Optimal Power Allocation for Secure Estimation of Multiple Parameters

Doga Gurgunoglu, *Member, IEEE*, Cagri Goken, and Sinan Gezici, *Senior Member, IEEE*

***Abstract*—Optimal power allocation for secure estimation of multiple deterministic parameters is investigated under a total power constraint. The goal is to minimize the Cramér-Rao lower bound (CRLB) at an intended receiver while keeping estimation errors at an eavesdropper above specified target levels. To that end, an optimization problem is formulated by considering measurement models involving linear transformation of the parameter vector and additive Gaussian noise. Although the proposed optimization problem is nonconvex, it is decomposed into convex sub-problems by utilizing the structure of the secrecy constraints. Then, optimal solutions to the sub-problems are characterized via optimization theoretic approaches. An algorithm utilizing that characterization is developed to obtain the optimal solution of the proposed problem.**

***Index Terms*—Cramér-Rao lower bound (CRLB), estimation, Fisher information, power adaptation, secrecy, optimization.**

I. Introduction

ESTIMATION theoretic secrecy has been investigated in various settings as an alternative to information theoretic secrecy, where the aim is the secure transmission of parameters to intended users in the presence of eavesdroppers [1]–[8]. In the literature, various approaches such as parameter encoding [4], beamforming [9], [10], [11], artificial noise generation [6], and encoder randomization [5] were adopted to maximize estimation accuracy at intended users while achieving secrecy. In [2], optimal deterministic encoding of a scalar parameter was proposed to minimize the expectation of the conditional Cramér-Rao bound of the parameter at an intended receiver under an estimation theoretic secrecy constraint. In [3], the problem of optimal secure transmission of a scalar parameter was investigated to maximize the worst-case Fisher information of the parameter at an intended receiver, which is a measure of robustness.

Optimal resource allocation for vector parameter estimation with respect to various performance metrics is the main focus in numerous studies on wireless sensor networks, wireless localization systems, and distributed radar systems, in which optimal transmission techniques are ubiquitously utilized (e.g., [12]–[15]). A common example of such techniques is to optimize a precoding or power allocation matrix by considering various scalarizations of the Fisher information matrix (FIM) as measures of estimation performance [4], [16], [17].

In certain scenarios, transmission of multiple parameters can be eavesdropped by malicious third parties to access critical information. In this letter, we investigate the use of power adaptation to mitigate estimation performance of an eavesdropper, which employs the maximum likelihood (ML) estimator. Our goal is to minimize the CRLB at an intended receiver while keeping the estimation errors of individual parameters at an eavesdropper above given target levels. To this aim, we first formulate a nonconvex optimal power allocation problem, and then propose an algorithm to solve it via decomposition into convex sub-problems, the solutions of which are characterized explicitly. The main motivation and novelty of this letter can be summarized as follows:

- With the motivation of enhancing security of parameter transmission in a practical scenario with multiple parameters and observations, we consider a vector of deterministic unknown parameters (with no prior statistical information), and propose an optimal power allocation problem to minimize the CRLB at the intended receiver while constraining the estimation performance of the ML estimator at the eavesdropper. This is unlike the problem formulations in [2], [4], which considered random parameters with known priors.
- We decompose the proposed problem into convex sub-problems and obtain their explicit solutions. Based on those explicit solutions, we propose an algorithm that solves the proposed problem exactly. We show that by adjusting transmission powers of individual parameters, it is possible to generate desired amounts of estimation errors at the eavesdropper while optimizing the estimation performance at the intended receiver.

II. Optimal Power Allocation With Secrecy Constraints

A. System Model and Problem Formulation

Consider a vector of unknown deterministic parameters denoted by $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_k]^T \in \mathbb{R}^k$. Based on the following linear models, measurements are obtained at an intended receiver and an eavesdropper:

$$\mathbf{Y}_r = \mathbf{F}_r^T \mathbf{P} \boldsymbol{\theta} + \mathbf{N}_r \tag{1}$$

$$\mathbf{Y}_e = \mathbf{F}_e^T \mathbf{P} \boldsymbol{\theta} + \mathbf{N}_e \tag{2}$$

where $\mathbf{Y}_r \in \mathbb{R}^{n_r}$ and $\mathbf{Y}_e \in \mathbb{R}^{n_e}$ denote the measurements at the intended receiver and the eavesdropper, respectively, $\mathbf{F}_r$

Manuscript received May 26, 2021; revised July 29, 2021; accepted August 8, 2021. Date of publication August 11, 2021; date of current version September 16, 2021. This work was supported by ASELSAN Inc. under the 5G Platform project which is partly funded by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 1160206. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Yunlong Cai. *(Corresponding author: Sinan Gezici.)*

Doga Gurgunoglu and Sinan Gezici are with the Department of Electrical and Electronics Engineering, Bilkent University, Ankara 06800, Turkey (e-mail: gurgunoglu@ee.bilkent.edu.tr; gezici@ieee.org).

