Pareto-Theory for Enabling Covert Intrapulse Radar-Embedded Communications

D. Ciuonzo*, A. De Maio*, G. Foglia† and M. Piezzo†
*DIETI, University of Naples "Federico II", Naples, Italy. E-mail: domenico.ciuonzo@ieee.org, ademaio@unina.it.
†ELETTRONICA S.p.A., Rome, Italy. E-mail: goffredo.foglia@gmail.com, marco.piezzo@unina.it.

***Abstract*—We deal with the problem of intrapulse radar-embedded communication, and propose a novel waveform design procedure based on multi-objective optimization. Precisely, under both energy and similarity constraints, we devise orthogonal signals aiming at maximization of the Signal-to-Interference Ratio (SIR) and minimization of a suitable correlation index (related to the possibility of waveform interception). The problem can be cast into a non-convex multi-objective optimization and solved via the so-called scalarization technique. Finally, performance of the proposed waveform design scheme is assessed in terms of both Symbol Error Rate (SER) and the so-called "intercept metric".**

I. Introduction

Establishing a covert communication has always represented a critical issue for defense-related applications. Along the years, various strategies have been proposed as viable means of masking the data transmission to hostile interceptors.

A possibility is to directly exploit a waveform already present in the probed environment, such as pre-existing communications [1] or the actual radar backscattered interference [2]. In such a case, a radio frequency tag/transponder, such as a radio frequency identifier (RFID) [3], is first employed to suitably remodulate the incident radiation, then to embed the devised communication signal in the ambient electromagnetic background, thus providing a natural masking in the clutter environment. The literature for this class of approaches has been quite fertile; in fact, starting from the seminal work of [4] (who first proposed using modulated reflectors for communication), various tag-based Radar-EMbedded (REM) modulation techniques have been proposed. A few examples are [2] and [5], where the radar illumination is modulated on an inter-pulse basis by applying phase-shift sequences over known Coherent Processing Intervals (CPI). However, even though a Low Probability of Intercept (LPI) is ensured (since the signaling is covert by the radar backscatter), a low data-rate is provided (in the order of bits-per-CPI).

In [6] a novel intrapulse REM communication procedure is proposed, based on the remodulation of the incident radar signaling, through an RF tag/transponder (within the probed environment), into one of the possible K different waveforms (acting as information symbols). Three approaches to the waveform design problem have been presented and deeply investigated. The idea is to properly exploit the natural masking provided by the ambient scatter, by devising symbols sharing a certain correlation with the surrounding radar reflections, so as to make very hard the recovery of the information for a hostile eavesdropper (thus ensuring a LPI). Moreover, the waveforms are sufficiently separated (mutually orthogonal in the ideal case) in order to minimize the mutual interference, thus ensuring a low Symbol Error Rate (SER), and should be distant enough from the backscatter in order to allow the intended receiver to extract the useful signal. This is achieved designing symbols that reside in (or very close to) the passband of the incident radar illumination, temporally (fast-time phase and amplitude) modulating them so that they still possess a manageable level of correlation with the radar scattering. Further developments are presented in [7], where two notable enhancements are the use of time-reversal for multipath mitigation and a two-stage detection/classification scheme at intended receiver which allows blind self-synchronization.

Intuitively, a tradeoff exists between the desire of ensuring a low SER and keeping a "low profile" in the communication. Therefore, following the hint of [6], we propose an intrapulse REM communication design procedure based on the joint optimization of the two aforementioned (conflicting) objectives; namely, we aim at producing orthogonal symbols which maximize the SIR and minimize the probability of intercept. The resulting waveform design problem can be cast into a non-convex multi-objective optimization and solved via the use of the Pareto-optimal theory [8], [9]. We prove that optimal points of the scalarized problem can be always found exploiting hidden convexity via semidefinite programming and rank-one decomposition theorems [10], [11]. Our approach is a general framework and includes, as special instances, the simple (but yet effective) waveform designs in [6].

The paper is organized as follows[1]. In Sec. II, we describe the system model while in Sec. III we discuss the figure of

[1]*Notation* - We use boldface for vectors $\boldsymbol{a}$ (lower case), and matrices $\boldsymbol{A}$ (upper case). The n-th element of $\boldsymbol{a}$ and the (m,ℓ)-th entry of $\boldsymbol{A}$ are denoted by $a(n)$ and $\boldsymbol{A}(m,\ell)$, respectively. The transpose, conjugate, Hermitian, Euclidean norm and trace operators are denoted by the symbols $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^\dagger$, $\|\cdot\|$ and $\mathrm{tr}(\cdot)$ respectively. $\boldsymbol{I}$ and $\boldsymbol{0}$ denote the identity matrix and the null matrix (when not underlined through a subscript, their size will be understood from the context), respectively. $\mathbb{R}^N$, $\mathbb{C}^N$, and $\mathbb{H}^N$ are the sets of N-dimensional vectors of real and complex numbers, and $N \times N$ Hermitian matrices, respectively. Given a vector $\boldsymbol{a} \in \mathbb{C}^N$, $\mathrm{diag}(\boldsymbol{a})$ indicates the N-dimensional diagonal matrix whose i-th diagonal element is $a(i)$, $i = 1, \ldots, N$. The curled inequality symbol $\succeq$ (and its strict form $\succ$) is used to denote generalized matrix inequality: for any $\boldsymbol{A} \in \mathbb{H}^N$, $\boldsymbol{A} \succeq \boldsymbol{0}$ (resp. $\boldsymbol{A} \succ \boldsymbol{0}$) means that $\boldsymbol{A}$ is a positive semidefinite (resp. positive definite) matrix. For any $x \in \mathbb{C}$, $|x|$ represents its modulus. The letter j denotes the imaginary unit (i.e. $j = \sqrt{-1}$). $\mathbb{E}[\cdot]$ and $\mathrm{var}[\cdot]$ denote the statistical expectation and variance, respectively. $\mathcal{CN}(\boldsymbol{0}, \boldsymbol{R})$ denotes a complex-valued multivariate Gaussian pdf with zero mean vector and covariance $\boldsymbol{R}$. Finally, for any optimization problem $\mathcal{P}$, we denote with $v(\mathcal{P})$ its optimal value.

978-1-4799-8232-5/151$31.00@2015IEEE

merits to optimize. In Sec. IV, we formulate the waveform design problem and present the algorithm providing Pareto-optimal waveforms. Finally, in Sec. V we assess the performance of our method in comparison with the design techniques in [6]; conclusions are drawn in Sec. VI.

