

Power Allocation for Estimation Outage Minimization with Secrecy Outage Constraints

Xiaoxi Guo, *Student Member, IEEE*, Alex S. Leong, *Member, IEEE* and Subhrakanti Dey, *Senior Member, IEEE*

Abstract—In this paper, we investigate the distortion outage minimization problem for a wireless sensor network (WSN) in the presence of an eavesdropper. The observation signals transmitted from the sensors to the fusion center (FC) are overheard by the eavesdropper. Both the FC and the eavesdropper reconstruct minimum mean squared error (MMSE) estimates of the physical quantity observed. We address the problem of transmit power allocation to minimize the distortion outage at the FC, subject to a long-term transmit power constraint among the sensors and a secrecy outage constraint at the eavesdropper. Applying a rigorous probabilistic power allocation technique we derive power policies for the full channel state information (CSI) case. Additional suboptimal power control policies are studied for the partial CSI case in order to reduce the high computational cost as the number of sensors or receive antennas grows. Numerical results show better performance can be achieved by adding multiple receive antennas at the FC.

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

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have attracted much recent research interests and have been widely studied due to many military as well as civilian applications such as environmental monitoring, traffic control, battlefield surveillance etc. A typical wireless sensor network normally consists of some small, inexpensive, and low-power sensors, which are deployed over a region and may communicate with a remote processor over wireless links [1]. In distributed estimation, sensors independently collect data about some phenomenon, which are sent to a fusion center (FC) and then combined to reconstruct a final estimate of the observed quantity.

In a WSN, the sensors typically have limited energy resources and replacing batteries is considered expensive. Many works have studied how to efficiently transmit the observations from sensors to the FC. In [2], [3], a digital approach was considered where the analog observations are digitised into bits and then modulated and transmitted. In [4], the authors showed that using uncoded analog forwarding of observed signals is asymptotically optimal in estimating a Gaussian source for a coherent Gaussian multiple access channel (MAC); and exactly optimal in [5] under certain situations. Deploying this analog-forwarding transmission, the authors in [6], [7] studied the optimal power scheduling problem in a sensor network. The diversity order of decentralized estimation in terms of increasing numbers of sensors has also been explored in [8], [9].

In the context of communications and information theory, the idea of *information outage* probability minimization was introduced in [10] for block-fading channels, and has been further extended in e.g. [11], [12]. A similar concept of

estimation outage probability for distributed estimation was introduced by the authors in [8], which is defined as the probability that the estimation distortion exceeds a certain threshold. With full channel state information (CSI), the authors in [13] considered a clustered WSN and derived the optimal power allocation for estimation outage minimization problem; the results were extended to partial CSI with limited feedback in [14].

Under open wireless media, when the measurements at individual sensors are confidential, maintaining secrecy in a wireless network becomes quite challenging. The traditional cryptographic encryption techniques suffer many vulnerabilities and can be difficult to implement in sensor networks under energy and computational constraints. As an alternative, the concept of physical layer security has recently garnered a lot of research interest. The concept of wiretap channel was introduced by Wyner in [15]. It showed that a non-zero secrecy capacity can only be obtained if the adversary's channel is of lower quality than that of the legitimate recipient. From an information theoretic perspective, the authors in [16], [17], [18] studied the secrecy capacity in the case of full CSI or partial CSI. Multiterminal source coding or CEO problems with secrecy constraints were also considered in [19], [20], [21]. However, although the secure source coding techniques enable one to gain information-theoretic insights, it does not provide a closed form expression for distortion achievable via multi-sensor estimation over fading channels. Thus motivated, we investigate the secure estimation problem from a signal processing viewpoint where sensors employ simple uncoded analog-forwarding techniques to transmit their observations to the FC. In this way, a direct expression for the distortion over fading channels can be obtained, which is more desirable for deriving analytical results. In fact, various secrecy schemes from a 'signal processing' rather than information theoretic point of view have also been studied in [22], [23], [24], where different performance metrics, such as bit-error-rate, signal-interference-to-noise ratio or Ali-Silvey distances were used to measure secrecy in a system.

Therefore, in favour of a closed form distortion expression for multi-sensor estimation over fading channels, we consider analog uncoded transmission at the sensors. Recently, the authors in [25] looked at the optimal power allocation for a decentralized estimation problem in the presence of an eavesdropper. To secure the system a minimum distortion threshold is set for the eavesdropper to ensure that the estimation error at the eavesdropper is no smaller than this threshold. However, due to the randomness of the fading channels, the quality of the estimate at the FC becomes a random variable. This might be detrimental to real-time applications when the distortion at the FC becomes large for a particular fading realisation, or the distortion at the eavesdropper becomes very small. Hence, for a delay constrained sensor network, instead of minimising a long-term average estimation error at the FC as in [25], it is more appropriate to maintain a target distortion level throughout the fading

X. Guo and A. S. Leong are with the Department of Electrical and Electronic Engineering, The University of Melbourne, VIC 3010, Australia. (e-mails: xiaoxig@student.unimelb.edu.au and asleong@unimelb.edu.au), Subhrakanti Dey is with the Department of Engineering Science, Uppsala University, Sweden. (subhrakanti.dey@angstrom.uu.se).

This work was supported by the Australian Research Council under grants DE120102012 and DP120101122.

process and minimise a *distortion outage probability*¹ at the FC and a secrecy outage constraint at the eavesdropper. This is the subject of our current work.

In this paper, we look at a WSN where each sensor independently measures a single point Gaussian source, and then transmits the noisy measurements to the FC using an uncoded analog scheme over an orthogonal MAC in the presence of an eavesdropper or adversary. Both the FC and the adversary attempt to reconstruct a minimum mean squared error (MMSE) estimate of the observations. Under this setting, the main contributions of the paper are: first, we consider power allocation problems that minimise the distortion outage probability at the FC, subject to a long-term transmit power constraint and a secrecy outage constraint at the eavesdropper, where a *estimation secrecy outage* is defined as the event that the mean squared error (MSE) at the eavesdropper is below a minimum acceptable distortion level. In this way, the entire network is guaranteed to operate under a specified power constraint; while maintaining a certain level of confidentiality. Second, we study the distortion outage probability at the FC that can be achieved by adding multiple receive antennas in both the full CSI and partial CSI cases. In addition, we propose suboptimal power allocation policies to alleviate the high computational cost issues raised by computing for the locally optimal power policy in the partial CSI case.

The rest of the paper is organized as follows. In Section II we present the system model for a multiple-sensor network. In Section III, we form and solve the outage minimization problem in full CSI case. The case of partial CSI is considered in Section IV, where we also propose a suboptimal method to compensate the high computational cost issues. Illustrative numerical results are provided in Section V, followed by concluding remarks in Section VI.

