2022 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR) | 978-1-6654-1066-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/CQR54764.2022.9918589

Anomaly Detection with Autoencoders for Spectrum Sharing and Monitoring

Stefan Tschimben
Dept. of Computer Science
University of Colorado Boulder
Boulder, CO, USA
stefan.tschimben@colorado.edu

Kevin Gifford
Dept. of Computer Science
University of Colorado Boulder
Boulder, CO, USA
kevin.gifford@colorado.edu

***Abstract*—Demand for wireless communication devices has been growing continuously since the advent of mobile communication. Even though spectral efficiency and throughput keep increasing, consumer demand continues to seemingly outpace that growth. Spectrum sharing is becoming a more attractive solution to solving various capacity constraints as the resulting perceived spectrum scarcity can mostly be attributed to inefficient spectrum management. However, increasingly complex sharing arrangements come with an increased risk of interference. This makes it necessary to address such events in a timely manner. At the same time, research into using machine learning for solving issues such as signal classification, decision-making processes, and anomaly detection in wireless communication has been growing. To support machine learning research in anomaly detection for wireless communications, this research uses IQ data to train two autoencoders for anomaly detection in shared spectrum: a Long Short-Term Memory (LSTM) and a Deep Autoencoder. These algorithms are used to successfully identify anomalies in the time and frequency domain of recorded IQ data in the form of unauthorized LTE transmissions on top of Wi-Fi communication.**

***Index Terms*—machine learning, spectrum sharing, wi-fi, lte**

I. Introduction

As demand for networked devices and services relying on wireless communication is growing relentlessly - 13.1 billion wireless connected devices expected by 2023 [1] - the need for efficient spectrum management becomes increasingly more important. While spectrum has traditionally been assigned based on exclusive use rights, the inefficiencies associated with exclusive use [2] and the simultaneously growing demand for spectrum emphasize a need for change in how spectrum is managed. As a result, governments and industries worldwide have increasingly moved towards sharing spectrum and opening up more bands for unlicensed use, most recently the 6 GHz band.

Simultaneously, many industries have begun relying upon machine learning to assist with a variety of tasks. Apple and Google for instance have begun equipping their processors with neural engines specialized on machine learning tasks to improve privacy on their mobile phones [3]. However, compared to developments in these related fields, wireless communication still only makes up a minor part of the machine learning field. While machine learning algorithms for the classification of images, sound, or text processing can easily be found, wireless communication examples are few and mostly limited to high level research. As a result, machine learning still offers large untapped potential for spectrum sharing and management.

One crucial aspect of spectrum sharing that could benefit from machine learning is anomaly detection. Currently, unauthorized radio operations are mainly handled by filing a complaint with the Federal Communications Commission (FCC). Significant time can elapse between noticing unusual performance and the anomalous behavior being dealt with. In fact, an example from Lisle, Illinois highlights that it can take up to a month just from the time FCC engineers analyze the unauthorized use to a notice being sent out to the unauthorized user [4], not including any amount of time it took for the behavior to be noticed and reported. Machine learning can significantly shorten the time between the anomalous behavior occurring and an action being taken by automating the detection and reporting of radio frequency (RF) anomalies.

II. Background

Radio spectrum anomalies can take a variety of forms: from unwanted interference in the form of noise or intentional transmissions in licensed or shared bands, to the absence of expected signals [5]. While detecting these anomalies in frequency, time, and location is becoming increasingly more important, managing anomaly detection manually can be inefficient and restricted to addressing a limited number of anomalies and measurement locations. Furthermore, continuously monitoring for anomalies in wireless spectrum raises a number of concerns, not only with regard to the considerable volume of data but moreover with regard to user privacy.