II. System Model

We consider the same model of [6]. Precisely, let $s(t)$, $t \in [0,T]$, be the complex-baseband (with bandwidth B) of the radar waveform illuminating a given area. By sampling the incident illumination at the Nyquist sampling rate (that is, B complex samples/second), a tag would obtain a discrete representation of the radar wave, collected in $N \approx BT$ complex samples, which however fully occupies the unambiguous bandwidth, thus leaving no spectral region where the symbol could be embedded. Thus, in order to acquire additional design Degrees-of-Freedom (DoFs), the tag oversamples the incident wave at a rate of MB complex samples/second, with $M > 1$ being the oversampling factor: by doing so, additional spectrum can be exploited so as to earn a new covert region where the communication signal can be embedded. Of course, the choice of M determines how much additional spectral space (DoFs) can be made available at the tag. Let $\boldsymbol{s} = \begin{bmatrix} s(1) & \dots & s(MN) \end{bmatrix}^T$ be the vector containing the MN samples. A discrete representation of the radar backscattering model involves the convolution of the discretized sequence $\boldsymbol{s}$ with the discretized version of the aggregate ambient scattering [6], which can be expressed in terms of the multiplication $\boldsymbol{S}\,\boldsymbol{x}$, where $\boldsymbol{S} \in \mathbb{C}^{MN \times (2MN-1)}$ is the matrix accounting for the shifted versions of the illuminating radar waveform (i.e. whose i-th row equals $\begin{bmatrix} \boldsymbol{0}_{i-1}^T & \boldsymbol{s}_f^T & \boldsymbol{0}_{MN-1-i}^T \end{bmatrix}^T$, with $\boldsymbol{s}_f$ being the flipped version of $\boldsymbol{s}$, i.e. $s_f(i) = s(MN+1-i)$) and $\boldsymbol{x} \in \mathbb{C}^{(2MN-1)\times 1}$ contains the range samples of the aggregate ambient radar scattering. Also, let $\boldsymbol{c}_k$, $k = 1, \dots, K$, be the k-th devised embedded symbol. Therefore, the discretized signal (when k-th waveform is transmitted) received by the (intentional and/or unintentional) receiver can be expressed as the following $MN \times 1$ dimensional column vector[2]:

$$\boldsymbol{y}_{rk} = \alpha \boldsymbol{c}_k + \beta \boldsymbol{S}\boldsymbol{x} + \boldsymbol{n}\,, \tag{1}$$

where $\alpha \in \mathbb{C}$ is the (unknown) echo amplitude (accounting for the transmit amplitude and channels propagation effects), $\beta \in \mathbb{R}^+$ subsumes the strength of the interference sources, and $\boldsymbol{n} \in \mathbb{C}^{MN\times 1}$ is the vector of the noise samples.

Without loss of generality, we draw out $\boldsymbol{x} \sim \mathcal{CN}\left(\boldsymbol{0}, \frac{1}{MN}\boldsymbol{I}\right)$ and $\boldsymbol{n} \sim \mathcal{CN}\left(\boldsymbol{0}, \frac{1}{MN}\boldsymbol{I}\right)$ in order to account for the average power of the embedded communication signal and that of the auto-interference directly in α and β, respectively. Indeed, by doing so, the input Signal-to-Noise Ratio (SNR) and SIR for k-th waveform are given by $\mathrm{SNR}_k \triangleq \mathbb{E}\left[\|\alpha \boldsymbol{c}_k\|^2\right] / \mathbb{E}\left[\|\boldsymbol{n}\|^2\right] = |\alpha|^2 \|\boldsymbol{c}_k\|^2$ and $\mathrm{SIR}_k \triangleq \mathbb{E}\left[\|\alpha \boldsymbol{c}_k\|^2\right] / \mathbb{E}\left[\|\beta \boldsymbol{S}\boldsymbol{x}\|^2\right] = (|\alpha|^2/\beta^2)(||\boldsymbol{c}_k||^2/||\boldsymbol{s}||^2)$, respectively.

[2]Hereinafter we will use the notation $\boldsymbol{y}_r$ when the actual symbol transmitted is not known at the receiver.

III. Performance measures

In this section we focus on the key performance measures to optimize or control in waveform design.

Output SIR: It is necessary, for the intended receiver, to have knowledge of the set of K communication symbols transmitted by the tag, since a coherent processing of the received signal is necessary to extrapolate the useful component from it. Thus, a set of properly designed K filters, say $\boldsymbol{w}_k$, $k = 1, \dots, K$, are assumed at receiver side. Given the signal model (1), the normalized (output) SIR for the k-th REM waveform is given by:

$$\mathrm{SIR}_{o,k} \triangleq \frac{1}{MN} \frac{\mathbb{E}\left[|\boldsymbol{w}_k^\dagger \boldsymbol{c}_k|^2\right]}{\mathbb{E}\left[|\boldsymbol{w}_k^\dagger \boldsymbol{S}\boldsymbol{x}|^2\right]} = \frac{|\boldsymbol{w}_k^\dagger \boldsymbol{c}_k|^2}{\boldsymbol{w}_k^\dagger (\boldsymbol{S}\boldsymbol{S}^\dagger)\boldsymbol{w}_k}\,. \tag{2}$$

It is well know [12] that the filter maximizing (2) has the form $\boldsymbol{w}_k^\star = (\boldsymbol{S}\boldsymbol{S}^\dagger)^{-1}\boldsymbol{c}_k$, which, after substitution, leads to the optimized k-th normalized SIR, i.e. $\mathrm{SIR}_{o,k}^\star = \boldsymbol{c}_k^\dagger (\boldsymbol{S}\boldsymbol{S}^\dagger)^{-1}\boldsymbol{c}_k$. The latter metric will be used as a performance measure to achieve low values of SER.

Orthogonal projection: Using the considered model, we can obtain a suited orthogonal basis for the waveforms design, computing the eigendecomposition of the correlation matrix of $\boldsymbol{S}$, i.e. $\boldsymbol{S}\boldsymbol{S}^\dagger = \boldsymbol{V}\boldsymbol{\Lambda}\boldsymbol{V}^\dagger$, where $\boldsymbol{\Lambda}$ is the diagonal matrix of the eigenvalues of $\boldsymbol{S}\boldsymbol{S}^\dagger$ (*sorted in increasing magnitude*, i.e. $\lambda_i \le \lambda_{i+1}$) and $\boldsymbol{V} = [\boldsymbol{v}_1\ \boldsymbol{v}_1\ \dots\ \boldsymbol{v}_{MN}]$ contains the corresponding MN eigenvectors. Those belonging to the non-dominant space possess the least correlation with the ambient scatter; thus, they can be exploited to design the symbols, so as to lower the SER, at the expenses of a higher probability of intercept (since the symbols are not sufficiently "covered"). Following the so-called "Dominant Projection" (DP) approach [6], we focus on projecting away the designed $\boldsymbol{c}_k$ from the dominant subspace. To this end, let us define the following quantities:

- The eigendecomposition $\boldsymbol{S}_{P,k-1}\boldsymbol{S}_{P,k-1}^\dagger = \boldsymbol{V}_{P,k-1}\boldsymbol{\Lambda}_{P,k-1}\boldsymbol{V}_{P,k-1}^\dagger$, where $\boldsymbol{S}_{P,k-1} \triangleq \begin{bmatrix} \boldsymbol{S} & \boldsymbol{c}_1 & \cdots & \boldsymbol{c}_{k-1} \end{bmatrix}$, $k = 1, \dots, K$, with the eigenvalues sorted in increasing magnitude.
- The specific index L of the eigenvectors belonging to the non-dominant space, but close enough to the dominant eigenspectrum (a typical choice would be $L = (M-1)\,N$).
- $\boldsymbol{V}_{D,k-1} \triangleq \begin{bmatrix} \boldsymbol{v}_{L-(k-1)+1} & \cdots & \boldsymbol{v}_{MN} \end{bmatrix}$ contains the $(MN-L+k-1)$ eigenvectors comprising the dominant space of $\boldsymbol{V}_{P,k-1}$.
- $\boldsymbol{P}_{k-1}^\perp \triangleq \boldsymbol{V}_{D,k-1}\boldsymbol{V}_{D,k-1}^\dagger$ and $\boldsymbol{P}_{k-1} \triangleq (\boldsymbol{I} - \boldsymbol{P}_{k-1}^\perp)$, $k = 1, \dots, K$, where $\boldsymbol{P}_{k-1}$ projects any waveform away from the space defined by the $(MN-L+k-1)$ vectors of the dominant space of $\boldsymbol{V}_{P,k-1}$.

Thus, *we search for waveforms complying with* $\boldsymbol{P}_{k-1}^\perp \boldsymbol{c}_k = \boldsymbol{0}$, $k = 1, \dots, K$. This strategy forces mutual orthogonality among the devised signals; also, due to the projection operation, the dominant space is wholly involved, which confers to

the design procedure an improved robustness with respect to other approaches based on the individual eigenvectors [6].

Energy constraint: A critical constraint is given by the energy radiated from the tag. Indeed, the power injected in the illuminated area has to be properly tuned in order to: (i) balance between an acceptable SER and a satisfying LPI; (ii) deal with energy source limitations (indeed for passive/semi-passive transponders no battery or power source may actually be present to supply an active transmission). Based on these reasons, we enforce the energy constraint $\|\boldsymbol{c}_k\|^2 = 1$.

Similarity constraint: Aiming at increasing symbols covertness, we enforce a spectral similarity with a given pseudo-random sequence (denoted here as $\boldsymbol{d}_{0,k}$) over the frequencies belonging to the spectral tail of the oversampled radar signal; thus the communication signal will appear as a noise-like waveform to a hostile eavesdropper scanning the whole spectrum. Let $\widehat{\boldsymbol{W}} \triangleq \begin{bmatrix} \boldsymbol{w}_{\hat{m}}^T & \boldsymbol{w}_{\hat{m}+1}^T & \cdots & \boldsymbol{w}_{\hat{m}+F-1}^T \end{bmatrix}^T$ be the $F \times MN$ (with $\widehat{N} > MN$) reduced Discrete Fourier Transform (DFT) matrix in which the $\widehat{n}$-th row ($\widehat{n} \in \{\hat{m}, \ldots, \hat{m}+F-1\}$) corresponds to the "discrete" frequency $\nu_{\hat{n}} \triangleq \frac{\widehat{n}-1}{\widehat{N}}$, that is $\boldsymbol{w}_{\widehat{n}} \triangleq \frac{1}{\sqrt{\widehat{N}}} \begin{bmatrix} 1 & e^{-j2\pi\nu_{\widehat{n}}} & \cdots & e^{-j2\pi\nu_{\widehat{n}}(MN-1)} \end{bmatrix}$. The similarity constraint is here enforced only on a subset of $F < \widehat{N}$ discrete frequencies corresponding to the additional tail skirt of the backscattered radar signal spectrum[3], that is:

$$\|\widehat{\boldsymbol{W}}\boldsymbol{c}_k - \widehat{\boldsymbol{W}}\boldsymbol{d}_{0,k}\|^2 \leq \epsilon \quad k = 1, \ldots, K, \tag{3}$$

where $\epsilon \in [0, 4)$ is a similarity parameter.

LPI metric: In [6], a simple metric is introduced to ascertain how accurately a (intentional/unintentional) receiver, with prior knowledge on $s(t)$ and M, would be able to extract the symbol embedded within the radar backscatter. The key point is represented by the projector $\widetilde{\boldsymbol{P}}_\ell \triangleq (\boldsymbol{I} - \boldsymbol{V}_\ell \boldsymbol{V}_\ell^\dagger)$, $\ell \in \{1, \ldots, MN\}$, where $\boldsymbol{V}_\ell \in \mathbb{C}^{MN \times \ell}$ is the matrix of eigenvectors corresponding to the ℓ largest eigenvalues[4] of $\boldsymbol{S}\boldsymbol{S}^\dagger$. The assumption is that the eavesdropper is able of getting the ℓ-th projection residue $\boldsymbol{z}_k^\ell \triangleq (\widetilde{\boldsymbol{P}}_\ell \, \boldsymbol{y}_{rk})$; by doing so, we can define the normalized correlation with the n-th waveform as

$$\eta_{n,k}^\ell \triangleq |\boldsymbol{c}_n^\dagger \boldsymbol{z}_k^\ell| \, / \, (\|\boldsymbol{c}_n\| \|\boldsymbol{z}_k^\ell\|) \quad \ell = 1, \ldots, MN-1\,, \tag{4}$$

where $|\boldsymbol{c}_n^\dagger \boldsymbol{z}_k^\ell| = |\alpha \boldsymbol{c}_n^\dagger \widetilde{\boldsymbol{P}}_\ell \boldsymbol{c}_k + \beta \boldsymbol{c}_n^\dagger \widetilde{\boldsymbol{P}}_\ell \boldsymbol{S}\boldsymbol{x} + \boldsymbol{c}_n^\dagger \widetilde{\boldsymbol{P}}_\ell \boldsymbol{n}|$. Though not directly linked to the probability of intercept, Eq. (4) still represents a viable tool to figure out how accurately the waveform (embedded in the radar backscattering) can be extracted by a eavesdropper, that is when $\eta_{n,k}^\ell$ (for a given index ℓ) gets higher values, $\boldsymbol{c}_n$ presumably has a higher similarity with the waveform embedded in the received signal. In summary, we assume that the correlation between $\boldsymbol{c}_n$ and $\widetilde{\boldsymbol{P}}_\ell \boldsymbol{c}_k$ has a greater impact, over the actual value of $\eta_{n,k}^\ell$, than the other two components[5]. Also, given the orthogonal projection employed, the mutual correlation between $\boldsymbol{c}_n$ and the residue $\widetilde{\boldsymbol{P}}_\ell \boldsymbol{c}_k$, for $k \neq n$ and $\ell = 1, \ldots, MN-1$, is designed to be extremely low. Consequently, we infer $\eta_{n,k}^\ell$ to be quite small for $k \neq n$, for all $\ell = 1, \ldots, MN-1$, at least when $k \neq n$; nevertheless, this supposition may not hold true anymore when $k = n$. Therefore, in order to lower $\eta_{n,n}^\ell$, we aim at *minimizing* $\boldsymbol{c}_n^\dagger \widetilde{\boldsymbol{P}}_\ell \boldsymbol{c}_n$ for all $\ell = 1, \ldots, MN-1$.