II. MULTIPLE SENSORS SCENARIO

A schematic diagram of the wireless sensor network model is shown in Fig. 1, where we have K sensors observing a single point Gaussian source with zero mean and variance σ_θ^2 , denoted by $\theta[t]$, $t = 0, 1, 2, \dots$. The measurement $x_k[t]$ received by the k th sensor at time t is corrupted with noise and is given by

$$x_k[t] = \theta[t] + \omega_k[t], \quad (1)$$

where $\omega_k[t]$ is the sensor measurement noise which is i.i.d. (independent and identically distributed) Gaussian with zero mean and variance $\sigma_{\omega_k}^2$.

The sensors are assumed to have a single transmit antenna. Each sensor amplifies and forwards their measurements to a N_r -antenna fusion center (FC) with amplification factor $\beta_k[t] \in \mathbb{C}$ via a slow-fading orthogonal multiple-access channel (MAC), e.g. by using frequency-division duplexing (FDD) or time-division duplexing (TDD) techniques. The transmissions are overheard by an eavesdropper who is equipped with N_e receive antennas. We assume that both the FC's and the eavesdropper's channels experience block fading, where the channels remain constant during each

¹This is analogous to the situation in wireless communication where the ergodic capacity describes the maximum achievable long term average rate without a delay constraint; however, in real-time applications because of the delay constraint it is more suitable to adopt the notion of the outage capacity, which determines the maximum achievable rate with an outage probability less than ϵ [10].

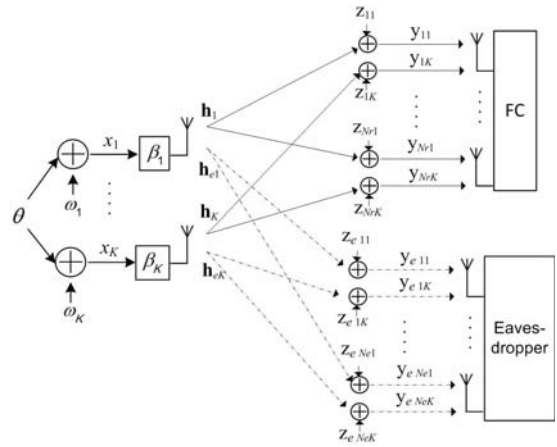


Fig. 1: Diagram of the wireless sensor network using orthogonal MAC scheme with the presence of an eavesdropper.

coherence time interval, and are i.i.d. over different time intervals [10]. The signals received by the FC and eavesdropper from the k th sensor are then given by, respectively,

$$\mathbf{y}_k[t] = \theta[t]\beta_k[t]\mathbf{h}_k[t] + \omega_k[t]\beta_k[t]\mathbf{h}_k[t] + \mathbf{z}_k[t], \quad (2a)$$

$$\mathbf{y}_{ek}[t] = \theta[t]\beta_k[t]\mathbf{h}_{ek}[t] + \omega_k[t]\beta_k[t]\mathbf{h}_{ek}[t] + \mathbf{z}_{ek}[t], \quad (2b)$$

where $\mathbf{y}_k[t] = [y_{1k}[t], \dots, y_{N_rk}[t]]^T$ and $\mathbf{y}_{ek}[t] = [y_{e1k}[t], \dots, y_{eN_ek}[t]]^T$, the entries of $\mathbf{h}_k[t]$ and $\mathbf{h}_{ek}[t]$ are the instantaneous zero mean i.i.d. complex Gaussian channels from sensor k to the FC and the eavesdropper with variances $\sigma_{h_k}^2$ and $\sigma_{h_{ek}}^2$ respectively, and $\mathbf{z}_k[t] = [z_{1k}[t], \dots, z_{N_rk}[t]]^T$ and $\mathbf{z}_{ek}[t] = [z_{e1k}[t], \dots, z_{eN_ek}[t]]^T$ represent i.i.d. additive Gaussian noise with zero mean and covariances $\sigma_k^2 \mathbf{I}_{N_r}$ at the FC and $\sigma_{ek}^2 \mathbf{I}_{N_e}$ at the eavesdropper respectively². The set of received signals at the FC from all sensors can be written as

$$\begin{aligned} \mathbf{Y}[t] &= [\mathbf{y}_1[t], \dots, \mathbf{y}_K[t]]^T \\ &= \theta[t] [\beta_1[t]\mathbf{h}_1[t], \dots, \beta_K[t]\mathbf{h}_K[t]]^T + [\mathbf{z}_1[t], \dots, \mathbf{z}_K[t]]^T \\ &\quad + [\omega_1[t]\beta_1[t]\mathbf{h}_1[t], \dots, \omega_K[t]\beta_K[t]\mathbf{h}_K[t]]^T. \end{aligned} \quad (3)$$

Using the fact that each sensor transmits through an orthogonal MAC, the covariance of the noise factor $[\omega_1[t]\beta_1[t]\mathbf{h}_1[t], \dots, \omega_K[t]\beta_K[t]\mathbf{h}_K[t]]^T + [\mathbf{z}_1[t], \dots, \mathbf{z}_K[t]]^T$ can be derived as a $KN_r \times KN_r$ matrix:

$$C[t] = \begin{bmatrix} \sigma_{\omega_1}^2 \beta_1^2[t] \mathbf{h}_1[t] \mathbf{h}_1^H[t] + \sigma_1^2 \mathbf{I}_{N_r} & & & \mathbf{0} \\ & \ddots & & \\ & & \sigma_{\omega_K}^2 \beta_K^2[t] \mathbf{h}_K[t] \mathbf{h}_K^H[t] + \sigma_K^2 \mathbf{I}_{N_r} & \\ \mathbf{0} & & & \end{bmatrix}$$

The linear minimum mean square error (MMSE) estimator is well known to be the optimal estimator for θ under the model (2) [26]. At time t the mean squared error (MSE) or *distortion* at the FC using the MMSE estimator is

$$\begin{aligned} D[t] &= \left(\frac{1}{\sigma_\theta^2} + \begin{bmatrix} \beta_1[t]\mathbf{h}_1[t] \\ \vdots \\ \beta_K[t]\mathbf{h}_K[t] \end{bmatrix}^H C[t]^{-1} \begin{bmatrix} \beta_1[t]\mathbf{h}_1[t] \\ \vdots \\ \beta_K[t]\mathbf{h}_K[t] \end{bmatrix} \right)^{-1} \\ &\stackrel{(a)}{=} \left[\frac{1}{\sigma_\theta^2} + \sum_{k=1}^K \beta_k^H[t]\beta_k[t] \left(\sigma_k^{-2} \mathbf{h}_k^H[t]\mathbf{h}_k[t] - \sigma_k^{-2} \mathbf{h}_k^H[t]\mathbf{h}_k[t] \right) \right. \\ &\quad \left. \left(\sigma_{\omega_k}^{-2} \beta_k^{-2}[t] + \sigma_k^{-2} \mathbf{h}_k^H[t]\mathbf{h}_k[t] \right)^{-1} \sigma_k^{-2} \mathbf{h}_k^H[t]\mathbf{h}_k[t] \right]^{-1} \\ &= \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^K \frac{g_k[t] p_k[t]}{\sigma_k^2 + g_k[t] \sigma_{\omega_k}^2 p_k[t]} \right)^{-1}, \end{aligned} \quad (4)$$

