




# Secrecy Rate Optimizations for MIMO Communication Radar

ANASTASIOS DELIGIANNIS , Member, IEEE  
ABDULLAHI DANIYAN, Student Member, IEEE  
SANGARAPILLAI LAMBOTHARAN , Senior Member, IEEE  
JONATHON A. CHAMBERS , Fellow, IEEE  
Loughborough University, Loughborough U.K.

**In this paper, we investigate transmit beam pattern optimization techniques for a multiple-input multiple-output radar in the presence of a legitimate communications receiver and an eavesdropping target. The primary objectives of the radar are to satisfy a certain target-detection criterion and to simultaneously communicate safely with a legitimate receiver by maximizing the secrecy rate against the eavesdropping target. Therefore, we consider three optimization problems, namely target return signal-to-interference-plus-noise ratio maximization, secrecy rate maximization, and transmit power minimization. However, these problems are nonconvex due to the nonconcavity of the secrecy rate function, which appears in all three optimizations either as the objective function or as a constraint. To solve this issue, we use Taylor series approximation of the nonconvex elements through an iterative algorithm, which recasts the problem as a convex problem. Two transmit covariance matrices are designed to detect the target and convey the information safely to the communication receiver. Simulation results are presented to validate the efficiency of the aforementioned optimizations.**

Manuscript received March 31, 2017; revised November 1, 2017 and February 26, 2018; released for publication February 26, 2018. Date of publication March 28, 2018; date of current version October 10, 2018.

DOI. No. 10.1109/TAES.2018.2820370

Refereeing of this contribution was handled by F. Gini.

This work was supported in part by the Engineering and Physical Sciences Research Council under Grant EP/K014307/1 and in part by the MOD University Defence Research Collaboration in Signal Processing.

Authors' addresses: A. Deligiannis, A. Daniyan, and S. Lambotharan are with The Wolfson School of Mechanical, Manufacturing and Electrical Engineering, Loughborough University, Loughborough LE11 3TU, U.K., E-mail: (A.Deligiannis@lboro.ac.uk; A.Daniyan@lboro.ac.uk; S.Lambotharan@lboro.ac.uk); J. A. Chambers is with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon Tyne NE1 7RU, U.K., E-mail: (jonathon.chambers@ncl.ac.uk). (*Corresponding author: Anastasios Deligiannis.*)

0018-9251 © 2018 CCBY

## I. INTRODUCTION

Multiple-Input multiple-output (MIMO) technology has been widely studied in the communication literature, providing exciting improvements to the capacity and coverage of a network. MIMO radar technology has also attracted significant interests recently. The key factor that makes a MIMO radar superior to other radar systems is its waveform diversity, indicating the ability of a MIMO radar to simultaneously emit several diverse, possibly orthogonal waveforms via multiple antennas, as compared to phased array radars that transmit scaled versions of the same waveform [1]. In the existing radar literature, there are two primary MIMO schemes, those that employ colocated antennas [2] and radars incorporating widely separated antennas (bistatic and multistatic radars) [3]. MIMO radar technology is exploited in the following dominant fields: beamforming, waveform design, target-detection optimization, and radar imaging [4]–[6]. Among the advantages of MIMO radar technology is the direct applicability of adaptive array techniques, adaptive beamforming [7], power allocation optimization [8], higher angular resolution, multiple targets detection [9], and the ability to acquire the target's geometrical characteristics through the spatial diversity of the target's radar cross section (RCS).

The gigantic growth of wireless multimedia applications and the need for faster communications in the last decade have led to an increasing demand on radio frequency bandwidth and an expanded share of existing frequency allocations. Hence, the coexistence of radar and wireless communication in a system has been proposed recently to ease the competition over spectrum bandwidth [10], [11]. In particular, this novel dual-function scheme employs the same transmit and receive elements to achieve simultaneously both radar target-detection purposes and information transfer to legitimate receivers [12]. A pioneering joint radar-communication system was introduced in [13], where the authors embedded information into the radar signal for communication purposes. More specifically, a set of unique radar waveforms was designed, each representing a communication symbol, while maintaining an acceptable radar performance. The ability of multisensor radar systems to control and introduce variations in the sidelobe level (SLL) toward a specific spatial direction has motivated the devise of time-modulated (TM) or amplitude-modulated dual-function radar-communication (DFRC) systems. The main idea is to maintain a radar function in the main lobe of the signal, while realizing a communication in the sidelobe. To achieve this, Euziere *et al.* [14] utilized sparse TM arrays or phase-only synthesis TM arrays to introduce variations in the SLL toward a desired direction. A DFRC system employing sidelobe control of the transmit beamforming and waveform diversity was developed in [15], where two transmit weight vectors are designed to carry multiple simultaneously transmitted orthogonal waveforms, embedding a sequence of information bits. Phase-rotational invariance in tandem with transmit beamforming techniques have been proposed in [16] for information embedding transmission.

Blunt *et al.* [17] and [18] addressed the problem of embedding a covert communication signal amongst the scattering from an incident radar pulse.

Most of the existing works in DFRC systems focused on techniques to transmit information toward a legitimate receiver, without paying much attention to the possibility of eavesdroppers in the environment. In the communication literature, the security of wireless transmission is of great importance [19], [20]. The additional degrees of freedom and the diversity gain offered by multiantenna elements can facilitate secret communications in MIMO communication systems [21]. Different MIMO secrecy rate optimizations have been investigated in [22], in the presence of a multiple-antenna eavesdropper. In particular, two optimization problems are designed, namely power minimization and secrecy rate maximization problems. A similar approach was studied in [23] with the addition of a multiple-antenna cooperative jammer to induce further interference to the eavesdropper, and hence maximize the secrecy rate at the legitimate receiver. Friendly jammer nodes have also been considered in [24] to confuse the eavesdroppers by transmitting interfering signals toward them and increase the physical layer security of a wiretap fading channel. Introducing cooperative transmission into secrecy communication systems to minimize the outage probability was studied in [25]. Krikidis *et al.* [26] utilized relay selection for secure cooperative networks. In particular, two relays were selected, one to assist the information delivery to the receiver and a second to create interference at the eavesdropper. Furthermore, another countermeasure against the eavesdropper is to embed artificial noise in the transmitted signal as investigated in [27] and [28], where an isotropic artificial noise scheme based on an orthogonal projection method [27] and a spatially selective artificial noise obtained by optimal beamformers design [28] were developed.

To the best of our knowledge, although the coexistence of radar-communication systems is a fast emerging research field, there is no previous work regarding secure transmissions in these systems. The need for safe communication in a DFRC system is further emphasized since the desired communication may contain sensitive information, such as target characterization and command and control signals. Thus, in this paper, we propose a DFRC system that provides simultaneous target detection capabilities and secure communication with a legitimate receiver. These aspects render this model particularly attractive for defense applications, when the information is usually sensitive and confidential. In particular, we introduce a DFRC system that consists of a tracking MIMO radar, a legitimate communication receiver, and a target equipped with multiple antennas. Principal objectives of the radar system are to attain a desired detection performance and to transmit information to the legitimate receiver while disabling the eavesdropper decoding the communication signals. Hence, apart from the target detection, safe communication is of utmost importance for our DFRC system. Following the aforementioned communication literature, we utilize the notion of secrecy

rate to guarantee the safe information transfer among the radar and the legitimate receiver, while satisfying a desired criterion for target detection. In the scenario under consideration, the target eavesdropper may intercept the communication signal transmitted from the MIMO radar to the legitimate receiver. In order to minimize the probability of interception, we transmit a pseudorandom distortion signal in addition to the information signal. This distortion signal cancels the ability of the eavesdropper to decode the information transmitted from the MIMO radar. However, the distortion signal can be used for target detection. Thus, we design transmit covariance matrices of both the communication signal and the distortion signal by solving three optimizations, namely secrecy rate maximization, target return signal-to-interference-plus-noise ratio (SINR) maximization, and transmit power minimization.

The secrecy rate function for our radar system is non-concave and renders all three optimizations nonconvex. In order to reformulate the optimization problems as convex problems, we utilize the Taylor series approximation of the secrecy rate function, which is proven to be concave. The resulting DFRC system enjoys both the required target-detection performance and secure communications under a specified resource budget.

