Estimation in Wireless Sensor Networks With Security Constraints

XIAOXI GUO, Student Member, IEEE
University of Melbourne, Melbourne, Australia

ALEX S. LEONG, Member, IEEE
Paderborn University, Paderborn, Germany

SUBHRAKANTI DEY, Senior Member, IEEE
Uppsala University, Uppsala, Sweden

In this paper, we investigate the performance of distributed estimation schemes in a wireless sensor network in the presence of an eavesdropper. The sensors transmit observations to the fusion center (FC), which at the same time are overheard by the eavesdropper. Both the FC and the eavesdropper reconstruct a minimum mean-squared error estimate of the physical quantity observed. We address the problem of transmit power allocation for system performance optimization subject to a total average power constraint on the sensor(s), and a security/secrecy constraint on the eavesdropper. We mainly focus on two scenarios: 1) a single sensor with multiple transmit antennas and 2) multiple sensors with each sensor having a single transmit antenna. For each scenario, given perfect channel state information (CSI) of the FC and full or partial CSI of the eavesdropper, we derive the transmission policies for short-term and long-term cases. For the long-term power allocation case, when the sensor is equipped with multiple antennas, we can achieve zero information leakage in the full CSI case, and dramatically enhance the system performance by deploying the artificial noise technique for the partial CSI case. Asymptotic expressions are derived for the long-term distortion at the FC as the number of sensors or the number of antennas becomes large. In addition, we also consider multiple-sensor multiple-antenna scenario, and simulations show that given the same total number of transmitting antennas the multiple-antenna sensor network is superior to the performance of the multiple-sensor single-antenna network.

Manuscript received May 20, 2016; revised November 16, 2015; released for publication July 25, 2016. Date of publication January 8, 2017; date of current version April 27, 2017.

DOI. No. 10.1109/TAES.2017.2649178

Refereeing of this contribution was handled by S. Marano.

Authors' addresses: X. Guo is with the Department of Electrical and Electronic Engineering, the University of Melbourne, Melbourne, VIC 3010, Australia, E-mail: (xiaoxig@student.unimelb.edu.au); A. S. Leong is with the Department of Electrical Engineering (EIM-E), Paderborn University, Paderborn 33098, Germany, E-mail: (alex.leong@upb.de); S. Dey is with the Department of Engineering Science, Uppsala University, Uppsala 75236, Sweden, E-mail: (subhrakanti.dey@angstrom.uu.se).

I. INTRODUCTION

Wireless sensor networks (WSNs) are networks consisting of some small, inexpensive, and low-power sensors, which are deployed over a region and may communicate with a remote processor over wireless links. Due to their low cost, robustness, and high flexibility, WSNs are widely employed in many military and civilian applications, such as environmental monitoring, traffic control, battlefield surveillance, so on. [1]. In distributed estimation, sensors independently collect data about some phenomena and send the measurements to a fusion center (FC) which then attempts to reconstruct the phenomenon.

One crucial issue in WSNs is the limited battery life of the sensors. As sensors are normally geographically widespread, replacing batteries can be costly. The problem of power allocation for distributed estimation has been well-studied. In [2], Xiao *et al.* look at an optimal power allocation scheme in an inhomogeneous Gaussian sensor network. In [3], Cui *et al.* considered the problems of minimizing transmit power under distortion [or mean-squared error (MSE)] constraints and minimizing distortion under power constraints for an orthogonal multiple access channel (MAC). Employing a universal decentralized quantization/estimation scheme and an uncoded quadrature amplitude modulated transmission strategy, Xiao *et al.* in [4] studied the optimal power scheduling problem in an inhomogeneous sensor network. In [5], Bahceci and Khandani investigated the energy-efficient distributed estimation problem for spatially correlated observations in WSNs. The power allocation for the distortion outage probability minimization was also well studied in [6] and [7].

Due to the broadcast nature of wireless communications, security and privacy issues have become one of the biggest challenges in WSNs. The traditional encryption schemes or cryptography might be vulnerable because of problems, such as secret key distribution and management. In addition, if an eavesdropper has sufficiently large computational power, cryptographic schemes with small key size may provide little secrecy. As an alternative, the notion of perfect secrecy,[1] introduced by Shannon [8], provides a different perspective on the data confidentiality. Later, in the 1970s, Wyner introduced the concept of wiretap channel [9], and showed that if the adversarys channel is a degraded version of the legitimate receivers, reliable information can be received at the legitimate receiver without the eavesdropper being able to extract almost any useful information. From an information-theoretic perspective, the secrecy capacity in the case of full channel state

[1] Perfect secrecy was first introduced in 1949 by Shannon. In this model, it is assumed that the confidential message W is encrypted and then transmitted over a noiseless channel [8]. In information theory, perfect secrecy requires that $I(W;Z)=0$; it indicates that the signal Z received by the eavesdropper does not provide any additional information about the transmitted message W. A weaker definition was given in [9], which requires the mutual information rate $\frac{1}{n}I(W;Z)$ goes to zero, as n, the number of bits in Z goes to infinity.

information (CSI) or partial CSI was studied in [10]–[12], and the MIMO channels were investigated in [13]–[15]. Multiterminal source coding or CEO problems with secrecy constraints were also considered in [16]–[19]. In particular, in [19], Villard and Piantanida 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. In [20], Kaspi and Merhav 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 provide a closed-form expression for distortion achievable via multisensor 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 [21] 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 and discussed in [22]–[27], where different performance metrics, such as Bayesian detection-operational privacy metric, 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 [22] and [28]–[30] to secure a system.

Moreover, it is known that the mutual information between the input and the output of a channel is at the core of information theory; given an input signal it measures the amount of coded information that can be reliably transmitted through a channel. Its counterpart, minimum mean-square error (MMSE), is a fundamental quantity in the estimation theory, which indicates how accurately the input signal can be retrieved from the channel output. In [31], Guo *et al.* discovered that regardless of the input distribution the derivative of the mutual information in nats w.r.t. SNR is equal to half the MMSE, as long as the input signals are observed through an additive Gaussian noise channel. In [17], Naghibi *et al.* related the equivocation rate to the normalized distortion at the eavesdropper in the CEO problem with additional secrecy constraints, where they showed that the estimation error at the eavesdropper is an upper bound of the equivocation rate.

Therefore, in the favor of a close form distortion expression for multisensor estimation over fading channels and close relation between MMSE and mutual information, we consider analog uncoded transmission at the sensors and introduce the MMSE as security metric to secure the system at the physical layer.

In this paper, we consider the estimation of a single-point Gaussian source by a sensor network in the presence of an eavesdropper, where the analog amplify and forward technique over a slow-fading orthogonal MAC[2] is used. We assume the same observed signal passes through another orthogonal MAC before reaching the eavesdropper, and both the FC and the eavesdropper attempt to obtain an MMSE estimation of the observations. The main contributions of the paper are as follows:

1) We consider power allocation problems that minimize the distortion at the FC subject to a total transmit power constraint at the sensor(s) and a security/secrecy constraint at the eavesdropper.
2) In the multiple-antenna single-sensor system, we can achieve zero information leakage in the full CSI case by transmitting the signal onto the eavesdropper’s channel null space, and also enhance the system performance dramatically by employing the technique of artificial noise for the partial CSI case. We give theoretical analysis on the long-term distortion for a power allocation scheme, where a beamforming vector is aligned with the FC’s channel direction. We also study the asymptotic distortion at the FC under the secrecy constraints when the number of antennas grows large.
3) In the multiple-sensor scenario, we consider a short-term power allocation problem in the full CSI case, and long-term power allocation problems in both the full CSI and partial CSI cases. The asymptotic behavior of the long-term distortion at the FC is also studied under the equal power allocation scheme as the number of sensors increases.

REMARK A preliminary version of this paper [32] was presented in SPAWC 2014, which contained only the power allocation results with long-term average power constraints for the multi-sensor single-antenna case. This paper extends these results to multiple directions including short-term power constraints, single-sensor multiantenna scenario with relays and artificial noise, multisensor multiantenna scenarios, and additional asymptotic results for the decay rate of the distortion at the FC (with respect to number of sensors/antennas) under the secrecy constraints at the eavesdropper.

This paper is organized as follows. In Section II, we give the general problem formulation of the decentralized estimation for a system with a multiple-antenna single sensor, and study the optimal power scheduling. We also explore other techniques that can be utilized in the multiple-antenna scenario. In Section III, we explore a multiple-sensor single-antenna network and solve the power allocation problems for different scenarios. In Section IV, we consider a multiple-sensor multiple-antenna network. In Section V, we look at the asymptotic long-term distortion

[2] When orthogonal MAC, such as TDMA and FDMA, is employed, only pairwise synchronization between each sensor and the FC is sufficient; whereas in the case of coherent MAC, synchronization between all sensors and the FC are required [3].

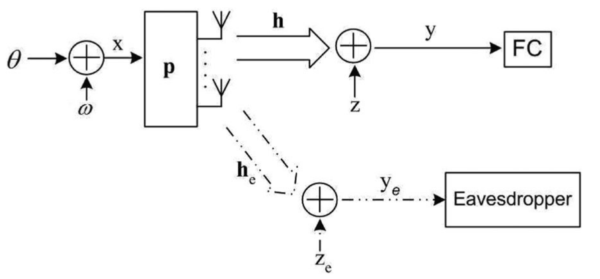

Fig. 1. Diagram of a multiple-antenna single-sensor system with the presence of an eavesdropper.

at the FC in a multiple-eavesdropper multiple-antenna scenario. Simulation results are given in Section VI, followed by concluding remarks in Section VII.

Throughout this paper, we use $^{\mathrm{T}}$ to denote transposition, * to denote complex conjugate, $^{\mathrm{H}}$ to denote conjugate transposition, $^{-1}$ to denote matrix inversion, $\mathbf{I}_M$ to denote the $M \times M$ identity matrix, $\|\mathbf{x}\|$ to denote the Euclidean norm of the vector $\mathbf{x}$, $|z|$ to denote the absolute value of z, and $\angle(\mathbf{x}, \mathbf{y})$ to denote the angle between two vectors $\mathbf{x}$ and $\mathbf{y}$. In addition, for two functions $f_1(\cdot)$ and $f_2(\cdot)$, we use the standard asymptotic notation and say that $f_1 \sim f_2$ as $t \to t_0$, if $f_1(t)/f_2(t) \to 1$ as $t \to t_0$ [33]. We also extend the use of the symbol $\sim$ to functions of the random variables; for function $f_1(t, \omega)$ and $f_1(t, \omega)$, we say that $f_1 \sim f_2$ w.p.1 as $t \to t_0$, if $f_1(t, \cdot)/f_2(t, \cdot) \to 1$ w.p.1 as $t \to t_0$, where w.p.1 is convergence with probability 1 or almost sure convergence.

II. MULTIPLE-ANTENNAS SCENARIO

Consider a scenario with one sensor equipped with N_t transmit antennas observing a single point Gaussian source, denoted by $\theta[t]$, $t = 0, 1, 2, \ldots$, which has zero mean and variance σ_θ^2. The measurement received by the sensor at time t is given as

$$x[t] = \theta[t] + \omega[t] \tag{1}$$

where we assume $\omega[t]$ is independent and identically distributed (i.i.d.) Gaussian noise over time t, with zero mean and variance σ_ω^2.

The analog amplify and forward techniques [34], [35] are employed, where the sensor transmits over fading channels a scaled version of the analog measurements to the FC. It has been shown in [34] that this technique is asymptotically optimal, and exactly optimal in [35] under certain situations for Gaussian source estimation in the coherent MAC. In our model, the sensor amplifies the signal with a beamforming vector $\mathbf{p}[t] \in \mathbb{C}^{N_t \times 1}$ before transmitting it to the FC in the presence of an eavesdropper, as illustrated in Fig. 1. We assume both channels experience block fading, i.e., the channels remain constant during each coherence time interval, and are i.i.d. over different time intervals [36]. We further assume that the CSI of the FC is available, while the eavesdropper's CSI may or may not be available to the FC. The FC designs the optimal power allocation strategy based on the available CSI, and then sends $\mathbf{p}[t]$ back to the sensor via a secure feedback link. Note that CSI at the FC can be obtained by employing pilot training signals transmitted from the sensor.

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

$$y[t] = \mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]\theta[t] + \mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]\omega[t] + z[t] \tag{2a}$$

$$y_e[t] = \mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]\theta[t] + \mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]\omega[t] + z_e[t] \tag{2b}$$

where both $z[t]$ and $z_e[t]$ are i.i.d. zero mean complex Gaussian channel noise at the FC and the eavesdropper with variance σ_n^2 and σ_e^2, respectively, and $\mathbf{h}[t] = [h[t]_1, \ldots, h_n[t], \ldots, h_{N_t}[t]]^{\mathrm{T}}$ and $\mathbf{h}_e[t] = [h_{e1}[t], \ldots, h_{en}[t], \ldots, h_{eN_t}[t]]^{\mathrm{T}}$ are, respectively, the channels from the sensor to the FC and to the eavesdropper. We assume that $\{h_n[t]\}$ are i.i.d. complex Gaussian with zero mean and variance σ_h^2, and the elements in $\mathbf{h}_e[t]$ are also i.i.d. complex Gaussian, with zero mean and variance $\sigma_{h_e}^2$.

In order to minimize the MSE or *distortion* at the FC, the MMSE estimator is used to estimate for θ under the model (2) [37]. At time t, the distortion at the FC and the eavesdropper can be shown to be, respectively, as

$$D[t] = \sigma_\theta^2 - \frac{\sigma_\theta^4 \left(\mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]\right)^{\mathrm{H}} \mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]}{\sigma_n^2 + \left(\sigma_\theta^2 + \sigma_\omega^2\right)\left(\mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]\right)^{\mathrm{H}} \mathbf{h}^{\mathrm{T}}[t]\mathbf{p}[t]} \tag{3a}$$

$$D_e[t] = \sigma_\theta^2 - \frac{\sigma_\theta^4 \left(\mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]\right)^{\mathrm{H}} \mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]}{\sigma_e^2 + \left(\sigma_\theta^2 + \sigma_\omega^2\right)\left(\mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]\right)^{\mathrm{H}} \mathbf{h}_e^{\mathrm{T}}[t]\mathbf{p}[t]}. \tag{3b}$$

For a limited transmission power budget $\mathcal{P}_{\mathrm{tot}}$, we would like to minimize the distortion at the FC by adapting the sensor' transmit power $\mathbf{p}[t]^{\mathrm{H}}\mathbf{p}[t]$, while maintaining a certain level of security of the transmission. In information-theoretic security, the secrecy capacity is defined as the maximum transmission rate at which the mutual information between the confidential message and the signal received by the eavesdropper is less than a threshold [11]. Motivated by this idea, plus a close relation between MMSE and the mutual information of the channel input and output [17], [31], we consider a notion of *secrecy in estimation* from a noninformation-theoretic viewpoint by requiring the distortion at the eavesdropper to be greater than a threshold $D_{\min}$. In this way, some level of confidentiality can be achieved at the FC. We will refer to the minimum distortion threshold $D_{\min}$ as the *secrecy threshold* in the following.