²The notation \mathbf{x}^T and \mathbf{x}^H refers to the transpose of \mathbf{x} and conjugate transpose of \mathbf{x} respectively.

where (a) results from applying the Matrix Inversion Lemma [27], $p_k[t] \triangleq \beta_k^H[t]\beta_k[t]$ is the power allocated on the k th sensor, and $g_k[t] \triangleq \mathbf{h}_k^H[t]\mathbf{h}_k[t] = \sum_{m=1}^{N_r} h_{mk}^H[t]h_{mk}[t]$ is the sum of channel power gains from the k th sensor to the FC with $h_{mk}[t]$ being the channel gain from sensor k to m th antenna at the FC. Note that for a given set of $\{p_k[t]\}$, any $\{\beta_k[t]\}$ satisfying $\beta_k[t]^H\beta_k[t] = p_k[t]$, $\forall k$ would result in the same distortion, hence we will mainly focus on $\{p_k[t]\}$ in the paper. We assume the optimal power allocation strategy is designed by the FC, and then $\{p_k[t]\}$ are wirelessly transmitted to the sensors via a public channel³. The minimum distortion level at the eavesdropper is achieved by implementing the linear MMSE estimator, shown as

$$D_e[t] = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^K \frac{g_{ek}[t]p_k[t]}{g_{ek}[t]p_k[t]\sigma_{\omega_k}^2 + \sigma_{e_k}^2} \right)^{-1}, \quad (5)$$

where $g_{ek}[t] \triangleq \mathbf{h}_{ek}^H[t]\mathbf{h}_{ek}[t] = \sum_{n=1}^{N_e} h_{enk}^H[t]h_{enk}[t]$ is the sum of channel power gains from the k th sensor to the eavesdropper and $h_{enk}[t]$ is the channel gain from sensor k to n th antenna at the eavesdropper. Due to the randomness of the fading channels, the instantaneous distortions at the FC and the eavesdropper, as shown in (4) and (5), change over time.

Different from our previous work [25] in which we studied optimal power allocation for distortion minimization with a security constraint at the eavesdropper, in this paper we focus on the distortion outage minimization problem. For a given maximum acceptable distortion level \mathbb{D} at the FC, we define a *distortion outage* to be the event that the instantaneous distortion $D[t]$ exceeds \mathbb{D} . The *distortion outage probability* at the FC is then given as $\Pr_{\text{outage_FC}} \triangleq \Pr[D[t] > \mathbb{D}]$. At the eavesdropper, for a given minimum acceptable distortion level \mathbb{D}_e , a *secrecy outage* event is declared if the instantaneous distortion $D_e[t]$ is less than \mathbb{D}_e (which means that the eavesdropper has a good quality estimate), and the *secrecy outage probability* is defined as $\Pr_{\text{outage_EVE}} \triangleq \Pr[D_e[t] < \mathbb{D}_e]$. We assume that the full channel state information (CSI) of the FC is available, while eavesdropper's channel information may or may not be aware by the FC.

In this paper, we wish to minimize the distortion outage probability at the FC by adapting the transmit powers of the sensors at each channel instance, while keeping the secrecy outage probability under a certain threshold, i.e., $\Pr_{\text{outage_EVE}} \leq \delta$, and the long-term average sum of sensor transmission powers, defined as $\mathbb{E} \left[\sum_{k=1}^K p_k \mathbb{E} [x_k^2[t]] \right] = \mathbb{E} \left[\sum_{k=1}^K p_k (\sigma_\theta^2 + \sigma_{\omega_k}^2) \right]$, to be less than a power budget \mathcal{P}_{tot} .

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

III. FULL CSI

In this section, we assume the FC not only knows the channel states between the sensors and the FC, it can also acquire the channel information between the sensors and the eavesdropper. Clearly, the requirement of full CSI of the eavesdropper channels is infeasible in practice. However, the optimal performance with this assumption is instructive as

³When the feedback link is secure, the estimation distortion seen by the eavesdropper will be even larger than $D_e[t]$ given in (5), due to the lack of $\{p_k[t]\}$.

well as useful as a benchmark for the performance with partial CSI of the eavesdropper channels, to be analysed subsequently.

Let the channel states at the FC and the eavesdropper be denoted by $\mathbf{g} = [g_1, \dots, g_K]$ and $\mathbf{g}_e = [g_{e1}, \dots, g_{eK}]$ respectively. The outage minimization problem is

$$\begin{aligned} & \min_{\mathbf{P}(\mathbf{G})} \Pr [D(\mathbf{G}, \mathbf{P}(\mathbf{G})) > \mathbb{D}] \\ & \text{s.t. } \Pr [D_e(\mathbf{G}, \mathbf{P}(\mathbf{G})) < \mathbb{D}_e] \leq \delta, \mathbb{E} [\langle \mathbf{P}(\mathbf{G}) \rangle] \leq \mathcal{P}_{\text{tot}}, \quad (6) \end{aligned}$$

where $\mathbf{G} = [\mathbf{g}; \mathbf{g}_e]$ and $\langle \mathbf{p}(\mathbf{G}) \rangle \triangleq \sum_{k=1}^K (\sigma_\theta^2 + \sigma_{\omega_k}^2) p_k(\mathbf{G})$ is the total power consumption. $\mathbf{P}(\mathbf{G})$ is a vector of random variables with conditional probability density function $f_{\mathbf{P}|\mathbf{G}}(\mathbf{p}|\mathbf{G})$, where $\mathbf{p}(\mathbf{G})$ is one of the deterministic schemes and $\mathbf{p} = [p_1, \dots, p_K]$ is the power of all the sensors.

Remark: In order to produce a meaningful solution to problem (6), \mathbb{D}_e is set to a suitable value such that the feasible region is not empty for a given transmit power budget \mathcal{P}_{tot} and a secrecy outage probability threshold δ .

In communications theory, it was shown in [12], [10] that for information outage minimization problems the optimal power allocation policy is in general a probabilistic policy, in particular this is often the case for discrete channel distributions. Motivated by these results, we start with a probabilistic power allocation $\mathbf{P}(\mathbf{G})$.