Cagri Goken is with the Department of Communications and Information Technologies, Aselsan Inc., Ankara 06800, Turkey (e-mail: cgoken@ee.bilkent.edu.tr).

Digital Object Identifier 10.1109/LSP.2021.3104245

and $\mathbf{F}_e$ are, respectively, $k \times n_r$ and $k \times n_e$ real matrices with full row ranks ($k \leq n_r$ and $k \leq n_e$), which are assumed to be known, $\mathbf{N}_r \in \mathbb{R}^{n_r}$ and $\mathbf{N}_e \in \mathbb{R}^{n_e}$ are the additive Gaussian noise vectors at the intended receiver and the eavesdropper, respectively, which are distributed according to $\mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_r)$ and $\mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_e)$ with $\mathbf{\Sigma}_r, \mathbf{\Sigma}_e \succ \mathbf{0}$, and $\mathbf{P}$ is a $k \times k$ diagonal power allocation matrix (to be optimized), which is expressed as

$$\mathbf{P} = \operatorname{diag}\left\{\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}\right\} . \tag{3}$$

In (1) and (2), $\mathbf{F}_r$ and $\mathbf{F}_e$ represent the channel matrices (e.g., in a multiple-input multiple-output system) between the transmitter and the intended receiver, and between the transmitter and the eavesdropper, respectively.

Similarly to [2], it is assumed that the eavesdropper is unaware of the power allocation procedure. Hence, the aim is to perform power allocation so as to achieve both accurate parameter estimation at the intended receiver and secrecy against the eavesdropper. As the eavesdropper does not know the power allocation procedure, it tries to estimate $\boldsymbol{\beta} \triangleq \mathbf{P}\boldsymbol{\theta}$. Therefore, the measurement vector of the eavesdropper in (2) can be stated as

$$\mathbf{Y}_e = \mathbf{F}_e^T \boldsymbol{\beta} + \mathbf{N}_e \tag{4}$$

The eavesdropper is modeled to employ the ML estimator, i.e., it declares its estimate of the parameter vector as the maximizer of the following likelihood function with respect to $\boldsymbol{\beta}$: $(2\pi)^{-n_e/2}|\mathbf{\Sigma}_e|^{-1} \exp\left\{-0.5(\mathbf{y}_e - \mathbf{F}_e^T\boldsymbol{\beta})^T \mathbf{\Sigma}_e^{-1}(\mathbf{y}_e - \mathbf{F}_e^T\boldsymbol{\beta})\right\}$. For the considered system model, the maximizer of this likelihood function, i.e., the ML estimate for $\boldsymbol{\beta}$, can be obtained after some manipulation as

$$\widehat{\boldsymbol{\beta}}_{\mathrm{ML}}(\mathbf{y}_e) = (\mathbf{F}_e \mathbf{\Sigma}_e^{-1} \mathbf{F}_e^T)^{-1} \mathbf{F}_e \mathbf{\Sigma}_e^{-1} \mathbf{y}_e \, . \tag{5}$$

From (2) and (5), the error covariance matrix between $\widehat{\boldsymbol{\beta}}_{\mathrm{ML}}(\mathbf{Y}_e)$ and $\boldsymbol{\theta}$ is calculated, after some manipulation, as

$$\begin{aligned} \mathbf{\Sigma}_{err} &= \mathrm{E}\left[\left(\widehat{\boldsymbol{\beta}}_{\mathrm{ML}}(\mathbf{Y}_e) - \boldsymbol{\theta}\right)\left(\widehat{\boldsymbol{\beta}}_{\mathrm{ML}}(\mathbf{Y}_e) - \boldsymbol{\theta}\right)^T\right] \\ &= \mathbf{P}\boldsymbol{\theta}\boldsymbol{\theta}^T\mathbf{P} - \mathbf{P}\boldsymbol{\theta}\boldsymbol{\theta}^T - \boldsymbol{\theta}\boldsymbol{\theta}^T\mathbf{P} + \boldsymbol{\theta}\boldsymbol{\theta}^T + (\mathbf{F}_e\mathbf{\Sigma}_e^{-1}\mathbf{F}_e^T)^{-1} \end{aligned} \tag{6}$$

