

OPTM3SEC: OPTIMIZING MULTICAST IRS-AIDED MULTIANTEENNA DFRC SECRECY CHANNEL WITH MULTIPLE EAVESDROPPERS

Kumar Vijay Mishra[†], Arpan Chattopadhyay[‡], Siddharth Sankar Acharjee[‡] and Athina P. Petropulu^{†‡}

[†]United States CCDC Army Research Laboratory, Adelphi, MD 20783 USA

[‡]Indian Institute of Technology, New Delhi 110016 India

[‡]Rutgers - The State University of New Jersey, Piscataway, NJ 08854 USA

ABSTRACT

With the use of common signaling methods for dual-function radar-communications (DFRC) systems, the susceptibility of eavesdropping on messages aimed at legitimate users has worsened. For DFRC systems, the radar target may act as an eavesdropper (ED) that receives a high-energy signal thereby leading to additional challenges. Unlike prior works, we consider a multicast multi-antenna DFRC system with multiple EDs. We then propose a physical layer design approach to maximize the secrecy rate by installing intelligent reflecting surfaces in the radar channels. Our *optimization of multiple ED multicast multi-antenna DFRC secrecy rate* (OptM3Sec) approach solves this highly nonconvex problem with respect to the precoding matrices. Our numerical experiments demonstrate the feasibility of our algorithm in maximizing the secrecy rate in this DFRC setup.

Index Terms— Dual-function radar-communications, intelligent reflecting surfaces, multicasting, precoding matrix, secrecy rate maximization.

1. INTRODUCTION

With the advent of mobile communications, portions of spectrum earlier solely assigned to radar are being re-allocated for dual-use with communications [1]. This has accelerated efforts to allow uncontested joint access to the bandwidth through coexisting radar and communications systems, apart from other emitters within the same RF spectrum [2]. In this context, dual-function radar-communications (DFRC) systems have emerged as a viable and relatively less contentious approach because it hosts both transmissions on the same hardware unit using same frequency band [3]. Since DFRC employs an identical waveform for both services, the delivery of information to both communications users and radar targets has increased chances of unauthorized users or *eavesdroppers* (EDs) intercepting it [4]. In this paper, we focus on secure DFRC transmission.

In general, cryptographic techniques are effective for secure transmission [5]. However, with the computational power available today, it is possible to break cryptographic codes [6]. A complementary approach lies in ensuring physical layer security so that EDs are not able to decode the message successfully, even if they knew the secret code. The physical layer secrecy seeks to maximize, by exploiting channel conditions, the rate of reliable information delivery to the intended receiver, with the ED being kept as ignorant of that information as

K. V. M. acknowledges support from the National Academies of Sciences, Engineering, and Medicine via Army Research Laboratory Harry Diamond Distinguished Fellowship. A. C. acknowledges support via professional development fund (PDF), professional development allowance (PDA) and faculty seed grant at IIT Delhi, grant MI02266G of IRD unit of IIT Delhi under the MFIRP scheme, grant RP04215G provided by I-Hub Foundation for Cobotics (IHFC) India, and the seed grant provided by IHFC.

possible. This line of research was pioneered by Wyner [7], who introduced the wiretap channel and the notion of *secrecy capacity*, i.e., the rate at which the legitimate receiver correctly decodes the source message, while an ED obtains no useful information about the source signal. For the classical source-destination-ED Gaussian wiretap channel, the secrecy capacity is zero when the quality of legitimate channel is worse than eavesdropping channel [8]. One way to achieve non-zero secrecy rates is to adopt *cooperative jamming* by introducing one [9–12] or more [13–17] relays (helpers), which transmit artificial noise in a beamforming fashion thereby acting as jammers for the purpose of degrading the channel to the ED. Alternatively, the source may embed artificial noise in its transmission and beamformed it not to interfere with the legitimate receiver [18, 19].

In a DFRC system, the radar target is illuminated by a high-energy signal, which also contains information intended for the communication users. This increases the susceptibility of eavesdropping on the communications messages and may be aggravated when DFRC employs multiple-input multiple-output (MIMO) antennas [20] because of its omnidirectional radiation pattern. Recent studies show that physical layer security could be a promising solution for a secure MIMO DFRC [21] by trading-off the secrecy rate (the achievable difference between the communication rates to the legitimate users and the target) for the data rate. The MIMO communications-radar system presented in [22] simultaneously transmitted jamming and communications messages to confuse an ED (co-located with the targets) while trying to enhance target detection. In [20], the MIMO DFRC employed artificial noise and minimized the signal-to-interference-and-noise ratio (SINR) at the eavesdropping target with an SINR constraint at the legitimate users. These systems were extended in [23] by incorporating an intelligent reflecting surface (IRS) in the channel. An IRS is a two-dimensional surface consisting of a large number of passive meta-material elements to reflect the incoming signal through a pre-computed phase shift [24]. The IRSs have emerged as feasible low cost, light-weight, and compact alternatives to large arrays for both communications [25, 26] and radar [27].