The remainder of this paper is organized as follows. The system model and the definition of the secrecy rate for a DFRC system is given in Section II. Section III focuses on the system optimizations and the reformulation of the problems to convex form utilizing Taylor series approximation. The simulation results and comments upon the results are presented in Section IV and the final concluding remarks are given in Section V.

*Notation:* We use bold lowercase letters and bold uppercase letters to denote column vectors and matrices, respectively.  $\mathbf{a}^H$  gives the Hermitian of the vector  $\mathbf{a}$  and  $\mathbf{a}^T$  denotes its transpose.  $\mathbf{A}(i, j)$  corresponds to the element located on the  $i$ th row and  $j$ th column of matrix  $\mathbf{A}$ . The trace of a matrix  $\mathbf{A}$  is represented by  $\text{Tr}(\mathbf{A})$ .  $\mathbf{I}_M$  stands for the  $M \times M$  identity matrix. The Euclidean norm is denoted by  $\|\cdot\|$ . An  $N \times 1$  vector of ones is indicated by  $\mathbf{1}_N$ . The notation  $[x]^+$  stands for  $\max\{x, 0\}$ .

## II. SYSTEM MODEL

We consider a joint radar/communication network that consists of a MIMO radar, a legitimate multiantenna receiver, and a target, as shown in Fig. 1. It is assumed that the target incorporates a multiantenna receiver and may intercept incoming signals. The two major objectives for the radar are to secure a certain detection criterion for the target and synchronously transmit information to the legitimate receiver, while disabling the eavesdropping target from decoding the information signal. In order to achieve this, the radar transmits two different signals at the same time, where both signals are used to detect the target. However, the first signal embeds the desired information for the legitimate receiver, whereas the second signal consists of false information to confuse the eavesdropper.

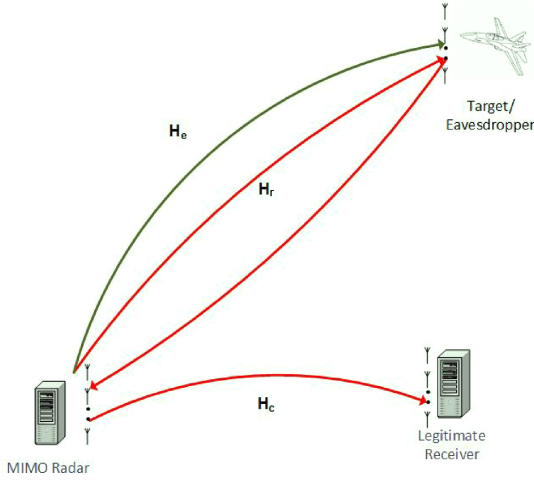


Fig. 1. Joint MIMO radar-communication system with a target that could also act as an eavesdropper.

It is presumed that the MIMO radar consists of  $M$  collocated transmit/receive antennas. The legitimate receiver and the eavesdropping target are equipped with  $N_c$  and  $N_e$  antennas, respectively. In order to detect the target and transmit the desired information to the legitimate receiver, the transmit array of the MIMO radar emits a modulated waveform  $s_1(t)$ , which consists of  $L_1$  information bits, defined as follows:

$$s_1(t) = \sum_{i=0}^{L_1-1} \delta_{1i} m(t - iT)$$

where  $\delta_{1i}$  denotes the  $i$ th information bit,  $m(t) = \sum_{i=0}^{L_m-1} c_i \Pi(t - iT_c)$  defines the modulation waveform,  $c_i$  denotes the  $i$ th chip value of the modulation sequence,  $\Pi(t)$  stands for the rectangular pulse of duration  $T_c$ ,  $T = L_m T_c$  represents the information bit duration, and  $L_m$  is the spreading gain [29]. To secure both the detection of the target and the interruption to the eavesdropper, the MIMO radar simultaneously transmits a pseudorandom distortional waveform  $s_2(t)$ , which is written as follows:

$$s_2(t) = \sum_{i=0}^{L_2-1} \delta_{2i} \Pi(t - iT_c)$$

where  $\delta_{2i}$  is the  $i$ th random bit of the distortional pseudorandom sequence and  $L_2$  denotes the length of the sequence. As expected, the distortion signal must be different from the information signal in order to confuse the eavesdropper and to cause decoding failure for the eavesdropper. Both  $s_1(t)$  and  $s_2(t)$  are assumed to have unit variance, however, the power of these signals will be controlled by the norm of the beamformer vectors. We expect very large values for  $L_1$  and  $L_2$ , so that both the information signal and distortion have almost zero autocorrelation (for nonzero time lags) and correlation values. This will provide desired range-Doppler ambiguity function for the radars. Another possible improvement to range-Doppler ambiguity function can be obtained by designing the distortion signals such that when added with the communication signals, the overall

waveform provides a good range-Doppler ambiguity function. However, it means that a set of distortion functions needs to be designed according to instantaneous information bits that are used for communication signals. Such waveform design is not considered in this paper, however, it may be an area of further investigation.

The channel gain coefficient matrix among the transmit and receive arrays of the MIMO radar for a signal impinging on a far-field target is denoted as  $\mathbf{H}_r \in \mathbb{C}^{M \times M}$  and it depends on the respective target position and RCS, as shown in the following definition [1]:

$$\mathbf{H}_r = \beta \mathbf{b}(\theta_t) \mathbf{a}(\theta_t)^T$$

where  $\beta$  is the complex amplitude proportional to the RCS of the target and  $\mathbf{a}(\theta_t)$  and  $\mathbf{b}(\theta_t)$  are the  $M \times 1$  transmit and receive steering vectors for the MIMO radar corresponding to the target, respectively, given as follows:

$$\begin{aligned} \mathbf{a}(\theta_t) &= [1, e^{j\frac{2\pi}{\lambda} d_r \sin(\theta_t)}, \dots, e^{j\frac{2\pi}{\lambda} (M-1) d_r \sin(\theta_t)}]^T \\ \mathbf{b}(\theta_t) &= [1, e^{j\frac{2\pi}{\lambda} d_r \sin(\theta_t)}, \dots, e^{j\frac{2\pi}{\lambda} (M-1) d_r \sin(\theta_t)}]^T \end{aligned}$$

where  $d_r$  denotes the distance between the adjacent antennas of the radar,  $\theta_t$  is the azimuth direction of the target when the radar is considered as reference, and  $\lambda$  is the wavelength of the transmitted signal. Furthermore, the channel coefficient matrices between the radar and the legitimate receiver as well as the eavesdropping target are represented by  $\mathbf{H}_c \in \mathbb{C}^{N_c \times M}$  and  $\mathbf{H}_e \in \mathbb{C}^{N_e \times M}$ , respectively.  $\mathbf{H}_e$  is obtained as follows:

$$\mathbf{H}_e = \alpha \tilde{\mathbf{b}}(\theta_r) \mathbf{a}(\theta_t)^T$$

where  $\alpha$  represents a predefined propagation loss variable,  $\tilde{\mathbf{b}}(\theta_r) = [1, e^{j\frac{2\pi}{\lambda} d_t \sin(\theta_r)}, \dots, e^{j\frac{2\pi}{\lambda} (N_e-1) d_t \sin(\theta_r)}]^T$  is the receive steering vector at the receiving antenna array of the eavesdropping target,  $d_t$  is the distance among the adjacent antennas of the eavesdropper, and  $\theta_r$  denotes the direction of the MIMO radar as observed from the eavesdropping target. Due to the line of sight of the aerial target, the matrices  $\mathbf{H}_r$  and  $\mathbf{H}_e$  are rank one according to the above-mentioned formulation. However, the matrix  $\mathbf{H}_c$  does not necessarily need to be rank one, due to multipath propagations and scatterers. Matrix  $\mathbf{H}_c$  can be estimated using training signals emitted from the MIMO radar and received at the legitimate receiver. We consider that the environment is quasi-stationary during the transmission of a number of data packets, and hence matrix  $\mathbf{H}_c$  is considered to be known to the legitimate receiver and the transmitter through appropriate feedback channel. In the simulation, we assume elements of this matrix to go through Rayleigh fading, hence assumed the elements to be zero mean circularly symmetric complex Gaussian variables. At this point, we can model the received signals at the radar receiver array, the legitimate receiver, and the eavesdropping target as follows:

