

Enhancing the Physical Layer Security of Dual-functional Radar Communication Systems

Nanchi Su, Fan Liu, Christos Masouros

Department of Electronic and Electrical Engineering, University College London, London, UK

{nanchi.su.18, fan.liu, c.masouros}@ucl.ac.uk,

Abstract—Dual-functional radar communication (DFRC) system has recently attracted significant academic attentions as an enabling solution for realizing radar-communication spectrum sharing. During the DFRC transmission, however, the critical information could be leaked to the targets, which might be potential eavesdroppers. Therefore, the physical layer security has to be taken into consideration. In this paper, fractional programming (FP) problems are formulated to minimize the signal-to-interference-plus-noise ratio (SINR) at targets under the constraints for the SINR of legitimate users. By doing so, the secrecy rate of communication can be guaranteed. We first assume that communication CSI and the angle of the target are precisely known. After that, problem is extended to the cases with uncertainty in the target's location, which indicates that the target might appear in a certain angular interval. Finally, numerical results have been provided to validate the effectiveness of the proposed method showing that it is viable to guarantee both radar and secrecy communication performances by using the techniques we propose.

Index Terms—DFRC system, physical layer security, FP problem, secrecy rate.

I. INTRODUCTION

With the rapid growth of the wireless communication industry, the requirement for extra spectrum resources is on the rise, which motivates the network providers and the policy regulators to seek the chance for reusing frequency bands that are currently under-utilized by the radar systems [1]. To this end, the research of radar-communication coexistence (RCC) has recently attracted considerable attention from both academia and industry [2]–[4]. While various techniques have been proposed for realizing RCC, one crucial drawback is that most of these approaches require frequent cooperation between radar and communication systems, which might be difficult to be implemented in practice. Therefore, a more promising methodology would be to share both the spectrum and the hardware platform between these two functionalities, which requires no additional coordinations, and has motivated the study of the dual-functional radar-communication (DFRC) system [5]–[7]. In [8], the authors proposed to embed communication symbols into the sidelobes of the radar transmit beampattern, with the mainlobe being employed for target detection, which allows information delivery to single or multiple communication directions outside the mainlobe of the radar. To enable the DFRC transmission for non-line-of-sight (NLoS) communication channels, a joint beamforming design has been presented by [9] for simultaneous target detection and multi-user communications, which aims at approaching

a desired radar beampattern while guaranteeing the quality-of-service (QoS) of the downlink communication users. As a step further, several novel waveform designs have been proposed in [9] with the purpose of minimizing the multi-user interference (MUI) for downlink communications under radar-specific constraints.

It is noteworthy that in the DFRC scenarios, the targets to be detected might be potential eavesdroppers. This is most likely to appear in defense-related applications, where radar targets are usually adversary's combat platforms. In that case, it is highly possible that the critical information will be leaked to the radar targets by the emission of the DFRC waveform. Given the fact above, physical layer security (PHY-security) must be considered in DFRC designs [10], [11]. Particularly, it has been widely understood that the communication secrecy could be enhanced by exploiting the artificial noise (AN). For instance, in [12], the directional modulation method was adopted together with the AN to improve the communication performance within the direction of interest while degrading that of other directions. In [13], the authors studied the AN-aided secrecy rate maximum problem with no structural restrictions on the AN in multiple-input multiple-output (MISO) channel. Furthermore, in [14], AN based linear precoding designs have been proposed to ensure the secrecy performance in the system of massive multiple-input multiple-output (MIMO). Aiming to guarantee the QoS of the downlink users while confusing the eavesdropper, AN has been exploited in [15] for transmit beamforming design. Nevertheless, to the best of our knowledge, little research efforts have been taken towards the direction of enhancing the PHY-security of the DFRC system.

In this paper, we study the transmission security for the DFRC system, where the downlink cellular users are regarded as legitimate receivers, with the radar targets being regarded as potential eavesdroppers. Optimization problems are designed to guarantee the communication secrecy by minimizing the signal-to-interference-plus-noise ratio (SINR) at the target with the help of AN. In the meantime, the communication secrecy rate for the legitimate users is guaranteed by imposing SINR thresholds. By employing the assumption of perfect communication CSI, the proposed optimization problems are designed under precise and uncertain knowledge about the location of the target, respectively, following with the complexity analysis of each algorithm. Finally, numerical results are provided by Monte-Carlo simulations, which show that the proposed

