Parameter Encoding for ECRB Minimization in the Presence of Jamming

Cuneyd Ozturk, Cagri Goken, and Sinan Gezici

***Abstract*—The optimal encoding of a scalar parameter is performed in the presence of jamming based on an estimation theoretic criterion. Namely, the aim is to obtain the optimal encoding function at the transmitter that minimizes the expectation of the conditional Cramér-Rao bound (ECRB) at the receiver when the jammer has access to the parameter and alters the received signal by sending an encoded version of the parameter. Via calculus of variations, the optimal encoding function at the transmitter is characterized explicitly, and an algorithm is proposed to calculate it. Numerical examples demonstrate benefits of the proposed optimal encoding approach.**

***Index Terms*— Parameter estimation, jamming, Cramér-Rao bound (CRB), optimization.**

I. Introduction

Communication systems can be vulnerable to various types of malicious attacks such as eavesdropping and jamming [1] (and references therein). While eavesdroppers aim to infer messages between transmitters and receivers, jammers try to disrupt communications among devices in a given network.

In the presence of eavesdropping, secure transmission of scalar and vector parameters is investigated in an estimation theoretic framework in [2]–[4]. In particular, the optimal encoding strategy for a scalar parameter is investigated in [2] by minimizing the expectation of the conditional Cramér-Rao bound (ECRB) at the intended receiver under a constraint on the mean-squared error (MSE) at the eavesdropper. In [4], the optimal encoding strategy for estimation theoretic security is analyzed, where the transmitter is allowed to perform randomization between two one-to-one and continuous encoding functions and the eavesdropper is fully aware of the encoding strategy at the transmitter.

Among various studies on jamming of communication systems, [5]–[9] formulate the problem of transmitting a parameter to a receiver under jamming attacks as a zero-sum game, and analyze optimal policies of the transmitter, receiver and jammer under various scenarios. Specifically, [5] investigates the problem of transmitting a sequence of independent and identically distributed Gaussian random variables through a Gaussian memoryless channel in the presence of an intelligent jammer. The optimal policies of the receiver and the jammer are determined, and the uniqueness of the solution is proved. In [6], by relaxing the Gaussian source and channel assumptions, optimal policies of the transmitter, jammer and receiver are obtained. The work in [6] is extended to the zero-delay jamming setting in [7].

In this letter, an optimal parameter encoding problem is proposed for ECRB minimization in the presence of a jammer. A scalar parameter is transmitted over a noisy and flat-fading channel to a receiver, and the jammer, which has access to the parameter as in [9], sends an encoded version of the parameter to the receiver for degrading estimation performance. Considering a generic prior distribution for the parameter, we formulate the problem of determining the optimal encoding strategy at the transmitter that minimizes the ECRB at the receiver in the presence of jamming for the first time in the literature. The optimal encoding function of the transmitter is determined among the class of differentiable and monotone increasing functions based on variational analyses (Proposition 1), which leads to nonlinear encoding functions in general (cf. [6]). To determine the optimal encoding function based on the theoretical results, an algorithm is proposed (Algorithm 1). In addition, the problem is analyzed for the general case by removing the monotonicity assumption over the encoding function of the transmitter (Proposition 2).

C. Ozturk and S. Gezici are with the Dept. of Electrical and Electronics Engineering, Bilkent University, Bilkent, Ankara 06800, Turkey, Tel: +90 (312) 290-3139, e-mails: {cuneyd,gezici}@ee.bilkent.edu.tr. C. Goken is with the Dept. of Communications and Information Technologies, Aselsan Inc., Ankara 06800, Turkey, e-mail: cgoken@aselsan.com.tr.

II. System Model and Problem Formulation

A transmitter sends a scalar parameter $\theta \in \Lambda$ to a receiver over a noisy and flat-fading channel in the presence of a jammer. The jammer has access to parameter θ (as in [9]), encodes it via a differentiable, real valued function $g : \Lambda \rightarrow \Gamma$, and sends the encoded parameter to the receiver. The aim is to perform accurate estimation of parameter θ at the receiver in the presence of jamming. To this aim, parameter θ is encoded by a differentiable, real valued function $f : \Lambda \rightarrow \Upsilon$ at the transmitter. Accordingly, the received signal Y becomes

$$Y = h_T f(\theta) + h_J g(\theta) + N \tag{1}$$

where h_T and h_J denote the channel fading coefficients between the transmitter and the receiver and between the jammer and the receiver, respectively, N is the noise term, which is modeled as a zero-mean Gaussian random variable with a known variance denoted by σ^2, and N and θ are assumed to be independent.