$$\begin{aligned} \mathbf{y}_r(t) &= \mathbf{H}_r \mathbf{x}_1(t - \tau_r) p(t) + \mathbf{H}_r \mathbf{x}_2(t - \tau_r) p(t) + \mathbf{n}_r(t) \\ \mathbf{y}_c(t) &= \mathbf{H}_c \mathbf{x}_1(t - \tau_c) + \mathbf{H}_c \mathbf{x}_2(t - \tau_c) + \mathbf{n}_c(t) \\ \mathbf{y}_e(t) &= \mathbf{H}_e \mathbf{x}_1(t - \tau_e) \hat{p}(t) + \mathbf{H}_e \mathbf{x}_2(t - \tau_e) \hat{p}(t) + \mathbf{n}_e(t) \end{aligned} \quad (1)$$

where  $\mathbf{x}_i(t) = \mathbf{w}_i s_i(t)$ ,  $i = 1, 2$ , represents the  $M \times 1$  signal intended for the communication receiver when  $i = 1$  and the distortional signal when  $i = 2$ ;  $\mathbf{w}_i$  denotes the  $M \times 1$  transmit beamforming vector corresponding to signal  $s_i(t)$ . The round-trip delay between the MIMO radar and the target is given by  $\tau_r$ , the delay between the radar and the communication receiver is denoted by  $\tau_c$  and the one-way delay from the radar to the target is  $\tau_e = \frac{\tau_r}{2}$ .  $p(t)$ , and  $\hat{p}(t)$  represents the Doppler effect at the radar receiver and the eavesdropper, respectively, where  $p(t) = e^{j2\pi f_D t}$  and  $\hat{p}(t) = e^{j2\pi \hat{f}_D t}$ ,  $f_{D,i}$  and  $\hat{f}_{D,i}$  denote the normalized Doppler shifts at the radar and the eavesdropper, respectively. Since we assume that the legitimate communication receiver is stationary, there is no Doppler effect at its receivers, however fading is considered according to Rayleigh fading model as described above. The noise vectors at the radar receive array, the legitimate receiver and the eavesdropping target are considered as zero mean circularly symmetric white Gaussian noise (WGN) with variance  $\sigma_r^2$ ,  $\sigma_c^2$ , and  $\sigma_e^2$ , and are denoted by  $\mathbf{n}_r(t)$ ,  $\mathbf{n}_c(t)$ , and  $\mathbf{n}_e(t)$ , respectively.

The waveform lengths  $L_1$  and  $L_2$  can be different, however, we assume we process the radar return at every  $L = \min(L_2, L_1 L_m)$  samples, i.e., at every  $LT_c$  seconds. We also assume  $L$  to be large enough so that  $\int_{LT_c} s_1(t)s_2(t)dt$  is arbitrarily small. The received signal  $\mathbf{y}_r(t)$  at the MIMO radar is sent to a bank of two matched filters, designed to match each of the orthogonal waveforms  $s_1(t)$  and  $s_2(t)$  over the period of  $L$  samples, incorporating the appropriate time delay and Doppler shift. Subsequently, the corresponding energy at the output of the matched filter is accumulated and the SINR regarding the detection of the target can be written as follows:

$$\text{SINR}_r = \frac{\|\mathbf{H}_r \mathbf{W}_1 \mathbf{H}_r^H\| + \|\mathbf{H}_r \mathbf{W}_2 \mathbf{H}_r^H\|}{\epsilon_1 + \epsilon_2 + \sigma_r^2} \quad (2)$$

where  $\mathbf{W}_1 = \mathbf{w}_1 \mathbf{w}_1^H$  and  $\mathbf{W}_2 = \mathbf{w}_2 \mathbf{w}_2^H$  denote the transmit covariance matrices of the legitimate information signal and the distortion signal, respectively,  $\epsilon_1 = \frac{\|\mathbf{H}_r \mathbf{W}_1 \mathbf{H}_r^H\|}{L}$  and  $\epsilon_2 = \frac{\|\mathbf{H}_r \mathbf{W}_2 \mathbf{H}_r^H\|}{L}$  represent the residual interference when matched filtering the received signal with  $s_2(t)$  and  $s_1(t)$ , respectively, and  $L$  denotes the radar matched filtering sequence length. Since we assume that  $L$  is arbitrarily large,  $\epsilon_1$  and  $\epsilon_2$  can be neglected for the rest of this paper. It is important to mention that both signals are utilized for target detection at the radar receiver, and thus they both appear at the numerator of (2). However, the legitimate receiver and the eavesdropper can harvest desired information only from  $\mathbf{x}_1(t)$ , while  $\mathbf{x}_2(t)$  is considered as interference. Both the legitimate receiver and the eavesdropper perform matched filtering on the received signal using the modulation waveform  $m(t)$  at every  $L_m T_c$  seconds to decode the information bits. Hence, the achievable transmission rate by the legitimate receiver can be expressed as [30] follows:

$$R_c = \log \left| \mathbf{I} + (\mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H) \left( \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} + \sigma_c^2 \right)^{-1} \right|. \quad (3)$$

Similarly, the achievable rate of the eavesdropper, while intercepting desired information transmitted from the MIMO radar and intended for the legitimate receiver can be written as follows:

$$R_e = \log \left| \mathbf{I} + (\mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H) \left( \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} + \sigma_e^2 \right)^{-1} \right|. \quad (4)$$

The secrecy rate of the legitimate user against the eavesdropper is defined as the difference between the achievable rates at the legitimate receiver and the eavesdropper [19], [31]:

$$\text{SR} = [R_c - R_e]^+. \quad (5)$$

### III. SYSTEM OPTIMIZATIONS

In this section, we consider three optimization problems that lead to an efficient system, in terms of target detection combined with secure communication and energy efficient operation. More specifically, we design a secrecy rate maximization problem, a power minimization problem, and a target return SINR maximization problem. It is assumed that the MIMO radar has private information on the target and the legitimate receiver locations, and hence perfect channel state information ( $\mathbf{H}_r$ ,  $\mathbf{H}_c$ ,  $\mathbf{H}_e$ ).

#### A. Secrecy Rate Maximization

It is typical in radar systems design, the target detection to be constrained by a certain SINR threshold. In order to satisfy the detection criterion and a maximum transmit power budget, we consider the following secrecy rate maximization problem:

$$\begin{aligned} & \max_{\mathbf{W}_1, \mathbf{W}_2} \text{SR} \\ & \text{s.t.} \quad \text{SINR}_r \geq \gamma_r \\ & \quad \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\ & \quad \mathbf{W}_1 \geq 0, \mathbf{W}_2 \geq 0 \end{aligned} \quad (6)$$

where  $\gamma_r$  represents the predefined SINR threshold and  $P_{\max}$  denotes the maximum available power for the system. The last two constraints suggest that the two transmit covariance matrices must be positive semidefinite. By substituting (2) and (5) into (6), we can reformulate the optimization problem as in the following equation:

$$\begin{aligned} & \max_{\mathbf{W}_1, \mathbf{W}_2} \log \left| \mathbf{I} + (\mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H) \left( \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} + \sigma_c^2 \right)^{-1} \right| - \log \\ & \quad \times \left| \mathbf{I} + (\mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H) \left( \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} + \sigma_e^2 \right)^{-1} \right| \\ & \text{s.t.} \quad \frac{\|\mathbf{H}_r \mathbf{W}_1 \mathbf{H}_r^H\| + \|\mathbf{H}_r \mathbf{W}_2 \mathbf{H}_r^H\|}{\sigma_r^2} \geq \gamma_r \\ & \quad \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\ & \quad \mathbf{W}_1 \geq 0, \mathbf{W}_2 \geq 0. \end{aligned} \quad (7)$$

However, the objective function of (7) is not concave in terms of the transmit covariance matrices  $\mathbf{W}_1$  and  $\mathbf{W}_2$ , and thus it cannot be straightforwardly solved via interior

point methods. To circumvent this deficiency, we can approximate the secrecy rate of the system using Taylor series approximation. To begin with, we can rewrite the secrecy rate function as follows:

$$\begin{aligned} \text{SR} = & \log \left| \sigma_c^2 \mathbf{I} + \mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| \\ & + \log \left| \sigma_e^2 \mathbf{I} + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right| - \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| \\ & - \log \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right|. \end{aligned} \quad (8)$$

