

Autoencoder based framework for drone RF signal classification and novelty detection

Sanjoy Basak^{*†}, Sreeraj Rajendran[†], Sofie Pollin[†], and Bart Scheers^{*}

Email: {sanjoy.basak, bart.scheers}@rma.ac.be,

{sreeraj.rajendran, sofie.pollin}@esat.kuleuven.be

^{*}Department CISS, Royal Military Academy, Belgium, [†]Department ESAT, KU Leuven, Belgium

Abstract—The increasing use of Unmanned Aerial Vehicles (UAVs) in modern civilian and military applications shows the urgency of having a robust drone detector that detects unseen drone RF signals. Ideally, the system can also classify known RF signals from known drones. This study aims to develop an incremental-learning framework which can classify the known RF signals, and further detect novel RF signals. We propose DE-FEND: a Deep residual network-based autoEncoder FramEwork for known drone signal classification, Novelty Detection, and clustering. The known signal classification and novelty detection are performed in a semi-supervised and unsupervised manner, respectively. We used commercial drone RF signals to evaluate the performance of our framework. With our framework, we obtained 100% novelty detection accuracy at 1.04% False Alarm Rate (FAR) and 97.4% classification accuracy with only 10% labelled samples. Furthermore, we show that our framework outperforms the state-of-the-art (SoA) algorithms in terms of novelty detection performance.

Index Terms—Deep neural networks, Unsupervised learning, UAV.

I. INTRODUCTION

TECHNOLOGICAL advancements in the last decade have made UAVs more affordable and easily accessible. UAVs now-a-days are becoming smaller and more agile. They are equipped with advanced sensors and technologies that enable features such as autonomous navigation, collision avoidance and face recognition. We have seen many beneficial applications of drones, such as damaged infrastructure inspections, urgent aid supply, search and rescue operations to remote and unreachable places and humanitarian demining. Drones are now also being used for precision farming, cinematography and recreational activities. However, the potential of UAVs has also captured the attention of criminals and terrorist organizations. The malicious uses include but are not limited to drug trafficking, firearm smuggling, bombing, activism and privacy invasion. Furthermore, private industries have also experienced attacks using UAVs at airports, oil plants and nuclear power plants. Due to the improvements in flight stability, autonomy and payload capabilities, commercial mini-UAVs have become capable of carrying explosives [1] and performing precise target bombing. The war in Ukraine shows the importance of having a drone detection and neutralization system on modern battlefields.

Conventional methods for detecting intruder drones include Radar detection, Visual detection, Acoustic detection, and RF-based detection. RF detection is one of the most promising

approaches since it does not require line of sight (LOS), can work passively, and is independent of weather and daylight conditions. The active RF communication between the drone and its ground control station (GCS) allows the RF detector to detect and classify a drone from kilometers away. Despite having so much potential, it is very challenging to identify and classify a drone signal since commercial drones operate in unlicensed ISM frequency bands. These frequency bands are used by many popular RF communication technologies such as WiFi, Bluetooth and Zigbee.

RF based drone signal detection and classification have been discussed in the literature in recent years. Researchers have utilized both classical and Deep Learning (DL)-based frameworks to perform the detection, classification and localization of UAVs. Nguyen et al. [2] proposed an RF-based drone identification system by counting the packet transfer rate between the drone and its GCS at the 2.4 GHz frequency band. In [3], the authors performed the identification and classification of drone signals by utilizing the time-frequency domain features extracted from a classical spectrum sensing method. Several authors have also utilized DL-based frameworks to identify and classify drone signals. In [4], the authors performed the identification and classification of drone signals by using a feed forward Deep Neural Network (DNN). In [5], the authors demonstrated an improvement in the classification performance using a Convolutional Neural Network (CNN)-based framework over the simple DNN-based frameworks.

The aforementioned studies address the problem of classifying drone RF signals present in the library. However, they do not solve the problem of unknown drone signal detection. Detecting and classifying drone RF signals in a congested and contested RF spectrum environment such as the ISM bands is a challenging task. Detecting an unseen drone signal is much more challenging. The drone industry is booming and we are getting new drones every year from different manufacturers. There is no standardized drone signal protocol. Every manufacturer is free to use a proprietary communication protocol that is unknown to other Counter Unmanned Aircraft Systems (C-UAS) and the industry. It is therefore very important to have an incremental learning framework which can identify unknown drone and non-drone RF signals along with classifying the known signals. Afterwards, the framework should learn the characteristics of the novel signals based on an expert's feedback. We presented drone RF signal detection using a classical spectrum sensing method in [6] under the

scope of an EU H2020 project called SafeShore. Afterwards, we developed a deep Residual Network (ResNet) architecture for classifying drone RF signals utilizing the frequency domain RF signatures [7]. Furthermore, we developed a combined drone RF signal detection and classification framework using a You Only Look Once (YOLO)-based framework and presented the results in [8].