While machine learning and neural networks are used in many areas, radio frequency (RF) applications only represent a small subset of the field. Existing research includes, among others, a large amount of classification problems such as the identification of digital modulation types based on known differences in amplitude [6] or the classification of modulation schemes using a CNN [7], or using a CNN-LSTM as a classifier [8]. Besides classification problems, machine learning was also used by [9] and [10] to detect the number of Wi-Fi

This work was supported by the National Science Foundation under Grant 2030233 and Grant 2139964.

access points for LTE-U carrier sensing adaptive transmission (CSAT). While [11] used 2D-HNNs to enable LTE-U and Wi-Fi coexistence in unlicensed spectrum, [12] used machine learning algorithms to predict path loss, [13] used a modified generative adversarial network (GAN) and spectrograms to detect anomalies, and [14] used deep autoencoders and spectrograms for anomaly detection. [15] used LSTM to predict future IQ data, where anomalies are detected based on prediction error. ALDO (anomaly detection framework for dynamic spectrum access networks) [16] and SAIFE reconstructed power spectral density data using an adversarial autoencoder to design a spectrum anomaly detector with interpretable features [5]. Akyilidiz proposes to use reinforcement learning-based sensing to improve spectrum sensing [17], and [18] used a convolutional network on 64x64, 128x128, and 256x256 spectrograms for spectrum sensing. [19] proposes the use of CNNs trained on waveform images to classify RF spectrum modulations and the use of Principal Component Analysis (PCA) for anomaly detection. [20] applies a LSTM mixture density network (MDN) to timeseries data of digital radio transmissions creating probability distribution functions for the expected signals as a function of time and to measure anomalies such as antenna disconnect, sampling frequency offset, and multipath interference.

Choosing an appropriate anomaly detection method is often data specific, typically requiring a good understanding of the data itself [21]. If the data does not fit the general assumptions of the model, poor results will be the outcome. Due to the fact that it can be very challenging to separate what is considered the "norm" from what is an "anomaly", anomaly detection algorithms typically don't work by classifying the anomaly by its own characteristics, but instead use semi-supervised learning (SSL) to create a model of normal patterns in the data and then detect anomalies in contrast to the norm by computing a score on the basis of the deviation from the norm [21], [22]. 100% correct detection is often impossible due to the fact that anomalies can be very heterogeneous, resulting in missed anomalous instances, misidentifying normal instances, and a generally low recall rate [23]. The emphasis is therefore often instead on controlling the amount of Type I (false positives) and Type II errors (false negatives) by adjusting the anomaly threshold. For SSL to be more accurate than supervised learning, the information gained from the unlabeled samples also has to be useful for the inference of a classification. Additionally, SSL needs to fulfill certain requirements such as the smoothness or continuity assumption, i.e. if x_1 and x_2 are close in a high density region, than y_1 and y_2 need to be close as well, the assumption that decision boundaries can be found in low density regions, and that the high-dimensional data lies on a low-dimensional manifold [24].

Overall, recent RF applications focus heavily on the classification of modulation schemes or types of signals with a large quantity of spectrograms as input with the occasional use of IQ data. Even though some research addresses anomaly detection in RF, due to the enormous amounts of data generated by recording IQ data, it is understandable that most research won't have access to the necessary hardware to execute algorithms on gigabytes or terabytes of training data. Unfortunately, using downsized spectrograms of larger bandwidth signals, such as a 20 MHz Wi-Fi transmission, will lose a considerable amount of detail and result in sub-optimal if not impossible anomaly detection. Therefore, instead of relying on CNNs or spectrograms, the focus of this research is the detection of anomalies in the form of unauthorized LTE transmissions interfering with Wi-Fi in a simulated shared band using semi-supervised learning in the form of autoencoders with a combination of IQ and power spectral density samples.

III. Methodology

A. Data Collection

With the objective of using real data for anomaly detection while avoiding the use of any personally identifiable information (PII), an Extreme Networks AP 650 access point (AP) was used to create an 802.11ax network with a 20 MHz channel at 5.825 GHz. This channel was chosen due to the fact that the FCC rule allowing the use of the bands with center frequencies upwards of 5.825 GHz, which would then allow the formation of up to 160 MHz bandwidth channels, was still relatively recent (November 2020 [25]) and had not been widely adopted yet, no other transmissions were detected at this frequency in this location. Without any other transmissions on the same band, no PII could be recorded.

The access point transmitted data using MCS 6 or 7 (64 QAM) to a laptop and an eNodeB was used to transmit a 64 QAM LTE signal to a smartphone nearby. As highlighted above, recent machine learning research has shown that a number of models have been able to distinguish between various RF modulation and coding schemes (MCS). Therefore, to ensure that the anomaly detection algorithm used on the collected data is not simply separating different modulations, both Wi-Fi and LTE were recorded with the same modulation and a similar coding scheme. To simulate a LTE signal interfering with a Wi-Fi signal in a shared band, the former was recorded at slightly higher received signal strength .