Prior works on IRS-aided MIMO DFRC secrecy assume a single ED/target with either unicast or broadcast transmissions. Further, the indirect path of target backscatter via IRS is often ignored in these studies [22, 23]. In this paper, we generalize the DFRC interception problem to *optimizing multiple ED multicast multi-antenna secrecy rate* (OptM3Sec). Our physical layer design approach maximizes the secrecy rate while meeting power constraints and maintaining a certain SINR for each radar target. In particular, we control the SINR at the radar target (ED SINR) by embedding in the transmit waveform a noise-like signal. The signal and the noise are precoded separately at the radar. We consider both direct and indirect (via IRS) paths for line-of-sight (LoS) and non-line-of-sight (NLoS) targets. We solve the resulting optimization problem with respect to the precoding

matrices following the strategy adopted from [23].

2. SYSTEM MODEL

Consider a DFRC system comprising a MIMO radar, L legitimate multi-antenna communications users, an IRS, and K targets which are also EDs with multiple antennas (Fig. 1). Assume that the MIMO radar has N_T transmit and receive antennas, each legitimate user is equipped with N_R receive antennas, and each ED receive antenna array has N_E elements. The IRS is equipped with a $\sqrt{N} \times \sqrt{N}$ square array of reflecting units. A number of channels in this DFRC system are of our interest. Denote the channel gain matrix for the channel from radar to k -th target and back to the radar as

$$\mathbf{H}_{rtr,k} = \beta_k \mathbf{a}_R(\theta_k) \mathbf{a}_T(\theta_k)^T \in \mathbb{C}^{N_T \times N_T}, \quad (1)$$

where β_k is the complex reflectivity that depends on the atmospheric attenuation and target's radar cross-section (RCS), θ_k is the azimuthal location of the target with respect to the radar, $\mathbf{a}_T(\theta_k) = [1, e^{j\frac{2\pi}{\lambda}d_r \sin(\theta_k)}, \dots, e^{j\frac{2\pi}{\lambda}(N_T-1)d_r \sin(\theta_k)}]^T$ ($\mathbf{a}_R(\theta_k) = [1, e^{j\frac{2\pi}{\lambda}d_r \sin(\theta_k)}, \dots, e^{j\frac{2\pi}{\lambda}(N_T-1)d_r \sin(\theta_k)}]^T$) is the transmit (receive) steering vector of k -th target, where d_r is the spacing between the antenna elements at the radar and λ is the transmit signal wavelength. Similarly, denote the other channel matrices as $\mathbf{H}_{ri} \in \mathbb{C}^{N \times N}$ for radar-IRS; $\mathbf{H}_{ru,l} \in \mathbb{C}^{N_R \times N_T}$ for radar-user; $\mathbf{H}_{re,k} \in \mathbb{C}^{N_E \times N_T}$ for radar-ED; $\mathbf{H}_{iu,l} \in \mathbb{C}^{N_R \times N}$ for IRS-user; $\mathbf{H}_{it,k} \in \mathbb{C}^{1 \times N}$ for IRS-target; $\mathbf{H}_{ie,k} \in \mathbb{C}^{N_E \times N}$ for IRS-ED; $\mathbf{H}_{ir} \in \mathbb{C}^{N_T \times N}$ for IRS-radar; and $\mathbf{H}_{ti,k} \in \mathbb{C}^{N \times 1}$ for target-IRS paths.

The radar transmits information bearing signal $\mathbf{m}(t) \in \mathbb{C}^{K \times 1}$ and artificial noise (AN) $\mathbf{s}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}) \in \mathbb{C}^{K \times 1}$ for jointly detecting the target and communicating with users. The AN is added to prevent targets eavesdropping on the information transmitted to the users. The transmit signal $\mathbf{x}(t) \in \mathbb{C}^{N_T \times 1}$ from the radar is

$$\mathbf{x}(t) = \mathbf{W}\mathbf{m}(t) + \mathbf{B}\mathbf{s}(t), \quad (2)$$

where $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_K] \in \mathbb{C}^{N_T \times K}$ is the precoding matrix for information and $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_K] \in \mathbb{C}^{N_T \times K}$ is the precoding matrix for the artificial noise.

Assume $\tau_{(\cdot),k}$ and $\omega_{(\cdot),k}$ are the range-time delay and Doppler shift corresponding to the target k for a given channel (denoted by the first subscript), the continuous-time received signal at the radar is:

$$\begin{aligned} \mathbf{r}(t) = & \sum_{k=1}^K \mathbf{H}_{rtr,k} \mathbf{x}(t - \tau_{rtr,k}) e^{j\omega_{rtr,k} t} \\ & + \sum_{k=1}^K \mathbf{H}_{tr,k} \mathbf{H}_{it,k} \Phi \mathbf{H}_{ri} \mathbf{x}(t - \tau_{ritr,k}) e^{j\omega_{ritr,k} t} \\ & + \sum_{k=1}^K \mathbf{H}_{ir} \Phi \mathbf{H}_{ti,k} \mathbf{H}_{rt,k} \mathbf{x}(t - \tau_{rtir,k}) e^{j\omega_{rtir,k} t} \\ & + \sum_{k=1}^K \mathbf{H}_{ir} \Phi \mathbf{H}_{ti,k} \mathbf{H}_{it,k} \Phi \mathbf{H}_{ri} \mathbf{x}(t - \tau_{ritir,k}) e^{j\omega_{ritir,k} t} + \mathbf{n}_T(t), \end{aligned} \quad (3)$$

where $\mathbf{n}_T \sim \mathcal{CN}(\mathbf{0}, \sigma_T^2 \mathbf{I})$ is the additive white Gaussian noise. The received signal from the radar-IRS-target-IRS-radar path is ignored here because it is much weaker and delayed than the other returns.

