentation Quality

Fig. 6 shows the validation accuracy, calculated as the number of correct divided pixels by the total count of pixels. The model without 5G-CCH (red) reached 99.94% at epoch 160 and 99.05% at epoch 143 with 5G-CCH (blue). Both models stopped early due to the implemented minimum learning rate. To decide which model performs better, a brute force approach is used over all possible pixel difference percentages with the complete processing method. Both models start at a relatively high accuracy, indicating that the training data has a high amount of default labels, in this case background noise without a present 5G signal. The high amount of background noise in each evaluation's images leads to this high initial accuracy. Additionally, the more inconsistent validation accuracy during training for the model with 5G-CCH suggests that the similarity of background noise and 5G-CCH images, as apparent in Fig. 3, has a noticeable effect. Still the model, as seen in Fig. 7, is outperforming the model without 5G-CCH at every possible pixel difference threshold. This means that the additional image type helped the network with generalization, resulting in better performance on the evaluation set. The other model plateaus at approximately 42% accuracy. This is due to the number of ”no anomaly” samples in the evaluation dataset. At a threshold of 40% pixel differences, almost all evaluation images are getting labeled as ”no anomaly”, which is displayed as the mentioned plateau. Therefore, only the model with signaling is used in the rest of the evaluation. In the following section at first the quality of both CNN models on the validation and evaluation dataset is explored. Then the differences of the two post-processing algorithms and their optimization are displayed. Lastly the detection results are discussed.

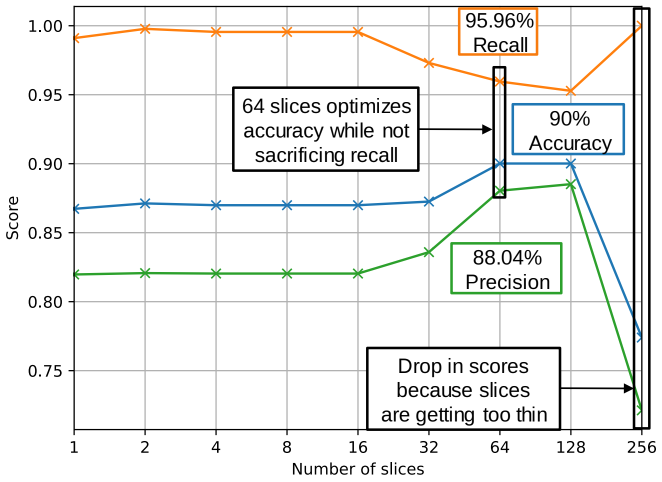

Fig. 8. For the **Slicing** approach the number of slices has to be optimized to maximize accuracy, recall and precision.

B. Post-processing

Two different types of post-processing procedures are explored. The first procedure focuses on full pixel error, which measures the percentage of correctly masked pixels over the full images. The second procedure is similar to the first one, but it splits the analysis into vertical slices, facilitating a more differentiated analysis. Optimization was performed initially on accuracy and then on recall. Accuracy denotes the number of correct predictions, while recall represents the number of true positives out of all positive predictions, thereby minimizing false negatives. The slicing approach required optimization for the number of slices, which was done through brute force as seen in Fig. 8. For this test setup the optimal number of slices is 64. The drop in performance at 256 slices is because each individual slice is getting too thin for a consistent analysis. However, it is important to note that this

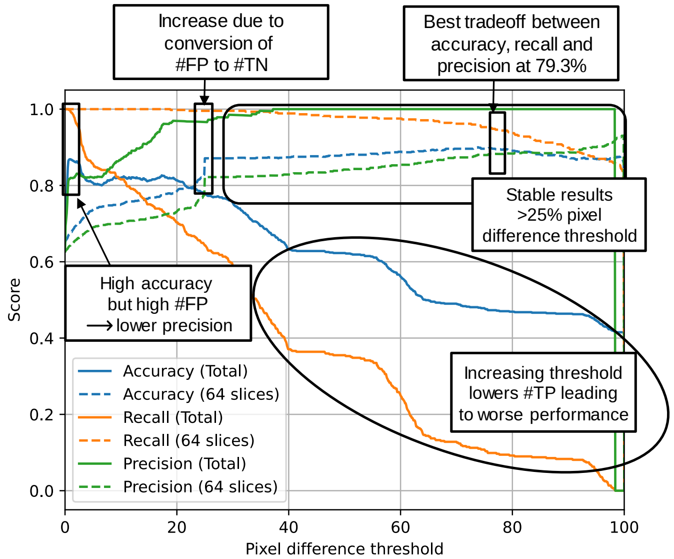

Fig. 9. Comparison of **Total** and **Slicing**. Analyzed by accuracy, recall and precision over all possible pixel differences

optimal value may vary with different types of anomalies in a real environment. The optimized number of slices results in a bandwidth per slice of approximately half of the smallest anomaly band (1.25 MHz) in Fig. 5. Furthermore, there is no positive impact in making even smaller slices, as seen in Fig. 8. To ensure optimal performance for each algorithms, the pixel difference percentage needs to be optimized as well.

