ON RADAR PRIVACY IN SHARED SPECTRUM SCENARIOS

Anastasios Dimas[1], *Matthew A. Clark*[2,3], *Bo Li*[4], *Konstantinos Psounis*[2], *and Athina P. Petropulu*[1]

[1]Rutgers, The State University of New Jersey, Piscataway, NJ
[2]University of Southern California, Los Angeles, CA
[3]The Aerospace Corporation, El Segundo, CA
[4]Aurora Innovation, Pittsburgh, PA

ABSTRACT

To satisfy the increasing demand for additional bandwidth from the wireless sector, regulatory bodies are considering to allow commercial wireless systems to operate on spectrum bands that until recently were reserved exclusively for military radar. Such co-existence would require mechanisms for controlling interference. One such mechanism is to assign a precoder to the communication system, which is designed to minimize the communication system's interference to the radar. This paper looks into whether the implicit radar information contained in such a precoder can be exploited by an adversary to infer the radar's location. For two specific precoder schemes, we simulate a machine learning based location inference attack. We show that the system information leaked through the precoder can indeed pose various degrees of risk to the radar's privacy, and further confirm this by computing the mutual information between the respective precoder and the radar location.

Index Terms— Machine Learning, Null space precoding, Radar Privacy, Spectrum co-existence, Spectrum sharing

I. INTRODUCTION

Historically, exclusive use of commercial spectrum is granted through a license to frequencies that do not overlap with those allocated for military purposes. It has been observed though [1], [2] that this access strategy leads to underutilization of the licensed spectrum for large periods of time. To overcome this issue, spectrum regulators have proposed allowing commercial cellular systems to have access to the band 3550-3700 MHz, which was previously restricted for use by military radar [3], [4]. Co-existence of cellular systems and radar on the same bands requires a mechanism to control the interference that one system exerts to the other [5]. Such mechanisms include enforcing large geographical separation between the two systems [6], or using dynamic spectrum allocation methods [7], [8]. Here, we consider a more bandwidth efficient solution that relies on spatial multiplexing [9], [10]. In that context, *spectrum sharing* between a multiple-input-multiple-output (MIMO) radar and a MIMO communication system has inspired a lot of research [11], [7], [8]. Existing works mostly offer designs that optimize the objective of one system or the other, such as the null space projection precoding schemes of [10], [12], [13], [11]. Co-design of radar and communication systems has been proposed in [14], [9], [15]

In [14], [9], [15], spectrum sharing is moderated by a *controller*, which collects information from the two systems and designs precoders for them, so that some performance objective is met. The precoders contain information about the two systems, which may raise privacy concerns. For example, consider a smartphone co-existing with a military radar; the smartphone is assigned a precoding matrix to control the interference that it generates towards the radar. If an adversary got access to the smartphone's precoding scheme, then it could potentially reverse engineer the precoder and obtain information about the radar, e.g. the radar's location. Of course, by using dedicated equipment one could localize the radar based on its high power. Here, however, the possibility opens up that somebody with a smartphone can localize a radar operating nearby.

In this paper, we consider a communication system consisting of a stationary MIMO smartphone that is communicating with a base station, operating in the same spectrum bands with a stationary collocated MIMO radar. The radar transmit antennas transmit orthogonal waveforms. The measurements of all receive antennas are forwarded to a fusion center for processing and target estimation. Interference towards the MIMO radar can occur either when the radar is obtaining the target echoes, or when forwarding these samples to the radar fusion center. To limit the interference towards the radar, a precoder matrix designed by a controller is assigned to the smartphone. Here, we assume that the controller is part of the MIMO radar fusion center, so as to eliminate the possibility of interference during communication with the controller, as well as the risk of radar information being sent to an untrusted node.

The prospect of an adversary obtaining information beyond that directly revealed by the controller, is referred to as an *inference attack*. In this paper, we are interested in examining the extent to which the information contained in the exchanged precoders can pose a privacy risk to the co-existent MIMO radar system. More specifically, we consider

an adversary, disguised as an operating smartphone that uses a machine leaning approach to determine the radar location. The adversary partitions its search area into cells, and proceeds by training a separate classifier for each cell, using precoder matrices sent to the smartphones in the past. Once the classifiers of all cells are trained, for every new precoder observation, the adversary can determine the cell in which the radar is located. The location privacy of the examined precoder schemes is directly related to the amount of information the precoder reveals about the radar location. To gain more insight on this claim, we estimate the mutual information (MI) [16] between the used precoder scheme and the radar location.