IV. Problem Formulation

The pursued idea is to design mutually orthogonal waveforms which jointly optimize the SER (via SIR maximization) and the LPI behavior (via minimization of $\boldsymbol{c}_n^\dagger \widetilde{\boldsymbol{P}}_\ell \boldsymbol{c}_n$, $\ell = 1, \ldots MN-1$), with a spectral similarity to a known pseudo-random sequence $\boldsymbol{d}_{0,k}$, and an energy constraint.

Based on these reasons, we formulate our problem in terms of a non-convex multi-objective (with MN objectives) optimization for k-th waveform as [8]

$$\mathcal{P}_1 \triangleq \begin{cases} \max\limits_{\boldsymbol{c}_k} & \left(\boldsymbol{c}_k^\dagger (\boldsymbol{S}\boldsymbol{S}^\dagger)^{-1} \boldsymbol{c}_k; \, -\{\boldsymbol{c}_k^\dagger \, \widetilde{\boldsymbol{P}}_\ell \, \boldsymbol{c}_k\}_{\ell=1}^{MN-1} \right) \\ \text{s.t.} & \boldsymbol{P}_{k-1}^\perp \boldsymbol{c}_k = \boldsymbol{0}\,, \quad \boldsymbol{c}_k^\dagger \boldsymbol{c}_k = 1\,, \\ & \|\widehat{\boldsymbol{W}}\boldsymbol{c}_k - \widehat{\boldsymbol{W}}\boldsymbol{d}_{0,k}\|^2 \leq \epsilon\,, \end{cases} \tag{5}$$

for $k = 1, \ldots, K$. Problem $\mathcal{P}_1$ is reduced in a single-objective form via the use of the "scalarization" technique [8]:

$$\mathcal{P}_2 \triangleq \begin{cases} \max\limits_{\boldsymbol{c}_k} & \boldsymbol{c}_k^\dagger (\gamma_1 \, \boldsymbol{R} - \gamma_2 \, \widetilde{\boldsymbol{P}}) \, \boldsymbol{c}_k \\ \text{s.t.} & \boldsymbol{P}_{k-1}^\perp \boldsymbol{c}_k = \boldsymbol{0}, \quad \boldsymbol{c}_k^\dagger \boldsymbol{c}_k = 1, \\ & \|\widehat{\boldsymbol{W}}\boldsymbol{c}_k - \widehat{\boldsymbol{W}}\boldsymbol{d}_{0,k}\|^2 \leq \epsilon\,, \end{cases} \tag{6}$$

where $\gamma_1 \triangleq (\zeta_1 / \lambda_{\max}(\boldsymbol{R}))$ and $\gamma_2 \triangleq (\zeta_2 / \lambda_{\max}(\widetilde{\boldsymbol{P}}))$ ($\gamma_i \in \mathbb{R}^+$) represent the weights[6], and we have denoted $\boldsymbol{R} \triangleq (\boldsymbol{S}\boldsymbol{S}^\dagger)^{-1}$, and $\widetilde{\boldsymbol{P}} \triangleq \sum_{\ell=1}^{MN-1} \widetilde{\boldsymbol{P}}_\ell$.

Due to the first constraint, a waveform $\widehat{\boldsymbol{c}}_k \in \mathbb{C}^{(L-k+1)}$ exists such that $\boldsymbol{c}_k = \boldsymbol{U}_{k-1} \widehat{\boldsymbol{c}}_k$, where $\boldsymbol{P}_{k-1} = \boldsymbol{U}_{k-1} \boldsymbol{U}_{k-1}^\dagger$ (i.e. the eigenvectors associated to the projector $\boldsymbol{P}_{k-1}$). Also, it is apparent that the similarity vector should be defined as $\boldsymbol{d}_{0,k} \triangleq \boldsymbol{U}_{k-1} \boldsymbol{d}_k / \|\boldsymbol{U}_{k-1} \boldsymbol{d}_k\|$, with $\boldsymbol{d}_k \in \mathbb{C}^{(L-k+1)\times 1}$ being a pseudo-random vector. Indeed, both the projection and the normalization operations are necessary in the definition of $\boldsymbol{d}_{0,k}$ in order to make the optimization feasible, since $\boldsymbol{d}_{0,k}$ has to be a direction vector belonging to the same subspace of $\boldsymbol{c}_k$. Then, we can focus on the design of $\widehat{\boldsymbol{c}}_k$. Also, $\mathcal{P}_2$

[3] A reasonable choice for F is given by the approximate number of discrete frequencies not occupied by the radar signal, that is $F \approx ((M-1)/M)\, \widehat{N}$.

[4] When $\ell = MN$, $\widetilde{\boldsymbol{P}}_{MN} = \boldsymbol{0}$, thus we do not consider this index.

[5] Indeed, $\boldsymbol{c}_n$ is designed to have a partial correlation with the backscatter; on the other hand, it is simultaneously designed to increase the output SIR (which enhances the useful component with respect to the backscattering term): hence, we expect the correlation with $\widetilde{\boldsymbol{P}}_\ell \boldsymbol{S}\boldsymbol{x}$ (which somehow encompasses the backscatter) to be non-null but yet sufficiently limited. Similarly, due to the independence $\boldsymbol{x}$ and $\boldsymbol{n}$, we reasonably guess that the correlation between $\boldsymbol{c}_n$ and $\widetilde{\boldsymbol{P}}_\ell \, \boldsymbol{n}$ is quite small. Of course, it is not our intention to claim that this statement holds true for all the possible design approaches, since it clearly depends on the intrapulse modulation technique adopted. Still, our simulations demonstrate the validity of our intuition.

[6] In formulating $\mathcal{P}_2$, we have assigned the same weight ζ_2 to the last $(MN-1)$ components of the vectorial objective function. This choice is only made for the of sake of simplicity and based on the assumption that, without any knowledge on the dominant space, an interceptor should reasonably give equal confidence to all the presumed non-dominant spaces $\widetilde{\boldsymbol{P}}_\ell$.

Algorithm 1 Waveforms design via solution of $\mathcal{P}_2$.