In both cases IQ data is collected in a binary, 16 bit unsigned integer format using USRP B200-mini-i software defined radios (SDR) with industrial enclosures while connected to a Raspberry Pi 4 single-board computer via a USB 3 connection (8 GB model). Each in-phase and each quadrature sample consists of 15 bits plus one bit used for the sign. For the LTE data collection an Ettus VERT 900 antenna (supports 1710 to 1990 MHz) was used with the SDR to record the 10 MHz wide LTE signal centered at 1.8425 GHz. For the Wi-Fi data collection an Ettus VERT 2450 was used to record the 20 MHz wide Wi-Fi signal centered at 5.825 GHz. The data was then combined to create an LTE signal interfering with Wi-Fi.

B. Anomaly Detection

The objective of the anomaly detection algorithm is to detect an anomaly in the frequency as well as the time domain of the recorded IQ data. While using spectrogram images

with a CNN model would potentially be able to provide a visual representation of an anomaly in shared spectrum and has already been demonstrated in a number of recent papers (e.g. [18], [26]) , this visual representation would first have to be translated into its time and frequency components before the visual information could be provided to other applications due to the FFT dependant dimensions of spectrograms. Furthermore CNNs can have a number of crucial disadvantages, such as spatial invariance spectrogram size limitations.

Instead, this anomaly detection algorithm consists of two autoencoder models: (1) a long short-term memory (LSTM) autoencoder to determine the anomaly's frequency domain location and (2), a deep autoencoder (DAE) to determine the anomaly's time domain location. In combination, these can be used to determine the anomaly in the frequency and time domain. Splitting the anomaly detection into frequency and time domain components makes it possible to precisely pinpoint the anomaly's location in time and frequency. Since the anomaly of concern consists of a large number of samples, it is sufficient to focus on precision as long as enough contiguous samples at the anomaly's edges are correctly identified as anomalous. Furthermore, by maintaining the indexing of the arrays containing the data and looking for the longest contiguous anomalies, it is possible to identify the exact range of the anomaly in time and frequency in an automated manner by identifying the first and last index containing the longest contiguous sequence of above threshold anomaly scores. With these values, the start and the end of the anomaly can then be identified and its actual location in time or frequency can be calculated.

The two autoencoder models are implemented using the Keras API with a TensorFlow backend and the "adam" optimizer. The models are trained and tested on an Alienware R11 with a GeForce RTX 3080 and 32 GB RAM. The performance of the three models is evaluated using their precision, recall, and ROC AUC scores. The following sections describe each implementation in detail, including the model's layers, activation functions and the format of the input data.

1) Deep Autoencoder: Autencoders are unsupervised artificial neural networks, sometimes also referred to as semi-supervised or self-supervised due to the fact that they generate their own labels while training, and consist of 4 main components: encoder, latent space, decoder, and reconstruction loss. They learn a low-dimensional feature representation of the data that allows the model to reconstruct the original data instances. Accordingly, Deep Autoencoders consist of multiple layers in the encoder and decoder.

Autoencoders are considered good when the reconstruction is as close as possible to the original input, i.e. the model's output has low reconstruction error. Due to the way reconstruction loss works, autoencoders can also be considered data specific as they are only able to efficiently compress and reconstruct data they have been trained on. Since the model has only learned how to reconstruct "normal" data, anomalies will be difficult to reconstruct and result in considerable reconstruction error. Autoencoders can also be used for sequential data in LSTM networks, to generate data in variational autoencoders (VAE) as generative models, and to pre-train supervised models by using the autoencoder's latent space output as the classifier's input [27], [28].

The DAE used for anomaly detection uses the following 4 features: real component, imaginary component, phase, and magnitude of the IQ sample. The encoder consists of 2 layers, with the decoder mirroring the encoder:

- Dense layer with 4 units and ELU activation function
- Dense layer with 3 units and ELU activation function

The latent space consists of a Dense layer with 2 units and the chosen loss function is the MSE.