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

A. Full CSI

In the case of full CSI, where we assume the FC can also acquire the channel information between the sensor and the eavesdropper, the power control policies can be derived such that the sensor is able to adjust the antenna transmission power 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 distortion performance with this assumption is instructive as well as useful as a benchmark for the distortion performance with partial CSI of the eavesdropper channels, to be analyzed subsequently.

1) *Long-Term Optimal Power Allocation:* In long-term power allocation, we assume that the crucial information lies in the long-term behavior of the estimates, such as long-term trends in the physical process observed, hence the FC would be more interested in the estimation over multiple fading blocks. We would like to minimize the long-term average distortion at the FC by adapting $\mathbf{p}$, where the average is across coherence time intervals, while keeping the long-term average sum of sensor transmission powers, defined as

$$\mathbb{E}\left[\mathbf{p}^{\mathrm{H}}\mathbf{p}\mathbb{E}\left[x_k^2\right]\right] = \mathbb{E}\left[\mathbf{p}^{\mathrm{H}}\mathbf{p}(\sigma_\theta^2 + \sigma_{\omega k}^2)\right] \tag{4}$$

to be less than the power budget $\mathcal{P}_{\mathrm{tot}}$. We also seek to maintain the average distortion at the eavesdropper to be greater than the threshold $D_{\min}$, i.e., $\mathbb{E}[D_e] \geq D_{\min}$, to ensure that some level of confidentiality can be achieved at the FC over the long term.

Furthermore, an additional constraint ensuring the average estimation quality being better at the FC is considered for more meaningful solutions. Therefore, the power control problem can be formulated as[3]

$$\begin{aligned}
\min_{\mathbf{p}} \quad & \mathbb{E}\left[D\right] \\
\text{s.t.} \quad & \mathbb{E}\left[\left(\sigma_\theta^2 + \sigma_\omega^2\right)\mathbf{p}^{\mathrm{H}}\mathbf{p}\right] \leq \mathcal{P}_{\mathrm{tot}} \\
& \mathbb{E}\left[D_e\right] \geq D_{\min}, \mathbb{E}\left[D_e\right] \geq \mathbb{E}\left[D\right].
\end{aligned} \tag{5}$$

Given the distortion expressions in (3), we can simplify problem (5) and rewrite it as

$$\min_{\mathbf{p}} \quad \mathbb{E}\left[\left(\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{-1}\right]$$

$$\text{s.t.} \quad \mathbb{E}\left[\mathbf{p}^{\mathrm{H}}\mathbf{p}\right] \leq \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2} \tag{6a}$$

$$\mathbb{E}\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{-1}\right] \geq D_{\mathrm{ma\_L}} \tag{6b}$$

$$\mathbb{E}\left[\frac{\alpha_e}{\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}}\right] \geq \mathbb{E}\left[\frac{\alpha}{\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}}\right] \tag{6c}$$

where

$$D_{\mathrm{ma\_L}} = \left(\frac{D_{\min}}{\frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2 + \sigma_\omega^2}} - 1\right) \Bigg/ \frac{\sigma_e^2\sigma_\theta^2}{(\sigma_\theta^2 + \sigma_\omega^2)\sigma_\omega^2}$$

$$\alpha = \frac{\sigma_n^2}{\sigma_\theta^2 + \sigma_\omega^2}$$

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

To solve problem (6), we apply the technique of Lagrange multipliers. The dual problem of (6) is defined as

$$\max_{\lambda, \nu, \tau} g(\lambda, \nu, \tau) \tag{7}$$

where λ, ν, and τ are nonnegative Lagrange multipliers, and the dual function $g(\lambda, \nu, \tau)$ associated with problem (6) is

$$\begin{aligned}
g(\lambda, \nu, \tau) = \min_{\mathbf{p}(\mathbf{h}, \mathbf{h}_e)} \int_{\mathbf{h}} \int_{\mathbf{h}_e} l\left(\mathbf{p}(\mathbf{h}, \mathbf{h}_e), \lambda, \nu, \tau\right)\ f_{\mathbf{h}} f_{\mathbf{h}_e}\, d\mathbf{h}\, d\mathbf{h}_e \\
+ \nu D_{\mathrm{ma\_L}} - \lambda \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2}
\end{aligned} \tag{8}$$

where $f_{\mathbf{h}} = \prod_{n=1}^{N_t} f(h_n)$ and $f_{\mathbf{h}_e} = \prod_{n=1}^{N_t} f(h_{en})$, with $f(\cdot)$ denoting the probability density function. Also

$$\begin{aligned}
l(\mathbf{p}(\mathbf{h}, \mathbf{h}_e), \lambda, \nu, \tau) = \frac{1 + \tau\sigma_n^2/\sigma_e^2}{\alpha + (\mathbf{h}^{\mathrm{T}}\mathbf{p})^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}} \\
+ \lambda\mathbf{p}^{\mathrm{H}}\mathbf{p} - \frac{\tau + \nu}{\alpha_e + (\mathbf{h}_e^{\mathrm{T}}\mathbf{p})^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}}.
\end{aligned}$$

It is not difficult to show that problem (6) is nonconvex. Let $[p_1(\mathbf{h}, \mathbf{h}_e), \ldots, p_{N_t}(\mathbf{h}, \mathbf{h}_e)]^{\mathrm{T}} = \mathbf{p}(\mathbf{h}, \mathbf{h}_e)$ be the complex gains allocated on each antenna, we can obtain a locally optimal solution from the following necessary Karush–Kuhn–Tucker (KKT) conditions [38] from the Lagrangian formulation for the optimal point:

$$\begin{aligned}
\frac{-h_n^{\mathrm{H}}\left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}}{\left[\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}\right]^2} + \frac{h_{en}^{\mathrm{H}}\left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}(\nu + \tau)}{(1 + \tau\sigma_n^2/\sigma_e^2)\left[\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right]^2} \\
+ \frac{\lambda}{1 + \tau\sigma_n^2/\sigma_e^2} p_n^{\mathrm{H}} = 0 \quad \forall n
\end{aligned} \tag{9a}$$

$$\lambda\left(\mathbb{E}\left[\mathbf{p}^{\mathrm{H}}\mathbf{p}\right] - \frac{\mathcal{P}_{\mathrm{tot}}}{{\sigma_\theta}^2 + {\sigma_\omega}^2}\right) = 0 \tag{9b}$$

$$\nu\left(D_{\mathrm{ma\_L}} - \mathbb{E}\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{-1}\right]\right) = 0 \tag{9c}$$

$$\begin{aligned}
\tau\left(\frac{\sigma_n^2}{\sigma_e^2}\mathbb{E}\left[\left(\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{-1}\right] - \mathbb{E}\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{-1}\right]\right) \\
= 0.
\end{aligned} \tag{9d}$$

To be more specific, we first assign arbitrary initial values to λ, ν, and τ, then iteratively apply the following Step 1 and Step 2 until (9b), (9c), and (9d) are satisfied.

STEP 1 With fixed $\tau^{(i)}$, $\lambda^{(i)}$, and $\nu^{(i)}$, find the optimal solution $\tilde{\mathbf{p}}$ of the Lagrange dual function (8), which can be obtained by solving the equations in (9a).

[3] In the long-term power allocation, the expectation $\mathbb{E}[\cdot]$ is taken w.r.t. both the sensor and the eavesdroppers channels, thus $\mathbb{E}[D(\mathbf{h}, \mathbf{h}_e)] = \int_{\mathbf{h}}\int_{\mathbf{h}_e} D(\mathbf{h}, \mathbf{h}_e)\, f_{\mathbf{h}} f_{\mathbf{h}_e}\, d\mathbf{h}\, d\mathbf{h}_e$, where $f(\cdot)$ denotes the probability density function.

STEP 2 With the resulting allocated power, apply the subgradient method to update the Lagrange multipliers, i.e.,

$$\begin{aligned}\lambda^{(i+1)} &= \left[\lambda^{(i)} + \epsilon \left(\mathbb{E}\left[\tilde{\mathbf{p}}^{\mathrm{H}}\tilde{\mathbf{p}}\right] - \frac{\mathcal{P}_{\mathrm{tot}}}{{\sigma_\theta}^2 + {\sigma_\omega}^2}\right)\right]^+ \\ \nu^{(i+1)} &= \left[\nu^{(i)} + \kappa\left(D_{\mathrm{ma\_L}} - \mathbb{E}\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{-1}\right]\right)\right]^+ \\ \tau^{(i+1)} &= \left[\tau^{(i)} + \upsilon\left(\frac{\sigma_n^2}{\sigma_e^2}\mathbb{E}\left[\left(\alpha + \left(\mathbf{h}^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{-1}\right]\right.\right. \\ &\qquad \left.\left. - \ \mathbb{E}\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\tilde{\mathbf{p}}\right)^{-1}\right]\right)\right]^+ \end{aligned} \tag{10}$$

where υ, κ, and ϵ are sufficiently small step-sizes for updating τ, ν, and λ, respectively.

REMARK To maximize the dual problem $g(\lambda, \nu, \tau)$, we applied subgradient methods to update Lagrange multipliers. This enables us to update all Lagrange multipliers simultaneously along certain directions. The subgradient method is guaranteed to converge, when the constant step-size, in our case υ, κ, and ϵ, are sufficiently small [39], [40]. In addition, in order to find the stationary point for the given Lagrange multipliers, we used fixed-point iteration [41] to solve a system of N_t nonlinear equations with N_t unknowns, where we use the most up-to-date information to solve for the nth variable in each iterate. As a result the dual function keeps decreasing until it reaches a minimum for the given Lagrange multipliers.

2) *Zero Information Leakage:* Other than diversity gain, another advantage with multiple transmit antennas is that we can employ techniques to hide the observation data from the eavesdropper by transmitting it onto the null space of the eavesdropper's channel. As a result, the eavesdropper is unable to detect any information about x.

Let the singular value decomposition[4] of $\mathbf{h}_e^{\mathrm{T}}$ be $\mathbf{h}_e^{\mathrm{T}} = \mathbf{USV}^{\mathrm{H}}$. The null space of the eavesdropper's channel can be represented by the span of the orthonormal column vectors of $\bar{\mathbf{V}}$, where $\bar{\mathbf{V}}$ is the last $N_t - 1$ columns of $\mathbf{V}$. Then, we can express the eavesdropper's channel null space as $\bar{\mathbf{V}}\bar{\mathbf{V}}^{\mathrm{H}}$ [42].

Next, we define a precoding matrix as

$$\mathbf{W} = \bar{\mathbf{V}}\bar{\mathbf{V}}^{\mathrm{H}} \tag{11}$$

where $\mathbf{W} \in \mathbb{C}^{N_t}$. The sensor sends $\mathbf{Wp}x$. The signal received by the FC and the eavesdropper are given by, respectively

$$y = \mathbf{h}^{\mathrm{T}}\mathbf{Wp}x + z = \mathbf{h}^{\mathrm{T}}\mathbf{Wp}\theta + \mathbf{h}^{\mathrm{T}}\mathbf{Wp}\omega + z \tag{12a}$$

$$y_e = \mathbf{h}_e^{\mathrm{T}}\mathbf{Wp}x + z_e = z_e \tag{12b}$$

and the transmission power can be computed as $((\mathbf{Wp})^{\mathrm{H}}\mathbf{Wp})(\sigma_\theta^2 + \sigma_\omega^2)$. Since the eavesdropper receives only noise, the distortion at the eavesdropper reaches its highest level of σ_θ^2, and hence we can remove constraints (6b) and (6c) in problem (6). In addition, we know that the beamforming vector should line-up with $\mathbf{h}^{\mathrm{T}}\mathbf{W}$ to minimize the distortion at the FC; thus, $\mathbf{p} = \sqrt{p_0}\frac{(\mathbf{h}^{\mathrm{T}}\mathbf{W})^{\mathrm{H}}}{\|\mathbf{hW}\|}$ with p_0 being real-valued. Therefore, problem (6) can be then simplified and rewritten as

$$\begin{aligned}\min_{p_0 \geq 0} \quad & \mathbb{E}\left[\left(\alpha + p_0\mathbf{h}^{\mathrm{T}}\mathbf{Wh}^*\right)^{-1}\right] \\ \text{s.t.} \quad & p_o \leq \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2}.\end{aligned} \tag{13}$$

It can be easily seen that when $p_0 = \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2}$ the long-term distortion at the FC reaches its minimum.

REMARK The signal is transmitted on the eavesdropper's null space via the precoding matrix $\mathbf{W}$. Therefore, we have the effective FC channel $\mathbf{h}^{\mathrm{T}}\mathbf{W}$, which is the projection of $\mathbf{h}^{\mathrm{T}}$ on the null space of $\mathbf{h}_e^{\mathrm{T}}$.

3) *Short-Term Optimal Power Allocation:* We can formulate a power allocation problem that minimizes the distortion at the FC, while satisfying a secrecy constraint at the eavesdropper and meeting the total power budget *in every transmission time slot*. We refer this as short-term power allocation. Note that for short-term optimal power allocation we cannot guarantee that the estimation quality is better at the FC at all times. Keeping this in mind, the optimal power allocation problem for a given set of channels can be cast as

$$\begin{aligned}\min_{\mathbf{p}} \quad & D = \min_{\mathbf{p}} \sigma_\theta^2 - \frac{\alpha\sigma_\theta^4}{\sigma_n^2}\left[1 - \frac{\alpha}{\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}^{\mathrm{T}}\mathbf{p}}\right] \\ \text{s.t.} \quad & \mathbf{p}^{\mathrm{H}}\mathbf{p} \leq \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2} \\ & \sigma_\theta^2 - \frac{\alpha_e\sigma_\theta^4}{\sigma_e^2}\left[1 - \frac{\alpha_e}{\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}}\right] \geq D_{\min}\end{aligned} \tag{14}$$

where $D_{\min}$ and $\mathcal{P}_{\mathrm{tot}}$ are, respectively, the distortion threshold at the eavesdropper and the total transmission power budget.

We aim to find an optimal beamforming vector $\mathbf{p}$ which meets the constraints in every fading block. The Lagrange multiplier technique is applied to solve this nonconvex optimization problem, and the details are omitted to avoid repetition.

B. Partial CSI

Due to the difficulties of perfectly acquiring the eavesdropper's CSI in practical setups, in this section we assume that the FC only has statistical knowledge of the eavesdropper's channel information. As it is not practical to consider short-term constraints that need to be satisfied at every time instant, we only look at the long-term scenario for the partial CSI case. We first explore the power allocation problem that minimizes the long-term distortion at the FC via the Lagrange multiplier technique. Next, we study the technique of artificial noise, where the artificial interference is transmitted to confuse the eavesdropper. We also analyze the asymptotic behavior

[4] Because $\mathbf{h}_e^{\mathrm{T}}$ is a row vector, $\mathbf{U}$ becomes a complex scalar and $\mathbf{S}$ is a complex row vector.