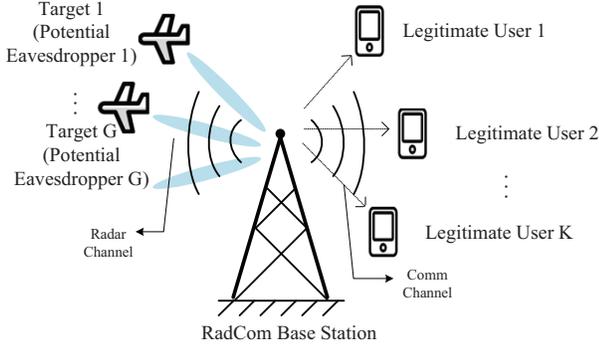


Fig. 1. Dual-functional Radar-Communication system detecting targets which work as potential eavesdroppers.

method is capable of guaranteeing the secrecy performance while formulating a desired spatial beam pattern towards the target.

II. SYSTEM MODEL

We consider a dual-functional MIMO RadCom system as shown in Fig. 1. The BS is equipped with an N -antenna uniform linear array (ULA). It serves K downlink single-antenna legitimate users while detecting targets at the same time. The targets are considered as potential eavesdroppers which may eavesdrop the information from the BS to legitimate users. For simplicity, we assume that there is a single target of interest in our system.

By exploiting the artificial noise in the beamforming design, the transmit matrix \mathbf{X} can be expressed as

$$\mathbf{X} = \mathbf{W}\mathbf{S} + \mathbf{N} \quad (1)$$

where $\mathbf{S} = [\mathbf{s}_1, \dots, \mathbf{s}_L] \in \mathbb{C}^{K \times L}$ is the desired signal from BS; $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_K]^T \in \mathbb{C}^{N \times K}$ is the beamforming matrix; $\mathbf{N} \in \mathbb{C}^{N \times L}$ is an artificial noise matrix generated artificially for avoiding leaking information to targets. Without the loss of generality, we assume $\mathbb{E}[\mathbf{s}_l \mathbf{s}_l^H] = \mathbf{I}$, where \mathbf{s}_l is the desired signal vector in the l -th time slot. It is assumed that $\mathbf{n}_i \sim \mathcal{CN}(0, \mathbf{R}_N)$, $\forall i$, where \mathbf{n}_i is i -th vector of \mathbf{N} . \mathbf{R}_N is the covariance matrix of the artificial noise. It follows that the covariance matrix of transmitted waveform can be written as

$$\mathbf{R}_X = \frac{1}{L} \mathbf{X} \mathbf{X}^H = \sum_{i=1}^K \mathbf{W}_i \mathbf{W}_i^H + \mathbf{R}_N. \quad (2)$$

where $\mathbf{W}_i \triangleq \mathbf{w}_i \mathbf{w}_i^H$. $\mathbb{E}\{\cdot\}$ denotes the statistical expectation and $(\cdot)^H$ represents the Hermitian transpose.

The received symbol at legitimate users is given as

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z} \quad (3)$$

where $\mathbf{H} \in \mathbb{C}^{K \times N}$ is the channel matrix; $\mathbf{X} \in \mathbb{C}^{N \times L}$ is the transmitted signal matrix, with L being the length of the radar pulse/communication frame, $\mathbf{Z} \in \mathbb{C}^{K \times L}$ is the noise matrix, with $\mathbf{z}_i \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_N)$, $\forall i$.

To evaluate the performance of the system, several performance metrics are employed in this paper. Firstly, the SINR of the i -th legitimate user is

$$\begin{aligned} \text{SINR}_i &= \frac{\mathbb{E} \left[|\mathbf{h}_i^H \mathbf{w}_i \mathbf{s}_i|^2 \right]}{\sum_{k \neq i, k=1}^K \mathbb{E} \left[|\mathbf{h}_i^H \mathbf{w}_k \mathbf{s}_k|^2 \right] + |\mathbf{h}_i^H \mathbf{N}_i|^2 + \sigma^2} \\ &= \frac{\text{tr}(\mathbf{h}_i^T \mathbf{W}_i \mathbf{h}_i^*)}{\sum_{k \neq i, k=1}^K \text{tr}(\mathbf{h}_i^T \mathbf{W}_k \mathbf{h}_i^*) + \text{tr}(\mathbf{h}_i^T \mathbf{R}_N \mathbf{h}_i^*) + \sigma^2}, \end{aligned} \quad (4)$$

