Security Issues in Spectrum Sharing Between Radar and Communication Systems

A. Dimas[1], M. Clark[2,3], B. Li[4], K. Psounis[2], A. 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] Qualcomm, San Diego, CA

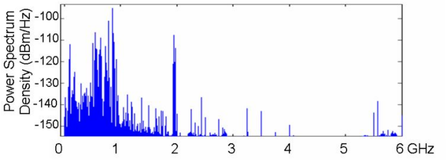
November 27, 2018

Outline

Outline

The Need for Spectrum Sharing

- Radar and communications jointly consume most of the spectrum below 6 GHz.
- Until recently, allocated spectrum for commercial and non-commercial purposes (i.e. military radar) were on distinct bands.
- S-band radar ($2-4$ GHz) partially overlaps with LTE and WiMax systems.

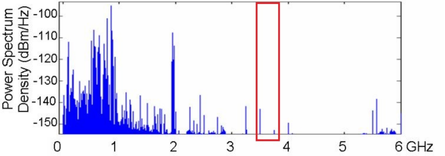


Freq (GHz)	0~1	1~2	2~3	3~4	4~5	5~6
Utilization(%)	54.4	35.1	7.6	0.25	0.128	4.6

Figure: Spectrum utilization in downtown Berkeley (UC Berkeley, 2007).

The Need for Spectrum Sharing

- As the number of connected devices grows, these band distinctions limit a more efficient use of the spectrum.
- Spectrum regulators have proposed to make the $3.55 - 3.7$ GHz band (used for military radar) available to commercial cellular systems.
- The need arises for an efficient use of the spectrum for both systems, without one interfering with the other $\rightarrow$ Spectrum sharing approaches.



Freq (GHz)	0~1	1~2	2~3	3~4	4~5	5~6
Utilization(%)	54.4	35.1	7.6	0.25	0.128	4.6

Figure: Spectrum utilization in downtown Berkeley (UC Berkeley, 2007).

Existing Approaches for Spectrum Sharing

1. Avoid interference by large spatial separation.

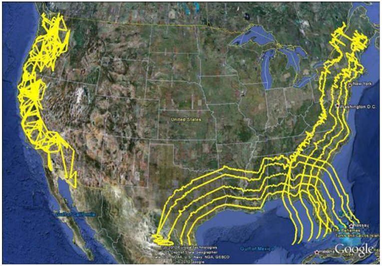


Figure: Shipborne radar exclusion zones in 3.5 GHz band (NTIA 2015).

2. Dynamic spectrum access based on spectrum sensing.

1. Avoid interference by large spatial separation.

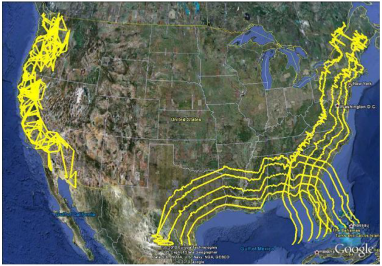


Figure: Shipborne radar exclusion zones in 3.5 GHz band (NTIA 2015).

2. Dynamic spectrum access based on spectrum sensing.
3. **Spatial multiplexing enabled by the multiple antennas at both the radar and communication systems.**

