Distortion Outage Minimization in Distributed Estimation with Estimation 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 minimise the distortion outage at the FC, subject to a long-term total transmit power constraint across the sensor(s) 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. Suboptimal power control policies are studied for the partial CSI case in order to reduce the high computational cost associated with large numbers of sensors or receive antennas. Numerical results show that significantly improved performance can be achieved by adding multiple receive antennas at the FC. In the case of multiple transmit antennas, the distortion outage at the FC can be dramatically reduced and in some cases completely eliminated, by transmitting the observations on the null space of the eavesdropper's channel or deploying an artificial noise technique, in full CSI and partial CSI cases respectively.**

***Index Terms*—Distributed estimation, outage probability, fading channels, secrecy outage, 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 centre (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], [5], 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 [6] under certain situations. Deploying this analog-forwarding transmission, the authors in [7] studied the optimal power scheduling problem in an inhomogeneous sensor network; while the power allocation policies for a vector source were investigated in [8]. The diversity order of decentralized estimation in terms of increasing numbers of sensors has also been explored in [9], [10].

In the context of communications and information theory, the idea of *information outage* probability minimization was introduced in [11] for block-fading channels, and has been further extended in e.g. [12], [13]. A similar concept of *estimation outage* probability for distributed estimation was introduced by the authors in [9], which is defined as the probability that the estimation distortion exceeds a certain threshold. With full channel state information, the authors in [14] 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 [15]. In [16], the authors explored the diversity order for distortion outage minimization over coherent multi-access channels. Optimal power allocation for estimation outage probability minimization was also studied in [17] for state estimation of linear dynamical systems.

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 [18]. 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 [19], [20], [21] studied the secrecy capacity in the case of full CSI or partial CSI, and investigated MIMO channels in [22], [23], [24]. Multiterminal source coding or CEO problems with secrecy constraints were also considered in [25], [26], [27], [28]. In particular, in [28], the authors investigated secure lossy source coding in the presence of an eavesdropper who is able to observe the coded information bits and has access to correlated side information. Under these assumptions, the authors derived inner and outer bounds on the achievable rate region. The authors in [29] considered a different scenario where the eavesdropper can obtain the size of the packets, thus parsing the bit stream into separate encrypted messages. Bounds on coding rate and key rate are derived for perfect zero-delay secrecy. However, although such secure source coding techniques enable one to gain information-theoretic insights, it does not

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).

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 [30] 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 [31], [32], [33], [34], where different performance metrics, such as bit-error-rate, signal-interference-to-noise ratio, Ali-Silvey distances or error probability were used to measure secrecy in a system. Related techniques based on cooperating relays, artificial noise generation or beamforming were also implemented in [31], [35], [36], [37] to secure 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 [38] 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 [38], it is more appropriate to maintain a target distortion level throughout the fading 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 multiple-access channel (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:

- 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.
- 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.
- As an alternative to having multiple sensors in a network, the scenario of a single sensor with multiple transmit antennas is investigated. Numerical studies illustrate that in both the full CSI and partial CSI cases, zero outage can be achieved at the FC with a sufficiently large power budget.

The rest of the paper is organised as follows. In Section II we present the system model for a multiple-sensor network and solve the outage minimization problem. In Section III investigate the secrecy outage problem for the multiple-antenna single sensor scenario and study optimal power control policies for both full and partial CSI. In Section IV, alternative problems that can be solved by applying similar techniques are formulated. 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 $\theta[t]$, $t = 0, 1, 2, \ldots$. The measurement $x_k[t]$ received by the kth 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 $\sigma_{\omega k}^2$.

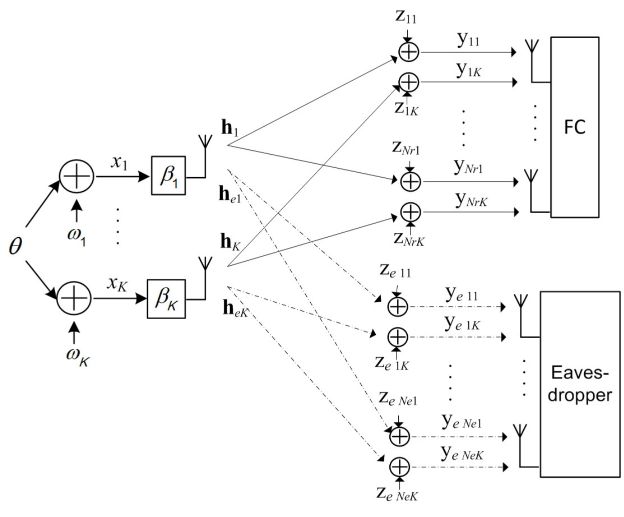

Fig. 1: Diagram of the wireless sensor network using orthogonal MAC scheme with the presence of an eavesdropper.

The sensors are assumed to have a single transmit antenna, see Section III for the case of multiple transmit antennas. Each sensor amplifies and forwards their measurements to a N_r-antenna fusion centre (FC) with amplification factor $\beta_k[t] \in \mathbb{C}$ via a slow-fading orthogonal MAC, e.g. by using OFDMA or TDMA 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 coherence time

[1]This 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 [39].

interval, and are i.i.d. over different time intervals [39]. The signals received by the FC and eavesdropper from the kth 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 $\mathbf{y}_k[t] = [y_{1k}[t], \ldots, y_{N_r k}[t]]^{\mathrm{T}}$ and $\mathbf{y}_{ek}[t] = \left[y_{e1k}[t], \ldots, y_{eN_e k}[t]\right]^{\mathrm{T}}$, 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 σ_{hk}^2 and $\sigma_{h_e k}^2$ respectively, and $\mathbf{z}_k[t] = [z_{1k}[t], \ldots, z_{N_r k}[t]]^{\mathrm{T}}$ and $\mathbf{z}_{ek}[t] = [z_{e1k}[t], \ldots, z_{eN_e k}[t]]^{\mathrm{T}}$ 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 respectively[2]. The set of received signals at the FC from all sensors can be written as

$$\begin{aligned}\mathbf{Y}[t] = &[\mathbf{y}_1[t], \ldots, \mathbf{y}_K[t]]^{\mathrm{T}} \\ =&\theta[t]\left[\beta_1[t]\mathbf{h}_1[t], \ldots, \beta_k[t]\mathbf{h}_k[t]\right]^{\mathrm{T}} + [\mathbf{z}_1[t], \ldots, \mathbf{z}_k[t]]^{\mathrm{T}} \\ &+ \left[\omega_1[t]\beta_1[t]\mathbf{h}_1[t], \ldots, \omega_k[t]\beta_k[t]\mathbf{h}_k[t]\right]^{\mathrm{T}}. \end{aligned} \quad (3)$$

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

$$C[t] = \begin{bmatrix} \sigma_{w1}^2\beta_1^2[t]\mathbf{h}_1[t]\mathbf{h}_1^{\mathrm{H}}[t] + \sigma_1^2\mathbf{I}_{N_r} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \sigma_{wK}^2\beta_K^2[t]\mathbf{h}_K[t]\mathbf{h}_K^{\mathrm{H}}[t] + \sigma_K^2\mathbf{I}_{N_r} \end{bmatrix} \quad (4)$$

The linear minimum mean square error (MMSE) estimator is well known to be the optimal estimator for θ under the model (2) [40]. At time t the mean squared error (MSE) or *distortion* at the FC using the MMSE estimator is

$$\begin{aligned} D[t] =& \left(\frac{1}{\sigma_\theta^2} + \begin{bmatrix} \beta_1[t]\mathbf{h}_1[t] \\ \vdots \\ \beta_K[t]\mathbf{h}_K[t] \end{bmatrix}^{\mathrm{H}} C[t]^{-1} \begin{bmatrix} \beta_1[t]\mathbf{h}_1[t] \\ \vdots \\ \beta_K[t]\mathbf{h}_K[t] \end{bmatrix} \right)^{-1} \\ \overset{(a)}{=}& \Bigg[\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \beta_k^{\mathrm{H}}[t]\beta_k[t] \Big(\sigma_k^{-2}\mathbf{h}_k^{\mathrm{H}}[t]\mathbf{h}_k[t] - \sigma_k^{-2}\mathbf{h}_k^{\mathrm{H}}[t]\mathbf{h}_k[t] \\ & \left(\sigma_{wk}^{-2}\beta_k^{-2}[t] + \sigma_k^{-2}\mathbf{h}_k^{\mathrm{H}}[t]\mathbf{h}_k[t] \right)^{-1} \sigma_k^{-2}\mathbf{h}_k^{\mathrm{H}}[t]\mathbf{h}_k[t] \Big) \Bigg]^{-1} \\ =& \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{g_k[t]p_k[t]}{\sigma_k^2 + g_k[t]\sigma_{wk}^2 p_k[t]} \right)^{-1}, \end{aligned} \quad (5)$$

where (a) results from applying the Matrix Inversion Lemma, $p_k[t] \triangleq \beta_k^{\mathrm{H}}[t]\beta_k[t]$ is the power allocated on the kth sensor, and $g_k[t] \triangleq \mathbf{h}_k^{\mathrm{H}}[t]\mathbf{h}_k[t] = \sum_{m=1}^{N_r} h_{mk}^{\mathrm{H}}[t]h_{mk}[t]$ is the sum of channel power gains from the kth sensor to the FC with $h_{mk}[t]$ being the channel gain from sensor k to mth antenna at the FC. Similarly, the distortion at the eavesdropper is given as:

$$D_e[t] = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{g_{ek}[t]p_k[t]}{g_{ek}[t]p_k[t]\sigma_{\omega k}^2 + \sigma_{ek}^2} \right)^{-1}, \quad (6)$$

where $g_{ek}[t] \triangleq \mathbf{h}_{ek}^{\mathrm{H}}[t]\mathbf{h}_{ek}[t] = \sum_{n=1}^{N_e} h_{enk}^{\mathrm{H}}[t]h_{enk}[t]$ is the sum of channel power gains from the kth sensor to the eavesdropper and $h_{enk}[t]$ is the channel gain from sensor k to nth antenna at the eavesdropper. Note that for a given set of $\{p_k[t]\}$, any $\{\beta_k[t]\}$ satisfying $\beta_k[t]^{\mathrm{H}}\beta_k[t] = p_k[t], \forall k$ would result in the same distortion, hence our primary focus is $\{p_k[t]\}$. Due to the randomness of the fading channels, the instantaneous distortions at the FC and the eavesdropper, as shown in (5) and (6), change over time.

Different from our previous work [38] in which we studied optimal power allocation for an expected 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 $\Pr_{\text{outage\_FC}} \triangleq \Pr\left[D[t] > \mathbb{D}\right]$. 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 $\Pr_{\text{outage\_EVE}} \triangleq \Pr\left[D_e[t] < \mathbb{D}_e\right]$. We assume that the full channel state information (CSI) of the sensor-to-FC channels are available at the FC, while eavesdropper's channel information may or may not be available at the FC. The FC designs the optimal power allocation strategy based on the availability CSI, and then sends $\{p_k[t]\}$ back to the sensors via a secure feedback link.

In this paper, we wish to minimise 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 $\mathbb{E}\left[\sum_{k=1}^{K} p_k \mathbb{E}\left[x_k^2[t]\right]\right] = \mathbb{E}\left[\sum_{k=1}^{K} p_k(\sigma_\theta^2 + \sigma_{\omega k}^2)\right]$, to be less than a power budget $\mathcal{P}_{\text{tot}}$.

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

A. Full CSI

In this section, we assume the FC can also acquire the channel information between the sensors and the eavesdropper. As a result, the power control policies can be derived such that sensors are able to adjust the transmission powers depending on both the FC's and the eavesdropper's channel information. Clearly, the requirement of full CSI of the eavesdropper channels is infeasible in practice. However, the optimal performance with this assumption is instructive as 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 $\mathbf{g} = [g_1, \ldots, g_K]$ and $\mathbf{g}_e = [g_{e1}, \ldots, g_{eK}]$ respectively. The outage minimization problem is

$$\begin{aligned} \min_{\mathbf{P}(\mathbf{G})} \quad & \Pr\left[D\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right) > \mathbb{D}\right] \\ s.t. \quad & \Pr\left[D_e\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right) < \mathbb{D}_e\right] \leq \delta, & (7a) \\ & \mathbb{E}_{\mathbf{G},\mathbf{p}}\left[\langle \mathbf{P}\left(\mathbf{G}\right) \rangle\right] \leq \mathcal{P}_{\text{tot}}, & (7b) \end{aligned}$$

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

Notice that, from the expression of D_e in (6), when zero power is allocated to the sensors we obtain $D_e|_{\mathbf{p}=\mathbf{0}} = \sigma_\theta^2$, giving the largest possible distortion at the eavesdropper,

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

while if the transmit power on each sensor approaches infinity we have the smallest possible distortion at the eavesdropper $D_e \rightarrow \left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{1}{\sigma_{\omega k}^2}\right)^{-1}$. Therefore, in order to produce a meaningful solution to problem (7), $\mathbb{D}_e$ should satisfy $\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{1}{\sigma_{\omega k}^2}\right)^{-1}<\kappa<\mathbb{D}_e<\sigma_\theta^2$, where κ is a nonnegative threshold to ensure constraint (7a) is achievable for a given transmit power budget $\mathcal{P}_{\rm tot}$ and a secrecy outage probability threshold δ.

