Privacy-aware Deep Learning based Localization of Spectrum Violators

Chibuikem Ezemaduka
Electrical, Computer, and Systems Engineering
Rensselaer Polytechnic Institute
Troy, NY, USA
ezemac@rpi.edu

Alhussein A. Abouzeid
Electrical, Computer, and Systems Engineering
Rensselaer Polytechnic Institute
Troy, NY, USA
abouzeid@ecse.rpi.edu

***Abstract*—In spectrum sharing environments such as the Citizens Broadband Radio Service (CBRS), spectrum "violators" are secondary users that transmit without permission from the spectrum manager and could therefore cause harmful interference to the primary user, such as a radar, through their illegal transmissions. In such systems, it is desirable to detect the geographic locations of such violators without revealing the location, i.e. privacy, of the primary user. In this paper we propose a privacy-aware violator localization algorithm based on deep learning. In this approach, data collected at sensors are processed in a privacy-aware manner using a Generative Adversarial Network (GAN) based algorithm, and relayed to the centralized spectrum manager, e.g., the Spectrum Access System (SAS). The spectrum manager then detects and geographically localizes the violators based on the received data, using an encoder-decoder Convolutional Neural Network (CNN). We evaluate the proposed solution for a CBRS setting and show that it is able to achieve localization error of only 14 meters when using the GAN processed data for localization. Results also show that it achieves reconstruction error of at most 20% at very low Signal-to-Noise (SNR) ratio of 10 dB at a sensor.**

I. Introduction

Dynamic Spectrum Access (DSA) has been proposed as a solution to the spectrum scarcity problem [1]. DSA typically involves secondary users opportunistically accessing a licensed spectrum owned by a primary user (PU) without causing harmful interference to the activity of the PU. Spectrum access can be governed by a centralized spectrum manager which is responsible for resource allocation to the secondary users while protecting the primary user from interference. The spectrum manager can control access by allocating spectrum access to the secondary users only when the PU is inactive in the channel and restricting access once the PU is determined to be active. An example is the United States Citizen Broadband Radio Service (CBRS) [2] in which the Spectrum Access System (SAS) is responsible for providing secondary users with access to channels in the 3.5 Ghz band only when the government incumbent is deemed as inactive by deployed sensors (e.g., measurements from Environmental Sensing Capability (ESC) sensors).

A key threat to the operation of such a spectrum sharing system is spectrum violators, who are secondary users that transmit in the channel without permission from the spectrum manager, and could therefore cause harmful interference to the PU through their illegal transmissions. The spectrum violators may or may not be registered with the spectrum manager. It is important that such violators are identified and located as part of a spectrum enforcement process to protect the PU and ensure smooth operation of the system. Spectrum enforcement is currently done manually by the Federal Communications Commission (FCC)'s Enforcement Bureau and is time consuming and expensive [3]. To automate the enforcement process, the spectrum manager can achieve localization of violators by using spectrum data of active transmissions in the channel measured by available sensors. Such process however constitutes a problem given that, since the PU is active in the channel together with the violators, the PU signal is also observed together with that of the violators' and shared with the spectrum manager. The collection of spectrum data at the spectrum manager entails a threat to the PU's information privacy and can even lead to compromise of the PU's location during the violator localization process. Such privacy violation is unacceptable in DSA systems such as the CBRS, in which the Federal Communication Commission (FCC) protects the incumbent's privacy by allowing the (ESC or other) sensors

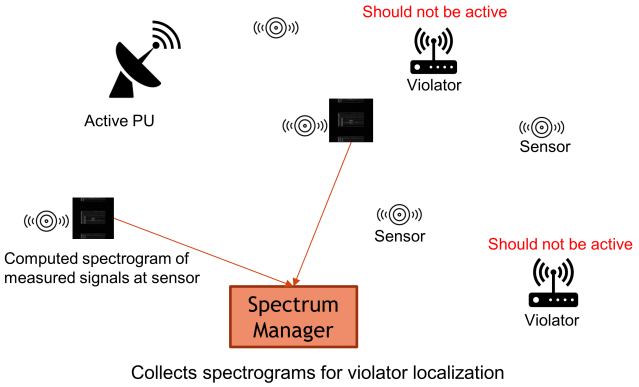


Fig. 1: Problem setting showing the violators transmitting at the same time as the PU. The collection of spectrograms at the spectrum manager constitute a threat to the PU's privacy as they contain implicit PU information together with that of the violators. The PU's information needs to be "hidden" before the spectrograms are sent to the manager.

to only report the presence of the PU and strictly prohibits any form of transmission of PU operating information from the sensors to the SAS in the rule: "*Ensure that the ESC operates without any connectivity to any military or other sensitive federal database or system and does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC*" [4]. The FCC also requires that the incumbent's location remains unknown to all system entities at all times.

Our objective in this work is therefore to develop a method for geographically localizing spectrum violators in a centralized spectrum sharing system without revealing the primary user's location information (henceforth termed PU privacy in this paper). Specifically, we propose a deep-learning based method to intelligently protect the privacy of the PU while localizing violators even when the PU is *non-informing*, i.e., even if the PU does not communicate with the spectrum manager. Our method consists of two stages in which we first employ a Generative Adversarial Network (GAN) to intelligently "hide" PU information from measured spectrum data at the sensors in the form of spectrograms, and then use the modified spectrograms at the spectrum manager to localize violators. Our problem setting is shown in Fig. 1. We evaluate our method in the context of the CBRS system, where we localize violators in the form of LTE transmitters that transmit when the incumbent (government) radar is active while hiding the radar information. To the best of our knowledge, our work is the first to address the problem of protecting PU privacy during localization of spectrum violators in a spectrum enforcement process. The specific contributions of our paper are:

- We treat the novel problem of protecting the PU's privacy while geographically localizing spectrum violators in a centralized spectrum sharing system by proposing a two-stage deep learning based approach.
- In the first stage we propose a method that employs a Generative Adversarial Network (GAN) to hide PU information from measured spectrograms at the monitoring sensors before they are sent to the spectrum manager. We design the problem as an image-to-image translation task.
- At the second stage, we propose a deep learning based localization method that uses spectrogram input through an encoder-decoder CNN to localize active violators in a shared spectrum area.
- We apply our proposed approach to the CBRS system and provide results from our evaluation.