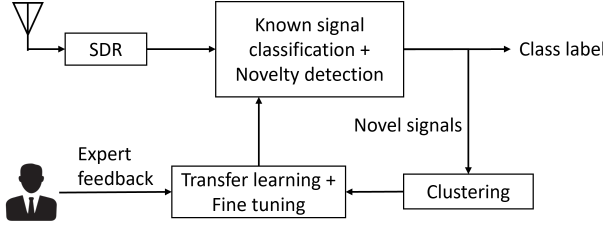


Fig. 1: Proposed Incremental Learning Schematic

The existing novel signal detection approaches include kernel density based, nearest neighbor based, and reconstruction based methods. The kernel density-based method estimates the data distribution in a non-parametric way using a large number of kernels [9]. The kernel density based method works well on small scale datasets. However, for high-dimensional and large datasets, it becomes computationally expensive and prone to overfitting [10]. The nearest neighbor-based methods can also be used for novelty detection in an unsupervised manner. The fundamental assumption for these methods is that the normal data points of the known classes stay in close proximity to each other and novel data points will stay far from the cluster of known classes [11]. However, the distance calculation for large datasets is computationally expensive with this method, and for higher dimensional datasets, it becomes more difficult to define the distance metric and perform the computations.

The reconstruction-based methods utilize an autoencoder-based framework to differentiate novel signals from the known classes. The assumption is that an autoencoder-based framework will reconstruct the known signals well and novel signals will have higher reconstruction errors. In [12], the authors utilized the reconstruction method to detect the anomalies using a deep autoencoder. The authors extended the spectrum prediction idea by using the spectrogram matrix as the input to determine the anomalies. This method will not work well for detecting novel drone RF signals because all commercial drones communicate using spread spectrum technology. A novel drone may use the same bandwidth and frequency channel while using the Direct Sequence Spread Spectrum (DSSS) or OFDM signal. Similarly, they may use the same hopping pattern when communicating using the Frequency Hopping Spread Spectrum (FHSS). Moreover, we are also interested in performing classification of the known drone RF signals.

In this paper, we develop an incremental learning framework which can classify the known drone RF signals and detect the unseen drone RF signals. The novelty detection is performed using the reconstruction-based method. The framework will later learn the features of the unseen signal in a re-iterative process where the labelling will be performed based on an

expert's feedback. The schematic of our proposal is presented in Fig. 1.

The main contribution of this paper is following:

- 1) We developed DEFEND, an Autoencoder (AE) based framework for detecting unknown signals and classifying known signals. We utilized the deep ResNet architecture to develop the framework. We show that the model can be trained in a semi-supervised fashion to classify known signals. The unseen signal detection is performed using the reconstruction-based method.
- 2) The novel signals are then clustered using the extracted features from the received signal and the reconstruction error score. We utilized the Principal Component Analysis (PCA) and the Density-based spatial clustering of applications with noise (DBSCAN) algorithms to cluster unknown signals.

The rest of the paper is organised as follows: Sections II and III, respectively, explain the most recent works and the problem statement. The technical approach, model description and the novelty detection approach are presented in sections IV, V and VI, respectively. The database development and the implementation details are described in section VII. The performance evaluation is presented in section VIII. Finally the discussion and remarks, and the conclusion are described in sections IX and X respectively.

II. RELATED WORKS

There are various anomaly detection methods proposed in the literature, such as One class Support Vector Machine (OSVM), Isolation Forest (IFO), Robust Covariance (RCOV) and Lightweight on-line detector of anomalies (LODA), which can be utilized to detect novel signals. These methods work in an unsupervised manner and they work on the assumption that the outliers represent the possible anomalies.

DL-based unknown signal detection has been discussed in a few literature in recent years. Rajendran et al. developed an Adversarial Autoencoder (AAE) based framework called SAIPE [13] for RF anomaly detection, feature extraction, and known signal classification. The study shows the strengths of AAE frameworks for anomaly detection in an unsupervised manner. The Saife framework learns the time-frequency signature (e.g., a single or multi-continuous transmission pattern or a hopping pattern) from a spectrogram matrix. Since commercial drones use pseudo-random frequency hopping patterns to communicate with their controllers, it is not possible to detect unknown drone signals using this concept. In [14], the authors developed a Generative Adversarial Network (GAN)-based framework for detecting rogue RF transmitters by utilizing the rise time signature. In [15], the authors developed an AE-based framework to detect unknown RF transmission sources utilizing frequency domain signatures.

In [13] and [15] novelty detection is performed using the reconstruction error score, whereas in [14], it utilizes the discriminator's score. We found the reconstruction-based method to be the most effective method for detecting novel transmission sources. We did not obtain a robust novelty detection performance using the discriminator's score of a

GAN framework. Therefore, we opted for the reconstruction-based method for novelty detection, which works by utilizing an encoding-decoding pipeline, where the unseen transmission sources are detected by comparing the reconstruction error score to a pre-defined threshold. Since the model is trained to reconstruct the known sources, it provides a higher loss while reconstructing the unknown sources. Unlike [15], we did not obtain good novelty detection performance only using the frequency domain signatures from the PSD dataset. Therefore, we utilized the IQ vectors for novelty detection. Alongside, we developed a ResNet-based AE framework which can capture RF signatures more efficiently to differentiate between known and novel signals.