Accordingly, the SINR at the target is given as

$$\text{SINR}_E = \frac{|\alpha|^2 \mathbf{a}^H(\theta) \sum_{i=1}^K \mathbf{W}_i \mathbf{a}(\theta)}{|\alpha|^2 \mathbf{a}^H(\theta) \mathbf{R}_N \mathbf{a}(\theta) + \sigma^2}, \quad (5)$$

where θ represents the azimuth angle of the target, $\mathbf{a}(\theta) = [1 \ e^{j2\pi\Delta \sin(\theta)} \ \dots \ e^{j2\pi(N-1)\Delta \sin(\theta)}]^T \in \mathbb{C}^{N \times 1}$ denotes the steering vector of the transmit antenna array; Δ is the antenna spacing between adjacent antennas being normalized by the signal wavelength. Following [16], the achievable secrecy rate can be defined as

$$\text{SR} = \frac{1}{2} \left[\min_i R_{C_i} - R_E \right]^+, \quad (6)$$

where $R_{C_i} = \log_2(1 + \text{SINR}_i)$, $R_E = \log_2(1 + \text{SINR}_E)$, $[\cdot]^+$ denotes $\max\{\cdot, 0\}$.

III. PROBLEM FORMULATION

A. Minimizing SINR_E With Perfect CSI and Precise Target Location

In this subsection, we aim to ensure secrecy rate by minimizing the SINR at target and guarantee the SINR at legitimate user maintaining above a certain threshold. Note that before designing the beamforming matrix and the artificial noise, an ideal radar beam pattern should be obtained as the benchmark, which can be given by solving the following constrained least-squares (LS) problem [17]

$$\begin{aligned} \min_{\eta, \mathbf{R}_d} \quad & \sum_{m=1}^M \left| \eta P_d(\theta_m) - \mathbf{a}^H(\theta_m) \mathbf{R}_d \mathbf{a}(\theta_m) \right|^2 \\ \text{s.t.} \quad & \text{tr}(\mathbf{R}_d) = P_0, \\ & \mathbf{R}_d \succeq 0, \mathbf{R}_d = \mathbf{R}_d^H, \\ & \eta \geq 0, \end{aligned} \quad (7)$$

where η is a scaling factor; P_0 is the transmission power budget, $\{\theta_m\}_{m=1}^M$ denotes an angular grid covering the detection angle range in $[-\pi/2, \pi/2]$, $\mathbf{a}(\theta_m)$ denotes steering vector, $P_d(\theta_m)$ is the desired ideal beam pattern gain at θ_m ,

\mathbf{R}_d represents the desired waveform covariance matrix. Given \mathbf{R}_d , our problem can be formulated as

$$\min_{\mathbf{W}_i, \mathbf{R}_N} \frac{|\alpha|^2 \mathbf{a}^H(\theta_0) \sum_{i=1}^K \mathbf{W}_i \mathbf{a}(\theta_0)}{|\alpha|^2 \mathbf{a}^H(\theta_0) \mathbf{R}_N \mathbf{a}(\theta_0) + \sigma^2}, \forall i \quad (8a)$$

$$s.t. \quad \|\mathbf{R}_X - \mathbf{R}_d\|^2 \leq \gamma_{bp}, \quad (8b)$$

$$\text{SINR}_i \geq \gamma_b, \forall i, \quad (8c)$$

$$P_t = P_0, \quad (8d)$$

$$\mathbf{W}_i = \mathbf{W}_i^H, \mathbf{W}_i \succeq 0, \forall i, \quad (8e)$$

$$\text{rank}(\mathbf{W}_i) = 1, \forall i, \quad (8f)$$

$$\mathbf{R}_N = \mathbf{R}_N^H, \mathbf{R}_N \succeq 0, \quad (8g)$$

where θ_0 denotes the location of targets known at the BS, γ_{bp} is a pre-defined threshold that constrains the mismatch between the designed covariance matrix \mathbf{R}_X and the desired \mathbf{R}_d . γ_b denotes the predefined SINR threshold of each legitimate user, and finally $\text{rank}(\cdot)$ is rank operator.