Defining $\mathbf{M} \triangleq (\mathbf{F}_e\mathbf{\Sigma}_e^{-1}\mathbf{F}_e^T)^{-1} \in \mathbb{R}^{k\times k}$, and denoting its diagonal entries as $\{m_{ii}\}_{i=1}^k$, the diagonal entries of $\mathbf{\Sigma}_{err}$ can be obtained as follows:

$$\mathbf{\Sigma}_{err}(i) = (p_i - 2\sqrt{p_i} + 1)\theta_i^2 + m_{ii} \tag{7}$$

for $i = 1, \ldots, k$. We consider the expression in (7) as a performance metric for quantifying the secrecy level for the ith parameter against the eavesdropper. It is noted that (7) corresponds to the MSE for the ith component of the parameter vector at the ML estimator of the eavesdropper (see (6)).

Regarding the estimation performance at the intended receiver, we consider the FIM of the measurements at the intended receiver (i.e., $\mathbf{Y}_r$ in (1)) with respect to the parameter vector $\boldsymbol{\theta}$, which is given by [16], [18, Lemma 5]

$$\mathbf{I}(\mathbf{Y}_r; \boldsymbol{\theta}) = \mathbf{P}\mathbf{F}_r\mathbf{\Sigma}_r^{-1}\mathbf{F}_r^T\mathbf{P} \, . \tag{8}$$

The inverse of the FIM, known as the CRLB, provides a lower bound on the MSE of any unbiased estimator $\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r)$ via the following matrix inequality [19]: $\operatorname{Cov}(\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r)) \geq \mathbf{I}^{-1}(\mathbf{Y}_r; \boldsymbol{\theta})$, where $\operatorname{Cov}(\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r)) = \mathrm{E}[(\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r) - \boldsymbol{\theta})(\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r) - \boldsymbol{\theta})^T]$ due to unbiasedness. Consequently, the lower bound on the MSE of the vector parameter can be stated as

$$\mathrm{E}\left[\|\widehat{\boldsymbol{\theta}}(\mathbf{Y}_r) - \boldsymbol{\theta}\|^2\right] \geq \operatorname{tr}\{\mathbf{I}^{-1}(\mathbf{Y}_r; \boldsymbol{\theta})\} \, . \tag{9}$$

The use of the CRLB metric for quantifying estimation performance facilitates a generic approach as it does not depend on the specific estimator structure at the intended receiver. In addition, the CRLB provides a tight limit for the ML estimator asymptotically [19].

For convenience, a system dependent matrix can be defined as $\mathbf{A} \triangleq (\mathbf{F}_r\mathbf{\Sigma}_r^{-1}\mathbf{F}_r^T)^{-1}$ and the inverse of the FIM in (8) can be stated as $\mathbf{I}^{-1}(\mathbf{Y}_r; \boldsymbol{\theta}) = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}^{-1}$. Then, defining the diagonal entries of $\mathbf{A}$ as $\{a_{ii}\}_{i=1}^k$, the CRLB in (9) becomes

$$\operatorname{tr}\{\mathbf{I}^{-1}(\mathbf{Y}_r; \boldsymbol{\theta})\} = \sum_{i=1}^{k} \frac{a_{ii}}{p_i} \, . \tag{10}$$

By considering the estimation performance metrics in (7) and (10) for the eavesdropper and the intended receiver, respectively, we propose the following optimal power allocation problem:

$$\min_{\{p_i\}_{i=1}^k} \quad \sum_{i=1}^{k} \frac{a_{ii}}{p_i} \tag{11a}$$

$$\text{s.t.} \quad \sum_{i=1}^{k} p_i \leq P_\Sigma \tag{11b}$$

$$p_i \geq 0, \quad i = 1, \ldots, k \tag{11c}$$

$$(\sqrt{p_i} - 1)^2\theta_i^2 + m_{ii} \geq \eta_i, \quad i = 1, \ldots, k \tag{11d}$$

where P_Σ is the total power constraint and η_i specifies the secrecy constraint for the ith parameter for $i \in \{1, \ldots, k\}$.[1]

It is assumed that $a_{ii} > 0$ in (11a) since p_i would not have any effects on the objective function if $a_{ii} = 0$; hence, the ith parameter could be left out of the optimal power allocation problem in that case. In addition, it is assumed that $\eta_i > m_{ii}$ since the secrecy constraints are trivially satisfied otherwise.