The rest of the paper is organized as follows. In Section II we provide an overview of the related work. In Section III we formally formulate our problem and its setting. The solution is presented in Section IV and its application for a CBRS scenario is presented in Section V. Section VI provides a performance evaluation of the spectrum enforcement solution.

II. Related Work

Several works have treated multiple transmitter localization using only received signal strength (RSS) measured at deployed sensors for localization. The solutions in [5] and [6] use particle swarm optimization and a quasi expectation-maximization algorithm, respectively, to find the transmitter locations. They both require prior knowledge of the number of transmitters and their transmit powers for their methods. A multiple transmitter localization problem is solved in [3] by finding the local maxima of aggregate received power on sensors to identify the number of transmitters and then reduce the problem to a set of single transmission localization tasks based on their proximity to sensors with the local maxima. A positioning system equipped unmanned aerial vehicle (UAV) with uniform linear array and beam steering capability is used in [7] to collect RSS readings which are then used to create score maps. K-means clustering and Gaussian mixture model fitting methods are applied to the score maps to localize multiple non-collaborative transmitters. The problem is approached using two convoluted neural network layers in [8]. The first layer to output the number of transmitters and second to output the locations of the transmitters. Their work requires prior knowledge of the maximum number of transmitters to be localized in order to build the CNN. Similarly, a CNN is also used in [9] but their model employs only one network compared to [8] and does not require prior knowledge of the number of transmitters. They treat the output of the CNN as a heat-map regression problem rather than coordinate regression. Another work that uses a deep learning approach is [10] which frames the multi-transmitter localization problem as a computer vision problem. A different approach is adapted in [11] which performs blind source separation of the sensor RSS values. Their method performs the blind source separation not at the receivers but at the fusion center and requires the sensors to only transmit their measured RSS values. Although the aforementioned works generally treat localizing transmitters in a given region, they do not consider localization in a shared spectrum system which has different types of users - primary and secondary. Such criteria are considered by [12] and [13] which localize unauthorized transmissions in the presence of a dynamically changing set of authorized users in a shared spectrum system. It is suggested in [12] that a framework of detecting all transmitters and then comparing with the known locations and power of the authorized users is unlikely to be effective in a wide environment where the number of authorized users can be large. They solve the localization problem by using a maximum a-posteriori approach in which they determine the locations of the unauthorized transmitters by selecting the hypotheses with the highest probability. The work in [10] is extended by [13] to consider the context of a shared spectrum system with active authorized users. Knowledge of the locations and operating information of the authorized PUs and SUs is required by both [12] and [13] in order to separate and localize unauthorized transmitters. Their approaches are not applicable in shared spectrum systems

where due to privacy constraints, prior knowledge or revelation of the location and operational information of the PU and even in some cases SUs is prohibited, which is the case considered in this paper.

Our work differs from the aforementioned works in that we consider privacy constraint in which the PU's operating information needs to be hidden from the system during localization of the unauthorized transmissions. We propose a deep learning based localization approach to handle intricacies in the problem such as the complex wireless environment, unknown number of unauthorized transmitters (violators) together with their unknown operating parameters and distributions, and also a non-informing PU which does not communicate with the spectrum manager. Additionally, we use spectrograms in which we have hidden the PU's information as input data to our localization method rather than just average RSS values. Spectrograms enable us to exploit the notable performance of CNN-based models on image data and learn important variations in the time-frequency representation of a signal. Deep-learning based works that have used spectrograms for identifying unauthorized transmissions in a shared spectrum include [14] who although treat identification of unauthorized 5G and LTE signals together with radar in the CBRS, but do not consider geographically localizing the violators or protecting the PU's privacy. Spectrograms are also used in [15] who use a GAN-based approach like we do but focus on detecting anomalous jamming signals and do not localize them.

Some other works have also considered preserving the PU's location privacy in a shared spectrum system. The works in [16], [17], [18], [19], [20], [21], [22], [23], [24], [25] treat scenarios where the PU's privacy can be compromised through SU queries to the spectrum database or resource allocation to the SUs. The CBRS case is considered in [26] where the safe zone information sent from the ESCs to SAS can compromise the PU privacy. In [27], a privacy preserving centralized DSA system is proposed that protects the PU and SU operation data during the spectrum allocation process. Different adversary techniques and obfuscation strategies that can defend against them are analyzed by [28]. Another work, [29] creates a generalized model in which privacy can be optimized irrespective of the type of adversary inference attack. In [30] the PU hides its location by altering its transmission patterns. However in our work, the PU is not required to change its behavior to achieve privacy (as applicable in systems like the CBRS). None of the aforementioned works that treat PU location privacy consider the scenario where the PU's privacy may be compromised due to localization of unauthorized transmissions in the system.

It should also be noted that some works such as [31], [32], [33], [34], [35] have treated the problem of detecting spectrum misuse by using spectrum permits and authentication of transmitters. However, they do not consider localization of the offenders. Spectrum permits are outside the scope of our work and our aim is not just to detect misuse but to localize spectrum violators in a shared spectrum system. In the next sections, we formulate the problem and outline our proposed solution.