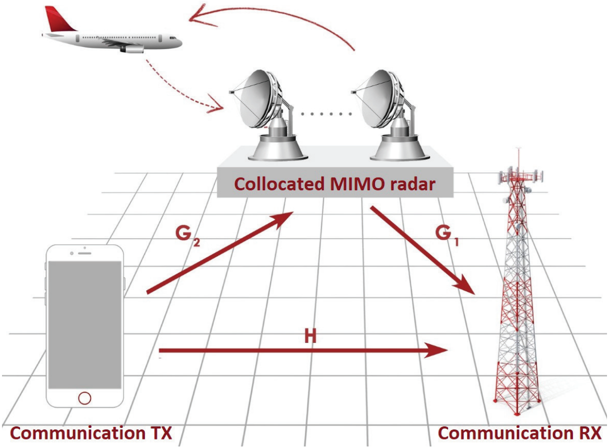
MIMO Shared Spectrum Literature

- Methods that address the objectives of one or the other system but not both.
  - Nullspace projection implemented by radar to reduce interference towards the communication system [Sodagari et al. 2012] or vice versa.
  - Nullspace projection precoding to avoid interference is possible on either the radar or the communication systems but not on both [Mahal et al.,2017].
- Co-design methods that address the constraints of both systems.
  - Communication system and/or radar precoding schemes are co-designed in order to maximize an objective function of one user (typically the radar), subject to meeting certain constraints for the other (typically the communication system) [Li, Kumar, and Petropulu, 2016] [Li, Petropulu, Trappe, 2016] [Li and Petropulu, 2017]

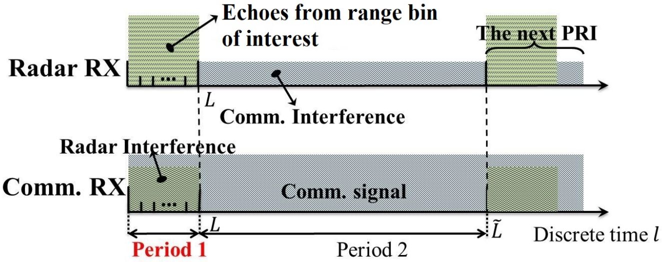
Outline

Spectrum Sharing Formulation

- $M_R^r \times M_R^t$ MIMO radar
- $M_C^r \times M_C^t$ MIMO communication system

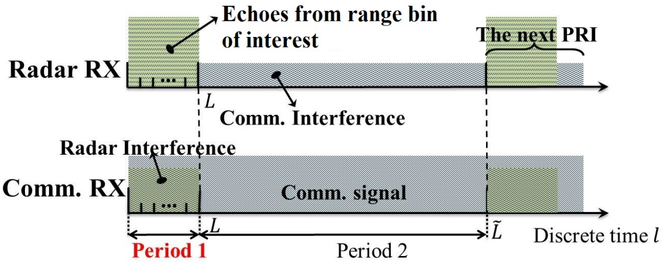


- Interference at the radar occurs when the radar is listening, or forwarding the obtained samples to the radar fusion center.



Interference During Spectrum Sharing

- Interference at the radar occurs when the radar is listening, or forwarding the obtained samples to the radar fusion center.



- Use transmit precoding to limit the interference to the radar.

The Coexistence Signal Model

- The received signals at the radar and communication RX are

Radar fusion center: (1a)

$$\boldsymbol{\Omega} \circ \mathbf{Y}_R = \boldsymbol{\Omega} \circ \big(\underbrace{\mathbf{DPS}}_{\text{signal}} + \underbrace{\mathbf{CPS} + \mathbf{G}_2\mathbf{X}\boldsymbol{\Lambda}_2}_{\text{interference}} + \underbrace{\mathbf{W}_R}_{\text{noise}}\big), \quad (1b)$$

Communication receiver: (1c)

$$\mathbf{Y}_C = \underbrace{\mathbf{HX}}_{\text{signal}} + \underbrace{\mathbf{G}_1\mathbf{PS}\boldsymbol{\Lambda}_1}_{\text{interference}} + \underbrace{\mathbf{W}_C}_{\text{noise}}, \quad (1d)$$

where

- $\mathbf{P}, \mathbf{S}, \boldsymbol{\Omega}$: radar precoder, waveforms, subsampling matrix
- $\mathbf{D} = \sum_{k=1}^{K} \sigma_{\beta_0}^2 \mathbf{v}_t^*(\theta_k)\mathbf{v}_t^T(\theta_k)$
- $\mathbf{C} \triangleq \sum_{k=1}^{K_c} \beta_k^c \mathbf{v}_r(\theta_k^c)\mathbf{v}_t^T(\theta_k^c)$: clutter response matrix
- $\mathbf{X} \triangleq [\mathbf{x}(1), \ldots, \mathbf{x}(L)]$: comm codewords $\mathbf{x}(l) \sim \mathcal{CN}(0, \mathbf{R}_{xl})$
- $\boldsymbol{\Lambda}_1$,$\boldsymbol{\Lambda}_2$: diagonal matrices denoting random phase offsets