2) Long Short-Term Memory Autoencoder: LSTM is designed to support input sequences of varying length without the need to change the model's size and is capable of learning the dynamics of a sequence's temporal order by remembering information across long sequences. LSTMs are the most successful attempt at improving the learning of recurrent neural networks by improving the flow of data from previous time steps and being able to forget states [29]. A LSTM cell can not only read and write information, but more importantly also delete information from its memory. Weights are shared across time and computations take historical information into account, which means a LSTM model is able to learn long term dependencies. A LSTM cell has 4 main components: input, forget, and output gate, and the current cell state. Together these components determine whether to let new input in, delete it, or let it become part of the current timestep's output.

LSTM autoencoders represent an autoencoder implementation specific to sequential data with LSTM cells in a single or multiple layers with a decreasing number of nodes in each layer. LSTM autoencoders read the input data step-by-step and the encoder's output represents a vector of the learned representation of the entire sequence of data. The decoder then interprets this vector and generates a sequential output. While sequence-to-sequence models such as the LSTM autoencoder are good at modeling data with temporal dependence, they can also be comparatively slow [30].

After experimenting with and comparing numerous configurations, the LSTM model settled on for the anomaly detection consists of 10 layers, including the input and output layer. The input consists of a single feature in the form of power values in dBFS gained by converting the provided IQ data via fast Fourier transform (FFT) into its power spectrum representation, which describes the input's frequencies and power distribution. Encoder and decoder are mirrored and consist of the following layers:

- Dense layer with 512 units and ELU activation.
- LSTM layer with 128 units and $tanh$ activation.
- LSTM layer with 32 units and $tanh$ activation
- LSTM layer with 8 units and $tanh$ activation

Due to restrictions in TensorFlow with regard to GPU use of LSTM cells, the default hyperbolic tangent activation function ($tanh$) is used for LSTM. The latent space of the LSTM

model consists of a repeat vector layer, which repeats the input a specified amount of times. The output finally consists of a Time Distributed layer, which makes it possible to apply a layer to every temporal slice of the input [31]. The loss function, as seen in previous examples, is the mean square error (MSE).

IV. Results

A. Frequency Domain Anomaly Detection

The Wi-Fi IQ data samples used for anomaly detection were collected at 20 MS/s (20 MHz bandwidth). In contrast, to simulate partial LTE interference, the LTE IQ data samples were recorded at 10 MS/s (10 MHz bandwidth). To be able to train the models on the available hardware, 2 million IQ samples of the Wi-Fi data and 1 million samples of the LTE data were used for the FFT. The data used for prediction consists of an independent Wi-Fi sample with interference caused by a 10 MHz wide LTE signal. The LSTM model was trained over 5 epochs with a batch size of 128 and a 20% validation split.

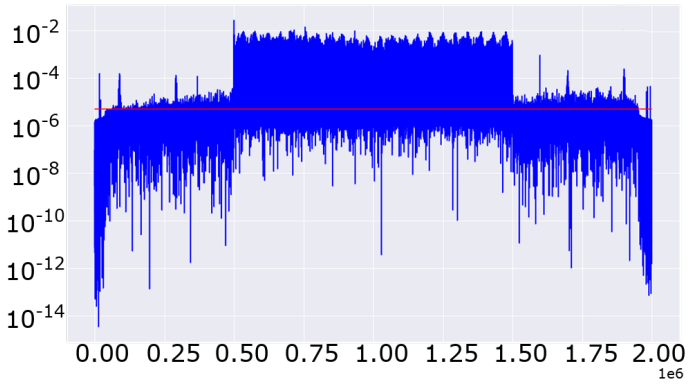

Fig. 1. Loss distribution of the LSTM model - highest scores achieved by the LTE anomaly.

Despite the reduced sample size, training took 683.87 seconds or 11 minutes and 23.87 seconds. The trained model was then used for prediction on Wi-Fi data from a different data collection that had LTE interference added to it. Prediction took 241.8 seconds or 4 minutes and 1.8 seconds and had its anomaly threshold optimized for precision while still achieving sufficient recall, resulting in 98.2% precision and 59.06% recall for a F1 score of 0.7376. Fig. 1 depicts the algorithm's achieved reconstruction loss (y-axis) across the 2 million samples (x-axis), clearly showing that the center LTE samples resulted in the highest reconstruction loss.