III. Problem Setting

In a given region, we consider a centralized spectrum sharing system in which a spectrum manager is responsible for spectrum access and resource allocation to secondary users (SUs). The incumbent of the shared frequency band is a non-informing primary user (PU) that does not explicitly communicate/coordinate with the spectrum manager. The spectrum manager authorizes registered SUs to transmit in a channel only if the PU is not active. Monitoring sensors are deployed in the region to constantly detect the activity status of the PU. We do not treat the setting in which the PU's activity is controlled by the spectrum management system as this is already handled extensively in literature [36], and does not address the case of interest in this paper which is the protection of PU information. During the period the PU is active, there could exist a number of SUs called *violators* who illegally transmit simultaneously with the PU. Let $V = \{v_1, ..., v_P\}$ denote the set of unknown location coordinates of P violators where v_p is the $[\theta_1, \theta_2]$ coordinate of the pth violator. The violators may or may not have been registered with the spectrum manager. To protect the PU's operation, the deployed sensors sense the channel for active transmissions and send the sensed data to the spectrum manager to be used to locate the violators if present. Let $S_i \in \mathbb{R}^{N \times M}$ denote the time-frequency representation of the received signal at the ith sensor which is computed by taking the short time Fourier transform (STFT) of the in-phase/quadrature I/Q samples. N and M are the number of time slots and frequency bins respectively. Since the PU and violators transmissions are both observed at the sensor, the sampled signal is a combination of the PU's signal, violators' signal, and receiver noise. Let S_{i_V} denote the time-frequency representation of the violators' signals plus noise at the ith sensor, and let $S_{i_{PU}}$ denote the PU's signal. Thus,

$$S_i = S_{i_V} + S_{i_{PU}}. \tag{1}$$

where S_i can be mapped to pixel values and visually represented as a spectrogram. The spectrum manager uses the collection of spectrograms $\{S_i\}_{i=1}^K$ from K sensors to localize active transmitters in order to find violators in the region. However, $\{S_i\}_{i=1}^K$ constitutes a privacy threat to the PU as it contains the PU's transmission information which should be kept hidden and could also lead to the spectrum manager revealing the PU's location together with that of the violators during its localization process. Therefore, the ith sensor, without communicating with other sensors, needs to hide $S_{i_{PU}}$ from its observation S_i, and send only the violators' data S_{i_V} to the spectrum manager.

Specifically, we have two objectives

1) Make an estimate $\hat{S}_{i_V}$ at the ith sensor of the unknown true violators' information which is then sent to the spectrum manager. $\hat{S}_{i_V}$ should be as close as possible to S_{i_V} so that the accuracy in estimating the violators' locations is not severely affected.

2) Use $\{\hat{S}_{i_V}\}_{i=1}^{K}$ at the spectrum manager to make an accurate estimate, $\hat{V} = \{\hat{v}_1, ..., \hat{v}_P\}$ of V.

It should be noted that the spectrum manager has no prior knowledge of the number of violators, if any, or their operating parameters.

IV. Violators Localization

We propose a two-stage deep learning based approach to achieve accurate violator localization without revealing PU information, as outlined below.

A. Hiding PU information at sensors

Motivated by the notable success of deep learning on image related tasks, we formulate the task of hiding the PU's information as an image-to-image translation problem. We are interested in translating the spectrogram of observed signal, S_i, which contains both the PU and violators' information, into a spectrogram $\hat{S}_{i_V}$ which contains only the violators' information. We employ a Generative Adversarial Network (GAN) [37] for this task. GANs, due to adversarial training, are powerful in learning the distribution of input image data and generating realistic images that follow the same distribution. In particular, we use a specific GAN variant, the Conditional GAN (cGAN), which enables a GAN's output image to be conditioned on particular input data. cGAN has been used successfully for image-to-image translation tasks [38]. Our cGAN takes as input condition the observed S_i spectrogram, and then outputs a new spectrogram, $\hat{S}_{i_V}$. For training the cGAN, a training dataset is formed of spectrogram samples $\{x, y\}$. x represents the observed spectrogram, S_i at a sensor which has both the PU and violators' signal while y represents the corresponding spectrogram S_{i_V} which has only the violators' signal.

The cGAN learns by training on the min-max objective

$$\min_G \max_D (\mathbb{L}_{GAN} + \mathbb{L}_{RECONST}) \tag{2}$$

where

$$\mathbb{L}_{GAN} = \mathbb{E}_{x,y}\left[\log D(x, y) + \log(1 - D(x, G(x))\right] \tag{3}$$

and

$$\mathbb{L}_{RECONST} = \mathbb{E}_{x,y}\|y - G(x)\|_1 \tag{4}$$

where $D(x, \cdot)$ is the discriminator D's output which is the probability that data sample $\{x, \cdot\}$ is real and drawn from the true data distribution (i.e., it is not produced by the generator), $\mathbb{L}_{GAN}$ is the adversarial loss through which in the min-max game, D learns to distinguish between the real combination of spectrograms $\{x, y\}$ and fake combination, and $\{x, G(x)\}$ and $G(x)$ is the spectrogram constructed by the generator G. Concurrently, G also learns to produce realistic spectrograms so as to fool the discriminator into classifying them as real. The L1 loss, $\mathbb{L}_{RECONST}$, guides G to construct spectrograms $G(x)$ that are close as possible to the ground truth y. The model G^* where

$$G^* = \arg\min_G \max_D (\mathbb{L}_{GAN} + \mathbb{L}_{RECONST}) \tag{5}$$

is then distributed to each of the sensors. During online operation, the ith sensor inputs its computed spectrogram S_i to G^* which reconstructs it and then outputs $\hat{S}_{i_V}$ which is then sent to the spectrum manager. This operation is replicated at all the sensors.

B. Localizing violators at the spectrum manager

The spectrum manager collects $\{\hat{S}_{i_V}\}_{i=1}^{K}$ from all K sensors and attempts to localize the violators using the received spectrograms. Inspired by [13] [1], we also frame the localization task as a deep learning image-to-image translation task and use a similar approach in the labeling of the transmitter locations as an image[2].