A similar scenario was studied in [17], where an adversary wanted to determine the probability that the licensed user is located in a cell. There, the authors assume an adversary conducting a series of queries from various positions requesting channel access. For every received query reply regarding channel availability, the adversary updates the probability that the licensed user is located in a cell. Once the probability exceeds a predefined threshold, the adversary achieves a level of confidence of the licensed user location. Our approach is different that [17] in that the adversary uses information that is sent to the users anyway. Further, our approach does not update the respective cell probabilities sequentially after each observation, but rather, given available training data, trains a separate classifier for each cell. In our previous work on the same topic [18], the adversary attempts to estimate the radar's angle using a particle filter and a metric derived from the precoder. However, the inferred angle in [18] cannot uniquely determine the radar's position, and also, mapping the actual precoder matrix to a metric, discards useful information.

In the following, Section II introduces the co-existence setup and the considered interference mitigation strategies. The adversary inference procedure is presented in Section III, followed by the simulations and conclusion in Section IV and V, respectively.

II. SYSTEM MODEL

Let us assume the setup depicted in Fig. 1, where a collocated MIMO radar with M_R^{tx} transmit and M_R^{rx} receive antennas co-exists on the same spectrum band with a communication system, i.e., a smartphone. The smartphone has M_C^{tx} transmit antennas and communicates with a local base station, which has M_C^{rx} receive antennas, through the uplink channel $\mathbf{H} \in \mathbb{C}^{M_C^{rx} \times M_C^{tx}}$. The uplink communication creates interference to the radar, occurring over channel $\mathbf{G_2} \in \mathbb{C}^{M_R^{rx} \times M_C^{tx}}$, while the downlink communication occurs in another frequency band and thus does not create interference. The MIMO radar creates interference to the base station over channel $\mathbf{G}_1 \in \mathbb{C}^{M_C^{rx} \times M_R^{tx}}$. The interference channel matrix is directly related to the radar location, as seen in the following model [19], [20]:

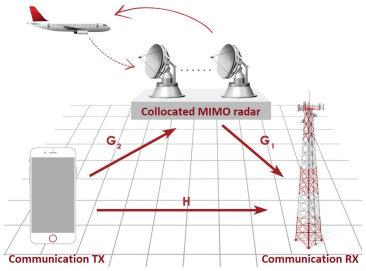

Fig. 1. A collocated MIMO radar sharing the same spectrum bands with a MIMO communications system.

$$\mathbf{G_2} = \frac{\sqrt{E_x}\lambda_c}{4\pi d\sqrt{M_C^{tx}}}\Big(\sqrt{\frac{K}{1+K}}\mathbf{S}_{\text{LoS}} + \sqrt{\frac{1}{1+K}}\mathbf{S}_{\text{NLoS}}\Big), \quad (1)$$

where λ_c is the carrier wavelength, E_x the transmit energy, and d the radar distance from the smartphone; K is the Rician factor [19], $\mathbf{S}_{\text{LoS}} = \mathbf{e}_r(\Omega_r)\mathbf{e}_t(\Omega_t)^T$, and $\mathbf{S}_{\text{NLoS}}$ is a matrix of i.i.d. $\mathcal{N}_{\mathbb{C}}(0,1)$ entries. The transmit and receiving steering vectors are given by

$$\begin{aligned}\mathbf{e}_t(\Omega_t) &= \Big[1, e^{-j\frac{2\pi\Delta_t}{\lambda_c}\Omega_t}, \ldots, e^{-j(M_C^{tx}-1)\frac{2\pi\Delta_t}{\lambda_c}\Omega_t}\Big]^T, \\ \mathbf{e}_r(\Omega_r) &= \Big[1, e^{-j\frac{2\pi\Delta_r}{\lambda_c}\Omega_r}, \ldots, e^{-j(M_R^{rx}-1)\frac{2\pi\Delta_r}{\lambda_c}\Omega_r}\Big]^T,\end{aligned} \quad (2)$$

with $\Omega_t = sin(\phi_t), \Omega_r = sin(\phi_r)$ corresponding to the angles of incidence of the Line-of-Sight path on the transmit and receive uniform linear arrays, respectively, and Δ_t and Δ_r, the transmit and receive antenna spacing, respectively.