Algorithm 1:

```
1: Initialize the iteration index $q = 0$, choose an
   arbitrary initial value for $\{p_n(\mathbf{h})^{(q)}\}_{n=1}^{N_t}$, and obtain
   $l^{(q)} = l(\{p_n(\mathbf{h})^{(q)}\}, \lambda, \nu, \tau)$ from (15).
2: repeat
3: For $j = 1 : N_t$
      1) Find the complex gain $p_j(\mathbf{h})$ on antenna $j$
         such that $l(\{\{p_n(\mathbf{h})^{(q)}\}_{n\neq j}, p_j(\mathbf{h})\}, \lambda, \nu, \tau)$ is
         minimized.
      2) Update the transmission power of antenna $j$
         by $[p_1(\mathbf{h})^{(q)}, \ldots, p'_j(\mathbf{h})^{(q)}, \ldots, p_K(\mathbf{h})^{(q)}]$.
4: update $l^{(q+1)} = l(\{p'_n(\mathbf{h})^{(q)}\}, \lambda, \nu, \tau)$, and
   $q = q + 1$.
5: until Convergence: $(l^{(q+1)} - l^{(q)})/(l^{(q+1)}) < \zeta$; set
   $\{\tilde{p}_n(\mathbf{h})\} = \{p'_n(\mathbf{h})^{(q)}\}$.
```

of the distortion at the FC when equal power allocation is employed.

The power allocation problem is formulated similar to (5) but now with $\mathbf{p}$ being a function of $\mathbf{h}$, rather than a function of $\mathbf{h}$ and $\mathbf{h}_e$ as in the full CSI case. As the problem is again nonconvex, a locally optimal solution can be obtained as follows. Similar to (8), we define the Lagrange dual function as

$$g(\lambda, \nu, \tau) = \min_{p_n(\mathbf{h})\forall n} \int_{\mathbf{h}} l\left(\{p_n(\mathbf{h})\}, \lambda, \nu, \tau\right) \; f_{\mathbf{h}}\, d\mathbf{h} + \nu D_{\mathrm{ma\_L}} - \lambda \frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2}$$

with $l(\{p_n(\mathbf{h})\}, \lambda, \nu, \tau)$ expressed as

$$l\left(\{p_n(\mathbf{h})\}, \lambda, \nu, \tau\right) = \frac{1 + \tau\sigma_n^2/\sigma_e^2}{\alpha + \left(\mathbf{h}^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}} \mathbf{h}^{\mathrm{T}}\mathbf{p}} + \lambda\mathbf{p}^{\mathrm{H}}\mathbf{p} - \int_{\mathbf{h}_e} \frac{\tau + \nu}{\alpha_e + \left(\mathbf{h}^{\mathrm{T}}{}_e\mathbf{p}\right)^{\mathrm{H}} \mathbf{h}_e^{\mathrm{T}}\mathbf{p}} f_{\mathbf{h}_e} d\mathbf{h}_e. \tag{15}$$

For any set of channels $\mathbf{h}$, the optimal transmission power of the sensor is determined by the stationary points (or KKT points). We can then adapt similar methods as described in Section II-A1. In Step 1, the power polices $\tilde{\mathbf{p}}(\mathbf{h})$ can be derived by applying Algorithm 1 below. For fixed $\tau^{(i)}$, $\lambda^{(i)}$, and $\nu^{(i)}$, Algorithm 1 sequentially updates the transmit power on each antenna by minimizing the function given in (15), until a locally optimal solution is found. In Step 2, we update the Lagrange multipliers via the subgradient method.

REMARK In Step 1, $\tau^{(i)}$, $\lambda^{(i)}$, and $\nu^{(i)}$ are fixed, hence we drop the iteration number i in Algorithm 1; and ζ is a prespecified convergence criterion. Additionally, Algorithm 1 only gives a locally optimal solution, as the different initial values of $\mathbf{p}(\mathbf{h})^{(0)}$ may lead l in (15) to converge to a different minimum. Thus, in practice, the FC begins with several different initial points, and chooses the best resulting powers and forwards them to the sensor.

1) *Artificial Noise:* To enhance the system performance, we can use the technique of artificial noise to degrade the eavesdropper's channel. The artificial noise is generated by the transmitter (the sensor) in a way that the additional noise lies in the null space of the intended receiver's (the FC's) channel; as a result, the noise would not cause any damage toward the message received by the FC but would degrade the eavesdropper's channel [28], [43].

To be more specific, let the column vectors of $\hat{\mathbf{W}}^{\mathrm{H}} = [\mathbf{w}_1 \mathbf{W}_2]$ be an orthonormal basis of $\mathbb{C}^{N_t}$, with $\mathbf{w}_1 \in \mathbb{C}^{1\times N_t}$ representing the signal space of $\mathbf{h}$. The sensor then transmits

$$\mathbf{w}_1\sqrt{\beta}x + \mathbf{W}_2\mathbf{v} \tag{16}$$

where $\mathbf{W}_2\mathbf{v}$ is the artificial noise, which is chosen to be a random vector in the null space of $\mathbf{h}^{\mathrm{T}}$ to reduce the possibility of small "noise" seen by the eavesdropper. Here, $\mathbf{v} \in \mathbb{C}^{(N_t-1)\times 1}$ has $N_t - 1$ i.i.d. complex Gaussian entries with each having zero mean and variance β_a. Hence, the transmit power in each fading block is given as $\beta(\sigma_\theta^2 + \sigma_\omega^2) + \beta_a(N_t - 1)$. The signal received by the FC and the eavesdropper are, respectively, given as follows:

$$\begin{aligned} y &= \mathbf{h}^{\mathrm{T}}\hat{\mathbf{W}}^{\mathrm{H}}\left[\sqrt{\beta}x, \mathbf{v}^{\mathrm{T}}\right]^{\mathrm{T}} + z = \mathbf{h}^{\mathrm{T}}\mathbf{w}_1\sqrt{\beta}x + \mathbf{h}^{\mathrm{T}}\mathbf{W}_2\mathbf{v} + z \\ &= \mathbf{h}^{\mathrm{T}}\mathbf{w}_1\sqrt{\beta}x + z \end{aligned} \tag{17a}$$

$$\begin{aligned} y_e &= \mathbf{h}_e^{\mathrm{T}}\hat{\mathbf{W}}^{\mathrm{H}}\left[\sqrt{\beta}x, \mathbf{v}^{\mathrm{T}}\right]^{\mathrm{T}} + z_e \\ &= \mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1\sqrt{\beta}x + \mathbf{h}_e^{\mathrm{T}}\mathbf{W}_2\mathbf{v} + z_e. \end{aligned} \tag{17b}$$

REMARK As $\mathbf{h}_e$ has i.i.d. entries and $\hat{\mathbf{W}}$ is a unitary matrix, we know that $\mathbf{h}_e^{\mathrm{T}}\hat{\mathbf{W}}^{\mathrm{H}}$ also has i.i.d. elements. This indicates that $\mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1$ is independent of $\mathbf{h}_e^{\mathrm{T}}\mathbf{W}_2$. As a result, the effective noise at the eavesdropper becomes $\mathbf{h}_e^{\mathrm{T}}\mathbf{W}_2\mathbf{v} + z_e$.

Our objective is to derive the power used to produce artificial noise and to forward the observation signal so that the long-term distortion at the FC is minimized, while satisfying the three long-term constraints as described in Section II-A1. Assuming both the FC and the eavesdropper use the optimal MMSE estimator, the functional optimization problem can be written as follows:

$$\begin{aligned} &\min_{\beta(\mathbf{h}),\beta_a(\mathbf{h})} \quad \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \frac{\beta(\mathbf{h})\mathbf{h}^{\mathrm{T}}\mathbf{h}^*}{\sigma_n^2 + \beta(\mathbf{h})\mathbf{h}^{\mathrm{T}}\mathbf{h}^*\sigma_\omega^2}\right)^{-1}\right] \\ &\text{s.t.} \;\; (\sigma_\theta^2+\sigma_\omega^2)\mathbb{E}\left[\beta(\mathbf{h})\right] + (N_t-1)\,\mathbb{E}\left[\beta_a(\mathbf{h})\right] \le \mathcal{P}_{\mathrm{tot}} \\ &\quad \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \frac{\beta(\mathbf{h})|\mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1|^2}{\sigma_e^2 + \beta(\mathbf{h})|\mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1|^2\sigma_\omega^2 + \mathbf{h}_e^{\mathrm{T}}\mathbf{W}_2\mathbf{W}_2^{\mathrm{H}}\mathbf{h}_e^*\beta_a(\mathbf{h})}\right)^{-1}\right] \\ &\qquad \ge D_{\min} \\ &\quad \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \frac{\beta(\mathbf{h})|\mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1|^2}{\sigma_e^2 + \beta(\mathbf{h})|\mathbf{h}_e^{\mathrm{T}}\mathbf{w}_1|^2\sigma_\omega^2 + \mathbf{h}_e^{\mathrm{T}}\mathbf{W}_2\mathbf{W}_2^{\mathrm{H}}\mathbf{h}_e^*\beta_a(\mathbf{h})}\right)^{-1}\right] \\ &\qquad \ge \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \frac{\beta(\mathbf{h})\mathbf{h}^{\mathrm{T}}\mathbf{h}^*}{\sigma_n^2 + \beta(\mathbf{h})\mathbf{h}^{\mathrm{T}}\mathbf{h}^*\sigma_\omega^2}\right)^{-1}\right]. \end{aligned} \tag{18}$$

To solve problem (18), we apply the technique of Lagrange multipliers and use two steps similar to those described in Section II-A1, where in Step 1, with fixed Lagrange multipliers, we need to sequentially find the $\beta(\mathbf{h})$ and $\beta_a(\mathbf{h})$.

2) *Asymptotic Analysis:* In this section, we are interested in seeing how the long-term distortion decays at the FC as the number of antennas N_t increases, under both the power constraint and the secrecy constraints.

We consider the case where the beamforming vector is chosen to be lined up with the FC's channel in order to minimize the distortion at the FC, i.e.,

$$\mathbf{p} = \frac{\sqrt{p_0}\mathbf{h}^*}{\|\mathbf{h}\|} \tag{19}$$

where

$$p_0 = \min\left[\frac{1-\alpha_e D_{\text{ma\_L}}}{\sigma_{h_e}^2 D_{\text{ma\_L}}}, \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}\right].$$

This choice of p_0 guarantees that the three long-term constraints are satisfied. To see this, we first rewrite $\mathbb{E}[(\alpha_e + (\mathbf{h}_e^{\mathrm{T}}\mathbf{p})^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p})^{-1}]$ as

$$\begin{aligned}\mathbb{E}&\left[\left(\alpha_e + \left(\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{\mathrm{H}}\mathbf{h}_e^{\mathrm{T}}\mathbf{p}\right)^{-1}\right]\\ &= \mathbb{E}\left[\left(\alpha_e + p_0\frac{\mathbf{h}^{\mathrm{T}}\mathbf{h}_e^*\mathbf{h}_e^{\mathrm{T}}\mathbf{h}^*}{\|\mathbf{h}\|^2}\right)^{-1}\right]\\ &= \mathbb{E}\left[\left(\alpha_e + p_0\left(\|\mathbf{h}_e\|\left|\tilde{\mathbf{h}}^{\mathrm{T}}\tilde{\mathbf{h}}_e^*\right|\right)^2\right)^{-1}\right]\end{aligned} \tag{20}$$

where $\tilde{\mathbf{h}}^{\mathrm{T}} = \frac{\mathbf{h}^{\mathrm{T}}}{\|\mathbf{h}\|}$ and $\tilde{\mathbf{h}}_e^{\mathrm{T}} = \frac{\mathbf{h}_e^{\mathrm{T}}}{\|\mathbf{h}_e\|}$, which are two independent isotropic vectors on the N_t-dimensional unit sphere.

The first thing to be noticed from (20) is that $\|\mathbf{h}_e\| \cdot |\tilde{\mathbf{h}}^{\mathrm{T}}\tilde{\mathbf{h}}_e^*|$ can be thought of as the magnitude of the vector $\mathbf{h}_e^{\mathrm{T}}$ projected onto the vector space of $\mathbf{h}^{\mathrm{T}}$, as the second term can be written as[5] $|\tilde{\mathbf{h}}^{\mathrm{T}}\tilde{\mathbf{h}}_e^*| = |\cos(\angle(\tilde{\mathbf{h}}, \tilde{\mathbf{h}}_e))|$. This also indicates that $|\tilde{\mathbf{h}}^{\mathrm{T}}\tilde{\mathbf{h}}_e^*|$ is only related to the difference in the two channel directions. Therefore, by exploiting the independence of channel norm and channel direction [44], we can simplify (20) as

$$\mathbb{E}\left[(\alpha_e + p_0 XY)^{-1}\right] \tag{21}$$

where $X = \|\mathbf{h}_e\|^2$ and $Y = |\tilde{\mathbf{h}}^{\mathrm{T}}\tilde{\mathbf{h}}_e^*|^2$ are two independent random variables, with X being gamma distributed as

$$X \sim \Gamma\left(N_t, \sigma_{h_e}^2\right), f_X(x) = \frac{x^{N_t-1}e^{-x/\sigma^2 h_e}}{\sigma_{h_e}^{2N_t}(N_t-1)!}.$$

In addition, as $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{h}}_e$ are independent isotropic vectors, we have Y being beta distributed with parameters 1 and $N_t - 1$

$$Y \sim \text{Beta}(1, N_t-1), f_Y(y) = (N_t-1)(1-y)^{N_t-2}.$$

Since (21) is convex with respect to XY, applying Jensen's inequality and using the fact that $\mathbb{E}[X] = \sigma_{h_e}^2 N_t$, $\mathbb{E}[Y] = \frac{1}{N_t}$, we obtain a lower bound of (21) as

$$\begin{aligned}\mathbb{E}\left[(\alpha_e + p_0XY)^{-1}\right] &\geq (\alpha_e + p_0\mathbb{E}[X]\mathbb{E}[Y])^{-1}\\ &= \left(\alpha_e + p_0\sigma_{h_e}^2\right)^{-1}\end{aligned} \tag{22}$$

from which we can obtain a lower bound of the long-term distortion at the eavesdropper given as

$$\mathbb{E}[D_e] \geq \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4/\left(\sigma_\theta^2+\sigma_\omega^2\right)}{1+\sigma_{h_e}^2 p_0\ /\alpha_e} \tag{23}$$

which is independent of the number of transmit antennas, and decreases to $\sigma_\theta^2\sigma_\omega^2/(\sigma_\theta^2+\sigma_\omega^2)$ when the total transmit power is increased to infinity (as the long-term transmit power is $(\sigma_\theta^2+\sigma_\omega^2)\mathbb{E}(\mathbf{p}^{\mathrm{H}}\mathbf{p}) = (\sigma_\theta^2+\sigma_\omega^2)p_0$). Hence, we can set

$$\frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4/(\sigma_\theta^2+\sigma_\omega^2)}{1+\sigma_{h_e}^2 p_0/\alpha_e} \geq D_{\min}$$

to guarantee that the secrecy constraint at the eavesdropper is satisfied, i.e.,

$$p_0 \leq \frac{1-\alpha_e D_{\text{ma\_L}}}{\sigma_{h_e}^2 D_{\text{ma\_L}}}.$$

Therefore, given a total transmit power budget $\mathcal{P}_{\text{tot}}$, we see that the long-term power constraint as well as the secrecy constraint are met when

$$p_0 = \min\left[\frac{1-\alpha_e D_{\text{ma\_L}}}{\sigma_{h_e}^2 D_{\text{ma\_L}}}, \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}\right].$$

Furthermore, using the beamforming vector (19) gives us the following long-term distortion at the FC.