We propose an encoder-decoder U-Net Convolutional Neural Network (CNN) architecture [39] would be suitable for the translation task. Due to the nature of our problem setting, we use spectrogram inputs and translate received spectrograms from the sensors to an image that encodes the violator locations. For the CNN training, the true violator locations that serve as a label to a set of collected spectrograms are represented as a grayscale image. We assume that the spectrum area is divided into grid cells where the centers of the cells are represented as pixels in the image. Instead of just assigning a pixel representing the exact location as a value of one and the others as zeros, we represent a violator location by a 5x5 box of pixel values that follow a Gaussian distribution as employed in [13] and [40] where the center pixel is the distribution's peak that corresponds to the exact violator location and the surrounding pixels have values according to the distribution's parameters. The aim of using a Gaussian representation of pixels rather than a single pixel to represent one location is to prevent gradient under-flows [40]. We use an 8-bit unsigned integer (uint8) image and as such select the value of the center pixel (Gaussian peak) as 255 with the remaining pixels in the 5x5 box having values following a standard deviation of 0.9. The rest of the pixels in the image that are not associated with any violator location are represented as zeros. During online operation, the CNN model which we call F^* takes as input $\{\hat{S}_{i_V}\}_{i=1}^{K}$ which are stacked in the form of a 3D multi-channel image where each channel corresponds to the spectrogram received from a particular sensor. F^* then outputs an image that has the violator locations in it. To obtain the values of the estimated locations from the output image, we use a simple method as described in [13] in which we locate pixels in the image that have local maximum values that are above a defined threshold and are higher than the values of the surrounding pixels in a chosen radius. We assign these local maximum pixels as the Gaussian peaks i.e. the estimated violator locations. F^* is trained using the L2 loss which is the

[1] [13] solves the localization problem as a computer vision task of translating scalar RSS values at sensors into an image of transmitter locations, which accommodates for not knowing in advance, the number of unauthorized transmitters to be located. Since we have no prior knowledge of the number of violators, we also represent the violator locations as an image, but instead employ spectrogram data as our input.

[2] As mentioned in Section II, unlike [13], we do not require knowledge of the locations and operating information of the authorized PUs and SUs.

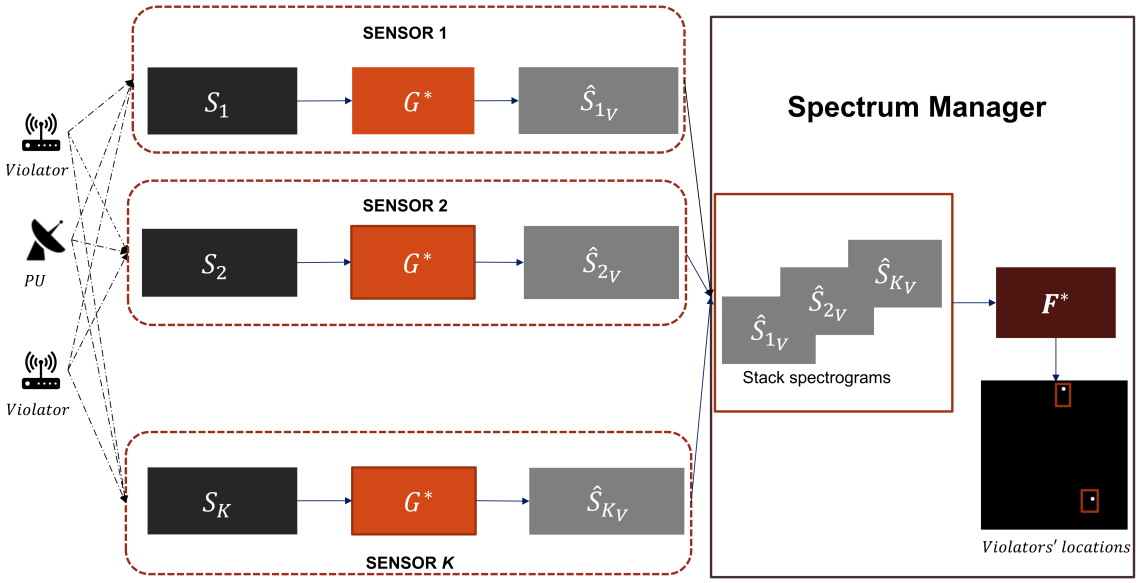


Fig. 2: Workflow showing the online operation of the system. The ith sensor computes spectrogram S_i from its observed signal and then feeds it to the trained GAN model G^* which outputs a reconstructed spectrogram $\hat{S}_{i_V}$ that has an estimate of only the violators' signals. $\hat{S}_{i_V}$ from all sensors are sent to the spectrum manager which stacks them as a 3D multi-channel image that is fed to F^* which then outputs a grayscale image of the estimated violators' locations.

mean squared error between the true violator locations image and the model's prediction at a pixel level. The workflow of the system is shown in Fig. 2.

V. Application to CBRS

We apply our proposed approach to the CBRS system. CBRS provides 3.55 to 3.7 GHz band in fifteen 10 MHz channels for opportunistic spectrum access by the Priority Access License (PAL) and General Authorized Access (GAA) secondary users. The incumbent, i.e., PU in this setting, is the US government radar. In the CBRS, when the radar has been detected as active by the sensors, FCC rules state that the Spectrum Access System (SAS) should require all SUs to vacate from the channel of interest. We classify any users that disobey this access policy as violators and desire to localize them if present. To enable localization of the violators, the sensors can sense the channels in which the radar's presence was identified, and then compute spectrograms of the measured signals which are to be sent to the SAS. We assume that all the violators operate in the same channel (this could be generalized in subsequent work). A violator could be registered with the SAS or unregistered. The SAS could compare the estimated violator locations with that of its registered users to determine if a violator is an internal actor (registered) or external (unregistered) which may require further investigation. To protect the radar's privacy, the radar information has to be hidden from the spectrograms generated at the sensors before they are sent to the SAS to be used for localization. We describe our dataset generation and model training below.