III. PROBLEM STATEMENT

Given: Let X_S represent a set of complex time series data, where x ($x \in X_S$) is the IQ vector. The dataset $X_S = X_{S0} \cup X_{S1} \dots \cup X_{Sn}$ contains drone RF signals from different frequency bands.

Goal: The first goal of the framework is to classify known signals in a semi-supervised fashion. Let X_S and Y_S represent the signal input and output labels, respectively. In the training dataset (X_S), L_S and U_S are the labelled and unlabelled samples, respectively, which can be shown as $L_S \cup U_S \subseteq X_S$. The aim is to construct a framework which can learn to efficiently classify signals while being trained with a limited number of labelled samples.

The second goal is to learn the source data distribution $p(X_S)$ and detect when an unknown signal is received. A significant deviation from the source data distribution will be expected as we receive a signal from an unknown source. The hypothesis can be shown as follows:

- H_K : Sample follows the source data distribution;
- H_U : Sample does not follow the source data distribution.

IV. TECHNICAL APPROACH

The algorithm starts with detecting the presence of a signal or noise in the received signal. The detection can be performed using a classical spectrum sensing method or a DNN-based method. In this study, we assume that the YOLO framework detects the presence of a signal from the spectrogram matrix and extracts useful signal features such as the operating frequency, bandwidth, and dwell time, which are further used to perform preprocessing on the signal burst. The estimation of signal features using a YOLO framework is demonstrated in [8]. The workflow is shown in Fig. 2.

Since commercial drones use the spread spectrum modulation technique, RF communication can happen at any relatively free or randomly chosen frequency channel in the ISM band. Obtaining frequency shift-invariant performance is one of the most difficult challenges. The framework should classify a known signal even if it appears at a different frequency compared to what it is trained for. In addition, the framework should also detect a novel signal at any frequency channel. There are two ways to achieve this: (i) perform preprocessing to have the frequency shift-invariant representation of the input; and (ii) develop a complex framework such that it learns

the shift-invariant representation from the signal automatically. We opt for the first option in this study since, with the extracted features from the YOLO framework, we can perform the preprocessing to make the signal frequency shift-invariant quite easily. We perform the preprocessing in three consecutive steps:

- Frequency centering: The frequency centering is performed using the detected operating frequency (i.e. F_C) of the transmitted drone signal from the YOLO framework.
- DownSampling: Since we receive the signals at a sampling rate of 100 MSps using the Universal Software Radio Peripheral (USRP) X310, we downsample them to a lower sampling rate using FIR filters. Generally, the bandwidth of drone video signals varies from 10 MHz to 20 MHz and for radio control (RC) signals it varies from 250 kHz to 4 MHz at 2.4 GHz. The video RF signals are downsampled to 25 MSps, and the RC signals are downsampled to 5 MSps. The downsampling rate for each signal is determined using the signal bandwidth extracted from the YOLO framework. Note that it is possible to use multiple downsampling pipelines. We decided to use two pipelines to simplify the calculation.
- Interpolation: The dwell time of each transmission will be different; therefore, after downsampling, we perform interpolation to bring it to a fixed IQ vector length (e.g. 1024).

Note that we used RF signals from commercial drones in this study to prepare the database (presented in section VII).

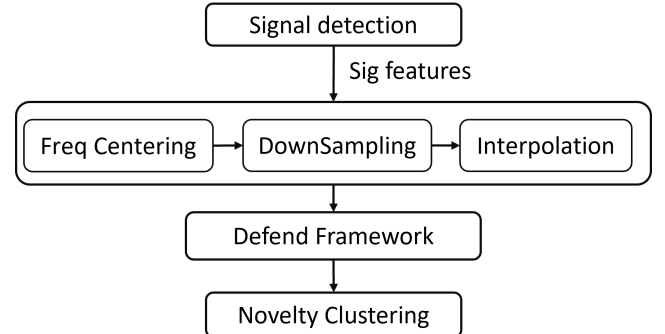


Fig. 2: The complete workflow including the preprocessing steps

V. MODEL DESCRIPTION

Our proposed DEFEND framework performs two tasks: (i) Novelty detection (ND) and (ii) Known Signal Classification (KSC), as shown in Fig. 3. We utilize the AE architecture to perform this task. The framework outline is provided in Fig. 4.

Our proposed framework consists of an encoder, a classifier, and a decoder. The encoder and classifier are Deep Residual Neural Network (DRNN) and the decoder is a simple CNN. The encoder compresses the input IQ signal to a lower-dimensional latent feature vector ($\mathbf{z}$). The classifier path is

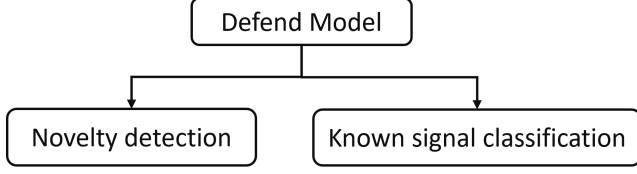


Fig. 3: DEFEND model tasks

trained to classify the known transmission sources. The decoder reconstructs the signal from the latent feature vector ($\mathbf{z}$) and the class labels.