The received signal at the k -th ED is:

$$\begin{aligned} \mathbf{z}_k(t) = & \mathbf{H}_{re}(\mathbf{W}\mathbf{m}(t - \tau_{re,k}) + \mathbf{B}\mathbf{s}(t - \tau_{re,k})) e^{j\omega_{re,k} t} \\ & + \mathbf{H}_{ie,k} \Phi \mathbf{H}_{ri}(\mathbf{W}\mathbf{m}(t - \tau_{rie,k}) + \mathbf{B}\mathbf{s}(t - \tau_{rie,k})) e^{j\omega_{rie,k} t} \\ & + \mathbf{n}_{E,k}(t), \end{aligned} \quad (4)$$

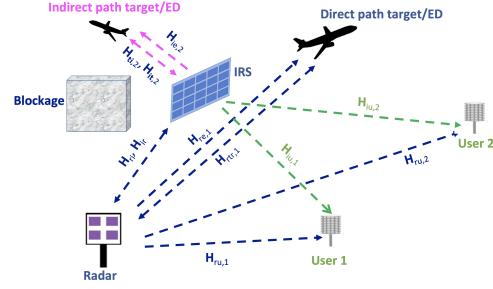


Fig. 1. MIMO-DFRC system with two targets/EDs and two users.

where $\mathbf{n}_{E,k}(t) \sim \mathcal{CN}(\mathbf{0}, \sigma_{E,k}^2 \mathbf{I})$ is the noise at the k -th ED.

The received signal at the l -th user is:

$$\begin{aligned} \mathbf{y}_l(t) = & \mathbf{H}_{ru}(\mathbf{W}\mathbf{m}(t - \tau_{ru,l}) + \mathbf{B}\mathbf{s}(t - \tau_{ru,l})) e^{j\omega_{ru,l} t} \\ & + \mathbf{H}_{iu,l} \Phi \mathbf{H}_{ri}(\mathbf{W}\mathbf{m}(t - \tau_{riu,l}) + \mathbf{B}\mathbf{s}(t - \tau_{riu,l})) e^{j\omega_{riu,l} t} \\ & + \mathbf{n}_U(t), \end{aligned} \quad (5)$$

where $\mathbf{n}_{U,k} \sim \mathcal{CN}(\mathbf{0}, \sigma_{U,k}^2 \mathbf{I})$ is the noise at the k -th ED.

The channel matrix for the path between radar and k -th ED is

$$\mathbf{G}_k = \alpha_k \mathbf{a}_{E,k}(\phi_k) \mathbf{a}_T(\theta_k)^T,$$

where α_k is the path attenuation, ϕ_k is the direction of the radar from ED's reference, and $\mathbf{a}_{E,k}(\phi_k)$ is the receive steering vector at target k defined as

$$\mathbf{a}_{E,k}(\phi_k) = [1, e^{j\frac{2\pi}{\lambda}d_e \sin(\phi_k)}, \dots, e^{j\frac{2\pi}{\lambda}(N_E-1)d_e \sin(\phi_k)}]^T$$

The channel matrix between radar and i -th legitimate receiver is \mathbf{F}_i .

Our goal is to determine the optimal precoding matrices \mathbf{W} and \mathbf{B} that maximize the secrecy rate and target detection [22]. Typical physical layer methods unrealistically assume that the channel to the ED is known. However, in the DFRC scenario, one could detect all the targets and estimate their channels. Thus, all but the legitimate receiver are classified as EDs with known channels.

3. MULTICAST WITH MULTIPLE EDS

Assume that the received signal at the radar $\mathbf{r}(t)$ is compensated for time delays and Doppler shifts and processed with matched filters corresponding to different targets [28]. The targets are sufficiently far apart so as not to interfere with each other's responses. We partition the targets into two sets \mathcal{D} and \mathcal{I} , such that $|\mathcal{D}| + |\mathcal{I}| = K$, for which only direct and indirect paths are available, respectively.

The signal returning via the IRS is delayed and very weak. Therefore, it can be neglected if the direct path is available. Denote $\mathbf{H}_{dc,k} = \mathbf{H}_{rtr,k}$ as the direct path channel for the k -th target, $k \in \mathcal{D}$. Then, the SINR corresponding to the k -th target with beamformer weights \mathbf{w}_k and \mathbf{b}_k is

$$\text{SINR}_{dc,k} = \frac{\text{Tr}(\mathbf{H}_{dc,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{dc,k}^H) + \text{Tr}(\mathbf{H}_{dc,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{dc,k}^H)}{\sigma_T^2}, \quad k \in \mathcal{D}. \quad (6)$$

However, if there is an obstacle in the direct path, then the direct path is ignored and we consider the following definition for targets $k \in \mathcal{I}$:

$$\text{SINR}_{in,k} = \frac{\text{Tr}(\mathbf{H}_{in,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{in,k}^H) + \text{Tr}(\mathbf{H}_{in,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{in,k}^H)}{\sigma_T^2}, \quad k \in \mathcal{I}, \quad (7)$$

where $\mathbf{H}_{in,k} = \mathbf{H}_{ir} \Phi \mathbf{H}_{ti,k} \mathbf{H}_{it,k} \Phi \mathbf{H}_{ri,k}$ is the channel gain for the indirect path for the k -th target.