A. Dataset generation

We assume for the sake of this evaluation case study of CBRS that the secondary users are LTE. We use MATLAB to generate two datasets for the two deep learning tasks. For the first task of hiding the PU information at a sensor, we generate a dataset of spectrograms that are random combinations of LTE signals with radar signal in randomized CBRS channels. Each generated spectrogram is labeled with a corresponding ground truth spectrogram that has only the LTE signals without the radar. Each spectrogram is a grayscale image with size 128 x 128 pixels. Since we focus on a single CBRS channel which is 10 MHz wide, The LTE signals are randomly generated in Time Division Duplex (TDD) mode with 10 MHz bandwidth of varying transmit powers. The channel is sampled with 10 MHz sampling rate for a duration of 20 ms for each spectrogram sample. The radar signals are generated using the National Institute of Standards and Technology (NIST) tool for CBRS radar signal generation [41]. [41] generates the radar pulses according to the specifications in [42] for CBRS radar types classified on their type of pulse modulation. To prevent class imbalance, we apply a uniform number of each radar type in generating the dataset. These radar signals are combined with the LTE signals to mimic a channel that has the radar PU transmitting together with the LTE violators. We also include few spectrograms that have LTE only, radar only, or just noise signals to represent scenarios in which a sensor may measure only one of those signals due to its relative positioning from the true radar and violators locations.

For the localization task, we use location label images of size 128 x 128 which correspond in size to the spectrogram

images. Each pixel in the image represents the center of a grid cell of 10 m length and width in the spectrum sharing area and a violator can be located at any of the pixel locations. We position LTE transmitters randomly at cell centers in the area and then place ten uniformly distributed sensors which compute spectrograms of the signal they sample in the channel. A data sample in the localization dataset is a 3D multi-channel image that is a combination of the spectrograms received from all the sensors for a particular location configuration of LTE transmitters. We create $6,000$ different data samples using diverse random location configurations for various number of LTE transmitters (up to three transmitters). Each created data sample is labeled with an image of its ground truth location configuration as outlined in Section IV-B.

B. Training

For the two tasks, we train our models using the generated datasets. We use a training dataset of $10,000$ samples for the first task, and adopt the pix2pix GAN architecture with skip connections [38] for our training. We adopt pix2pix because it has been quite successful for various image-to-image translation tasks in different domains. We modify the architecture to enable it function with our spectrogram input size of 128 x 128 by removing one 512 filter convolutional layer from the encoder and another from the decoder. Instead of using 3 filters at the last layer, we use only one filter so that the model outputs a 1-channel grayscale image. We use a learning rate of 0.0002 and 0.0001 with the Adam optimizer to train the generator and discriminator respectively and train for 100 epochs.

For the localization task, as stated in IV-B, we choose to employ a U-NET architecture CNN model as it gives the best performance from our tests. Since the generator in the pix2pix architecture is essentially a U-NET encoder-decoder model with skip connections, we decide to use its architecture for the localization albeit with some modifications. Firstly, because we use a multi-channel input data of spectrograms from the 10 deployed sensors, our input image size becomes 128 x 128 x 10. We also do not normalize the uint8 image input before feeding it to the model as we observed that normalizing the input produces poor results. We also observed that a filter size of 3 x 3 at each convolutional layer performed better than the 4 x 4 size which is the default in pix2pix. Finally, rather than tanh, we use Relu as our activation function in the last layer with only one filter which results in a 1-channel output. The rest of the model is the same as that of the pix2pix generator. We train the model with a learning rate of 0.0001 with Adam optimizer for 100 epochs. In the next section we evaluate our approach and outline the results.

VI. Evaluation

We evaluate our method with three performance metrics: reconstruction error, localization error and cardinality error.

A. Reconstruction Error

The reconstruction error R_e is the percentage error between a sensor's estimate of the spectrogram with violators' only information and the ground truth. It is given as

$$R_e(\%) = \frac{|\hat{S}_V - S_V|}{T} \times 100 \tag{6}$$

where $\hat{S}_V$ and S_V are the GAN constructed output and ground truth of the spectrogram with only violators' information respectively. T is the total number of pixels in a spectrogram. The difference between the spectrograms is taken pixel wise with the pixels normalized to between 0 and 1 thereby making the maximum possible difference between two pixels to be 1. We evaluate our trained G^* model on test spectrogram samples that have LTE and Radar signals combined together. The test dataset is made up of $1,500$ samples for each of the five CBRS radar type [42].

In Fig. 3, we show the cumulative distribution function (CDF) for different signal to noise ratios (SNR) at a sensor for the different radar types. The combination of LTE and radar make up the sensed signal, while the noise is represented as additive white Gaussian noise (AWGN). For all the radar types, we observe that G^* performs better as the SNR increases which is expected because at a lower SNR, the model would have more difficulty in distinguishing the signals from noise which would increase the likelihood for error and as such have lower performance in estimating the true value of the LTE only spectrogram. As the SNR increases, the signals are better distinguished and G^* can produce a closer estimate of the LTE only spectrogram with the radar information filtered out. However, even at a very low SNR of 10 dB, we achieve the best performance of at most 20% error on all test samples for the PON1 radar which is currently the radar type deployed in the CBRS. Fig. 4 shows some visual examples of the GAN filtering process in which the radar information is hidden from the reconstructed spectrograms.