II-A. Interference Mitigation

In order to mitigate the interference to the radar, the communication system is assigned a precoder matrix. Two separate precoder schemes are considered here.

Null Space Precoder: This precoder [10], [12], [13] zero forces the interference to the radar receive antennas. It equals the null space of the interference channel $\mathbf{G_2}$, i.e.

$$\mathbf{P}_n = null(\mathbf{G_2}). \quad (3)$$

To ensure that a null space exists, the number of radar receive antennas needs to be smaller than the number of communication transmit antennas.

Optimized Precoder: This precoder [14], [9], [15] aims to minimize the interference power to the radar, subject to meeting power and rate constraints. The precoder $\mathbf{P}_o = \mathbf{R}_x^{1/2}$ is the solution to the optimization problem

$$\arg\min_{\mathbf{R}_x} \text{tr}(\mathbf{G}_2\mathbf{R}_x\mathbf{G}_2^H) \quad (4)$$

$$\text{s.t. tr}(\mathbf{R}_x) \leq P_t \quad (5)$$

$$C_{avg} = \log_2 \det(\mathbf{I} + \mathbf{R}_{in}^{-1}\mathbf{H}\mathbf{R}_x\mathbf{H}^H) \geq C \quad (6)$$

where $\mathbf{R}_x$ is the covariance matrix of the transmitted codewords. P_t is the transmit power budget of the smartphone and C is the minimum communication rate. $\mathbf{R}_{in}$ is the interference plus noise covariance at the communication receiver, which is assumed to be known.

III. ADVERSARY ESTIMATION

We consider a scenario in which an adversary operating a set of S independent smartphones, observes at every point in time $t = 1, \ldots, T$ all precoder matrices $\mathcal{P}^t = \{\mathbf{P}_1^t, \ldots, \mathbf{P}_S^t\}$ which are sent to the smartphones by the controller. Each precoder is in general a function of $\mathbf{G}_2$, i.e., $\mathbf{P}_i = f(\mathbf{G}_2^i + \mathbf{W})$, $i = 1, \ldots, S$, where $\mathbf{W}$ is additive white Gaussian noise (AWGN). For simplicity, we assume that each precoder is obtained independently of the others, and they are all stacked into a long vector. We also assume the adversary is not capable of estimating $\mathbf{G}_2$; otherwise, it would not need to reverse engineer the precoding matrix, as $\mathbf{G}_2$ contains direct information about the radar location.

To initiate its search, the adversary considers a number of discrete possible radar locations $\mathbf{R}_i, i = 1, \ldots, N_R$, within the region of interest. In the assumed inference attack, location privacy is the goal, so the adversary treats the unknown radar locations as a random variable R, and attempts to create an estimate of its probability density function (pdf), p_R, based on the observed precoders sent by the controller. This can be formulated as a Bayesian inference problem, where the conditional pdf of a sequence of T candidate radar locations given a sequence of T precoders equals

$$p_R\left(R^1, \ldots, R^T | \mathcal{P}^1, \ldots, \mathcal{P}^T\right) = \frac{p_{P|R}\left(\mathcal{P}^1, \ldots, \mathcal{P}^T | R^1, \ldots, R^T\right)}{p_P\left(\mathcal{P}^1, \ldots, \mathcal{P}^T\right)} p_R\left(R^1, \ldots, R^T\right) \tag{7}$$

where $p_{P|R}$ is the probability of the observed precoder matrices given a specific location. The adversary has no prior information about the radar location, so it must assume that all radar candidate locations are equally likely a-priori, i.e. $p_R\left(R^1, \ldots, R^T\right)$ is a constant. The controller assignments are assumed memoryless, so it follows from (7) that

$$p_R\left(R^1, \ldots, R^T | \mathcal{P}^1, \ldots, \mathcal{P}^T\right) = \frac{\prod_{t=1}^{T} p_{P|R}\left(\mathcal{P}^t | R^t\right)}{\sum_{\mathcal{R}} \prod_{t=1}^{T} p_{P|R}\left(\mathcal{P}^t | R^t\right)}, \tag{8}$$

where the denominator refers to the sum over all possible candidate location sequences $\mathcal{R}$. If the adversary was familiar with the a-priori probabilities $p_{P|R}\left(\mathcal{P}^t | R^t\right)$, e.g. by past experience, then computing (8) for every possible combination of candidate locations would produce the optimal estimate of the pdf. However, this is computationally prohibitive due to the large candidate space.