Denote the indicator function by $1(x)$, where $1(x) = 1$ if x is true; otherwise $1(x) = 0$. With the assumption on the fading channels and perfect CSI at the FC, the distortion outage probability at the FC and the secrecy outage probability at the eavesdropper can be expressed as, respectively,

$$\begin{aligned} & \Pr [D(\mathbf{G}, \mathbf{P}) > \mathbb{D}] \\ & = \iint 1 \{D(\mathbf{G}, \mathbf{p}) > \mathbb{D}\} f_{\mathbf{P}|\mathbf{G}}(\mathbf{p}|\mathbf{G}) d\mathbf{p}(\mathbf{G}) dF(\mathbf{G}), \quad (7) \end{aligned}$$

$$\begin{aligned} & \Pr [D_e(\mathbf{G}, \mathbf{P}) < \mathbb{D}_e] \\ & = \iint 1 \{D_e(\mathbf{G}, \mathbf{p}) < \mathbb{D}_e\} f_{\mathbf{P}|\mathbf{G}}(\mathbf{p}|\mathbf{G}) d\mathbf{p}(\mathbf{G}) dF(\mathbf{G}). \quad (8) \end{aligned}$$

We outline the strategy involved in solving problem (6), which are similar to techniques used in [12]. We first show that for an arbitrary feasible probabilistic power allocation $\mathbf{P}(\mathbf{G})$, which can be divided into four non-overlapping power regions, we can always construct another feasible probabilistic power allocation $\hat{\mathbf{P}}(\mathbf{G})$ that contains three power regions, with the powers in one of the regions all equal to zero, and such that $\hat{\mathbf{P}}(\mathbf{G})$ gives no worse performance than $\mathbf{P}(\mathbf{G})$. Next, based on $\hat{\mathbf{P}}(\mathbf{G})$ we construct another feasible power scheme $\mathbf{P}'(\mathbf{G})$ which is randomized among three deterministic power schemes $\{\mathbf{p}_i(\mathbf{G})\}$, $i = 1, 2, 3$ with corresponding weighting factors $\{\omega_i(\mathbf{G})\}$. Furthermore, we show that $\mathbf{P}'(\mathbf{G})$ performs at least as well as $\hat{\mathbf{P}}(\mathbf{G})$.

First, given a feasible probabilistic power scheme $\mathbf{P}(\mathbf{G})$, we partition the powers into four non-overlapping power regions as given in (9).

$$\begin{aligned} \mathcal{A}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \{\mathbf{p}(\mathbf{G}) : D(\mathbf{G}, \mathbf{p}(\mathbf{G})) \leq \mathbb{D}, D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) \geq \mathbb{D}_e | \mathbf{G}\} \\ \mathcal{A}_2(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \{\mathbf{p}(\mathbf{G}) : D(\mathbf{G}, \mathbf{p}(\mathbf{G})) \leq \mathbb{D}, D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) < \mathbb{D}_e | \mathbf{G}\} \\ \mathcal{A}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \{\mathbf{p}(\mathbf{G}) : D(\mathbf{G}, \mathbf{p}(\mathbf{G})) > \mathbb{D}, D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) \geq \mathbb{D}_e | \mathbf{G}\} \\ \mathcal{A}_4(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \{\mathbf{p}(\mathbf{G}) : D(\mathbf{G}, \mathbf{p}(\mathbf{G})) > \mathbb{D}, D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) < \mathbb{D}_e | \mathbf{G}\} \quad (9) \end{aligned}$$

The objective is to minimize the distortion outage probability at the FC with the secrecy outage probability at the eavesdropper being less than δ . As $\mathcal{A}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ and $\mathcal{A}_4(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ are power regions where outage occurs at the FC, and both $D(\mathbf{G}, \mathbf{p}(\mathbf{G}))$ and $D_e(\mathbf{G}, \mathbf{p}(\mathbf{G}))$ are convex

functions over $\mathbf{p}(\mathbf{G})$, we can replace the power regions $\mathcal{A}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ and $\mathcal{A}_4(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ by a region where all the powers are set to $\mathbf{0}$, which saves transmit power and does not violate the constraints in problem (6). We denote this new feasible probabilistic power scheme as $\hat{\mathbf{P}}(\mathbf{G})$, which has three non-overlapping power regions for a given \mathbf{G} , namely,

$$\begin{aligned} \mathcal{B}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \mathcal{A}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}), \quad \mathcal{B}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) = \{\mathbf{0}\}, \\ \mathcal{B}_2(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) &= \mathcal{A}_2(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) \end{aligned} \quad (10)$$

with all powers in $\mathcal{B}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ equal to zero.

Any optimal probabilistic power scheme can always be divided into the four non-overlapping regions as defined in (9). As $\mathcal{A}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ and $\mathcal{A}_4(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ are two sets of powers that result in outage at the FC, replacing these two regions with $\mathcal{B}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ would not change the distortion outage probability at the FC, but maintains or even reduces the secrecy outage probability at the eavesdropper. Therefore, we conclude that if a probabilistic power allocation policy is the optimal solution of problem (6), it shares or can be transformed into the same form as $\hat{\mathbf{P}}(\mathbf{G})$.

Next, we construct from $\hat{\mathbf{P}}(\mathbf{G})$ another probabilistic power scheme $\mathbf{P}'(\mathbf{G})$ which randomizes among three deterministic power allocations $\{\mathbf{p}_i(\mathbf{G})\}$ with time-sharing factors $\{\omega_i(\mathbf{G})\}$, i.e.,

$$\mathbf{P}'(\mathbf{G}) = \sum_{i=1}^3 \mathbf{p}_i(\mathbf{G}) \mathbb{1}(X(\mathbf{G}) = i), \quad (11)$$

where $X(\mathbf{G})$ is defined as

$$X(\mathbf{G}) = q, \quad \text{with probability } \omega_q(\mathbf{G}), \quad q = 1, 2, 3. \quad (12)$$

The deterministic power schemes $\{\mathbf{p}_i(\mathbf{G})\}$ are defined by averaging the powers in each of the regions (10), i.e.,

$$\begin{aligned} \mathbf{p}_1(\mathbf{G}) &= \mathbb{E} \left[\hat{\mathbf{P}}(\mathbf{G}) \mid \mathbf{p}(\mathbf{G}) \in \mathcal{B}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}), \mathbf{G} \right], \\ \mathbf{p}_2(\mathbf{G}) &= \mathbb{E} \left[\hat{\mathbf{P}}(\mathbf{G}) \mid \mathbf{p}(\mathbf{G}) \in \mathcal{B}_2(\mathbb{D}, \mathbb{D}_e, \mathbf{G}), \mathbf{G} \right], \\ \mathbf{p}_3(\mathbf{G}) &= \mathbb{E} \left[\hat{\mathbf{P}}(\mathbf{G}) \mid \mathbf{p}(\mathbf{G}) \in \mathcal{B}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G}), \mathbf{G} \right] = \mathbf{0}. \end{aligned} \quad (13)$$

The corresponding weighting functions $\{\omega_i(\mathbf{G})\}$ are defined as the probability of using each deterministic power strategy $\{\mathbf{p}_i(\mathbf{G})\}$, i.e.

$$\omega_q(\mathbf{G}) = \Pr \left[\mathbf{p}(\mathbf{G}) \in \mathcal{B}_q(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) \mid \mathbf{G} \right], \quad q = 1, 2, 3. \quad (14)$$

Remark: Given the fact that all powers in $\mathcal{B}_3(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ are zero, we know that in this case the distortion at both the FC and the eavesdropper has the largest possible value of σ_θ^2 . Furthermore, for a given channel state \mathbf{G} , if $\mathcal{B}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) = \emptyset$, then we must have $\omega_1(\mathbf{G}) = 0$, as there are no powers in $\mathcal{B}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G})$ satisfying $D(\mathbf{G}, \mathbf{p}(\mathbf{G})) \leq \mathbb{D}$ and $D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) \geq \mathbb{D}_e$ simultaneously.