The last two terms of (8) cause the nonconcavity of the secrecy rate function. By exploiting Taylor series expansion, we can approximate (8), as shown in (9). It is apparent that (9) is concave with regard to  $\mathbf{W}_1$  and  $\mathbf{W}_2$  since the first two terms are concave functions and the rest are either constant or affine. The proof of the Taylor series approximation of the secrecy rate function can be found in the Appendix

$$\begin{aligned} \text{SR} \approx & \log \left| \sigma_c^2 \mathbf{I} + \mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| + \log \\ & \times \left| \sigma_e^2 \mathbf{I} + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right| - \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right| \\ & - \text{Tr} \left[ \left( \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right)^{-1} \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right] \\ & + \text{Tr} \left[ \left( \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right)^{-1} \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right] \\ & - \log \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right| \\ & - \text{Tr} \left[ \left( \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right)^{-1} \right. \\ & \times \left. \left( \mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right) \right] \\ & + \text{Tr} \left[ \left( \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right)^{-1} \right. \\ & \times \left. \left( \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right) \right] \triangleq \tilde{\text{SR}}. \end{aligned} \quad (9)$$

By replacing the objective function of (7) with (9), we obtain the following approximated convex optimization problem:

$$\begin{aligned} \max_{\mathbf{W}_1, \mathbf{W}_2} \quad & \tilde{\text{SR}} \\ \text{s.t.} \quad & \text{SINR}_r \geq \gamma_r \\ & \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\ & \mathbf{W}_1 \geq 0, \mathbf{W}_2 \geq 0 \end{aligned} \quad (10)$$

where  $\tilde{\text{SR}}$  is defined in (9). The solution of (10) is dependent on the selection of the initial values  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$  and is

---

### Algorithm 1: System Optimizations.

---

- 1 Set initialization values for transmit covariance matrices:  $\tilde{\mathbf{W}}_1 = \mathbf{0}$ ,  $\tilde{\mathbf{W}}_2 = \mathbf{0}$  for case I or  $\tilde{\mathbf{W}}_1 = \mathbf{W}_{\text{opt1}}$ ,  $\tilde{\mathbf{W}}_2 = \mathbf{W}_{\text{opt2}}$  for case II.
  - 2 **while** the required accuracy is not reached **do**:
  - 3 Obtain the suboptimal  $\mathbf{W}_1^*$  and  $\mathbf{W}_2^*$ , by performing the optimizations (10), (14), and (16) for approximated secrecy rate maximization, approximated SINR maximization, and approximated transmit power minimization, respectively.
  - 4 Update  $\tilde{\mathbf{W}}_1 \leftarrow \mathbf{W}_1^*$  and  $\tilde{\mathbf{W}}_2 \leftarrow \mathbf{W}_2^*$
  - 5 **end while**
- 

derived by iteratively solving (10) based on updating  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$ . Thus, we consider two different initializations for the initial  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$ : I) all zero transmit matrices for both signals (i.e.,  $\tilde{\mathbf{W}}_1 = \mathbf{0}$ ,  $\tilde{\mathbf{W}}_2 = \mathbf{0}$ ); and II) transmit covariance matrices obtained from the solution of an SINR maximization problem subject to only a maximum power constraint and without the secrecy rate constraint (i.e.,  $\tilde{\mathbf{W}}_1 = \mathbf{W}_{\text{opt1}}$ ,  $\tilde{\mathbf{W}}_2 = \mathbf{W}_{\text{opt2}}$ )

$$\begin{aligned} \max_{\mathbf{W}_{\text{opt1}}, \mathbf{W}_{\text{opt2}}} \quad & \text{SINR}_{\text{opt}} = \frac{\|\mathbf{H}_r \mathbf{W}_{\text{opt1}} \mathbf{H}_r^H\| + \|\mathbf{H}_r \mathbf{W}_{\text{opt2}} \mathbf{H}_r^H\|}{\sigma_r^2} \\ \text{s.t.} \quad & \text{Tr}(\mathbf{W}_{\text{opt1}}) + \text{Tr}(\mathbf{W}_{\text{opt2}}) \leq P_{\max}. \end{aligned} \quad (11)$$

The transmit beamforming vectors  $\mathbf{w}_{\text{opt1}}$  and  $\mathbf{w}_{\text{opt2}}$  derived by  $\mathbf{W}_{\text{opt1}}$  and  $\mathbf{W}_{\text{opt2}}$ , respectively, produce a distortionless response at the direction of the target. Considering the aforementioned initializations I and II, we derive the solution of (10) using the iterative algorithm presented in Algorithm 1, performing optimization (10). It should be highlighted at this point that there are two cases for deriving  $\mathbf{w}_{\text{opt1}}$  and  $\mathbf{w}_{\text{opt2}}$ . If the rank of the respective transmit covariance matrix is one, which is the ideal case, the optimal beamforming vector is derived directly as the principal eigenvector of the transmit covariance matrix multiplied by the square root of the principal eigenvalue. On the other hand, if the rank of  $\mathbf{W}_{\text{opt1}}$  or  $\mathbf{W}_{\text{opt2}}$  is greater than one, we resort to randomization techniques to extract the transmit beamforming vectors as explained in [32].

### B. SINR Maximization

In the case when the secure communication with the legitimate receiver demands a certain secrecy rate threshold and there is a specific power budget imposed to the system, we formulate an SINR maximization problem as follows:

$$\begin{aligned} \max_{\mathbf{W}_1, \mathbf{W}_2} \quad & \text{SINR}_r \\ \text{s.t.} \quad & \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\ & \text{SR} \geq \kappa_r \\ & \mathbf{W}_1 \geq 0, \mathbf{W}_2 \geq 0 \end{aligned} \quad (12)$$

where  $\kappa_r$  represents a desired secrecy rate threshold. By using (2) and (5), the optimization problem (12) can be

written as in (13).

$$\begin{aligned}
& \max_{\mathbf{W}_1, \mathbf{W}_2} \frac{\|\mathbf{H}_r \mathbf{W}_1 \mathbf{H}_r^H\| + \|\mathbf{H}_r \mathbf{W}_2 \mathbf{H}_r^H\|}{\sigma_r^2} \\
& \text{s.t. } \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\
& \log \left| \mathbf{I} + (\mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H) \left( \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} + \sigma_c^2 \right)^{-1} \right| - \log \\
& \left| \mathbf{I} + (\mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H) \left( \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} + \sigma_e^2 \right)^{-1} \right| \geq \kappa_r \\
& \mathbf{W}_1 \geq \mathbf{0}, \mathbf{W}_2 \geq \mathbf{0}.
\end{aligned} \tag{13}$$

Similarly to the secrecy rate maximization problem (7), the secrecy rate function causes the nonconvexity of the optimization problem (13). Following the same approach as in the previous section, we substitute the secrecy rate function with the concave Taylor series approximated function (9). Thus, we resort to the following convex problem:

$$\begin{aligned}
& \max_{\mathbf{W}_1, \mathbf{W}_2} \text{SINR}_r \\
& \text{s.t. } \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \leq P_{\max} \\
& \tilde{\text{SR}} \geq \kappa_r \\
& \mathbf{W}_1 \geq \mathbf{0}, \mathbf{W}_2 \geq \mathbf{0}.
\end{aligned} \tag{14}$$

Following the methodology in Section III-A, we solve the convex problem (14) by applying Algorithm 1, using optimization (14). It is evident from (9), that if  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$  are equal to  $\mathbf{W}_1$  and  $\mathbf{W}_2$ , respectively, then the four trace terms cancel out and the approximate secrecy rate  $\tilde{\text{SR}}$  at  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$  will be exactly the same as the real secrecy rate SR from (5). Hence, since at convergence,  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$  are equal to  $\mathbf{W}_1$  and  $\mathbf{W}_2$  (within the required accuracy), the actual secrecy rate SR satisfies the secrecy rate threshold constraint in (13) ( $\text{SR} \geq \kappa_r$ ).