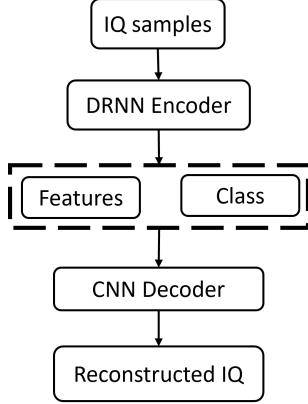


Fig. 4: Framework Components

A. Encoder

The encoder consists of five residual stacks and two fully connected (FC) layers. The residual units and stacks are inspired by [16] and are shown in Fig. 5. We observed significant improvement in the classification and encoding performance with the use of residual networks, and therefore, the residual network structures were used for the encoder and classifier path. The *Tanh* activation was used in the encoder path as shown in Fig. 6, since we obtained lower reconstruction loss with it. Following the residual stacks are two fully connected layers (FCLs) with *Tanh* activation and one fully connected layer (FCL) with linear activation. After the first two FCLs, we used dropout layers with a drop probability of 0.1. The number of units for FCLs, the number of residual stacks and the number of features in the latent space were selected manually through a trial-and-error method. We obtained better performance with 100 features, therefore, we used $\mathbf{z} = 100$ for all experiments in this study.

B. Classifier

The classifier path is connected with the Res Stack3 as shown in Fig. 6. We used three residual stacks with the rectified linear unit (RELU) activation since we observed better classification performance with it. Two FCLs with the scaled exponential linear unit (SeLU) activation and one FCL with softmax activation are used after the residual stacks. After the first two FCLs, we used alpha dropout with a dropout rate of 0.3. Afterwards, we concatenate the latent feature vector ($\mathbf{z}$) and class labels (i.e. one hot vector).

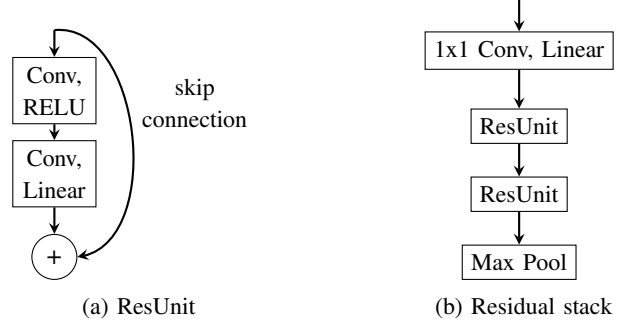


Fig. 5: Building blocks of the DRNN-based encoder and classifier

C. Decoder

The decoder receives the concatenated vector from the encoder and classifier, and reconstructs the input signal. We have used a simple CNN architecture as the decoder, as shown in Fig. 6. Similar to the encoder architecture, we have used *Tanh* activation with the FCL and the convolution operations. The convolution layers are followed by an upsampling operation and finally, we have used two FCLs with the *Tanh* and linear activations, respectively.

VI. NOVELTY DETECTION AND CLUSTERING

A. Novelty detection

Novelty detection is performed using the reconstruction error score. The AE framework should reconstruct the known data samples with lower reconstruction loss whereas the reconstruction loss for unknown samples should be very high. The reconstruction error is calculated as follows:

$$R_l = \sum_{n=1}^{n=N} (x - \hat{x})^2, \quad (1)$$

where, x is the input IQ signal, $\hat{x}$ is the reconstructed IQ signal and N is the sample length. We utilized an n-sigma threshold approach to calculate the threshold for detecting unknown/novel signals. A test signal is considered to be novel if N_{score} is True:

$$N_{score} = (R_l > (\mu_{R_{lt}} + n * \sigma_{R_{lt}})) \quad (2)$$

The mean ($\mu_{R_{lt}}$) and variance ($\sigma_{R_{lt}}$) are calculated from known training signals.

B. Novelty Clustering

The novelty clustering is performed using the extracted features from the YOLO framework and the reconstruction error. During experiments, we observed that the reconstruction loss is often specific to the transmission technology. For a particular transmission protocol, the AE encodes and decodes in a certain way, which is completely unique to that protocol. As a result, we observed different reconstruction errors for different transmission protocols (e.g. DJI Ocusync, DJI Lightbridge, Frysky etc.). This statement may not be always true, however, in most cases, we observed this behavior from