B. Minimizing SINR_E With Perfect CSI and Target Location Uncertainty

In this subsection, we consider the case that the target's position is roughly known within the angular interval $\Phi = [\theta_0 - \Delta\theta, \theta_0 + \Delta\theta]$ due to the uncertainty in the target parameter estimation. To guarantee the secrecy rate from transmitter to legitimate users, the objective function is reformulated to minimize the sum of target's SINR at the possible locations in the angular interval aforementioned. To this end, wider beam needs to be formulated towards the uncertain interval to avoid missing the target. Inspired by the 3dB beam pattern design approach in [18], in our problem, we formulate the beam pattern aiming to keep the power equivalent in the angular interval where the target is estimated to locate at. The proposed optimization problem can be formulated as

$$\min_{\mathbf{W}_i, \mathbf{R}_N} \sum_{\theta_m \in \Phi} \frac{|\alpha|^2 \mathbf{a}^H(\theta_m) \sum_{i=1}^K \mathbf{W}_i \mathbf{a}(\theta_m)}{|\alpha|^2 \mathbf{a}^H(\theta_m) \mathbf{R}_N \mathbf{a}(\theta_m) + \sigma^2}, \forall i \quad (9a)$$

$$s.t. \quad \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0) - \mathbf{a}^H(\theta_m) \mathbf{R}_X \mathbf{a}(\theta_m) \geq \gamma_s, \quad (9b)$$

$$\forall \theta_m \in \Omega$$

$$\mathbf{a}^H(\theta_k) \mathbf{R}_X \mathbf{a}(\theta_k) \leq (1 + \alpha) \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0), \quad (9c)$$

$$\forall \theta_k \in \Phi$$

$$(1 - \alpha) \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0) \leq \mathbf{a}^H(\theta_k) \mathbf{R}_X \mathbf{a}(\theta_k), \quad (9d)$$

$$\forall \theta_k \in \Phi$$

$$\text{SINR}_i \geq \gamma_b, \forall i, \quad (9e)$$

$$P_t = P_0, \forall i, \quad (9f)$$

$$\mathbf{W}_i = \mathbf{W}_i^H, \mathbf{W}_i \succeq 0, \forall i, \quad (9g)$$

$$\text{rank}(\mathbf{W}_i) = 1, \forall i, \quad (9h)$$

$$\mathbf{R}_N = \mathbf{R}_N^H, \mathbf{R}_N \succeq 0, \quad (9i)$$

where θ_0 is the main-beam location, Ω denotes the sidelobe region of interest, γ_s is a bound of sidelobe power.

IV. THE PROPOSED APPROACH

A. Approaches to Problem (8) and (9)

In this section, we propose an iterative algorithm to solve the above optimization problems. Initially, it is straightforward to see that (7) is convex, which can be readily solved by use of standard numerical tools, such as CVX. According to [19], the problem (8) and (9) presented in section III can be both regarded as fraction programming (FP) problem. Let us denote

$$M = |\alpha|^2 \mathbf{a}^H(\theta_0) \sum_{i=1}^K \mathbf{W}_i \mathbf{a}(\theta_0), \forall i,$$

$$N = |\alpha|^2 \mathbf{a}^H(\theta_0) \mathbf{R}_N \mathbf{a}(\theta_0) + \sigma^2$$

By the above notations, problem (8) can be relaxed in a convex form as

$$\begin{aligned} & \min_{\mathbf{W}_i, \mathbf{R}_N} M - cN, \\ s.t. \quad & \|\mathbf{R}_X - \mathbf{R}_d\|^2 \leq \gamma_{bp}, \\ & \text{SINR}_i \geq \gamma_b, \forall i, \\ & P_t = P_0, \\ & \mathbf{W}_i = \mathbf{W}_i^H, \mathbf{W}_i \succeq 0, \forall i, \\ & \text{rank}(\mathbf{W}_i) = 1, \forall i, \\ & \mathbf{R}_N = \mathbf{R}_N^H, \mathbf{R}_N \succeq 0, \end{aligned} \quad (10)$$

To solve the original problem (8), the scaling factor c needs to be updated in each iteration, yielding

$$c[t+1] = \frac{M[t]}{N[t]}, \quad (11)$$

where t is the index of iteration. To solve (10), SDR technique can be adopted by omitting the rank-1 constraint. For clarity, we summarize the above procedure in Algorithm 1.

Algorithm 1 Algorithm for solving FP problem (8)

Input: $\mathbf{H}, \mathbf{a}(\theta_0), \sigma^2, \alpha, \gamma_b, P_0, iter_{max} \geq 2, \gamma_{bp}$.

Output: $\mathbf{W}_i^{(iter)}, \mathbf{R}_N^{(iter)}, i = 1, \dots, K$.