In communications theory, it was shown in [13], [39] 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,

$$\begin{aligned}&\Pr\left[D\left(\mathbf{G},\mathbf{P}\right)>\mathbb{D}\right]\\&=\iint 1\left\{D\left(\mathbf{G},\mathbf{p}\right)>\mathbb{D}\right\} f_{\mathbf{P}|\mathbf{G}}\left(\mathbf{p}|\,\mathbf{G}\right)d\mathbf{p}\left(\mathbf{G}\right)dF\left(\mathbf{G}\right), \quad (8)\\&\Pr\left[D_e\left(\mathbf{G},\mathbf{P}\right)<\mathbb{D}_e\right]\\&=\iint 1\left\{D_e\left(\mathbf{G},\mathbf{p}\right)<\mathbb{D}_e\right\} f_{\mathbf{P}|\mathbf{G}}\left(\mathbf{p}|\,\mathbf{G}\right)d\mathbf{p}\left(\mathbf{G}\right)dF\left(\mathbf{G}\right). \quad (9)\end{aligned}$$

We outline the strategy involved in solving problem (7), which are similar to techniques used in [13]. 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 randomised 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 (10).

$$\begin{aligned}&\mathcal{A}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\{\mathbf{p}(\mathbf{G}):D(\mathbf{G},\mathbf{p}(\mathbf{G}))\leq\mathbb{D},D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))\geq\mathbb{D}_e|\mathbf{G}\}\\&\mathcal{A}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\{\mathbf{p}(\mathbf{G}):D(\mathbf{G},\mathbf{p}(\mathbf{G}))\leq\mathbb{D},D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))<\mathbb{D}_e|\mathbf{G}\}\\&\mathcal{A}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\{\mathbf{p}(\mathbf{G}):D(\mathbf{G},\mathbf{p}(\mathbf{G}))>\mathbb{D},D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))\geq\mathbb{D}_e|\mathbf{G}\}\\&\mathcal{A}_4(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\{\mathbf{p}(\mathbf{G}):D(\mathbf{G},\mathbf{p}(\mathbf{G}))>\mathbb{D},D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))<\mathbb{D}_e|\mathbf{G}\}\end{aligned} \quad (10)$$

The objective is to minimise 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 (7a) and (7b), 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,

$$\begin{aligned}&\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\mathcal{A}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\quad \mathcal{B}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\{\mathbf{0}\},\\&\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\mathcal{A}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})\end{aligned} \quad (11)$$

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 (10). 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 (7), it 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 randomises among three deterministic power allocations $\{\mathbf{p}_i(\mathbf{G})\}$ with time-sharing factors $\{\omega_i(\mathbf{G})\}$, i.e.,

$$\mathbf{P}'(\mathbf{G})=\sum_{i=1}^{3}\mathbf{p}_i(\mathbf{G})\,1\left(X(\mathbf{G})=i\right), \quad (12)$$

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

$$X(\mathbf{G})=\begin{cases}1, & \text{with probability } \omega_1(\mathbf{G}),\\ 2, & \text{with probability } \omega_2(\mathbf{G}),\\ 3, & \text{with probability } \omega_3(\mathbf{G}).\end{cases} \quad (13)$$

The deterministic power schemes $\{\mathbf{p}_i(\mathbf{G})\}$ are defined by averaging the powers in each of the regions (11), i.e.,

$$\begin{aligned}&\mathbf{p}_1(\mathbf{G})=\mathbb{E}\left[\hat{\mathbf{P}}(\mathbf{G})\middle|\,\mathbf{p}(\mathbf{G})\in\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\mathbf{G}\right],\\&\mathbf{p}_2(\mathbf{G})=\mathbb{E}\left[\hat{\mathbf{P}}(\mathbf{G})\middle|\,\mathbf{p}(\mathbf{G})\in\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\mathbf{G}\right],\\&\mathbf{p}_3(\mathbf{G})=\mathbb{E}\left[\hat{\mathbf{P}}(\mathbf{G})\middle|\,\mathbf{p}(\mathbf{G})\in\mathcal{B}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\mathbf{G}\right]=\mathbf{0}.\end{aligned} \quad (14)$$

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.

$$\begin{aligned}\omega_1(\mathbf{G})=&\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})|\,\mathbf{G}\right],\\\omega_2(\mathbf{G})=&\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})|\,\mathbf{G}\right],\\\omega_3(\mathbf{G})=&\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G})|\,\mathbf{G}\right].\end{aligned} \quad (15)$$

Remark: From the definition of the power regions given in (11), we know that $\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ is a set of transmit powers resulting in non-outage at both the FC and eavesdropper, while $\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ is the region resulting in outage at the eavesdropper and non-outage at the FC. In addition, $\mathcal{B}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ represents the power region leading to outage at the FC and non-outage at the eavesdropper. 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 (7) of the form $\mathbf{P}^*(\mathbf{G})=\sum_{i=1}^{3}\mathbf{p}_i(\mathbf{G})\,1\left(X(\mathbf{G})=i\right)$, where $\{\mathbf{p}_i(\mathbf{G})\}$ and $X(\mathbf{G})$ are respectively defined in (14) and (13), and

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

The proof is given in Appendix A.

Applying *Lemma 1*, problem (7) can be reformulated into another optimization problem, shown as:

$$\min_{\{\omega_j(\mathbf{G})\},\{\mathbf{p}_j(\mathbf{G})\}} \quad 1-\mathbb{E}\left[\omega_1(\mathbf{G})+\omega_2(\mathbf{G})\right]$$

$$\begin{aligned}
s.t.\ & \mathbb{E}\left[\omega_2(\mathbf{G})\right]\le\delta, && (16a)\\
& \mathbb{E}\left[\langle\omega_1(\mathbf{G})\,\mathbf{p}_1(\mathbf{G})\rangle+\langle\omega_2(\mathbf{G})\,\mathbf{p}_2(\mathbf{G})\rangle\right]\le\mathcal{P}_{\text{tot}}, && (16b)\\
& \omega_1(\mathbf{G})\,D_e(\mathbf{G},\mathbf{p}_1(\mathbf{G}))-\omega_1(\mathbf{G})\,\sigma_\theta^2+\omega_2(\mathbf{G})\left(\mathbb{D}_e-\sigma_\theta^2\right) \\
& \qquad\qquad \ge\mathbb{D}_e-\sigma_\theta^2, && (16c)\\
& \omega_1(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_1(\mathbf{G}))+\omega_2(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_2(\mathbf{G})) \\
& \qquad -\left(\omega_1(\mathbf{G})+\omega_2(\mathbf{G})\right)\mathbb{D}\le 0, && (16d)\\
& \omega_1(\mathbf{G})+\omega_2(\mathbf{G})\le 1, && (16e)\\
& 0\le\omega_j(\mathbf{G})\le 1, \qquad j=1,2. && (16f)
\end{aligned}$$

The functional optimization problem (16) 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 (16a)-(16e) respectively. The generalised Karush-Kuhn-Tucker (KKT) conditions [41] are:

$$\frac{\partial l(\dots)}{\partial p_{jk}^*(\mathbf{G})}\begin{cases}=0, & p_{jk}^*(\mathbf{G})>0\\ \ge 0, & p_{jk}^*(\mathbf{G})=0\end{cases}\qquad k=1,\dots,K \tag{17}$$

$$\frac{\partial l(\dots)}{\partial \omega_j^*(\mathbf{G})}\begin{cases}=0, & 0<\omega_j^*(\mathbf{G})<1\\ \ge 0, & \omega_j^*(\mathbf{G})=0\\ \le 0, & \omega_j^*(\mathbf{G})=1\end{cases} \tag{18}$$

$$\gamma^*\left(\mathbb{E}\left[\omega_2^*(\mathbf{G})-\delta\right]\right)=0,\qquad \gamma^*\ge 0, \tag{19}$$

$$\lambda^*\left(\mathbb{E}\left[\left\langle\sum_{j=1}^{2}\omega_j^*(\mathbf{G})\,\mathbf{p}_j^*(\mathbf{G})\right\rangle\right]-\mathcal{P}_{\text{tot}}\right)=0,\qquad \lambda^*\ge 0, \tag{20}$$

$$\begin{aligned}
&\nu_e^*(\mathbf{G})\left[\left(\mathbb{D}_e-\sigma_\theta^2\right)\left(1-\omega_2^*(\mathbf{G})\right)-\omega_1^*(\mathbf{G})\,D_e(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))\right.\\
&\qquad\left.+\omega_1^*(\mathbf{G})\,\sigma_\theta^2\right]=0,\qquad \nu_e^*(\mathbf{G})\ge 0, && (21)\\
&\nu^*(\mathbf{G})\left[\omega_1^*(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))+\omega_2^*(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_2^*(\mathbf{G}))\right.\\
&\qquad\left.-\left(\omega_1^*(\mathbf{G})+\omega_2^*(\mathbf{G})\right)\mathbb{D}\right]=0,\ \ \nu^*(\mathbf{G})\ge 0, && (22)\\
&s^*(\mathbf{G})\left[\omega_1^*(\mathbf{G})+\omega_2^*(\mathbf{G})-1\right]=0,\qquad s^*(\mathbf{G})\ge 0. && (23)
\end{aligned}$$

where γ^*, λ^*, $\nu_e^*(\mathbf{G})$, $\nu^*(\mathbf{G})$, $s^*(\mathbf{G})$ are the optimal Lagrange multipliers, and $\left\{\mathbf{p}_j^*(\mathbf{G})\right\}$ $\left\{\omega_j^*(\mathbf{G})\right\}$ are the optimal primal variables, and $l\left(\gamma,\lambda,\nu_e(\mathbf{G}),\nu(\mathbf{G}),s(\mathbf{G}),\{\mathbf{p}_j(\mathbf{G})\},\{\omega_j(\mathbf{G})\}\right)$ is defined as

$$\begin{aligned}
&l\left(\gamma,\lambda,\nu_e(\mathbf{G}),\nu(\mathbf{G}),s(\mathbf{G}),\{\mathbf{p}_j(\mathbf{G})\},\{\omega_j(\mathbf{G})\}\right)\\
&=-\sum_{j=1}^{2}\omega_j(\mathbf{G})+\gamma\omega_2(\mathbf{G})+\lambda\left\langle\sum_{j=1}^{2}\omega_j(\mathbf{G})\,\mathbf{p}_j(\mathbf{G})\right\rangle\\
&\quad+\nu_e(\mathbf{G})\left[\omega_1(\mathbf{G})\,\sigma_\theta^2-\omega_1(\mathbf{G})\,D_e(\mathbf{G},\mathbf{p}_1(\mathbf{G}))-\omega_2(\mathbf{G})\left(\mathbb{D}_e-\sigma_\theta^2\right)\right]\\
&\quad+\nu(\mathbf{G})\left[\omega_1(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_1(\mathbf{G}))+\omega_2(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_2(\mathbf{G}))\right.\\
&\qquad\left.-\left(\omega_1(\mathbf{G})+\omega_2(\mathbf{G})\right)\mathbb{D}\right]+s(\mathbf{G})\left[\omega_1(\mathbf{G})+\omega_2(\mathbf{G})\right].
\end{aligned} \tag{24}$$

From (17), we know that for any nonnegative $p_{1k}^*(\mathbf{G})$ and $p_{2k}^*(\mathbf{G})$, they must satisfy, respectively,

$$\begin{aligned}
&\lambda^*\omega_1^*(\mathbf{G})\left(\sigma_{\omega k}^2+\sigma_\theta^2\right)-\nu_e^*(\mathbf{G})\,\omega_1^*(\mathbf{G})\,\frac{\partial D_e(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})}\\
&+\nu^*(\mathbf{G})\,\omega_1^*(\mathbf{G})\,\frac{\partial D(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})}=0,\quad k=1,\dots,K,
\end{aligned} \tag{25}$$

and

$$\lambda^*\omega_2^*(\mathbf{G})\left(\sigma_{\omega k}^2+\sigma_\theta^2\right)-\nu^*(\mathbf{G})\,\omega_2^*(\mathbf{G})\,\frac{\partial D(\mathbf{G},\mathbf{p}_2^*(\mathbf{G}))}{\partial p_{2k}^*(\mathbf{G})}=0. \tag{26}$$

Furthermore, from (21)-(24) we can obtain the Lagrangian at the optimal points for each channel state $\mathbf{G}$ as

$$\begin{aligned}
&l\left(\gamma^*,\lambda^*,\nu_e^*(\mathbf{G}),s^*(\mathbf{G}),\{\mathbf{p}_j^*(\mathbf{G})\},\{\omega_j^*(\mathbf{G})\}\right)\\
&=-\sum_{j=1}^{2}\omega_j^*(\mathbf{G})+\gamma^*\omega_2^*(\mathbf{G})+\lambda^*\left\langle\sum_{j=1}^{2}\omega_j^*(\mathbf{G})\,\mathbf{p}_j^*(\mathbf{G})\right\rangle\\
&\quad-\nu_e^*(\mathbf{G})\left(\mathbb{D}_e-\sigma_\theta^2\right)+s^*(\mathbf{G}),
\end{aligned} \tag{27}$$

from which we can obtain

$$\frac{\partial l(\dots)}{\partial\omega_1^*(\mathbf{G})}=-1+\lambda^*\langle\mathbf{p}_1^*(\mathbf{G})\rangle, \tag{28}$$

and

$$\frac{\partial l(\dots)}{\partial\omega_2^*(\mathbf{G})}=-1+\lambda^*\langle\mathbf{p}_2^*(\mathbf{G})\rangle+\gamma^*. \tag{29}$$

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 (18) and (28)-(29) we obtain the following result:

$$\omega_j^*(\mathbf{G})=\begin{cases}1, & \frac{\partial l(\dots)}{\partial\omega_j^*(\mathbf{G})}\le 0,\\ 0, & \frac{\partial l(\dots)}{\partial\omega_j^*(\mathbf{G})}>0.\end{cases}\qquad j=1,2. \tag{30}$$

Remark: From the structure of the power allocation in (12) and (30), we see that for continuous fading channel distributions, the optimal power allocation policies are deterministic.