C. Evaluation

Fig. 9 presents an analysis of all possible thresholds for both methods and their accuracy, recall and precision values. Intuitively, the accuracy is higher at smaller thresholds for **Total** due to large portions of the masks being identical. This results in a high peak at the beginning, due to the high number of false positives, which can be seen in the relatively low precision value. As the threshold is increasing, the number of false negatives is rising steadily, which leads to a decrease in overall accuracy compared to the slicing approach. The precision converges to 1 due to the fact, that after a threshold of approximately 40%, no test case is getting labeled as ”anomaly”, which results in no false and true positives.

The 64-slicing on the other hand starts to overtake at approximately 25% of differing pixels. The jump in accuracy and precision is due to the ”no anomaly” data, which have a mean pixel difference percentage of under 25%. This leads to a high number of data being converted from false positive to true negative. **Slicing** consistently outperforms **Total** after that threshold and the accuracy is very consistent. This implies that even a not perfectly optimized pixel difference threshold can lead to acceptable detection result using this approach. For the tested setup, when optimizing for accuracy, the optimal threshold for slicing was determined to be 73.9%, resulting in a 90% accuracy, 95.96% recall and precision of 88.04% with a false negative rate of 2.37%. This system therefore allows to detect a wide range of potentially malicious activities and therefore enables operators to initiate counter measures.

V. Conclusion

This paper introduces a highly precise anomaly detection methodology tailored for the STING-system. Our approach enables continuous monitoring for potential anomalous signals while incorporating a degree of localization capability through the utilization of SDRs. To achieve this, a CNN structure named U-Net is employed, which proficiently analyzes PSD waterfall diagrams and categorizes each pixel as either pertaining to 5G signals or background noise. Leveraging key system parameters such as bandwidth and center frequency of the private 5G network, a robust detection accuracy of approximately 90%, with only 2.37% occurrences of false negatives is demonstrated in a controlled environment featuring one active 5G UE and one signal generator.

The focus in future works is to add additional network types to the training data, as well as testing a wider range of anomalies in a real-world environment. Additionally the case that an anomaly is entirely within the 5G signal requires further investigation. The ultimate objective is to develop an anomaly detection system with real-life localization capabilities, enabling precise identification of the source of anomalous signals.

Acknowledgment

This work has been partly funded by the Ministry of Economic Affairs, Industry, Climate Protection and Energy of the State of North Rhine-Westphalia (MWIKE NRW) along with the *5Guarantee* project under grant 005-2008-0077 as well as the German Federal Ministry of Education and Research (BMBF) in the course of the *6G-ANNA* project under grant 16KISK101 and supported by the *6GEM* research hub under grant 16KISK038.

References

[1] 5G-ACIA, “5G Non-Public Networks for Industrial Scenarios,” 5G Alliance for Connected Industries and Automation, Tech. Rep., 09 2021.

[2] D. Sinha, A. K. Verma, and S. Kumar, “Software defined radio: Operation, challenges and possible solutions,” in *Int. Conf. on Intelligent Systems and Control (ISCO)*, 2016.

[3] C. Arendt, M. Patchou, S. Böcker, J. Tiemann, and C. Wietfeld, “Pushing the Limits: Resilience Testing for Mission-Critical Machine-Type Communication,” in *Proc. IEEE VTC-Fall*, 2021.

[4] C. Arendt, S. Böcker, C. Bektas, and C. Wietfeld, “Better Safe Than Sorry: Distributed Testbed for Performance Evaluation of Private Networks,” in *Proc. IEEE FNWF*, 2022.

[5] O. Ronneberger, P.Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” in *Medical Image Computing and Computer-Assisted Intervention (MICCAI)*, ser. LNCS, vol. 9351. Springer, 2015, pp. 234–241.

[6] W. O’Quinn and S. Mao, “Technology Agnostic Anomaly Detection Using Multi-modal Sensory Data in Industrial IoT,” in *Proc. IEEE GLOBECOM*, 2023.

[7] Y. Zhang and Z. Luo, “A Review of Research on Spectrum Sensing Based on Deep Learning,” *Electronics*, vol. 12, no. 21, 2023.

[8] C. P. Robinson, D. Uvaydov, S. D’Oro, and T. Melodia, “DeepSweep: Parallel and Scalable Spectrum Sensing via Convolutional Neural Networks,” in *Proc. IEEE ICMLCN*, 2024.

[9] A. Sebbar, O. Cherqi, K. Chougdali, and M. Boulmalf, “Real-Time Anomaly Detection in SDN Architecture Using Integrated SIEM and Machine Learning for Enhancing Network Security,” in *Proc. IEEE GLOBECOM*.

[10] T. J. O’Shea, T. C. Clancy, and R. W. McGwier, “Recurrent neural radio anomaly detection,” *arXiv preprint*, vol. abs/1611.00301, 2016.

[11] S. Rajendran, W. Meert, V. Lenders, and S. Pollin, “Unsupervised Wireless Spectrum Anomaly Detection With Interpretable Features,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, 2019.