From received signal $\mathbf{z}_k(t)$ at the k -th ED, its rate is

$$R_{e,k} = \log \det \left(\mathbf{I} + \left(\sigma_{E,k}^2 \mathbf{I} + \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H \right)^{-1} \left(\mathbf{G}_k \mathbf{W} \mathbf{W}^H \mathbf{G}_k^H \right) \right). \quad (8)$$

In a multicast setting, radar transmits a common message m to all users. Denote the channel matrix between the radar and user l by \mathbf{F}_l and the message for the l -th user, $l = 1, 2, \dots, L$ by $m_l(t)$. The received signal at the l -th user, with $\mathbf{m}(t) = [m_1(t), m_2(t), \dots, m_K(t)]^T$, is

$$\mathbf{y}_l(t) = \mathbf{F}_l(\mathbf{W}\mathbf{m}(t) + \mathbf{B}\mathbf{s}(t)) + \mathbf{n}_l(t) \quad (9)$$

where $\mathbf{n}_l \sim \mathcal{CN}(\mathbf{0}, \sigma_l^2 \mathbf{I})$ is the receiver noise. Hence, the rate at the l -th user is [29]

$$R_{u,l} = \log \det \left(\mathbf{I} + \left(\sigma_{R,l}^2 \mathbf{I} + \mathbf{F}_l \mathbf{B} \mathbf{B}^H \mathbf{F}_l^H \right)^{-1} \left(\mathbf{F}_l \mathbf{W} \mathbf{W}^H \mathbf{F}_l^H \right) \right). \quad (10)$$

The secrecy rate is maximized by solving the optimization problem:

$$\begin{aligned} & \text{maximize}_{\mathbf{W}, \mathbf{B}} \min_{l,k} [R_{u,l} - R_{e,k}]^+ \\ & \text{subject to } \text{Tr}(\mathbf{B} \mathbf{B}^H) + \text{Tr}(\mathbf{W} \mathbf{W}^H) \leq P, \\ & \text{Tr}(\mathbf{H}_{dc,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{dc,k}^H) + \text{Tr}(\mathbf{H}_{dc,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{dc,k}^H) \geq \gamma_k, k \in \mathcal{D}, \\ & \text{Tr}(\mathbf{H}_{in,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{in,k}^H) + \text{Tr}(\mathbf{H}_{in,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{in,k}^H) \geq \gamma_k, k \in \mathcal{I}, \end{aligned} \quad (11)$$

where P denotes the transmit power constraint and γ_k denotes the SINR threshold for target k .

4. SECRECY RATE MAXIMIZATION

In order to solve (12), our OptM3Sec algorithm follows a three-step approach as in [23]. However, unlike [23], our algorithm updates \mathbf{W} and \mathbf{B} through a nonconvex optimization problem, whose nonconvex feasible region is convexified via linearization of the SNR constraints. Further, the optimization over Φ is highly nonconvex in our problem and, therefore we use a specific version of stochastic gradient ascent as opposed to the semidefinite relaxation in [23]. Our algorithm consists of the following steps.

Optimizing over auxiliary matrices: Rewrite (11) as

$$\begin{aligned} & \text{maximize}_{\mathbf{W}, \mathbf{B}} \lambda \\ & \text{subject to } \text{Tr}(\mathbf{B} \mathbf{B}^H) + \text{Tr}(\mathbf{W} \mathbf{W}^H) \leq P, \\ & \text{Tr}(\mathbf{H}_{dc,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{dc,k}^H) + \text{Tr}(\mathbf{H}_{dc,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{dc,k}^H) \geq \gamma_k, k \in \mathcal{D}, \\ & \text{Tr}(\mathbf{H}_{in,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{in,k}^H) + \text{Tr}(\mathbf{H}_{in,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{in,k}^H) \geq \gamma_k, k \in \mathcal{I}, \\ & R_{u,l} - R_{e,k} \geq \lambda \geq 0 \forall l, k. \end{aligned} \quad (12)$$

After some tedious algebra, we obtain

$$\begin{aligned} & R_{u,l} - R_{e,k} \\ &= \underbrace{\log \det \left(\mathbf{I} + \mathbf{F}_l \mathbf{W} \mathbf{W}^H \mathbf{F}_l^H \left(\sigma_{R,l}^2 \mathbf{I} + \mathbf{F}_l \mathbf{B} \mathbf{B}^H \mathbf{F}_l^H \right)^{-1} \right)}_{\triangleq G_1} \\ &+ \underbrace{\log \det \left(\sigma_{E,k}^2 \mathbf{I} + \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H \right)}_{\triangleq G_2} \\ &- \underbrace{\log \det \left(\sigma_{E,k}^2 \mathbf{I} + \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H + \mathbf{G}_k \mathbf{W} \mathbf{W}^H \mathbf{G}_k^H \right)}_{\triangleq G_3}. \end{aligned} \quad (13)$$