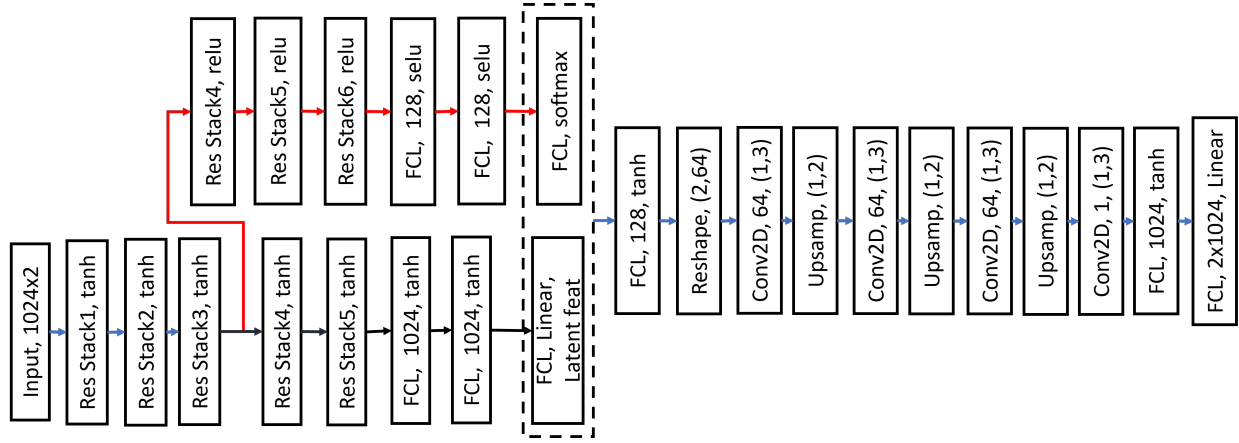


Fig. 6: The Complete model architecture

the AE. Therefore, the reconstruction error is used for the clustering of unknown signals. The features used for clustering are: (i) Bandwidth, (ii) Dwell time, and (iii) Reconstruction loss. We use the PCA method to reduce the feature dimension from 3D to 2D. We did not observe any negative impact of feature reduction on novelty detection performance. Afterwards, DBSCAN was used on the reduced features to perform clustering as mentioned earlier.

VII. DATABASE DEVELOPMENT AND MODEL TRAINING

A. Database development

We have constructed the drone signal library using all available commercial drones at our institute as listed in Tables I and II. Among the available drones, we used the ones with relatively popular RF protocols as the known sources and the rest as unseen sources. The recording was performed at the semi-anechoic chamber of the RMA using the Ettus USRP X310. We recorded raw IQ signals with the USRP. The drones were placed 10 meters apart from the antenna. We recorded clean drone signals without any interference from any other communication signals.

Our model is trained with the RF signals from drones and controllers listed in Table I. The RF signals from drones and controllers listed in Table II are unknown to the model. The classification performance is tested with known drone signals and the novelty detection performance is evaluated using both known and unseen drone signals.

TABLE I: Drones and Radio Controllers (Known sources)

Nr.	Name	Protocol
1	Spektrum DX4e RC	DSM
2	DJI mini 2 RC	Ocusync 2.0
3	DJI mini 2 Video	Ocusync 2.0
4	DJI inspire 2 RC	Lightbridge 2
5	DJI inspire 2 Video	Lightbridge 2
6	DJI Matrice pro RC	Lightbridge 2
7	DJI Matrice pro Video	Lightbridge 2
8	RadioMaster, Taranis RC	Fryskey

TABLE II: Drones and Radio Controllers (Unknown sources)

Nr.	Name	Signal Type
1	NineEagles	RC
2	WiToys	RC
3	Q205	RC
4	SJRC pro	RC

B. Implementation details

The framework is implemented using TensorFlow [17] in Python. We used the Adam optimizer [18] with a learning rate of 0.0001 for training in all phases. The framework is trained to reduce the mean squared error between the input and decoded IQ samples in an unsupervised fashion and to learn the class labels in a semi-supervised fashion. The training was performed for 500 epochs on a server computer at KU Leuven equipped with eight GPU RTX 2080 Ti cards. We also used early stopping to stop training if no improvements are observed for 20 consecutive epochs.

VIII. RESULT AND DISCUSSION

In this section, we analyze the performance of our framework. First, we evaluate the known RF signal classification performance. Then the novelty detection performance is evaluated using the known and unknown RF signals. Next, we analyze the novelty clustering performance. The numbers of training, test and unseen samples are provided in the following table.

TABLE III: Number of samples used for evaluation

Name	Sample numbers
Train samples	27347
Test samples	6837
Unseen samples	10758

A. Semi-supervised classification performance

The classification performance is evaluated using the known transmission sources as mentioned in the earlier sections.

The average classification accuracy for different numbers of labelled samples is presented in Fig. 7. We obtained a 70.3% classification accuracy with only 1% labelled samples (i.e., approximately 34 labelled samples per class). With the increase in labelled samples, the average accuracy increases and it reaches 97.4% with 10% labelled samples. The accuracy further increases and reaches 99.6% with 50% labelled samples. The confusion matrix with 50% labelled samples is presented in Fig. 8.

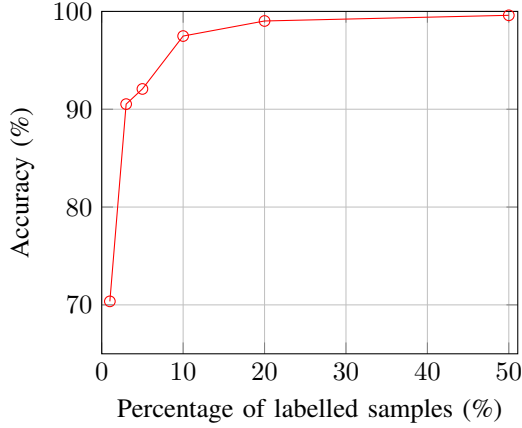


Fig. 7: Classification accuracy under different amount of labelled samples; Test samples: 6837