The prior information on parameter θ is represented by a probability density function (PDF) denoted by $w(\theta)$ for $\theta \in \Lambda$. Also, the channel coefficients are supposed to be known by the transmitter and the receiver. In addition, it is assumed that the receiver knows both mappings $f(\cdot)$ and $g(\cdot)$, and the transmitter has the knowledge of $g(\cdot)$. The motivation and justification for these assumptions are as follows: (i) In a sensor network in which jamming is caused by another transmitter in the same network unintentionally, these assumptions can hold. (ii) Under these assumptions, we obtain an upper bound on the estimation performance at the receiver in the presence of jamming. (This bound becomes tight when the transmitter is smart and the jammer is dummy.) (iii) The analysis under these assumptions leads to the best response strategy of the transmitter for a given jammer strategy, which forms an important step towards a game theoretic analysis.

To quantify the estimation accuracy at the receiver, the ECRB is employed as a performance metric since it converges to the MSE of the maximum a-posteriori probability (MAP) estimator in the high SNR regime [10], does not depend on specific estimator structures, and facilitates theoretical analyses (leading to explicit expressions for the optimal encoder function at the transmitter). The ECRB is defined as the

expectation of the conditional Cramér-Rao bound [10] and calculated as follows: $\mathbb{E}_\theta\{\mathcal{I}(\theta)^{-1}\} = \int_\Lambda w(\theta)\frac{1}{\mathcal{I}(\theta)}\,d\theta$, where $\mathcal{I}(\theta)$ denotes the Fisher information, i.e.,

$$\mathcal{I}(\theta) = \int \left(\frac{\partial \log p_{Y|\theta}(y)}{\partial \theta}\right)^2 p_{Y|\theta}(y)\,dy \tag{2}$$

with $p_{Y|\theta}(y)$ representing the conditional PDF of Y for a given value of θ. For the system model in (1), $p_{Y|\theta}(y)$ is expressed as $p_{Y|\theta}(y) = (2\pi\sigma^2)^{-0.5}\exp\left(-(y-h_T f(\theta)-h_J g(\theta))^2/(2\sigma^2)\right)$. Then, the Fisher information in (2) can be obtained as

$$\mathcal{I}(\theta) = \left(h_T f'(\theta) + h_J g'(\theta)\right)^2/\sigma^2 \tag{3}$$

where $f'(\theta)$ and $g'(\theta)$ denote the derivatives of $f(\theta)$ and $g(\theta)$, respectively.[1] Based on a reasoning similar to that in [2], the ranges of θ, $g(\theta)$, and $f(\theta)$ are modeled as $\Lambda = [a,b]$, $\Gamma = [k,l]$, and $\Upsilon = [c,d]$, respectively, for some $a,b,c,d,k,l \in \mathbb{R}$. In particular, for $\theta \in [a,b]$, $f(\cdot)$ must be a differentiable function that satisfies $c \le f(\theta) \le d$. By setting lower and upper limits on $f(\theta)$, we effectively impose a peak power constraint on the transmitted signal, which in turn limits the average transmit power, as well. Hence, for given $g(\cdot)$, we propose the following optimization problem for parameter encoding at the transmitter:

$$\min_{f} \quad \int_a^b w(\theta)\frac{\sigma^2}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^2}\,d\theta \tag{4a}$$

$$\text{subject to} \quad c \le f(\theta) \le d\,,\ \forall\,\theta \in [a,b] \tag{4b}$$

That is, the aim is to obtain the optimal encoding function at the transmitter that minimizes the ECRB at the receiver for a given jammer and under the constraint in (4b).