Theorem Let $\mathbf{p} = \frac{\sqrt{p_0}\mathbf{h}^*}{\|\mathbf{h}\|}$. Assuming h_n's are exponentially distributed with mean σ_h^2, then the long-term distortion at the FC using orthogonal access scheme follows:

$$\mathbb{E}[D] \sim \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2\sigma_h^2 p_0}\frac{1}{N_t} \text{ as } N_t \to \infty. \tag{24}$$

Proof We have

$$D = \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2}\left(\alpha + p_0\|\mathbf{h}\|^2\right)^{-1} \tag{25a}$$

$$= \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2}\left(\alpha + p_0\sum_{n=1}^{N_t}|h_n|^2\right)^{-1} \tag{25b}$$

$$\overset{(a)}{\sim} \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2}\left(\alpha + p_0 N_t\mathbb{E}\left[|h_n|^2\right]\right)^{-1} \text{ w.p.1} \tag{25c}$$

where (a) holds providing the expectation $\mathbb{E}[|h_n|^2]$ exists and applying the strong law of large numbers.

As h_n's are exponentially distributed with mean σ_h^2, then $\mathbb{E}[|h_n|^2] = \sigma_h^2$. Therefore

$$\begin{aligned}\mathbb{E}[D] &\sim \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2}\left(\alpha + p_0 N_t\sigma_h^2\right)^{-1}\\ &\sim \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2\sigma_h^2 p_0 N_t}\end{aligned} \tag{26}$$

[5] As $\angle(\mathbf{x}, \mathbf{y})$ is the angle between two vectors $\mathbf{x}$ and $\mathbf{y}$, we obtain $|\cos(\angle(\mathbf{x}, \mathbf{y}))| = \frac{|\mathbf{x}^{\mathrm{H}}\mathbf{y}|}{\|\mathbf{x}\|\cdot\|\mathbf{y}\|}$.

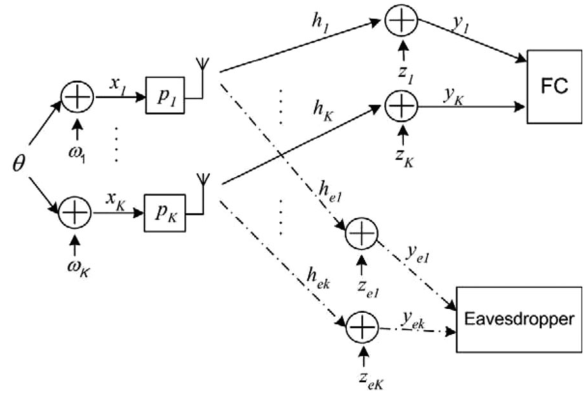

Fig. 2. Diagram of the WSN using orthogonal MAC scheme with the presence of an eavesdropper.

which is asymptotically equal to the constant $\sigma_\theta^2\sigma_\omega^2/(\sigma_\theta^2+\sigma_\omega^2)$ plus a term that decays to zero at the rate $1/N_t$. ■

From (26), we notice that if the beamforming vector has the form $\mathbf{p}=\sqrt{p_0}\mathbf{h}^*/\|\mathbf{h}\|$, the long-term distortion at the FC decreases as we increase N_t, whereas the lower bound of the distortion at the eavesdropper, as shown in (23), is dependent on the transmission power. Therefore, we conclude that, given a limited transmit power budget, the long-term distortion at the FC is always smaller than the distortion at the eavesdropper when the number of transmission antennas is large; in other words, all three long-term constraints can be satisfied when $\mathbf{p}=\sqrt{p_0}\mathbf{h}^*/\|\mathbf{h}\|$ with

$$p_0=\min\left[\frac{1-\alpha_e D_{\mathrm{ma\_L}}}{\sigma_{h_e}^2 D_{\mathrm{ma\_L}}},\frac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2+\sigma_\omega^2}\right].$$

III. MULTIPLE-SENSORS SCENARIO

For the single-point source estimation, if applying multiple antennas is not an option, an alternative way to improve the estimation accuracy at the FC is to employ multiple sensors. Therefore, in this section, we investigate the behavior of a multiple-sensor single-antenna system, followed by multiantenna multisensor systems in Section IV. In both cases, we assume that the FC and eavesdropper have a single receive antenna.

A schematic diagram of the wireless system model is shown in Fig. 2. We assume that the same single point Gaussian source θ as defined in Section II is observed by K sensors. The measurement received by the kth sensor is corrupted with noise ω_k and given as

$$x_k=\theta+\omega_k \tag{27}$$

where we assume ω_k is i.i.d. Gaussian noise over time, with zero mean and variance $\sigma_{\omega k}^2$. We assume pairwise synchronization between each sensor and the FC. The sensors employ the analog amplify and forward technique [34], [35] to scale the signal with $p_k\in\mathbb{C}$ before sending it to the FC via a set of orthogonal channels $[h_1,\ldots,h_K]$. The observation $\{x_k\}$ is also listened to by the eavesdropper via another set of orthogonal channels $[h_{e1},\ldots,h_{eK}]$.

The signals received by the FC and the eavesdropper from the kth sensor are given by, respectively

$$y_k=h_kp_k\theta+h_kp_k\omega_k+z_k \tag{28a}$$
$$y_{ek}=h_{ek}p_k\theta+h_{ek}p_k\omega_k+z_{ek} \tag{28b}$$

where both h_k and h_{ek} are zero mean i.i.d. complex Gaussian channels (Rayleigh fading) from sensor k to the FC and the eavesdropper with variances $\sigma_{h_k}^2$ and $\sigma_{h_ek}^2$, respectively, and z_k and z_{ek} represent i.i.d. complex Gaussian noise with zero mean and variances $\sigma_{n\,k}^2$ at the FC and $\sigma_{e\,k}^2$ at the eavesdropper, respectively.

The MMSE estimator is used at both the FC and the eavesdropper to estimate θ. At each channel instant, the MSE or *distortion* at the FC and the eavesdropper can be shown to be, respectively

$$D=\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^K\frac{(h_kp_k)^{\mathrm{H}}h_kp_k}{(h_kp_k)^{\mathrm{H}}h_kp_k\sigma_{\omega k}^2+\sigma_{n\,k}^2}\right)^{-1}$$
$$=\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^K\frac{g_k\beta_k}{g_k\beta_k\sigma_{\omega k}^2+\sigma_{n\,k}^2}\right)^{-1} \tag{29c}$$
$$D_e=\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^K\frac{(h_{ek}p_k)^{\mathrm{H}}h_{ek}p_k}{(h_{ek}p_k)^{\mathrm{H}}h_{ek}p_k\sigma_{\omega k}^2+\sigma_{e\,k}^2}\right)^{-1}$$
$$=\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^K\frac{g_{ek}\beta_k}{g_{ek}\beta_k\sigma_{\omega k}^2+\sigma_{e\,k}^2}\right)^{-1} \tag{29d}$$

where $g_k=h_k^{\mathrm{H}}h_k\in\mathbb{R}$ and $g_{ek}=h_{ek}^{\mathrm{H}}h_{ek}\in\mathbb{R}$ are, respectively, the channel power gains from sensor k to the FC and the eavesdropper, and $\beta_k=p_k^{\mathrm{H}}p_k\in\mathbb{R}$ is the power allocated on the kth sensor. This means that for a given set of $\{\beta_k\}$, any $\{p_k\}$ satisfying $p_k^{\mathrm{H}}p_k=\beta_k,\forall k$ would result in the same distortion, which implies p_k does not necessarily need to line-up with sensor k's channel direction; hence we focus on $\{\beta_k\}$ in multiple-sensor scenario.

In the following, we first look at the optimal power allocation, where the optimal power policies are designed by the FC based on the available CSI, and then sends $\{\beta_k\}$ back to the sensors via a secure feedback link. Applying a similar idea as in Section II-B1 of increasing the interference seen by the adversary in such a way that the channel is degraded while the channel of the legitimate receiver is not, we then consider a scenario where some of the sensors are employed to broadcast artificial interference which can be canceled off at the FC, but will in general degrade the eavesdropper's channel. The asymptotic behavior is also studied for the partial CSI case at the end of this section.

A. Full CSI–Optimal Power Allocation

In order to extend sensors' lifespan meanwhile maintaining a certain level of security for the network, we would like to minimize the distortion at the FC by adapting the sensors' transmit powers while satisfying the same three constraints as considered in multiple-antenna scenarios. With full knowledge of the eavesdropper's channel information, the power control problem can be formulated as

$$
\begin{aligned}
\min_{\beta_k(g_k, g_{e_k})\geq 0, \forall k} \quad & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{g_k\beta_k}{g_k\beta_k\sigma_{\omega k}^2+\sigma_{n\,k}^2}\right)^{-1}\right]\\
\text{s.t.} \quad & \mathbb{E}\left[\sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k\right]\leq \mathcal{P}_{\text{tot}}\\
& \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{g_{e_k}\beta_k}{g_{e_k}\beta_k\sigma_{\omega k}^2+\sigma_{e\,k}^2}\right)^{-1}\right]\geq D_{\min}\\
& \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{g_{e_k}\beta_k}{g_{e_k}\beta_k\sigma_{\omega k}^2+\sigma_{e\,k}^2}\right)^{-1}\right]\\
& \geq \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2}+\sum_{k=1}^{K}\frac{g_k\beta_k}{g_k\beta_k\sigma_{\omega k}^2+\sigma_{n\,k}^2}\right)^{-1}\right].
\end{aligned}
\tag{30}
$$

Similar setups have been considered in [32], where a minimum distortion threshold is set at the eavesdropper to ensure that the estimation error at the eavesdropper is no smaller than the requirement. In (30), an additional constraint guaranteeing a larger error always occurs at the eavesdropper is considered, hence one would expect no better performance being achieved at the FC compared with the results in [32] because of a smaller feasible region. Despite this, one can use the same methods as described in [32] by applying KKT condition and then numerically obtain locally optimal solutions for problem (30). Simulation results are given in Section VI.

Next, we explore the short-term distortion performance at the FC while satisfying a secrecy constraint at the eavesdropper and a total power constraint at the sensor *in every transmission instant*. As for the short-term optimal power allocation we cannot guarantee the distortion to be smaller at the legitimate receiver than the distortion at the eavesdropper for every fading block. For example, if the instantaneous channel SNR of the eavesdropper is greater than the channel SNR of the FC ($g_{ek}/\sigma_{e\,k}^2 > g_k/\sigma_{n\,k}^2, \forall k$), all sensors will have to stop transmitting, which is not so interesting. Therefore, the power allocation problem in short-term scenario is considered only in the case of full CSI. We can formulate the optimization problem and rewrite it as

$$
\begin{aligned}
\min_{\beta_k\geq 0\forall k} \quad & \sum_{k=1}^{K}\frac{-g_k\beta_k}{g_k\beta_k\sigma_{\omega k}^2+\sigma_{n\,k}^2}\\
\text{s.t.} \quad & \sum_{k=1}^{K}\left(\sigma_\theta^2+\sigma_{\omega k}^2\right)\beta_k\leq \mathcal{P}_{\text{tot}} && \text{(31a)}\\
& \sum_{k=1}^{K}\frac{g_{e_k}\beta_k}{g_{e_k}\beta_k\sigma_{\omega k}^2+\sigma_{e\,k}^2}\leq I_{\text{ms}} && \text{(31b)}
\end{aligned}
$$

where

$$
I_{\text{ms}}=\frac{1}{D_{\min}}-\frac{1}{\sigma_\theta^2}.
$$

As similar techniques depicted in Section II-A3 can be used to find a locally optimal solution, we omit details to avoid repetition.

REMARK Once the Lagrange dual functions are written for problem (30) and problem (31), one could notice that in the short-term scenario, for the given λ and ν, the power on the kth sensor depends only on its own channel conditions; whereas in the long-term scenario the transmission power of sensor k is a function of all sensors' channel information.

B. Partial CSI

1) *Optimal Power Allocation:* The optimal power allocation in partial CSI case is considered when the FC can access its own channel information but only has statistical knowledge of the eavesdropper. In this scenario, the problem is formulated similarly as problem (30) with the power scheme $\{\beta_k\}$ only being a function of the FC's channel information. A locally optimal solution can be then derived by applying similar techniques as used in [32] and Section II-B; thus details regarding the optimal power allocation in partial CSI case are omitted. The simulation results are given in Section VI for comparison.

2) *Partial CSI—Artificial Noise With Relays:* In a multiple-sensor network with only the FC's channel information, artificial noise can be produced when the observation information is crucial or there is a high security requirement. Different from Section II-B1, the concept of artificial noise in the multiple-sensor scenario is to transmit some random signals from different sensors which can be cancelled off at the intended receiver (the FC), but would significantly degrade the eavesdropper's channel [28]. Instead of forwarding the observation signal to the FC, some sensors broadcast artificial noise to confuse the eavesdropper in the network. In this section, we assume that a total number of M sensors estimate the source θ and then transmit the observation information $\{x_m\}_{m=1}^{M}$ to the FC, while the remaining $K-M$ sensors work as relays aiming to boost the secret transmission of the information $\{x_m\}$. This extends the setup of [28] in which there is one transmitter and $K-1$ relays.

The transmission is completed in two stages.