The Co-Design Problem

- **Radar SINR:**

$$\text{SINR} = \frac{m\,\mathsf{Tr}\left(\mathbf{P}\mathbf{P}^H\mathbf{D}\right)}{m\,\mathsf{Tr}\left(\mathbf{P}\mathbf{P}^H\mathbf{C}\right) + \sum_{l=1}^{L}\mathsf{Tr}\left(\mathbf{G}_{2l}\mathbf{R}_{xl}\mathbf{G}_{2l}^H\right) + m\sigma_R^2}. \quad (2)$$

Constraints:

- The power budget at the communication transmitter: $\sum_{l=1}^{L}\mathsf{Tr}(\mathbf{R}_{xl}) \leq P_t$,
- The requirement on the average communication rate achieved during the L symbol periods

$$\mathsf{C}_{\mathsf{avg}}(\{\mathbf{R}_{xl}\}) \triangleq \frac{1}{L}\sum_{l=1}^{L}\log_2\left|\mathbf{I} + \mathbf{R}_{\mathsf{Cin}}^{-1}\mathbf{H}\mathbf{R}_{xl}\mathbf{H}^H\right| \geq C \quad (3)$$

$$\mathbf{R}_{\mathsf{Cin}} = \mathbf{G}_1\mathbf{P}\mathbf{P}^H\mathbf{G}_1^H + \sigma_C^2\mathbf{I}.$$

The Co-Design Problem

- Cooperate on estimating $\mathbf{G}_1$, $\mathbf{G}_2$. Share $\mathbf{H}$, $\mathbf{G}_1$, and $\mathbf{G}_2$ with the controller.
- The controller designs $\mathbf{\Phi} = \mathbf{P}\mathbf{P}^H$, $\mathbf{\Omega}$ and $\{\mathbf{R}_{xl}\}$ as

$$\max_{\{\mathbf{R}_{xl}\}\succeq 0, \mathbf{\Phi}\succeq 0, \mathbf{\Omega}} \mathsf{SINR}\left(\{\mathbf{R}_x\}, \mathbf{\Omega}, \mathbf{\Phi}\right),$$

$$\text{s.t.} \quad C_{\mathsf{avg}}(\{\mathbf{R}_{xl}\}, \mathbf{\Phi}) \geq C, \tag{4a}$$

$$\sum_{l=1}^{L} \mathsf{Tr}\left(\mathbf{R}_{xl}\right) \leq P_C, L\mathsf{Tr}\left(\mathbf{\Phi}\right) \leq P_R, \tag{4b}$$

$$\mathbf{\Omega} \text{ is proper} \tag{4c}$$

The Interference Channel

- The interference channel matrix is directly related to the radar location, as seen in the following model [Heath, 2017] [Molisch, 2012]

$$\mathbf{G_2} = \frac{\sqrt{E_x}\lambda_c}{4\pi d\sqrt{M_C^t}}\left(\sqrt{\frac{K}{1+K}}\mathbf{S}_{\mathsf{LoS}} + \sqrt{\frac{1}{1+K}}\mathbf{S}_{\mathsf{NLoS}}\right) \qquad (5)$$