The optimization problem in (11) is non-convex due to the secrecy constraints in (11d). By defining $\alpha_i \triangleq (\eta_i - m_{ii})/\theta_i^2$, the inequalities in (11d) can be stated more explicitly as follows:

$$p_i \geq (1 + \sqrt{\alpha_i})^2, \text{ if } \alpha_i > 1, \tag{12}$$

$$p_i \leq (1 - \sqrt{\alpha_i})^2 \text{ or } p_i \geq (1 + \sqrt{\alpha_i})^2, \text{if } \alpha_i \leq 1 \tag{13}$$

for $i = 1, \ldots, k$. Depending on the values of α_i's, we partition the index set into two subsets.

$$\mathcal{A} \triangleq \{i \in \{1, \ldots, k\} \,|\, \alpha_i > 1\} \, , \tag{14}$$

$$\mathcal{B} \triangleq \{i \in \{1, \ldots, k\} \,|\, \alpha_i \leq 1\} \, . \tag{15}$$

For each index belonging to set $\mathcal{A}$, the secrecy constraint in (11d) corresponds to a convex set as in (12). For indices in set $\mathcal{B}$, the secrecy constraints lead to non-convex regions as in (13).

B. Optimal Power Allocation Via Convex Sub-Problems

Based on the statements in (12) and (13), it is deduced that the solution of (11) must satisfy one of the following inequalities: $p_i \geq \varepsilon_i$ or $p_i \leq \gamma_i$, where $\varepsilon_i \triangleq (1 + \sqrt{\alpha_i})^2$ and $\gamma_i \triangleq (1 - \sqrt{\alpha_i})^2$. By combining these inequalities with those in (11c), we can state that each p_i must satisfy

$$p_i \geq \varepsilon_i \text{ or } 0 \leq p_i \leq \gamma_i \, . \tag{16}$$

[1] In (11), it is assumed that the eavesdropper knows $\mathbf{F}_e$ and $\mathbf{\Sigma}_e$, the receiver knows $\mathbf{F}_r$, $\mathbf{\Sigma}_r$ and $\mathbf{P}$, and the transmitter knows $\mathbf{F}_r$, $\mathbf{F}_e$, $\mathbf{\Sigma}_r$ and $\mathbf{\Sigma}_e$.

for $i = 1, \ldots, k$. We define a binary vector that specifies which inequality in (16) is satisfied for each index; that is, $\boldsymbol{b} \triangleq [b(1), \ldots, b(k)] \in \{0,1\}^k$, where $b(i) = 1$ and $b(i) = 0$ imply the satisfaction of the first and second inequalities in (16), respectively. According to the entries of vector $\boldsymbol{b}$, we define a subset of the index set and its complement as follows:

$$\mathcal{S} \triangleq \{i \in \{1, \ldots, k\} \,|\, b(i) = 1\}, \tag{17}$$

$$\mathcal{S}' \triangleq \{i \in \{1, \ldots, k\} \,|\, b(i) = 0\}. \tag{18}$$

Based on the preceding definitions, we formulate the following *convex* problem:

$$\min_{\{p_i\}_{i=1}^k} \quad \sum_{i=1}^{k} \frac{a_{ii}}{p_i} \tag{19a}$$

$$\text{s.t.} \quad \sum_{i=1}^{k} p_i \le P_\Sigma \tag{19b}$$

$$p_i \ge \varepsilon_i, \quad i \in \mathcal{S} \tag{19c}$$

$$0 \le p_i \le \gamma_i, \quad i \in \mathcal{S}' \tag{19d}$$

It is noted that (19) can be regarded as a sub-problem of (11) for a given $\mathcal{S}$ since p_i's are set to specific regions in (19c) and (19d) unlike the constraints in (11d), which are equivalent to (12) or (13). The indices in set $\mathcal{A}$ in (14) correspond to the inequality in (12), which is in the form of (19c). Hence, set $\mathcal{A}$ is always contained in set $\mathcal{S}$ in (19c). However, the indices in set $\mathcal{B}$ in (15) can correspond to either of the intervals in (13), which can be in the form of (19c) or (19d). Therefore, by considering all possible intervals for the indices in set $\mathcal{B}$, i.e., by solving (19) for all $2^{|\mathcal{B}|}$ possible sets $\mathcal{S}$ and $\mathcal{S}'$ and by choosing the best solution, the solution of (11) can be obtained. The explicit solution of (19) is presented in the following proposition.

