Power Allocation for Distortion Minimization in Distributed Estimation with Security Constraints

Xiaoxi Guo[1], Alex S. Leong[1], and Subhrakanti Dey*[2]

[1]Department of Electrical and Electronic Engineering, University of Melbourne
[2]Signals and Systems, Department of Engineering Science, Uppsala University, * Corresponding Author

***Abstract*—In this paper we explore the distortion performance of distributed estimation schemes in wireless sensor networks (WSNs) in the presence of an eavesdropper. The sensors use an uncoded amplify and forward scheme to transmit their observations to the fusion center (FC), which at the same time can be overheard by the eavesdropper. Both the FC and the eavesdropper reconstruct a minimum mean squared error (MMSE) estimate of the physical quantity observed. In this paper, we address the problem of transmit power allocation for system performance optimization subject to a total average power constraint on the sensors and a security constraint on the eavesdropper. In the case of full channel state information (CSI) the proposed scheme allows the sensors to adapt their transmission strategy based on the instantaneous channel gains of both the FC and the eavesdropper. In the partial CSI case, transmit power is allocated only according to the FC instantaneous channel gains and statistical channel gains of the eavesdropper. Numerical results illustrate the performance of the power allocation algorithms.**

***Index Terms*—Distributed estimation, fading channels, physical layer security, sensor networks, power allocation**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are networks consisting of small, inexpensive, and low-power sensors, which are deployed over a region and can communicate with each other over wireless links. Due to their low cost, robustness, and high flexibility, WSNs are widely used in event monitoring and data collection [1]. In distributed estimation, sensors independently collect data about some phenomenon and send the measurements to the fusion center (FC) which then attempt to reconstruct the phenomenon.

One crucial issue in WSNs is the limited battery life of the sensors. As sensors are normally geographically widespread, replacing batteries can be costly or sometimes even impossible. Many works [2], [3], [4], [5] have studied the power allocation problems for distributed estimation in WSNs. In [2], the authors solve the problem of minimizing power under distortion constraints and minimizing distortion under power constraints for an orthogonal multiple access channel (MAC). Using a universal decentralized quantization/estimation scheme and an uncoded quadrature amplitude modulated transmission strategy, the authors in [3] study the optimal power scheduling problem in an inhomogeneous sensor network. The power scheduling of a vector source is derived in [4] for a coherent MAC. In [5], the authors study the power allocation problem when the observations are spatially correlated.

Due to the broadcast nature of wireless communications, security and privacy issues have become one of the biggest challenges in WSNs. In many real world settings such as security systems, intelligent buildings, and hospitals, there is a high need not only for data security but also for privacy. However, the characteristics of WSNs such as the wireless environment and mobility make incorporating security very challenging, as traditional encryption schemes or cryptography normally require high computational abilities and consume large amounts of power, which is impractical for implementation in WSNs [6]. To this point, many works have focused on adapting security techniques to WSNs by reducing the key size and power consumption [7], [8], [9].

However, key-establishment protocol is not the only technique to provide security for WSNs. As a matter of fact, if an eavesdropper has sufficiently large computational power, cryptographic schemes with small key sizes may not be very effective. The notion of perfect security, first introduced by Shannon [10], provides a different way to achieve data confidentiality. With full channel state information (CSI), the authors in [11] investigate the communication of confidential messages for the fading broadcast channel, where they establish the secrecy capacity region and derive the optimal power allocation scheme to achieve the secrecy capacity region boundary. The secrecy capacity for the partial CSI scenario is considered in [12]. For distributed detection in WSNs, approaches proposed in [13], [14], [15], [16] explore the ability of the physical layer as a solution in keeping the data confidential. In [13], the authors address the data confidentiality issue by intentionally inducing decision errors that randomly flip binary local decisions before transmission. The scheme proposed in [14] allows the binary local decision of each sensor to be flipped according to the instantaneous channel gain between the sensor and the FC, and achieves perfect secrecy. Using divergence as the detection performance metric, the authors in [15] also consider a distributed binary detection problem, where they show how the perfect secrecy requirement impacts on the achievable performance and propose the related divergence per unit cost function as the most economical way to characterise the detection information.

In this paper, we consider distributed estimation with multiple sensors in the network and the presence of an eavesdropper, where the sensors use the analog amplify and forward scheme [17], [18], [19] to communicate with the FC over a slow-fading orthogonal MAC[1] (e.g., by TDMA/FDMA). The same information passes through a different set of fading orthogonal MAC before being received by the eavesdropper. The motivation for using orthogonal multiple-access channel

[1]The case of coherent MAC can also be analyzed using similar techniques to this paper.

