Radar Privacy Violation in Spectrum Sharing Systems Using Neural Networks

Huda Noman Obeid¹, Mohanad Al-Ibadi² and Hussein Ali Hussein Al Naffakh¹

¹Department of Medical Laboratory Techniques, University of Alkafeel, Najaf, Iraq  
²Department of Engineering Technical College of Al-Najaf, University of Al-Furat Al-Awsat Technical, Najaf, Iraq

Abstract. This paper presents the problem of interference management and radar privacy risks in shared spectrum scenarios between radar and communications systems. We propose a deep neural network that is designed and trained to reveal the location of the radar. The input of the network is a precoding matrix that a mobile terminal can use to transmit information via an uplink channel to a near-by base-station such that the amount of interference towards the radar is minimized while at the same time preserving the communications data rate above the required threshold. The results of this work suggest the need for a more complex precoder design procedures to protect the location of the radar in shared-spectrum systems. The results for detecting the radar location are compared to the available models, and we show an 92.05% improvement in detection capability in terms of the absolute error between the true radar location angle and the predicted angle, as measured with respect to the location of the mobile terminal in the communications system.

I. INTRODUCTION

Spectrum sharing between radar and communication systems is becoming a necessity to better utilize the available frequency spectrum, especially at sub-6 GHz band. Since both systems use the same frequency band to communicate, and in order to maintain good link quality, the interference arising from the shared spectrum needs to be minimized.

The literature of the shared spectrum systems is dominated by the attempts to find feasible solutions to the mutual interference problem arising in these systems, in addition to the radar privacy issues stemming from the known radar location that is required to design the interference mitigation algorithms.

A zero-forcing precoder has been proposed in [1] to eliminate the interference from the radar towards the communication receivers. The authors show that although this transmit precoder degrades the estimation performance of the radar target, the accuracy can be improved at the cost of non-zero interference at communication users.

The authors in [2] and [3] proposed two methods to reduce the effective interference power (EIP) between radar and communications shared-spectrum systems. In the first method, the authors proposed to design a transmit covariance matrix to minimize EIP, given that the sampling scheme of the radar is known, while keeping the average channel capacity and power budget of the communication system above a given threshold. In the second method, however, a joint transmit covariance matrix and radar sampling scheme was designed to further reduce the interference at the radar.

The authors in [4] proposed an iterative interference alignment approach to minimize the interference between the radar and communication systems within the shared frequency band, where the signal-to-interference-plus-noise (SINR) ratio of the radar system is maximized, in addition to maximizing the average sum-rate of the communications system. This goal was achieved by jointly optimizing the transmit and receive beamformers of the two shared systems via an alternating optimization procedure.

The authors in [5], two Reconfigurable Intelligent Surfaces (RISs) were used to enhance the communication signals and suppress the mutual interference between radar and communication systems. The authors proposed an algorithm to jointly optimize the beamforming of the RIS and radar and maximize the communications performance. In addition, they studied the role of radar transmit power level, where the communication channel determines the beamforming design of the shared system in high transmit power radars, while the mutual interference was minimized using the block coordinate descent method in low power radars.

* Corresponding author: huda.noman@alkafeel.edu.iq
In [6], the spectrum sharing between a full duplex multi-cell multi-user MIMO cellular system and a MIMO radar system was discussed, where the objective of the optimization problem was to maximize the rate of the communication system subject to power level constraints and interference constraint towards the radar.

In [7], the authors perform a joint optimization of the radar transmit precoder, the radar subsampling scheme, and the communication transmit covariance matrix to maximize the radar SINR and preserve the constraints on the communication capacity and power budgets. The authors show, via simulations, that their proposed scheme can enhance the performance of the shared spectrum systems.

In [8], the authors discussed the possibility of radar privacy violation by an adversary user using the precoding matrix designed for interference mitigation purpose. The authors show that the precoding matrix contains enough information about the radar direction that can be estimated using solely the observed precoder. On the same line of research, the authors in [9] proposed a machine learning based inference algorithm to infer the location of the radar based on the precoder matrix. In addition, in [10], a gradient enforcement based model was proposed to hide the identity of the radar that was otherwise be revealed using the precoder matrix as well.