Proposition 1: The solution to the problem in (19), denoted by $\{p_i^*\}_{i=1}^k$, is specified as follows:

Case 1: If $\mathcal{S} \neq \emptyset$,

$$p_i^* = \begin{cases} \max\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, \varepsilon_i\right\}, & \text{if } i \in \mathcal{S} \\ \min\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, \gamma_i\right\}, & \text{if } i \in \mathcal{S}' \end{cases} \tag{20}$$

where $\upsilon^* \ge 0$ is a scalar that satisfies

$$\sum_{i \in \mathcal{S}} \max\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, \varepsilon_i\right\} + \sum_{i \in \mathcal{S}'} \min\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, \gamma_i\right\} = P_\Sigma. \tag{21}$$

Case 2: If $\mathcal{S} = \emptyset$, $\{p_i^*\}_{i=1}^k$ is given by one of the following:

a) $p_i^* = \gamma_i$ for $i = 1, \ldots, k$ with $\sum_{i=1}^k \gamma_i < P_\Sigma$.

b) $p_i^* = \min\{\sqrt{a_{ii}/\upsilon^*}, \gamma_i\}$, for $i = 1, \ldots, k$, where $\upsilon^* \ge 0$ satisfies $\sum_{i=1}^k \min\{\sqrt{a_{ii}/\upsilon^*}, \gamma_i\} = P_\Sigma$.

Proof: The Lagrangian function of the problem in (19) is

$$\mathcal{L}\left(\{p_i\}_{i=1}^k, \upsilon, \{\mu_i\}_{i\in\mathcal{S}}, \{\kappa_i, \lambda_i\}_{i\in\mathcal{S}'}\right) = \sum_{i=1}^{k} \frac{a_{ii}}{p_i} - \sum_{i\in\mathcal{S}'} \lambda_i p_i + \upsilon\left(\sum_{i=1}^{k} p_i - P_\Sigma\right) + \sum_{i\in\mathcal{S}} \mu_i(\varepsilon_i - p_i) + \sum_{i\in\mathcal{S}'} \kappa_i(p_i - \gamma_i) \tag{22}$$

where υ, μ_i, κ_i, and λ_i are the dual variables. Note that, by definition, $\mu_i = 0$ if $i \in \mathcal{S}'$ and $\kappa_i = \lambda_i = 0$ if $i \in \mathcal{S}$.

Since the problem is convex, the Karush-Kuhn-Tucker (KKT) conditions are necessary and sufficient for optimality. Among the KKT conditions, the primal feasibility conditions are part of the problem formulation (namely, (19b)–(19d)) and the dual feasibility implies non-negative dual variables. In addition, the stationarity and complementary slackness conditions can be expressed via (22) as follows:

Stationarity: For $i = 1, \ldots, k$,

$$\frac{\partial \mathcal{L}}{\partial p_i}\Big|_{p_i = p_i^*} = -\frac{a_{ii}}{(p_i^*)^2} + \upsilon^* - \mu_i^* + \kappa_i^* - \lambda_i^* = 0 \tag{23}$$

Complementary Slackness:

$$\upsilon^*\left(\sum_{i=1}^{k} p_i^* - P_\Sigma\right) = 0 \tag{24}$$

$$\mu_i^*(\varepsilon_i - p_i^*) = 0, \quad i \in \mathcal{S} \tag{25}$$

$$\kappa_i^*(p_i^* - \gamma_i) = 0, \quad i \in \mathcal{S}' \tag{26}$$

$$\lambda_i^* p_i^* = 0, \quad i \in \mathcal{S}' \tag{27}$$

As $a_{ii} > 0$, p_i^* cannot be zero for minimizing the objective function in (19a), meaning that $p_i^* > 0$ for $i = 1, \ldots, k$. Then, the complementary slackness condition (27) implies that $\lambda_i^* = 0$ for $i \in \mathcal{S}'$. Accordingly, the stationarity condition in (23) can be rewritten as

$$-a_{ii}/(p_i^*)^2 + \upsilon^* - \mu_i^* = 0, \quad i \in \mathcal{S} \tag{28}$$

$$-a_{ii}/(p_i^*)^2 + \upsilon^* + \kappa_i^* = 0, \quad i \in \mathcal{S}' \tag{29}$$