Instead, the adversary may follow a sub-optimal location estimation method, such as the supervised machine learning approach we consider here. Our formulation uses the individual complex elements of the precoding matrices sent to every colluding smartphone, separated into their real and imaginary parts, and stacked into a vector, as features to a classification problem. A classifier is trained for every separate grid cell using a balanced training set, along with the respective training labels which describe for each training sample the radar cell location they intend to protect. We consider two separate classifiers, namely the Naive Bayes and the SVM, to make sure our formulation is not classifier dependent. Once the training is performed, the adversary can test every new precoder observation with all grid cells in parallel, in order to determine the radar location for which the respective precoders were meant to protect.

III-A. Mutual Information

One way to quantify the amount of information a precoder reveals about the radar location is to measure the MI between the precoder and the radar location. Here, MI determines the potential reduction in the adversary's uncertainty of the true radar position.

Let the random variable R be described by the joint pdf of radar coordinates in cell c, i.e. $p(R_x, R_y)$. Corresponding to R is the precoder random variable, P, described by the joint pdf of its elements, $p\left(P(1), \ldots, P(n)\right)$, where n the number of individual precoder matrix elements. The MI between these continuous random variables is defined as [16]

$$I(R;P) \triangleq \iint p(R,P) \log_2 \frac{p(R,P)}{p(R)p(P)} dR dP \tag{9}$$

where $p(R,P)$ the joint radar-precoder pdf and $p(R)$, $p(P)$ the respective marginal pdfs. Due to the difficulty in obtaining closed form expressions for these pdfs, we proceed to estimate them numerically, using a multi-dimensional histogram.

IV. SIMULATION RESULTS

We simulated a scenario that examined the adversary's inference potential. The adversary had partitioned the 2×2 km search area into 500×500 sq.m. imaginary cells, in order to make a binary decision as to whether the radar is located in each cell. We assumed that the adversary was controlling $S = 5$ smartphones. The smartphones had coordinates that are uniformly chosen in $[0, 1000]$, and were communicating with a common base station, as shown in Fig. 2. The radar system had $M_R^{rx} = M_R^{tx} = 6$ antennas and the communication system had $M_C^{tx} = M_C^{rx} = 8$ antennas. We should note that although current smartphones incorporate 4×4 MIMO, LTE-advanced can support up to 8×8 MIMO [21]. We further model $\mathbf{H}$ as a $\mathcal{N}_{\mathbb{C}}(0,1)$ Rayleigh fading channel, and $\mathbf{G}_1$ as a Rician fading channel. The carrier frequency was taken to be 3.55 GHz. As mentioned before, it is assumed that the adversary is not capable of estimating the interference channel. Nevertheless, as a baseline approach for comparison in our simulations, we considered the case in which the adversary observes $\mathbf{G}_2$, denoted by $\mathbf{P}_b$. Three separate balanced training sets $\mathcal{L}_b^c$, $\mathcal{L}_n^c$, $\mathcal{L}_o^c$, of 6000 samples each were created for cell $c = 4$ of Fig. 2, for the cases where the adversary observes the baseline precoder, $\mathbf{P}_b$, the null space precoder, $\mathbf{P}_n$, and the optimal precoder, $\mathbf{P}_o$, respectively. A separate test set $\mathcal{T}^c$ for $c = 4$ was created, consisting of 2375 samples, where 500 samples correspond

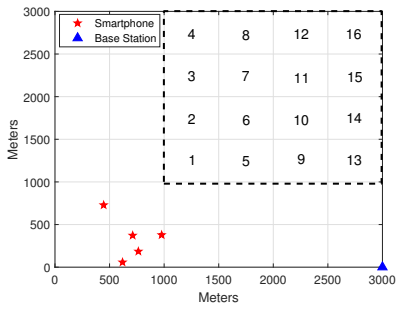

Fig. 2. The adversary search area is confined within the dashed square and is divided into cells.

to precoders of radar locations in $c = 4$, and 1875 samples to no radar in $c = 4$. To avoid over-fitting, the radar locations used for $\mathcal{T}^c$ differ from those used in $\mathcal{L}^c$. In general, the analysis is independent of the chosen grid cell.