Let h_{s_mF}, h_{s_me}, and $h_{s_mr_k}$ be the channels from sensor m to the FC, the eavesdropper, and relay k, respectively. Denote h_{Fe} and h_{Fr_k} as the channels from the FC to the eavesdropper and relay k, respectively. In the first stage, as shown in Fig. 3, sensor m and the FC transmit $n_s h_{s_mF}$ and n_F, respectively, and the eavesdropper and relay k receive, respectively

$$
y_{e,1}=n_s\sum_{m=1}^{M}h_{s_mF}h_{s_me}+h_{\text{Fe}}n_F+z_{e,1} \tag{32a}
$$

$$
y_{r_k,1}=n_s\sum_{m=1}^{M}h_{s_mF}h_{s_mr_k}+h_{\text{Fr}_k}n_F+z_{k,1} \tag{32b}
$$

where $z_{e,1}$ and $z_{k,1}$ are zero mean i.i.d. complex Gaussian channel noises at the eavesdropper and at the kth relay with

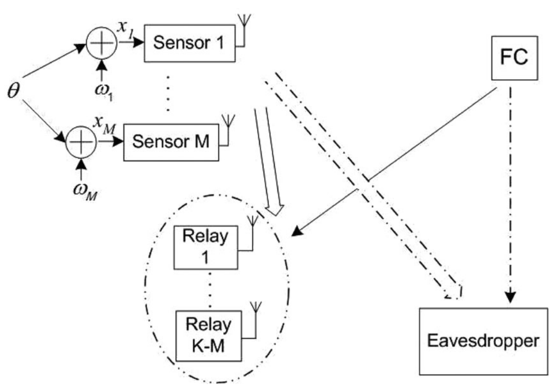

Fig. 3. Diagram of stage one transmission in the artificial noise with relays.

variances σ_e^2 and σ_r^2, respectively. n_s and n_F are artificial noises with variances σ_{ns}^2 and σ_{nF}^2, respectively.

At the second stage, sensor m forwards to the FC the amplified observation signal $x_m p_m$, and it also utilizes the public weight sequences $\{\bar{\gamma}_k\}$, which is a publicly available sequence of weights that are known to every participant (may also be seen by the eavesdropper) in the network, to transmit $-n_s \sum_{k=1}^{K-M} \bar{\gamma}_k h_{s_m r_k} h_{r_{\text{kF}}}$. We assume all the public sequences $\{\bar{\gamma}_k\}$ are i.i.d. zero mean complex Gaussian random variables with variance $\beta_{\bar{\gamma}}$, thus $\{\bar{\gamma}_k\}$ varies at each transmission to reduce the probability of the artificial noise being nulled at the eavesdropper. On the other hand, relay k transmits $\bar{\gamma}_k y_{r_k,1}$. Therefore, at the second stage the eavesdropper and the FC receive, respectively

$$\begin{aligned} y_{e,2} = & \sum_{m=1}^{M} x_m h_{s_m e} p_m \\ & + n_s \sum_{k=1}^{K-M} \bar{\gamma}_k \sum_{m=1}^{M} h_{s_m r_k} \left(h_{s_m F} h_{r_{\text{ke}}} - h_{r_{\text{kF}}} h_{s_m e} \right) \\ & + n_F \sum_{k=1}^{K-M} \bar{\gamma}_k h_{\text{Fr}_k} h_{r_{\text{ke}}} + \sum_{k=1}^{K-M} \bar{\gamma}_k h_{r_{\text{ke}}} z_{k,1} + z_{e,2} \quad (33) \\ y = & \sum_{m=1}^{M} x_m h_{sF} p_m + \sum_{k=1}^{K-M} \bar{\gamma}_k h_{r_{\text{kF}}} \left(h_{\text{Fr}_k} n_F + z_{k,1} \right) + z \\ \overset{(b)}{\Longrightarrow} & \sum_{m=1}^{M} x_m h_{s_m F} p_m + \sum_{k=1}^{K-M} \bar{\gamma}_k z_{k,1} h_{r_{\text{kF}}} + z \quad (34) \end{aligned}$$

where $z_{e,2}$ and z are zero mean i.i.d. complex Gaussian channel noises at the eavesdropper and the FC, respectively, with variances σ_e^2 and σ_n^2. In (34), (b) holds as n_F is known to the FC which can be cancelled off. Note that we assume synchronization between all sensors and the FC is available in this part of work, and the two-stage transmission can be completed in one fading block, as a result all the channels remain the same at the second stage transmission.

REMARK It is clear that the second term of (33) corresponds to the artificial noise generated from the M sensors at the first stage of transmission, which vanishes at the second stage as it reaches the FC [as can be seen in (34)]. In channel conditions where $h_{s_m F} h_{r_{\text{ke}}}$ is close to $h_{r_{\text{kF}}} h_{s_m e}$, instead of increasing the transmit power at both the first and the second stage transmissions to boost noise level, we expect to use the third term of (33) to increase the noise level at the eavesdropper with little power consumption.

Combining the two-stage transmission, we have that the signal received by the eavesdropper is given as

$$\mathbf{y}_e = \left[0, \sum_{m=1}^{M} h_{s_m e} p_m (\theta + \omega_m) \right]^{\text{T}} + \mathbf{H}_{\text{re}} \left[n_s, n_F \right]^{\text{T}} + \mathbf{z}_e \quad (35)$$

where $\mathbf{z}_e = [z_{e,1}, \sum_{k=1}^{K-M} \bar{\gamma}_k h_{r_{\text{ke}}} z_{k,1} + z_{e,2}]^{\text{T}}$ and $\mathbf{H}_{\text{re}}$ is expressed in (36), shown at the bottom of the page. Hence, the total power consumption P_{stages} for the two-stage transmission can be also derived as

$$\begin{aligned} P_{\text{stages}} = \sigma_{\text{ns}}^2 & \left(\sum_{m=1}^{M} |h_{s_m F}|^2 + \beta_{\bar{\gamma}} \sum_{m=1}^{M} |h_{s_m F}|^2 \sum_{k=1}^{K-M} |h_{s_m r_k}|^2 \right. \\ & \left. + \beta_{\bar{\gamma}} \sum_{m=1}^{M} \sum_{k=1}^{K-M} |h_{s_m r_k}|^2 |h_{r_{\text{kF}}}|^2 \right) \\ & + \beta_{\bar{\gamma}} (K - M) \sigma_r^2 + \sigma_{\text{nF}}^2 \beta_{\bar{\gamma}} \sum_{k=1}^{K-M} |h_{\text{Fr}_k}|^2 \\ & + \sum_{m=1}^{M} |p_m|^2 \left(\sigma_{\omega m}^2 + \sigma_{\omega}^2 \right). \end{aligned} \quad (37)$$

Let $\mathbf{K}_e$ be the covariance matrix of $[0, \sum_{m=1}^{M} h_{s_m e} p_m \omega_m]^{\text{T}} + \mathbf{H}_{\text{re}}[n_s, n_F]^{\text{T}} + \mathbf{z}_e$. As n_s, n_F, $z_{e,1}$, $z_{e,2}$, $\{z_{k,1}\}$, and $\{\omega_m\}$ are all independent random noises, $\mathbf{K}_e$ can be easily computed as

$$\mathbf{K}_e = \begin{bmatrix} \sigma_{\text{ns}}^2 \sum_{m=1}^{M} |h_{s_m F}|^2 |h_{s_m e}|^2 + \sigma_{\text{nF}}^2 |h_{\text{Fe}}|^2 + \sigma_e^2 & 0 \\ 0 & k_{e22} \end{bmatrix} \quad (38)$$

where k_{e22} is given as

$$\begin{aligned} k_{e22} = \beta_{\bar{\gamma}} \sigma_{\text{ns}}^2 & \sum_{k=1}^{K-M} \sum_{m=1}^{M} |h_{s_m r_k}|^2 \left| h_{s_m F} h_{r_{\text{ke}}} - h_{r_{\text{kF}}} h_{s_m e} \right|^2 \\ & + \beta_{\bar{\gamma}} \sigma_{\text{nF}}^2 \sum_{k=1}^{K-M} |h_{\text{Fr}_k}|^2 |h_{r_{\text{ke}}}|^2 + \beta_{\bar{\gamma}} \sigma_r^2 \sum_{k=1}^{K-M} |h_{r_{\text{ke}}}|^2 \\ & + \sum_{m=1}^{M} |p_m h_{s_m e}|^2 \sigma_{\omega m}^2 + \sigma_e^2. \end{aligned} \quad (39)$$

$$\mathbf{H}_{\text{re}} = \begin{bmatrix} \sum_{m=1}^{M} h_{s_m F} h_{s_m e} & h_{\text{Fe}} \\ \sum_{k=1}^{K-M} \bar{\gamma}_k \sum_{m=1}^{M} h_{s_m r_k} \left(h_{s_m F} h_{r_{\text{ke}}} - h_{r_{\text{kF}}} h_{s_m e} \right) & \sum_{k=1}^{K-M} \bar{\gamma}_k h_{\text{Fr}_k} h_{r_{\text{ke}}} \end{bmatrix} \quad (36)$$

Using the optimal MMSE estimator [37], from (34), (35), and (39) we can express the distortion D at the FC and the distortion D_e at the eavesdropper as

$$D = \left(\frac{1}{\sigma_\theta^2} + \frac{\left|\sum_{m=1}^{M} p_m h_{s_m F}\right|^2}{\sum_{m=1}^{M} |h_{s_m F} p_m|^2 \sigma_{\omega m}^2 + \beta_{\bar{\gamma}} \sigma_r^2 \sum_{k=1}^{K-M} |h_{r_{\mathrm{kF}}}|^2 + \sigma_n^2}\right)^{-1} \tag{40}$$

$$D_e = \sigma_\theta^2 \left(1 - \frac{\sigma_\theta^2 \left|\sum_{m=1}^{M} h_{s_m e} p_m\right|^2}{k_{e22} + \sigma_\theta^2 \left|\sum_{m=1}^{M} h_{s_m e} p_m\right|^2}\right). \tag{41}$$

In the partial CSI scenario, the FC is able to obtain the channel information of $\{h_{s_m F}\}$, $\{h_{\mathrm{Fr}_k}\}$, $\{h_{s_m r_k}\}$, and $\{h_{r_{\mathrm{kF}}}\}$ at each fading block, thus it can develop an intelligent transmission strategy such that the $\{p_m\}$, the variance of the public sequences $\beta_{\bar{\gamma}}$, and the artificial noise powers σ_{ns}^2, σ_{nF}^2 can be adapted in different fading blocks, while satisfying the long-term constraints as described in Section III-A. Let $G = [\{h_{s_m F}\}, \{h_{\mathrm{Fr}_k}\}, \{h_{s_m r_k}\}, \{h_{r_{\mathrm{kF}}}\}]$. The functional optimization problem can be then formulated as

$$\begin{aligned} \min_{\{p_m(G)\}, \beta_{\bar{\gamma}}(G), \sigma_{\mathrm{ns}}^2(G), \sigma_{\mathrm{nF}}^2(G)} \quad & \mathbb{E}[D] \\ \text{s.t.} \quad & \mathbb{E}\left[P_{\mathrm{stages}}\right] \leq \mathcal{P}_{\mathrm{tot}} \\ & \mathbb{E}[D_e] \geq D_{\min} \\ & \mathbb{E}[D_e] \geq \mathbb{E}[D] \end{aligned} \tag{42}$$

where P_{stages}, D, and D_e are expressed in (37), (40), and (41), which are functions of $\{p_m\}$, $\beta_{\bar{\gamma}}$, σ_{ns}^2, and σ_{nF}^2. We can then employ the same Lagrange multiplier technique as described in Section II-B to solve problem (42), where in Algorithm 1, we need to sequentially find $\{p_m(G)\}$, $\beta_{\bar{\gamma}}(G)$, $\sigma_{\mathrm{ns}}^2(G)$, and $\sigma_{\mathrm{nF}}^2(G)$. The details are omitted for brevity.

3) *Partial CSI—Asymptotic Analysis:* In order to see how the system performs as the number of sensors increases, in this section, we explore the asymptotic long-term distortion at the FC in the case of partial CSI. For analytical tractability, we consider a homogeneous WSN where all the measurement noise and fading distributions are i.i.d. As a consequence, we denote $\sigma_{\omega k}^2 = \sigma_\omega^2$, $\mathbb{E}[g_k] = \sigma_h^2$, $\mathbb{E}[g_{ek}] = \sigma_{h_e}^2$, $\sigma_{n\,k}^2 = \sigma_n^2$, and $\sigma_{e\,k}^2 = \sigma_e^2$, $\forall k$[6]. We also assume that the channel conditions of the FC and the eavesdropper satisfy $\sigma_h^2/\sigma_n^2 \geq \sigma_{h_e}^2/\sigma_e^2$, as a result the FC always has better estimation quality than that of the eavesdropper when the number of sensors is sufficiently large. In addition, if the secrecy constraint and the transmit power constraint are satisfied at every transmission, the long-term power constraint as well as the long-term secrecy constraint can also be met.