The conditions in (25) and (28) imply that either $p_i^* = \varepsilon_i$ or $p_i^* = \sqrt{a_{ii}/\upsilon^*} \ge \varepsilon_i$ for $i \in \mathcal{S}$. Similarly, the joint consideration of (26) and (29) implies that either $p_i^* = \gamma_i$ or $p_i^* = \sqrt{a_{ii}/\upsilon^*} \le \gamma_i$ for $i \in \mathcal{S}'$. Regarding the complementary slackness condition in (24), the scenario with $\sum_{i=1}^k p_i^* < P_\Sigma$ corresponds to $\upsilon^* = 0$; hence, (28) and (29) become

$$-a_{ii}/(p_i^*)^2 - \mu_i^* = 0, \quad i \in \mathcal{S} \tag{30}$$

$$-a_{ii}/(p_i^*)^2 + \kappa_i^* = 0, \quad i \in \mathcal{S}' \tag{31}$$

If $\mathcal{S} \neq \emptyset$, (30) cannot be satisfied due to the dual feasibility condition, meaning that $\sum_{i=1}^k p_i^* < P_\Sigma$ is not possible unless $\mathcal{S}$ is empty. Hence, $\sum_{i=1}^k p_i^* = P_\Sigma$ must hold for any non-empty $\mathcal{S}$, i.e., in Case 1 in the proposition. Consequently, the optimal power allocation strategy in Case 1 becomes as in (20), where υ^* is a non-negative real number satisfying the equality of $\sum_{i=1}^k p_i^* = P_\Sigma$, as explicitly stated in (21).

Finally, the case of $\mathcal{S} = \emptyset$ (i.e., Case 2) is considered. In this case, the relevant conditions are given by (24), (26), and (29) with $\mathcal{S}' = \{1, \ldots, k\}$. As before, (26) and (29) implies that either $p_i^* = \gamma_i$ or $p_i^* = \sqrt{a_{ii}/\upsilon^*} \le \gamma_i$ for $i \in \mathcal{S}' = \{1, \ldots, k\}$. Then, based on (24), the following two scenarios can be considered:

a): $\sum_{i=1}^k p_i^* < P_\Sigma$ and $\upsilon^* = 0$: In this scenario, $\kappa_i > 0$ holds due to (31), leading to $p_i^* = \gamma_i$ via (26) for $i = 1, \ldots, k$.

b): $\sum_{i=1}^k p_i^* = P_\Sigma$ and $\upsilon^* \ge 0$: In this scenario, either $p_i^* = \gamma_i$ or $p_i^* = \sqrt{a_{ii}/\upsilon^*} \le \gamma_i$ can hold, as discussed previously. Also, the value of υ^* can be found by solving $\sum_{i=1}^k p_i^* = P_\Sigma$ with $p_i^* = \min\{\gamma_i, \sqrt{a_{ii}/\upsilon^*}\}$. □

Based on Proposition 1, the solution of (19) can be obtained in a low complexity manner. Namely, a one-dimensional search for parameter υ^* in Proposition 1 should be performed to specify the solution of (19). Once the solution of (19) is obtained, it can be solved for $2^{|\mathcal{B}|}$ times for all possible sets $\mathcal{S}$ and $\mathcal{S}'$, as explained previously. In order to obtain the solution of the optimal power allocation problem in (11) based on the convex sub-problems in (19), we propose Algorithm 1. In this algorithm, the calculation of υ^* constitutes the most complex operation. Overall, υ^* must be calculated $2^{|\mathcal{B}|}$ times. Compared to the original

Algorithm 1: Proposed Algorithm to Find the Optimal Power Allocation Strategy $\boldsymbol{p}^{\mathrm{opt}}$ Corresponding to (11).

Result: $\boldsymbol{p}^{\mathrm{opt}}$, $\mathrm{CRLB}_{\min}$
$\mathrm{CRLB}_{\min} = \infty$ and $\boldsymbol{p}^{\mathrm{opt}} = [0, \ldots, 0]$;
Set $b[i] = 1$ for $i \in \mathcal{A}$;
% Consider Case 1 and Case 2-b);
for $j = 1, \ldots, 2^{|\mathcal{B}|}$ **do**
  Let x be the $|\mathcal{B}|$-bit (binary) representation of $j-1$;
  Set $b[\mathcal{B}(l)] = x(l)$ for $l = 1, \ldots, |\mathcal{B}|$;
  Find υ^* that solves $\sum_{i=1}^{k} b[i] \max\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, (1+\sqrt{\alpha_i})^2\right\} + (1-b[i]) \min\left\{\sqrt{\frac{a_{ii}}{\upsilon^*}}, (1-\sqrt{\alpha_i})^2\right\} = P_\Sigma$;
  for $i = 1, \ldots, k$ **do**
    $p_i^* = \max\{(1+\sqrt{\alpha_i})^2, \sqrt{\frac{a_{ii}}{\upsilon^*}}\}$ **if** $b[i] = 1$;
    $p_i^* = \min\{(1-\sqrt{\alpha_i})^2, \sqrt{\frac{a_{ii}}{\upsilon^*}}\}$ **if** $b[i] = 0$;
    $\mathrm{CRLB} = \sum_{i=1}^{k} a_{ii}/p_i^*$;
    if $\mathrm{CRLB} < \mathrm{CRLB}_{\min}$ **then**
      $\mathrm{CRLB}_{\min} = \mathrm{CRLB}$;
      $\boldsymbol{p}^{\mathrm{opt}} = \boldsymbol{p}^*$;
    end
  end
end
% Consider Case 2-a);
if $|\mathcal{A}| = 0$ & $\sum_{i=1}^{k}(1-\sqrt{\alpha_i})^2 < P_\Sigma$ **then**
  if $\sum_{i=1}^{k} \frac{a_{ii}}{(1-\sqrt{\alpha_i})^2} < \mathrm{CRLB}_{\min}$ **then**
    $\boldsymbol{p}^{\mathrm{opt}}(i) = (1-\sqrt{\alpha_i})^2$ for $i = 1, \ldots, k$;
    $\mathrm{CRLB}_{\min} = \sum_{i=1}^{k} \frac{a_{ii}}{(1-\sqrt{\alpha_i})^2}$;
  end
end