Input: L, M, $\boldsymbol{S}$, $\boldsymbol{U}_{k-1}$, $\widehat{\boldsymbol{W}}$, $\boldsymbol{d}_{0,k}$, ϵ, γ;
Output: An optimal solution $\boldsymbol{c}_k^\star$ to problem $\mathcal{P}_2$;

1) solve problem $\mathcal{P}_4$, getting a solution $\boldsymbol{X}_{\rm sdr}$;
2) find $\boldsymbol{x}^\star = \mathcal{D}\left(\boldsymbol{X}_{\rm sdr}, \boldsymbol{Q}_0, \boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{Q}_3\right)$; let $\boldsymbol{x}^\star = \left[(\boldsymbol{z}^\star)^T \quad y^\star\right]^T$;
3) set $\widehat{\boldsymbol{c}}_k^\star = \boldsymbol{z}^\star / y^\star$.
4) return $\boldsymbol{c}_k^\star = \boldsymbol{U}_{k-1}\widehat{\boldsymbol{c}}_k^\star$.

can be shown to be equivalent to the quadratically-constrained quadratic-programming reformulation:

$$\mathcal{P}_3 \triangleq \begin{cases} \max\limits_{\widehat{\boldsymbol{c}}_k, t} & \mathrm{tr}\left(\boldsymbol{Q}_0\,\boldsymbol{X}\right) \\ \text{s.t.} & \mathrm{tr}\left(\boldsymbol{Q}_1\,\boldsymbol{X}\right) \geq 0, \quad \mathrm{tr}\left(\boldsymbol{Q}_2\,\boldsymbol{X}\right) = 1, \\ & \mathrm{tr}\left(\boldsymbol{Q}_3\,\boldsymbol{X}\right) = 1, \quad \boldsymbol{X} \triangleq (\boldsymbol{c}_{k,e}\,\boldsymbol{c}_{k,e}^\dagger), \end{cases} \tag{7}$$

where $\boldsymbol{c}_{k,e} \triangleq \left[\widehat{\boldsymbol{c}}_k^T \quad t\right]^T$ and the matrices $\boldsymbol{Q}_i$ are defined as

$$\boldsymbol{Q}_0 \triangleq \begin{bmatrix} \boldsymbol{A}_0 & \boldsymbol{0} \\ \boldsymbol{0} & 0 \end{bmatrix}, \quad \boldsymbol{Q}_1 \triangleq \begin{bmatrix} -\boldsymbol{A}_1 & \boldsymbol{r}_1 \\ \boldsymbol{r}_1^\dagger & \boldsymbol{B}_1 \end{bmatrix}, \tag{8}$$

$$\boldsymbol{Q}_2 \triangleq \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{0} & 0 \end{bmatrix}, \quad \boldsymbol{Q}_3 \triangleq \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & 1 \end{bmatrix}. \tag{9}$$

with $\boldsymbol{A}_0 \triangleq (\boldsymbol{U}_{k-1}^\dagger \boldsymbol{T}(\gamma) \boldsymbol{U}_{k-1})$, $\boldsymbol{A}_1 \triangleq (\boldsymbol{U}_{k-1}^\dagger \boldsymbol{K} \boldsymbol{U}_{k-1})$, $\boldsymbol{B}_1 \triangleq (\epsilon - \boldsymbol{d}_{0,k}^\dagger \boldsymbol{K}\, \boldsymbol{d}_{0,k})$ and $\boldsymbol{r}_1 \triangleq (\boldsymbol{U}_{k-1}^\dagger \boldsymbol{K}\, \boldsymbol{d}_{0,k})$. Also, $\boldsymbol{T}(\gamma) \triangleq (\boldsymbol{R} - \gamma \widetilde{\boldsymbol{P}})$, $\gamma \triangleq (\gamma_2/\gamma_1)$ and $\boldsymbol{K} \triangleq (\widehat{\boldsymbol{W}}^\dagger \widehat{\boldsymbol{W}})$. Given Eq. (7), an optimal solution $\boldsymbol{X}^\star$ to $\mathcal{P}_3$ can be found in two (efficient) steps. The first step involves the solution of a semidefinite programming problem [8], which is the relaxation of $\mathcal{P}_3$ obtained by dropping the rank-one constraint on $\boldsymbol{X}$:

$$\mathcal{P}_4 \triangleq \begin{cases} \max\limits_{\boldsymbol{X}} & \mathrm{tr}\left(\boldsymbol{Q}_0\,\boldsymbol{X}\right) \\ \text{s.t.} & \mathrm{tr}\left(\boldsymbol{Q}_1\,\boldsymbol{X}\right) \geq 0,\ \mathrm{tr}\left(\boldsymbol{Q}_2\,\boldsymbol{X}\right) = 1\,, \\ & \mathrm{tr}\left(\boldsymbol{Q}_3\,\boldsymbol{X}\right) = 1,\ \boldsymbol{X} \succeq \boldsymbol{0}\,. \end{cases} \tag{10}$$

The second step consists in the application of a rank-one matrix decomposition theorem [10, Thm. 2.3] in order to obtain a vector $\boldsymbol{x}^\star = \left[(\boldsymbol{z}^\star)^T \quad y^\star\right]^T$ such that $\boldsymbol{X}^\star = \boldsymbol{x}^\star(\boldsymbol{x}^\star)^\dagger$. This operation is denoted as $\mathcal{D}\left(\boldsymbol{X}_{\rm sdr}, \boldsymbol{Q}_0, \boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{Q}_3\right)$, with $\boldsymbol{X}_{\rm sdr}$ denoting the solution to $\mathcal{P}_4$. Therefore, an optimal solution to problem $\mathcal{P}_2$ is consequently found as $\boldsymbol{c}_k^\star = \boldsymbol{U}_{k-1}\widehat{\boldsymbol{c}}_k^\star$ and $\widehat{\boldsymbol{c}}_k^\star = \boldsymbol{z}^\star / y^\star$.

We underline that above theorem can be applied since $\mathcal{P}_4$ and its dual are *solvable*[7] [10]. Finally**,** in **Algorithm 1** we summarize the procedure leading to an optimal solution to $\mathcal{P}_2$.

V. Performance Analysis

We assess performance of $\boldsymbol{c}_k^{\textbf{Alg1}}$, $k = 1, \ldots, K$, produced via **Alg. 1**, in terms of SER and Intercept Metric (IM).

We consider a unitary norm LFM pulse as the incident radar signal, with a duration $T = 133$ μs, bandwidth $B = 750$ kHz, and a chirp rate $K_s = (\frac{750}{133} \times 10^9)$ Hz/s; when sampled at Nyquist rate f_s, we obtain $s(n) = (1/\sqrt{N})\, e^{j 2\pi \frac{K_s}{2}((n-1)/f_s)^2}$, $n = 1, \ldots, N = 100$. The signal is oversampled by the tag with a factor $M = 2$, resulting in 200 samples. The number of waveforms (symbols) is set to $K = 4$ (2 bits). Finally, we set $L = 100$ and, with reference to similarity in Eq. (3), $\widehat{N} = 8\,MN$ and $F = 806$, respectively.