978-1-4799-4903-8/14/$31.00 ©2014 IEEE

schemes is that it removes the need for perfect synchronization between all the sensors and the FC, but only requires pairwise synchronization between each sensor and the FC [2]. After receiving the observation signals, both the FC and the eavesdropper attempt to reconstruct a minimum mean squared error (MMSE) estimate of the observations. We study the optimal power allocation scheme that minimizes the distortion or mean squared error (MSE) at the FC, subject to both an average transmit sum power constraint at the sensors and a security constraint at the eavesdropper, to guarantee that the system is operating under the limited power budget and to ensure that not much useful information can be extracted by the eavesdropper. We consider two different scenarios: full CSI and partial CSI. In the idealistic full CSI case, we assume perfect channel knowledge of the links from the sensors to both the FC and the eavesdropper; while in the case of partial CSI, only statistical channel knowledge of the eavesdropper is available. In both scenarios, the considered optimization problems are non-convex, but we present algorithms to find locally optimal solutions by applying the Karush-Kuhn-Tucker (KKT) conditions.

The rest of the paper is organized as follows. Section II presents the system model. Section III presents the full CSI power allocation results and in Section IV, the power allocation results for partial CSI are presented. Section V briefly presents the two extreme cases of no power constraint and no security constraint for comparison purposes. Section VI presents numerical results followed by concluding remarks in Section VII.

II. SYSTEM MODEL

We consider a sensor network with K sensors observing a single point Gaussian source, denoted by $\theta[t], t = 0, 1, 2, \ldots$, which has zero mean and variance σ_θ^2, and is independent and identically distributed (i.i.d.) in time. The measurement received by the kth sensor at time t is corrupted by noise $\omega_k[t]$ and given as

$$x_k[t] = \theta[t] + \omega_k[t], \ k = 1, \ldots, K, \tag{1}$$

where we assume that $\omega_k[t]$ is i.i.d. Gaussian with zero mean and variance $\sigma_{\omega k}^2$.

The analog amplify and forward technique [17], [18], [19] is used, where sensors transmit over fading channels a scaled version of their analog measurements to the FC. It has been shown in [18] that this technique is asymptotically optimal, and exactly optimal in [19] under certain situations for Gaussian source estimation in the coherent MAC, which can give better performance than separate source channel coding. In our model, each sensor amplifies the signal with a power gain of $\beta_k[t]$ before transmitting it to the FC via a set of orthogonal channels, with the same information leaked to an eavesdropper via another set of orthogonal channels, as illustrated in Fig. 1. We assume that all channels experience block fading [20], where the channel gains remain constant during each coherence time interval, and are i.i.d. over different time intervals. The signal received by the FC and the eavesdropper are given by, respectively

$$z_k[t] = \sqrt{h_k[t]\beta_k[t]}\theta[t] + \sqrt{h_k[t]\beta_k[t]}\omega_k[t] + n_k[t], \tag{2a}$$

$$z_{ek}[t] = \sqrt{h_{ek}[t]\beta_k[t]}\theta[t] + \sqrt{h_{ek}[t]\beta_k[t]}\omega_k[t] + n_{ek}[t], \tag{2b}$$

where $\sqrt{h_k[t]}$ and $\sqrt{h_{ek}[t]}$ are respectively the instantaneous channel gains from sensor k to the FC and the eavesdropper, and $n_k[t]$ and $n_{ek}[t]$ respectively represent the i.i.d. additive Gaussian noise with zero mean and variance σ_{nk}^2 at the FC and variance σ_{ek}^2 at the eavesdropper.

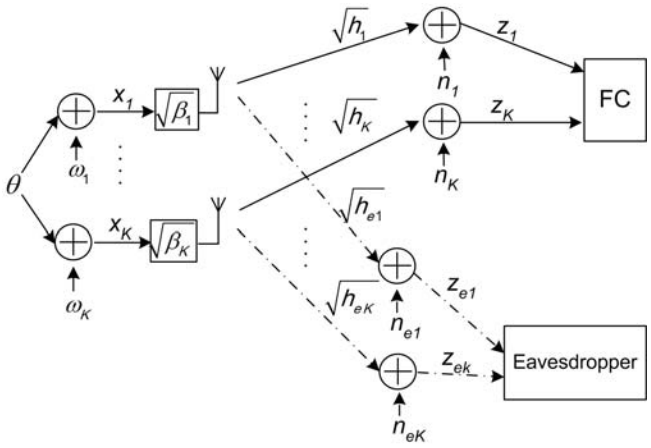

Fig. 1. Diagram of the wireless sensor network using orthogonal MAC scheme with the presence of an eavesdropper.