It follows from [30, Lemma 4.1] that

$$\begin{aligned} G_1 &= \max_{\mathbf{W}_b \succ \mathbf{0}, \mathbf{U}_b} (\log \det(\mathbf{W}_b) - \text{Tr}(\mathbf{W}_b \mathbf{E}_b(\mathbf{U}_b, \mathbf{W}, \mathbf{B}))) \\ &+ \text{constant}, \end{aligned}$$

where $\mathbf{W}_b, \mathbf{U}_b$ are auxiliary matrices of appropriate dimensions, and $\mathbf{E}_b(\mathbf{U}_b, \mathbf{W}, \mathbf{B}) \doteq (\mathbf{I} - \mathbf{U}_b^H \mathbf{F}_l \mathbf{W})(\mathbf{I} - \mathbf{U}_b^H \mathbf{F}_l \mathbf{W})^H + \mathbf{U}_b^H (\sigma_{R,l}^2 \mathbf{I} + \mathbf{F}_l \mathbf{B} \mathbf{B}^H \mathbf{F}_l^H) \mathbf{U}_b$. The optimal solution $(\mathbf{W}_{b,l,k}^*, \mathbf{U}_{b,l,k}^*)$ is

$$\begin{aligned} \mathbf{U}_{b,l,k}^* &= \arg \max_{\mathbf{U}_b} (\log \det(\mathbf{W}_b) - \text{Tr}(\mathbf{W}_b \mathbf{E}_b(\mathbf{U}_b, \mathbf{W}, \mathbf{B}))) \\ &= (\sigma_{R,l}^2 \mathbf{I} + \mathbf{F}_l \mathbf{B} \mathbf{B}^H \mathbf{F}_l^H + \mathbf{F}_l \mathbf{W} \mathbf{W}^H \mathbf{F}_l^H)^{-1} \mathbf{F}_l \mathbf{W}, \end{aligned} \quad (14)$$

and $\mathbf{W}_{b,l,k}^* = (\mathbf{E}_b(\mathbf{U}_{b,l,k}^*, \mathbf{W}, \mathbf{B}))^{-1}$. Similarly, we use auxiliary matrices $\mathbf{W}_e, \mathbf{U}_e$ to define

$$G_2 = \max_{\mathbf{W}_e \succ \mathbf{0}, \mathbf{U}_e} (\log \det(\mathbf{W}_e) - \text{Tr}(\mathbf{W}_e \mathbf{E}_e(\mathbf{U}_e, \mathbf{B}))) + \text{constant},$$

where

$$\begin{aligned} \mathbf{E}_e(\mathbf{U}_e, \mathbf{B}) &\doteq \left(\mathbf{I} - \frac{1}{\sigma_{E,k}} \mathbf{U}_e^H \mathbf{G}_k \mathbf{B} \right) \left(\mathbf{I} - \frac{1}{\sigma_{E,k}} \mathbf{U}_e^H \mathbf{G}_k \mathbf{B} \right)^H \\ &+ \mathbf{U}_e^H \mathbf{U}_e. \end{aligned} \quad (15)$$

This yields $\mathbf{U}_{e,l,k}^* = \left(\mathbf{I} + \frac{1}{\sigma_{E,k}^2} \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H \right)^{-1} \frac{\mathbf{G}_k}{\sigma_{E,k}} \mathbf{B}$, and $\mathbf{W}_{e,l,k}^* = (\mathbf{E}_e(\mathbf{U}_{e,l,k}^*, \mathbf{B}))^{-1}$. Similarly, define

$$G_3 = \max_{\mathbf{W}_z \succ \mathbf{0}} (\log \det(\mathbf{W}_z) - \text{Tr}(\mathbf{W}_z \mathbf{E}_z(\mathbf{W}, \mathbf{B}))) + \text{constant},$$

$$\text{and } \mathbf{W}_{z,l,k}^* = \left(\mathbf{I} + \frac{1}{\sigma_{E,k}^2} \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H + \frac{1}{\sigma_{E,k}^2} \mathbf{G}_k \mathbf{W} \mathbf{W}^H \mathbf{G}_k^H \right)^{-1}.$$

Define $\mathbf{T} \doteq \{\mathbf{U}_b, \mathbf{W}_b, \mathbf{U}_e, \mathbf{W}_e, \mathbf{W}_z, \mathbf{W}, \mathbf{B}, \Phi\}$ as the collection of all unknown parameters. We solve (12) using the block coordinate descent (BCD) method.

Optimizing over (\mathbf{W}, \mathbf{B}) given Φ : Here, the SNR and secrecy rate constraints in (12) lead to a non-convex feasible region. The secrecy rate constraint can be convexified by (16). We linearize the SNR constraints by first-order Taylor series approximation around some initial approximations $\tilde{\mathbf{w}}_k$ and $\tilde{\mathbf{b}}_k$. Define $f_{dc}(\mathbf{w}_k, \mathbf{b}_k) = \text{Tr}(\mathbf{H}_{dc,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{dc,k}^H) + \text{Tr}(\mathbf{H}_{dc,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{dc,k}^H)$. Then, $f_{dc}(\mathbf{w}_k, \mathbf{b}_k) \approx f_{dc}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k) + \text{Re}(\nabla_{\mathbf{w}_k, \mathbf{b}_k}^T f_{dc}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k)(\mathbf{d}_k - \tilde{\mathbf{d}}_k))$, where $\mathbf{d}_k = [\mathbf{w}_k^T \mathbf{b}_k^T]^T$, $\nabla_{\mathbf{w}_k, \mathbf{b}_k} f_{dc} = [\frac{\partial f_{dc}}{\partial \mathbf{w}_k^T} \frac{\partial f_{dc}}{\partial \mathbf{b}_k^T}]^T$, and $\frac{\partial f_{dc}}{\partial \mathbf{w}_k^T} = 2\mathbf{w}_k^H \mathbf{H}_{dc,k} \mathbf{H}_{dc,k}^H$, and $\frac{\partial f_{dc}}{\partial \mathbf{b}_k^T} = 2\mathbf{b}_k^H \mathbf{H}_{dc,k} \mathbf{H}_{dc,k}^H$. This yields