The receiver operating characteristic (ROC) for cell $c = 4$, obtained using the Naive Bayes and SVM classifiers is shown in Fig. 3. The true positives represent the cases in which the classifier correctly determined that the radar was located in $c = 4$, while the false positives represent the cases in which the classifier decided the the radar was present in $c = 4$, when in reality it was not. Fig. 3 clearly shows that the information contained in $\mathbf{P}_b$ would yield a near perfect radar location prediction by the adversary. On the other hand, the use of $\mathbf{P}_o$ results in an almost diagonal ROC curve, which essentially corresponds to a random adversary guess. Moreover, we also see that $\mathbf{P}_o$ can be considered a better option as compared to $\mathbf{P}_n$ in protecting the radar privacy.

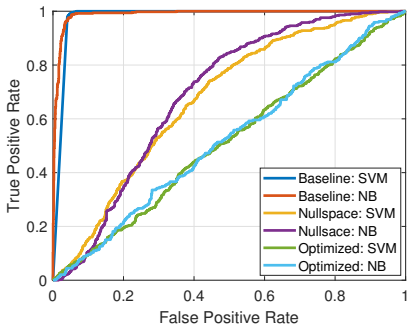

Fig. 3. The ROC curve for the test set of $c = 4$.

The MI was computed numerically for all assumed precoders in $c = 4$. Depending on the precoder, the bins of the multi-dimensional histogram where created from the positive samples of $\mathcal{L}_b^c$, $\mathcal{L}_n^c$, or $\mathcal{L}_o^c$, using the K-means clustering algorithm [22]. The MI for a varying number of antennas, is shown in Fig. 4. The setup is similar to before, only now we consider a single smartphone located at $(0, 0)$ and no AWGN present in $\mathbf{G}_2$. A first observation from Fig. 4 is that

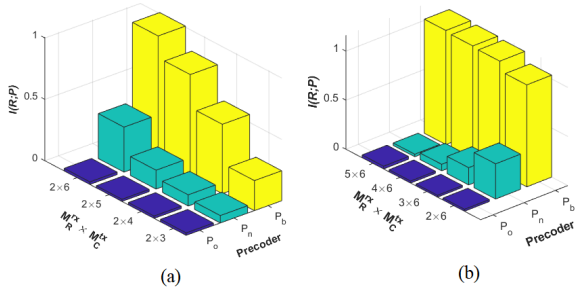

Fig. 4. MI between precoders and radar positions for a varying number of (a) transmit and (b) receive antennas.

$$I(R; P_o) < I(R; P_n) < I(R; P_b), \tag{10}$$

which basically means there is a greater reduction in the uncertainty of R when observing P_b than when observing P_o. In other words, $\mathbf{P}_b$ reveals the most information about a radar location, while $\mathbf{P}_o$ the least. The right inequality of (10) is also a consequence of the data processing inequality [16], which states that for a Markov chain $R \to P_b \to P_n$, processing cannot increase information.

From Fig. 4a we observe that when using $\mathbf{P}_b$ or $\mathbf{P}_n$, an increase in the number of transmit antennas at the communication system results in an increase in MI. This can be justified by the respective increase in the column space of $\mathbf{P}_b$, which directly affects the size of $\mathbf{P}_n$ as well. On the other hand, in Fig. 4b we see a reduction of the MI for a fixed number of communication system antennas as the number of receive antennas at the radar increase. The final observation from Fig. 4 is that $I(R; P_o)$ is very small. This indicates that R and P_o are close to being independent, with most of the radar information being suppressed in the optimized precoder. This is due to the fact that, as opposed to $\mathbf{P}_n$ which is only a function of $\mathbf{G}_2$, $\mathbf{P}_o$ is additionally a function of $\mathbf{H}, \mathbf{G}_1$. The channel $\mathbf{H}$ by definition has no information regarding the radar position. Also, $\mathbf{P}_o$ is obtained as the solution of a constrained optimization problem, which makes the contribution of $\mathbf{G}_1$ to the final solution less transparent. Although the optimal precoder seems to be better for the radar privacy, it does involve more computational complexity.

V. CONCLUSIONS

This paper considered a co-existence scenario between a collocated MIMO radar and a set of stationary MIMO smartphones, where the latter are controlled by an adversary. We examined the extent to which the adversary can infer radar location information from the communication system precoder matrix, using a machine learning based inference attack. Depending on the used precoder scheme, our simulations indicated that this was indeed possible, a result further supported by our estimation of the mutual information between the precoder matrix and radar location.