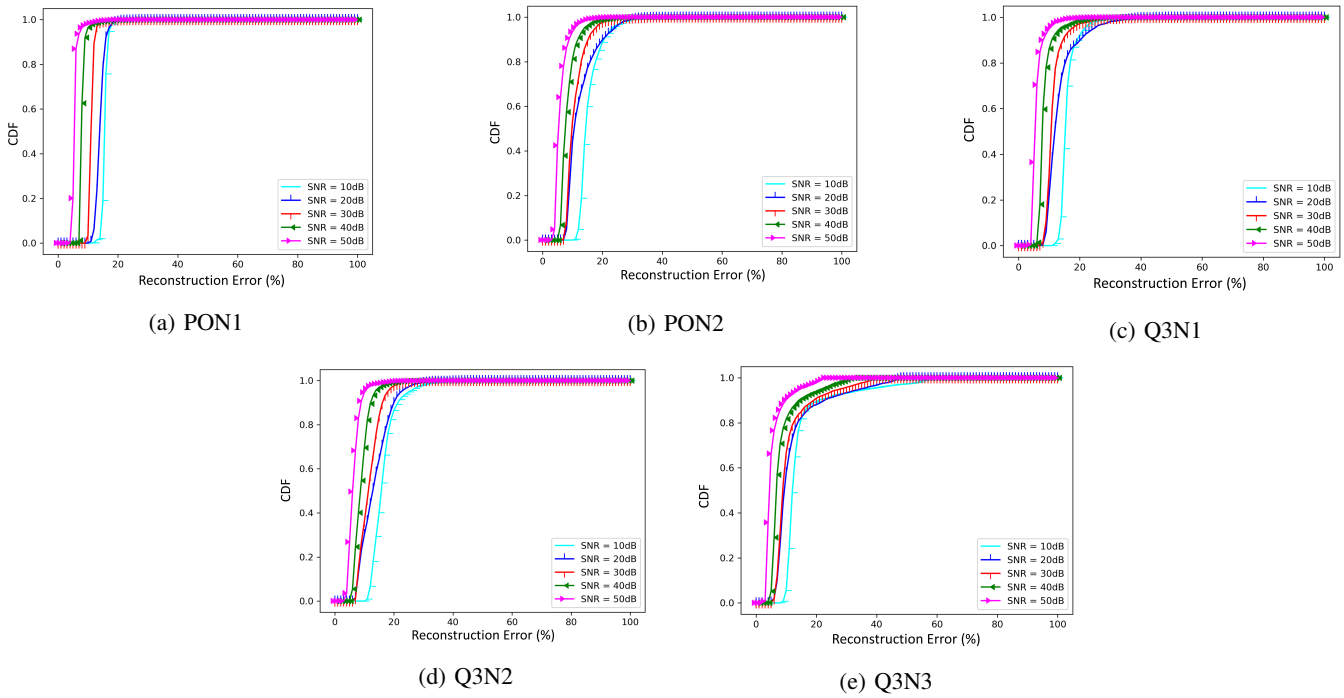
B. Localization Error

The localization error, L_e is the root mean squared error of the best mapping i.e. the mapping that results in the minimum error while considering all possible mappings between the estimated and true violators' locations [43]. It is given as:

$$L_e = \min_h \left(\frac{1}{B} \sum_{i=1}^{|V|} \sum_{j=1}^{|\hat{V}|} \|v_i - \hat{v_j}\|^2 h_{i,j} \right)^{\frac{1}{2}} \tag{7}$$

where h is a one-to-one mapping of estimated locations to the true locations. $h_{i,j} = 1$ if for mapping h, $\hat{v}_j$ is assigned as the estimate of v_i but 0 otherwise. B is the size of the mapping (number of one-to-one assignments in h) and is equal to $|\hat{V}| = |V|$ if the number of estimated and true locations match. If $|\hat{V}| \neq |V|$ then $B = \min\left(|\hat{V}|, |V|\right)$ and we consider the minimum error over all possible mappings of size B.

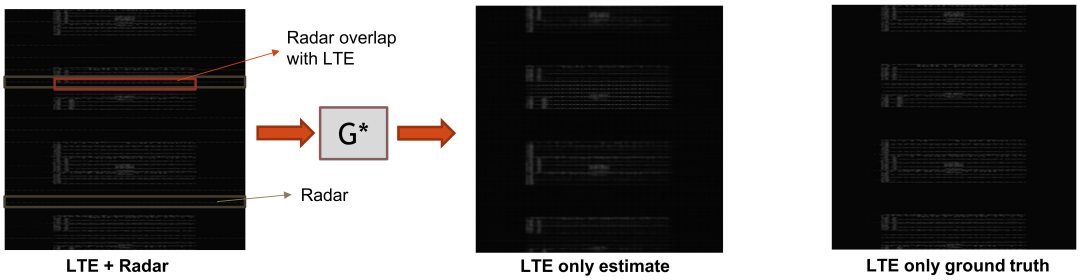
In Fig. 5, we show the localization error when the spectrum manager uses $\{\hat{S}_{iv}\}_{i=1}^{K}$ for localization compared to using



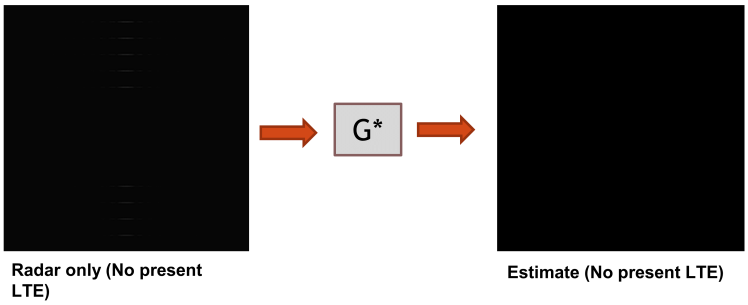
(a) PON1 (b) PON2 (c) Q3N1

(d) Q3N2 (e) Q3N3

Fig. 3: Cummulative Distribution Function (CDF) plot of the reconstruction error at different signal-to-noise ratios (SNR) for the five CBRS radar types



(a) Reconstruction of Q3N3 radar + LTE spectrogram



(b) Reconstruction of PON1 radar only spectrogram

Fig. 4: Figures showing the GAN reconstruction of a spectrogram at a sensor. In (4a), a sensor measures a spectrogram that has the Q3N3 radar type together with an LTE signal. The radar signal can be seen distributed horizontally across the spectrogram, at times overlapping with the LTE. The spectrogram has length of 20 ms and is 10 MHz wide but is depicted with some allowance at the sides to aid in visualization of the distinct signals. The GAN model G^* reconstructs the spectrogram to hide the radar information and produces an estimate of only the LTE information. The ground truth is also shown. In (4b), the measured spectrogram consists only of PON1 radar. LTE is not observed due to the relative position of the sensor from the transmitter. G^* hides the radar information and produces an output with just noise in it.