The linear minimum mean square error (MMSE) estimator is well known to be the optimal[2] estimator for θ under the model (1) [21]. At time t the mean squared error or distortion at the FC and the eavesdropper can be easily shown as, respectively

$$D[t] = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{h_k[t]\beta_k[t]}{h_k[t]\beta_k[t]\sigma_{\omega k}^2 + \sigma_{nk}^2} \right)^{-1}, \tag{3a}$$

$$D_e[t] = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{h_{ek}[t]\beta_k[t]}{h_{ek}[t]\beta_k[t]\sigma_{\omega k}^2 + \sigma_{ek}^2} \right)^{-1}. \tag{3b}$$

In this paper, we assume that the crucial information lies in the long term behaviour of the estimates, such as long term trends, hence the FC would be more interested in the estimation over multiple fading blocks. Given a limited transmission power budget P_{tot}, we would like to minimize the long-term average distortion at the FC by adapting $\beta_k[t]$, where the expectation is across coherence time intervals, while keeping the long term average sum of sensor transmission powers, defined as

$$\mathbb{E}\left[\sum_{k=1}^{K} \beta_k[t] \mathbb{E}\left[x_k^2[t]\right] \right] = \mathbb{E}\left[\sum_{k=1}^{K} \beta_k[t](\sigma_\theta^2 + \sigma_{\omega k}^2) \right] \tag{4}$$

to be less than P_{tot}.

In addition, we also wish to have a security constraint at the eavesdropper. In information theoretic security, the secrecy capacity is defined as the maximum transmission rate at which the mutual information between the confidential message and the signal received by the eavesdropper is less than a threshold [12]. Motivated by this idea, we consider a notion of security in estimation by requiring the distortion at the eavesdropper to be greater than a threshold. In our setting, one can either consider expected distortion (averaged over a large number of fading channel blocks) or the distortion outage probability (in the case where the estimate for each fading block contains

[2]It is also the best linear estimator for the case of non-Gaussian noise.

valuable information) as the performance metric. In this paper, we assume that the FC is interested in estimating the data over a large number of fading blocks and extracting important long term information, and estimates over individual fading blocks do not contain the desired information. Since the desired information can only be obtained from data transmitted over multiple fading blocks, we assume that the eavesdropper is also interested in long term trends in the data in order to make strategic decisions. Therefore, we consider a security constraint by maintaining the average distortion at the eavesdropper to be greater than a threshold D_E, i.e. $\mathbb{E}[D_e] \geq D_E$, to guarantee that a certain amount of confidentiality can be achieved at the FC.

Due to the assumption of system independence over time t, we will neglect the time index t for the rest of the paper.

III. FULL CSI POWER ALLOCATION

Let $\mathbf{h} = [h_1, \ldots, h_K]^T$ and $\mathbf{h}_e = [h_{e1}, \ldots, h_{eK}]^T$ be the channel gains between the sensors and FC, and between the sensors and eavesdropper, respectively. In this section we assume that the FC knows both $\mathbf{h}$ and $\mathbf{h}_e$. We can then formulate a power control problem that minimizes the distortion at the FC while satisfying a long-term total power constraint and security constraint at the eavesdropper, where the powers are computed at the FC and then fed back to the sensors. The power allocation can be obtained by solving the following functional optimization problem:

$$\begin{aligned}\min_{\beta_k(\mathbf{h},\mathbf{h}_e)\geq 0,\ \forall k}\ & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{h_k\beta_k(\mathbf{h},\mathbf{h}_e)}{h_k\beta_k(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{nk}^2}\right)^{-1}\right]\\ s.t.\ & \mathbb{E}\left[\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k(\mathbf{h},\mathbf{h}_e)\right]\leq P_{\text{tot}},\\ & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)}{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{ek}^2}\right)^{-1}\right]\\ & \qquad\geq D_E, \qquad (5)\end{aligned}$$

where $\beta_k(\mathbf{h}, \mathbf{h}_e)$ is a function of both $\mathbf{h}$ and $\mathbf{h}_e$ due to the assumption of full CSI.