Fig. 2 shows the model's precision and recall in numerical form using its confusion matrix, where each row consists of data in the actual class while each column represents data predicted as that class. The first row illustrates that, of 1 million Wi-Fi data points, 989,175 have been correctly identified as Wi-Fi, and only 10,825 falsely identified as LTE. Of the 1 million anomalous LTE data points, 590,636 have been correctly identified as LTE while 409,364 data points

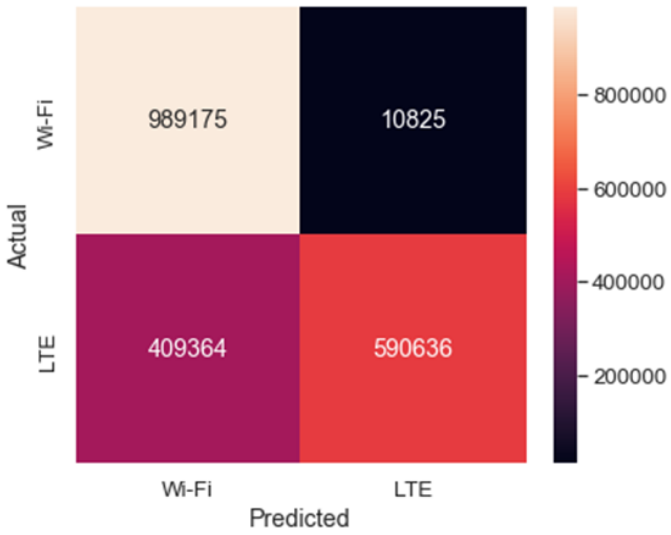

Fig. 2. LSTM Confusion Matrix.

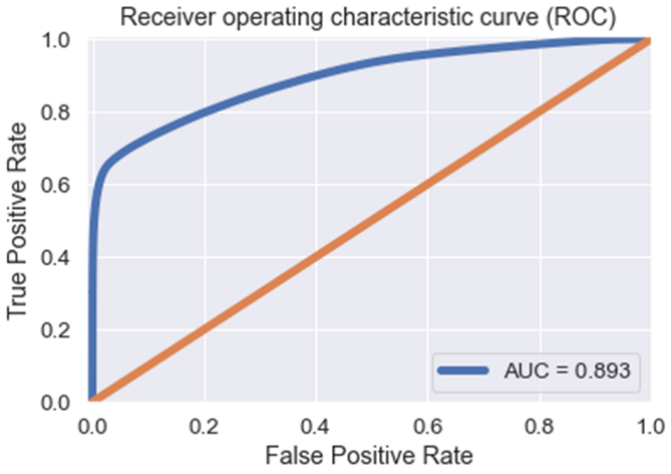

Fig. 3. LSTM ROC Curve.

have been missed. The AUC in Fig. 3 (b) shows a score of 0.893, indicating that the model is a well-working predictor. Python code was then used to identify the longest contiguous series of samples above the anomaly threshold and as a result the anomaly's edges. With this information, the algorithm identified the anomaly from $\sim$ 5820.0 MHz to $\sim$ 5830.0 MHz.

B. Time Domain Anomaly Detection

The time domain anomaly detection used 2 million Wi-Fi IQ samples – the equivalent of 0.1 seconds of a 20 MHz wide IQ data recording - and 200,000 LTE IQ data samples located from index 900,000 to 1,100,000 of the array (0.045 to 0.055 seconds). The complex samples were split into real and imaginary components as their own feature in addition to phase and magnitude representations for a total of 4 features. Previous research has shown that adding more features did

not noticeably improve training and sometimes was even detrimental [32].

The DAE was trained over 15 epochs with a batch size of 64 for a total training time of 1728.4 seconds or 28 minutes and 48.4 seconds. While training time was much longer compared to the LSTM model, prediction time was considerably shorter at 68.09 seconds. Fig. 4 shows the model's reconstruction loss distribution highlighting again the anomaly in its center and its proportionally much higher reconstruction loss. Fig. 5 shows the DAE's confusion matrix, highlighting 96.78% precision and 85.75% recall in the anomaly detection task for a F1 score of 0.91 and an AUC score of 0.966 (see Fig. 6). The Python algorithm was again able to correctly identify the anomaly's edges and identified LTE samples from 0.045 to 0.055 seconds.