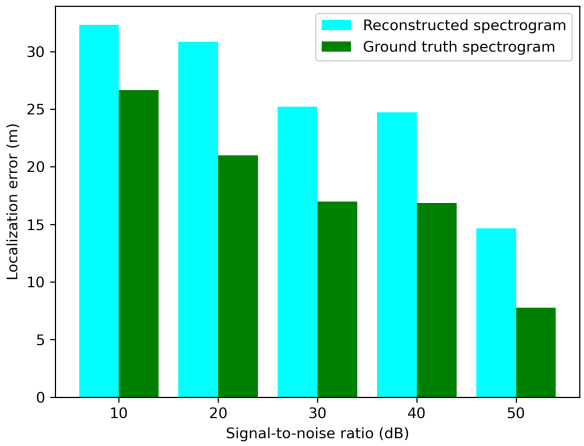


Fig. 5: Figure showing the localization error when the spectrum manager uses the reconstructed spectrograms received from the sensors, compared to when it uses the ground truth. The error is shown for different signal-to-noise ratios (SNR) at the sensors.

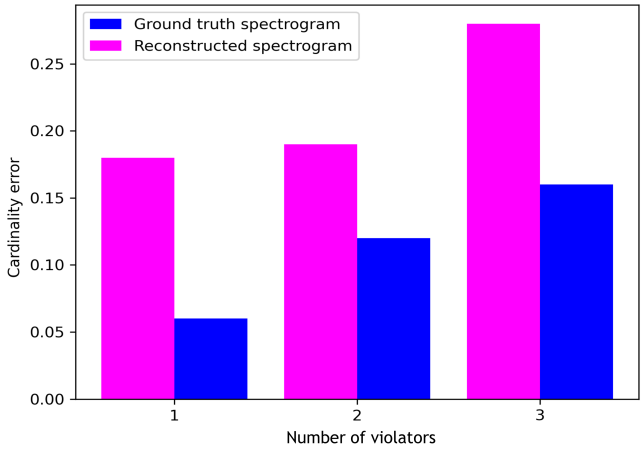


Fig. 6: Figure showing the cardinality error when the spectrum manager uses the reconstructed spectrograms, compared to the ground truth for different number of active violators. The spectrograms are measured at 50 dB.

$\{S_{i_V}\}_{i=1}^{K}$ for different SNR levels at the sensors. We simulate 100 trials in which the number of violators and their locations are randomized in the 1280 m x 1280 m sharing area together with a PON1 radar incumbent which is also placed at random locations. We set the maximum possible number of violators to be three. The localization error is averaged across all trials and scaled by 0.1, since each location (pixel) corresponds to a grid cell of 10 m. We observe that as expected, the error is higher when using the reconstructed spectrograms compared to using the ground truth for each SNR value. The error however decreases considerably as the SNR increases, with error of only 8 meters when using the ground truth and 14 meters when using the reconstructed spectrograms at an SNR of 50 dB.

C. Cardinality error

The Cardinality error, C_e is the fraction of time in which the estimated number of violators differs from the true value [3]. In Fig. 6, we observe that C_e, for a varying number of violators when using both the reconstructed and ground truth spectrograms, increases with the number of violators, which is intuitive as the likelihood of error in predicting the exact number of violators would be greater given a larger number.

VII. Conclusion and Future Work

In this paper we proposed a two-stage deep learning based approach for localizing spectrum violators while protecting the privacy (i.e., location) of the PU information in a spectrum sharing system. We evaluated our method in a CBRS setting where we used a GAN model in the first stage to hide the incumbent's radar information by reconstructing measured spectrograms at the sensors (termed ESC sensors in CBRS systems), such that the radar is filtered out (as much as possible) with only the original violators' information remaining. We used an encoder-decoder CNN at the second stage to localize the spectrum violators in the form of active LTE transmitters. The evaluation results show that the solution achieves a reconstruction error of at most 20% even at a very low SNR of 10 dB and localization error of only 14 meters while using the reconstructed spectrograms compared to an error of 8 meters when using the ground truth. For future work, it would be valuable to evaluate this approach on a physical testbed and real life CBRS data. We would also like to extend our method to a multi-channel scenario in which spectrum violators with different bandwidths are operating in different channels.

Acknowledgment

This material is based upon work supported in part by the National Science Foundation under grant number 2007454.

References

[1] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[2] Federal Communications Commission (FCC), "Amendment of the commission's rules with regard to commercial operations in the 3550-3650 mhz band," *Report and order and second further notice of proposed rulemaking*, 2015.

[3] M. Khaledi, M. Khaledi, S. Sarkar, S. Kasera, N. Patwari, K. Derr, and S. Ramirez, "Simultaneous power-based localization of transmitters for crowdsourced spectrum monitoring," ser. MobiCom '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 235–247. [Online]. Available: https://doi.org/10.1145/3117811.3117845

[4] Federal Communications Commission (FCC), "Title47/chapteri/subchapterd/part96," *Code of Federal Regulations*, 2015. [Online]. Available: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-D/part-96

[5] J. K. Nelson, M. U. Hazen, and M. R. Gupta, "Global optimization for multiple transmitter localization," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, 2006, pp. 1–7.

[6] J. K. Nelson, M. R. Gupta, J. E. Almodovar, and W. H. Mortensen, "A quasi em method for estimating multiple transmitter locations," *IEEE Signal Processing Letters*, vol. 16, no. 5, pp. 354–357, 2009.

[7] Z. Li, A. Giorgetti, and S. Kandeepan, "Multiple radio transmitter localization via uav-based mapping," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8811–8822, 2021.