To solve this problem, we will apply the technique of Lagrange multipliers. More specifically, the dual problem of (5) is defined as:

$$\max_{\lambda,\ \nu} g(\lambda, \nu), \qquad (6)$$

where λ and ν are nonnegative Lagrange multipliers, and the Lagrange dual function $g(\lambda, \nu)$ associated with the constrained optimization Problem (5) is

$$\begin{aligned}g(\lambda,\nu) = & \min_{\beta_k(\mathbf{h},\mathbf{h}_e)\geq 0,\ \forall k}\int_{\mathbf{h}}\int_{\mathbf{h}_e} l\left(\{\beta_k(\mathbf{h},\mathbf{h}_e)\},\lambda,\nu\right)\ f_{\mathbf{h}}f_{\mathbf{h}_e}\,d\mathbf{h}\,d\mathbf{h}_e\\ & -\lambda P_{\text{tot}}+\nu D_E, \qquad (7)\end{aligned}$$

with

$$\begin{aligned}& l\left(\{\beta_k(\mathbf{h},\mathbf{h}_e)\},\lambda,\nu\right)\\ &= \left(R_k+\frac{h_k\beta_k(\mathbf{h},\mathbf{h}_e)}{h_k\beta_k(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{nk}^2}\right)^{-1}+\lambda\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k(\mathbf{h},\mathbf{h}_e)\\ &\quad -\nu\left(R_{ek}+\frac{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)}{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{ek}^2}\right)^{-1}, \qquad (8)\end{aligned}$$

where $R_k = \frac{1}{\sigma_\theta^2}+\sum_{j\neq k}^{K}\frac{h_j\beta_j(\mathbf{h},\mathbf{h}_e)}{h_j\beta_j(\mathbf{h},\mathbf{h}_e)\sigma_{\omega j}^2+\sigma_{nj}^2}$, $R_{ek} = \frac{1}{\sigma_\theta^2}+\sum_{j\neq k}^{K}\frac{h_{ej}\beta_j(\mathbf{h},\mathbf{h}_e)}{h_{ej}\beta_j(\mathbf{h},\mathbf{h}_e)\sigma_{\omega j}^2+\sigma_{ej}^2}$, and $f_{\mathbf{h}} = \prod_{k=1}^{K} f(h_k)$, $f_{\mathbf{h}_e} = \prod_{k=1}^{K} f(h_{ek})$, with $f(\cdot)$ denoting the probability density function.

Due to the non-convexity of optimization Problem (5), applying the Lagrangian formulation gives us the following necessary generalized KKT conditions [22] for the optimal point

$$\begin{aligned}& \frac{-h_k\sigma_{nk}^2}{\left(h_k\beta_k(\mathbf{h},\mathbf{h}_e)\hat{R}_k+R_k\sigma_{nk}^2\right)^2}+\frac{\nu h_{ek}\sigma_{ek}^2}{\left(h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)\hat{R}_{ek}+R_{ek}\sigma_{ek}^2\right)^2}\\ &+\lambda\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)=0, \quad \forall k, \qquad (9a)\\ & \lambda\left(\mathbb{E}\left[\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k(\mathbf{h},\mathbf{h}_e)\right]-P_{\text{tot}}\right)=0, \qquad (9b)\\ & \nu\left(D_E-\mathbb{E}\left[\left(R_{ek}+\frac{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)}{h_{ek}\beta_k(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{ek}^2}\right)^{-1}\right]\right)=0, \qquad (9c)\end{aligned}$$

where $\hat{R}_k = R_k\sigma_{\omega k}^2+1$ and $\hat{R}_{ek} = R_{ek}\sigma_{\omega k}^2+1$.

In order to solve the dual problem (6), we will first assign arbitrary initial values to λ and ν, then iteratively apply the following **Step 1** and **Step 2** until we reach a pre-specified convergence criterion.

Step 1: With fixed $\lambda^{(i)}$ and $\nu^{(i)}$, where i is the iteration number, find the optimal solution of the Lagrange dual problem (7), which can be obtained by solving equations in (9a). Note that (9a) can be transformed to a set of polynomial equations, thus all the roots can be found by applying techniques such as Gröbner Bases methods [23].