III. Optimal Encoding Function at Transmitter

A. f is strictly monotone increasing

If f is strictly monotone increasing, $f'(\theta) > 0$ for each $\theta \in [a,b]$. By adding the constraint $f'(\theta) > 0$ to (4), we formulate the proposed optimization problem as follows:

$$\min_{f} \quad \int_a^b w(\theta)\left(h_T f'(\theta) + h_J g'(\theta)\right)^{-2}\,d\theta \tag{5a}$$

$$\text{subject to} \quad c \le f(\theta) \le d\,,\ \forall\,\theta \in [a,b] \tag{5b}$$

$$f'(\theta) > 0,\ \forall\,\theta \in [a,b] \tag{5c}$$

where the constant term σ^2 is removed from the objective function for notational convenience. It is noted that the objective function in (5a) remains constant if we shift all $f(\theta)$ values by the same scalar number. Due to the monotonicity of $f(\cdot)$, if we ensure that $f(b) - f(a) \le d - c$, we can find the optimal $f(\cdot)$ up to a constant. We can then adjust this constant term such that $f(\cdot)$ remains in $[c,d]$. Another way of writing $f(b) - f(a) \le d - c$ is $\int_a^b f'(\theta)\,d\theta \le d - c$. Hence, by replacing (5b) with $\int_a^b f'(\theta)\,d\theta \le d - c$, we can concentrate on the following problem:

$$\min_{f} \quad \int_a^b w(\theta)\left(h_T f'(\theta) + h_J g'(\theta)\right)^{-2}\,d\theta \tag{6a}$$

$$\text{subject to} \quad \int_a^b f'(\theta)\,d\theta \le d - c \tag{6b}$$

$$f'(\theta) > 0,\ \forall\,\theta \in [a,b] \tag{6c}$$

Next, we replace the constraint in (6c) by the equality constraint $f'(\theta) = \epsilon + \mu^2(\theta)$ for a sufficiently small number $\epsilon > 0$ and for some function $\mu(\cdot)$. We also define a function $t(\cdot)$ such that $\int_a^b f'(\theta) + t^2(\theta)\,d\theta = d - c$. Hence, we can reformulate (6) as

$$\min_{f,t,\mu} \quad \int_a^b w(\theta)\left(h_T f'(\theta) + h_J g'(\theta)\right)^{-2}\,d\theta \tag{7a}$$

$$\text{subject to} \quad \int_a^b f'(\theta) + t^2(\theta)\,d\theta = d - c \tag{7b}$$

$$f'(\theta) = \mu^2(\theta) + \epsilon\,,\ \forall\,\theta \in [a,b] \tag{7c}$$

The following proposition characterizes the solution of (7).

Proposition 1: A solution to (7) admits one of the following two alternative forms:

- either $f'(\theta) = \epsilon$ for all $\theta \in [a,b]$,
- or, there exists $\emptyset \subseteq S \subseteq [a,b]$ such that

$$f'(\theta) = \epsilon, \text{ if } \theta \in S, \tag{8}$$

$$f'(\theta) = \frac{(\tilde{K}w(\theta))^{1/3} - h_J g'(\theta)}{h_T} > 0, \text{ if } \theta \in S^c, \tag{9}$$

where $S^c = [a,b] \setminus S$ and $\tilde{K}$ is chosen such that

$$\int_a^b f'(\theta)\,d\theta = d - c. \tag{10}$$

Proof: Let $H(\theta, f', \mu, t, \gamma, \lambda)$ be given by

$$H(\theta, f', \mu, t, \gamma, \lambda) = w(\theta)\left(h_T f'(\theta) + h_J g'(\theta)\right)^{-2} + \lambda\left(f'(\theta) + t^2(\theta)\right) + \gamma(\theta)\left(\mu^2(\theta) + \epsilon - f'(\theta)\right). \tag{11}$$

where λ and $\gamma(\theta)$ are Lagrange multipliers. Finding the extremals of (7) is equivalent to finding the extremals of $\mathcal{H}[f', \mu, t, \gamma]$, where

$$\mathcal{H}[f', \mu, t, \gamma] = \int_a^b H(\theta, f', \mu, t, \gamma, \lambda)\,d\theta\,. \tag{12}$$

From (11), Euler-Lagrange equations [11, p. 36] lead to[2]

$$\frac{\partial H}{\partial f} - \frac{d}{d\theta}\frac{\partial H}{\partial f'} = -\frac{d}{d\theta}\Bigg(-\frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3} + \lambda - \gamma(\theta)\Bigg) = 0 \tag{13}$$

$$\frac{\partial H}{\partial \mu} - \frac{d}{d\theta}\frac{\partial H}{\partial \mu'} = 2\gamma(\theta)\mu(\theta) = 0 \tag{14}$$

$$\frac{\partial H}{\partial \gamma} - \frac{d}{d\theta}\frac{\partial H}{\partial \gamma'} = \mu^2(\theta) + \epsilon - f'(\theta) = 0 \tag{15}$$

$$\frac{\partial H}{\partial t} - \frac{d}{d\theta}\frac{\partial H}{\partial t'} = 2\lambda t(\theta) = 0. \tag{16}$$