Theorem 1. *Consider the following optimization problems* (31) *and* (32)*:*

$$\min_{\boldsymbol{p}}\ \langle\boldsymbol{p}(\boldsymbol{G})\rangle \quad s.t.\ D_e(\boldsymbol{G},\boldsymbol{p}(\boldsymbol{G}))\ge\mathbb{D}_e,\quad D(\boldsymbol{G},\boldsymbol{p}(\boldsymbol{G}))\le\mathbb{D}, \tag{31}$$

and

$$\min_{\boldsymbol{p}}\ \langle\boldsymbol{p}(\boldsymbol{G})\rangle,\quad s.t.\ D(\boldsymbol{G},\boldsymbol{p}(\boldsymbol{G}))=\mathbb{D}, \tag{32}$$

with optimal solutions $\boldsymbol{p}_a^*(\boldsymbol{G})$ *and* $\boldsymbol{p}_b^*(\boldsymbol{G})$ *respectively. Then a locally optimal solution to problem* (16) *is given by:*

$$\boldsymbol{P}^*(\boldsymbol{G})=\begin{cases}\boldsymbol{p}_a^*(\boldsymbol{G}), & \text{if}\ \ \omega_1^*(\boldsymbol{G})=1\\ \boldsymbol{p}_b^*(\boldsymbol{G}), & \text{if}\ \ \omega_2^*(\boldsymbol{G})=1\ \text{and}\\ & \quad D_e(\boldsymbol{G},\boldsymbol{p}_b^*(\boldsymbol{G}))<\mathbb{D}_e\\ \boldsymbol{0}, & \text{otherwise}.\end{cases} \tag{33}$$

The proof is given in Appendix B.

Remark: We may have no feasible solutions for problem (31), 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 $\omega_1^*(\mathbf{G})=0$.

Consider the channel states where problem (31) has solution $\mathbf{p}_a^*(\mathbf{G})$, and $\mathbf{p}_b^*(\mathbf{G})$ satisfying $D_e(\mathbf{G},\mathbf{p}_b^*(\mathbf{G}))<\mathbb{D}_e$. As both $D(\mathbf{G},\mathbf{p}(\mathbf{G}))$ and $D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))$ are convex over $\mathbf{p}(\mathbf{G})$, we obtain $D(\mathbf{G},\mathbf{p}_a^*(\mathbf{G},))=\mathbb{D}$ and $D_e(\mathbf{G},\mathbf{p}_a^*(\mathbf{G}))=\mathbb{D}_e$, and $\langle\mathbf{p}_a^*(\mathbf{G})\rangle\ge\langle\mathbf{p}_b^*(\mathbf{G})\rangle$ since problem (31) has a smaller feasible region than problem (32). As a consequence, there is a trade off between choosing $\mathbf{p}_a^*(\mathbf{G})$ or $\mathbf{p}_b^*(\mathbf{G})$ to transmit at each channel instance; $\mathbf{p}_a^*(\mathbf{G})$ leads to non-outage at both the FC and the eavesdropper, whereas $\mathbf{p}_b^*(\mathbf{G})$ results in outage at the eavesdropper but consumes less power.

Define a non-negative transmit power difference $p_{\text{diff}}(\mathbf{G})=\langle\mathbf{p}_a^*(\mathbf{G})\rangle-\langle\mathbf{p}_b^*(\mathbf{G})\rangle$. We may then further categorise the power transmission policy into two different types, depending on the given secrecy outage probability threshold δ and power budget $\mathcal{P}_{\text{tot}}$.

- When $\lambda^* p_{\text{diff}}(\mathbf{G}) \geq \gamma^*$, we obtain either $\mathbf{P}^*(\mathbf{G}) = \mathbf{p}_b^*(\mathbf{G})$ or $\mathbf{P}^*(\mathbf{G}) = \mathbf{0}$. In these channel states, the transmission policies are chosen to use less transmit power by sacrificing either an outage at the eavesdropper, i.e., to use $\mathbf{p}_b^*(\mathbf{G})$, or not transmit leading to an outage at the FC. By doing this, transmit power can be saved for future 'higher potential' channel states where outage occurs neither at the FC nor at the eavesdropper. Furthermore, when $\gamma^* = 0$, from (18) we have $\mathbb{E}[\omega_2^*(\mathbf{G})] \leq \delta$, which indicates that we either have a small total power budget or a loose security requirement at the eavesdropper, i.e., a large δ. Intuitively, the optimal transmit policy under such circumstances should be more energy conservative and aim to meet the maximum acceptable distortion level $\mathbb{D}$ at the FC.
- When $\lambda^* p_{\text{diff}}(\mathbf{G}) < \gamma^*$, which implies that either $\langle \mathbf{p}_a^*(\mathbf{G})\rangle$ is fairly close to $\langle \mathbf{p}_b^*(\mathbf{G})\rangle$ or we have a relatively small λ^*, we should have $\mathbf{P}^*(\mathbf{G}) = \mathbf{p}_a^*(\mathbf{G})$ or $\mathbf{P}^*(\mathbf{G}) = \mathbf{0}$. When $p_{\text{diff}}(\mathbf{G})$ is small or the transmit power budget is large, instead of using $\mathbf{p}_b^*(\mathbf{G})$, which would result in outage at the eavesdropper, using $\mathbf{p}_a^*(\mathbf{G})$ guarantees non-outage at both the FC and the eavesdropper. If the incremental power $p_{\text{diff}}(\mathbf{G})$ is too large, the sensors will stop transmitting to save power.

B. 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 long-term distortion at the FC via the Lagrange multiplier technique. To reduce computational cost we then consider suboptimal power allocation policies.

From the analysis in Section II-A 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 (7), the Lagrangian in the partial CSI case can be constructed as

$$l(\mathbf{g},\nu,\lambda) = \int_{\mathbf{g}} \Big[1\{D(\mathbf{g},\mathbf{p}(\mathbf{g})) > \mathbb{D}\} + \lambda \langle \mathbf{p}(\mathbf{g})\rangle + \nu \int_{\mathbf{g}_e} 1\{D_e(\mathbf{g}_e,\mathbf{p}(\mathbf{g})) < \mathbb{D}_e\}\, dF(\mathbf{g}_e) \Big] dF(\mathbf{g}), \quad (34)$$

where λ and ν are non-negative Lagrange multipliers satisfying the following equations at the optimal point:

$$\begin{aligned} &\lambda^* \left(\mathcal{P}_{\text{tot}} - \mathbb{E}[\langle \mathbf{p}^*(\mathbf{g})\rangle]\right) = 0, \\ &\nu^* \left(\delta - \Pr[D_e(\mathbf{g}_e, \mathbf{p}^*(\mathbf{g})) < \mathbb{D}_e]\right) = 0. \end{aligned} \quad (35)$$

To minimise the Lagrangian given in (34), 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 minimised.

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 satisfy $0 \leq 1\{D(\mathbf{g},\mathbf{p}^*(\mathbf{g})) > \mathbb{D}\} + \xi(\mathbf{p}^*(\mathbf{g})) \leq 1$.

The proof is given in Appendix C.

In order to minimise $1\{D(\mathbf{g},\mathbf{p}(\mathbf{g})) > \mathbb{D}\} + \xi(\mathbf{p}(\mathbf{g}))$, 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 $1\{D(\mathbf{g},\mathbf{p}^*(\mathbf{g})) > \mathbb{D}\} = 0$. To be more specific,

- When $D(\mathbf{g},\mathbf{p}^*(\mathbf{g})) > \mathbb{D}$, we see that $1\{D(\mathbf{g},\mathbf{p}^*(\mathbf{g})) > \mathbb{D}\} = 1$ indicates an outage at the FC. Furthermore, we must have the optimal power allocation at this channel instant being equal to zero for all sensors, since a non-zero power would result in a nonnegative value of $\lambda \langle \mathbf{p}^*(\mathbf{g})\rangle + \nu \int 1\{D_e(\mathbf{g}_e,\mathbf{p}^*(\mathbf{g})) < \mathbb{D}_e\} f(\mathbf{g}_e)\, d\mathbf{g}_e$. Intuitively, knowing that an outage will happen at the FC, the sensors would stop transmitting to save power and to reduce the possibility of information being leaked to the eavesdropper.
- When $D(\mathbf{g},\mathbf{p}^*(\mathbf{g})) \leq \mathbb{D}$, which implies non-outage at the FC. In this situation, either the FC has relatively good channel conditions that a small amount of power would secure non-outage at the FC, or the constraints are quite loose (i.e. a large power budget and/or a loose security requirement at the eavesdropper).

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

$$\mathbf{p}^*(\mathbf{g}) = \begin{cases} \hat{\mathbf{p}}(\mathbf{g}), & \text{if } \ \xi(\hat{\mathbf{p}}(\mathbf{g})) < 1 \\ \mathbf{0}, & \text{otherwise}, \end{cases} \quad (36)$$

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

$$\begin{aligned} \min_{\mathbf{p}(\mathbf{g})} \ & \lambda \langle \mathbf{p}(\mathbf{g})\rangle + \nu \int 1\{D_e(\mathbf{g}_e,\mathbf{p}(\mathbf{g})) < \mathbb{D}_e\} f(\mathbf{g}_e)\, d\mathbf{g}_e \\ s.t. \ & D(\mathbf{g},\mathbf{p}(\mathbf{g})) \leq \mathbb{D}. \end{aligned} \quad (37)$$

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 (37), which has high computational costs, in this part we will look at a suboptimal power allocation scheme based on sensor scheduling.

In a multiple-sensor system, instead of activating all the sensors, we can selectively choose one sensor to forward its measurement to the FC. This may be useful in scenarios where bandwidth is at a premium or there are very strict interference constraints. Let $g_m = \max(g_1,\ldots,g_K)$, and $g_{em} = \max(g_{e1},\ldots,g_{eK})$ where m corresponds to the index of the sensor with the largest channel gain. One possible sensor scheduling policy is that only the sensor with the best channel transmits. The distortion at the FC and the eavesdropper then become:

$$D = \left(\frac{1}{\sigma_\theta^2} + \frac{g_m p_m}{g_m p_m \sigma_{\omega m}^2 + \sigma_{nm}^2}\right)^{-1}, \quad (38a)$$

$$D_e = \left(\frac{1}{\sigma_\theta^2} + \frac{g_{em} p_m}{g_{em} p_m \sigma_{\omega m}^2 + \sigma_{em}^2}\right)^{-1}. \quad (38b)$$

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 $\frac{1}{\bar{\lambda}}$ and $\frac{1}{\bar{\lambda}_e}$ 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_{em}.

Following similar techniques as in Section II-B, problem

(37) is then reduced to

$$\min_{p(g_m)} \quad \lambda \langle p(g_m) \rangle + \nu \int 1\{D_e(g_{em}, p(g_m)) < \mathbb{D}_e\} \, dF(g_{em})$$
$$s.t. \quad D(g_m, p(g_m)) \le \mathbb{D}, \tag{39}$$

from which we can then compute the optimal solution as

$$\hat{p}(g_m) = \frac{\sigma_{nm}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D}(\sigma_\theta^2 + \sigma_{\omega m}^2) - \sigma_\theta^2 \sigma_{\omega m}^2} \frac{1}{g_m}. \tag{40}$$

Knowing that the eavesdropper's channel is exponentially distributed, we can derive the outage probability at the eavesdropper for a given FC channel state as

$$\begin{aligned} &\Pr\left[D_e(g_{em}, \hat{p}(g_m)) < \mathbb{D}_e \,|\, g_m\right] \\ =&1 - \Pr\left[g_{em} \le \frac{\sigma_{em}^2 (\sigma_\theta^2 - \mathbb{D}_e)}{\mathbb{D}_e \sigma_{\omega m}^2 - \sigma_\theta^2 (\sigma_{\omega m}^2 - \mathbb{D}_e)} \frac{1}{\hat{p}(g_m)} \middle| \, g_m \right] \\ =&e^{-\frac{D_{\text{th}}}{\lambda_e} g_m}, \end{aligned} \tag{41}$$

where $D_{\text{th}} = \frac{\sigma_{em}^2}{\sigma_{nm}^2} \frac{(\sigma_\theta^2 - \mathbb{D}_e)[\mathbb{D}(\sigma_\theta^2 + \sigma_{\omega m}^2) - \sigma_\theta^2 \sigma_{\omega m}^2]}{(\sigma_\theta^2 - \mathbb{D})[\mathbb{D}_e(\sigma_\theta^2 + \sigma_{\omega m}^2) - \sigma_\theta^2 \sigma_{\omega m}^2]}$.