Step 2: With the resulting allocated power, we update the Lagrange multipliers through a gradient descent, i.e.:

$$\lambda^{(i+1)} = \left[\lambda^{(i)}+\epsilon\left(\mathbb{E}\left[\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k^*(\mathbf{h},\mathbf{h}_e)\right]-P_{\text{tot}}\right)\right]^+, \qquad (10a)$$

$$\nu^{(i+1)} = \left[\nu^{(i)}+\kappa\left(D_E-\mathbb{E}\left[\left(R_{ek}+\frac{h_{ek}\beta_k^*(\mathbf{h},\mathbf{h}_e)}{h_{ek}\beta_k^*(\mathbf{h},\mathbf{h}_e)\sigma_{\omega k}^2+\sigma_{ek}^2}\right)^{-1}\right]\right)\right]^+, \qquad (10b)$$

where $[\cdot]^+ = \max(0,\ \cdot)$, and ϵ and κ are sufficiently small step-sizes for updating $\lambda^{(i)}$ and $\nu^{(i)}$ respectively.

IV. PARTIAL CSI POWER ALLOCATION

Due to the difficulties of perfectly acquiring the eavesdropper's CSI in practice, in this section we assume that the FC knows $\mathbf{h}$, but only has statistical knowledge of $\mathbf{h}_e$. Hence, sensors will adapt their transmission power only according to $\mathbf{h}$.

Similar to problem (7), we define the Lagrange dual function as:

$$\begin{aligned}g(\lambda,\nu) = & \min_{\beta_k(\mathbf{h})\geq 0,\ \forall k}\int_{\mathbf{h}} l\left(\{\beta_k(\mathbf{h})\},\lambda,\nu\right)\ f_{\mathbf{h}}\,d\mathbf{h}\\ & -\lambda P_{\text{tot}}+\nu D_E, \qquad (11)\end{aligned}$$

with

$$\begin{aligned}& l\left(\{\beta_k(\mathbf{h})\},\lambda,\nu\right)\\ &= \left(R_k+\frac{h_k\beta_k(\mathbf{h})}{h_k\beta_k(\mathbf{h})\sigma_{\omega k}^2+\sigma_{nk}^2}\right)^{-1}+\lambda\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k(\mathbf{h})\\ &\quad -\nu\int_{\mathbf{h}_e}\left(R_{ek}+\frac{h_{ek}\beta_k(\mathbf{h})}{h_{ek}\beta_k(\mathbf{h})\sigma_{\omega k}^2+\sigma_{ek}^2}\right)^{-1} f_{\mathbf{h}_e}\,d_{\mathbf{h}_e}. \qquad (12)\end{aligned}$$

The necessary optimality condition for problem (11) is given by

$$\frac{-h_k\sigma_{n\,k}^2}{\left(h_k\beta_k(\mathbf{h})\hat{R}_k+R_k\sigma_{n\,k}^2\right)^2}+\nu\int_{\mathbf{h}_e}\frac{h_{e\,k}\sigma_{e\,k}^2}{\left(h_{e\,k}\beta_k(\mathbf{h})\hat{R}_{e\,k}+R_{e\,k}\sigma_{e\,k}^2\right)^2}f_{\mathbf{h}_e}\,d_{\mathbf{h}_e}$$
$$+\lambda\left(\sigma_\theta^2+\sigma_{\omega\,k}^2\right)=0,\quad\forall k, \tag{13}$$

where λ and ν satisfy, respectively

$$\lambda\left(\mathbb{E}\left[\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega\,k}^2\right)\beta_k(\mathbf{h})\right]-P_{\text{tot}}\right)=0, \tag{14a}$$

$$\nu\left(D_E-\mathbb{E}\left[\left(R_{e\,k}+\frac{h_{e\,k}\beta_k(\mathbf{h})}{h_{e\,k}\beta_k(\mathbf{h})\sigma_{\omega\,k}^2+\sigma_{e\,k}^2}\right)^{-1}\right]\right)=0. \tag{14b}$$

For any channel power gains $\mathbf{h}$, the optimal transmission power of sensor k is determined by equation (13). We can then similarly adapt the two steps depicted in Section III, where in **Step 1** the optimal power $\{\beta_k^*(\mathbf{h})\}$ can be derived by applying **Algorithm 1** below.