With equal power allocation, i.e., $\beta_k = \beta \forall k$, we can rewrite the short-term secrecy constraint (31b) as

$$\frac{K}{\sigma_\omega^2 \beta} \frac{1}{K} \sum_{k=1}^{K} \frac{1}{g_{ek} + \frac{\sigma_e^2}{\sigma_\omega^2 \beta}} \geq \frac{K - I_{\mathrm{ms}} \sigma_\omega^2}{\sigma_e^2}. \tag{43}$$

It is straightforward to show that $\frac{1}{g_{ek} + \frac{\sigma_e^2}{\sigma_\omega^2 \beta}}$ is convex in g_{ek} $\forall k$. For large K, applying Jensen's inequality we have

$$\begin{aligned} \frac{K}{\sigma_\omega^2 \beta} \frac{1}{K} \sum_{k=1}^{K} \frac{1}{g_{ek} + \frac{\sigma_e^2}{\sigma_\omega^2 \beta}} &\geq \frac{K}{\sigma_\omega^2 \beta} \frac{1}{\frac{\sum_{k=1}^{K} g_{ek}}{K} + \frac{\sigma_e^2}{\sigma_\omega^2 \beta}} \\ &\sim \frac{K}{\sigma_\omega^2 \beta} \frac{1}{\sigma_{h_e}^2 + \frac{\sigma_e^2}{\sigma_\omega^2 \beta}} \text{w.p.1.} \end{aligned} \tag{44}$$

Therefore, we can set

$$\frac{K}{\sigma_\omega^2 \beta} \frac{1}{\sigma_{h_e}^2 + \sigma_e^2/(\sigma_\omega^2 \beta)} \geq \frac{K - I_{\mathrm{ms}} \sigma_\omega^2}{\sigma_e^2}$$

to guarantee that the secrecy constraint is met (for large K). Let $r_e = \sigma_{h_e}^2/\sigma_e^2$. Together with the short-term transmit power constraint (31a), the transmission power is given as

$$\beta = \min\left[\frac{\mathcal{P}_{\mathrm{tot}}}{K\left(\sigma_\omega^2 + \sigma_\theta^2\right)}, \frac{I_{\mathrm{ms}}}{r_e\left(K - I_{\mathrm{ms}} \sigma_\omega^2\right)}\right]. \tag{45}$$

When $\beta = \frac{I_{\mathrm{ms}}}{r_e(K - I_{\mathrm{ms}} \sigma_\omega^2)}$, from (29a) we have

$$\begin{aligned} D &= \left(\frac{1}{\sigma_\theta^2} + \frac{1}{\sigma_\omega^2} \sum_{k=1}^{K} \frac{g_k}{g_k + \frac{\sigma_n^2}{\sigma_\omega^2 \beta}}\right)^{-1} \\ &= \left(\frac{1}{\sigma_\theta^2} + \frac{1}{\sigma_\omega^2} \sum_{k=1}^{K} \frac{g_k}{g_k + \frac{\sigma_n^2 r_e}{\sigma_\omega^2 I_{\mathrm{ms}}} K - \sigma_n^2 r_e}\right)^{-1} \\ &\overset{(c)}{\sim} \left(\frac{1}{\sigma_\theta^2} + \frac{K}{\sigma_\omega^2} \mathbb{E}\left[\frac{g_1}{g_1 + \frac{\sigma_n^2 r_e}{\sigma_\omega^2 I_{\mathrm{ms}}} K - \sigma_n^2 r_e}\right]\right)^{-1} \text{w.p.1} \end{aligned} \tag{46}$$

provided the expectation $\mathbb{E}[\frac{g_k}{g_k + \sigma_e^2/(\sigma_\omega^2 \beta)}]$ exists. (c) is the result of applying a strong law of large numbers for triangular arrays [45]. Hence, the long-term distortion at the FC is given as

$$\mathbb{E}[D] \sim \left(\frac{1}{\sigma_\theta^2} + \frac{K}{\sigma_\omega^2} \mathbb{E}\left[\frac{g_1}{g_1 + \frac{\sigma_n^2 r_e}{\sigma_\omega^2 I_{\mathrm{ms}}} K - \sigma_n^2 r_e}\right]\right)^{-1}. \tag{47}$$

[6] As both channels of the FC and the eavesdropper are distributed as i.i.d. zero mean complex Gaussian (Rayleigh fading) with variances σ_h^2 and $\sigma_{h_e}^2$, respectively, we know that the channel power gains g_k and g_{ek} are exponentially distributed with means σ_h^2 and $\sigma_{h_e}^2$, respectively.

As g_k, $\forall k$ is exponentially distributed with mean σ_h^2, we have

$$\begin{aligned}
&\mathbb{E}\left[\frac{g_1}{g_1 + \frac{\sigma_n^2 r_e}{\sigma_\omega^2 I_{\mathrm{ms}}} K - \sigma_n^2 r_e}\right] = 1 \\
&+ \frac{-\sigma_n^2 r_e \left(K - \sigma_\omega^2 I_{\mathrm{ms}}\right)}{\sigma_h^2 \sigma_\omega^2 I_{\mathrm{ms}}} e^{\frac{\sigma_n^2 r_e \left(K-\sigma_\omega^2 I_{\mathrm{ms}}\right)}{\sigma_h^2 \sigma_\omega^2 I_{\mathrm{ms}}}} \mathrm{E}_1\left[\frac{\sigma_n^2 r_e \left(K - \sigma_\omega^2 I_{\mathrm{ms}}\right)}{\sigma_h^2 \sigma_\omega^2 I_{\mathrm{ms}}}\right] \\
&\sim \frac{\sigma_h^2 \sigma_\omega^2 I_{\mathrm{ms}}}{\sigma_n^2 r_e \left(K - \sigma_\omega^2 I_{\mathrm{ms}}\right)} - \frac{2\sigma_h^4 \sigma_\omega^4 I_{\mathrm{ms}}^2}{\sigma_n^4 r_e^2 \left(K - \sigma_\omega^2 I_{\mathrm{ms}}^2\right)^2}
\end{aligned} \tag{48}$$

where function $\mathrm{E}_1[z]$ is related to the exponential integral $\mathrm{Ei}[z]$ through the expression $\mathrm{E}_1[z] = -\mathrm{Ei}[-z] = \int_z^\infty e^{-t} t^{-1} dt$ [46].

The case when $\beta = \mathcal{P}_{\mathrm{tot}}/(K(\sigma_\omega^2 + \sigma_\theta^2))$ has been explored in [47]. Therefore, combining the results of (45), (47), and (48), we have the long-term distortion at the FC being written as

$$\begin{aligned}
\mathbb{E}[D] &\sim \frac{\sigma_\theta^2 \sigma_n^4}{\sigma_n^4 + \sigma_h^2 \sigma_\theta^2 \sigma_n^2 \psi - \frac{2\sigma_h^4 \sigma_\omega^2 \sigma_\theta^2 \psi^2}{K}} \\
&\sim \frac{\sigma_\theta^2 \sigma_n^2}{\sigma_n^2 + \sigma_h^2 \sigma_\theta^2 \psi} + \frac{2\sigma_h^4 \sigma_\omega^2 \psi^2 \sigma_\theta^4}{\left(\sigma_n^2 + \sigma_h^2 \psi \sigma_\theta^2\right)^2 K}
\end{aligned} \tag{49}$$

where

$$\psi = \begin{cases} \dfrac{I_{\mathrm{ms}}}{r_e (1 - I_{\mathrm{ms}})}, & I_{\mathrm{ms}} < \dfrac{\mathcal{P}_{\mathrm{tot}} r_e K}{K\left(\sigma_\theta^2 + \sigma_\omega^2\right) + \mathcal{P}_{\mathrm{tot}} r_e \sigma_\omega^2} \\ \dfrac{\mathcal{P}_{\mathrm{tot}}}{\sigma_\theta^2 + \sigma_\omega^2}, & \text{otherwise.} \end{cases} \tag{50}$$

REMARK It can be noticed from (49) and (50), that when the channel conditions of the FC and the eavesdropper satisfy $\sigma_h^2/\sigma_n^2 \geq \sigma_{h_e}^2/\sigma_e^2$, for any given total transmission power $\mathcal{P}_{\mathrm{tot}}$ and secrecy threshold at the eavesdropper $D_{\min}$ [$I_{\mathrm{ms}} = 1/D_{\min} - 1/\sigma_\theta^2$ as defined in (31)], ψ is fixed for all fading blocks. In addition, the distortion at the FC decays to $\sigma_\theta^2 \sigma_n^2/(\sigma_n^2 + \sigma_h^2 \sigma_\theta^2 \psi)$ (as the number of sensors increases) at the rate $1/K$.

IV. MULTIPLE-SENSORS MULTIPLE-ANTENNAS SCENARIO

In this section, we want to explore the distortion performance for multiple sensors of two different multiple-antenna scenarios: 1) each sensor is equipped with single transmit antenna while the two receivers, namely the FC and the eavesdropper, are loaded with multiple receiving antennas and 2) multiple transmit antennas at each sensor but with a single receive antenna at the FC and the eavesdropper.

A. Multiple Antennas at the Receivers

Similar setups as in Section III are used, where the sensors are assumed to have a single transmit antenna. Each sensor amplifies and forwards their measurements to an N_r antenna FC with amplification factor $p_k \in \mathbb{C}$ via a slow-fading orthogonal MAC. 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. The signals received by the FC and eavesdropper from the kth sensor are then given by, respectively

$$\mathbf{y}_k = \theta p_k \mathbf{h}_k + \omega_k p_k \mathbf{h}_k + \mathbf{z}_k \tag{51a}$$

$$\mathbf{y}_{ek} = \theta p_k \mathbf{h}_{ek} + \omega_k p_k \mathbf{h}_{ek} + \mathbf{z}_{ek} \tag{51b}$$

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

$$\begin{aligned}
\mathbf{Y} &= [\mathbf{y}_1, \ldots, \mathbf{y}_K]^{\mathrm{T}} \\
&= \theta [p_1 \mathbf{h}_1, \ldots, p_k \mathbf{h}_k]^{\mathrm{T}} + [\omega_1 p_1 \mathbf{h}_1, \ldots, \omega_k p_k \mathbf{h}_k]^{\mathrm{T}} \\
&\quad + [\mathbf{z}_1, \ldots, \mathbf{z}_k]^{\mathrm{T}}.
\end{aligned} \tag{52}$$

Using the fact that each sensor transmits through an orthogonal MAC, the covariance of the noise factor $[\omega_1 p_1 \mathbf{h}_1, \ldots, \omega_k p_k \mathbf{h}_k]^{\mathrm{T}} + [\mathbf{z}_1, \ldots, \mathbf{z}_k]^{\mathrm{T}}$ can be derived as a $KN_r \times KN_r$ matrix:

$$C = \begin{bmatrix} \sigma_w^2 1 p_1^2 \mathbf{h}_1 \mathbf{h}_1^{\mathrm{H}} + \sigma_1^2 \mathbf{I}_{N_r} & & 0 \\ & \ddots & \\ 0 & & \sigma_{w\,K}^2 p_K^2 \mathbf{h}_K \mathbf{h}_K^{\mathrm{H}} + \sigma_K^2 \mathbf{I}_{N_r} \end{bmatrix}. \tag{53}$$

Applying the MMSE estimator, at time t the distortion at the FC is

$$\begin{aligned}
D &= \left(\frac{1}{\sigma_\theta^2} + \begin{bmatrix} p_1 \mathbf{h}_1 \\ \vdots \\ p_K \mathbf{h}_K \end{bmatrix}^{\mathrm{H}} C^{-1} \begin{bmatrix} p_1 \mathbf{h}_1 \\ \vdots \\ p_K \mathbf{h}_K \end{bmatrix}\right)^{-1} \\
&\overset{(d)}{=} \Bigg[\frac{1}{\sigma_\theta^2} + \sum_{k=1}^K p_k^{\mathrm{H}} p_k \\
&\quad \times \Big(\sigma_k^{-2} \mathbf{h}_k^{\mathrm{H}} \mathbf{h}_k - \sigma_k^{-2} \mathbf{h}_k^{\mathrm{H}} \mathbf{h}_k \\
&\quad\quad \times \left(\sigma_{w_k}^{-2} p_k^{-2} + \sigma_k^{-2} \mathbf{h}_k^{\mathrm{H}} \mathbf{h}_k\right)^{-1} \sigma_k^{-2} \mathbf{h}_k^{\mathrm{H}} \mathbf{h}_k\Big)\Bigg]^{-1} \\
&= \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^K \frac{g_k \beta_k}{\sigma_k^2 + g_k \sigma_{w\,k}^2 \beta_k}\right)^{-1}
\end{aligned} \tag{54}$$

where (d) results from applying the matrix inversion lemma, $\beta_k \triangleq p_k^{\mathrm{H}} p_k$ is the power allocated on the kth sensor, and $g_k \triangleq \mathbf{h}_k^{\mathrm{H}} \mathbf{h}_k = \sum_{m=1}^{N_r} h_{mk}^{\mathrm{H}} h_{mk}$ is the sum of channel power gains from the kth sensor to the FC with h_{mk} being the channel gain from sensor k to the mth antenna at the FC.

Similarly, the distortion at the eavesdropper is given as

$$D_e = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{g_{ek}\beta_k}{g_{ek}\beta_k \sigma_{\omega k}^2 + \sigma_{e\,k}^2} \right)^{-1} \tag{55}$$

where $g_{ek} \triangleq \mathbf{h}_{ek}^{\mathrm{H}} \mathbf{h}_{ek} = \sum_{n=1}^{N_e} h_{enk}^{\mathrm{H}} h_{enk}$ is the sum of channel power gains from the kth sensor to the eavesdropper and h_{enk} is the channel gain from sensor k to the nth antenna at the eavesdropper.

It can be seen that the distortion at the FC and the eavesdropper, i.e., (54) and (55) share the same expression with (29a) and (29b) of Section III. However, because both receivers are now equipped with multiple antennas, g_k and g_{ek} become the summation of channel power gains from the kth sensor to the FC and the eavesdropper, respectively. Therefore, the functional optimization problem that minimize the overall distortion at the FC while satisfying power and security constraints are cast and solved in the same way as (30).

B. Multiple Antennas at the Sensors

Let

$$\mathbf{h}_k = [h_{k,1}, \ldots, h_{k,N_k}]^{\mathrm{T}}$$
$$\mathbf{h}_{ek} = [h_{ek,1}, \ldots, h_{ek,N_k}]^{\mathrm{T}}$$

be the channels from the kth sensor to the FC and the eavesdropper, respectively. We assume the entries of both $\mathbf{h}_k$ and $\mathbf{h}_{ek}$ are i.i.d. distributed zero mean complex Gaussian with variances $\{\sigma_{h\,k}^2\}$ and $\{\sigma_{h_e k}^2\}$, respectively. At each transmission, sensor k adopts the analog amplify and forward techniques by scaling the measurement with an amplifying factor $\mathbf{p}_k \in \mathbb{C}^{N_k \times 1}$. The FC and the eavesdropper receive, respectively

$$y_k = \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k \theta + \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k \omega_k + z_k \tag{56a}$$
$$y_{ek} = \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k \theta + \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k \omega_k + z_{ek}. \tag{56b}$$

As a result, by employing the MMSE estimator, the distortion D at the FC and the distortion D_e at the eavesdropper can be written as

$$D = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}^{\mathrm{T}}{}_k \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}^{\mathrm{T}}{}_k \mathbf{p}_k}{\left(\mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{n\,k}^2} \right)^{-1} \tag{57a}$$

$$D_e = \left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k}{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{e k}^2} \right)^{-1}. \tag{57b}$$

In the long-term optimal power allocation, we have an additional constraint to ensure that the FC has a better estimation quality than at the eavesdropper; thus, the functional optimization problem can be expressed as

$$\begin{aligned} \min_{\mathbf{p}_k, \forall k} \; & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k}{\left(\mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{n\,k}^2} \right)^{-1} \right] \\ \text{s.t.} \; & \mathbb{E}\left[\sum_{k=1}^{K} \mathbf{p}_k^{\mathrm{H}} \mathbf{p}_k \left(\sigma_{\omega k}^2 + \sigma_\theta^2\right) \right] \le \mathcal{P}_{\text{tot}} \\ & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k}{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{e k}^2} \right)^{-1} \right] \\ & \quad \ge D_{\min} \\ & \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k}{\left(\mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{e k}^2} \right)^{-1} \right] \\ & \ge \mathbb{E}\left[\left(\frac{1}{\sigma_\theta^2} + \sum_{k=1}^{K} \frac{\left(\mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_{ek}^{\mathrm{T}} \mathbf{p}_k}{\left(\mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k\right)^{\mathrm{H}} \mathbf{h}_k^{\mathrm{T}} \mathbf{p}_k \sigma_{\omega k}^2 + \sigma_{n\,k}^2} \right)^{-1} \right]. \end{aligned} \tag{58}$$

We can apply the same techniques as previous sections to solve problem (58). We omit the details to avoid repetition.