(13) implies that there exists a constant $K \in \mathbb{R}$ such that

$$\frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3} + \gamma(\theta) = K + \lambda\,. \tag{17}$$

Multiplying both sides of (17) with $\mu(\theta)$ and using (14) and

[1] Intuitively, the jammer would like to cancel the transmitted signal to set the Fisher information to zero. However, it does not know the encoder at the transmitter and can design its encoder based on previous experience. When the transmitter employs a differential encoding strategy for ease of implementation, the jammer can also be modeled to employ a differential encoding strategy for cancellation purposes.

[2] The partial derivative notation is used for derivatives with respect to functions; otherwise, the regular derivative notation is employed.

(15), we obtain

$$\frac{2h_T w(\theta)\mu(\theta)}{\left(h_T\mu^2(\theta)+h_T\epsilon+h_J g'(\theta)\right)^3}=(K+\lambda)\mu(\theta). \tag{18}$$

It is noted from (11) that the following relations hold: $H_f=\frac{\partial H}{\partial f}=0$, $H_{ff'}=\frac{\partial^2 H}{\partial f\partial f'}=0$, $H_{ff}=\frac{\partial^2 H}{\partial f^2}=0$, and $H_{f'f'}=\frac{\partial^2 H}{\partial f'^2}=\frac{6h_T^2 w(\theta)}{(h_T f'(\theta)+h_J g'(\theta))^4}>0$. Then, the second variation $\delta^2\mathcal{H}|_f(\eta)$ is given by

$$\begin{aligned}\delta^2\mathcal{H}|_f(\eta)&=\frac{1}{2}\int_a^b\left[\eta^2\left(H_{ff}-\frac{d}{d\theta}H_{ff'}\right)\right]+\eta'^2H_{f'f'}\,d\theta\\&=\frac{1}{2}\int_a^b\eta'^2H_{f'f'}\,d\theta>0\end{aligned} \tag{19}$$

for any perturbation $\eta(\theta)$ [11, p. 25]. It is noted that as (19) holds for any perturbation, it also holds for the admissible perturbations. Hence, it is deduced that the interval $[a,b]$ contains no points conjugate to a [11, Thm. 2, p. 109]. Based on (19), any $f(\cdot)$ satisfying (13)–(16) also satisfies the sufficient conditions to be a minimizer of (7) [11, p. 116]. Hence, it is concluded that the resulting $f(\cdot)$ is a minimizer of (7). Therefore, the aim becomes finding a solution $f(\cdot)$ that satisfies the Euler-Lagrange equations. To obtain a solution, K can be set to zero; i.e., $K=0$. Then, based on (16), there exist two cases; namely, $\lambda=0$ or $\lambda\neq 0$: (i) $\underline{\lambda=0}$: From (18), $\mu(\theta)=0$ is obtained for any θ. Hence, $f'(\theta)=\epsilon$ for all $\theta\in[a,b]$ due to (15). (ii) $\underline{\lambda\neq 0}$: From (16), $t(\theta)=0$ for any θ. Hence, the solution $f(\cdot)$ should satisfy $\int_a^b f'(\theta)\,d\theta=d-c$. Moreover, $\mu(\cdot)$ should satisfy the following equation:

$$\mu(\theta)\left[\left(h_T\mu^2(\theta)+h_T\epsilon+h_J g'(\theta)\right)^3-\tilde{K}w(\theta)\right]=0 \tag{20}$$

where $\tilde{K}=2h_T/\lambda$, meaning that there exists a set $S\subseteq[a,b]$ such that $f'(\theta)$ is specified by (8) and (9), and $\tilde{K}$ is chosen to satisfy (10). ■

By comparing the ECRB values corresponding to the encoding functions obtained for the two alternatives in Proposition 1, we can select the encoding function that yields the lower ECRB. Next, the following corollary is presented.

Corollary 1: If θ is uniformly distributed and $g(\cdot)$ is a linear mapping, the optimal encoding function is given by

$$f(\theta)=c+(d-c)(\theta-a)/(b-a) \tag{21}$$

regardless of the values of h_J and h_T.