non-convex problem in (11), which requires optimization over a $k-$dimensional space, the proposed algorithm involves $2^{|\mathcal{B}|}$ one-dimensional searches, where $|\mathcal{B}| \leq k$. If $|\mathcal{B}|$ is very large, a suboptimal solution with lower complexity can be obtained by limiting the number of times the sub-problems are solved; that is, by performing the for loop in Algorithm 1 for a limited number of times by choosing distinct and random values for x. Alternatively, the binary genetic algorithm [20] with a limited number of iterations can be used to determine the elements of $\boldsymbol{b}$.[2]

Remark 1: In broadcast scenarios with multiple intended receivers and eavesdroppers, the formulation in (11) can be extended by including secrecy constraints (as in (11d)) for all eavesdroppers and replacing the objective function in (11a) with a weighted combination of the CRLBs related to intended receivers. Then, all the approaches can directly be applied.

III. Numerical Results and Conclusions

In this section, we provide a numerical example for investigating the performance of the proposed optimal power allocation algorithm. For comparison purposes, the optimal power allocation strategy in the absence of the secrecy constraint [16] is considered, as well. In the simulations, the individual secrecy constraints in (11d) are kept equal to each other, i.e., $\eta_i = \eta$ for all $i \in \{1, \ldots, k\}$. The system matrices for the intended receiver and the eavesdropper, i.e., $\mathbf{F}_r$ and $\mathbf{F}_e$ in (1) and (2), are generated via i.i.d. random entries, each uniformly distributed in $[-0.1, 0.1]$ as a single realization in MATLAB with seed 1. The additive noise vectors at the intended receiver and the eavesdropper, $\mathbf{N}_r$ and $\mathbf{N}_e$, comprise i.i.d. Gaussian random variables with mean 0 and variance 10^{-6}. The components of the parameter vector $\boldsymbol{\theta}$ are modeled as i.i.d. random variables with uniform distribution between 1 and 2, where a single realization is generated in MATLAB with seed 1.

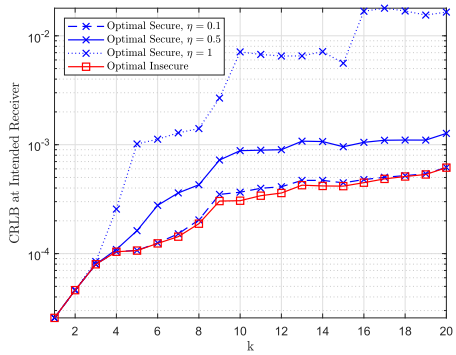

Fig. 1. CRLB at intended receiver versus dimension of parameter vector.

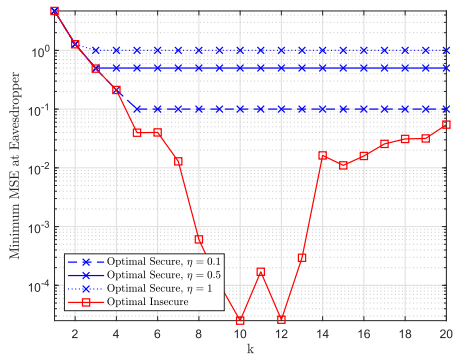

Fig. 2. Minimum MSE at eavesdropper versus dimension of parameter vector.