Algorithm 1

1: Initialize the iteration index $q=0$, choose an arbitrary initial value for $\left\{\beta_k(\mathbf{h})^{(q)}\right\}_{k=1}^{K}$, and obtain $l^{(q)}=l\left(\left\{\beta_k(\mathbf{h})^{(q)}\right\},\lambda,\nu\right)$ from equation (12).
2: **repeat**
3: For $k=1:K$
  1) Let $\beta_k(\mathbf{h})^+$ denote one of the non-negative roots of equation (13), then solve $\beta_k'(\mathbf{h})=\arg\min_{\beta_k(\mathbf{h})^+}\left[l\left(\beta_k(\mathbf{h})^+,\lambda,\nu\right),\ l\left(0,\lambda,\nu\right)\right]$.
  2) Update the transmission power of sensor k by $\left[\beta_1(\mathbf{h})^{(q)},\ldots,\beta_k'(\mathbf{h})^{(q)},\ldots,\beta_K(\mathbf{h})^{(q)}\right]$.
4: update $l^{(q+1)}=l\left(\left\{\beta_k'(\mathbf{h})^{(q)}\right\},\lambda,\nu\right)$, and $q=q+1$.
5: **until** Convergence: $\frac{l^{(q+1)}-l^{(q)}}{l^{(q+1)}}<\zeta$; Set $\{\beta_k^*(\mathbf{h})\}=\left\{\beta_k'(\mathbf{h})^{(q)}\right\}$.

Remark: In **Step 1**, $\lambda^{(i)}$ and $\nu^{(i)}$ are fixed, hence we can drop the iteration number i in **Algorithm 1**; and ζ is a pre-specified convergence criterion.

V. Extreme cases

For our proposed wireless sensor network model, if the sensors have a large transmission power budget then we might expect the system to behave close to the case where there is no power constraint. Similarly, when the security threshold is sufficiently small the system could be similar to the case with no security constraint. Therefore, in this section we investigate how the system behaves when the total transmission power budget goes to infinity, and how the power allocation strategy changes where there is no security constraint.

A. No power constraint

In the case of no power constraint, the optimal transmission power level is obtained by setting λ to 0 in the Lagrange dual function. For the case of full CSI, let $\beta_k(\mathbf{h},\mathbf{h}_e)^+=\max(0,\frac{\sqrt{h_{e\,k}\sigma_{e\,k}^2\nu R_k\sigma_{n\,k}^2}-\sqrt{h_k\sigma_{n\,k}^2}R_{e\,k}\sigma_{e\,k}^2}{\sqrt{h_k\sigma_{n\,k}^2}\hat{R}_{e_k}h_{e\,k}-\sqrt{h_{e\,k}\sigma_{e\,k}^2}\nu\hat{R}_kh_k})$. We can then derive $\beta_k'(\mathbf{h},\mathbf{h}_e)$ given in (15) of the next page, which is then employed in the third step of **Algorithm 1**.

B. No security constraint

The case without the presence of an eavesdropper can be derived similar to [24], with $\beta_k'(\mathbf{h})$ in **Algorithm 1** being

$$\beta_k'(\mathbf{h})=\begin{cases}\frac{1}{\hat{R}_k}\sqrt{\frac{\sigma_{n\,k}^2}{\lambda h_k\left(\sigma_\theta^2+\sigma_{\omega\,k}^2\right)}}-\frac{R_k\sigma_{n\,k}^2}{\hat{R}_kh_k}, & \frac{h_k}{\lambda R_k^2\sigma_{n\,k}^2\left(\sigma_\theta^2+\sigma_{\omega\,k}^2\right)}>1\\ 0, & \text{otherwise}\end{cases} \tag{16}$$

We notice that the kth sensor will remain silent if its channel power gain is less than $\lambda R_k^2\sigma_{n\,k}^2\left(\sigma_\theta^2+\sigma_{\omega\,k}^2\right)$.

VI. Numerical results

In this section, we show the performance of the proposed power allocation algorithms via numerical simulations. In the simulation, we consider a multiple-sensor network with a random source θ distributed as $N(0,1)$. For simplicity, we assume that all sensors have the same measurement sensitivity of $\sigma_{\omega\,k}^2=10^{-3},\forall k$. We also consider the same noise levels for both the FC's and eavesdropper's channels, where $\sigma_{n\,k}^2=\sigma_{e\,k}^2=10^{-8},\forall k$. From (3b), we know that the distortion D_e at the eavesdropper attains the maximum value of σ_θ^2 when $\beta_k=0,\forall k$, and $D_e\to\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{1}{\sigma_{\omega\,k}^2}\right)^{-1}$ as $\beta_k,\forall k$ approaches infinity, which gives the bounds, $\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{1}{\sigma_{\omega\,k}^2}\right)^{-1}\le\mathbb{E}[D_e]\le\sigma_\theta^2$. Therefore, the security threshold at the eavesdropper in this simulation is chosen from the range $0.05\le D_E\le 0.3$, with the average power constraint set to 30mW. Additionally, we consider the signal power at the FC and the eavesdropper to follow the free-space pathloss model [25]