Combining the results of (36), (40) and (41) we obtain the transmit power policy:

$$p^*(g_m) = \begin{cases} \frac{\sigma_{nm}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D}(\sigma_\theta^2 + \sigma_{\omega m}^2) - \sigma_\theta^2 \sigma_{\omega m}^2} \frac{1}{g_m}, & \text{if } g_m > g_{m\_th}, \\ 0, & \text{otherwise}, \end{cases} \tag{42}$$

where g_{m_th} satisfies $\nu^* e^{-\frac{D_{\text{th}}}{\lambda_e} g_{m\_th}} + \frac{P_{\text{t}} \lambda^*}{g_{m\_th}} = 1$, with $P_{\text{t}} = \frac{\sigma_{nm}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D} - \frac{\sigma_\theta^2 \sigma_{\omega m}^2}{\sigma_\theta^2 + \sigma_{\omega m}^2}}$, and with λ^* and ν^* being the optimal Lagrange multipliers chosen to satisfy the power constraint and secrecy outage constraint at the eavesdropper.

Notice that as g_m is continuous and $\nu^* e^{-\frac{D_{\text{th}}}{\lambda_e} g_m} + \frac{P_{\text{t}} \lambda^*}{g_m}$ is monotonic decreasing with g_m, we obtain the 'on-off' transmit power policy in (42), where if $g_m > g_{m\_th}$ the sensor uses $\hat{p}(g_m)$ to transmit with non-outage at the FC achieved, and the sensor does not transmit when $g_m \le g_{m\_th}$ which leads to an outage to occur at the FC. In addition, the overall outage probability at the FC can be expressed as

$$\begin{aligned} &\Pr\left[D(g_m, p^*(g_m)) > \mathbb{D}\right] \\ =&\frac{K}{\lambda} \int_0^{g_{m\_th}} \left(1 - e^{-\frac{g_m}{\lambda}}\right)^{K-1} e^{-\frac{g_m}{\lambda}} dg_m = \left(1 - e^{-\frac{g_{m\_th}}{\lambda}}\right)^K. \end{aligned}$$

From (41) and (42), which are two monotonic decreasing functions with respect to g_m, we obtain that $g_{m\_th}(\lambda^*, \nu^*)$ must satisfy either $\int_{g_{m\_th}(\lambda^*, \nu^*)}^{\infty} e^{-\frac{D_{\text{th}}}{\lambda_e} g_m} f(g_m) dg_m = \delta$ or $\frac{\sigma_{nm}^2 (\sigma_\theta^2 - \mathbb{D})}{\mathbb{D}(\sigma_\theta^2 + \sigma_{\omega m}^2) - \sigma_\theta^2 \sigma_{\omega m}^2} \int_{g_{m\_th}(\lambda^*, \nu^*)}^{\infty} \frac{1}{g_m} f(g_m) dg_m = \mathcal{P}_{\text{tot}}$, where $f(g_m) = \frac{K}{\lambda} \left(1 - e^{-\frac{g_m}{\lambda}}\right)^{K-1} e^{-\frac{g_m}{\lambda}}$. This is because for a given total power budget and outage probability threshold at the eavesdropper, there is zero probability of finding a g_{m_th} to meet both constraints with equality. From the KKT conditions for the optimal points we then derive that either

$$P_t \int_{P_t \lambda^*}^{\infty} \frac{1}{g_m} f(g_m) dg_m = \mathcal{P}_{\text{tot}}, \quad \nu^* = 0, \tag{43}$$

or

$$\int_{\frac{\lambda_e log \nu^*}{D_{\text{th}}}}^{\infty} e^{-\frac{D_{\text{th}}}{\lambda_e} g_m} f(g_m) dg_m = \delta, \quad \lambda^* = 0. \tag{44}$$

III. Single Sensor with Multiple Antennas Scenario

In order to compare with the multiple-sensor scenario as well as for analytical tractability, in this part of work we consider a situation where only one sensor with multiple-antenna is in the network observing the source.[3] In this scenario, similar performance gains as in having multiple sensors can be achieved. In fact, with multiple antennas additional techniques can be used to further enhance the system performance. In this section, we investigate the multiple-antenna single sensor system.

A schematic diagram is shown in Fig. 2. We assume that the same single point Gaussian source θ as defined in Section II is observed by a sensor with N_t transmit antennas, which employs the analog amplify and forward technique to scale the observed signal with a complex vector $\boldsymbol{\beta} \in \mathbb{C}^{N_t \times 1}$, before sending it to the FC via a set of complex fading channels $\mathbf{H} \in \mathbb{C}^{Nr \times Nt}$. The observed signal x is also listened to by the eavesdropper after passing through another set of channels $\mathbf{H}_e \in \mathbb{C}^{Ne \times Nt}$, where we assume that the FC and the eavesdropper are equipped with N_r and N_e receive antennas respectively.

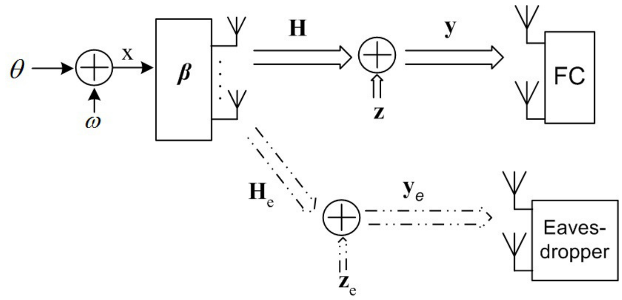

Fig. 2: Diagram of a single sensor multiple-antenna scenario with the presence of an eavesdropper.

The signals received by the FC and the eavesdropper are, respectively,

$$\mathbf{y} = \mathbf{H}\boldsymbol{\beta}\theta + \mathbf{H}\boldsymbol{\beta}\omega + \mathbf{z}, \tag{45a}$$
$$\mathbf{y}_e = \mathbf{H}_e\boldsymbol{\beta}\theta + \mathbf{H}_e\boldsymbol{\beta}\omega + \mathbf{z}_e, \tag{45b}$$

where both $\mathbf{z} \in \mathbb{C}^{Nr \times 1}$ and $\mathbf{z}_e \in \mathbb{C}^{Ne \times 1}$ are complex Gaussian channel noise at the FC and the eavesdropper with covariance $\sigma^2 \mathbf{I}_{N_r}$ and $\sigma_e^2 \mathbf{I}_{N_e}$ respectively.

The optimal linear minimum mean square error (MMSE) estimator, is used at both the FC and the adversary to measure θ. For a given channel instance, the distortion D at the FC can be obtained as

$$\begin{aligned} D =& \left(\frac{1}{\sigma_\theta^2} + (\mathbf{H}\boldsymbol{\beta})^{\text{H}} \Sigma^{-1} \mathbf{H}\boldsymbol{\beta}\right)^{-1}, \\ \overset{(b)}{=}& \sigma_\theta^2 \left(1 - (\mathbf{H}\boldsymbol{\beta})^{\text{H}} \left[\mathbf{H}\boldsymbol{\beta}(\mathbf{H}\boldsymbol{\beta})^{\text{H}} (\sigma_\theta^2 + \sigma_\omega^2) + \sigma^2 \mathbf{I}_{N_r}\right]^{-1} \mathbf{H}\boldsymbol{\beta}\sigma_\theta^2\right), \\ \overset{(c)}{=}& \sigma_\theta^2 \left[1 - \frac{\sigma_\theta^2}{\sigma_\theta^2 + \sigma_\omega^2} \left(1 - \frac{\alpha}{\alpha + (\mathbf{H}\boldsymbol{\beta})^{\text{H}} \mathbf{H}\boldsymbol{\beta}}\right)\right], \end{aligned} \tag{46}$$

where $\Sigma \triangleq \mathbf{H}\boldsymbol{\beta}(\mathbf{H}\boldsymbol{\beta})^{\text{H}} \sigma_\omega^2 + \sigma^2 \mathbf{I}_{N_r}$ is the covariance matrix of $\mathbf{H}\boldsymbol{\beta}\omega + \mathbf{z}$, $\alpha \triangleq \frac{\sigma^2}{\sigma_\omega^2 + \sigma_\theta^2}$, and (b)-(c) result from applying the Matrix Inversion Lemma. Similarly, the mean squared error (MSE) or *distortion* at the eavesdropper is given as

$$D_e = \sigma_\theta^2 \left[1 - \frac{\sigma_\theta^2}{\sigma_\theta^2 + \sigma_\omega^2} \left(1 - \frac{\alpha_e}{\alpha_e + (\mathbf{H}_e\boldsymbol{\beta})^{\text{H}} \mathbf{H}_e\boldsymbol{\beta}}\right)\right], \tag{47}$$

where $\alpha_e \triangleq \frac{\sigma_e^2}{\sigma_\omega^2 + \sigma_\theta^2}$.

[3] Multiple-sensor-multiple-antenna (MSMA) is not studied in the work due to its complexity involving non-convex optimization problems and will be investigated in future work. However, techniques that are explored in the partial CSI case of this section can be also implemented in MSMA case.

We set a maximum acceptable distortion level $\mathbb{D}$ at the FC and define *the distortion outage probability* as

$$\Pr_{\text{outage\_FC}} = \Pr\left[D > \mathbb{D}\right] = \Pr\left[\frac{1}{(\mathbf{H}\boldsymbol{\beta})^{\text{H}}\mathbf{H}\boldsymbol{\beta}} > \mathbb{S}\right], \quad (48)$$

where $\mathbb{S} \triangleq \frac{\sigma_\omega^2+\sigma_\theta^2}{\sigma^2}\left[\frac{\sigma^4}{\sigma^4-\mathbb{D}\left(\sigma_\omega^2+\sigma_\theta^2\right)+\sigma_\omega^2\sigma_\theta^2}-1\right]$. We also set a minimum acceptable distortion level $\mathbb{D}_e$ at the eavesdropper and assume that if $D_e < \mathbb{D}_e$ the measurement information at this channel instance can be successfully retrieved by the eavesdropper leading to a security breach. Letting $\mathbb{S}_e \triangleq \frac{\sigma_\omega^2+\sigma_\theta^2}{\sigma_e^2}\left[\frac{\sigma_e^4}{\sigma_e^4-\mathbb{D}_e\left(\sigma_\omega^2+\sigma_\theta^2\right)+\sigma_\omega^2\sigma_\theta^2}-1\right]$, the *secrecy outage probability* at the eavesdropper can be expressed as

$$\Pr_{\text{outage\_EVE}} = \Pr\left[D_e < \mathbb{D}_e\right] = \Pr\left[\frac{1}{(\mathbf{H}_e\boldsymbol{\beta})^{\text{H}}\mathbf{H}_e\boldsymbol{\beta}} < \mathbb{S}_e\right].$$

With a given power budget at the sensor, our objective is to minimise the distortion outage probability at the FC, while keeping the secrecy outage probability at the eavesdropper below δ. Hence the optimization problem can be cast as:

$$\begin{aligned}\min_{\boldsymbol{\beta}} \quad & \Pr\left[\frac{1}{(\mathbf{H}\boldsymbol{\beta})^{\text{H}}\mathbf{H}\boldsymbol{\beta}} > \mathbb{S}\right] \\ s.t. \quad & \Pr\left[\frac{1}{(\mathbf{H}_e\boldsymbol{\beta})^{\text{H}}\mathbf{H}_e\boldsymbol{\beta}} < \mathbb{S}_e\right] \le \delta, \quad \mathbb{E}\left[\boldsymbol{\beta}^{\text{H}}\boldsymbol{\beta}\right] \le \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}.\end{aligned} \quad (49)$$

In the following, we focus on the full CSI scenario where both the FC and eavesdropper's channel information are available, and the partial CSI scenario where we assume only the FC's channel states are perfectly known. In both scenarios, we first focus on finding the best $\boldsymbol{\beta}$ that minimises the objective while satisfying all the constraints. We then consider other techniques that can be used in the multiple-antenna systems to further enhance the performance.