Proof: Under the conditions in the corollary, the ratio $\left((\tilde{K}w(\theta))^{1/3}-h_J g'(\theta)\right)/h_T$ becomes a constant value that is independent of θ, which we call L. If we choose $L=(d-c)/(b-a)$ and $S=\emptyset$, it is seen that all of the Euler-Lagrange equations are satisfied. Therefore, $f'(\theta)$ must be equal to $(d-c)/(b-a)$ for all $\theta\in[a,b]$. Hence, $f(\theta)$ is given by $f(\theta)=f(a)+(d-c)(\theta-a)/(b-a)$. By choosing $f(a)=c$, we find a solution that satisfies all of the Euler-Lagrange equations and is feasible for (5). ■

To find the encoding function specified by Proposition 1, we should determine set S and parameter $\tilde{K}$ such that (8)–(10) are satisfied. To determine S, Algorithm 1 is proposed. In Algorithm 1, if $S^{(0)}$ is not empty, in each iteration $i\geq 1$, we exclude the interval in which $\alpha_i(\theta)<0$. Since we have $d-c-\epsilon(b-a)=\int_{[a,b]}\alpha_i(\theta)\,d\theta<\int_{R^{(i)}}\alpha_i(\theta)\,d\theta$ and $\tilde{K}^{(i+1)}$ is computed such that the integral of $\alpha_{i+1}(\theta)$ over the region $R^{(i)}$ is equal to $d-c-\epsilon(b-a)$, it is evident that $\tilde{K}^{(i)}\geq\tilde{K}^{(i+1)}$. This also means that $S^{(i)}\subseteq S^{(i+1)}$. By comparing the ECRB values corresponding to the encoding functions obtained by the proposed algorithm and $f'(\theta)=\epsilon$, we can determine an optimal encoding function.

Algorithm 1 Proposed Algorithm for Determining S and $f'(\cdot)$

Input: $w(\cdot), g'(\cdot), h_T, h_J, \epsilon$.
Output: $S, f'(\cdot)$.

To find $\tilde{K}^{(0)}$, solve the following integral equation $\int_a^b \frac{(\tilde{K}^{(0)}w(\theta))^{1/3}-h_T\epsilon-h_J g'(\theta)}{h_T}\,d\theta=d-c-\epsilon(b-a)$
Set $\alpha_0(\theta)=\frac{(\tilde{K}^{(0)}w(\theta))^{1/3}-h_T\epsilon-h_J g'(\theta)}{h_T}$ for all $\theta\in[a,b]$.
Find $S^{(0)}=\{\theta\in[a,b]\mid\alpha_0(\theta)<0\}$
if $S^{(0)}=\emptyset$ **then**
  $\rho=0$, $S\leftarrow S^{(0)}$, $\alpha(\cdot)\leftarrow\alpha_0(\cdot)$, $f'(\cdot)\leftarrow\alpha(\cdot)+\epsilon$.
else
  $\rho=1$, $i\leftarrow 0$, $R^{(0)}\leftarrow[a,b]\setminus S^{(0)}$.
end if
while $\rho=1$ **do**
  $i\leftarrow i+1$, and compute $\tilde{K}^{(i)}$ by solving the integral equation $\int_{R^{(i-1)}}\frac{(\tilde{K}^{(i)}w(\theta))^{1/3}-h_T\epsilon-h_J g'(\theta)}{h_T}\,d\theta=d-c-\epsilon(b-a)$.
  Set $\alpha_i(\theta)=\frac{(\tilde{K}^{(i)}w(\theta))^{1/3}-h_T\epsilon-h_J g'(\theta)}{h_T}$ for all $\theta\in R^{(i-1)}$.
  Find $S^{(i)}=\{\theta\in[a,b]\mid\alpha_i(\theta)<0\}$
  $R^{(i)}\leftarrow[a,b]\setminus S^{(i)}$
  if $S^{(i)}\setminus S^{(i-1)}=\emptyset$ **then**
    $\rho=0$, $S\leftarrow S^{(i)}$, $\alpha(\cdot)\leftarrow\alpha_i(\cdot)$, $f'(\cdot)\leftarrow\alpha(\cdot)+\epsilon$.
  end if
end while

Remark 1: When $f(\cdot)$ is strictly monotone decreasing, $-f(\cdot)$ becomes a strictly monotone increasing function. Therefore, if we define $p(\theta)\triangleq -f(\theta)$ for each θ, an optimization problem in the same form as that in (5) can be formulated and the same approach as in Section III-A can be employed.