VI. REFERENCES

[1] Paul J. Kolodzy, "Spectrum policy task force," *Federal Communications Commission, Washington, DC, Rep. ET Docket*, vol. 40, no. 4, pp. 147–158, 2002.

[2] Mark A. McHenry, "NSF spectrum occupancy measurements project summary," *Shared spectrum company report*, 2005.

[3] Federal Communications Commission, "Enabling innovative small cell use in 3.5 GHz band NPRM & order," *FCC 12*, vol. 148, 2012.

[4] Federal Communications Commission, "Order on reconsideration and second report and order. in the matter of amendment of the commission's rules with regard to commercial operations in the 3550-3650 MHz band, GN Docket no. 12-354, released May 2016," 2016.

[5] Frank H. Sanders, Robert L. Sole, Brent L. Bedford, David Franc, and Timothy Pawlowitz, "Effects of RF interference on radar receivers," *NTIA Report TR-06-444*, 2006.

[6] Alex Lackpour, Michael Luddy, and Jack Winters, "Overview of interference mitigation techniques between WiMAX networks and ground based radar," in *Wireless and Optical Communications Conference (WOCC), 2011 20th Annual*. IEEE, 2011, pp. 1–5.

[7] Qing Zhao and Ananthram Swami, "A survey of dynamic spectrum access: Signal processing and networking perspectives," in *Acoustics, speech and signal processing, 2007. ICASSP 2007. IEEE international conference on*. IEEE, 2007, vol. 4, pp. IV–1349.

[8] Rathapon Saruthirathanaworakun, Jon M. Peha, and Luis M. Correia, "Opportunistic sharing between rotating radar and cellular," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1900–1910, 2012.

[9] Bo Li, Harshat Kumar, and Athina P. Petropulu, "A joint design approach for spectrum sharing between radar and communication systems," in *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on*. IEEE, 2016, pp. 3306–3310.

[10] Shabnam Sodagari, Awais Khawar, T. Charles Clancy, and Robert McGwier, "A projection based approach for radar and telecommunication systems coexistence," in *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012, pp. 5010–5014.

[11] Jasmin A. Mahal, Awais Khawar, Ahmed Abdelhadi, and T. Charles Clancy, "Spectral coexistence of MIMO radar and MIMO cellular system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 2, pp. 655–668, 2017.

[12] Alireza Babaei, William H. Tranter, and Tamal Bose, "A nullspace-based precoder with subspace expansion for radar/communications coexistence," in *Global Communications Conference (GLOBECOM), 2013 IEEE*. IEEE, 2013, pp. 3487–3492.

[13] Awais Khawar, Ahmed Abdelhadi, and T. Charles Clancy, "Coexistence analysis between radar and cellular system in LoS channel," *IEEE Antennas and Wireless Propagation Letters*, vol. 15, pp. 972–975, 2016.

[14] Bo Li, Athina P. Petropulu, and Wade Trappe, "Optimum co-design for spectrum sharing between matrix completion based MIMO radars and a MIMO communication system," *IEEE Transactions on Signal Processing*, vol. 64, no. 17, pp. 4562–4575, 2016.

[15] Bo Li and Athina P. Petropulu, "Joint transmit designs for coexistence of MIMO wireless communications and sparse sensing radars in clutter," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 6, pp. 2846–2864, 2017.

[16] Thomas M. Cover and Joy A. Thomas, *Elements of information theory*, John Wiley & Sons, 2012.

[17] Behnam Bahrak, Sudeep Bhattarai, Abid Ullah, Jung-Min Park, Jeffery Reed, and David Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 236–247.

[18] Anastasios Dimas, Bo Li, Matthew Clark, Konstantinos Psounis, and Athina P. Petropulu, "Spectrum sharing between radar and communication systems: Can the privacy of the radar be preserved?," in *51st Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, 2017.

[19] Robert W. Heath, *Introduction to Wireless Digital Communication: A Signal Processing Perspective*, Prentice Hall, 2017.

[20] Andreas F. Molisch, *Wireless communications*, vol. 34, John Wiley & Sons, 2012.

[21] "LTE-advanced," http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced, Accessed 28-10-2018.

[22] K Krishna and M Narasimha Murty, "Genetic k-means algorithm," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 29, no. 3, pp. 433–439, 1999.