Lemma 1: There exists an optimal solution to problem (6) of the form $\mathbf{P}^*(\mathbf{G}) = \sum_{i=1}^3 \mathbf{p}_i(\mathbf{G}) \mathbb{1}(X(\mathbf{G}) = i)$, where $\{\mathbf{p}_i(\mathbf{G})\}$ and $X(\mathbf{G})$ are respectively defined in (13) and (12), and

- $\omega_1(\mathbf{G}) D_e(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) + \omega_3(\mathbf{G}) D_e(\mathbf{G}, \mathbf{p}_3(\mathbf{G})) - (\omega_1(\mathbf{G}) + \omega_3(\mathbf{G})) \mathbb{D}_e \geq 0$,
- $\omega_1(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) + \omega_2(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_2(\mathbf{G})) - (\omega_1(\mathbf{G}) + \omega_2(\mathbf{G})) \mathbb{D} \leq 0$,
- $\sum_{i=1}^3 \omega_i(\mathbf{G}) = 1$,
- $\mathbb{E}[\omega_2(\mathbf{G})] \leq \delta$,
- $\mathbb{E} \left[\left\langle \sum_{j=1}^3 \omega_j(\mathbf{G}) \mathbf{p}_j(\mathbf{G}) \right\rangle \right] \leq \mathcal{P}_{\text{tot}}$.

We can first show the feasibility of $\mathbf{P}^*(\mathbf{G})$, that is $\mathbf{P}^*(\mathbf{G})$ satisfies the total transmit power constraint and the secrecy outage constraint at the eavesdropper. Next, we employ

Jensen's inequality to show that using $\mathbf{P}^*(\mathbf{G})$ is no worse than using $\mathbf{P}'(\mathbf{G})$. The proof details are omitted.

Applying *Lemma 1*, problem (6) can be reformulated into the another optimization problem, shown as:

$$\begin{aligned} \min_{\{\omega_j(\mathbf{G})\}, \{\mathbf{p}_j(\mathbf{G})\}} \quad & 1 - \mathbb{E}[\omega_1(\mathbf{G}) + \omega_2(\mathbf{G})] \\ \text{s.t.} \quad & \mathbb{E}[\omega_2(\mathbf{G})] \leq \delta, \end{aligned} \quad (15a)$$

$$\mathbb{E}[\langle \omega_1(\mathbf{G}) \mathbf{p}_1(\mathbf{G}) \rangle + \langle \omega_2(\mathbf{G}) \mathbf{p}_2(\mathbf{G}) \rangle] \leq \mathcal{P}_{\text{tot}}, \quad (15b)$$

$$\begin{aligned} \omega_1(\mathbf{G}) D_e(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) - \omega_1(\mathbf{G}) \sigma_\theta^2 + \omega_2(\mathbf{G}) (\mathbb{D}_e - \sigma_\theta^2) \\ \geq \mathbb{D}_e - \sigma_\theta^2, \end{aligned} \quad (15c)$$

$$\begin{aligned} \omega_1(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) + \omega_2(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_2(\mathbf{G})) \\ - (\omega_1(\mathbf{G}) + \omega_2(\mathbf{G})) \mathbb{D} \leq 0, \end{aligned} \quad (15d)$$

$$\omega_1(\mathbf{G}) + \omega_2(\mathbf{G}) \leq 1, \quad (15e)$$

$$0 \leq \omega_j(\mathbf{G}) \leq 1, \quad j = 1, 2. \quad (15f)$$

The functional optimization problem (15) is in general non-convex. Let γ , λ , $\nu_e(\mathbf{G})$, $\nu(\mathbf{G})$, and $s(\mathbf{G})$ denote the nonnegative Lagrange multipliers for the constraints (15a)-(15e) respectively. The generalized Karush-Kuhn-Tucker (KKT) conditions [28] are:

$$\frac{\partial l(\dots)}{\partial p_{jk}^*(\mathbf{G})} \begin{cases} = 0, & p_{jk}^*(\mathbf{G}) > 0 \\ \geq 0, & p_{jk}^*(\mathbf{G}) = 0 \end{cases} \quad k = 1, \dots, K \quad (16)$$

$$\frac{\partial l(\dots)}{\partial \omega_j^*(\mathbf{G})} \begin{cases} = 0, & 0 < \omega_j^*(\mathbf{G}) < 1 \\ \geq 0, & \omega_j^*(\mathbf{G}) = 0 \\ \leq 0, & \omega_j^*(\mathbf{G}) = 1 \end{cases} \quad (17)$$

$$\gamma^* (\mathbb{E}[\omega_2^*(\mathbf{G})] - \delta) = 0, \quad \gamma^* \geq 0, \quad (18)$$

$$\lambda^* \left(\mathbb{E} \left[\left\langle \sum_{j=1}^2 \omega_j^*(\mathbf{G}) \mathbf{p}_j^*(\mathbf{G}) \right\rangle \right] - \mathcal{P}_{\text{tot}} \right) = 0, \quad \lambda^* \geq 0, \quad (19)$$

$$\begin{aligned} \nu_e^*(\mathbf{G}) \left[(\mathbb{D}_e - \sigma_\theta^2) (1 - \omega_2^*(\mathbf{G})) - \omega_1^*(\mathbf{G}) D_e(\mathbf{G}, \mathbf{p}_1^*(\mathbf{G})) \right. \\ \left. + \omega_1^*(\mathbf{G}) \sigma_\theta^2 \right] = 0, \quad \nu_e^*(\mathbf{G}) \geq 0, \end{aligned} \quad (20)$$

$$\begin{aligned} \nu^*(\mathbf{G}) \left[\omega_1^*(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_1^*(\mathbf{G})) + \omega_2^*(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_2^*(\mathbf{G})) \right. \\ \left. - (\omega_1^*(\mathbf{G}) + \omega_2^*(\mathbf{G})) \mathbb{D} \right] = 0, \quad \nu^*(\mathbf{G}) \geq 0, \end{aligned} \quad (21)$$

$$s^*(\mathbf{G}) \left[\omega_1^*(\mathbf{G}) + \omega_2^*(\mathbf{G}) - 1 \right] = 0, \quad s^*(\mathbf{G}) \geq 0, \quad (22)$$

where $\{\mathbf{p}_j^*(\mathbf{G})\}$, $\{\omega_j^*(\mathbf{G})\}$, γ^* , λ^* , $\nu_e^*(\mathbf{G})$, $\nu^*(\mathbf{G})$, $s^*(\mathbf{G})$ are the optimal points, and $l(\dots)$ is defined as