$$\begin{aligned} & \text{maximize}_{\mathbf{W}, \mathbf{B}} \lambda \\ & \text{subject to } \text{Tr}(\mathbf{B} \mathbf{B}^H) + \text{Tr}(\mathbf{W} \mathbf{W}^H) \leq P, \\ & f_{dc}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k) + \text{Re}(\nabla_{\mathbf{w}_k, \mathbf{b}_k}^T f_{dc}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k)(\mathbf{d}_k - \tilde{\mathbf{d}}_k)) \geq \gamma_k, k \in \mathcal{D}, \\ & f_{in}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k) + \text{Re}(\nabla_{\mathbf{w}_k, \mathbf{b}_k}^T f_{in}(\tilde{\mathbf{w}}_k, \tilde{\mathbf{b}}_k)(\mathbf{d}_k - \tilde{\mathbf{d}}_k)) \geq \gamma_k, k \in \mathcal{I}, \\ & R_{u,l} - R_{e,k} \geq \lambda \geq 0 \forall l, k. \end{aligned} \quad (17)$$

This convex optimization problem is solved by any standard solver.

Optimizing Φ for given \mathbf{W}, \mathbf{B} : The SNR constraint for the direct

$$\begin{aligned}
& R_{u,l} - R_{e,k} \\
= & (\log \det(\mathbf{W}_b) - \text{Tr}(\mathbf{W}_b \mathbf{E}_b(\mathbf{U}_b, \mathbf{W}, \mathbf{B}))) + (\log \det(\mathbf{W}_e) - \text{Tr}(\mathbf{W}_e \mathbf{E}_e(\mathbf{U}_e, \mathbf{B}))) + (\log \det(\mathbf{W}_z) - \text{Tr}(\mathbf{W}_z \mathbf{E}_z(\mathbf{W}, \mathbf{B}))) + \text{constant} \\
= & \text{Tr}(\mathbf{W}_b (\mathbf{U}_b^H \mathbf{F}_l \mathbf{W} + \mathbf{W}^H \mathbf{F}_l^H \mathbf{U}_b)) - \text{Tr}(\mathbf{W}_b \mathbf{U}_b^H \mathbf{F}_l \mathbf{W} \mathbf{W}^H \mathbf{F}_l^H \mathbf{U}_b) - \frac{1}{\sigma_{E,k}^2} \text{Tr}(\mathbf{W}_z \mathbf{G}_k \mathbf{W} \mathbf{W}^H \mathbf{G}_k^H) \\
& + \text{Tr}(\mathbf{W}_e (\mathbf{U}_e^H \mathbf{G}_k \mathbf{B} + \mathbf{B}^H \mathbf{G}_k^H \mathbf{U}_e)) - \text{Tr}(\mathbf{W}_b \mathbf{U}_b^H \mathbf{F}_l \mathbf{B} \mathbf{B}^H \mathbf{F}_l^H \mathbf{U}_b) - \text{Tr}(\mathbf{W}_e \mathbf{U}_e^H \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H \mathbf{U}_e) - \text{Tr}\left(\frac{1}{\sigma_{E,k}^2} \mathbf{W}_z \mathbf{G}_k \mathbf{B} \mathbf{B}^H \mathbf{G}_k^H\right) \\
& + g(\mathbf{W}_b, \mathbf{W}_e, \mathbf{W}_z) + \text{constant}.
\end{aligned} \tag{16}$$

radar-target-radar links and the secrecy rates in (12) do not depend on Φ . Denote $h(\Phi) = \mathbf{H}_{in,k} \mathbf{w}_k \mathbf{w}_k^H \mathbf{H}_{in,k}^H + \mathbf{H}_{in,k} \mathbf{b}_k \mathbf{b}_k^H \mathbf{H}_{in,k}^H$. This results in the following optimization problem

$$\underset{\Phi}{\text{maximize}} \quad \underbrace{\min_{k \in \mathcal{I}} \text{Tr}(h(\Phi)) - \gamma_k}_{\doteq f(\Phi) = \tilde{f}(\tilde{\Phi})}. \tag{18}$$