A. Full CSI

With full knowledge of the eavesdropper's channel information, problem (49) can be solved using similar techniques as in Section II-A, where we start from an arbitrary feasible probabilistic power allocation scheme, from which it can be used to construct another feasible power allocation scheme that provides no worse performance, and based on which we construct three deterministic schemes $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$, and $\boldsymbol{\beta}_3 = \mathbf{0}$. We then show that the optimal $\boldsymbol{\beta}^*$, which is a function of $\mathbf{H}$ and $\mathbf{H}_e$, can be found by considering a probabilistic power allocation scheme that randomises among the three deterministic schemes $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$, and $\boldsymbol{\beta}_3$ with corresponding weighting factors $\{\omega_i\}_{i=1}^3$. The problem (49) then becomes

$$\min_{\{\boldsymbol{\beta}_j(\mathbf{H},\mathbf{H}_e)\},\ \{\omega_j(\mathbf{H},\mathbf{H}_e)\}} \quad 1-\mathbb{E}\left[\omega_1+\omega_2\right]$$

$$s.t.\ \mathbb{E}\left[\omega_2\right] \le \delta, \quad (50a)$$

$$\mathbb{E}\left[\sum_{j=1}^{2}\omega_j\boldsymbol{\beta}_j^{\text{H}}\boldsymbol{\beta}_j\right] \le \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}, \quad (50b)$$

$$\frac{\omega_1}{(\mathbf{H}_e\boldsymbol{\beta}_1)^{\text{H}}\mathbf{H}_e\boldsymbol{\beta}_1} \ge (1-\omega_2)\,\mathbb{S}_e, \quad (50c)$$

$$\frac{\omega_1}{(\mathbf{H}\boldsymbol{\beta}_1)^{\text{H}}\mathbf{H}\boldsymbol{\beta}_1} + \frac{\omega_2}{(\mathbf{H}\boldsymbol{\beta}_2)^{\text{H}}\mathbf{H}\boldsymbol{\beta}_2} \le (\omega_1+\omega_2)\,\mathbb{S}, \quad (50d)$$

$$0 \le \omega_1+\omega_2 \le 1, \quad 0 \le \omega_1,\omega_2 \le 1, \quad (50e)$$

where the derivation is similar to that of problem (16) and is thus omitted to avoid repetition. As problem (50) is again a non-convex problem the result we derive is a locally optimal solution. With the assumption that both $\mathbf{H}$ and $\mathbf{H}_e$ are continuously distributed, the solution of problem (49) in the case of full CSI is given as

$$\boldsymbol{\beta}^*(\mathbf{H},\mathbf{H}_e) = \begin{cases} \boldsymbol{\beta}_1^*(\mathbf{H},\mathbf{H}_e), & \text{if } \lambda^*\boldsymbol{\beta}_1^{*\text{H}}\boldsymbol{\beta}_1^* \le 1, \\ \boldsymbol{\beta}_2^*(\mathbf{H},\mathbf{H}_e), & \text{if } \lambda^*\boldsymbol{\beta}_2^{*\text{H}}\boldsymbol{\beta}_2^* \le 1-\gamma^* \text{ and} \\ & \quad (\mathbf{H}_e\boldsymbol{\beta}_2^*)^{\text{H}}\mathbf{H}_e\boldsymbol{\beta}_2^* > \mathbb{S}_e^{-1} \\ \mathbf{0}, & \text{otherwise}, \end{cases} \quad (51)$$

where λ^* and $\gamma^*(\mathbf{H},\mathbf{H}_e)$ are the optimal Lagrange multipliers chosen to satisfy the constraints $\mathbb{E}\left[\sum_{j=1}^{2}\omega_j^*\boldsymbol{\beta}_j^{\text{H}*}\boldsymbol{\beta}_j^*\right] \le \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}$ and $\mathbb{E}\left[\omega_2^*\right] \le \delta$ respectively; and $\boldsymbol{\beta}_1^*$ and $\boldsymbol{\beta}_2^*$ are respectively the optimal solutions of the following two problems:

$$\begin{aligned}\min_{\boldsymbol{\beta}_1(\mathbf{H},\ \mathbf{H}_e)} \quad & \boldsymbol{\beta}_1^{\text{H}}\boldsymbol{\beta}_1 \\ s.t. \quad & (\mathbf{H}\boldsymbol{\beta}_1)^{\text{H}}\mathbf{H}\boldsymbol{\beta}_1 \ge \mathbb{S}^{-1}, \ (\mathbf{H}_e\boldsymbol{\beta}_1)^{\text{H}}\mathbf{H}_e\boldsymbol{\beta}_1 \le \mathbb{S}_e^{-1};\end{aligned} \quad (52)$$

and

$$\min_{\boldsymbol{\beta}_2(\mathbf{H})} \ \boldsymbol{\beta}_2^{\text{H}}\boldsymbol{\beta}_2, \qquad s.t.\ (\mathbf{H}\boldsymbol{\beta}_2)^{\text{H}}\mathbf{H}\boldsymbol{\beta}_2 \ge \mathbb{S}^{-1}. \quad (53)$$

Note that as all the constraints and objective functions in problem (50), (52), (53) are real-valued over the complex field, we need to consider both the real and imaginary parts when applying the KKT conditions for the optimal points [42], [43]. Furthermore, because problem (52) is a non-convex optimization problem, while (53) is a convex problem; we obtain $\boldsymbol{\beta}_1^*$ being a locally optimal solution of the problem (52) and $\boldsymbol{\beta}_2^*$ being the globally optimal solution of the problem (53).

1) Zero Outage Probability at the Eavesdropper: If the sensor has more transmit antennas than the number of receive antennas at the eavesdropper, i.e., $N_t > N_e$, then it can transmit the observation signal x onto the null space of the eavesdropper's channel, thus leaking no useful information to the eavesdropper. To be more specific, let the singular value decomposition of $\mathbf{H}_e$ be $\mathbf{H}_e = \mathbf{USV}^{\text{H}}$. Then we can express the eavesdropper's channel null space as $\tilde{\mathbf{V}}\tilde{\mathbf{V}}^{\text{H}}$, where $\tilde{\mathbf{V}}$ contains the last $N_t - N_e$ columns of $\mathbf{V}$ [44]. Define a precoding matrix $\mathbf{W} = \tilde{\mathbf{V}}\tilde{\mathbf{V}}^{\text{H}} \in \mathbb{C}^{N_t}$. The signals received by the FC and the eavesdropper are then given by, respectively,

$$\mathbf{y} = \mathbf{HW}\boldsymbol{\beta}\theta + \mathbf{HW}\boldsymbol{\beta}\omega + \mathbf{z}, \quad (54)$$

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{W}\boldsymbol{\beta}\theta + \mathbf{H}_e\mathbf{W}\boldsymbol{\beta}\omega + \mathbf{z}_e = \mathbf{z}_e. \quad (55)$$

On the eavesdropper side, as no information about x is received, we obtain the secrecy outage probability $\Pr_{\text{outage\_EVE}} = 0$.

The outage minimization problem can then be given as

$$\min_{\boldsymbol{\beta}(\mathbf{H})} \ \Pr\left[\frac{1}{(\mathbf{HW}\boldsymbol{\beta})^{\text{H}}\mathbf{HW}\boldsymbol{\beta}} > \mathbb{S}\right], \quad s.t.\ \mathbb{E}\left[\boldsymbol{\beta}^{\text{H}}\boldsymbol{\beta}\right] \le \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}. \quad (56)$$

Similar techniques as used in Section II-A can be employed to solve problem (56), and it can be shown that the globally optimal $\boldsymbol{\beta}^*$ is constructed by randomizing among two deterministic power schemes $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2 = \mathbf{0}$ with corresponding weighting factors ω and $1-\omega$. Furthermore, problem (56) can be reformulated into the following problem:

$$\min_{\boldsymbol{\beta}_1(\mathbf{H}),\ \omega(\mathbf{H})} \quad 1-\mathbb{E}\left[\omega\right]$$
$$s.t.\ \ \mathbb{E}\left[\omega\boldsymbol{\beta}_1^{\mathrm{H}}\boldsymbol{\beta}_1\right] \leq \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2+\sigma_\omega^2} \tag{57a}$$
$$\left(\mathbf{HW}\boldsymbol{\beta}_1\right)^{\mathrm{H}}\mathbf{HW}\boldsymbol{\beta}_1 \geq \mathbb{S}^{-1}. \tag{57b}$$

The solution is given as

$$\boldsymbol{\beta}^*\left(\mathbf{H}\right) = \begin{cases} \boldsymbol{\beta}_1^*\left(\mathbf{H}\right), & \text{if } \ \lambda^*\left(\sigma_\theta^2+\sigma_\omega^2\right)\boldsymbol{\beta}_1^{\mathrm{H}^*}\boldsymbol{\beta}_1^* < 1 \\ \mathbf{0}, & \text{otherwise,} \end{cases} \tag{58}$$

where λ^* is the optimal Lagrange multiplier associated with the power constraint (57a) which is obtained numerically, and $\boldsymbol{\beta}_1^*$ is the globally optimal solution of the problem:

$$\min_{\boldsymbol{\beta}_1(\mathbf{H})} \left(\sigma_\theta^2+\sigma_\omega^2\right)\boldsymbol{\beta}_1^{\mathrm{H}}\boldsymbol{\beta}_1, \quad s.t.\ \left(\mathbf{HW}\boldsymbol{\beta}_1\right)^{\mathrm{H}}\mathbf{HW}\boldsymbol{\beta}_1 \leq \mathbb{S}^{-1}.$$

Remark: With this scheme, the FC's effective channel is $\mathbf{HW}$, which is the projection of $\mathbf{H}$ onto the null space of $\mathbf{H}_e$ via the precoding matrix $\mathbf{W}$. Moreover, if the FC has only one receive antenna, i.e., $N_r = 1$, we obtain the beamforming vector $\boldsymbol{\beta}_1^*\left(\mathbf{H}\right) = \sqrt{\frac{\mathbb{S}^{-1}}{(\mathbf{HW})^{\mathrm{H}}\mathbf{HW}}}\frac{(\mathbf{HW})^{\mathrm{H}}}{||\mathbf{HW}||}$ (where the notation $||\mathbf{x}||$ refers to the Euclidean norm of the vector $\mathbf{x}$), which lines up with the effective channel $\mathbf{HW}$ while satisfying the power constraint.[4]

B. Partial CSI

In this part of the work, we consider a case where the FC can acquire its channel information but only has statistical knowledge of the eavesdropper's. From the full CSI case, we know that a deterministic power allocation is optimal for continuously distributed fading channels. Therefore, applying the results derived in Section II-B, we can obtain a locally optimal $\boldsymbol{\beta}^*$ at each FC channel instance as:

$$\boldsymbol{\beta}^*\left(\mathbf{H}\right) = \begin{cases} \hat{\boldsymbol{\beta}}\left(\mathbf{H}\right), & \text{if } \nu\left(\mathbf{H}\right)\int_{\mathbf{H}_e} 1\left\{\left(\mathbf{H}_e\hat{\boldsymbol{\beta}}\right)^{\mathrm{H}}\mathbf{H}_e\hat{\boldsymbol{\beta}} > \frac{1}{\mathbb{S}_e}\right\} dF\left(\mathbf{H}_e\right) \\ & \qquad + \lambda\hat{\boldsymbol{\beta}}^{\mathrm{H}}\hat{\boldsymbol{\beta}} < 1 \\ \mathbf{0}, & \text{otherwise,} \end{cases}$$

where $\hat{\boldsymbol{\beta}}$ is a locally optimal solution to the problem:

$$\min_{\boldsymbol{\beta}(\mathbf{H})} \ \lambda\boldsymbol{\beta}^{\mathrm{H}}\boldsymbol{\beta} + \nu\left(\mathbf{H}\right)\int_{\mathbf{H}_e} 1\left\{\left(\mathbf{H}_e\boldsymbol{\beta}\right)^{\mathrm{H}}\mathbf{H}_e\boldsymbol{\beta} > \mathbb{S}_e^{-1}\right\} dF\left(\mathbf{H}_e\right)$$
$$s.t. \ \ \left(\mathbf{H}\boldsymbol{\beta}\right)^{\mathrm{H}}\mathbf{H}\boldsymbol{\beta} \geq \mathbb{S}^{-1}, \tag{59}$$

with λ and $\nu\left(\mathbf{H}\right)$ being nonnegative Lagrange multipliers corresponding to respectively the power constraint and the secrecy outage constraint at the eavesdropper.

1) Artificial Noise: Assuming that the sensor is equipped with more transmit antennas than the number of receive antennas at the FC, we can employ the technique of artificial noise [35], [45] to enhance the system performance. The idea is to increase the noise level seen by the adversary in a way that its channel is degraded while the channel of the legitimate receiver is not. With this method, the artificial noise is generated by the sensor and transmitted onto the null space of the FC, thus it does not impact the message received by the FC but increase the noise level at the eavesdropper.

Let $[\mathbf{W}_1, \mathbf{W}_2]$ be an orthonormal basis of $\mathbb{C}^{N_t}$ with $\mathbf{W}_1 \in \mathbb{C}^{N_t\times N_r}$ and $\mathbf{W}_2 \in \mathbb{C}^{N_t\times(N_t-N_r)}$ representing respectively the signal space and the null space of $\mathbf{H}$. The signals received by the FC and the eavesdropper are, respectively,

$$\mathbf{y} = \mathbf{HW}_1\boldsymbol{\beta}x+\mathbf{HW}_2\mathbf{v}+\mathbf{z} = \mathbf{HW}_1\boldsymbol{\beta}\theta+\mathbf{HW}_1\boldsymbol{\beta}\omega+\mathbf{z}, \tag{60a}$$
$$\begin{aligned}\mathbf{y}_e &= \mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta}x + \mathbf{H}_e\mathbf{W}_2\mathbf{v} + \mathbf{z}_e \\ &= \mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta}\theta + \mathbf{H}_e\mathbf{W}_1\omega + \mathbf{H}_e\mathbf{W}_2\mathbf{v} + \mathbf{z}_e.\end{aligned} \tag{60b}$$

where the artificial noise $\mathbf{v} \in \mathbb{C}^{(N_t-N_r)\times 1}$ has $N_t - N_r$ i.i.d. complex Gaussian elements with zero mean and variance p_a.