V. MULTIPLE-EAVESDROPPER MULTIPLE-ANTENNAS SCENARIO

In this section, we look at how the long-term distortion at the FC decays as the number of transmit antennas increases when multiple eavesdroppers are present in the partial CSI scenario, where we first formulate the optimization problem, followed by asymptotic analysis.

Denote the channel vector at the jth eavesdropper as $\mathbf{h}_{e\,j}^{\mathrm{T}}$, where the entries of $\mathbf{h}_{e\,j}^{\mathrm{T}}$ are i.i.d. complex Gaussian variables with zero mean and variance $\sigma_{h_e\,j}^2$. Therefore, the signal received by eavesdropper j is given by

$$y_{e\,j} = \mathbf{h}_{ej}^{\mathrm{T}} \mathbf{p} \theta + \mathbf{h}_{ej}^{\mathrm{T}} \mathbf{p} \omega + z_{ej} \tag{59}$$

where the Gaussian source θ and the measurement sensitivity ω are the same as defined in Section II; z_{ej} is i.i.d. zero mean complex Gaussian channel noise at the jth eavesdropper with variance $\sigma_{e\,j}^2$.

In the multiple eavesdroppers scenario, we would like to maintain the average distortion at all eavesdroppers to be larger than the threshold $D_{\min}$ and the long-term distortion at the FC. Hence, the optimization problem is cast as

$$\min_{\mathbf{p}} \quad \mathbb{E}\left[D\right]$$
$$\text{s.t.} \quad \mathbb{E}\left[\left(\sigma_\theta^2 + \sigma_\omega^2\right) \mathbf{p}^{\mathrm{H}} \mathbf{p}\right] \le \mathcal{P}_{\text{tot}} \tag{60a}$$
$$\mathbb{E}\left[D_{ej}\right] \ge D_{\min} \tag{60b}$$
$$\mathbb{E}\left[D_{ej}\right] \ge \mathbb{E}\left[D\right], \; j = 1, \ldots, N_E \tag{60c}$$

where

$$D_{ej} = \sigma_\theta^2 - \frac{\sigma_\theta^4 (\mathbf{h}_{e\,j}^{\mathrm{T}} \mathbf{p})^{\mathrm{H}} \mathbf{h}_{e\,j}^{\mathrm{T}} \mathbf{p}}{\sigma_{e\,j}^2 + (\sigma_\theta^2 + \sigma_\omega^2)(\mathbf{h}_{e\,j}^{\mathrm{T}} \mathbf{p})^{\mathrm{H}} \mathbf{h}_{e\,j}^{\mathrm{T}} \mathbf{p}}.$$

In problem (60), apart from the two sets of security constraints, it almost shares the same features as the single eavesdropper case as shown in (30). One could use the similar approaches to obtain the locally optical solution. Therefore, in the section, we concentrate on the asymptotic analysis.

THEOREM Choose the beamforming vector $\mathbf{p}$ to be lined up with the FC's channel, i.e., $\mathbf{p} = \frac{\sqrt{\hat{p}}\mathbf{h}^*}{\|\mathbf{h}\|}$. Then, the long-term distortion at the FC using orthogonal access scheme follows:

$$\mathbb{E}\,[D] \sim \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2\sigma_h^2\hat{p}}\frac{1}{N_t}\text{as}N_t \to \infty \tag{61}$$

where

$$\hat{p} = \min\left[\left(\frac{\frac{\sigma_\theta^4}{\sigma_\omega^2+\sigma_\theta^2}}{D_{\min} - \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2}} - 1\right)\frac{1}{SNR_{\max}}, \frac{\mathcal{P}_{\text{tot}}}{\sigma_\theta^2+\sigma_\omega^2}\right]$$

with

$$\text{SNR}_{\max} = \max\frac{\sigma_{h_e j}^2}{\sigma_{e\,j}^2}$$

being the largest SNR among all the eavesdroppers.

We outline the proof, which is similar to that given in Section II-B2. First, because the eavesdroppers' channels are independent we can show that the long-term distortion at eavesdropper j is lower bounded by

$$\frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4/(\sigma_\theta^2+\sigma_\omega^2)}{1+\sigma_{h_e j}^2\hat{p}/\alpha_{ej}}$$

where $\alpha_{ej} = \sigma_{e\,j}^2/(\sigma_\theta^2+\sigma_\omega^2)$. To satisfy the secrecy constraints in (60b) and (60c), $\hat{p}$ is set to meet

$$\min\left[\frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4/(\sigma_\theta^2+\sigma_\omega^2)}{1+\sigma_{h_e j}^2\hat{p}/\alpha_{ej}}\right] \geq D_{\min}$$

which gives

$$\hat{p} \leq \left(\frac{\frac{\sigma_\theta^4}{\sigma_\omega^2+\sigma_\theta^2}}{D_{\min} - \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2}} - 1\right)\frac{1}{SNR_{\max}}.$$

Next, applying the strong law of large numbers we obtain

$$\mathbb{E}[D] \sim \frac{\sigma_\theta^2\sigma_\omega^2}{\sigma_\theta^2+\sigma_\omega^2} + \frac{\sigma_\theta^4\alpha^2}{\sigma_n^2\sigma_h^2\hat{p}}\frac{1}{N_t} \quad \text{as} \quad N_t \to \infty.$$

We also notice that the long-term distortion at the FC reduces to the single eavesdropper case when the eavesdroppers' channel gains and channel noise variances are identical, i.e., $\sigma_{h_e j}^2 = \sigma_{h_e}^2$ and $\sigma_{e\,j}^2 = \sigma_e^2, \forall j$.

VI. NUMERICAL RESULTS

In this section, we first show the performance of a multiple-antenna single-sensor system via numerical simulations. For simplicity, we consider the source θ to be Gaussian distributed with zero mean and variance $\sigma_\theta^2 = 1$ mW. The sensor measurement sensitivity is set to $\sigma_\omega^2 = 10^{-3}$ mW. We assume the same noise level for both the FC and the eavesdropper's channel, where $\sigma_n^2 = \sigma_e^2 = 10^{-8}$ mW. In the following simulation, the secrecy threshold is chosen from the range $0.05 \leq D_{\min} \leq 0.65$. Furthermore, we consider the pathloss of signal power, in decibel scale, at the FC and the eavesdropper following the free-space pathloss model [48]

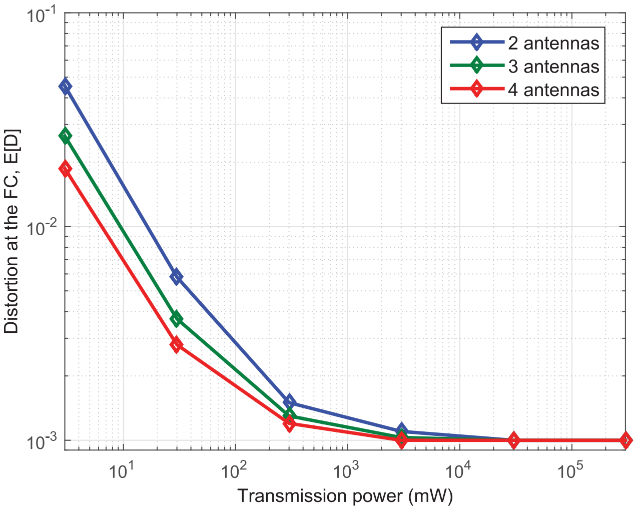

Fig. 4. Performance comparison when zero information leakage is achieved.

$$PL = 20\log_{10}(\text{Dist}) + 20\log_{10}(f) - 27.55 \tag{62}$$

where Dist ∈ $\{d, d_e\}$ is the distance between the sensor and the FC or the eavesdropper in meters, and f is the signal frequency in megahertz (we assume the network uses operation frequency of 800 MHz, and the sensor is closer to the FC than to the eavesdropper with the distance from the sensor to the FC and to the eavesdropper being set to 127 and 130 m, respectively). Thus, the channel power gain follows an exponential distribution with mean of $10^{-\frac{PL}{10}}$ mW.

Fig. 4 illustrates the distortion performance at the FC when zero information leakage is achieved with the number of transmit antennas $N_t \in \{2, 3, 4\}$, for a wide range of transmission power budgets. With the eavesdropper's full CSI, we can rotate and transmit the information on the null space of the eavesdropper's channel by sacrificing only a proportion of the FC's channel gain, and hence no information is leaked to the eavesdropper. As $\mathcal{P}_{\text{tot}}$ increases, the distortion gradually approaches its lower bound $\sigma_\theta^2 - (\sigma_\theta^2/(\sigma_\theta^2+\sigma_\omega^2))$, i.e., 9.99×10^{-4}.

Fig. 5 depicts the distortion performance at the FC versus the secrecy threshold for a three-antenna single-sensor system. For comparison, we plot the system performance under four scenarios: long-term full CSI, partial CSI, partial CSI with artificial noise, and short-term full CSI. First, owing to the channel knowledge of both the FC and the eavesdropper, it is not surprising to see that the performance of the full CSI scenario is superior to the performance of partial CSI. Similar performance gains can be

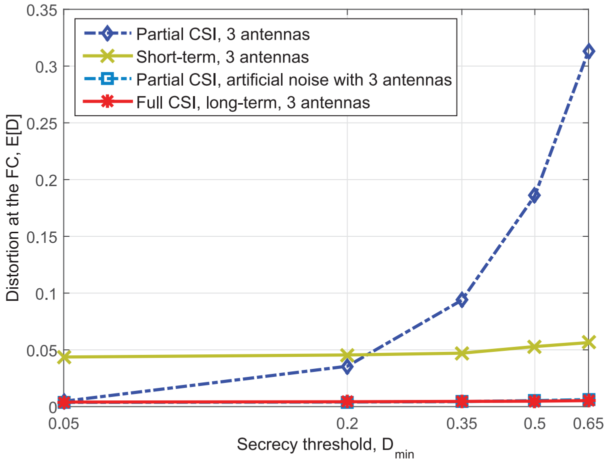

Fig. 5. Performance comparison between full CSI, partial CSI, and artificial noise in a multiple-antenna single-sensor system.

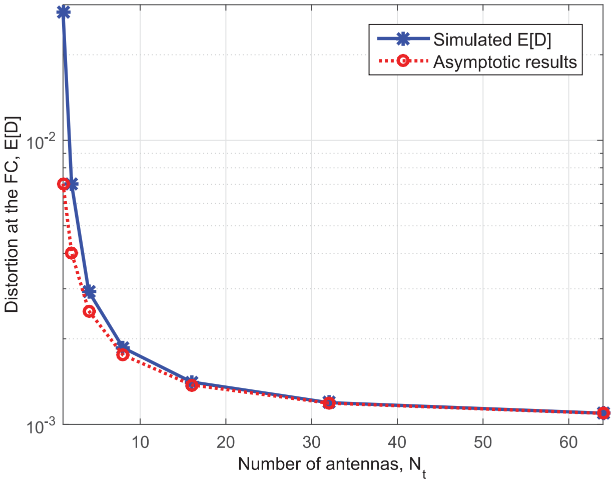

Fig. 6. Asymptotic behavior of $\mathbb{E}[D]$ in a multiple-antenna system.

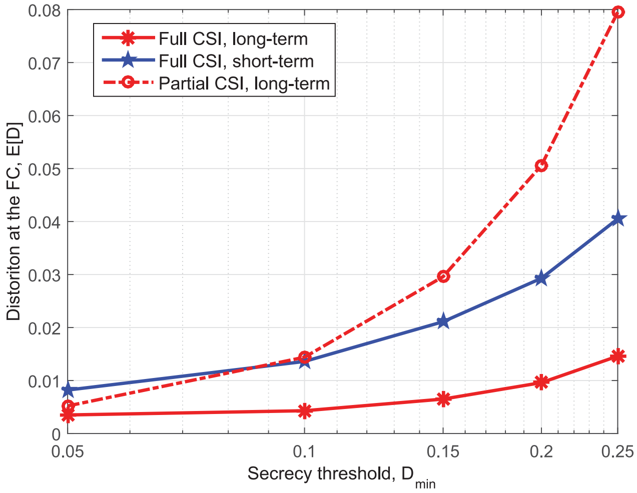

Fig. 7. Performance comparison in an eight-sensor network, with $\sigma^2_\omega = 10^{-3}$ mW, and the distance from each sensor to the FC and to the eavesdropper are 125, 126, 127, 128, 129, 130, 131, 132, and 139 m, 138, 137, 136, 135, 131, 130, and 129 m, respectively.

seen for the full CSI short-term distortion. We also notice the superior performance of artificial noise in the partial CSI case. This is because in the full CSI scenario, due to the full channel information of both FC and the eavesdropper, the direction of the beamformer can be designed to benefit the FC with little information being leaked to the eavesdropper; and in the case of artificial noise, a small amount of "noise" is deliberately generated to degrade the eavesdropper's channel, which indicates that the secrecy threshold can be easily achieved without sacrificing much transmit power; whereas for the case of partial CSI without artificial noise, some antennas need to be switched OFFto achieve the secrecy requirements, which is also the case for the short-term scenario.

We next present results for the asymptotic behavior for the multiple-antenna single-sensor scenario, where the beamforming vector is aligned with the FC's channel direction. In Fig. 6, we can see that the asymptotic distortion performance of the results given in (26) match closely the distortion at the FC obtained through simulations, and the gap gradually vanishes as N_t keeps increasing. Note that the asymptotic behavior in a multiple-sensor network, obtained by applying (49), can be plotted similarly as Fig. 6.

In the following, we study the distortion performance at the FC for a multiple-sensor network, where we assume the total transmit power budget is 30 mW and all sensors share the same measurement sensitivity, i.e., $\sigma^2_{\omega_k} = \sigma^2_\omega, \forall k$. We apply the same pathloss model (62) and we consider the same noise level for both the FC and the eavesdropper's channel, where $\sigma^2_n = \sigma^2_e = 10^{-8}$ mW. From (29b) we notice that the distortion at the eavesdropper D_e drops to its minimum value $\sigma^2_\theta \sigma^2_\omega / (K\sigma^2_\theta + \sigma^2_\omega)$ as all the transmission powers approach infinity, and D_e would reach its maximum value σ^2_θ when $\beta_k = 0, \forall k$.

In Fig. 7, the secrecy threshold is chosen from the range $0.05 \leq D_{\min} \leq 0.25$. In the plot, the short-term distortion result is obtained by averaging over 10 000 channel realizations. Not surprisingly, we can see that long-term distortion performances are superior to the performances of short-term power allocation problem due to a smaller feasibility region for the latter, where the sensors are required to ensure that the power constraint and the secrecy constraint are satisfied in every transmission slot.