In our comparison we consider the following alternative design techniques: (i) the "Eigenvectors-As-Waveform" (EAW) approach [6], ($\boldsymbol{c}_k^{\rm EAW} = \boldsymbol{v}_k$, $k = 1, \ldots, K$, i.e. the K eigenvectors corresponding to the smallest K eigenvalues are used as the symbols). (ii) The DP approach of [6], where the K waveforms are sequentially designed by "projecting away" from the (accumulated) whole dominant space a set of pseudo-random vectors $\boldsymbol{d}_k^{\rm DP} \in \mathbb{C}^{MN \times 1}$, $k = 1, \ldots, K$ ($\boldsymbol{c}_k^{\rm DP} = \boldsymbol{P}_{k-1}\boldsymbol{d}_k^{\rm DP}$, $k = 1, \ldots, K$, where $\boldsymbol{d}_k^{\rm DP} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I})$ and $\boldsymbol{c}_k^{\rm DP}$ is scaled to have unitary norm). (iii) The *minimum LPI* approach, i.e. the K waveforms $\boldsymbol{c}_k^{\rm LPI}$ are an optimal solution to $\mathcal{P}_2$ when $\gamma = 0$. As to the filtering strategy, following [6], we assume that the intender receiver employs ($k = 1, \ldots, K$): (i) either a matched filter (MF), i.e., $\boldsymbol{w}_k = \boldsymbol{c}_k$ or (ii) a decorrelating filter (DF)[8], i.e., $\boldsymbol{w}_k = (\boldsymbol{C}\boldsymbol{C}^\dagger)^{-1}\boldsymbol{c}_k$, where $\boldsymbol{C} \triangleq [\boldsymbol{S}\, \boldsymbol{c}_1\, \ldots\, \boldsymbol{c}_K]$. Given the received signal $\boldsymbol{y}_r$, the symbol estimate is obtained as $\overline{\boldsymbol{c}} \triangleq \arg \max\limits_{\{\boldsymbol{c}_1, \ldots \boldsymbol{c}_K\}} |\boldsymbol{w}_k^\dagger\, \boldsymbol{y}_r|$.

SER and IM (Eq. (4)) curves are obtained by designing 10 sets of K symbols[9]. For each set the corresponding SER (10^5 instances) and IM (200 instances) are evaluated. In the latter case we assume that $\boldsymbol{c}_1$ is transmitted[10] (i.e. $\boldsymbol{y}_{1r}$ is considered). Then, the SER and IM are averaged over the total number of available sets. We consider three different values of SIR (i.e., SIR $\in \{-40, -35, -30\}$ dB), assuming an SNR $\in [-15, 0]$ dB for the SER. Differently, the results for IM are shown for (SIR,SNR) $= (-35, -10)$ dB.

In Figs. 2-3-4, we analyze the SER vs. SNR for $\boldsymbol{c}_k^{\textbf{Alg1}}$, for different values of ϵ and γ ($\gamma \in \{0, 2, 2.3\}$), when either a MF or a DF is employed, and compare the results with those achieved by $\boldsymbol{c}_k^{\rm LPI}$ (Figs. 1-2-3-4), $\boldsymbol{c}_k^{\rm EAW}$ (Figs. 1-2) and $\boldsymbol{c}_k^{\rm DP}$ (Figs. 3-4). More specifically, Figs. 1-a1, 1-b1, 2-c1, and 2-d1 refer to MF case, while Figs. 1-a2, 1-b2, 2-c2, and 2-d2 refer to DF case, for $\epsilon = 0.01$, 0.05, 0.1, and 0.5, respectively. The same structure has been adopted for the plots in Figs. 3-4.

A first inspection of the curves obtained with $\boldsymbol{c}_k^{\textbf{Alg1}}$ reveals that lower SER is achieved with small values of γ; this follows from mediative role of the Pareto weight, which enhances the *reliability* of the communication over its *covertness* as γ is decreased; hence, we expect higher interception probabilities to be swapped for lower SER values. Indeed, as ϵ increases (i.e. the similarity constraint is loosen and additional DOFs are available), the cases $\gamma \in \{0, 2\}$ (resp. $\gamma = 2.3$) achieve SER improvements (resp. experiences partial loss of SER). This is

[7] The proof is rather tedious and omitted for the sake of brevity.

[8] Hereinafter we do not report the performance for the filter which maximizes the SIR in Eq. (2), i.e. $\boldsymbol{w}_k = (\boldsymbol{S}\boldsymbol{S}^\dagger)^{-1}\boldsymbol{c}_k$, since *nearly identical* SER values to the DF has been observed numerically in the considered scenarios.

[9] Different sets of K symbols correspond to different instances of the random vectors $\boldsymbol{b}_k$, $\boldsymbol{d}_k^{\rm DP}$, and $\boldsymbol{d}_k$, respectively for WC, DP, and **Alg. 1** approaches. By iterating the experiment over a multitude of possible sets, we aim at reducing the variation of SER and IM with respect to set selection.

[10] Indeed, it has been observed numerically that considering other waveforms in the set leads to similar behaviours in terms of intercept curves.

observed when either DF or MF is employed (with DF outperforming MF due to its interference cancellation capabilities). On the other hand, when ϵ is taken to be very small, both $\boldsymbol{c}_k^{\mathbf{Alg1}}$ and $\boldsymbol{c}_k^{\mathrm{LPI}}$ collapse to DP performance, since a strict similarity to noise-like waveforms is enforced and symbols are designed to comply with the constraints $\boldsymbol{P}_{k-1}^{\perp}\boldsymbol{c}_k = \mathbf{0}$, $k = 1, \dots K$.

Also, SER for EAW is identical with both MF and DF, and is lower than that achieved with Alg. 1. Indeed $\boldsymbol{c}_k^{\mathrm{EAW}}$ use the eigenvectors possessing the least correlation with the backscatter; hence, they are more easily "pulled out" from the received signal than $\boldsymbol{c}_k^{\mathbf{Alg1}}$ (which are instead designed to exhibit a partial correlation with the backscatter). Also, since each $\boldsymbol{c}_k^{\mathrm{EAW}}$ is associated to a distinct eigenvector of $\boldsymbol{S}\boldsymbol{S}^{\dagger}$, EAW does not get any profit from the use of DF (i.e. $\boldsymbol{c}_k^{\mathrm{EAW}}$ already provide interference cancellation). On the other hand, when $\gamma \in \{0, 2\}$, Alg. 1 is comparable with, or totally outperforms, DP strategy in terms of reliability. This result can be easily explained noticing that, for the above values of γ, the SIR levels attained with the codes $\boldsymbol{c}_k^{\mathbf{Alg1}}$ are still higher than those achieved by $\boldsymbol{c}_k^{\mathrm{DP}}$. Then, even if the two techniques possess a partial correlation with the backscatter (in spite of EAW), our approach still allows for easier extraction of the embedded symbol for the intended receiver. When $\gamma = 2.3$, we experience a SER loss with respect to EAW and DP; this loss is clearly due to the existing trade-off between the SER and the covertness capability of the tag (the loss will be payed off with lower probabilities of interception). Finally, we observe that, when a MF is adopted, $\boldsymbol{c}_k^{\mathrm{LPI}}$ achieves similar SER to $\boldsymbol{c}_k^{\mathbf{Alg1}}$ for $\gamma = 2.3$; different situation occurs, instead, with DF.