It can be seen from (60) that the sensor transmits observation information $\mathbf{W}_1\boldsymbol{\beta}x$ plus a 'noise' term $\mathbf{W}_2\mathbf{v}$, which is chosen to be a random vector in the null space of $\mathbf{H}$, to reduce the possibility of small noise being seen by the eavesdropper. As $[\mathbf{W}_1, \mathbf{W}_2]$ is a unitary matrix, we obtain that $\mathbf{H}_e\mathbf{W}_1$ is independent of $\mathbf{H}_e\mathbf{W}_2$, giving the effective noise at the eavesdropper as $\mathbf{H}_e\mathbf{W}_2\mathbf{v}+\mathbf{z}_e$. The transmit power in each fading block is given as $\left(\sigma_\theta^2+\sigma_\omega^2\right)\boldsymbol{\beta}^{\mathrm{H}}\boldsymbol{\beta} + \left(N_t-N_r\right)p_a$.

We want to minimise the distortion outage probability at the FC, by finding the best $\boldsymbol{\beta}^*\left(\mathbf{H}\right)$ and $p_a^*\left(\mathbf{H}\right)$ to meet the long-term power constraint and the secrecy outage constraint at the eavesdropper. Assuming that both the FC and the eavesdropper use the MMSE estimator, the optimization problem can be written as

$$\min_{p_a(\mathbf{H}),\ \boldsymbol{\beta}(\mathbf{H})} \ \Pr\left[\left(\mathbf{HW}_1\boldsymbol{\beta}\right)^{\mathrm{H}}\mathbf{HW}_1\boldsymbol{\beta} < \mathbb{S}^{-1}\right]$$
$$s.t. \ \ \Pr\left[\left(\mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta}\right)^{\mathrm{H}}\left(\left(\sigma_\theta^2+\sigma_\omega^2\right)\mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta}\left(\mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta}\right)^{\mathrm{H}}+\sigma_e^2\mathbf{I}_{N_e}\right.\right.$$
$$\left.\left. p_a\mathbf{H}_e\mathbf{W}_2\left(\mathbf{H}_e\mathbf{W}_2\right)^{\mathrm{H}}\right)^{-1}\mathbf{H}_e\mathbf{W}_1\boldsymbol{\beta} > \left(\sigma^2-\mathbb{D}_e\right)/\,\sigma^4\right] \leq \delta$$
$$\mathbb{E}\left[\left(\sigma_\theta^2+\sigma_\omega^2\right)\boldsymbol{\beta}^{\mathrm{H}}\boldsymbol{\beta} + \left(N_t-N_r\right)p_a\right] \leq \mathcal{P}_{\mathrm{tot}}. \tag{61}$$

In order to solve problem (61), we can employ similar techniques as described in Section II-B, which are omitted for brevity. For the special case of a single receive antenna at both the FC and the eavesdropper, the problem is reduced to finding p and p_a, where $p \triangleq \boldsymbol{\beta}^{\mathrm{H}}\boldsymbol{\beta} \in \mathbb{R}$. Let $\hat{p}_a$ be the solution of

$$\hat{p}_a\left(\mathbf{H}\right) = \arg\min_{\hat{p}_a\geq 0} \lambda\left(N_t-1\right)\hat{p}_a + \nu d\left(\mathbf{H},\hat{p}_a\right), \tag{62}$$

where λ and ν are the corresponding Lagrange multipliers for the long-term power constraint and secrecy outage constraint of problem (61), and $d\left(\mathbf{H},\hat{p}_a\right) = \int_{\mathbf{H}_e} 1\left\{\hat{p}_a < \frac{\mathbb{S}^{-1}|\mathbf{H}_e\mathbf{W}_1|^2}{|\mathbf{HW}_1|^2|\mathbf{H}_e\mathbf{W}_2|^2}\frac{\mathbb{D}_e\left(\sigma_\theta^2+\sigma_\omega^2\right)-\sigma_\omega^2\sigma_\theta^2}{\sigma_\theta^2-\mathbb{D}_e} - \frac{\sigma_e^2}{|\mathbf{H}_e\mathbf{W}_2|^2}\right\} dF\left(\mathbf{H}_e\right)$. We then derive the locally optimal $p^*\left(\mathbf{H}\right)$ and $p_a^*\left(\mathbf{H}\right)$ as

$$\begin{cases} p^*\left(\mathbf{H}\right) = \frac{\mathbb{S}^{-1}}{|\mathbf{HW}_1|^2}, & \text{if } \ \frac{\lambda\left(\sigma_\theta^2+\sigma_\omega^2\right)\mathbb{S}^{-1}}{|\mathbf{HW}_1|^2} + \nu d\left(\mathbf{H},\hat{p}_a\right) \\ p_a^*\left(\mathbf{H}\right) = \hat{p}_a\left(\mathbf{H}\right); & \qquad + \lambda\left(N_t-1\right)\hat{p}_a\left(\mathbf{H}\right) < 1 \\ p^*\left(\mathbf{H}\right) = p_a^*\left(\mathbf{H}\right) = 0, & \text{otherwise.} \end{cases}$$

IV. Alternative formulations

In Sections II and III we considered problems that minimise the distortion outage probability at the FC while maintaining the secrecy outage probability at the eavesdropper and overall power consumption to be below certain thresholds. Alternative problems can also be formulated. For instance, we can minimise the secrecy outage probability at the eavesdropper, with a distortion outage constraint at the FC and a long-term power constraint among sensors, given

[4] One could also use the techniques in [11] to solve the problem, which will give the same result.

as

$$\min_{\mathbf{P}(\mathbf{G})} \Pr\left[D_e\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right) < \mathbb{D}_e\right]$$
$$s.t.\ \Pr\left[D\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right) > \mathbb{D}\right] \leq \phi,\ \mathbb{E}\left[\langle \mathbf{P}\left(\mathbf{G}\right)\rangle\right] \leq \mathcal{P}_{\rm tot}, \quad (63)$$

where ϕ is the distortion outage probability threshold at the FC. Another potential problem would be to minimise the long-term expected estimation error at the FC subject to a secrecy outage constraint at the eavesdropper and a long-term power constraint among the sensors, written as

$$\min_{\mathbf{P}(\mathbf{G})} \mathbb{E}\left[D\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right)\right]$$
$$s.t.\ \Pr\left[D_e\left(\mathbf{G}, \mathbf{P}\left(\mathbf{G}\right)\right) < \mathbb{D}_e\right] \leq \delta,\ \mathbb{E}\left[\langle \mathbf{P}\left(\mathbf{G}\right)\rangle\right] \leq \mathcal{P}_{\rm tot}. \quad (64)$$

For both problems, we could consider the full CSI and the partial CSI cases, which can both be solved using similar techniques as in Section II. Note that problems (63), (64) are formulated for the multiple-sensor scenario. Similar problem formulations could also be constructed for a multiple-antenna scenario.

V. Numerical results

We first 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 following the free-space path-loss model [46]

$$PL = 20\log_{10}(d) + 20\log_{10}(f) - 27.55, \quad (65)$$

where $d \in \{d_k, d_{ek}\}$ 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. In addition, the total power budget range is set to 1 mW $\leq \mathcal{P}_{\rm tot} \leq$ 11 mW, to ensure that the secrecy outage probability requirement at the eavesdropper is achievable. 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.

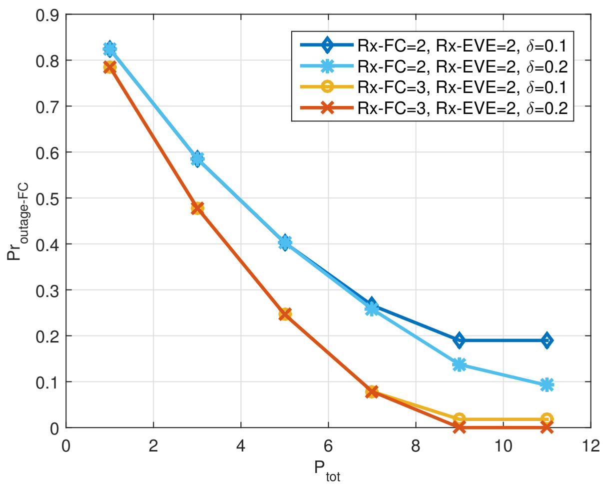

Fig. 3: Performance comparison in a three-sensor network with $N_e = 2$ and full CSI of the FC and the eavesdropper.

Fig. 3 shows the distortion outage probability at the FC with two antennas at the eavesdropper, under different secrecy outage probability requirements at the eavesdropper, namely 0.1 and 0.2. When the number of receive antennas at the FC is fixed, it is seen that for both sets (i.e., $N_r = 2$ and $N_r = 3$) the outage probability at the FC behaves similarly for the two different outage requirements at the eavesdropper when $\mathcal{P}_{\rm tot}$ is small. As we increase the total power budget, they start to decrease until saturation. This is because when $\mathcal{P}_{\rm tot}$ is small, the sensors are more likely to choose small power consumption policies that only guarantee non-outage at the FC, or the sensors would simply stop transmitting to save power. As the transmission power budget increases, sensors begin to transmit in channel states where outage happens neither at the FC nor at the eavesdropper, until a point where more incremental power would lead to the secrecy outage probability at the eavesdropper being greater than the security requirement δ, at which the distortion outage probability at the FC saturates.

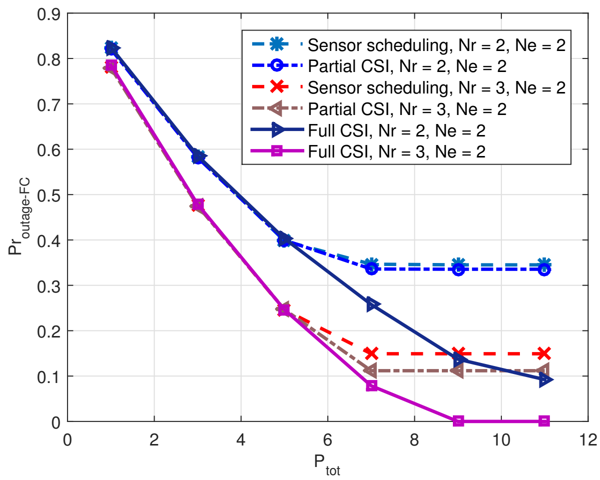

Fig. 4: Performance comparison in a three-sensor network with $N_e = 2$ and $\delta = 0.2$.

In Fig. 4, 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, similar to Fig. 3, the outage probability at the FC is smaller when the FC is equipped with more antennas for all three cases. In addition, the performance of sensor scheduling follows closely the partial CSI case, and it even has similar performance as the full CSI case when the transmit power budget is small.

The distortion outage probability at the FC versus different transmit power budgets is plotted in Fig. 5, where we compare the performance of sensor scheduling to the partial CSI case with the secrecy outage probability constraint at the eavesdropper set to 0.14, 0.18 and 0.22. The first thing to be noticed is the close performance of sensor-scheduling and partial CSI power allocation in all three scenarios (i.e, $\delta = 0.14$, $\delta = 0.18$ and $\delta = 0.22$) when the power budget $\mathcal{P}_{\rm tot}$ is relatively small. In addition, the results stated in (43) and (44) can be easily verified from the behaviour of sensor-scheduling. When we have a small power budget, $\Pr_{\rm outage\_FC}$ performs the same for all scenarios regardless of the different secrecy outage requirements at the eavesdropper, which implies that the total power constraint satisfies equality at the optimal points, whereas the secrecy outage constraint is

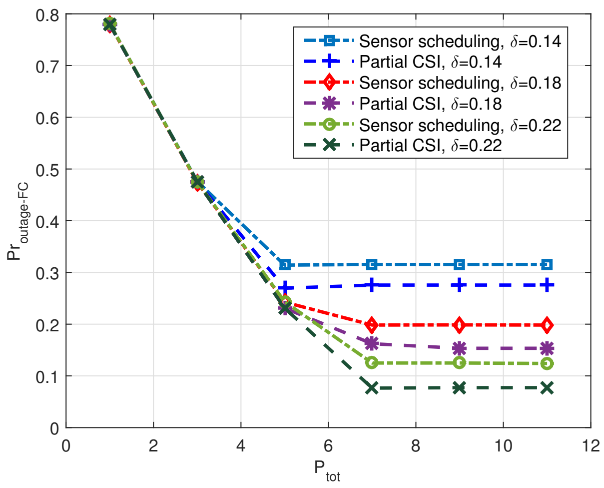

Fig. 5: Performance comparison in a three-sensor network with $N_r = 3$ and $N_e = 2$.

loose. As we keep increasing the power budget, $\mathrm{Pr}_{\mathrm{outage\_FC}}$ 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.