[8] A. Zubow, S. Bayhan, P. Gawłowicz, and F. Dressler, "Deeptxfinder: Multiple transmitter localization by deep learning in crowdsourced spectrum sensing," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020, pp. 1–8.

[9] M. Lin, Y. Huang, B. Li, and Z. Huang, "Heatmap-based multiple co-channel transmitter localization with fully convolutional network," in *2021 International Applied Computational Electromagnetics Society (ACES-China) Symposium*, 2021, pp. 1–2.

[10] C. Zhan, H. Ghaderibaneh, P. Sahu, and H. Gupta, "Deepmtl: Deep learning based multiple transmitter localization," in *2021 IEEE 22nd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2021, pp. 41–50.

[11] E. Testi and A. Giorgetti, "Rss-based localization of multiple radio transmitters via blind source separation," *IEEE Communications Letters*, pp. 1–1, 2021.

[12] C. Zhan, H. Gupta, A. Bhattacharya, and M. Ghaderibaneh, "Efficient localization of multiple intruders in shared spectrum system," in *2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2020, pp. 205–216.

[13] C. Zhan, M. Ghaderibaneh, P. Sahu, and H. Gupta, "Deepmtl pro: Deep learning based multiple transmitter localization and power estimation," *Pervasive and Mobile Computing*, vol. 82, p. 101582, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119222000311

[14] N. Soltani, V. Chaudhary, D. Roy, and K. Chowdhury, "Finding waldo in the cbrs band: Signal detection and localization in the 3.5 ghz spectrum," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 4570–4575.

[15] 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.

[16] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, 2014, pp. 236–247.

[17] P. R. Vaka, S. Bhattarai, and J.-M. J. Park, "Location privacy of non-stationary incumbent systems in spectrum sharing," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.

[18] M. Liu, X. Zhou, and M. Sun, "Bilateral privacy-utility tradeoff in spectrum sharing systems: A game-theoretic approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 5144–5158, 2021.

[19] N. Rajkarnikar, J. M. Peha, and A. Aguiar, "Location privacy from dummy devices in database-coordinated spectrum sharing," in *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2017, pp. 1–10.

[20] A. M. Salama, M. Li, L. Lazos, Y. Xiao, and M. Krunz, "Privacy-utility tradeoff in dynamic spectrum sharing with non-cooperative incumbent users," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[21] A. Ben Mosbah, T. A. Hall, M. Souryal, and H. Afifi, "An analytical model for inference attacks on the incumbent's frequency in spectrum sharing," in *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2017, pp. 1–2.

[22] A. Robertson, J. Molnar, and J. Boksiner, "Spectrum database poisoning for operational security in policy-based spectrum operations," in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 382–387.

[23] X. Dong, T. Zhang, D. Lu, G. Li, Y. Shen, and J. Ma, "Preserving geo-indistinguishability of the primary user in dynamic spectrum sharing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8881–8892, 2019.

[24] S. Bhattarai, P. R. Vaka, and J.-M. Park, "Thwarting location inference attacks in database-driven spectrum sharing," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 2, pp. 314–327, 2018.

[25] A. Dimas, M. A. Clark, B. Li, K. Psounis, and A. P. Petropulu, "On radar privacy in shared spectrum scenarios," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 7790–7794.

[26] H. Li, Y. Dou, C. Lu, D. Zabransky, Y. Yang, and J.-M. J. Park, "Preserving the incumbent users' location privacy in the 3.5 ghz band," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2018, pp. 1–10.

[27] Y. Dou, K. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li, "p^2 - sas: Privacy-preserving centralized dynamic spectrum access system," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 1, pp. 173–187, 2017.

[28] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016, pp. 1–9.

[29] ——, "Optimizing primary user privacy in spectrum sharing systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 533–546, 2020.

[30] Y. Lin, Y. Ye, and Y. Yang, "Preserving incumbent user's location privacy against environmental sensing capability," in *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019, pp. 1–10.

[31] V. Kumar, H. Li, J.-M. J. Park, and K. Bian, "Crowd-sourced authentication for enforcement in dynamic spectrum sharing," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 625–636, 2019.

[32] A. Nika, Z. Zhang, B. Y. Zhao, and H. Zheng, "Toward practical spectrum permits," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 1, pp. 112–122, 2017.

[33] X. Zhang, P. Huang, Q. Jia, and L. Guo, "Cream: Unauthorized secondary user detection in fading environments," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2018, pp. 406–414.

[34] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," *IEEE Transactions on Mobile Computing*, vol. 17, no. 12, pp. 2925–2938, 2018.

[35] V. Kumar, H. Li, J.-M. J. Park, and K. Bian, "Enforcement in spectrum sharing: Crowd-sourced blind authentication of co-channel transmitters," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2018, pp. 1–10.

[36] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[37] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, p. 139–144, oct 2020. [Online]. Available: https://doi.org/10.1145/3422622

[38] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, "Image-to-image translation with conditional adversarial networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.

[39] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," in *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015*, N. Navab, J. Hornegger, W. M. Wells, and A. F. Frangi, Eds. Cham: Springer International Publishing, 2015, pp. 234–241.

[40] R. Ayyalasomayajula, A. Arun, C. Wu, S. Sharma, A. R. Sethi, D. Vasisht, and D. Bharadia, "Deep learning based wireless localization for indoor navigation," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3372224.3380894

[41] R. Caromi and M. Souryal, "Simulated radar waveform and rf dataset generator for incumbent signals in the 3.5 ghz cbrs band," *National Institute of Standards and Technology*, 2020.

[42] F. H. Sanders, "Procedures for laboratory testing of environmental sensing capability sensor devices," Institute for Telecommunication Sciences, Tech. Rep., 2017.

[43] J. Hoffman and R. Mahler, "Multitarget miss distance via optimal assignment," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 34, no. 3, pp. 327–336, 2004.