Denote the phase shift induced by the i -th reflection unit of the IRS as $\phi_i \in [0, \pi]$ and $\tilde{\Phi} \doteq [\phi_1 \ \phi_2 \ \dots \ \phi_N]^T$. Since the objective function $\tilde{f}(\tilde{\Phi})$ is nonconvex in $(\tilde{\Phi})$, we solve it by simultaneous perturbation stochastic approximation (SPSA) [31], which is a specific version of stochastic gradient ascent. In SPSA, we iteratively update $\tilde{\Phi}(t)$. In the t -th iteration, a zero-mean perturbation vector $\Delta(t) \in \mathbb{R}^{N \times 1}$ is generated independently, where each of its entries $\{\Delta_i(t) : 1 \leq i \leq N\}$ is chosen from the set $\{-1, 1\}$ with equal probability. Then the iterate $\tilde{\Phi}(t)$ is perturbed in two opposite directions as $\tilde{\Phi}^+(t) \doteq \tilde{\Phi}(t) + c(t)\Delta(t)$ and $\tilde{\Phi}^-(t) \doteq \tilde{\Phi}(t) - c(t)\Delta(t)$. Next, for all $1 \leq i \leq N$, the i -th component of $\tilde{\Phi}(t)$ is updated as

$$\phi_i(t+1) = \phi_i(t) + a(t) \times \frac{\tilde{f}(\tilde{\Phi}^+(t)) - \tilde{f}(\tilde{\Phi}^-(t))}{2c(t)\Delta_i(t)}, \tag{19}$$

and the iterates are projected onto the interval $[0, \pi]$ to ensure feasibility. The *positive* step size sequences $\{a(t)\}_{t \geq 1}$ and $\{c(t)\}_{t \geq 1}$ need to satisfy the following conditions: (i) $\sum_{t=1}^{\infty} a(t) = \infty$, (ii) $\sum_{t=1}^{\infty} a^2(t) < \infty$, (iii) $\lim_{t \rightarrow \infty} c(t) = 0$, and (iv) $\sum_{t=1}^{\infty} \frac{a^2(t)}{c^2(t)} < \infty$. The SPSA iteration is run until a suitable stopping criterion is met. Algorithm 1 summarizes the steps of our OptM3Sec method.

Algorithm 1 Optimization of multiple ED multicast multi-antenna DFRC secrecy rate (OptM3Sec)

- Input:** All channel gains and noise covariances, P , $\{\gamma_k : k \in \mathcal{D}, k \in \mathcal{I}\}$.
- Output:** $\mathbf{W}, \mathbf{B}, \tilde{\Phi}$
- 1: **Initialisation:** $\mathbf{W}(0), \mathbf{B}(0), \tilde{\Phi}(0)$, and $\tau = 0$.
- 2: **for** $\tau = 1, 2, 3, \dots$ **do**
- 3: Given $\mathbf{W}(\tau-1), \mathbf{B}(\tau-1), \tilde{\Phi}(\tau-1)$, compute $\mathbf{U}_{b,l,k}^*(\tau), \mathbf{W}_{b,l,k}^*(\tau), \mathbf{U}_{e,l,k}^*(\tau), \mathbf{W}_{e,l,k}^*(\tau), \mathbf{W}_{z,l,k}^*(\tau)$ for all l, k .
- 4: For given $\mathbf{U}_{b,l,k}^*(\tau), \mathbf{W}_{b,l,k}^*(\tau), \mathbf{U}_{e,l,k}^*(\tau), \mathbf{W}_{e,l,k}^*(\tau), \mathbf{W}_{z,l,k}^*(\tau)$ and $\tilde{\Phi}(\tau-1)$, find $\mathbf{W}(\tau)$ and $\mathbf{B}(\tau)$ by solving (17).
- 5: For given $\mathbf{U}_{b,l,k}^*(\tau), \mathbf{W}_{b,l,k}^*(\tau), \mathbf{U}_{e,l,k}^*(\tau), \mathbf{W}_{e,l,k}^*(\tau), \mathbf{W}_{z,l,k}^*(\tau)$ and given $\mathbf{W}^*(\tau)$ and $\mathbf{B}^*(\tau)$, find $\tilde{\Phi}(\tau)$ by running many iterations of SPSA.
- 6: Stop when a suitable criterion is met.

5. EXPERIMENTS AND SUMMARY

We validated our proposed method through numerical experiments. We considered a system with a single IRS, a radar, two multiple

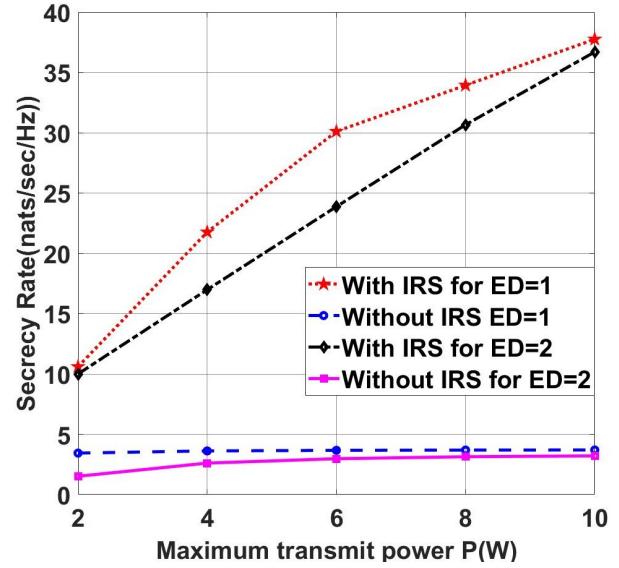


Fig. 2. Achieved Secrecy rate against different maximum power limits and for different ED/target.