$$\begin{aligned} l(\gamma, \lambda, \nu_e(\mathbf{G}), \nu(\mathbf{G}), s(\mathbf{G}), \{\mathbf{p}_j(\mathbf{G})\}, \{\omega_j(\mathbf{G})\}) \\ = - \sum_{j=1}^2 \omega_j(\mathbf{G}) + \gamma \omega_2(\mathbf{G}) + \lambda \left\langle \sum_{j=1}^2 \omega_j(\mathbf{G}) \mathbf{p}_j(\mathbf{G}) \right\rangle \\ + \nu_e(\mathbf{G}) \left[\omega_1(\mathbf{G}) \sigma_\theta^2 - \omega_1(\mathbf{G}) D_e(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) - \omega_2(\mathbf{G}) (\mathbb{D}_e - \sigma_\theta^2) \right] \\ + \nu(\mathbf{G}) \left[\omega_1(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_1(\mathbf{G})) + \omega_2(\mathbf{G}) D(\mathbf{G}, \mathbf{p}_2(\mathbf{G})) \right. \\ \left. - (\omega_1(\mathbf{G}) + \omega_2(\mathbf{G})) \mathbb{D} \right] + s(\mathbf{G}) \left[\omega_1(\mathbf{G}) + \omega_2(\mathbf{G}) - 1 \right]. \end{aligned} \quad (23)$$

From (16), we know that for any nonnegative $p_{1k}^*(\mathbf{G})$ and $p_{2k}^*(\mathbf{G})$, they must satisfy, respectively,

$$\begin{aligned} \lambda^* \omega_1^*(\mathbf{G}) (\sigma_{\omega_k}^2 + \sigma_\theta^2) - \nu_e^*(\mathbf{G}) \omega_1^*(\mathbf{G}) \frac{\partial D_e(\mathbf{G}, \mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})} \\ + \nu^*(\mathbf{G}) \omega_1^*(\mathbf{G}) \frac{\partial D(\mathbf{G}, \mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})} = 0, \quad k = 1, \dots, K, \end{aligned} \quad (24)$$

and

$$\lambda^* \omega_2^*(\mathbf{G}) (\sigma_{\omega_k}^2 + \sigma_\theta^2) - \nu^*(\mathbf{G}) \omega_2^*(\mathbf{G}) \frac{\partial D(\mathbf{G}, \mathbf{p}_2^*(\mathbf{G}))}{\partial p_{2k}^*(\mathbf{G})} = 0.$$

Furthermore, from (20)-(23) we can obtain the Lagrangian at the optimal points for each channel state \mathbf{G} , and from which we can obtain

$$\frac{\partial l(\dots)}{\partial \omega_1^*(\mathbf{G})} = -1 + \lambda^* \langle \mathbf{p}_1^*(\mathbf{G}) \rangle, \quad (25)$$

and

$$\frac{\partial l(\dots)}{\partial \omega_2^*(\mathbf{G})} = -1 + \lambda^* \langle \mathbf{p}_2^*(\mathbf{G}) \rangle + \gamma^*. \quad (26)$$

Note that if the channel distributions of both the eavesdropper and the FC are continuous, then the events $\lambda^* \langle \mathbf{p}_1^*(\mathbf{G}) \rangle = 1$ or $\lambda^* \langle \mathbf{p}_2^*(\mathbf{G}) \rangle = 1 - \gamma^*$ have zero probability. Thus, from condition (17) and (25)-(26) we obtain the following result:

$$\omega_j^*(\mathbf{G}) = \begin{cases} 1, & \frac{\partial l(\dots)}{\partial \omega_j^*(\mathbf{G})} \leq 0, \\ 0, & \frac{\partial l(\dots)}{\partial \omega_j^*(\mathbf{G})} > 0. \end{cases} \quad j = 1, 2. \quad (27)$$

Remark: From the structure of the power allocation in (11) and (27), we see that for continuous fading channel distributions, the optimal power allocation policies are deterministic.

Theorem 1. Consider the following optimization problems (28) and (29):

$$\begin{aligned} \min_{\mathbf{p}} \langle \mathbf{p}(\mathbf{G}) \rangle \\ \text{s.t. } D_e(\mathbf{G}, \mathbf{p}(\mathbf{G})) \geq \mathbb{D}_e, \quad D(\mathbf{G}, \mathbf{p}(\mathbf{G})) \leq \mathbb{D}, \end{aligned} \quad (28)$$

and

$$\min_{\mathbf{p}} \langle \mathbf{p}(\mathbf{G}) \rangle, \quad \text{s.t. } D(\mathbf{G}, \mathbf{p}(\mathbf{G})) = \mathbb{D}, \quad (29)$$

with optimal solutions $\mathbf{p}_a^*(\mathbf{G})$ and $\mathbf{p}_b^*(\mathbf{G})$ respectively. Then a locally optimal solution to problem (15) is given by:

$$\mathbf{P}^*(\mathbf{G}) = \begin{cases} \mathbf{p}_a^*(\mathbf{G}, \lambda^*), & \text{if } \omega_1^*(\mathbf{G}) = 1 \\ \mathbf{p}_b^*(\mathbf{G}, \lambda^*), & \text{if } \omega_2^*(\mathbf{G}) = 1 \text{ and} \\ & D_e(\mathbf{G}, \mathbf{p}_b^*(\mathbf{G}, \lambda^*)) < \mathbb{D}_e \\ \mathbf{0}, & \text{otherwise.} \end{cases}$$

The proof is omitted to save space.

Remark: We may have no feasible solutions for problem (28), which corresponds to the channel conditions where there are no power allocations satisfying non-outage at both the FC and the eavesdropper, i.e., $\mathcal{B}_1(\mathbb{D}, \mathbb{D}_e, \mathbf{G}) = \emptyset$. In this case, we have $\omega_1^*(\mathbf{G}) = 0$.

IV. PARTIAL CSI

Due to the practical difficulties in obtaining the full channel information of the eavesdropper, in this subsection we will assume that the FC only has statistical knowledge of the eavesdropper. We first explore the power allocation problem that minimises the distortion outage at the FC via the Lagrange multiplier technique. To reduce computational cost we then consider suboptimal power allocation policies.