Remark 2: The theoretical results in this section can also be extended for single-input multiple-output systems. In that case, the Fisher information becomes $\mathcal{I}(\theta)=\sum_{k=1}^M(h_T^{(k)}f'(\theta)+h_J^{(k)}g'(\theta))^2/\sigma_k^2$, where M is the number of receivers (antennas), σ_k^2 is the noise variance of the kth receiver, and $h_T^{(k)}$ and $h_J^{(k)}$ denote the channel fading coefficients between the transmitter and the kth antenna, and between the jammer and kth antenna, respectively. Since the Fisher information can be expressed as a second-degree polynomial of $f'(\theta)$ as in (6), the techniques in the proof of Proposition 1 can also be employed for this case.

B. f is not necessarily monotone

In this case, $c\leq f(\theta)\leq d$ implies that there exist $\mu(\cdot)$ and $t(\cdot)$ such that $f(\theta)=c+\mu^2(\theta)$ and $f(\theta)=d-t^2(\theta)$ for each θ. Then, (4) can be reformulated as

$$\min_f \quad \int_a^b w(\theta)(h_T f'(\theta)+h_J g'(\theta))^{-2}\,d\theta \tag{22a}$$

$$\text{subject to} \quad f(\theta)=c+\mu^2(\theta),\forall\,\theta\in[a,b] \tag{22b}$$

$$f(\theta)=d-t^2(\theta),\forall\,\theta\in[a,b] \tag{22c}$$

The following proposition characterizes the solution of (22).

Proposition 2: If $\mathcal{P}=\{\theta\mid f(\theta)=c \text{ or } f(\theta)=d\}$ has zero measure and there exists $\xi\in\mathbb{R}$ such that

$$\max_{\theta\in[a,b]}\frac{c-\psi(\theta)-f(a)}{W(\theta)}<\xi<\min_{\theta\in[a,b]}\frac{d-\psi(\theta)-f(a)}{W(\theta)}, \tag{23}$$

then any $f(\theta)=f(a)+\psi(\theta)+\xi W(\theta)$ that satisfies the Euler-Lagrange equations is an optimal solution for (22), where $\psi(\theta)\triangleq -h_J(g(\theta)-g(a))/h_T$ and $W(\theta)\triangleq\int_a^\theta w(\tau)^{1/3}\,d\tau$.

Proof: Let $F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})$ be given by

$$F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)}) = w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2} + \gamma^{(1)}(\theta)(\mu^2(\theta) + c - f(\theta)) + \gamma^{(2)}(\theta)(f(\theta) - d + t^2(\theta)) \quad (24)$$

where $\gamma^{(1)}(\theta)$ and $\gamma^{(2)}(\theta)$ are Lagrange multipliers. Finding the extremals of (22) is equivalent to finding the extremals of $\mathcal{F}(f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})$, which is given by $\mathcal{F}(f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)}) = \int_a^b F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})\, d\theta$. From (24), the Euler-Lagrange equations can be obtained as $\frac{\partial F}{\partial f} - \frac{d}{d\theta}\frac{\partial F}{\partial f'} = -\gamma^{(1)}(\theta) + \gamma^{(2)}(\theta) + \frac{d}{d\theta}\left(\frac{2h_T w(\theta)}{(h_T f'(\theta) + h_J g'(\theta))^3}\right) = 0$, $\frac{\partial F}{\partial \mu} - \frac{d}{d\theta}\frac{\partial F}{\partial \mu'} = 2\mu(\theta)\gamma^{(1)}(\theta) = 0$, $\frac{\partial F}{\partial t} - \frac{d}{d\theta}\frac{\partial F}{\partial t'} = 2t(\theta)\gamma^{(2)}(\theta) = 0$, $\frac{\partial F}{\partial \gamma^{(1)}} - \frac{d}{d\theta}\frac{\partial F}{\partial \gamma^{(1)'}} = \mu^2(\theta) + c - f(\theta) = 0$, and $\frac{\partial F}{\partial \gamma^{(2)}} - \frac{d}{d\theta}\frac{\partial F}{\partial \gamma^{(2)'}} = f(\theta) - d + t^2(\theta) = 0$. As $\mathcal{P}$ defined in Proposition 2 is assumed to have zero measure, we concentrate on the case of $\mu(\theta) \neq 0$ and $t(\theta) \neq 0$. From the first Euler-Lagrange equation above, for some $\beta \in \mathbb{R}$, the following relation is obtained: $\frac{2h_T w(\theta)}{(h_T f'(\theta) + h_J g'(\theta))^3} = \beta + \int_a^\theta \left(-\gamma^{(1)}(\tau) + \gamma^{(2)}(\tau)\right) d\tau = \beta + \int_{[a,\theta]\cap\mathcal{P}} \left(-\gamma^{(1)}(\tau) + \gamma^{(2)}(\tau)\right) d\tau = \beta$. Therefore, $f'(\theta) = ((\tilde{\beta} w(\theta))^{1/3} - h_J g'(\theta))/h_T$, where $\tilde{\beta} = 2h_T/\beta$. Then, $f(\theta)$ is expressed as $f(\theta) = f(a) + \int_a^\theta \frac{(\tilde{\beta} w(\tau))^{1/3} - h_J g'(\tau)}{h_T}\, d\tau$. Let $\xi \triangleq \tilde{\beta}^{1/3}/h_T$. Then, $f(\theta)$ can be written as