In this work, starting from [9] and [10], we propose an artificial neural network (DNN) architecture to detect the radar location using the precoding matrix at the adversary user. The proposed DNN is trained using the upper triangular portion of the precoding matrix, generated at the base-station for different radar locations.

Our contribution to this work can be summarized as follows: we design and train a deep neural network to detect the location of the radar in shared-spectrum systems based on the precoding matrix that the mobile user uses to communicate with the base-station while at the same time minimize its interference towards the radar. This work emphasizes the riskiness of the naive precoding matrix designs that contain implicit information about the radar location, and necessitates designing a more robust precoders to enable the coexistence of the radar and communication systems that share the same frequency band.

The rest of the paper is organized as follows: Section II presents the system model of the shared spectrum scenario used in this work. Section III provides an overview of the mathematical model of the interference mitigation problem in shared spectrum systems. The proposed DNN architecture is detailed in Section IV. The simulation results are presented in Section V, and the conclusion on the results of the proposed system in Section VI.

II. SYSTEM MODEL

Consider the radar-communications system shown in Figure 1, where a mobile user in a cellular system sharing the same frequency platform with a radar system is attempting to communicate with a nearby base station (BTS). The MIMO radar is equipped with $M_{tx}$ transmit antennas and $M_{rx}$ receive antennas, and the communications system is equipped with $M_{tx}$ transmit antennas at the mobile terminal (MT) and $M_{rx}$ receive antennas at the BTS. All arrays are assumed to be mounted along the y-axis, and the elevation angle is assumed to be constant. The MT connects with the base station via channel $G \in \mathbb{C}^{M_{tx}\times M_{rx}}$, and the MIMO radar connects with the BTS via channel $H_1 \in \mathbb{C}^{M_{tx}\times M_{rx}}$ and with the MT via channel $H_2 \in \mathbb{C}^{M_{tx}\times M_{rx}}$.

In our work, we are interested in the radar-MT channel, $H_2$, and MT-BTS channel, $G$, only, which we assume to follow a Rician model with Rician factor $K$, which is modeled as follows [9, 10]:

$$H_2 = \sqrt{\frac{k}{k+1}} H_d + \sqrt{\frac{1}{k+1}} H_s$$

(1)

where $H_d$ is the direct line-of-sight (LoS) channel with power $pd$, and $H_s$ is the multipath channel, which has Rayleigh distribution with power $ps$. $K$ is defined as the ratio between the strength of the LoS component relative to the sum of the multipath components, that is $K = pd/ps$.

The direct channel, $H_d$, represents the array response $a$ to a signal received from the MT, which is located at angle $\theta$ relative to the radar, and received by the radar array.

Mathematically, the LoS channel can be modeled as the outer product of the receive and transmit array responses as follows:

$$H_d = a(\mu_{rx}) \times a^H(\mu_{tx})$$

(2)

where $a(\mu)$ can be modeled as follows:

$$a(\mu) = \begin{bmatrix} e^{j|\mu|} & e^{j|\mu|} e^{j(M-1)|\mu|} & \cdots & e^{j(M-1)|\mu|} \end{bmatrix}^T$$

(3)

and,

$$\mu_i = \frac{-2\pi}{\Delta} \Delta \sin \theta$$

(4)

where $\lambda$ is the signal wavelength, and $\Delta$ is the inter-elements spacing of the array. In our work, we assume that the array is a uniform linear array (ULA) with $\Delta = \lambda/2$. 

\[ \text{Figure 1: Radar-Communications System} \]
III. PROBLEM FORMULATION

The main design problem in shared spectrum systems is to control the interference from the MT to the radar, which are both operating on the same frequency band, in addition to maintaining the quality of service of the communications system (i.e., MT to BTS) above the required threshold. To achieve these two conditions simultaneously, the authors in [3] has suggested to design a precoding matrix $R_x$ that is used by the MT to null the transmitted signal in the direction of the radar and keep the communications data rate above the minimum acceptable communications rate $C$.