### C. Transmit Power Minimization

To attenuate the threat of the eavesdropper and provide secure information transfer, a certain secrecy rate threshold is applied to the joint radar-communication scheme. Since the other objective of the system is target detection, a pre-defined SINR constraint is also required. In the case when both constraints must be satisfied simultaneously, we formulate a transmit power minimization problem at the radar transmit array as follows:

$$\begin{aligned}
& \min_{\mathbf{W}_1, \mathbf{W}_2} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \\
& \text{s.t. } \text{SR} \geq \kappa_r \\
& \text{SINR}_r \geq \gamma_r \\
& \mathbf{W}_1 \geq \mathbf{0}, \mathbf{W}_2 \geq \mathbf{0}.
\end{aligned} \tag{15}$$

As mentioned in Sections III-A and III-B, the secrecy rate constraint introduces nonconvexity to the optimization problem (15). Similar to the previous optimizations, we replace the secrecy rate function with the Taylor series approximated secrecy rate from (9) and (15) and can be

written as follows:

$$\begin{aligned}
& \min_{\mathbf{W}_1, \mathbf{W}_2} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \\
& \text{s.t. } \tilde{\text{SR}} \geq \kappa_r \\
& \text{SINR}_r \geq \gamma_r \\
& \mathbf{W}_1 \geq \mathbf{0}, \mathbf{W}_2 \geq \mathbf{0}.
\end{aligned} \tag{16}$$

The minimization problem (16) is convex and can be solved using Algorithm 1 with optimization (16) and CVX software [33]. Similarly to Section III-B, the actual secrecy rate also satisfies the target secrecy rate constraint of (16) when the algorithm converges.

## IV. SIMULATION RESULTS

For the simulations, we consider a system similar to Fig. 1 that consists of a MIMO radar, a multiple antenna communication receiver, and an eavesdropping target. The results illustrate the performance of the transmit covariance matrices for all three different optimizations, namely the secrecy rate maximization, the target return SINR maximization, and the transmit power minimization. It is assumed that the MIMO radar consists of ten transmit/receive antennas ( $M = 10$ ), the legitimate receiver, and the target incorporate five receive antennas ( $N_c = N_e = 5$ ). We also presume that the tracking MIMO radar has information regarding the approximate location of the legitimate receiver and the target. More specifically, the referential direction of the target as seen from the radar is set to  $\theta_t = 72^\circ$ . Moreover, the eavesdropper is aware of the location of the radar, which is placed at azimuth angle  $\theta_r = -85^\circ$ , as observed from the target. The legitimate receiver channel gain coefficients ( $\mathbf{H}_c$ ) are perfectly known and for the simulations were generated using zero-mean circularly symmetric independent and identically distributed complex Gaussian random variables. The RCS coefficient and the propagation loss variable are fixed equal to 0.1 and 1, respectively ( $\beta = 0.1, \alpha = 1$ ). The variance of the background WGN at the radar receive array, the legitimate receiver and the eavesdropping target are set equal to 1 ( $\sigma_r^2 = \sigma_c^2 = \sigma_e^2 = 1$ ), and the spreading gain of the modulation waveform is fixed to 8 b ( $L_m = 8$ ).

### A. Secrecy Rate Maximization

The first algorithm designs the transmit covariance matrices for both the information and the distortion signals, by utilizing Taylor series approximation to convert the secrecy rate maximization problem to an approximated convex optimization problem. Fig. 2 illustrates the convergence of both the actual and the approximated secrecy rate to the solution by considering the maximum transmit power  $P_{\max} = 10$  W, the SINR threshold  $\gamma_r = 5$ , and two different cases for Taylor approximation initialization values regarding the transmit covariance matrices ( $\tilde{\mathbf{W}}_1 = \mathbf{0}, \tilde{\mathbf{W}}_2 = \mathbf{0}$  for case I and  $\tilde{\mathbf{W}}_1 = \mathbf{W}_{\text{opt1}}, \tilde{\mathbf{W}}_2 = \mathbf{W}_{\text{opt2}}$  for case II). It is evident that for both initialization points, the algorithm converges to the same solution within six iterations. Furthermore, it is important to notice that the approximated secrecy rate is almost identical to the actual secrecy rate at convergence,

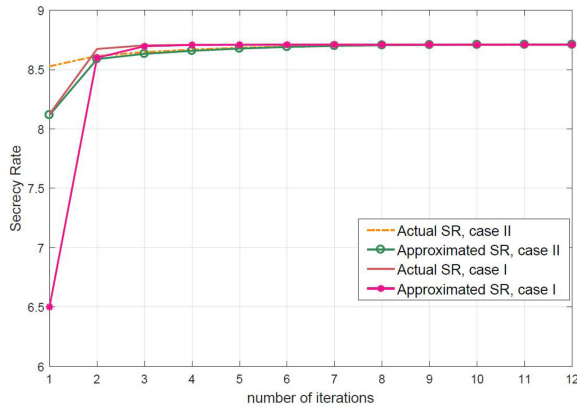


Fig. 2. Convergence of secrecy rate for the secrecy rate maximization problem (10).

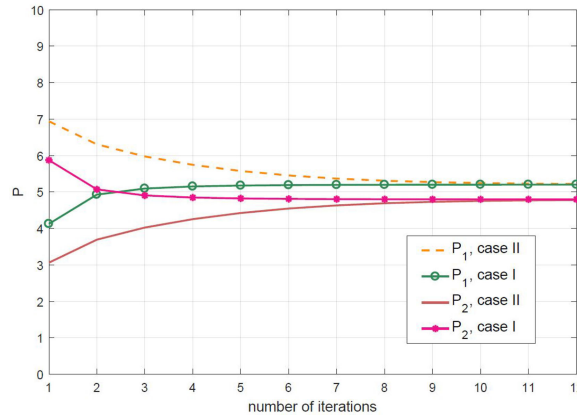


Fig. 3. Convergence of transmit power for the secrecy rate maximization problem (10).

proving that the Taylor series approximation is efficient and reliable.

The convergence of the transmit power of the two signals  $\mathbf{x}_1$  and  $\mathbf{x}_2$  is depicted in Fig. 3. It is obvious that independent of the initial power allocation,  $P_1$  and  $P_2$  converge to the same solution after eight iterations. An interesting assumption from Fig. 3 is that the MIMO radar opts to allocate the majority of the power budget to the information signal, using less power to induce deliberate interference to the eavesdropper. In Fig. 4, we demonstrate the dependence between the secrecy rate and the transmit power when we keep the SINR threshold constant at  $\gamma_r = 5$ . Specifically, it is shown that the secrecy rate of the system increases as the power budget increases, which is expected, as more power is available for the communication signal toward the legitimate receiver, and moreover, for the distortion signal toward the eavesdropper. In order to demonstrate the efficiency of the proposed algorithm, we compare the achieved secrecy rate from (10) with that of the secrecy rate maximization method in [28]. In order for the algorithm in [28] to be applicable to our system model, we modify the suggested optimization by adding an SINR constraint and removing the interference temperature constraints. The achieved secrecy rate against the SINR target for a specific power budget of

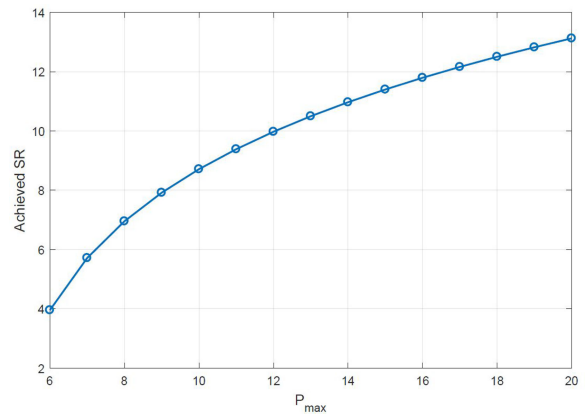


Fig. 4. Achieved secrecy rate for different maximum power allowance for the secrecy rate maximization problem (10).

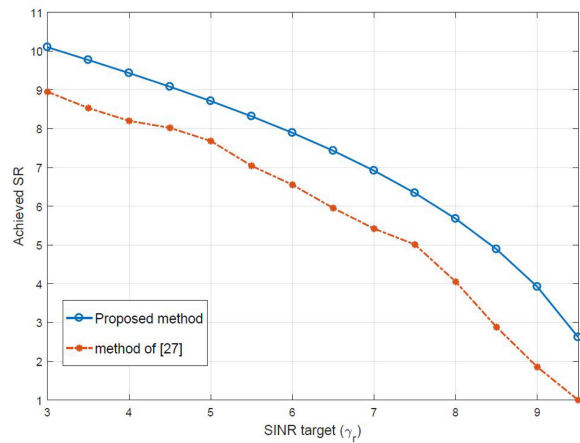


Fig. 5. Achieved secrecy rate for different SINR thresholds for the secrecy rate maximization problem (10) and the method of [28].