In Figs. 5-6, we show the IM of $\boldsymbol{c}_k^{\mathbf{Alg1}}$, for $\epsilon \in \{0.01, 0.05, 0.1, 0.5\}$ and $\gamma \in \{0, 2, 2.3\}$, and compare it with $\boldsymbol{c}_k^{\mathrm{LPI}}$ (Figs. 5-6), $\boldsymbol{c}_k^{\mathrm{EAW}}$ (Figs. 5), and $\boldsymbol{c}_k^{\mathrm{DP}}$ (Figs. 6). Higher values of γ correspond to lower correlation values for waveform 1 obtained with Alg. 1, and the IM of $\boldsymbol{c}^{\mathrm{LPI}}$ in this case is approached, which denotes the actual lower bound (see e.g.. Fig. 5-a). Also, our approach surpasses EAW and DP, by ensuring lower correlation when γ is sufficiently big. Differently, covertness "worsen" for smaller γ, since more importance is given to SIR objective (however the IM is quite low, thus a covert conversation is still virtually possible). By increasing ϵ, this trend is more apparent (cf. Figs. 5). In particular, when $\gamma = 2.3$, $\boldsymbol{c}_k^{\mathbf{Alg1}}$ ensures a more covert transmission; differently, the reverse effect is displayed for $\gamma \in \{0, 2\}$, where slightly higher correlations are obtained for all the waveforms. Also, when γ is kept limited, Alg. 1 outperforms EAW for all the settings of ϵ; however, it displays a behavior comparable with that of DP only when $\epsilon < 0.1$, once again displaying the conflicting nature of the two objectives. Nevertheless, by properly adjusting both ϵ and γ, Alg. 1 proves to be better than, or at least comparable with, the EAW and the DP, in terms of covertness and reliability.

VI. Conclusions

We have focused on intrapulse REM communication, where the incident radar illumination is remodulated, through an RF tag, into one of possible K orthogonal symbols. Waveforms have been designed according to jointly constrained SIR maximization (link reliability) maximization and IM minimization (link covertness). The problem has been cast into a constrained multi-objective optimization and codes have been constructed as Pareto-optimal points through scalarization. The proposed algorithm was compared to state of the art in terms of SER and IM, thus showing its capability to suitably trade-off the reliability and the covertness of the established link.

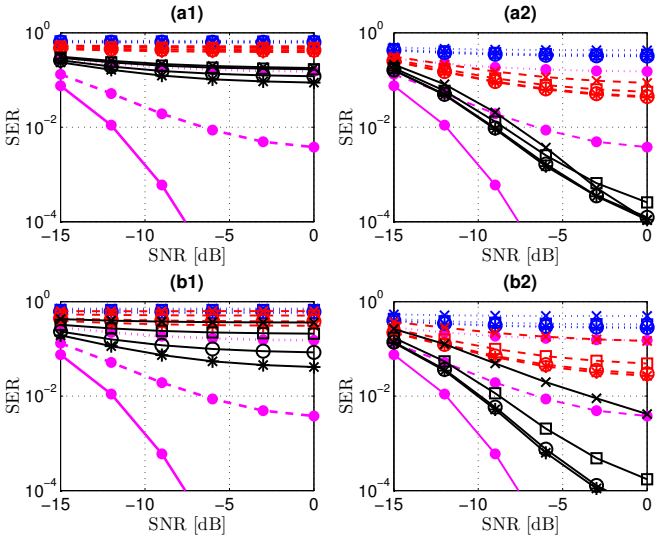

Fig. 1. SER vs SNR (dB); SIR $\in \{-30, -35, -40\}$ dB (solid, dashed and dotted lines). EAW: ●-markers; **Alg. 1**, $\gamma = 0$: ∗-markers; **Alg. 1**, $\gamma = 2$: ○-markers; **Alg. 1**, $\gamma = 2.3$: □-markers; **min. LPI**: x-markers. **a1)** $\epsilon = .01$, MF; **a2)** $\epsilon = .01$, DF; **b1)** $\epsilon = .05$, MF; **b2)** $\epsilon = .05$, DF.

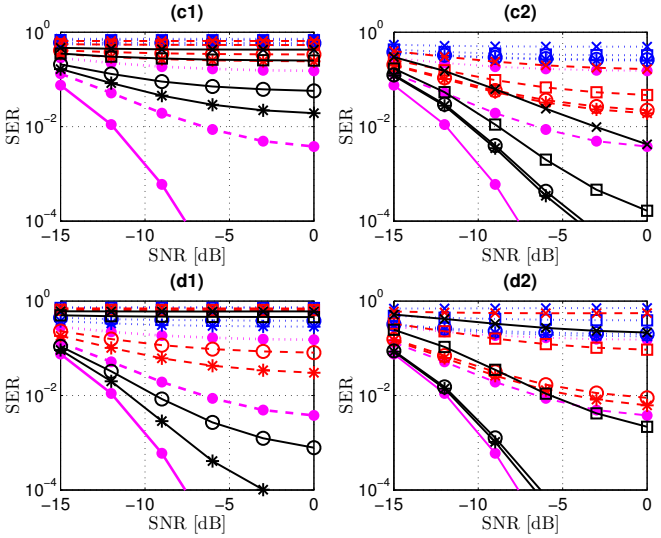

Fig. 2. SER vs SNR (dB); SIR $\in \{-30, -35, -40\}$ dB (solid, dashed and dotted lines). EAW: ●-markers; **Alg. 1**, $\gamma = 0$: ∗-markers; **Alg. 1**, $\gamma = 2$: ○-markers; **Alg. 1**, $\gamma = 2.3$: □-markers; **min. LPI**: x-markers. **c1)** $\epsilon = .1$, MF; **c2)** $\epsilon = .1$, DF; **d1)** $\epsilon = .5$, MF; **d2)** $\epsilon = .5$, DF.

References

[1] Z. Hijaz and V. S. Frost, "Exploiting OFDM systems for covert communication," in *IEEE Military Communications Conference (MILCOM)*, 2010, pp. 2149–2155.

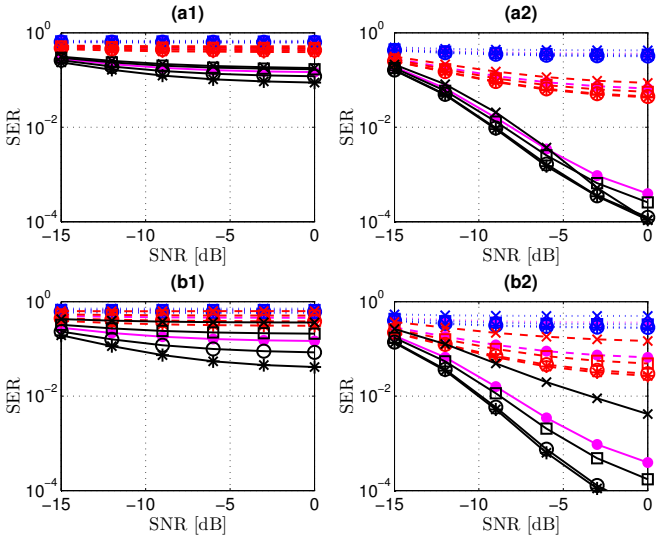

Fig. 3. SER vs SNR (dB); SIR $= \{-30, -35, -40\}$ dB (solid, dashed and dotted lines). DP: ●-markers; **Alg. 1**, $\gamma = 0$: $*$-markers; **Alg. 1**, $\gamma = 2$: ○-markers; **Alg. 1**, $\gamma = 2.3$: □-markers; **min. LPI**: x-markers. **a1)** $\epsilon = .01$, MF; **a2)** $\epsilon = .01$, DF; **b1)** $\epsilon = .05$, MF; **b2)** $\epsilon = .05$, DF.