1. Compute \mathbf{R}_d . Reformulate problem (8) by (10). Set the iteration threshold $\varepsilon > 0$. Initialize $c^{(0)}, c^{(1)}, |c^{(1)} - c^{(0)}| > \varepsilon$.
 - while** $iter \leq iter_{max}$ and $|c^{iter+1} - c^{iter}| \geq \varepsilon$ **do**
 2. Solve the new convex optimization problem.
 3. Update c by (11).
 4. Get updated $\mathbf{W}_i, \forall i$, and \mathbf{R}_N by solving (10) using SDR.
 5. $iter = iter + 1$.
 - end while**
 6. Obtain approximate solutions by eigenvalue decomposition or Gaussian randomization.
-

According to [19], it can be easily proven that c is non-decreasing during the iterations. Consequently, the convergence of Algorithm 1 can be guaranteed.

Following the similar procedure, we denote

$$A(\theta_m) = |\alpha|^2 \mathbf{a}^H(\theta_m) \mathbf{R}_N \mathbf{a}(\theta_m) + \sigma^2$$

$$B(\theta_m) = |\alpha|^2 \mathbf{a}^H(\theta_m) \sum_{i=1}^K \mathbf{W}_i \mathbf{a}(\theta_m)$$

Problem (9) can be rewritten in the form

$$\begin{aligned}
& \max_{\mathbf{w}_i, \mathbf{R}_N, \mathbf{y}} \sum_{\theta_m \in \Phi} \left(2y_m \sqrt{A(\theta_m)} - y_m^2 B(\theta_m) \right) \\
s.t. & \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0) - \mathbf{a}^H(\theta_m) \mathbf{R}_X \mathbf{a}(\theta_m) \geq \gamma_s, \forall \theta_m \in \Omega \\
& \mathbf{a}^H(\theta_k) \mathbf{R}_X \mathbf{a}(\theta_k) \leq (1 + \alpha) \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0), \forall \theta_k \in \Phi \\
& (1 - \alpha) \mathbf{a}^H(\theta_0) \mathbf{R}_X \mathbf{a}(\theta_0) \leq \mathbf{a}^H(\theta_k) \mathbf{R}_X \mathbf{a}(\theta_k), \forall \theta_k \in \Phi \\
& \text{SINR}_i \geq \gamma_b, \forall i, \\
& P_t = P_0, \forall i, \\
& \mathbf{W}_i = \mathbf{W}_i^H, \mathbf{W}_i \succeq 0, \forall i, \\
& \text{rank}(\mathbf{W}_i) = 1, \forall i, \\
& \mathbf{R}_N = \mathbf{R}_N^H, \mathbf{R}_N \succeq 0.
\end{aligned} \tag{12}$$

Let \mathbf{y} denote a collection of variables $\{y_1, \dots, y_M\}$, where y_m is updated iteratively by the following closed form when θ_m is fixed

$$y_m^* = \frac{\sqrt{A(\theta_m)}}{B(\theta_m)}. \tag{13}$$

The problem (12) can be solved again by the SDR technique. We note that eigenvalue decomposition or Gaussian randomization is required to obtain an approximate solution. For clarity, the above procedure is summarized in Algorithm 2.

Algorithm 2 Algorithm for solving FP problem (9)

Input: \mathbf{H} , $\mathbf{a}(\theta)$ or $\mathbf{a}(\theta_m)$, σ^2 , α , γ_b , P_0 , $iter_{max} \geq 2$, $\Delta\theta$.

Output: $\mathbf{W}_i^{(iter)}$, $\mathbf{R}_N^{(iter)}$, $i = 1, \dots, K$.

1. Compute \mathbf{R}_d . Reformulate problem (9) by (12). Set the iteration threshold $\varepsilon > 0$.

while $iter \leq iter_{max}$ and $\|\mathbf{y}^{iter+1} - \mathbf{y}^{iter}\| \geq \varepsilon$ **do**

2. Solve the new convex optimization problem.

3. Update \mathbf{y} by (13).

4. Get updated $\mathbf{W}_i, \forall i$, and \mathbf{R}_N by solving (12) using SDR.

5. $iter = iter + 1$.