Next, we study the distortion outage probability at the FC for the multiple-antenna single sensor scenario, where we assume that the sensor is 127m away from the FC, and 130m away from the eavesdropper. For simplicity, we assume that the sensor is equipped with three antennas, whereas there is only one antenna at the FC and one or two antennas at the eavesdropper. We consider the maximum acceptable distortion level $\mathbb{D}_e$ at the eavesdropper being set to 0.013, which is twice as large as the required minimum distortion level $\mathbb{D}$ at the FC. We assume the same noise level for both the FC and the eavesdropper, where $\sigma^2 = \sigma_e^2 = 10^{-8}$ mW.

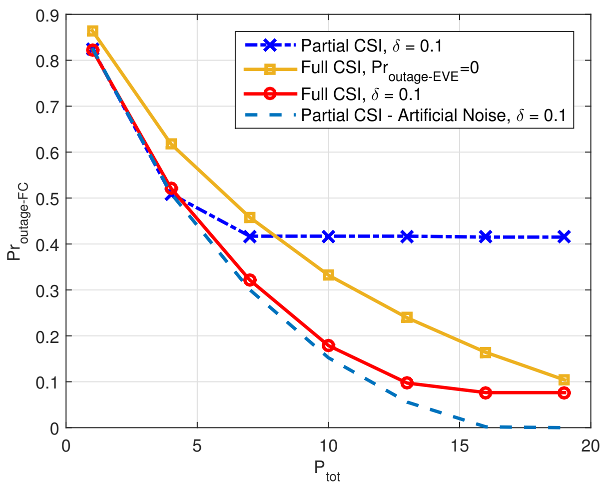

Fig. 6: Performance comparison for a single sensor multiple-antenna scenario with $N_r = N_e = 1$ and $\delta = 0.1$.

In Fig. 6, the distortion outage probability at the FC versus the long-term power budget is plotted for full CSI, full CSI with $\mathrm{Pr}_{\mathrm{outage\_EVE}} = 0$, partial CSI and partial CSI-Artificial Noise schemes. As we can see, the full CSI case outperforms the partial CSI case, and in both cases the distortion outage probability at the FC saturates. By contrast, the full CSI with $\mathrm{Pr}_{\mathrm{outage\_EVE}} = 0$ and partial CSI-Artificial Noise schemes perform better when we have a relatively large transmit power budget, where $\mathrm{Pr}_{\mathrm{outage\_FC}}$ keeps decreasing as $\mathcal{P}_{\mathrm{tot}}$ increases. More interestingly, it is seen from that the full CSI $\mathrm{Pr}_{\mathrm{outage\_EVE}} = 0$ scheme performs no better than the partial CSI-Artificial Noise scheme across the entire power range. This is owing to the fact that the effective channel gains of the FC are largely reduced when projecting it onto the eavesdropper's channel null space, whereas in the case of partial CSI-Artificial Noise, only a small portion of the transmit power is used to generate 'noise'.

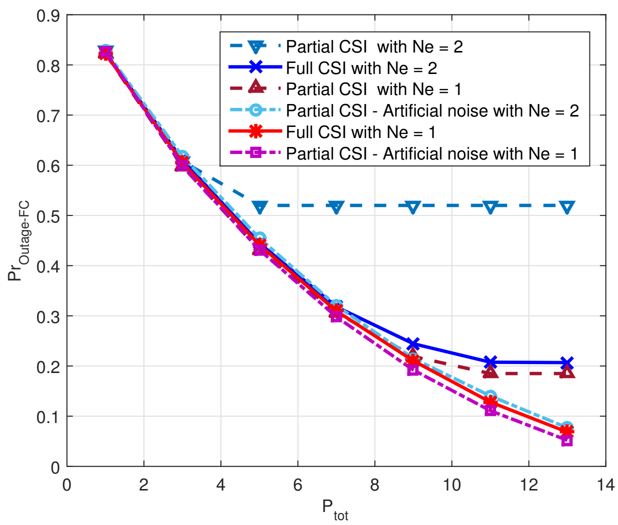

Fig. 7: Performance comparison for a single sensor multiple-antenna scenario with $N_r = 1$ and $\delta = 0.2$.

To closely observe the performance of $\mathrm{Pr}_{\mathrm{outage\_FC}}$ using artificial noise, in Fig.7 we look at scenarios where the eavesdropper has more receive antennas than the FC, and we also plot the full CSI and partial CSI cases for comparison. It is noticeable that when the eavesdropper has more antennas, $\mathrm{Pr}_{\mathrm{outage\_FC}}$ in the partial CSI case quickly saturates which is then followed by the full CSI case, as at certain channel states the sensor has to stop transmitting in order to maintain the required secrecy outage probability at the eavesdropper. Whereas in the case of partial CSI-Artificial Noise, because the sensor can intentionally generate noise to degrade the eavesdropper's channel, it can explore more channel states to transmit the observation signals to the FC. Similar behaviour is seen when the eavesdropper has the same number of antennas as the FC, where the partial CSI-Artificial Noise gives better performance, as less 'noise' needs to be produced which means more power can be used to forward the observations. Therefore, the simulation results in Fig.6 and Fig.7 indicate that injecting artificial noise into the eavesdropper's channel appears to be a better solution for the single sensor multiple-antenna scenario.

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 two different scenarios: multiple sensor single antenna scenario and multiple antenna single sensor scenario. We proposed a suboptimal solution (for the partial CSI case) to overcome the high computational cost in the multiple-sensor scenario. With multiple transmit antennas at the sensor, we investigated techniques that can achieve zero outage at the eavesdropper. Simulation results showed that better performance can be achieved with additional receive antennas at the FC for the multiple-sensor scenario, and in the multiple antenna single sensor scenario the distortion outage probability at the FC can be reduced to zero if the transmit power budget is sufficiently large.

APPENDIX

A. Proof of Lemma 1

We will show that the power allocation policy given in (12) is feasible, i.e. $\mathbf{P}'(\mathbf{G})$ satisfies the secrecy outage constraint at the eavesdropper (7a) and the total transmit power constraint (7b); and that $\mathbf{P}'(\mathbf{G})$ performs at least as well as $\hat{\mathbf{P}}(\mathbf{G})$.

Since $\hat{\mathbf{P}}(\mathbf{G})$ is feasible, $\hat{\mathbf{P}}(\mathbf{G})$ must satisfy all the constraints, i.e.,

$$\begin{aligned}&\Pr\left[D_e\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)<\mathbb{D}_e\right]\\&=\mathbb{E}_{\mathbf{G}}\left[\Pr\left[D_e\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)<\mathbb{D}_e\middle|\mathbf{G}\right]\right]=\mathbb{E}_{\mathbf{G}}\left[\omega_2(\mathbf{G})\right]\le\delta,\end{aligned}$$

and

$$\begin{aligned}&\mathbb{E}_{\mathbf{G},\mathbf{p}}\left[\left\langle\hat{\mathbf{P}}(\mathbf{G})\right\rangle\right]\\&=\mathbb{E}_{\mathbf{G}}\left[\left\langle\sum_{i=1}^{3}\mathbb{E}_{\mathbf{p}}\left(\hat{\mathbf{P}}(\mathbf{G})\middle|\mathbf{p}(\mathbf{G})\in\mathcal{B}_i(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\mathbf{G}\right)\right.\right.\\&\qquad\left.\left.\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_i(\mathbb{D},\mathbb{D}_e,\mathbf{G})\middle|\mathbf{G}\right]\right\rangle\right]\\&=\mathbb{E}_{\mathbf{G}}\left[\left\langle\sum_{i=1}^{3}\mathbf{p}_i(\mathbf{G})\,\omega_i(\mathbf{G})\right\rangle\right]\le\mathcal{P}_{\rm tot}.\end{aligned}\tag{66}$$

Remark: As $\hat{\mathbf{P}}(\mathbf{G})$ has three non-overlapping regions as defined in (11), with all powers in $\mathcal{B}_3(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ being zero, we know that the only power region leading to outage at the eavesdropper is $\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})$. In addition, the probability of choosing a power in $\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ is given as $\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_2(\mathbb{D},\mathbb{D}_e,\mathbf{G})|\,\mathbf{G}\right]$, which is the same as the time-sharing factor $\omega_2(\mathbf{G})$ defined in (15).

As the new probabilistic power allocation $\mathbf{P}'(\mathbf{G})$ is randomised among the three deterministic power policies given in (14), we can easily find the long-term average power consumption of $\mathbf{P}'(\mathbf{G})$ as

$$\begin{aligned}\mathbb{E}\left[\langle\mathbf{p}(\mathbf{G})\rangle\right]&=\mathbb{E}_{\mathbf{G}}\left[\langle\mathbb{E}_{\mathbf{p}}\left[\mathbf{p}(\mathbf{G})|\,\mathbf{G}\right]\rangle\right]\\&=\mathbb{E}_{\mathbf{G}}\left[\left\langle\sum_{i=1}^{3}\mathbf{p}_i(\mathbf{G})\,\omega_i(\mathbf{G})\right\rangle\right],\end{aligned}\tag{67}$$

and hence $\mathbf{P}'(\mathbf{G})$ satisfies the power constraint (7b).

In addition, as both $D(\mathbf{G},\mathbf{p}(\mathbf{G}))$ and $D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))$ are continuous and convex over $\mathbf{p}(\mathbf{G})$, by the Mean Value Theorem (MVT) for integration, we know that, for a given channel realisation $\mathbf{G}$, there exists a $\hat{\mathbf{p}}_1(\mathbf{G})\in\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})$ such that $\hat{\mathbf{p}}_1(\mathbf{G})=\mathbb{E}\left[\hat{\mathbf{P}}(\mathbf{G})\middle|\mathbf{p}(\mathbf{G})\in\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G}),\mathbf{G}\right]$. Together with the definition of $\mathbf{p}_1(\mathbf{G})$ in (14), we know that $D(\mathbf{G},\mathbf{p}_1(\mathbf{G}))\le\mathbb{D}$ and $D_e(\mathbf{G},\mathbf{p}_1(\mathbf{G}))\ge\mathbb{D}_e$. Similarly, only when $\mathbf{P}'(\mathbf{G})=\mathbf{p}_2(\mathbf{G})$ does outage occur at the eavesdropper. Therefore, we can compute the secrecy outage probability at the eavesdropper when using the probabilistic power policy $\mathbf{P}'(\mathbf{G})$ as

$$\begin{aligned}\Pr\left[D_e\left(\mathbf{G},\mathbf{P}'(\mathbf{G})\right)<\mathbb{D}_e\right]&=\mathbb{E}_{\mathbf{G}}\left[\Pr\left[\mathbf{P}'(\mathbf{G})=\mathbf{p}_2(\mathbf{G})|\,\mathbf{G}\right]\right]\\&=\mathbb{E}_{\mathbf{G}}\left[\omega_2(\mathbf{G})\right]\le\delta.\end{aligned}\tag{68}$$

Remark: Note that for the channel states where $\mathcal{B}_1(\mathbb{D},\mathbb{D}_e,\mathbf{G})=\emptyset$, the result given in (68) can be also established, since for those channel states we have $\omega_1(\mathbf{G})=0$. By following the above arguments and applying the MVT, we see that outage occurs at the eavesdropper only when $\mathbf{P}'(\mathbf{G})=\mathbf{p}_2(\mathbf{G})$.