- λ_c: carrier wavelength; E_x: transmit energy; d: the radar distance from the smartphone; K is the Rician factor.
- $\mathbf{S}_{\mathsf{LoS}} = \mathbf{e}_r(\Omega_r)\mathbf{e}_t(\Omega_t)^T$ and $\mathbf{S}_{\mathsf{NLoS}}$ a matrix of i.i.d. $\mathcal{N}_{\mathbb{C}}(0,1)$ entries.
- $\Omega_t = sin(\phi_t)$ and $\Omega_r = sin(\phi_r)$ the angles of incidence of the Line-of-Sight path on the TX and RX steering vectors

$$\mathbf{e}_t(\Omega_t) = \left[1, e^{-j\frac{2\pi\Delta_t}{\lambda_c}\Omega_t}, \ldots, e^{-j(M_C^t-1)\frac{2\pi\Delta_t}{\lambda_c}\Omega_t}\right]^T,$$

$$\mathbf{e}_r(\Omega_r) = \left[1, e^{-j\frac{2\pi\Delta_r}{\lambda_c}\Omega_r}, \ldots, e^{-j(M_R^r-1)\frac{2\pi\Delta_r}{\lambda_c}\Omega_r}\right]^T$$

Security of Spectrum Sharing

[Li and Petropulu, 2017]

- The controller is incorporated into the MIMO radar.
  - This avoids interference during communication with the radar.
  - Also, the controller is a trusted node.
- The controller collects information from the two systems and designs the precoders so that some performance objective is met.
- The computed precoder is passed to the communication system.

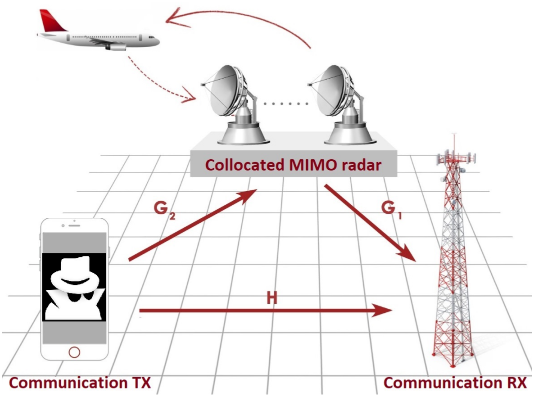
Security of Spectrum Sharing

[Li and Petropulu, 2017]

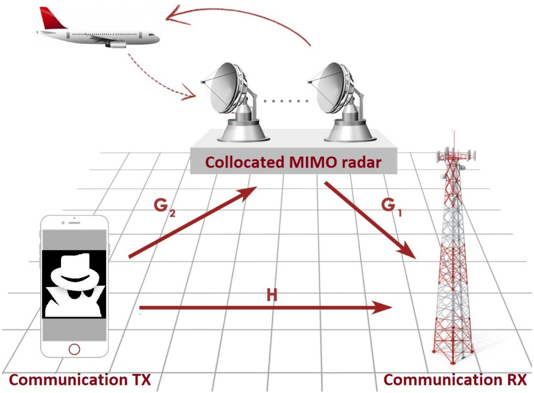
- The controller is incorporated into the MIMO radar.
  - This avoids interference during communication with the radar.
  - Also, the controller is a trusted node.
- The controller collects information from the two systems and designs the precoders so that some performance objective is met.
- The computed precoder is passed to the communication system.
- The precoder contains *implicit* information about the radar.

Security Concern

- Can the precoder be used by an adversary to launch an inference attack?



- Can the precoder be used by an adversary to launch an inference attack?



- Can the adversary reverse engineer the precoder matrix to infer the radar location?

Communication System Precoders

- Two precoders are examined here:
  - **Null Space Precoder** - Zero forces the interference at the radar receive antennas

$$\mathbf{P}_n = nullspace(\mathbf{G}_2)$$

    Assumes more comm system TX antennas than radar RX antennas

    [Sodagari et al. 2012, Babaei et. al., 2013, Khawar et. al.]

  - **Optimized Precoder** - Designed to minimize interference at the radar RX, subject to the comm system meeting certain rate and power constraints.