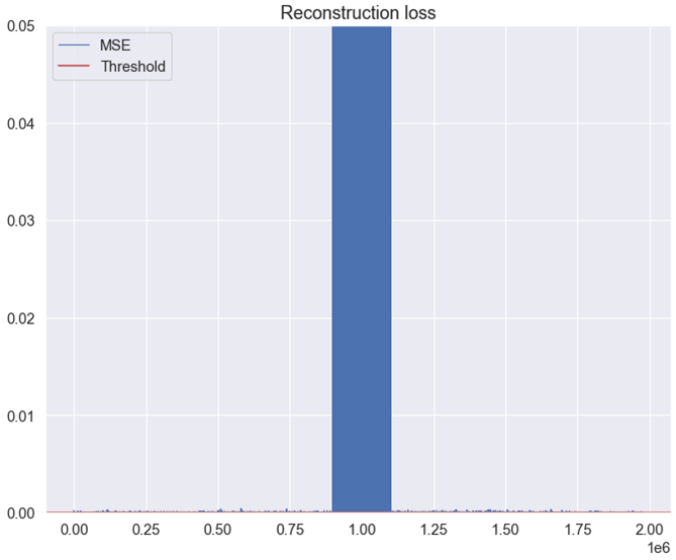

Fig. 4. Loss distribution of the DAE model - highest scores achieved by the LTE anomaly.

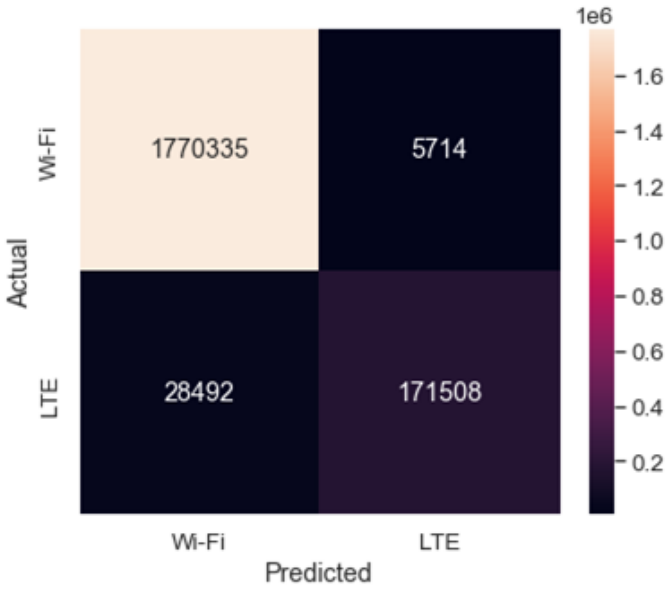

Fig. 5. DAE Confusion Matrix.

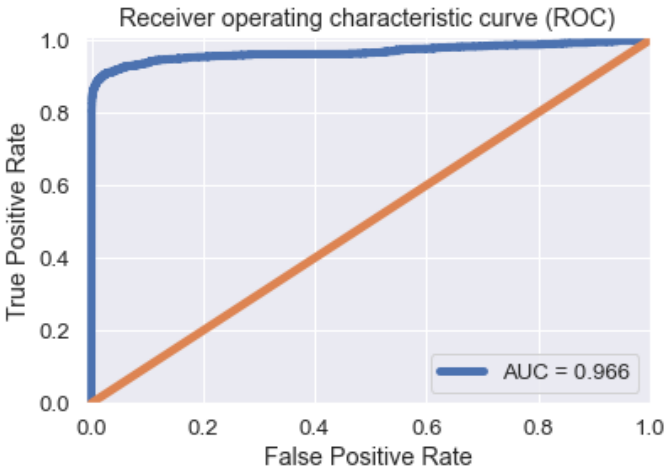

Fig. 6. DAE ROC Curve.

V. Conclusion

This research demonstrated how two autoencoders, one for frequency domain anomaly detection and one for time domain anomaly detection, can be used for anomaly detection on real data collected with relatively inexpensive SDRs. Wi-Fi and LTE IQ data have been used to simulate a band shared between both where an LTE transmission is interfering with Wi-Fi. Sharing between Wi-Fi and LTE still requires considerable optimization, but is ultimately the way forward as LTE-LAA systems continue being deployed. As a result, detecting anomalous behavior of either signals will become increasingly more important. The trade-off between faster prediction time, slightly higher recall, and overall model score needs to be balanced. Furthermore, since collecting IQ data can produce large amounts of data within a short amount of time, it would not be feasible to continuously check for anomalies. Instead, to minimize the amount of data collected and to avoid statistical bias, samples should be collected in random intervals. How often these intervals occur depends on computational cost and benefit trade-offs.