From the analysis in Section III we notice that the optimal transmit power policies are deterministic if both the FC's and eavesdropper's fading channels have continuous distributions, based on which, in this part of the work we aim to develop deterministic transmit power policies with full knowledge of only the sensor-to-FC channels. Using a similar setup as problem (6), the Lagrangian in the partial CSI case can be constructed as

$$\begin{aligned} l(\mathbf{g}, \nu, \lambda) = \int_{\mathbf{g}} [1 \{D(\mathbf{g}, \mathbf{p}(\mathbf{g})) > \mathbb{D}\} + \lambda \langle \mathbf{p}(\mathbf{g}) \rangle \\ + \nu \int_{\mathbf{g}_e} 1 \{D_e(\mathbf{g}_e, \mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} dF(\mathbf{g}_e)] dF(\mathbf{g}), \end{aligned} \quad (30)$$

where ν and λ are non-negative Lagrange multipliers satisfying $\nu^* (\delta - \Pr[D_e(\mathbf{g}_e, \mathbf{p}^*(\mathbf{g})) < \mathbb{D}_e]) = 0$ and $\lambda^* (\mathcal{P}_{\text{tot}} - \mathbb{E}[\langle \mathbf{p}^*(\mathbf{g}) \rangle]) = 0$ at the optimal point.

To minimize the Lagrangian given in (30), we need to find the optimal power allocation for each channel state at the FC such that $1 \{D(\mathbf{g}, \mathbf{p}(\mathbf{g})) > \mathbb{D}\} + \lambda \langle \mathbf{p}(\mathbf{g}) \rangle + \nu \int_{\mathbf{g}_e} 1 \{D_e(\mathbf{g}_e, \mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} dF(\mathbf{g}_e)$ is minimized.

Lemma 2: Let $\xi(\mathbf{p}(\mathbf{g})) = \lambda \langle \mathbf{p}(\mathbf{g}) \rangle + \nu \int_{\mathbf{g}_e} 1 \{D_e(\mathbf{g}_e, \mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} dF(\mathbf{g}_e)$. Then the optimal $\mathbf{p}^*(\mathbf{g})$ must meet $0 \leq 1 \{D(\mathbf{g}, \mathbf{p}^*(\mathbf{g})) > \mathbb{D}\} + \xi(\mathbf{p}^*(\mathbf{g})) \leq 1$.

The proof is easy to derive and hence is omitted.

In order to minimize $1 \{D(\mathbf{g}, \mathbf{p}(\mathbf{g})) > \mathbb{D}\} + \xi(\mathbf{p}(\mathbf{g}))$, we either obtain $D(\mathbf{g}, \mathbf{p}^*(\mathbf{g})) > \mathbb{D}$ where we declare an outage at the FC, or the distortion at the FC is no larger than \mathbb{D} and so $1 \{D(\mathbf{g}, \mathbf{p}^*(\mathbf{g})) > \mathbb{D}\} = 0$.

Therefore, for a given channel state at the FC, the sensors either choose to forward the information to the FC (with non-outage at the FC achieved) or keep silent. Hence, by applying Lemma 2 we obtain that the optimal power allocation $\mathbf{p}^*(\mathbf{g})$ has the form

$$\mathbf{p}^*(\mathbf{g}) = \begin{cases} \hat{\mathbf{p}}(\mathbf{g}), & \text{if } \xi(\hat{\mathbf{p}}(\mathbf{g})) < 1 \\ \mathbf{0}, & \text{otherwise,} \end{cases} \quad (31)$$

where $\hat{\mathbf{p}}(\mathbf{g})$ is a locally optimal solution of the following problem:

$$\begin{aligned} \min_{\mathbf{p}(\mathbf{g})} \lambda \langle \mathbf{p}(\mathbf{g}) \rangle + \nu \int 1 \{D_e(\mathbf{g}_e, \mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} f(\mathbf{g}_e) d\mathbf{g}_e \\ \text{s.t. } D(\mathbf{g}, \mathbf{p}(\mathbf{g})) \leq \mathbb{D}. \end{aligned} \quad (32)$$

1) *Partial CSI Suboptimal Solution:* Due to the difficulties of explicitly expressing $\int 1 \{D_e(\mathbf{g}_e, \mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} f(\mathbf{g}_e) d\mathbf{g}_e$ and deriving a locally optimal solution to problem (32), which has high computational costs, in this part we look at a suboptimal power allocation scheme based on sensor scheduling.

In a multiple-sensor network, instead of activating all the sensors, we can selectively choose only one sensor with the best channel to forward its measurement to the FC. Let $g_m = \max(g_1, \dots, g_K)$ where m corresponds to the index of the sensor with the largest channel gain. The estimation distortion at the FC and the eavesdropper then become functions depending on g_m and g_{e_m} respectively.

To explicitly illustrate the power policies in this scheme, we will assume that the channel power gains are exponentially distributed at both the FC and the eavesdropper with means $\frac{1}{\lambda}$ and $\frac{1}{\lambda_e}$ respectively. We can then obtain the probability density function of g_m as $K\bar{\lambda} \left(1 - e^{-g_m \bar{\lambda}}\right)^{K-1} e^{-\bar{\lambda} g_m}$, and similarly for g_{e_m} .

Following similar techniques as in Section IV, we obtain the transmit power policy:

$$p^*(g_m) = \begin{cases} \frac{\sigma_{n,m}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D} (\sigma_\theta^2 + \sigma_{\omega,m}^2) - \sigma_\theta^2 \sigma_{\omega,m}^2} \frac{1}{g_m}, & \text{if } g_m > g_{m,th}, \\ 0, & \text{otherwise,} \end{cases}$$

where $g_{m,th}$ satisfies $\nu^* e^{-\frac{D_{th}}{\lambda_e} g_{m,th}} + \frac{P_t \lambda^*}{g_{m,th}} = 1$, with $P_t = \frac{\sigma_{n,m}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D} - \frac{\sigma_\theta^2 \sigma_{\omega,m}^2}{\sigma_\theta^2 + \sigma_{\omega,m}^2}}$ and $D_{th} = \frac{\sigma_{n,m}^2 (\sigma_\theta^2 - \mathbb{D}) [\mathbb{D} (\sigma_\theta^2 + \sigma_{\omega,m}^2) - \sigma_\theta^2 \sigma_{\omega,m}^2]}{\sigma_{n,m}^2 (\sigma_\theta^2 - \mathbb{D}) [\mathbb{D} (\sigma_\theta^2 + \sigma_{\omega,m}^2) - \sigma_\theta^2 \sigma_{\omega,m}^2]}$, and with λ^* and ν^* being the optimal Lagrange multipliers chosen to satisfy the power constraint and secrecy outage constraint at the eavesdropper. In addition, the overall outage probability at the FC can be computed and expressed as

$$\Pr[D(g_m, p^*(g_m)) > \mathbb{D}] = \left(1 - e^{-\frac{g_{m,th}}{\lambda}}\right)^K. \quad (33)$$

V. NUMERICAL RESULTS

We consider a situation with three sensors. For simplicity, we consider the source σ_θ^2 to be distributed as $N(0, 1)$, and all three sensors share the same measurement sensitivity of $\sigma_{\omega,k}^2 = 10^{-3}, \forall k$. We assume that the distances from each sensor to the eavesdropper are 125m, 127m and 129m, whereas it is 125m, 130m and 135m to the FC respectively. Furthermore, we consider the path-loss of the signal power at the FC and the eavesdropper as the free-space path-loss model [29]: $PL = 20 \log_{10}(d) + 20 \log_{10}(f) - 27.55$, where

$d \in \{d_k, d_{e_k}\}$ is the distance between sensor k and the FC or the eavesdropper in meters, and f is the signal frequency in megahertz (we assume the network uses an operation frequency of 800MHz). Then, the channel power gain follows an exponential distribution with mean $10^{-\frac{PL}{10}}$ mW. The maximum acceptable distortion level \mathbb{D} at the FC is set to 0.007 while the required minimum distortion level \mathbb{D}_e at the eavesdropper is 0.01.