$$PL_k=20\log_{10}(D_k)+20\log_{10}(f)-27.55, \tag{17}$$

where $D_k=\{d_k,d_{e\,k}\}$ is the distance between sensor k and the FC or the eavesdropper in meters, and f is the signal frequency in megahertz. Thus, the channel power gain follows an exponential distribution with mean $10^{-\frac{PL_k}{10}}\text{mW}$. We further assume that the network utilizes an operation frequency of 800MHz; and the distance from each sensor to the FC, and the distance from each sensor to the eavesdropper, to be 130m, i.e., $d_{e\,k}=d_k,\forall k$.

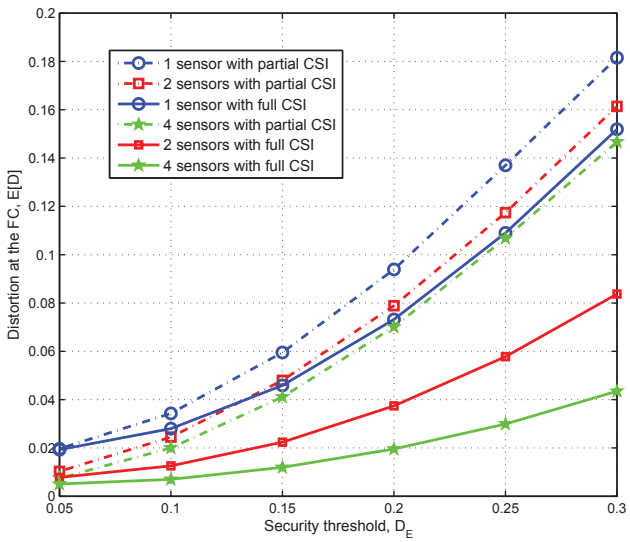

Fig. 2. Performance comparison between full CSI and partial CSI in a 1, 2 and 4 sensors network with $P_{\text{tot}}=30\text{mW}$.

$$\beta_k'(\mathbf{h},\mathbf{h}_e)=\begin{cases}\beta_k(\mathbf{h},\mathbf{h}_e)^+, & \frac{h_k\beta_k(\mathbf{h},\mathbf{h}_e)^+\sigma_{w_k}^2+\sigma_{n_k}^2}{h_k\beta_k(\mathbf{h},\mathbf{h}_e)^+\hat{R}_k+R_k\sigma_{n_k}^2}-\nu\frac{h_{e_k}\beta_k(\mathbf{h},\mathbf{h}_e)^+\sigma_{\omega_k}^2+\sigma_{e_k}^2}{h_{e_k}\beta_k(\mathbf{h},\mathbf{h}_e)^+\hat{R}_{e_k}+R_{e_k}\sigma_{e_k}^2}<\frac{1}{R}-\frac{\nu}{R_{e_k}}\\ 0. & \text{otherwise}\end{cases} \tag{15}$$

In Fig. 2 we plot the average distortion at the FC versus the security threshold at the eavesdropper D_E, for both the full CSI and partial CSI cases in a 2 and 4 sensor network. For comparison, we also plot the case of one sensor. The first thing to be noticed is the similar performance between partial CSI and full CSI when D_E is very small across all three different scenarios, but the differences gradually increase as we enlarge D_E. Additionally, the performance gap between full CSI and partial CSI increases when the number of sensors increases, which indicates the crucial role of the eavesdropper's CSI in a network with a large number of sensors.

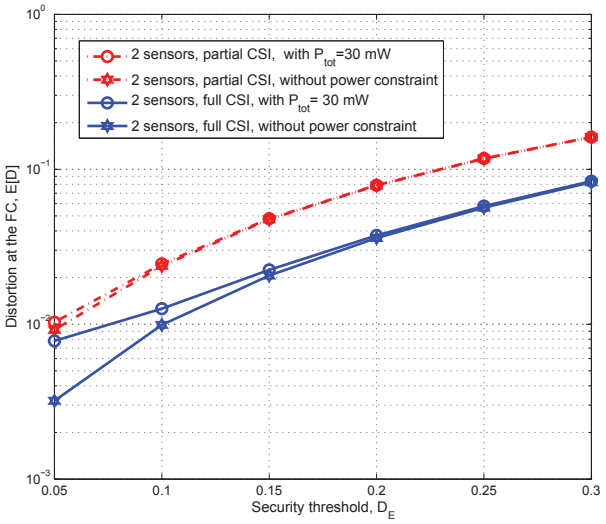

Fig. 3. Performance comparison between power constraint with $P_{\text{tot}} = 30$mW and no power constraint case in a 2 sensors network.