The combination of models and algorithm presented here also have the advantage of providing a clear machine and human interpretable result. However, due to the inherent characteristics of IQ data of representing magnitude and phase, machine learning algorithms mainly learn these two features when using IQ data, whereby magnitude is the strongest indicator, considerably improving results as it is increased. The large amounts of data generated by IQ data collections can be addressed by using more advanced hardware, reducing the time frame of a single anomaly detection analysis, decimating the IQ samples, or by making the algorithm more adaptive.

Additionally, the presented data collection procedures can easily be adapted for continuous spectrum monitoring by

automating the collection of IQ data in intervals and executing the algorithm on the recorded data. As a result, spectrum enforcement could be expedited considerably or automated entirely. Since automated enforcement might require considerable policy changes, using the presented data collection procedure for an automated notification regarding detected anomalies might be faster to implement. Instead of collecting data at predetermined intervals, a short sample can be collected at random intervals in order to avoid statistical bias or once an unusual change in signal strength is detected. Additional algorithms such as the one proposed in [33] could then be used to further determine the anomaly's geographical location, which can be used to further isolate the anomalous IQ data and use it for classification.

With regard to anomaly detection, multi-user anomalies have not been investigated and offer potential for future research. Although the autoencoder algorithm should be able to detect multiple anomalies, it has not yet been tested. Additionally, it should be investigated how large the minimum difference between a trained signal and the anomaly needs to be in order for the algorithm to identify the anomaly. These could be combined into a resource limited scenario, to investigate what a system's minimum capabilities need to be in order to collect the minimum amount of data necessary to identify multiple anomalies at minimum distance from a signal or noise.

REFERENCES

[1] Cisco annual internet report (2018–2023) white paper. Cisco. Online; accessed 09-January-2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] M. L. Goldstein, "Ntia planning and processes need strengthening to promote the efficient use of spectrum by federal agencies," Government Accountability Office, 2011, report to Congressional Committees. [Online]. Available: https://www.gao.gov/assets/gao-11-352.pdf

[3] T. Simonite. Apple's and google's new ai wizardry promises privacy—at a cost. Wired. Online; accessed 09-January-2022. [Online]. Available: https://www.wired.com/story/apple-googles-ai-wizardry-promises-privacy-cost/

[4] Ebonie may; eyescream media; bolingbrook, illinois. Federal Communications Commission. Online; accessed 09-January-2022. [Online]. Available: https://www.fcc.gov/edocs/search-results?t=advanced&fileNumber=EB-FIELDNER-19-00029887

[5] S. Rajendran, W. Meert, V. Lenders, and S. Pollin, "Saife: Unsupervised wireless spectrum anomaly detection with interpretable features," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2018, pp. 1–9.

[6] E. E. Azzouz and A. K. Nandi, "Automatic identification of digital modulation types," *Signal Processing*, vol. 47, no. 1, pp. 55–69, 1995.

[7] T. J. O'Shea, T. Roy, and T. C. Clancy, "Over-the-air deep learning based radio signal classification," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168–179, 2018.

[8] D. Czech, A. Mishra, and M. Inggs, "A cnn and lstm-based approach to classifying transient radio frequency interference," *Astronomy and computing*, vol. 25, pp. 52–57, 2018.

[9] V. Sathya, M. Merhnoush, M. Ghosh, and S. Roy, "Energy detection based sensing of multiple wi-fi bsss for lte-u csat," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–7.

[10] A. Dziedzic, V. Sathya, M. I. Rochman, M. Ghosh, and S. Krishnan, "Machine learning enabled spectrum sharing in dense lte-u/wi-fi coexistence scenarios," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 173–189, 2020.

[11] M. Alsenwi, I. Yaqoob, S. R. Pandey, Y. K. Tun, A. K. Bairagi, L.-w. Kim, and C. S. Hong, "Towards coexistence of cellular and wifi networks in unlicensed spectrum: A neural networks based approach," *IEEE Access*, vol. 7, pp. 110 023–110 034, 2019.