We investigate the impact of the dimension of the parameter vector, k, on the performance of the optimal power allocation algorithms, where the numbers of measurements in (1) and (2) are set to $n_e = n_r = 2k$, $P_\Sigma = 10$, and $\eta \in \{0.1, 0.5, 1\}$. Figs. 1 and 2 illustrate, respectively, the CRLB at the intended receiver and the minimum MSE for the parameter vector at the eavesdropper, i.e., $\min_{i \in \{1,\ldots,k\}} \boldsymbol{\Sigma}_{err}(i)$ (see (7)), versus k for both the proposed optimal power allocation algorithm (labeled 'Optimal Secure') and the optimal power allocation algorithm that minimizes the CRLB at the intended receiver in the absence of the secrecy constraint [16] (labeled 'Optimal Insecure').[3] It is observed from Fig. 1 that as the secrecy constraint η increases, the proposed algorithm results in higher CRLBs since the secrecy requirement becomes more strict. By sacrificing from the CRLB at the intended receiver, the proposed algorithm is able to satisfy the secrecy constraint as noted from Fig. 2. Since the eavesdropper is not aware of the power allocation algorithm and aims to estimate $\boldsymbol{\beta} \triangleq \mathbf{P}\boldsymbol{\theta}$, the optimal insecure power allocation algorithm, which ignores the secrecy constraint, leads to lowest minimum MSEs around $P_\Sigma = k = 10$, where the secrecy limits are violated as seen in Fig. 2. However, the proposed algorithm satisfies the secrecy limits in all cases.

[2]If $\eta_i \leq m_{ii}$ for an index $i \in \{1, \ldots, k\}$, then we can include that index in set $\mathcal{A}$ (in set $\mathcal{S}$) by setting $\varepsilon_i = 0$ in (19c). In this way, Algorithm 1 can be employed when $\eta_i \leq m_{ii}$ for some i, as well.

[3]For $\eta_i = \eta$, $i = 1 \ldots, k$, the secrecy constraint in (11d) becomes $\min_{i \in \{1,\ldots,k\}} \boldsymbol{\Sigma}_{err}(i) \geq \eta$; hence, the minimum MSE is considered in the simulations.

REFERENCES

[1] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 2, pp. 273–289, Jun. 2008.

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

[3] C. Goken and S. Gezici, "Optimal parameter encoding based on worst case Fisher information under a secrecy constraint," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1611–1615, Nov. 2017.

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

[5] C. Goken and S. Gezici, "Estimation theoretic secure communication via encoder randomization," *IEEE Trans. Signal Process.*, vol. 67, no. 23, pp. 6105–6120, Dec. 2019.

[6] A. Ozcelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2234–2238, Dec. 2015.

[7] J. Zhang, R. S. Blum, and H. V. Poor, "Approaches to secure inference in the Internet of Things: Performance bounds, algorithms, and effective attacks on IoT sensor networks," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 50–63, Sep. 2018.

[8] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[9] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[10] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure beamforming for cognitive satellite terrestrial networks with unknown eavesdroppers," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2186–2189, Jun. 2021.

[11] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 251–255, Feb. 2021.

[12] A. Sani and A. Vosoughi, "Distributed vector estimation for power and bandwidth-constrained wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 3879–3894, Aug. 2016.

[13] M. Fanaei, M. C. Valenti, and N. A. Schmid, "Power allocation for distributed BLUE estimation with full and limited feedback of CSI," in *Proc. IEEE Mil. Commun. Conf.*, 2013, pp. 418–423.

[14] T. Wang, G. Leus, and L. Huang, "Ranging energy optimization for robust sensor positioning based on semidefinite programming," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4777–4787, Dec. 2009.

[15] Z. Lin, M. Lin, T. de Cola, J.-B. Wang, W.-P. Zhu, and J. Cheng, "Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11123–11134, Jul. 2021.

[16] D. Gurgunoglu, B. Dulek, and S. Gezici, "Power adaptation for vector parameter estimation according to Fisher information based optimality criteria," 2020. [Online]. Available: https://arxiv.org/abs/2011.10609

[17] M. Shirazi and A. Vosoughi, "On Bayesian Fisher information maximization for distributed vector estimation," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 4, pp. 628–645, Dec. 2019.

[18] R. Zamir, "A proof of the Fisher information inequality via a data processing argument," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1246–1250, May 1998.

[19] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. Berlin, Germany: Springer, 1994.

[20] R. L. Haupt and S. E. Haupt, *Practical Genetic Algorithms*. New York, NY, USA: Wiley, 1998.