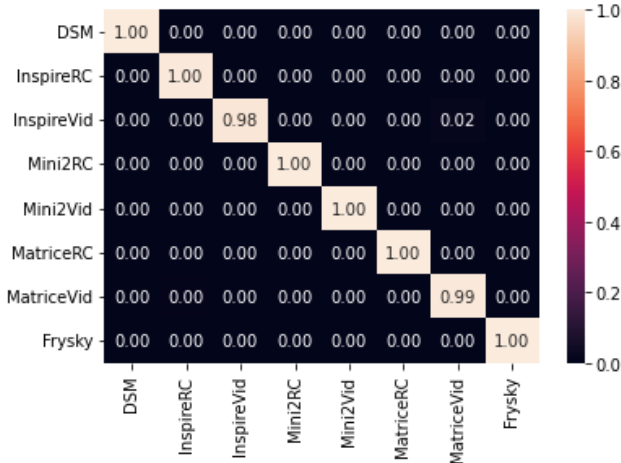


Fig. 8: Confusion Matrix for model trained with 50% labelled samples and tested on 6837 samples; Average classification accuracy: 99.6%

B. Unknown signal detection performance

The novelty detection is performed using the reconstruction error score as described earlier. Fig. 9 depicts the probability distributions of the reconstruction losses of known and unknown signals. We obtained much higher reconstruction losses for the unseen signals compared to the known signals. Although there is a clear separation between the reconstruction loss of known and unseen signals, we observed higher reconstruction errors for known signals in very few cases.

After investigation, we found that higher losses with the known drone signals resulted from the preprocessing errors (Fig. 2). Note that we rely on YOLO detection to determine the start and end position of a signal burst. Moreover, we observed minor frequency offsets in the YOLO detection result. Although the errors are negligible most of the time, in some cases they result in a slightly different variant of the IQ signal, which causes higher reconstruction loss for known signals.

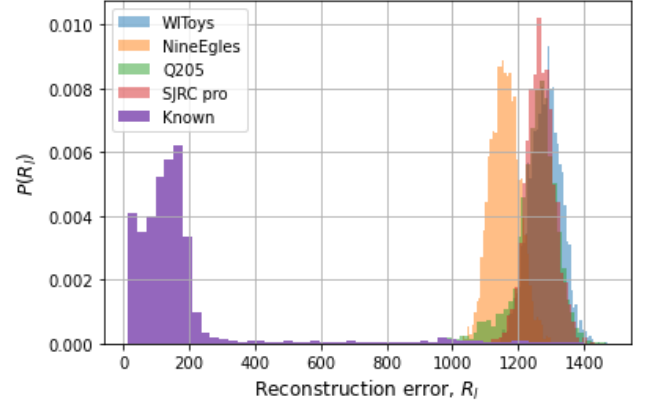


Fig. 9: Probability density function plot of reconstruction error

We used the n-sigma (eq. 2) threshold approach to evaluate the novelty detection performance. With $n = 4$, we obtained 100% detection accuracy on the unseen signals. However, it provided 1.58% FAR on the known signals.

C. Clustering performance

After the novel signals are detected using the reconstruction method, we perform clustering. Prior to clustering, we perform normalization to remove the mean and scale to unit variance using the StandardScaler package from Scikit-learn. Afterwards, we use the RBF kernel PCA to reduce the feature dimension and obtain the key features in 2D, which is presented in Fig. 10. For better visualization, we used different colors for different transmission sources. From the figure, it can be clearly understood that the unseen drone signals can be differentiated using a simple clustering algorithm.

As discussed earlier, we used the DBSCAN to perform clustering. We varied the number of unseen signals to evaluate the clustering performance. The expected and predicted numbers of clusters are plotted in Fig. 11. The clustering algorithm provided an accurate prediction for different numbers of unseen drone signals.

D. Performance comparison with other frameworks

We compared the novelty detection performance of our framework against the SoA algorithms such as Saife [13], GAN [14], OSVM, IFO [19] and LODA [20]. For a given range of thresholds, we calculated the detection accuracy on the unseen drone signals and the FAR on the known signals. As we decrease the threshold, the probability of FAR for the known signals increases and the detection accuracy of

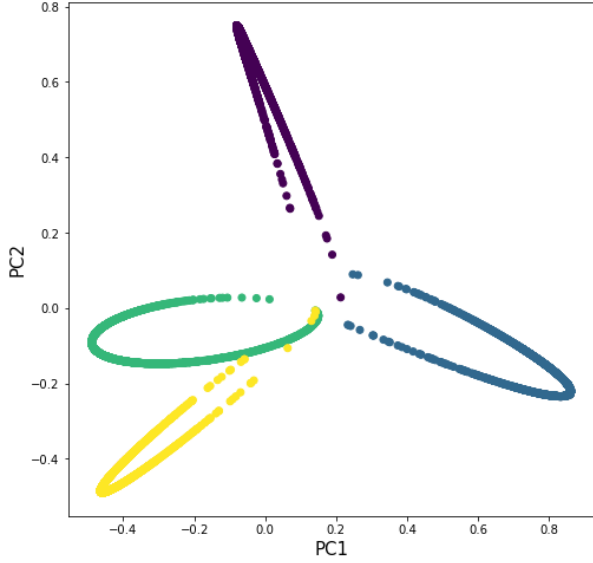


Fig. 10: Plot of two principal components of the PCA test result; Different signals are indicated with different colors.