The precoder $R_x$ is a complex symmetric positive definite matrix that is designed by the base-station or a third-party controller to enable the coexistence of the radar and communications systems. It is used by the mobile user to pre-code the uplink transmitted signal, and thus it is a form of beamforming, where the main user’s array beam direction is focused towards the base-station while a null is placed at the radar location. Thus, the precoding matrix contains embedded information about the radar angle with respect to the user, and this fact brings a security/privacy risk on the radar.

Mathematically, the following optimization problem needs to be solved [3]:

$$\min_{R_x} \text{Tr}(H_2 R_x H_2^H)$$

subject to

$$\log|I + R_{in} G R_x^H G^H| \geq C$$

where $\text{Tr}()$ is the trace operator, $I$ is the identity matrix, $R_{in}$ is the noise covariance matrix, and $P_t$ is the MT power budget. Since the radar location and the MT location are known to the BTS, and given the user’s limited power budget $P_t$, the objective function in Eq. (5) guarantees that the designed precoding matrix $R_x$ minimizes the interference towards the radar, while at the same time the link quality of the communications system does not drop below the required threshold.

IV. THE PROPOSED APPROACH

It has been shown in [10] that, given the precoding matrix $R_x$, an adversary can violate the privacy of the radar and detect its direction information, while the distance to the radar cannot be revealed using a single user. In this section we propose a machine learning approach to reveal the identity (i.e., the direction information) of the radar embedded in the designed precoding matrix. We describe the details of the proposed artificial neural network (DNN) architecture that is used to detect the location of the radar using the designed precoder, in addition to the training, validation and testing procedures. It is worth noting that the proposed DNN structure can be used by the opponent to violate the privacy of the radar and detect its direction information.

A. Neural Network Architecture

The proposed artificial neural network (DNN) architecture consists of eleven layers (input, output, and nine hidden layers), as depicted in Figure 2. The input features of the DNN are the entries of the upper or lower triangular portion of the precoding matrix, excluding the diagonal entries since they do not have angle information. It is worth noting that the complex-valued entries of $R_x$ are split into their real and imaginary values before they are fed into the network.
The outputs of the fully connected layers (FC) layers (except the last hidden layer) are normalized, then thresholded using a rectified linear unit (ReLU) before they are propagated to the following hidden layer. The data normalization is performed by subtracting the mean value and dividing by the standard deviation across all layer outputs. This normalization step is necessary to control the relative importance of the input features propagated through the hidden layers.

Mathematically, let the input features of the DNN be \( f_i, i \in \{1, \ldots, 9\} \), and the output of the nine hidden layers block be \( Y \). The number of neurons in each hidden layer is set 7000, 4000, 3000, 2000, 1000, 500, 300, 100 and 1 at the last hidden layer respectively. Also, let \( f_{10} \) denote the regression layer, which is the output layer of the network.

The outputs of each of the hidden layers (except the ninth layer, which does not include normalization and thresholding steps) is given as follows:

\[
\max \left(0, f_i(X_{i-1})\right), \quad i \in \{1, \ldots, 8\}
\]

where, \( X_i \) is the output of the \( i \)th hidden layer. The DNN final output is produced as follows:

\[
Z = f_{10}(Y, b) + e = b_0 + b_1Y + e
\]

where, \( e \) is the random error term of the prediction model, and it is a zero-mean Gaussian random variable. The unknown parameters \( \alpha_1, \alpha_2 \) are predicted by minimizing the mean of the squared-error between the true and predicted outputs, as follows:

\[
\min_b E(Z - f_{10}(Y, b))
\]

where, \( E(\cdot) \) is the expectation operator.