antenna receivers. We set $N_T = 4$ for radar transmit and receive antennas, $N_R = 4$ for user receive antennas, and $N_E = 4$ receive antennas for each ED. The IRS is equipped with $N = 10$ array of reflecting units. We consider two attack scenarios for our simulations, the first being when the attack is performed by a single ED and the second when the attack is done by two EDs. In the first attack setup we consider the target's true directions with respect to the radar as $\theta_1 = 72^\circ$ and from the reference of two EDs, the radar is located at $\phi_1 = -85^\circ$. In the second scenario the target's true directions with respect to the radar are $\theta_1 = 72^\circ$ and $\theta_2 = 78^\circ$. From the reference of two EDs, the radar is located at $\phi_1 = -85^\circ$ and $\phi_2 = -88^\circ$. The RCS coefficient and path loss variables are set as $\alpha_1 = 0.1$, $\alpha_2 = 0.1$, $\beta_1 = 0.1$, and $\beta_2 = 0.1$. The variances of all Gaussian noise variables are set to unity.

For all channels involved, we sampled each channel coefficient from an independent circularly symmetric complex Gaussian random variable with zero mean and variance of unity. Fig 2 shows that in presence of a single ED, with our OptM3Sec algorithm, the secrecy rate increases with the maximum transmit power P compared to the case when there is no IRS present. It is also evident from Fig 2 that in presence of two EDs, the secrecy rate also increases with the maximum transmit power P , however it can be observed that due to the increase in the number of EDs there is a slight decrease in the secrecy rate which is very intuitive. The above results highlight the significance of IRS in secrecy rate performance for multicast IRS-aided MIMO DFRC system with multiple EDs.

6. REFERENCES

- [1] H. Griffiths, L. Cohen, S. Watts, E. Mokole, C. Baker, M. Wicks, and S. Blunt, "Radar spectrum engineering and management: Technical and regulatory issues," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 85–102, 2015.
- [2] K. V. Mishra, M. B. Shankar, V. Koivunen, B. Ottersten, and S. A. Vorobyov, "Toward millimeter-wave joint radar communications: A signal processing perspective," *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 100–114, 2019.
- [3] 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, 2015.
- [4] B. K. Chalise and M. G. Amin, "Performance tradeoff in a unified system of communications and passive radar: A secrecy capacity approach," *Digital Signal Processing*, vol. 82, pp. 282–293, 2018.
- [5] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 358–370, 2011.
- [6] 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*, vol. 21, no. 2, pp. 1773–1828, 2018.
- [7] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.
- [9] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, 2011.
- [10] L. Li, Z. Chen, and J. Fang, "On secrecy capacity of Gaussian wiretap channel aided by a cooperative jammer," *IEEE Signal Processing Letters*, vol. 21, no. 11, pp. 1356–1360, 2014.
- [11] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.
- [12] Z. Chu, K. Cumanan, Z. Ding, and et. al, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.
- [13] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.
- [14] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *Signal Processing, IEEE Transactions on*, vol. 59, no. 10, pp. 4985–4997, 2011.
- [15] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.
- [16] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 7, pp. 1081–1090, 2013.
- [17] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: secure DoF and jammer scaling law," *IEEE Transactions on Signal Processing*, vol. 62, no. 4, pp. 828–839, 2014.
- [18] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.
- [19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
- [20] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 83–95, 2020.
- [21] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8139–8151, 2017.
- [22] A. Deligiannis, A. Daniyan, S. Lambotharan, and J. A. Chambers, "Secrecy rate optimizations for MIMO communication radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 5, pp. 2481–2492, 2018.
- [23] S. Fang, G. Chen, P. Xu, J. Tang, and J. A. Chambers, "SINR maximization for RIS-assisted secure dual-function radar communication systems," in *IEEE Global Communications Conference*, 2021, in press.
- [24] A. M. Elbir and K. V. Mishra, "A survey of deep learning architectures for intelligent reflecting surfaces," *arXiv preprint arXiv:2009.02540*, 2020.
- [25] J. A. Hodge, K. V. Mishra, and A. I. Zaghloul, "Intelligent time-varying metasurface transceiver for index modulation in 6G wireless networks," *IEEE Antennas and Wireless Propagation Letters*, vol. 19, no. 11, pp. 1891–1895, 2020.
- [26] M. F. Ahmed, K. P. Rajput, N. K. Venkategowda, K. V. Mishra, and A. K. Jagannatham, "Joint transmit and reflective beamformer design for secure estimation in IRS-aided WSNs," *IEEE Signal Processing Letters*, 2022, in press.
- [27] Z. Esmaeilbeig, K. V. Mishra, and M. Soltanalian, "IRS-aided radar: Enhanced target parameter estimation via intelligent reflecting surfaces," *arXiv preprint arXiv:2110.13251*, 2021.
- [28] B. Friedlander, "On transmit beamforming for MIMO radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 4, pp. 3376–3388, 2012.
- [29] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
- [30] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2841–2853, 2015.
- [31] J. C. Spall *et al.*, "Multivariate stochastic approximation using a simultaneous perturbation gradient approximation," *IEEE Transactions on Automatic Control*, vol. 37, no. 3, pp. 332–341, 1992.