    [Li, Petropulu, Trappe, 2016],[Li, Kumar, and Petropulu, 2016], [Li and Petropulu, 2017]

Outline

Adversary Inference Attack

- Suppose an adversary is operating S independent smartphones, and observes at every point in time $t = 1, \ldots, T$ all precoder matrices $\mathcal{P}^t = \{\mathbf{P}_1^t, \ldots, \mathbf{P}_S^t\}$ sent to the smartphones by the controller.
- For simplicity, each precoder is obtained independently of the others.
- The adversary is not capable of estimating $\mathbf{G}_2$; otherwise it would easily locate the radar.
- The adversary treats the unknown radar location as a random variable R, and attempts to create an estimate of its pdf, p_R, based on the observed precoders sent by the controller.

Optimal Adversary Estimation I

- 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

$$p_R\left(R^1,\ldots,R^T|\mathcal{P}^1,\ldots,\mathcal{P}^T\right) = \frac{p_{P|R}\left(\mathcal{P}^1,\ldots,\mathcal{P}^T|R^1,\ldots,R^T\right)}{p_P\left(\mathcal{P}^1,\ldots,\mathcal{P}^T\right)} p_R\left(R^1,\ldots,R^T\right) \tag{6}$$

- $p_{P|R}$ is the probability of the observed precoder matrices given a specific radar location.
- May assume that all candidate locations are equally likely, i.e., the a priori pdf $p_R\left(R^1,\ldots,R^T\right)$ is a constant.

Optimal Adversary Estimation II

- May also assume that the controller assignments are memoryless, i.e.,

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

  $\mathcal{R}$ is he set of all candidate location sequences.
- If the adversary knew $p_{P|R}\left(\mathcal{P}^t|R^t\right)$, it could compute (7) for every possible combination of candidate locations.

Optimal Adversary Estimation II

- May also assume that the controller assignments are memoryless, i.e.,

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

  $\mathcal{R}$ is he set of all candidate location sequences.

- If the adversary knew $p_{P|R}\left(\mathcal{P}^t|R^t\right)$, it could compute (7) for every possible combination of candidate locations.
- Optimal estimation is computationally prohibitive → use a supervised machine learning approach for radar location estimation.

Machine Learning Estimation

- Adversary divides search area into cells.
- Adversary trains a classifier for every separate cell, using training data and their corresponding labels.
- Features in the classification problem are the precoding matrices, separated into real and imaginary parts, and stacked in a long vector.
- Once training has been completed, the adversary can decide which cell a new precoder corresponds to. This task can be parallelized.

Mutual Information

- One way to quantify the amount of information a precoder reveals about the radar location is via the *Mutual Information (MI)*.
- $R = (R_x, R_y) \sim p(R_x, R_y)$ denote radar coordinates, and $P = [P_1, ..., P_n]^T \sim p\,(P_1, \ldots, P_n)$ the precoder vector.

Mutual Information $I(R; P) \triangleq$

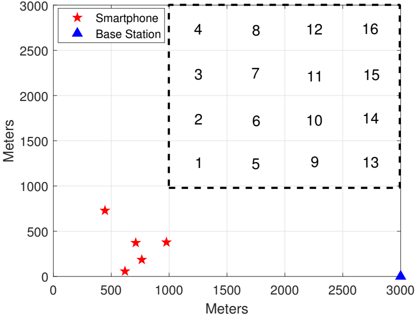
$$\int \cdots \int p(R_x, \ldots, P_n) \log_2 \frac{p(R_x, \ldots, P_n)}{p(R_x, R_y) p\,(P_1, \ldots, P_n)} dR_x \ldots dP_n \quad (8)$$

- MI can be estimated numerically using multi-dimensional histograms.