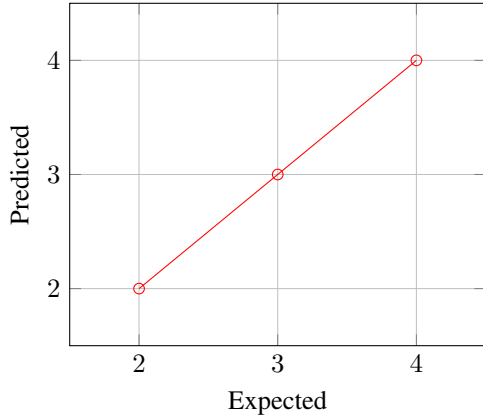


Fig. 11: Expected vs predicted number of clusters by the DBSCAN method. The clustering predictions were averaged and verified with 5000 trials.

the unseen signal also increases. The detection accuracy over the FAR for all frameworks is plotted in Fig. 12. With our proposed framework, we obtained 100% novelty detection accuracy at 1.04% FAR on the known signals. Saife provided a close novelty detection performance compared to our AE-based model. It provided 100% novelty detection accuracy at 3.81% FAR. The IFO and OSVM provided similar performances. They provided 100% novelty detection accuracy at 25.85% and 27.45% FAR, respectively. LODA provided a poor performance compared to the other tested frameworks. Similarly, the GAN framework also provided poor novelty detection performance. In this test, we used the GAN model with a single output and sigmoid activation on the final layer. Please note that the evaluation was performed using the higher dimensional input (i.e. the IQ dataset) for all frameworks, not from the feature space.

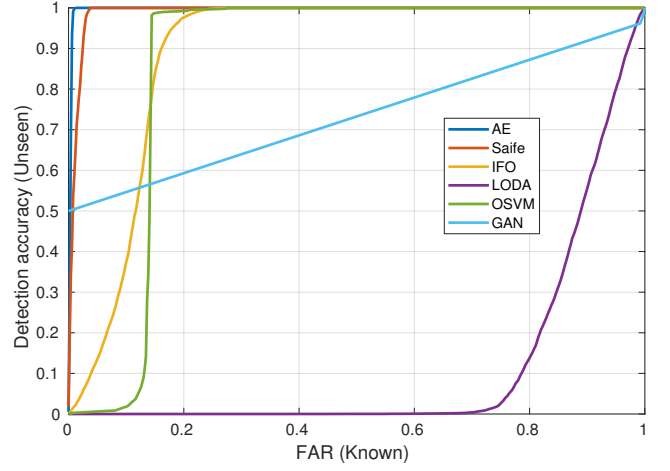


Fig. 12: Performance comparison with other SoA frameworks.

IX. DISCUSSION AND REMARKS

Novelty detection in the Frequency domain: The novelty detection was also tested in the frequency domain using the spectrogram matrix and Power Spectral Density (PSD) vector separately. We obtained poor novelty detection performance using only the frequency domain information. Therefore, in this study, the evaluation was conducted using the IQ vector.

Novelty detection using an AAE: A few studies have reported that the discriminator's score of an AAE can be used to detect unseen signals. We have also tested this during our study. We obtained an unreliable novelty detection performance using the discriminator's score.

Furthermore, we compared the reconstruction-based novelty detection performance of an AAE with our proposed framework. We did not observe any improvement in the novelty detection performance with the use of discriminators.

Novelty clustering without additional features: We have also tested novelty clustering without any additional features (i.e. bandwidth and dwell time). This test was performed using the RADIOML 2018.01A dataset [16]. During this test, we used the features ($\mathbf{z}$) generated by an AE or an AAE framework for clustering. However, even with a ResNet or ResNext-based framework, we did not achieve a good performance. We will study this in depth in the future to investigate the possibility of unseen signal clustering without any additional features.

X. CONCLUSION AND FUTURE WORKS

In this paper, we presented an AE-based framework for known drone signal protocol classification and unknown drone signal detection. In addition, we demonstrated the clustering performance using the extracted features from novel signals without any available prior information. The evaluation was performed using popular commercial drone signals. The classification was performed in a semi-supervised manner and we obtained 97.4% classification accuracy with only 10% labelled samples. The novelty detection was performed in an unsupervised manner and we obtained 100% detection accuracy at 1.04% FAR.