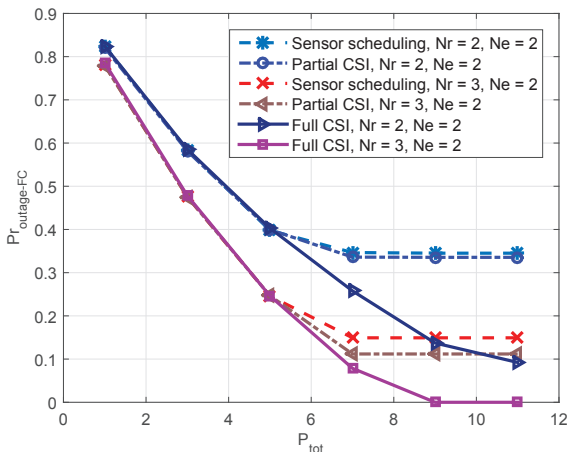


Fig. 2: Performance comparison in a three-sensor network with $N_e = 2$ and $\delta = 0.2$.

In Fig. 2, we compare the distortion outage probability at the FC with the sensor scheduling scheme, partial CSI, and full CSI schemes in a three-sensor network, with the FC having two or three antennas. As we can see, the outage probability at the FC is smaller when the FC is equipped with more antennas for all three cases. Additionally, in Fig. 3, the performance of sensor scheduling closely follows the partial CSI case when the transmit power budget is small. As we keep increasing the power budget, Pr_{outage_FC} settles down to a point at which the secrecy outage constraint is satisfied with equality but the power constraint is loose, since any power increment makes no improvement.

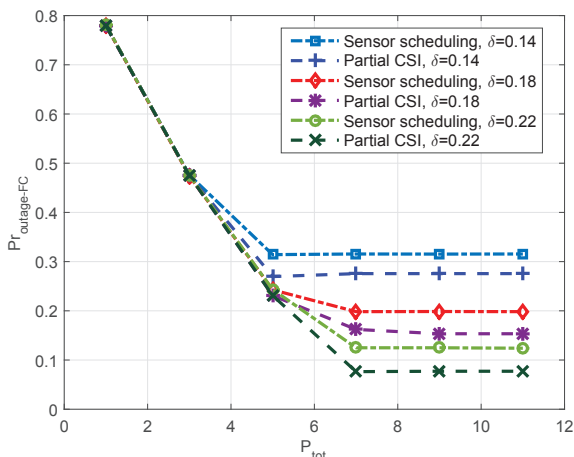


Fig. 3: Performance comparison in a three-sensor network with $N_r = 3$ and $N_e = 2$.

VI. CONCLUSION

In this paper, we have considered the problem of transmit power allocation for distortion outage probability minimization in the presence of an eavesdropper. We studied the distortion outage probability performance for both full CSI and

partial CSI under the multi-sensor single antenna scenario. We proposed a suboptimal solution to overcome the high computational cost in the case of partial CSI. Simulation results showed that better performance can be achieved with additional receive antennas at the FC. In addition, the current work can be extended to the multiple transmit antennas case, where the artificial noise technique [30] can be employed by the sensor to confuse the eavesdropper.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, "Wireless sensor networks: A survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [2] J.-J. Xiao and Z.-Q. Luo, "Decentralized estimation in an inhomogeneous sensing environment," *Information Theory, IEEE Transactions on*, vol. 51, no. 10, pp. 3564–3575, 2005.
- [3] S. Cui, A. Goldsmith, and A. Bahai, "Energy-constrained modulation optimization," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 5, pp. 2349–2360, Sept 2005.
- [4] M. Gastpar and M. Vetterli, "Source-channel communication in sensor networks," in *Information Processing in Sensor Networks*. Springer, 2003, pp. 162–177.
- [5] 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.
- [6] 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.
- [7] —, "Linear coherent decentralized estimation," *Signal Processing, IEEE Transactions on*, vol. 56, no. 2, pp. 757–770, Feb 2008.
- [8] 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.
- [9] 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.
- [10] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *Information Theory, IEEE Transactions on*, vol. 45, no. 5, pp. 1468–1489, 1999.
- [11] R. Negi and J. Cioffi, "Delay-constrained capacity with causal feedback," *Information Theory, IEEE Transactions on*, vol. 48, no. 9, pp. 2478–2494, Sep 2002.
- [12] J. Luo, R. Yates, and P. Spasojevic, "Service outage based power and rate allocation for parallel fading channels," *Information Theory, IEEE Transactions on*, vol. 51, no. 7, pp. 2594–2611, 2005.
- [13] C.-H. Wang and S. Dey, "Power allocation for distortion outage minimization in clustered wireless sensor networks," in *Wireless Communications and Mobile Computing Conference, 2008. IWCMC'08. International*. IEEE, 2008, pp. 395–400.
- [14] —, "Distortion outage minimization in rayleigh fading using limited feedback," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE, 2009, pp. 1–8.
- [15] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [16] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2453–2469, 2008.
- [17] 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.
- [18] 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.
- [19] F. Naghibi, S. Salimi, and M. Skoglund, "The CEO problem with secrecy constraints," in *Information Theory (ISIT), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 756–760.
- [20] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *Information Theory, IEEE Transactions on*, vol. 59, no. 6, pp. 3668–3692, June 2013.
- [21] Y. Kaspi and N. Merhav, "Zero-delay and causal secure source coding," *Information Theory, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.
- [22] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *Signal Processing, IEEE Transactions on*, vol. 59, no. 3, pp. 1202–1216, 2011.
- [23] 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.
- [24] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *Communications, IET*, vol. 6, no. 3, pp. 353–362, 2012.
- [25] X. Guo, A. Leong, and S. Dey, "Power allocation for distortion minimization in distributed estimation with security constraints," in *Signal Processing Advances in Wireless Communications (SPAWC), 2014 IEEE 15th International Workshop on*, June 2014, pp. 299–303.
- [26] S. M. Kay, *Fundamentals of statistical signal processing: Estimation theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.
- [27] D. G. Manolakis, V. K. Ingle, and S. M. Kogon, *Statistical and adaptive signal processing: spectral estimation, signal modeling, adaptive filtering, and array processing*. Artech House Norwood, 2005, vol. 46.
- [28] D. G. Luenberger, *Optimization by vector space methods*. John Wiley & Sons, 1968.
- [29] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
- [30] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, June 2008.