$$f(\theta) = f(a) + \psi(\theta) + \xi W(\theta). \quad (25)$$

We must find ξ such that $c < f(\theta) < d$ for any $\theta \in [a, b]$. Equivalently, ξ must satisfy the condition in (23) of Proposition 2. If there exists no ξ satisfying (23), the Euler-Lagrange equations do not yield any solution; otherwise, $f(\theta)$ can be found from (25). If there is such a ξ, similar to the proof of Proposition 1, one can see that $F_f = F_{ff'} = F_{ff} = 0$ and $F_{f'f'} > 0$ for each θ. Hence, via similar arguments, we can argue that f is the local minimizer of (22). ■

As a corollary to Proposition 2, if θ is distributed uniformly, g is a linear function of θ, and the condition in Proposition 2 holds, it is concluded that the encoding function at the transmitter is linear as in the monotone case. Furthermore, once $g(\cdot)$ and $w(\cdot)$ are known, the knowledge of $\psi(\cdot)$ and $W(\cdot)$ also becomes available. Hence, $\max_{\theta\in[a,b]} (c - \psi(\theta) - f(a))/W(\theta)$ and $\min_{\theta\in[a,b]} (d - \psi(\theta) - f(a))/W(\theta)$ can easily be found in terms of $f(a)$. By adjusting the value of $f(a)$, one can determine whether the condition in (23) is satisfied.

Remark 3: Since the optimal encoding functions in Propositions 1 and 2 are local minimizers, we can compare the ECRBs achieved by these encoding functions and choose the one that achieves the lower ECRB.

IV. Numerical Results and Conclusions

In this section, a numerical example is presented when parameter θ is uniformly distributed between 0 and 1; that is, $\Lambda = [a, b]$ with $a = 0$ and $b = 1$. In other words, $w(\theta) = 1$ if $\theta \in [0, 1]$ and $w(\theta) = 0$ otherwise. We restrict our search space to strictly monotone increasing mappings for the encoding function $f(\cdot)$ at the transmitter. Also, two different encoding functions are considered for the jammer as $g(\theta) = \theta$ and $g(\theta) = \theta^2$. Hence, $g(\theta) \in \Gamma = [k, l]$ with $k = 0$ and $l = 1$. In addition, it is assumed that the range of the encoding function $f(\cdot)$ is given by $[0, 1]$. In the simulations, ϵ in (7) is set to 0.001 and the variance of N in (1) is given by $\sigma^2 = 1$.

In Fig. 1, the optimal encoding functions, $f(\theta)$, are plotted for $g(\theta) = \theta$ and $g(\theta) = \theta^2$ when $h_T/h_J \in \{0.01, 0.1, 1, 10, 100\}$. It is observed that $f(\theta) = \theta$ regardless of the value of h_T/h_J when $g(\theta) = \theta$; that is, $f(\theta)$ is also linear in accordance with Corollary 1. When $g(\theta) = \theta^2$ and $h_T = h_J$, it is known via (8) and (9) that $f'(\theta) = \epsilon$ if $\theta \in S$ and $f'(\theta) = \nu - 2\theta$ if $\theta \in [0, 1] \setminus S$ for some $\nu \in \mathbb{R}$. By choosing $\nu = 2$ and $S = \emptyset$, we obtain the desired solution. Hence, the optimal encoding function is given by $f(\theta) = 2\theta - \theta^2$ in that case, as can be verified from Fig. 1. Also, as h_T gets significantly larger than h_J, the jamming becomes inconsequential and the optimal encoding function converges to the linear one. This is intuitive since it is known via [2, Prop.1] that in the absence of jamming, the optimal encoding function is a linear mapping for uniformly distributed parameters.