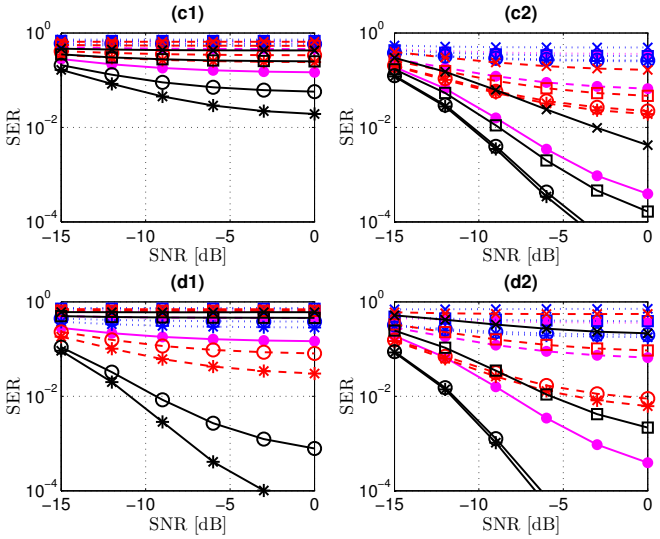

Fig. 4. SER vs SNR (dB); SIR $\in \{-30, -35, -40\}$ dB (solid, dashed and dotted lines). DP: ●-markers; **Alg. 1**, $\gamma = 0$: $*$-markers; **Alg. 1**, $\gamma = 2$: ○-markers; **Alg. 1**, $\gamma = 2.3$: □-markers; **min. LPI**: x-markers. **c1)** $\epsilon = .1$, MF; **c2)** $\epsilon = .1$, DF; **d1)** $\epsilon = .5$, MF; **d2)** $\epsilon = .5$, DF.

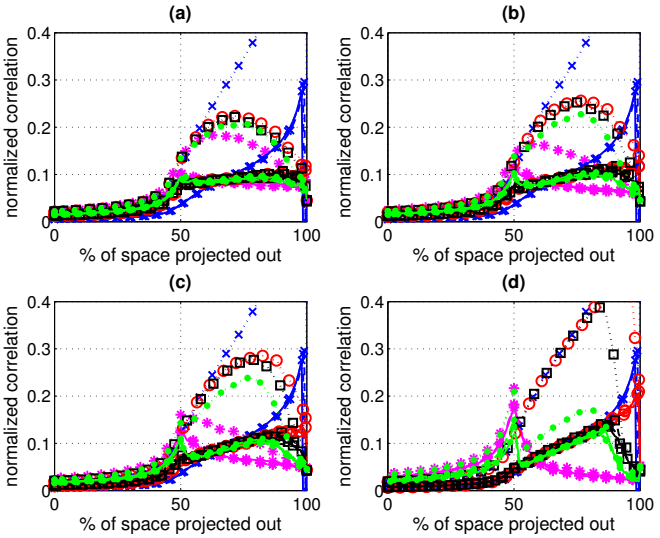

Fig. 5. IM - Wav-1 (dotted lines); Wav-2 (dashed lines); Wav-3 (dot-dashed lines); Wav-4 (solid lines). EAW: blue x-markers; **Alg. 1**, $\gamma = 0$: red ○-markers; **Alg. 1**, $\gamma = 2$: black □-markers; **Alg. 1**, $\gamma = 2.3$: green ●-markers; **min. LPI**: magenta $*$-markers. a) $\epsilon = .01$; b) $\epsilon = .05$; c) $\epsilon = .1$; d) $\epsilon = .5$.

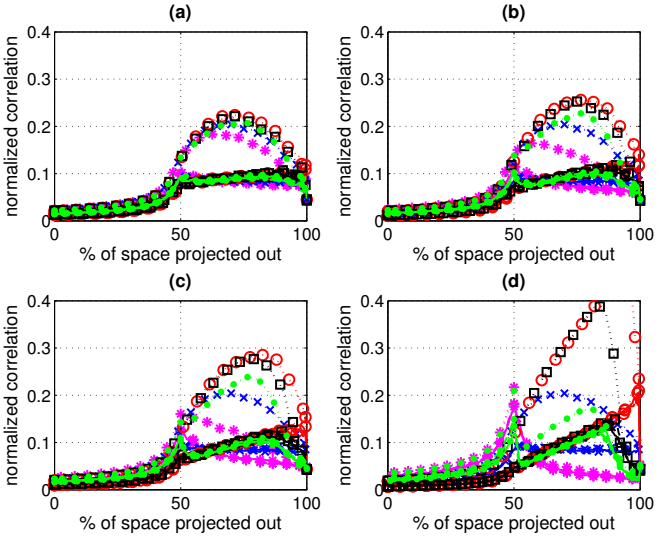

Fig. 6. IM - Wav-1 (dotted lines); Wav-2 (dashed lines); Wav-3 (dot-dashed lines); Wav-4 (solid lines). DP: blue x-markers; **Alg. 1**, $\gamma = 0$: red ○-markers; **Alg. 1**, $\gamma = 2$: black □-markers; **Alg. 1**, $\gamma = 2.3$: green ●-markers; **min. LPI**: magenta $*$-markers. a) $\epsilon = .01$; b) $\epsilon = .05$; c) $\epsilon = .1$; d) $\epsilon = .5$.

[2] D. Hounam and K.-H. Wagel, "A technique for the identification and localization of SAR targets using encoding transponders," *IEEE Trans. Geosci. Remote Sens.*, vol. 39, no. 1, pp. 3–7, Jan. 2001.

[3] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, ser. Communications engineering series. Elsevier Science, 2007.

[4] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, Oct. 1948.

[5] R. M. Axline, G. R. Sloan, and R. E. Spalding, "Radar transponder apparatus and signal processing technique," Jan. 1996, US Patent 5,486,830.

[6] 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.

[7] S. D. Blunt, J. G. Metcalf, C. R. Biggs, and E. Perrins, "Performance characteristics and metrics for intra-pulse radar-embedded communication," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2057–2066, Dec. 2011.

[8] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[9] A. De Maio, M. Piezzo, A. Farina, and M. Wicks, "Pareto-optimal radar waveform design," *IET, Radar, Sonar & Navigation*, vol. 5, no. 4, pp. 473–482, Apr. 2011.

[10] W. Ai, Y. Huang, and S. Zhang, "New results on Hermitian matrix rank-one decomposition," *Mathematical Programming*, vol. 128, no. 1-2, pp. 253–283, 2011.

[11] A. De Maio, Y. Huang, D. P. Palomar, S. Zhang, and A. Farina, "Fractional QCQP with applications in ML steering direction estimation for radar detection," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 172–185, Jan. 2011.

[12] J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proc. IEEE*, vol. 57, no. 8, pp. 1408–1418, Aug. 1969.