end while

6. Obtain approximate solutions by eigenvalue decomposition or Gaussian randomization.

B. Complexity Analysis

In this subsection, we analyze the computational complexity of problem (8) and (9), both of which have been transformed to SDP problem solved by interior point method (IPM) [20]. Given $\epsilon > 0$, we obtain an ϵ -optimal solution after the required number of iterations. In the first optimization problem, to generate the ideal beampattern \mathbf{R}_d in (7), which is a typical SDP problem including a linear matrix inequality (LMI) constraint of size $2N$, two LMI constraints of size N , and an LMI constraint of size 1, so the complexity is $\mathcal{O}(\sqrt{4N+1}(4N^6 + 3N^5 + N^4 + N^2) \ln(1/\epsilon))$. It is notable that problem (8) involves both LMI and second-order cone (SOC) constraints, which contains $2K + 1$ LMI constraints of size N , $K + 1$ LMI constraints of size $2N$, an LMI

constraint of size 1 and an SOC constraint of size N . Accordingly, the computational complexity in (8) can be given in (14). We note that $\mathcal{O}((K + 1)N^3)$ is the complexity of eigenvalue decomposition¹. For simplicity, the computational complexity can be commonly given as $\mathcal{O}(N_{iter}K^{3.5}N^{6.5} \ln(1/\epsilon)) + \mathcal{O}((K + 1)N^3)$, where N_{iter} represents iteration times.

Similarly, in problem (9), we regard both Ω and Φ as discrete domains which represent a collection of angles region. This problem involves LMI constraints only. Specifically, it includes $K + 1$ LMI constraints of size $2N$, $2K + 2\Phi + \Omega + 1$ LMI constraints of size N , an LMI constraints of size 1. The iteration complexity is shown in (15). Then, the computational complexity can be approximately given as $\mathcal{O}(N_{iter}K^{3.5}N^{6.5} \ln(1/\epsilon)) + \mathcal{O}((K + 1)N^3)$.

V. SIMULATION RESULTS

In this section, we present the simulation results of proposed methods. For all simulations, we employ a ULA with half-wavelength spacing between adjacent antennas. The length of communication frame/radar pulse is set as $L = 30$. Without loss of generality, each entry of the channel matrix \mathbf{H} is assumed to obey standard Complex Gaussian distribution, i.e., $h_{i,j} \sim \mathcal{CN}(0, 1)$.

We first show in Fig. 2 the obtained radar beampatterns with precise and uncertain target angles, which are formulated by solving problem (8) and (9) respectively. We set $\Delta\theta = 5^\circ$ and $\Delta\theta = 10^\circ$ when the target location is known roughly, which represented by dashed. For the case of precise target angle, it is noted that a narrow beam is formulated towards the direction of interest. For the cases with uncertain target angles, on the other hand, the mainbeam power decreases with the angle of location uncertainty being broadened, which demonstrates the tradeoff between the power of beampattern pointing to the target location and the precision of target location known at transmitter.

The convergence of SINR at eavesdropper is demonstrated in Fig. 3. It is obvious that both Algorithm 1 and 2 converge to the optimum within a modest number of iterations.

The secrecy rate of the legitimate communication link in terms of a rising SINR threshold γ_b is shown in Fig. 4, with $\gamma_{bp} = 60$, $\gamma_s = 10^4$. It can be observed that the secrecy rate increases with the growth of the SINR threshold at legitimate users. It is noteworthy that the secrecy rate for the case with precisely known target location is higher than that of the case with uncertain target location. Additionally, the secrecy rate reduces with the descending tendency of the power budget.

Finally, Fig. 5 represents the secrecy rate performance versus the given threshold of sidelobe γ_s , with $P_0 = 30\text{dBm}$, $\Delta\theta = 5^\circ$, and the SINR threshold at users is given as $\gamma_b = 10\text{dB}$ and $\gamma_b = 20\text{dB}$ respectively. It is notable that the secrecy rate decreases with the increasing of γ_s . It is notable that the decreasing tendency of secrecy rate gets obvious when γ_s is greater than 30dB.

¹We adopt eigenvalue decomposition method to get the approximate result because of the high complexity of Gaussian randomization.

$$\begin{aligned} & \mathcal{O} \left(N_{iter} \ln(1/\varepsilon) \sqrt{2N(K+1) + K + 3} \cdot KN^2 \left((K+1)(KN^2 + 1) + 2N^3(K^2N + KN + K + 1) \right) \right) \\ & + \mathcal{O} \left(N_{iter} \ln(1/\varepsilon) \sqrt{2N(K+1) + K + 3} \cdot KN^4 (K^2N^2 + 1) \right) + \mathcal{O} \left((K+1)N^3 \right) \end{aligned} \quad (14)$$

$$\begin{aligned} & \mathcal{O} \left(N_{iter} \ln(1/\varepsilon) \sqrt{2N(K+1) + K + \Omega_0 + 2\Phi_0 + 1} \cdot KN^2 (KN^2 + 1) (K + \Omega_0 + 2\Phi_0 + 1) \right) \\ & + \mathcal{O} \left(N_{iter} \ln(1/\varepsilon) \sqrt{2N(K+1) + K + \Omega_0 + 2\Phi_0 + 1} \cdot KN^2 (2N^3(K^2N + KN + K + 1) + K^2N^4) \right) \\ & + \mathcal{O} \left((K+1)N^3 \right) \end{aligned} \quad (15)$$