Outline

Simulation Setup

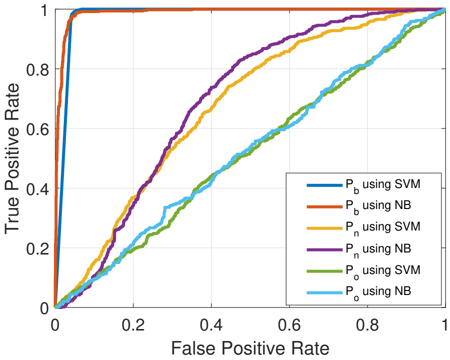
- The adversary will test all cells and make a binary decision on the presence of the radar in a particular cell.
- We assume the adversary is controlling $S = 5$ smartphones.
- The radar has $M_R^r = M_R^t = 6$ antennas and the communication system has $M_C^t = M_C^r = 8$ antennas.



Simulation Setup

- Baseline approach $(\mathbf{P}_b) \rightarrow$ the adversary observes $\mathbf{G}_2$.
- 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 $c = 4$, for the cases where the adversary observes $\mathbf{P}_b$, $\mathbf{P}_n$, and $\mathbf{P}_o$, respectively.
- A separate test set $\mathcal{T}^c$ for $c = 4$ was created, consisting of 2375 samples; 500 samples correspond to precoders for radar locations in $c = 4$, and $1,875$ samples for the radar in all other cells (125 samples for each $c \neq 4$.
- To avoid over-fitting, the radar locations used for training were different that those used in testing.
- For training we used the Support Vector Machine (SVM) and Naive Bayes (NB) classifiers (Matlab functions *fitcsvm* and *fitcnb*, respectively).

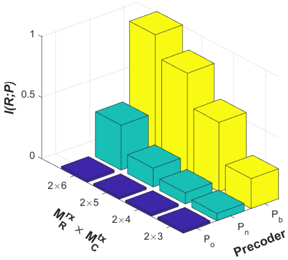
Simulation Setup



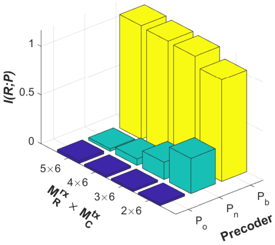
- ROC for cell $c = 4$
- $\mathbf{P}_b$ results in almost perfect radar location prediction.
- Using $\mathbf{P}_o$ results in a random adversary guess $\rightarrow$ $\mathbf{P}_o$ a better option in protecting the radar privacy.

Mutual Information

- Numerically computed mutual information for all assumed precoders.
- Depending on 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.



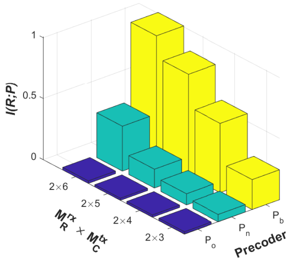
(a)



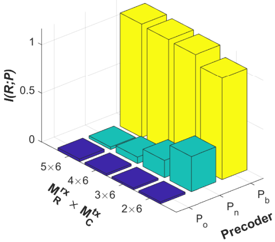
(b)

Mutual Information

- Notice that $I(R; P_o) < I(R; P_n) < I(R; P_b) \rightarrow$ 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.



(a)



(b)

Mutual Information

- For $\mathbf{P}_b$ or $\mathbf{P}_n$, an increase in the # of transmit antennas at the communication system results in an increase to the mutual information $\rightarrow$ respective increase in the column space of $\mathbf{P}_b$ directly affects the size of $\mathbf{P}_n$ as well.
- The value of $I(R; P_o)$ is very small $\rightarrow$ R and P_o are close to being independent, with most of the radar information being suppressed in the optimized precoder.
- $\mathbf{P}_n$ is only a function of $\mathbf{G}_2$ but $\mathbf{P}_o$ is additionally a function of $\mathbf{H}, \mathbf{G}_1$.
- $\mathbf{P}_o$ is obtained as the solution of a constrained optimization problem $\rightarrow$ contribution of $\mathbf{G}_1$ to the final solution less transparent and $\mathbf{H}$ by definition has no information regarding the radar position.
- The optimal precoder $\mathbf{P}_o$ seems to be better for the radar privacy but involves more computational complexity.