$P_{max} = 10$  W is presented in Fig. 5 for both schemes. It can be observed that the secrecy rate decreases as the SINR target increases for both methods. This is because as the SINR demand rises, the MIMO radar spends more energy to focus the beamformers of both signals at the direction of the target, and thus less power is used for the information signal emission toward the direction of the legitimate receiver. The proposed method offers higher secrecy rates for different SINR targets as compared to the work in [28].

In a realistic scenario, the MIMO radar may have only limited information regarding the number of the receiving antennas of the eavesdropper. Hence, it is essential to investigate the sensitivity of our assumption regarding the number of antennas of the eavesdropper. Hence, we solved (10) for different numbers of eavesdropper's receiving antennas ( $N_e$ ) and present the results in Table I. It is obvious that for different numbers of  $N_e$ , both the achieved secrecy rate and the eavesdropper's achievable capacity remain almost identical. Thus, it is safe to presume that setting the number of antennas at the receiving array of the eavesdropper at  $N_e = 5$  does not affect the achieved secrecy rate from (10).

TABLE I  
Achieved Secrecy Rate and Achievable Rate  
of the Eavesdropper for Different  
Values of  $N_e$ .

$N_e$	Achieved SR	Achieved $R_e$
5	8.7100	0.3895
10	8.7042	0.3724
15	8.7027	0.3695
20	8.7018	0.3766
25	8.7013	0.3749
30	8.7009	0.3737

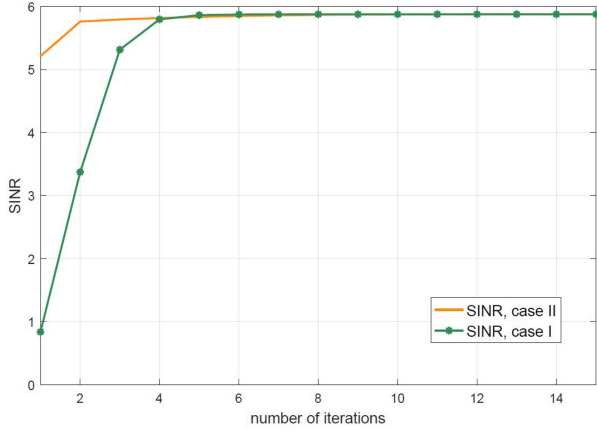


Fig. 6. Convergence of SINR for the SINR maximization problem (14).

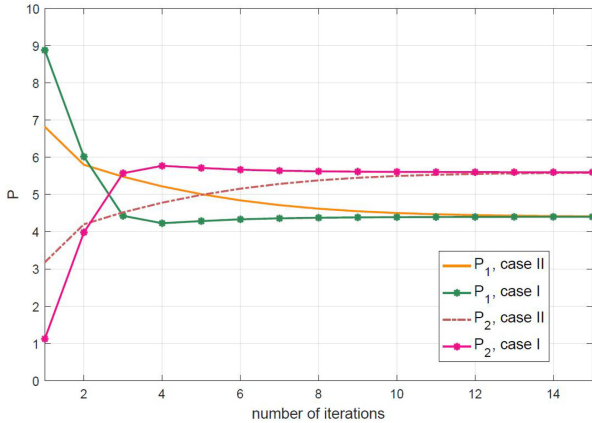


Fig. 7. Convergence of transmit power for the SINR maximization problem (14).

## B. SINR Maximization

In this section, we employ Algorithm 1 and optimization (14) to design  $\mathbf{W}_1$  and  $\mathbf{W}_2$  that provide the maximum possible SINR under a target secrecy rate and a maximum power constraints. In particular, we set  $\kappa_r = 8$  and  $P_{\max} = 10$  W. Fig. 6 shows the convergence regarding the SINR maximization problem (14) using two different initial sets for  $\tilde{\mathbf{W}}_1$  and  $\tilde{\mathbf{W}}_2$ . The algorithm converges within five iterations. The convergence of the transmit power for the two signals is depicted in Fig. 7. As opposed to the secrecy rate

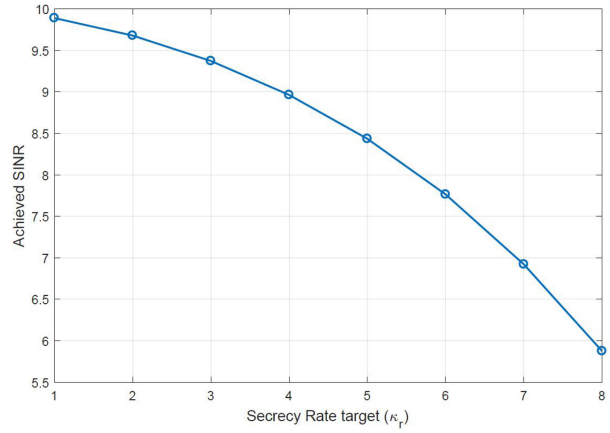


Fig. 8. Achieved SINR for different secrecy rate targets for the SINR maximization problem (14).

TABLE II  
Average SINR for  
 $\epsilon_{\theta_t} \sim \mathcal{U}(-m_{\text{rob}}, m_{\text{rob}})$ .

$m_{\text{rob}}$	Average SINR
$0.0^\circ$	5.8763
$0.5^\circ$	5.7996
$1.0^\circ$	5.7670
$1.5^\circ$	5.6329
$2.0^\circ$	5.5040
$2.5^\circ$	4.9852

maximization problem results, the distortion signal is emitted with increased power as compared to the information signal. In Fig. 8, we demonstrate the relation among the desired secrecy rate target and the achieved SINR, obtained from the convex optimization problem (14) when the available power is set to  $P_{\max} = 10$  W. It is obvious that when the secrecy rate target increases, the achieved SINR decreases since a greater part of the available power is allocated to provide a safer communication with the legitimate receiver, restraining the target detection efficiency.

The next example evaluates the sensitivity of the proposed algorithm against potential mismatch between the estimated target location, as seen from the radar, and the actual location of the target. In order to examine the performance loss, we perform 100 Monte Carlo simulations using Algorithm 1 and optimization (14), when the estimate of the angle of the target, as seen from the radar, is set to  $\hat{\theta}_t = \theta_t \pm \epsilon_{\theta_t}$ , where the mismatch  $\epsilon_{\theta_t}$  between the true angle and its estimate is uniformly distributed in the interval  $[-m_{\text{rob}}, m_{\text{rob}}]$ . For each set of Monte Carlo simulations, we set  $m_{\text{rob}} = 0.5^\circ, 1^\circ, 1.5^\circ, 2^\circ$ , respectively, and obtain the average SINR. It is observed from Table II that the bigger the range of the mismatch, the greater the SINR performance drop of the radar system. Combating the angle mismatch case and implementing a robust DFRC system against channel uncertainty can be a topic for future research.



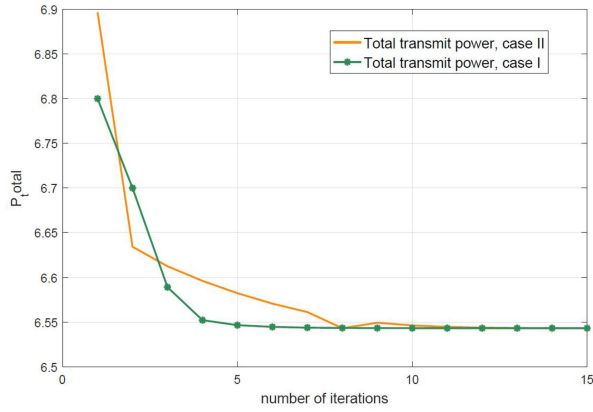


Fig. 9. Convergence of the total transmit power for the power minimization problem (16).

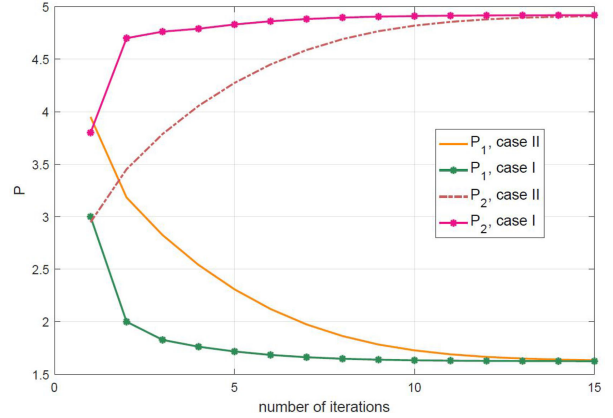


Fig. 10. Convergence of transmit power for the power minimization problem (16).