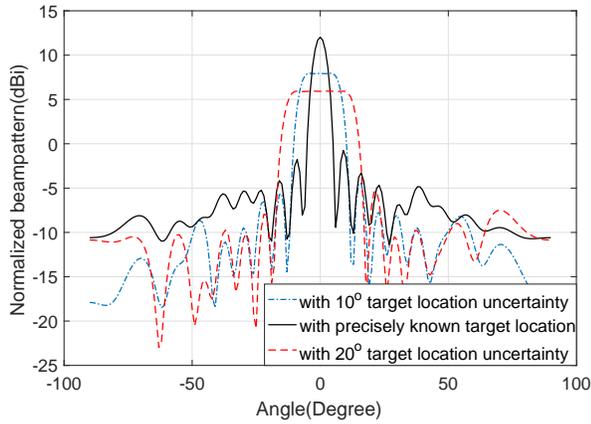


Fig. 2. Radar beam pattern obtained on different circumstances, $N = 18$, $K = 4$, $\gamma_b = 10$, $P_0 = 30\text{dBm}$.

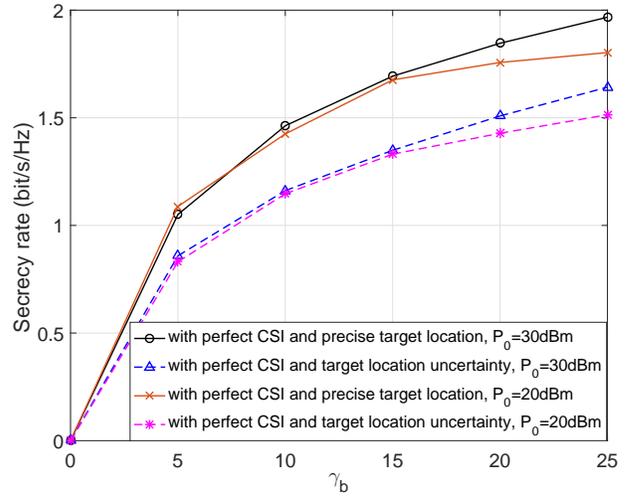


Fig. 4. Achievable secrecy rate versus the threshold of SINR at legitimate users, $N = 18$, $K = 4$.

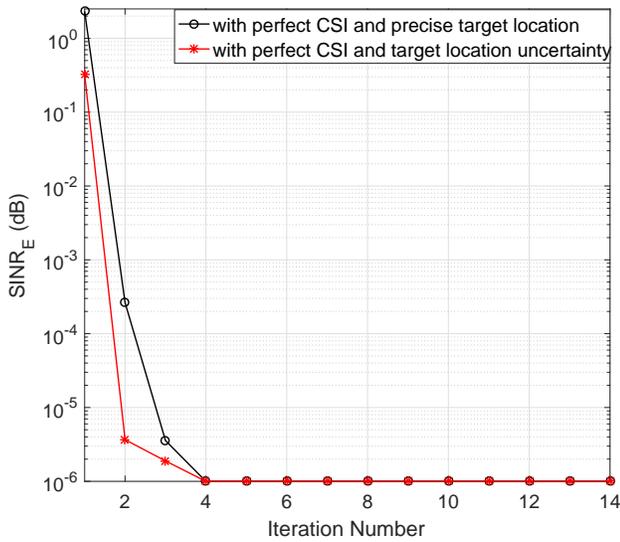


Fig. 3. SINR at eavesdropper with iteration number variance, $N = 18$, $K = 4$, $\gamma_b = 10$, $P_0 = 30\text{dBm}$.