The feasibility of $\mathbf{P}'(\mathbf{G})$ has thus been proved. In order to see that the probabilistic power policy $\mathbf{P}'(\mathbf{G})$ performs no worse than $\hat{\mathbf{P}}(\mathbf{G})$, we first show that for each channel realisation, the distortion outage probability at the FC when using $\mathbf{P}'(\mathbf{G})$ is at least as small as when using $\hat{\mathbf{P}}(\mathbf{G})$. We then conclude that for a fixed maximum acceptable distortion level $\mathbb{D}$ at the FC, $\mathbf{P}'(\mathbf{G})$ would result in the same or smaller outage probability at the FC. Given the channel realisation $\mathbf{G}$, the distortion outage probability at the FC is:

$$\begin{aligned}&\Pr\left[\mathrm{D}\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)>\mathbb{D}\middle|\mathbf{G}\right]\\&=\sum_{i=1}^{3}\Pr\left[\mathrm{D}\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)>\mathbb{D}\middle|\mathbf{p}(\mathbf{G})\in\mathcal{B}_{\rm i},\mathbf{G}\right]\Pr\left[\mathbf{p}(\mathbf{G})\in\mathcal{B}_{\rm i}|\,\mathbf{G}\right]\\&\overset{(a)}{=}\sum_{i=1}^{3}\mathbb{E}_{\mathbf{p}}\left[1\left\{D\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)>\mathbb{D}\middle|\mathbf{p}(\mathbf{G})\in\mathcal{B}_i,\mathbf{G}\right\}\right]\omega_i(\mathbf{G})\\&\overset{(b)}{\ge}\sum_{i=1}^{3}1\left\{D\left(\mathbf{G},\mathbb{E}_{\mathbf{p}}\left[\hat{\mathbf{P}}(\mathbf{G})\middle|\mathbf{p}(\mathbf{G})\in\mathcal{B}_i,\mathbf{G}\right]\right)>\mathbb{D}\right\}\omega_i(\mathbf{G})\\&=\Pr\left[D\left(\mathbf{G},\mathbf{P}'(\mathbf{G})\right)>\mathbb{D}|\,\mathbf{G}\right],\end{aligned}\tag{69}$$

where (a) follows from the definition of $\{\omega_i(\mathbf{G})\}$ given in (15) and (b) follows from Jensen's inequality, since $D(\mathbf{G},\mathbf{p}(\mathbf{G}))$ is a convex function over $\mathbf{p}(\mathbf{G})$, and the last equality follows from (12). Therefore, the resulting distortion outage probability at the FC from using $\mathbf{P}'(\mathbf{G})$ is no worse than using $\hat{\mathbf{P}}(\mathbf{G})$, i.e.,

$$\Pr\left[D\left(\mathbf{G},\mathbf{P}'(\mathbf{G})\right)>\mathbb{D}\right]\le\Pr\left[D\left(\mathbf{G},\hat{\mathbf{P}}(\mathbf{G})\right)>\mathbb{D}\right].\tag{70}$$

Combining (67), (68) and (70), we conclude that a probabilistic power allocation scheme $\mathbf{P}'(\mathbf{G})$ with the form (12) is feasible and gives the same or smaller outage probability at the FC compared to an arbitrary probabilistic power allocation. Furthermore, from the definition of $\{\mathbf{p}_i(\mathbf{G})\}$ given in (14), we have the following:

$$\begin{aligned}\mathbb{D}_e\le&\,\mathbb{E}_{\mathbf{p}}\left[D_e\left(\mathbf{G},\mathbf{P}'(\mathbf{G})\right)|\,D_e(\mathbf{G},\mathbf{p}(\mathbf{G}))\ge\mathbb{D}_e,\mathbf{G}\right]\\&\overset{(c)}{=}\frac{\omega_3(\mathbf{G})\,\sigma_\theta^2}{\omega_1(\mathbf{G})+\omega_3(\mathbf{G})}+\frac{\omega_1(\mathbf{G})\,D_e(\mathbf{G},\mathbf{p}_1(\mathbf{G}))}{\omega_1(\mathbf{G})+\omega_3(\mathbf{G})}\end{aligned}\tag{71}$$

$$\begin{aligned}\mathbb{D}\ge&\,\mathbb{E}_{\mathbf{p}}\left[D\left(\mathbf{G},\mathbf{P}'(\mathbf{G})\right)|\,D(\mathbf{G},\mathbf{p}(\mathbf{G}))\le\mathbb{D},\mathbf{G}\right]\\&\overset{(d)}{=}\frac{\omega_1(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_1(\mathbf{G}))}{\omega_1(\mathbf{G})+\omega_2(\mathbf{G})}+\frac{\omega_2(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_2(\mathbf{G}))}{\omega_1(\mathbf{G})+\omega_2(\mathbf{G})},\end{aligned}\tag{72}$$

where (c) and (d) are obtained by applying conditional expectations.

B. Proof of Theorem 1

We will consider the case $\omega_j^*(\mathbf{G})=1$, as when $\omega_j^*(\mathbf{G})=0$, the solution of $\mathbf{p}_j^*(\mathbf{G})$ has no impact on the optimization problem.

(1) When $\nu^*(\mathbf{G})=0$: From the KKT condition (22), we need to have $\omega_1^*(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))+\omega_2^*(\mathbf{G})\,D(\mathbf{G},\mathbf{p}_2^*(\mathbf{G}))-(\omega_1^*(\mathbf{G})+\omega_2^*(\mathbf{G}))\,\mathbb{D}=0$. If $\omega_1^*(\mathbf{G})=1$, we must have $\omega_2^*(\mathbf{G})=0$, and so $D(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))=\mathbb{D}$. However, we also know that $\frac{\partial l(\dots)}{\partial p_{1k}^*(\mathbf{G})}=\lambda^*\omega_1^*(\mathbf{G})\left(\sigma_{\omega k}^2+\sigma_\theta^2\right)-\nu_e^*(\mathbf{G})\,\omega_1^*(\mathbf{G})\,\frac{\partial D_e(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})}\ge0$. Combining with (17) we see that $\mathbf{p}_1^*(\mathbf{G})=\mathbf{0}$, which contradicts the requirement that

$D\left(\mathbf{G},\mathbf{p}_1^*\left(\mathbf{G}\right)\right)=\mathbb{D}$. Similar arguments apply for the case when $\omega_2^*\left(\mathbf{G}\right)=1$. Therefore, we conclude that if $\nu^*\left(\mathbf{G}\right)=0$ we must have $\omega_1^*\left(\mathbf{G}\right)=\omega_2^*\left(\mathbf{G}\right)=0$.

(2) When $\nu^*\left(\mathbf{G}\right)>0$ **and** $\nu_e^*\left(\mathbf{G}\right)=0$: Here, one should have $\omega_1^*\left(\mathbf{G}\right)\left[D_e\left(\mathbf{G},\mathbf{p}_1^*\left(\mathbf{G}\right)\right)-\sigma_\theta^2\right]+\omega_2^*\left(\mathbf{G}\right)\left(\mathbb{D}_e-\sigma_\theta^2\right)\geq\mathbb{D}_e-\sigma_\theta^2$ and $\omega_1^*\left(\mathbf{G}\right)D\left(\mathbf{G},\mathbf{p}_1^*\left(\mathbf{G}\right)\right)+\omega_2^*\left(\mathbf{G}\right)D\left(\mathbf{G},\mathbf{p}_2^*\left(\mathbf{G}\right)\right)-\left(\omega_1^*\left(\mathbf{G}\right)+\omega_2^*\left(\mathbf{G}\right)\right)\mathbb{D}=0$. If $\omega_1^*\left(\mathbf{G}\right)=1$, we obtain $\omega_2^*\left(\mathbf{G}\right)=0$, $D\left(\mathbf{G},\mathbf{p}_1^*\left(\mathbf{G}\right)\right)=\mathbb{D}$ and $D_e\left(\mathbf{G},\mathbf{p}_1^*\left(\mathbf{G}\right)\right)\geq\mathbb{D}_e$. In addition, from (25) we see that $p_{1k}^*\left(\mathbf{G}\right)$ satisfies $\left(\sigma_{\omega k}^2+\sigma_\theta^2\right)-\frac{\nu^*(\mathbf{G})}{\lambda^*}\frac{\partial D(\mathbf{G},\mathbf{p}_1^*(\mathbf{G}))}{\partial p_{1k}^*(\mathbf{G})}=0$. For problem (31), from the KKT conditions, we know that the optimal solution $\mathbf{p}_a^*\left(\mathbf{G}\right)$ must satisfy $D\left(\mathbf{G},\mathbf{p}_a^*\left(\mathbf{G}\right)\right)=\mathbb{D}$, $D_e\left(\mathbf{G},\mathbf{p}_a^*\left(\mathbf{G}\right)\right)\geq\mathbb{D}_e$, and $\left(\sigma_{\omega k}^2+\sigma_\theta^2\right)-\hat{\nu}^*\left(\mathbf{G}\right)\frac{\partial D(\mathbf{G},\mathbf{p}_a^*(\mathbf{G}))}{\partial p_{ak}^*(\mathbf{G})}=0$, $\forall k$, which shares the same form as $\mathbf{p}_1^*\left(\mathbf{G}\right)$, where $\hat{\nu}^*\left(\mathbf{G}\right)$ is the optimal Lagrange multiplier corresponding to the distortion constraint at the FC for problem (31). Therefore, if $\omega_1^*\left(\mathbf{G}\right)=1$ we have $\mathbf{p}_1^*\left(\mathbf{G}\right)=\mathbf{p}_a^*\left(\mathbf{G}\right)$. Similarly, for $\omega_2^*\left(\mathbf{G}\right)=1$, we obtain $\mathbf{p}_2^*\left(\mathbf{G}\right)=\mathbf{p}_b^*\left(\mathbf{G}\right)$ if $D_e\left(\mathbf{G},\mathbf{p}_b^*\left(\mathbf{G}\right)\right)<\mathbb{D}_e$.

(3) When $\nu^*\left(\mathbf{G}\right)>0$ **and** $\nu_e^*\left(\mathbf{G}\right)>0$: The same results can be derived by using similar arguments as for case **(2)**.

C. Proof of Lemma 2

First, from (34) we know that the optimal power $\mathbf{p}^*\left(\mathbf{G}\right)$ should minimise $1\left\{D\left(\mathbf{g},\mathbf{p}^*\left(\mathbf{g}\right)\right)>\mathbb{D}\right\}+\xi\left(\mathbf{p}^*\left(\mathbf{g}\right)\right)$ at each channel instant. When $\mathbf{p}\left(\mathbf{G}\right)=\mathbf{0}$, we obtain $\xi\left(\mathbf{p}\left(\mathbf{g}\right)\right)=0$ and $1\left\{D\left(\mathbf{g},\mathbf{p}\left(\mathbf{g}\right)\right)>\mathbb{D}\right\}+\xi\left(\mathbf{p}\left(\mathbf{g}\right)\right)=1$, which indicates that $1\left\{D\left(\mathbf{g},\mathbf{p}^*\left(\mathbf{g}\right)\right)>\mathbb{D}\right\}+\xi\left(\mathbf{p}^*\left(\mathbf{g}\right)\right)$ is upper bounded by 1. If $\mathbf{p}^*\left(\mathbf{G}\right)$ is a nonzero vector, we must have $\xi\left(\mathbf{p}^*\left(\mathbf{g}\right)\right)>0$. Furthermore, as $1\left\{D\left(\mathbf{g},\mathbf{p}^*\left(\mathbf{g}\right)\right)>\mathbb{D}\right\}+\xi\left(\mathbf{p}^*\left(\mathbf{g}\right)\right)\leq1$, we obtain $\xi\left(\mathbf{p}^*\left(\mathbf{g}\right)\right)\leq1$ and $1\left\{D\left(\mathbf{g},\mathbf{p}^*\left(\mathbf{g}\right)\right)>\mathbb{D}\right\}=0$.

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] 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] W. Bajwa, A. Sayeed, and R. Nowak, "Matched source-channel communication for field estimation in wireless sensor network," in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, April 2005, pp. 332–339.

[6] 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.

[7] 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.

[8] ——, "Linear coherent decentralized estimation," *Signal Processing, IEEE Transactions on*, vol. 56, no. 2, pp. 757–770, Feb 2008.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] ——, "Distortion outage minimization in rayleigh fading using limited feedback," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE, 2009, pp. 1–8.

[16] C.-H. Wang, A. S. Leong, and S. Dey, "Distortion outage minimization and diversity order analysis for coherent multiaccess," *Signal Processing, IEEE Transactions on*, vol. 59, no. 12, pp. 6144–6159, 2011.

[17] A. S. Leong, S. Dey, G. N. Nair, and P. Sharma, "Power allocation for outage minimization in state estimation over fading channels," *Signal Processing, IEEE Transactions on*, vol. 59, no. 7, pp. 3382–3397, 2011.

[18] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] 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.

[20] 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.

[21] 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.

[22] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[23] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 3, 2009.

[24] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 6, pp. 2547–2553, 2009.

[25] E. Ekrem and S. Ulukus, "Secure lossy transmission of vector gaussian sources," *Information Theory, IEEE Transactions on*, vol. 59, no. 9, pp. 5466–5487, 2013.

[26] 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.

[27] G. Bagherikaram and K. N. Plataniotis, "Secure hybrid digital-analog wyner-ziv coding," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*. IEEE, 2011, pp. 1161–1166.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] R. Soosahabi and M. Naraghi-Pour, "Scalable phy-layer security for distributed detection in wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 4, pp. 1118–1126, Aug 2012.

[35] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[36] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, 2010.

[37] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Smart Antennas (WSA), 2010 International ITG Workshop on*. IEEE, 2010, pp. 394–401.

[38] X. Guo, A. Leong, and S. Dey, "Power allocation for distortion minimization in distributed estimation with security constraints," in *Proc. IEEE Symposium on Signal Processing Advances in Wireless Communications (SPAWC)*, Toronto, Canada, June 2014, p. 6 pages.

[39] 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.

[40] S. M. Kay, *Fundamentals of statistical signal processing: Estimation theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[41] D. G. Luenberger, *Optimization by vector space methods*. John Wiley & Sons, 1968.

[42] D. Messerschmitt, "Stationary points of a real-valued function of a complex variable," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2006-93*, 2006.

[43] L. Sorber, M. V. Barel, and L. D. Lathauwer, "Unconstrained optimization of real functions in complex variables," *SIAM Journal on Optimization*, vol. 22, no. 3, pp. 879–898, 2012.

[44] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 3, pp. 528–541, March 2006.

[45] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3. IEEE; 1999, 2005, p. 1906.

[46] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.