In Fig. 8, we study the system performance of a three-sensor network with two sensors working as relays to generate artificial noise. The secrecy threshold is set to $0.05 \leq D_{\min} \leq 0.8$. All the sensors (including two relays) are 127 m away from the FC which is 3 m closer than to the eavesdropper, and we also assume the distances from the two relays to the sensor are 10 and 20 m, respectively. Due to diversity gains, it is clear to see the superior performance of the three-sensor network. As for the one-sensor two-relay network, it performs the same way as the one-sensor system when the distortion threshold is small; however, as the secrecy requirement increases at the eavesdropper, the performance gap grows. This is because the two relays are activated only when $D_{\min}$ is relatively large, where a small portion of the total transmit power is used to produce artificial noise to reach the secrecy threshold; whereas in the other two systems, without the eavesdropper's channel

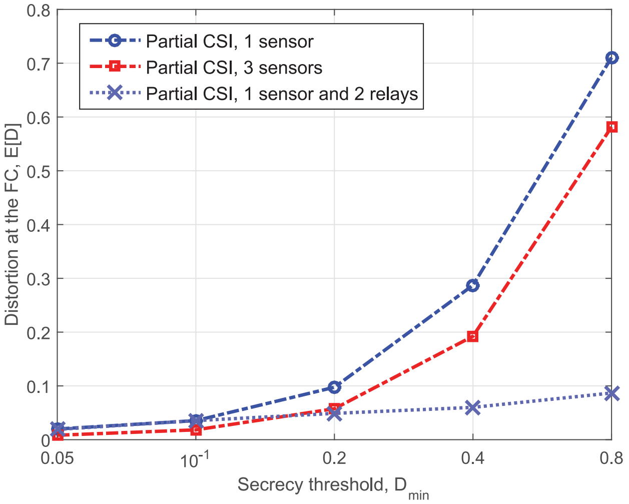

Fig. 8. Multiple-sensor network with relays, with $\sigma_\omega^2 = 10^{-3}$ mW.

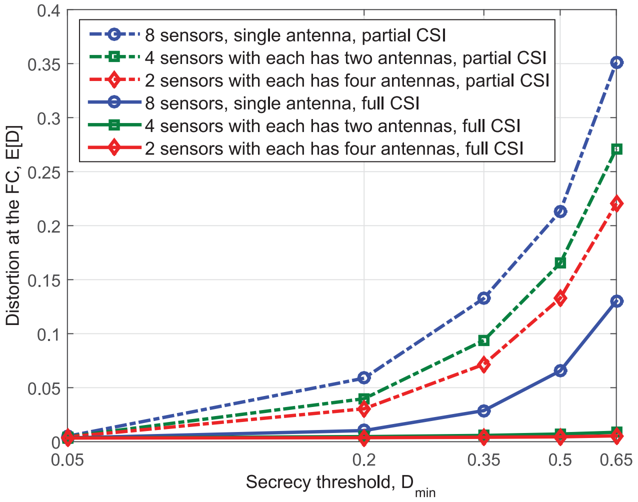

Fig. 9. Performance comparison among multiple-sensor networks with the total number of transmitting antennas of eight.

information, the sensor(s) may need to reduce the transmission power to achieve the high secrecy requirement.

In Fig. 9, we compare the distortion performance of three different types of multiple-sensor network with a fixed total number of transmitting antennas of eight. It is seen that the distortion performance of the four-antenna two-sensors network is followed by the performance of a two-antenna four-sensor network, which are both superior to the single-antenna eight-sensor scenario. This suggests that we can better utilize a multiple-antenna system for a point source estimation to achieve a better performance at the FC under the secrecy constraints.

VII. Conclusion

In this paper, we have considered the problem of transmit power allocation for distortion minimization in multisensor estimation in the presence of an eavesdropper, where the sensors can also have multiple transmit antennas. We studied the asymptotic behavior for the long-term distortion at the FC under the equal power allocation for the multiple-sensor scenario, and also for the multiple-antenna single-sensor scenario, where the transmit beamforming vector at the sensor is aligned with the direction of the FC. In addition, in a multiple-sensor network, when the secrecy requirement is high, some sensors can be deployed to artificially produce noise to improve the transmission security. For the multiple-antenna single-sensor system, depending on the availability of the eavesdropper's channel information, we can achieve zero information leakage or degrade the eavesdropper's channel and enhance the system performance by exploiting multiple-antenna techniques under the long-term power allocation scenario. Future work includes a study optimal power allocation in secrecy outage problems, where an outage event is declared if the instantaneous distortion at the eavesdropper is less than the target secrecy threshold, and also with multiple receive antennas at the FC and the eavesdropper.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci
Wireless sensor networks: A survey
Computer Netw., vol. 38, no. 4, pp. 393–422, 2002.

[2] J. J. Xiao, Z. Q. Luo, S. Cui, and A. J. Goldsmith
Power-efficient analog forwarding transmission in an inhomogeneous Gaussian sensor network
In *Proc. IEEE 6th Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2005, pp. 121–125.

[3] S. Cui, J.-J. Xiao, A. Goldsmith, Z.-Q. Luo, and H. Poor
Estimation diversity and energy efficiency in distributed sensing
IEEE Trans. Signal Process., vol. 55, no. 9, pp. 4683–4695, Sep. 2007.

[4] J.-J. Xiao, S. Cui, Z.-Q. Luo, and A. Goldsmith
Power scheduling of universal decentralized estimation in sensor networks
IEEE Trans. Signal Process., vol. 54, no. 2, pp. 413–422, Feb. 2006.

[5] I. Bahceci and A. Khandani
Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation
IEEE Trans. Commun., vol. 56, no. 7, pp. 1146–1156, Jul. 2008.

[6] C.-H. Wang and S. Dey
Power allocation for distortion outage minimization in clustered wireless sensor networks
In *Proc. IEEE Wireless Commun. Mobile Comput. Conf.*, 2008, pp. 395–400.

[7] C.-H. Wang, A. S. Leong, and S. Dey
Distortion outage minimization and diversity order analysis for coherent multiaccess
IEEE Trans. Signal Process., vol. 59, no. 12, pp. 6144–6159, Dec. 2011.

[8] C. E. Shannon
Communication theory of secrecy systems
Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[9] A. D. Wyner
The wire-tap channel
Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[10] A. Khisti, A. Tchamkerten, and G. W. Wornell
Secure broadcasting over fading channels
IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[11] P. K. Gopala, L. Lai, and H. El-Gamal
On the secrecy capacity of fading channels
IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[12] Y. Liang, H. Poor, and S. Shamai
Secure communication over fading channels
IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[13] A. Khisti and G. W. Wornell
Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel
IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[14] R. Bustin, R. Liu, H. V. Poor, and S. Shamai
An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel
EURASIP J. Wireless Commun. Netw., vol. 2009, 2009, Art. no. 370970.

[15] T. Liu and S. Shamai
A note on the secrecy capacity of the multiple-antenna wiretap channel
IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[16] E. Ekrem and S. Ulukus
Secure lossy transmission of vector Gaussian sources
IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5466–5487, Sep. 2013.

[17] F. Naghibi, S. Salimi, and M. Skoglund
The CEO problem with secrecy constraints
In *Proc. IEEE Int. Symp. Inf. Theory*, 2014, pp. 756–760.

[18] G. Bagherikaram and K. N. Plataniotis
Secure hybrid digital-analog wyner-ziv coding
In *Proc. IEEE 22nd Int. Symp. Pers. Indoor Mobile Radio Commun.*, 2011, pp. 1161–1166.

[19] J. Villard and P. Piantanida
Secure multiterminal source coding with side information at the eavesdropper
IEEE Trans. Inf. Theory, vol. 59, no. 6, pp. 3668–3692, Jun. 2013.

[20] Y. Kaspi and N. Merhav
Zero-delay and causal secure source coding
IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 6238–6250, Nov. 2015.

[21] M. Gastpar, B. Rimoldi, and M. Vetterli
To code, or not to code: lossy source-channel communication revisited
IEEE Trans. Inf. Theory, vol. 49, no. 5, pp. 1147–1158, May 2003.

[22] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi
QoS based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach
IEEE Trans. Signal Process., vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[23] R. Soosahabi and M. Naraghi-Pour
Scalable phy-layer security for distributed detection in wireless sensor networks
IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1118–1126, Aug. 2012.

[24] Z. Li and T. J. Oechtering
Privacy-aware distributed Bayesian detection
IEEE J. Select. Topics Signal Process., vol. 9, no. 7, pp. 1345–1357, Oct. 2015.

[25] B. Kailkhura, V. Nadendla, and P. Varshney
Distributed inference in the presence of eavesdroppers: A survey
IEEE Commun. Mag., vol. 53, no. 6, pp. 40–46, Jun. 2015.

[26] V. S. S. Nadendla and P. K. Varshney
Design of binary quantizers for distributed detection under secrecy constraints
IEEE Trans. Signal Process., vol. 64, no. 10, pp. 2636–2648, May 2016.

[27] V. S. S. Nadendla, S. Liu, and P. K. Varshney
Design of transmit-diversity schemes in detection networks under secrecy constraints
In *Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2015, pp. 794–801.

[28] S. Goel and R. Negi
Guaranteeing secrecy using artificial noise
IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[29] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor
Improving wireless physical layer security via cooperating relays
IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[30] S. Gerbracht, A. Wolf, and E. A. Jorswieck
Beamforming for fading wiretap channels with partial channel information
In *Proc. IEEE Int. ITG Workshop Smart Antennas*, 2010, pp. 394–401.

[31] D. Guo, S. Shamai, and S. Verdú
Mutual information and minimum mean-square error in Gaussian channels
IEEE Trans. Inf. Theory, vol. 51, no. 4, pp. 1261–1282, Apr. 2005.

[32] X. Guo, A. Leong, and S. Dey
Power allocation for distortion minimization in distributed estimation with security constraints
presented at the IEEE 15th Symp. Signal Process. Adv. Wireless Commun., Toronto, ON, Canada, Jun. 2014.

[33] R. Wong
Asymptotic Approximations of Integrals, vol. 34. Philadelphia, PA, USA: SIAM, 2001.

[34] M. Gastpar and M. Vetterli
Source-channel communication in sensor networks
In *Information Processing in Sensor Networks*. New York, NY, USA: Springer, 2003, pp. 162–177.

[35] M. Gastpar
Uncoded transmission is exactly optimal for a simple Gaussian "sensor" network
IEEE Trans. Inf. Theory, vol. 54, no. 11, pp. 5247–5251, Nov. 2008.

[36] 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.

[37] S. M. Kay
Fundamentals of Statistical Signal Processing: Estimation Theory. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[38] S. Boyd and L. Vandenberghe
Convex Optimization. New York, NY, USA: Cambridge Univ. Press, 2004.

[39] D. P. Bertsekas
Nonlinear Programming. Belmont, MA, USA: Athena Scientific, 1999.

[40] S. Boyd, L. Xiao, and A. Mutapcic
Subgradient methods
Stanford University, Stanford, CA, USA, Lecture Notes EE392o, Autumn Quarter, 2003, vol. 2004, pp. 2004–2005.

[41] C. Kelley
Iterative Methods for Linear and Nonlinear Equations. Philadelphia, PA, USA: Soc. Ind. Appl. Math., 1995.

[42] T. Yoo and A. Goldsmith
On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming
IEEE J. Sel. Areas Commun., vol. 24, no. 3, pp. 528–541, Mar. 2006.

[43] R. Negi and S. Goel
Secret communication using artificial noise
In *Proc. IEEE 1999 Veh. Technol. Conf.*, 2005, vol. 62, no. 3, Paper no. 1906.

[44] N. Jindal
MIMO broadcast channels with finite-rate feedback

IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 5045–5060, Nov. 2006.

[45] T.-C. Hu, F. Moricz, and R. Taylor
Strong laws of large numbers for arrays of rowwise independent random variables
Acta Mathematica Hungarica, vol. 54, no. 1, pp. 153–162, 1989.

[46] A. Jeffrey and D. Zwillinger
Table of Integrals, Series, and Products.Amsterdam, The Netherlands: Elsevier, 2007.

[47] A. Leong and S. Dey
On scaling laws of diversity schemes in decentralized estimation
IEEE Trans. Inf. Theory, vol. 57, no. 7, pp. 4740–4759, Jul. 2011.

[48] A. Goldsmith
Wireless Communications. Cambridge, U.K.: Cambridge Univ. Press, 2005.

Xiaoxi Guo (S’15) was born in Zhumadian, China, in 1988. He received the B.E. degree (first class Hons.) in telecommunications engineering from the University of Wollongong, Wollongong, NSW, Australia, in 2010, and the M.E. degree in telecommunications engineering and the Ph.D. degree in electrical engineering both from the University of Melbourne, Parkville, VIC, Australia, in 2012 and 2016, respectively. His doctoral research focused on energy efficiency and security of the wireless sensor network.

His research interests include statistical signal processing, wireless communications, and physical layer security.

Alex S. Leong (S’03–M’08) was born in Macau in 1980. He received the B.S. degree in mathematics and B.E. degree in electrical engineering in 2003, and the Ph.D. degree in electrical engineering in 2008, all from the University of Melbourne, Parkville, VIC, Australia.

He is currently working as a Research Associate at Paderborn University, Paderborn, Germany. From 2008 to 2015, he was in the Department of Electrical and Electronic Engineering, University of Melbourne. His research interests include networked control systems, signal processing for sensor networks, and statistical signal processing.

Dr. Leong received the L. R. East Medal from Engineers Australia in 2003, an Australian Postdoctoral Fellowship from the Australian Research Council in 2009, and a Discovery Early Career Researcher Award from the Australian Research Council in 2012.

Subhrakanti Dey (M’96–SM’06) was born in India in 1968. He received the B.Tech. and M.Tech. degrees from the Indian Institute of Technology, Kharagpur, India, in 1991 and 1993, respectively, and the Ph.D. degree from the Research School of Information Sciences and Engineering, Australian National University, Canberra, ACT, Australia, in 1996.

He is currently a Professor in the Department of Engineering Sciences, Uppsala University, Uppsala, Sweden. Prior to this, he was a Professor in the Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, VIC, Australia, from 2000 until early 2013. From September 1995 to September 1997, and September 1998 to February 2000, he was a Postdoctoral Research Fellow in the Department of Systems Engineering, Australian National University. From September 1997 to September 1998, he was a Postdoctoral Research Associate in the Institute for Systems Research, University of Maryland, College Park, MD, USA. His current research interests include networked control systems, wireless communications and networks, signal processing for sensor networks, and stochastic and adaptive signal processing and control.

Prof. Dey currently serves on the editorial board of the IEEE TRANSACTIONS ON SIGNAL PROCESSING and IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He was also an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 2007–2010 and the IEEE TRANSACTIONS ON AUTOMATIC CONTROL during 2004–2007, and an Associate Editor for Elsevier *Systems and Control Letters* during 2003–2013.