### C. Transmit Power Minimization

$$\begin{aligned}
& \log \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right| \simeq \log \\
& \times \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right| \\
& + \text{vec} \left[ \mathbf{H}_e \left( \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right)^{-1} \mathbf{H}_e^H \right] \\
& \times \text{vec} \left[ (\mathbf{W}_1 + \mathbf{W}_2) - (\tilde{\mathbf{W}}_1 + \tilde{\mathbf{W}}_2) \right] \\
& = \log \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right| \\
& + \text{Tr} \left[ \left( \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right)^{-1} \right. \\
& \times \left. \left( \mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right) \right] \\
& - \text{Tr} \left[ \left( \sigma_e^2 \mathbf{I} + \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right)^{-1} \right. \\
& \times \left. \left( \mathbf{H}_e \tilde{\mathbf{W}}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \tilde{\mathbf{W}}_2 \mathbf{H}_e^H}{L_m} \right) \right]. \quad (17)
\end{aligned}$$

By imposing target SINR and secrecy rate constraints, we can design the transmit covariance matrices that minimize the transmitted energy using Algorithm 1 and optimization (16). We set  $\gamma_r = 5$  and  $\kappa_r = 5$ . Fig. 9 depicts the convergence of the total transmitted power from the MIMO radar when performing Algorithm 3. It is obvious that the algorithm converges within ten iterations. The allocation of the transmission power regarding the communication signal  $P_1$  and the distortion signal  $P_2$  for both cases I and II is shown in Fig. 10. Finally the interdependence among the total transmitted power and the secrecy rate threshold when the SINR target is set to  $\gamma_r = 5$  is depicted in Fig. 11. As expected, as the system requirements for safe communication

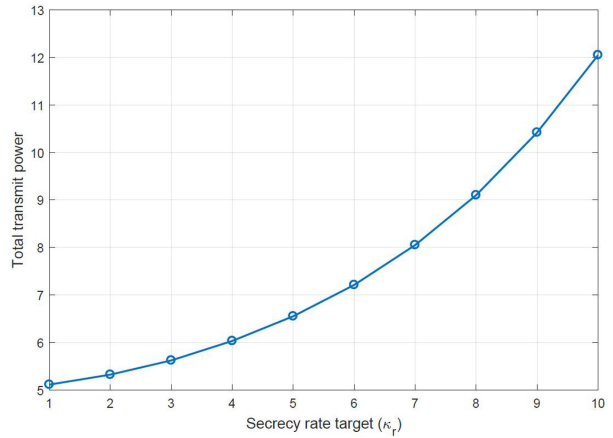


Fig. 11. Total transmit power used to achieve different secrecy rate targets for the secrecy rate maximization problem (10).

become more demanding (secrecy rate target increases), the MIMO radar needs more power to satisfy the constraints.

### V. CONCLUSION

This paper has studied optimization techniques for a DFRC system, consisting of a MIMO radar, a legitimate receiver, and an eavesdropping target. Initially, we defined the SINR for the MIMO radar and the secrecy rate regarding the legitimate receiver against the eavesdropper. Apart from detecting the target, the MIMO radar aims to synchronously provide secure information transfer to the legitimate receiver. To succeed that, we proposed three different optimizations, namely secrecy rate maximization, SINR maximization, and transmit power minimization. To overcome the nonconvexity of the aforementioned optimizations, we utilize Taylor series approximation for the secrecy rate function. The simulation results confirm that the system can provide both efficient target detection, guaranteeing a predefined SINR threshold and also secure communication, by achieving a target secrecy rate, under a given resource budget.

APPENDIX  
TAYLOR SERIES APPROXIMATION OF THE SECRECY  
RATE

The secrecy rate of the system defined in (5) is a difference of two concave functions, which does not guarantee concavity of (5). By rearranging (5), we have the following equation as shown in (8):

$$\begin{aligned} \text{SR} = & \log \left| \sigma_c^2 \mathbf{I} + \mathbf{H}_c \mathbf{W}_1 \mathbf{H}_c^H + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| \\ & + \log \left| \sigma_e^2 \mathbf{I} + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right| - \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| \\ & - \log \left| \sigma_e^2 \mathbf{I} + \mathbf{H}_e \mathbf{W}_1 \mathbf{H}_e^H + \frac{\mathbf{H}_e \mathbf{W}_2 \mathbf{H}_e^H}{L_m} \right| \end{aligned}$$

where the last two negative log terms generate the non-concavity of the secrecy rate function. Hence, to convert SR into a concave function, we employ Taylor series approximation for the last two terms in (8). A first-order Taylor series approximation of a function  $f(\mathbf{X}) : \mathbb{R}^{M \times N} \rightarrow \mathbb{R}$  can be derived at an initial approximation  $\tilde{\mathbf{X}}$  as [34] follows:

$$f(\mathbf{X}) = f(\tilde{\mathbf{X}}) + \text{vec}(f'(\tilde{\mathbf{X}})) \text{vec}(\mathbf{X} - \tilde{\mathbf{X}}). \quad (18)$$

By employing (18) and  $\partial(\log |\mathbf{X}|) = \text{Tr}(\mathbf{X}^{-1} \partial \mathbf{X})$ , the last two terms of (8) can be reformulated to an affine first-order Taylor series approximation as follows:

$$\begin{aligned} \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right| & \simeq \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right| \\ & + \text{vec} \left[ \mathbf{H}_c \left( \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right)^{-1} \mathbf{H}_c^H \right] \text{vec}(\mathbf{W}_2 - \tilde{\mathbf{W}}_2) \\ = & \log \left| \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right| \\ & + \text{Tr} \left[ \left( \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right)^{-1} \frac{\mathbf{H}_c \mathbf{W}_2 \mathbf{H}_c^H}{L_m} \right] \\ & - \text{Tr} \left[ \left( \sigma_c^2 \mathbf{I} + \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right)^{-1} \frac{\mathbf{H}_c \tilde{\mathbf{W}}_2 \mathbf{H}_c^H}{L_m} \right] \end{aligned} \quad (19)$$

and (17), respectively.