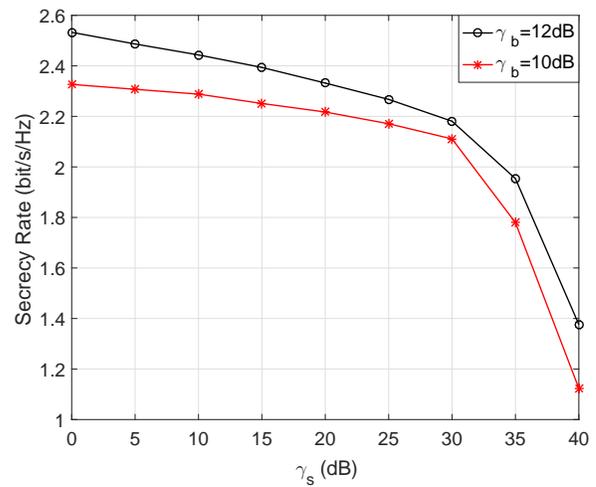


Fig. 5. Achievable secrecy rate versus the threshold of sidelobe power with different SINR threshold at legitimate users, $N = 18$, $K = 4$, $P_0 = 30\text{dBm}$.

VI. CONCLUSION

We have studied the AN-aided method to ensure the physical layer security in DFRC system. It is assumed that the communication CSI is perfectly known while the target location might be inaccurately estimated. To guarantee communication secrecy while detecting targets (which are potential eavesdroppers), we have minimized the SINR at the targets by formulating FP optimization problems, which can be equivalently recast as a series of sub-problems with convex objective functions. By dropping the rank-1 constraint, each sub-problem can be relaxed as an SDP, and can be thus solved by numerical tools. Numerical results have been provided to verify the effectiveness of the proposed approaches, which show that it is feasible to guarantee both the performance of the radar beam pattern and the communication secrecy by the proposed optimization based designs.

ACKNOWLEDGEMENT

This work has received funding from the the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 793345 and China Scholarship Council (CSC).

REFERENCES

- [1] M. Rihan and L. Huang, "Optimum co-design of spectrum sharing between MIMO radar and MIMO communication systems: An interference alignment approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11 667–11 680, 2018.
- [2] F. Liu, C. Masouros, A. Li, and T. Ratnarajah, "Robust MIMO beamforming for cellular and radar coexistence," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 374–377, June 2017.
- [3] J. A. Mahal, A. Khawar, A. Abdelhadi, and T. C. 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.
- [4] F. Liu, C. Masouros, A. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *arXiv preprint arXiv:1906.00789*, 2019.
- [5] F. Liu, L. Zhou, C. Masouros, A. Li, W. Luo, and A. Petropulu, "Toward dual-functional radar-communication systems: Optimal waveform design," *IEEE Transactions on Signal Processing*, vol. 66, no. 16, pp. 4264–4279, Aug 2018.
- [6] F. Liu, C. Masouros, A. Li, T. Ratnarajah, and J. Zhou, "Mimo radar and cellular coexistence: A power-efficient approach enabled by interference exploitation," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3681–3695, July 2018.
- [7] F. Liu, A. Garcia-Rodriguez, C. Masouros, and G. Geraci, "Interfering channel estimation in radar-cellular coexistence: How much information do we need?" *IEEE Transactions on Wireless Communications*, pp. 1–1, 2019.
- [8] A. Hassanien, M. G. Amin, Y. D. Zhang, and F. Ahmad, "Dual-function radar-communications: Information embedding using sidelobe control and waveform diversity," *IEEE Transactions on Signal Processing*, vol. 64, no. 8, pp. 2168–2181, 2016.
- [9] F. Liu, C. Masouros, A. Li, H. Sun, and L. Hanzo, "MU-MIMO communications with MIMO radar: From co-existence to joint transmission," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2755–2770, April 2018.
- [10] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.
- [11] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.
- [12] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6658–6662, 2018.
- [13] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.
- [14] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.
- [15] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.
- [16] S. Parsaefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE transactions on information forensics and security*, vol. 10, no. 10, pp. 2095–2107, 2015.
- [17] D. R. Fuhrmann and G. San Antonio, "Transmit beamforming for MIMO radar systems using signal cross-correlation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 44, no. 1, pp. 171–186, 2008.
- [18] J. Li and P. Stoica, "MIMO radar with colocated antennas," *IEEE Signal Processing Magazine*, vol. 24, no. 5, pp. 106–114, 2007.
- [19] K. Shen and W. Yu, "Fractional programming for communication systems: part i: Power control and beamforming," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2616–2630, 2018.
- [20] K. Wang, A. M. So, T. Chang, W. Ma, and C. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Transactions on Signal Processing*, vol. 62, no. 21, pp. 5690–5705, Nov 2014.