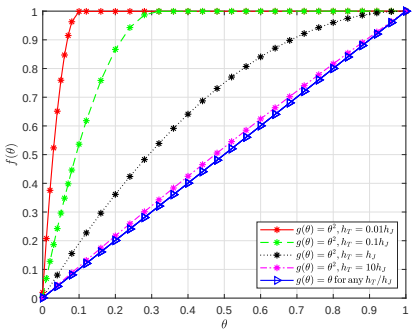

Fig. 1. $f(\theta)$ versus θ for two different encoding functions of jammer.

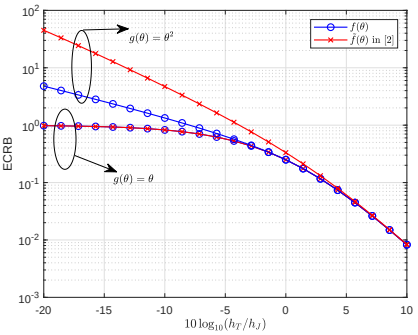

Fig. 2. ECRB versus $10\log_{10}(h_T/h_J)$ for different encoding functions.

For comparison purposes, we consider the encoding function in [2], which is optimal in the absence of jamming (and would be used if the transmitter were unaware of jamming). In that case, the encoding function, denoted by $\tilde{f}(\theta)$, has the following derivative [2]: $\tilde{f}'(\theta) = (d - c)w(\theta)/\int_a^b w(\theta)^{1/3}\, d\theta$. In Fig. 2, the ECRB values achieved by $f(\theta)$ (proposed in this work) and $\tilde{f}(\theta)$ are plotted versus h_T/h_J for $g(\theta) = \theta$ and $g(\theta) = \theta^2$. For $g(\theta) = \theta$, $f(\theta) = \tilde{f}(\theta)$; hence, the same ECRB performance is attained. For $g(\theta) = \theta^2$, the proposed encoding function leads to lower ECRB values especially for $h_T < h_J$, demonstrating the benefits of the proposed optimal encoding approach. Also, for $h_T < h_J$, the ECRB values are lower for the case of $g(\theta) = \theta$ than the case with $g(\theta) = \theta^2$. This means that the linear mapping at the jammer is not as destructive for the ECRB performance at the receiver as the nonlinear one in this scenario. Moreover, when h_T is significantly larger than h_J, all the ECRB values converge since the signal component due to the transmitter becomes dominant at the receiver and the encoding functions become the same as seen in Fig. 1.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] C. Goken and S. Gezici, "ECRB-based optimal parameter encoding under secrecy constraints," *IEEE Transactions on Signal Processing*, vol. 66, no. 13, pp. 3556–3570, 2018.

[3] C. Goken, S. Gezici, and O. Arikan, "Estimation theoretic optimal encoding design for secure transmission of multiple parameters," *IEEE Transactions on Signal Processing*, vol. 67, no. 16, pp. 4302–4316, 2019.

[4] C. Goken and S. Gezici, "Estimation theoretic secure communication via encoder randomization," *IEEE Transactions on Signal Processing*, vol. 67, no. 23, pp. 6105–6120, 2019.

[5] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[6] E. Akyol, K. Rose, and T. Basar, "On optimal jamming over an additive noise channel," in *52nd IEEE Conference on Decision and Control*, 2013, pp. 3079–3084.

[7] ——, "Optimal zero-delay jamming over an additive noise channel," *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4331–4344, 2015.

[8] X. Gao, E. Akyol, and T. Basar, "On communication scheduling and remote estimation in the presence of an adversary as a nonzero-sum game," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 2710–2715.

[9] E. Akyol, "On optimal jamming in strategic communication," in *2019 IEEE Information Theory Workshop (ITW)*, 2019, pp. 1–5.

[10] H. L. V. Trees and K. L. Bell, *Bayesian Bounds for Parameter Estimation and Nonlinear Filtering/Tracking*. Wiley-IEEE Press, 2007.

[11] I. M. Gelfand and S. V. Fomin, *Calculus of Variations*, 1963, revised English edition translated and edited by Richard A. Silverman.