Outline

- 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.

Future work

The precoder $\mathbf{P} = \sqrt{\mathbf{R}_{xl}}$ is the solution to:

$$\begin{aligned}
\min_{\mathbf{R}_{xl}} \quad & \sum_{l=1}^{L} Tr(\mathbf{G}_2 \mathbf{R}_{xl} \mathbf{G}_2^H) \\
\text{s.t.} \quad & \sum_{l=1}^{L} Tr(\mathbf{R}_{xl}) \leq P_C \quad \text{(restricts comm. TX antenna power)} \\
& \frac{1}{L} \sum_{l=1}^{L} \log_2 |\mathbf{I} + \mathbf{R}_{wl}^{-1} \mathbf{H} \mathbf{R}_{xl} \mathbf{H}^H| \geq C \quad \text{(restricts comm. average capaci} \\
& I(\mathbf{R}; \mathbf{P}) \leq M
\end{aligned}$$

where $\mathbf{R}_{xl}$ is the transmit covariance matrix, M an accepted scalar value for which we assume privacy is achieved.

Thank you!
Questions?

References I

B. Li and A.P. Petropulu,

Spectrum sharing between matrix completion based MIMO radars and a MIMO communication system

IEEE International Conference on Acoustics, Speech and Signal Processing April 2015, pp. 2444–2448.

B. Li, H. Kumar, and A.P. Petropulu,

A joint design approach for spectrum sharing between radar and communication systems

IEEE International Conference on Acoustics, Speech and Signal Processing March 2016, pp. 33063310.

B. Li, A.P. Petropulu,

Joint Transmit Design for Co-Existence of MIMO Wireless Communications and Sparse Sensing Radars in Clutter

IEEE Trans. on Aerospace and Electronic Systems, to appear in 2017.

References II

Z. Gao, H. Zhu, Y. Liu, M. Li, Z. Cao,
Location privacy in database-driven cognitive radio networks: Attacks and countermeasures.
INFOCOM, 2013 Proceedings IEEE (pp. 2751-2759). IEEE.

B. Bahrak, S. Bhattarai, A. Ullah, J-M Park, J. Reed, D. Gurney,
Protecting the primary users operational privacy in spectrum sharing
IEEE DySPAN 2014, pp. 236-247

J.A. Mahal, A. Khawar, A. Abdelhadi, T.C. Clancy,
Spectral Coexistence of MIMO Radar and MIMO Cellular System
IEEE Transactions on Aerospace and Electronic Systems, 53(2), 655-668.

B. Li, A.P. Petropulu, and W. Trappe,
Optimum Co-Design for Spectrum Sharing Between Matrix Completion Based MIMO Radars and a MIMO Communication System,
IEEE Transaction on Signal Processing, vol. 64, no. 17, pp. 4562-4575, 2016

S. Sodagari, A. Khawar, T. C. Clancy, and R. McGwier,
A projection based approach for radar and telecommunication systems coexistence,
IEEE Global Communications Conference (GLOBECOM), pp. 5010-5014.

R. Saruthirathanaworakun, J. M. Peha, and L. M. Correia,
Opportunistic sharing between rotating radar and cellular,
IEEE Journal on Selected Areas in Communications, vol. 30, no. 10, pp. 1900-1910.

A. Babaei, W. Tranter, T. Bose,
A nullspace-based precoder with subspace expansion for radar/communications coexistence,
IEEE Global Communications Conference (GLOBECOM), pp. 3487-3492.

A. Khawar, A. Abdelhadi, C.T. Clancy,
Coexistence analysis between radar and cellular system in LoS channel,
IEEE Antennas and Wireless Propagation Letters, vol. 15, pp. 972-975.

References IV

R.W. Heath,
Introduction to Wireless Digital Communication: A Signal Processing Perspective
Prentice Hall, 2017

A.F. Molisch
Wireless communications
John Wiley & Sons, 2012