**B. Training and Testing Procedures**

In order to train the DNN, a handful samples need to be generated and propagated through the network to optimize the weights between the consecutive hidden layers. In this work, we select a random angle between the 0° to 90° and generate a precoder \( R_x \) for this angle by solving the minimization problem in Eq.(5). In order to generate a large number of examples for each randomly chosen angle, we use 50,000 Monte Carlo trials, and change the random part of the channel \( H_2 \), which is Rayleigh distributed, and keep the LoS term for all trials. We call this procedure the direct method. A more efficient indirect procedure for generating the training data is to use a linear combination of the precoders as follows:

\[
R_x = t R_{x1} + (1 - t) R_{x2}
\]

where, \( R_{x1} \) and \( R_{x2} \) are two precoders that share the same LoS component (i.e., generated for the same angle), but different non-LoS components. \( t \) is a scaling factor that can take any value between 0 and 1 (i.e., \( t \in (0, 1) \)). In this work, we use 50 values for \( t \) in each combination for 1000 generated precoders (i.e., the total number of input feature samples is now 50,000). In this way, we increase the training data sample 50 times, in addition to the new properties embedded in the resultant precoder as a result of this linear combination. In both direct and indirect procedures, the generated precoders are split into 70% for training, 15% for testing, and 15% for validation.
V. SIMULATION RESULTS

In this section, we present the results of the network detection accuracy, where we measure the absolute error between the true and predicted radar location angles with respect to the MT. MATLAB 2021a software is used to generate the results in this section.

Figure 4 shows the histogram plot of the prediction errors using the model from [3,10] in Figure 4 (a) and our proposed DNN model with direct and indirect data generation procedures in Figure 4 (b) and Figure 4 (c), respectively. The error is calculated as the absolute difference between the true radar angle (with respect to the user) and the predicted angle. For Figure 4 (a), the predictions are performed by solving the optimization problem in Eq. (5). However, in Figure 4 (b) and (c) the angles are predicted using the proposed DNN shown in Figure 2.

We can notice that the angle prediction errors are distributed near zero in the machine learning approach, as opposed to the approach in [10]. In numbers, the mean absolute error using the approach in [10] is 0.692 rad (or 39.685°), and for our DNN approach with direct and indirect training data generation are 0.212 rad and 0.055 rad (that is, 12.141° and 3.138°), respectively. To calculate the percentage of violation performance, we divide the difference by the mean absolute error of the original model in Figure 4 (b) - (Original Number) then: divide the answer by the mean absolute error of the proposed model (Original Number) and multiply by 100. The improvement in the performance radar privacy violation of the DNN approach as compared to the naive model in Eq. (5) is owed to the powerful DNN learning capabilities using the huge number of training examples generated for this purpose, in addition to the specific network architecture used in the training. For the proposed DNN approach, the linear combination of the precoders, as in Eq. (9) has resulted in far better detection performance compared to the direct method (without linear combination). We think that the reason for this improvement is due to the new features that resulted from mixing the precoders which helped the network to better adjust their weights to optimize the network’s objective function as in Figure 3 of training progress.

VI. CONCLUSIONS

In this paper, we have discussed the privacy issues of precoder designs in shared-spectrum radar and communications systems in single user scenario. The main goal of this work is to bring the attention of researchers to the riskiness of the naive design procedures of the precoding matrix that contains implicit information about the radar location. By designing and training a neural network, we have shown that these naive precoder designs are not suitable for radar-communications coexistence in shared-spectrum systems, which necessitates more complex design procedures it is not possible to violate its privacy using a well-designed and trained neural network unless precoder design techniques become more complex and robust. This is an invitation to interested researchers to think about more complex designs to enable the safe coexistence of the radar with communications systems. We designed a neural network with nine hidden layers to predict the angle information embedded in the designed precoder using linear regression model. Also, a direct and indirect data generation procedures to train the proposed network has been proposed in this work, where the upper-triangular portion of the precoding matrix is used in the direct method, while a linear combination of the precoders is used in the indirect method. The results of this work recommend a more complex precoder designs to protect the privacy of the radar in shared spectrum scenarios.
**Fig. 4.** The absolute error levels performance comparison between (a) Model-based approach from [10], (b) Our data-based approach with direct training data generation, and (c) Our data-based approach with indirect training data generation.
References