In Fig. 3 we study the distortion performance at the FC in a 2 sensor network with no power constraint for both the full CSI and partial CSI scenarios, and also the case with power constraint of $P_{\text{tot}} = 30$mW. It is seen, in both scenarios, that the distortion in the no power constraint case is always superior to the case with a power constraint. However, the performance of the two cases are very close to each other, and the performance gap gradually vanishes as the security threshold increases. This is because in order to achieve large distortion at the eavesdropper (to meet the security constraint), the sensors have to reduce the transmission power (or stop transmitting in some situations) even though they have an infinite power budget (i.e. no power constraint).

VII. Conclusion

In this paper, we have considered a problem of transmit power allocation for estimation performance optimization in a multiple-sensor network with the presence of an eavesdropper. We first assumed that the sensors know the CSI of both the FC and eavesdropper channel, and derived the power allocation strategy that meets the security requirement. Then, we considered the case where the sensors only know the FC's channel and again derived the power allocation strategy at the eavesdropper. Future work will consider a secrecy outage constraint, by requiring the outage probability for the eavesdropper to be smaller than a certain value, where the outage probability is defined as the probability that the distortion at the eavesdropper is less than a maximum distortion threshold. In addition, the current work can be extended to the multi-antenna case, where the artificial noise technique [26] would be deployed to confuse the eavesdropper.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.
[2] S. Cui, J.-J. Xiao, A. Goldsmith, Z.-Q. Luo, and H. Poor, "Estimation diversity and energy efficiency in distributed sensing," *Signal Processing, IEEE Transactions on*, vol. 55, no. 9, pp. 4683–4695, Sept 2007.
[3] J.-J. Xiao, S. Cui, Z.-Q. Luo, and A. Goldsmith, "Power scheduling of universal decentralized estimation in sensor networks," *Signal Processing, IEEE Transactions on*, vol. 54, no. 2, pp. 413–422, Feb 2006.
[4] ——, "Linear coherent decentralized estimation," *Signal Processing, IEEE Transactions on*, vol. 56, no. 2, pp. 757–770, Feb 2008.
[5] I. Bahceci and A. Khandani, "Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation," *Communications, IEEE Transactions on*, vol. 56, no. 7, pp. 1146–1156, July 2008.
[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.
[7] J. Zhang and V. Varadharajan, "A new security scheme for wireless sensor networks," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–5.
[8] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *Communications Magazine, IEEE*, vol. 44, no. 4, pp. 122–130, 2006.
[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 41–47.
[10] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
[11] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2470–2492, 2008.
[12] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, 2008.
[13] T. Aysal and K. Barner, "Sensor data cryptography in wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 273–289, 2008.
[14] H. Jeon, J. Choi, S. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 4, pp. 619–625, 2013.
[15] S. Marano, V. Matta, and P. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *Signal Processing, IEEE Transactions on*, vol. 57, no. 5, pp. 1976–1986, 2009.
[16] ——, "On the divergence-cost function in distributed detection with a secrecy constraint," in *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*, 2008, pp. 1357–1360.
[17] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: lossy source-channel communication revisited," *Information Theory, IEEE Transactions on*, vol. 49, no. 5, pp. 1147–1158, 2003.
[18] M. Gastpar and M. Vetterli, "Source-channel communication in sensor networks," in *Information Processing in Sensor Networks*. Springer, 2003, pp. 162–177.
[19] M. Gastpar, "Uncoded transmission is exactly optimal for a simple gaussian "sensor" network," *Information Theory, IEEE Transactions on*, vol. 54, no. 11, pp. 5247–5251, 2008.
[20] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.
[21] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.
[22] D. G. Luenberger, *Optimization by Vector Space Methods*. New York: Wiley-Interscience, 1969.
[23] D. A. Cox, J. Little, and D. OSHEA, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 2007.
[24] A. Leong and S. Dey, "On scaling laws of diversity schemes in decentralized estimation," *Information Theory, IEEE Transactions on*, vol. 57, no. 7, pp. 4740–4759, 2011.
[25] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
[26] R. Negi and S. Goel, "Secret communications using artificial noise," in *Proc. VTC*, Dallas, TX, Sep. 2005, pp. 1906–1910.