REFERENCES

- [1] J. Li and P. Stoica  
*MIMO Radar Signal Processing*. Hobokon, NJ, USA: Wiley, 2009.
- [2] J. Li and P. Stoica  
MIMO radar with colocated antennas  
*IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 106–114, Sep. 2007.
- [3] A. M. Haimovich, R. S. Blum, and L. J. Cimini  
MIMO radar with widely separated antennas  
*IEEE Signal Process. Mag.*, vol. 25, no. 1, pp. 116–129, Jan. 2008.
- [4] D. R. Fuhrmann, J. P. Browning, and M. Rangaswamy  
Signaling strategies for the hybrid MIMO phased-array radar  
*IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 1, pp. 66–78, Feb. 2010.
- [5] A. J. Duly, D. J. Love, and J. V. Krogmeier  
Time-division beamforming for MIMO radar waveform design  
*IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1210–1223, Apr. 2013.
- [6] A. Tajer *et al.*  
Optimal joint target detection and parameter estimation by MIMO radar  
*IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 1, pp. 127–145, Feb. 2010.
- [7] A. Deligiannis, S. Lambbotharan, and J. A. Chambers  
Beamforming for fully-overlapped two-dimensional phased-MIMO radar  
In *Proc. IEEE Radar Conf.*, Arlington, VA, USA, 2015, pp. 0599–0604.
- [8] A. Deligiannis, A. Panoui, S. Lambbotharan, and J. A. Chambers  
Game-theoretic power allocation and the Nash equilibrium analysis for a multistatic MIMO radar network  
*IEEE Trans. Signal Process.*, vol. 65, no. 24, pp. 6397–6408, Dec. 2017.
- [9] A. Deligiannis, S. Lambbotharan, and J. A. Chambers  
Game theoretic analysis for MIMO radars with multiple targets  
*IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 6, pp. 2760–2774, Dec. 2016.
- [10] H. Griffiths, S. Blunt, L. Cohen, and L. Savy  
Challenge problems in spectrum engineering and waveform diversity  
In *Proc. IEEE Radar Conf.*, Ottawa, ON, Canada, 2013.
- [11] D. W. Bliss  
Cooperative radar and communications signaling: The estimation and information theory odd couple  
In *Proc. IEEE Radar Conf.*, Cincinnati, OH, USA, 2014, pp. 50–55.
- [12] A. Hassanien, M. G. Amin, Y. D. Zhang, and F. Ahmad  
Signaling strategies for dual-function radar-communications: An overview  
*IEEE Aerosp. Electron. Syst. Mag.*, vol. 31, no. 10, pp. 36–45, Oct. 2016.
- [13] S. D. Blunt, M. R. Cook, and J. Stiles  
Embedding information into radar emissions via waveform implementation  
In *Proc. 2010 Int. Waveform Diversity Des. Conf.*, 2010, pp. 195–199.
- [14] J. Euziere, R. Guinvarc’h, and M. Lesturgie  
Dual function radar communication time-modulated array  
In *Proc. 2014 Int. Radar Conf.*, Lille, France, 2014.
- [15] A. Hassanien, M. G. Amin, Y. D. Zhang, and F. Ahmad  
Dual-function radar-communications: Information embedding using sidelobe control and waveform diversity  
*IEEE Trans. Signal Process.*, vol. 64, no. 8, pp. 2168–2181, Apr. 2016.
- [16] A. Hassanien, M. G. Amin, Y. D. Zhang, and F. Ahmad  
Dual-function radar-communications using phase-rotational invariance  
In *Proc. 23rd Eur. Signal Process. Conf.*, 2015, pp. 1346–1350.
- [17] S. D. Blunt, P. Yatham, and J. Stiles  
Intrapulse radar-embedded communications  
*IEEE Trans. Aerosp. Electron. Syst.*, vol. 46, no. 3, pp. 1185–1200, Jul. 2010.
- [18] S. D. Blunt, J. G. Metcalf, C. R. Biggs, and E. Perrins  
Performance characteristics and metrics for intra-pulse radar-embedded communications  
*IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2057–2066, Dec. 2011.

- [19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor  
Improving wireless physical layer security via cooperating relays  
*IEEE Trans. Signal Process.*, vol. 58, no. 3 part 2, pp. 1875–1888, Mar. 2010.
- [20] X. Tang, R. Liu, P. Spasojević, and H. V. Poor  
Interference assisted secret communication  
*IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
- [21] A. Khisti and G. W. Wornell  
Secure transmission with multiple antennas—Part II: The MI-MOME wiretap channel  
*IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [22] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung  
Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper  
*IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.
- [23] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff  
Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer  
*IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.
- [24] G. Zheng, L. C. Choo, and K. K. Wong  
Optimal cooperative jamming to enhance physical layer security using relays  
*IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
- [25] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley  
On the application of cooperative transmission to secrecy communications  
*IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.
- [26] I. Krikidis, J. S. Thompson, and S. McLaughlin  
Relay selection for secure cooperative networks with jamming  
*IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
- [27] S. Goel and R. Negi  
Guaranteeing secrecy using artificial noise  
*IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [28] Q. Li and W.-K. Ma  
Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization  
*IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
- [29] S. Verdú  
*Multuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
- [30] I. E. Telatar  
Capacity of multi-antenna Gaussian channels  
*Eur. Trans. Telecommun.*, vol. 10, pp. 585–595, 1999.
- [31] Y. Liang, H. Poor, and S. Shamai  
Secure communication over fading channels  
*IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [32] A. Deligiannis, J. A. Chambers, and S. Lambotharan  
Transmit beamforming design for two-dimensional phased-MIMO radar with fully-overlapped subarrays  
In *Proc. Sensor Signal Process. Def.*, Edinburgh, U.K., 2014.
- [33] S. Boyd and L. Vandenberghe  
*Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [34] K. Cumanan, R. Zhang, and S. Lambotharan  
A new design paradigm for MIMO cognitive radio with primary user rate constraint  
*IEEE Commun. Lett.*, vol. 16, no. 5, pp. 706–709, May 2012.



**Anastasios Deligiannis** (S'13–M'16) received the Diploma (Bachelor's and Master's degrees equivalent) from the School of Electrical and Computer Engineering, University of Patras, Patras, Greece, in 2012, and the Ph.D. degree in radar signal processing from Loughborough University, Loughborough, U.K., in 2016. Since 2013, he has been working toward the Ph.D. degree at the Signal Processing and Networks Research Group, The Wolfson School of Mechanical, Manufacturing and Electrical Engineering, Loughborough University.

Since June 2016, he has been a Research Associate in signal processing with Loughborough University. His research interests include signal processing algorithms, sparse array design, convex optimization, and game theoretic methods, within the radar network framework and wireless communications.



**Abdullahi Daniyan** (S'13) received the B.Eng. (Hons.) degree in electrical and electronic engineering from the University of Bradford, Bradford, U.K., in 2010, and the M.Sc. degree in signal processing for communication systems from Loughborough University, Loughborough, U.K., in 2014. He is currently working toward the Ph.D degree at the Signal Processing and Networks Research Group, The Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, U.K.

His research interests include multiple target tracking, sensor data fusion, machine linear and nonlinear filtering and estimation, optimization techniques, radar systems, and renewable energy.



**Sangarapillai Lambotharan** (SM'06) received the Ph.D. degree in signal processing from the Imperial College London, London, U.K., in 1997

He was a Visiting Scientist with the Engineering and Theory Center, Cornell University, Ithaca, NY, USA, in 1996. He was with the Imperial College London until 1999 where he was a Postdoctoral Research Associate. From 1999 to 2002, he was with the Motorola Applied Research Group, U.K., as a Research Engineer, working on various projects, including physical-link layer modeling and performance characterization of GPRS, EGPRS, and UTRAN. From 2002 to 2007, he was with the King's College London, London, U.K., and Cardiff University, Cardiff, U.K., as a Lecturer and Senior Lecturer, respectively. He is currently a Professor in digital communications and the Head of Signal Processing and Networks Research Group, Loughborough University, Loughborough, U.K. His research interests include wireless communications, cognitive radio networks, smart grids, radars, convex optimizations, and game theory. He has authored or coauthored more than 180 conference and journal articles in these areas.

Dr. Lambotharan is currently an Associate Editor for the *EURASIP Journal on Wireless Communications and Networking*.



**Jonathon A. Chambers** (S'83–M'90–SM'98–F'11) received the Ph.D. and D.Sc. degrees in signal processing from the Imperial College of Science, Technology and Medicine (Imperial College London), London, U.K., in 1990 and 2014, respectively.

From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Center, Cambridge, U.K. In 1994, he returned to the Imperial College London as a Lecturer in signal processing and was promoted to Reader (Associate Professor) in 1998. From 2001 to 2004, he was the Director of the Center for Digital Signal Processing and a Professor in signal processing with the Division of Engineering, King's College London and is currently a Visiting Professor. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Cardiff, U.K. Between 2007 and 2014, he led the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University, and is currently a Visiting Professor. In 2015, he joined the School of Electrical and Electronic Engineering, and from August 1, 2017, he was a Professor in signal and information processing and the Head of the Intelligent Sensing and Communications Group, School of Engineering, Newcastle University, where he is currently a Visiting Professor. Since December 1, 2017, he has been the Head of the Engineering Department, The University of Leicester, Leicester, U.K., and is also an International Honorary Dean and a Guest Professor with the Department of Automation, Harbin Engineering University, Harbin, China. He has advised 80 Ph.D. graduate researchers and authored or coauthored more than 500 conference proceedings and journal articles, many of which are in the IEEE journals. His research interests include adaptive signal processing and machine learning and their application in communications, defense, and navigation systems.

Dr. Chambers is a Fellow of the Royal Academy of Engineering, London, U.K., the Institution of Engineering and Technology, and the Institute of Mathematics and its Applications. He was the Technical Program Co-Chair for the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Prague, Czech Republic, and is serving on the organizing committees of ICASSP 2019, Brighton, U.K., and ICASSP 2022, Singapore. He was on the IEEE Signal Processing Theory and Methods Technical Committee for six years, the IEEE Signal Processing Society Awards Board for three years, and the Jack Kilby Medal Committee for three years.