[12] Y. Zhang, J. Wen, G. Yang, Z. He, and J. Wang, "Path loss prediction based on machine learning: Principle, method, and data expansion," *Applied Sciences*, vol. 9, no. 9, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/9/1908

[13] X. Zhou, J. Xiong, X. Zhang, X. Liu, and J. Wei, "A radio anomaly detection algorithm based on modified generative adversarial network," *IEEE Wireless Communications Letters*, vol. 10, no. 7, pp. 1552–1556, 2021.

[14] Q. Feng, Y. Zhang, C. Li, Z. Dou, and J. Wang, "Anomaly detection of spectrum in wireless communication via deep auto-encoders," *J. Supercomput.*, vol. 73, no. 7, p. 3161–3178, 07 2017. [Online]. Available: https://doi.org/10.1007/s11227-017-2017-7

[15] T. J. O'Shea, T. C. Clancy, and R. W. McGwier, "Recurrent neural radio anomaly detection," 2016.

[16] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "Aldo: An anomaly detection framework for dynamic spectrum access networks," in *IEEE INFOCOM 2009*, 2009, pp. 675–683.

[17] B. F. Lo and I. F. Akyildiz, "Reinforcement learning-based cooperative sensing in cognitive radio ad hoc networks," in *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2010, pp. 2244–2249.

[18] T. J. O'Shea, T. Roy, and T. Erpek, "Spectral detection and localization of radio events with learned convolutional neural features," in *2017 25th European Signal Processing Conference (EUSIPCO)*, 2017, pp. 331–335.

[19] M. A. Conn and D. Josyula, "Radio frequency classification and anomaly detection using convolutional neural networks," in *2019 IEEE Radar Conference (RadarConf)*, 2019, pp. 1–6.

[20] M. Walton, M. Ayache, L. Straatemeier, D. Gebhardt, and B. Migliori, "Unsupervised anomaly detection for digital radio frequency transmissions." IEEE, 2017, pp. 826–832.

[21] C. C. Aggarwal, *Outlier Analysis*. Springer, Cham, 2017.

[22] S. Alla and S. K. Adari, *Beginning Anomaly Detection Using Python-Based Deep Learning*. Apress, 2019.

[23] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: A review," vol. 54, no. 2, 03 2021. [Online]. Available: https://doi.org/10.1145/3439950

[24] O. Chapelle, B. Schölkopf, and A. Zien, *Semi-Supervised Learning*. The MIT Press, 09 2006. [Online]. Available: https://doi.org/10.7551/mitpress/9780262033589.001.0001

[25] F. C. Commission, "Fcc modernizes 5.9 ghz band to improve wi-fi and automotive safety," 11 2020. [Online]. Available: https://www.fcc.gov/document/fcc-modernizes-59-ghz-band-improve-wi-fi-and-automotive-safety-0

[26] J. Fontaine, E. Fonseca, A. Shahid, M. Kist, L. A. DaSilva, I. Moerman, and E. De Poorter, "Towards low-complexity wireless technology classification across multiple environments," *Ad Hoc Networks*, vol. 91, p. 101881, 2019.

[27] Y. Bengio and Y. LeCun, "Scaling learning algorithms towards ai," *MIT Press*, 2007.

[28] D. Erhan, Y. Bengio, A. Courville, P. Manzagol, P. Vincent, and S. Bengio, "Why does unsupervised pre-training help deep learning?" *Why Does Unsupervised Pre-training Help Deep Learning?*, vol. 10, pp. 625–660, 2010.

[29] Q. V. Le, "A tutorial on deep learning part 2: Autoencoders, convolutional neural networks and recurrent neural networks," Tech. Rep. [Online]. Available: https://cs.stanford.edu/ quoc/le/tutorial2.pdf

[30] (2020, February) Deep learning for anomaly detection. Cloudera Fast Forward. Online; accessed 09-January-2022. [Online]. Available: https://ff12.fastforwardlabs.com

[31] (n.d.) Timedistributed layer. Keras. Online; accessed 09-January-2022. [Online]. Available: https://keras.io/api/layers/recurrent_layers/time_distributed/

[32] S. Subray, S. Tschimben, and K. Gifford, "Towards enhancing spectrum sensing: Signal classification using autoencoders," *IEEE Access*, vol. 9, pp. 82 288–82 299, 2021.

[33] P. Pinchuk and J.-L. Margot, "A machine-learning-based direction-of-origin filter for the identification of radio frequency interference in the search for technosignatures," 2021.