REFERENCES

- [1] G. De Cubber, "Explosive drones: How to deal with this new threat?" in *International workshop on Measurement, Prevention, Protection and Management of CBRN Risks (RISE)*, Belgium, 04 2019.
- [2] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, and T. Vu, "Investigating cost-effective rf-based detection of drones," in *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, ser. DroNet '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 17–22. [Online]. Available: <https://doi.org/10.1145/2935620.2935632>
- [3] P. Stoica, S. Basak, C. Molder, and B. Scheers, "Review of counter-uav solutions based on the detection of remote control communication," in *2020 13th International Conference on Communications (COMM)*, 2020, pp. 233–238.
- [4] M. Al-Sa'd, A. Al-Ali, T. Khattab, and A. Erbad, "Rf-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Generation Computer Systems*, vol. 100, 05 2019.
- [5] S. Al-Emadi and F. Al-Senaïd, "Drone detection approach based on radio-frequency using convolutional neural network," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 29–34.
- [6] S. Basak and B. Scheers, "Passive radio system for real-time drone detection and doa estimation," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2018, pp. 1–6.
- [7] S. Basak, S. Rajendran, S. Pollin, and B. Scheers, "Drone classification from rf fingerprints using deep residual nets," in *2021 International Conference on Communication Systems and NETWORKS (COMSNETS)*, 2021, pp. 548–555.
- [8] —, "Combined rf-based drone detection and classification," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 1, pp. 111–120, 2022.
- [9] S. Subramaniam, T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Online outlier detection in sensor data using non-parametric models," in *Proceedings of the 32nd International Conference on Very Large Data Bases*, ser. VLDB '06. VLDB Endowment, 2006, p. 187–198.
- [10] A. Gritsenko, Z. Wang, T. Jian, J. Dy, K. Chowdhury, and S. Ioannidis, "Finding a 'new' needle in the haystack: Unseen radio detection in large populations using deep learning," in *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019, pp. 1–10.
- [11] V. Hautamaki, I. Karkkainen, and P. Franti, "Outlier detection using k-nearest neighbour graph," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, vol. 3, 2004, pp. 430–433 Vol.3.
- [12] N. Tandiya, A. Jauhar, V. Marojevic, and J. H. Reed, "Deep predictive coding neural network for rf anomaly detection in wireless networks," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, pp. 1–6.
- [13] 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.
- [14] D. Roy, T. Mukherjee, M. Chatterjee, and E. Pasilio, "Detection of rogue rf transmitters using generative adversarial nets," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–7.
- [15] A. Baset, C. Becker, K. Derr, S. Ramirez, S. Kasera, and A. Bhaskara, "Towards wireless environment cognizance through incremental learning," in *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2019, pp. 256–264.
- [16] 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, Feb 2018.
- [17] M. Abadi, A. Agarwal *et al.*, "TensorFlow: Large-scale machine learning on heterogeneous systems," 2015, software available from tensorflow.org. [Online]. Available: <https://www.tensorflow.org/>
- [18] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *CoRR*, vol. abs/1412.6980, 2015.
- [19] F. T. Liu, K. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," *ACM Transactions on Knowledge Discovery From Data - TKDD*, vol. 6, pp. 1–39, 03 2012.
- [20] T. Pevný, "Loda: Lightweight on-line detector of anomalies," *Machine Learning*, vol. 102, 07 2015.



Sanjoy Basak received the M.Sc. degree in electrical engineering and information technology from Karlsruhe Institute of Technology, Karlsruhe, Germany, in 2016. He joined the Royal Military Academy, Belgium as a Researcher in 2016, where he is currently pursuing a joint doctoral study in association with KU Leuven in the Department of Electrical Engineering since 2019. His research interests include deep learning algorithms for wireless signal detection and classification.



Sreeraj Rajendran received the master's degree in communication and signal processing from the Indian Institute of Technology Bombay, India, in 2013, and the Ph.D. degree from KU Leuven, Belgium, in 2019, where he is a Post-Doctoral Researcher with the Networked Systems Group. In 2013, he was a Senior Design Engineer with the Baseband Team, Cadence (Tensilica). He was also an ASIC Verification Engineer with Wipro Technologies from 2007 to 2010. His main research interests include machine learning algorithms for wireless spectrum awareness and low power wireless sensor networks.



Sofie Pollin (Senior Member, IEEE) received the Ph.D. degree (Hons.) from KU Leuven, Leuven, Belgium, in 2006. From 2006 to 2008, she continued her research on wireless communication, energy-efficient networks, cross-layer design, coexistence, and cognitive radio at UC Berkeley. In November 2008, she returned to IMEC, Leuven, to become a Principal Scientist in the Green Radio Team. Since 2012, she has been a tenure track Assistant Professor with the Department of Electrical Engineering, KU Leuven. Her research centers around networked systems that require networks that are ever more dense, heterogeneous, battery-powered, and spectrum constrained. Prof. Pollin is a fellow of the BAEF and Marie Curie.



Bart Scheers was born in Rumst, Belgium, in November 1966. He received the M.S. degree in engineering, with a specialisation in communication from the Royal Military Academy, Brussels, Belgium in 1991 and a joint Ph.D. degree in 2001 from the Université catholique de Louvain, Ottignies-Louvain-la-Neuve, Belgium/Royal Military Academy, where he presented his Ph.D. dissertation on the use of ground penetrating radars in the field of humanitarian demining. After his studies, he was an Officer in a territorial signal unit of the Belgian Army. In 1994, he was an Assistant in the field of signal processing with the Royal Military Academy, where since 2003, he has been a Military Professor with the Communications Information Systems and Sensors (CISS) department, and is also the Director of the research unit on radio networks. His current domains of interest are mobile ad hoc networks (layers 2 and 3), cognitive radio, and internet of things.