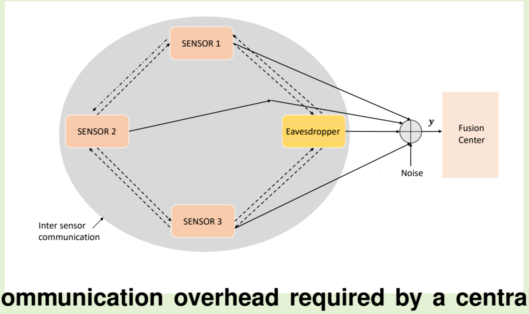
Privacy-Preserving Distributed Beamformer Design Techniques for Correlated Parameter Estimation

Mohammad Faisal Ahmed, *Graduate Student Member, IEEE,* Kunwar Pritiraj Rajput, *Member, IEEE,*
Naveen K. D. Venkategowda, *Senior Member, IEEE,* Aditya K. Jagannatham, *Senior Member, IEEE,* and
Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—Privacy-preserving distributed beamforming designs are conceived for temporally correlated vector parameter estimation in an orthogonal frequency division multiplexing (OFDM)-based wireless sensor network (WSN). The temporal correlation inherent in the parameter vector is exploited by the rate distortion theory-based bit allocation framework used for the optimal quantization of the sensor measurements. The proposed distributed beamforming designs are derived via fusion of the dual consensus alternating direction method of multipliers (DC-ADMM) technique with a pertinent privacy-preserving framework. This makes it possible for each SN to design its transmit precoders in a distributed fashion, which minimizes the susceptibility of vital information to malicious eavesdropper (Ev) nodes, while simultaneously avoiding the significant communication overhead required by a centralized approach for the transmission of the state information to the fusion center (FC). The Bayesian Cramer Rao Bound (BCRB) is derived for benchmarking the estimation performance of the proposed transmit beamformer and receiver combiner designs, while our simulation results illustrate the performance and explicitly demonstrate the trade-off between the privacy and estimation performance.**



***Index Terms*—Alternating direction method of multipliers (ADMM), coherent MAC, distributed beamforming, decentralized parameter estimation, privacy-preserving, wireless sensor networks.**

I. Introduction

Wireless sensor networks (WSNs) are expected to play a key role in the Internet of Things (IoT) supporting cutting-edge applications in several areas such as remote surveillance [1], [2], industrial automation [3], smart agriculture [4], and health care [5] etc. A typical WSN is comprised of several miniature sensor nodes (SNs) that continuously sense a single phenomena or multiple phenomena of interest, followed by transmission of the measurements to a central node, termed as the fusion center (FC), since it combines multiple observations for final estimation of the pertinent parameter(s). In such systems, optimal transmit and receive processing, achieved via transmit precoding (TPC) at the SNs and receiver combining (RC) at the FC, respectively, is critically important both for overcoming the hostile wireless channel effects, and for efficiently using the limited power/ bandwidth at the SNs [6]. Additionally, the correlation inherent in the parameter of interest can also be exploited for enhancing the estimation accuracy [7].

In a centralized WSN, the TPCs and RCs are traditionally designed as follows. To begin with, the SNs share their relevant individual system information, pertaining to the sensing/ channel matrices, and the observation noise statistics, among others, with the FC. Subsequently, the central node, i.e., the FC, designs the TPCs and RCs followed by the feedback of the former to the individual SNs [6], [8]–[10]. However, this process suffers from two drawbacks. Firstly, the transmission of such a large amount of information to the FC leads to a significant communication overhead. Furthermore, there is a high likelihood of the security of the system being

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1, EP/X01228X/1 and EP/Y026721/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028). The work of Aditya K. Jagannatham was supported in part by the Qualcomm Innovation Fellowship, and in part by the Arun Kumar Chair Professorship.

M. F. Ahmed is with Cisco Systems India Pvt. Ltd., Bengaluru, India (e-mail: mdfaisal165@gmail.com)

K. P. Rajput was with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, Kanpur, 208016, India. He is now with the interdisciplinary center of security reliability and trust (SnT), University of Luxembourg, 1855, Luxembourg (e-mail: kunwar.rajput@uni.lu)

A. K. Jagannatham is with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, Kanpur, 208016, India (e-mail:adityaj@iitk.ac.in)

N. K. D. Venkategowda is with the Department of Science and Technology, Linköping University, 60174 Norrköping, Sweden (e-mail: naveen.venkategowda@liu.se.)

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk)

compromised in this process, since the transmission of vital information by each SN to the FC can be intercepted by an eavesdropper (Ev). It is imperative to address the above drawbacks to ease implementation and alleviate the security concerns experienced in WSNs. An attractive option to overcome the communication overhead, is to design a distributed approach wherein the SNs design their TPCs in a distributed fashion via only local exchange of information, thus avoiding the transmission of sensitive information to the FC. The dual consensus-based alternating direction method of multipliers (DC-ADMM) approach [11] is eminently suited for achieving this goal, since it requires the SNs to only share their dual variables with their respective immediate neighbours. Furthermore, the above second drawback can be readily overcome by using a suitably designed privacy-preserving algorithm [12] that prevents interception of the local messages by an Ev. Thus, this paper focuses on the design of efficient privacy-preserving techniques for distributed TPC design in a multiple-input multiple-output (MIMO) orthogonal frequency division multiplexing (OFDM)-based WSN. A comprehensive survey of the related works in the existing literature is presented next.

A. State-of-the-art

The authors of [9], [10] developed iterative linear transceiver designs for vector parameter estimation in a MIMO WSN. While both the designs offer similar MSE performance, the algorithm developed by Liu *et al.* [10] offers faster convergence. Majorization theory based non-iterative closed-form transceiver designs were developed in [8] and [13] for the scenarios relying on both perfect and imperfect channel state information (CSI) availability, respectively. A novel scheme was developed for joint channel estimation and robust linear transceiver design to achieve sparse parameter estimation in [14]. Since all of the above-mentioned contributions are based on a centralized WSN implementation, they suffer from a high communication overhead and are also susceptible to security breaches. This can be avoided via distributed implementations, as reviewed next.

Khobahi *et al.* [15] developed an ADMM-based distributed estimation scheme wherein the SNs themselves estimate the underlying parameter of interest without requiring an FC. A linear minimum MSE (LMMSE) constrained distributed estimation framework is developed by Akhtar and Rajawat [16] for time varying parameter estimation. A novel sensor collaboration strategy was proposed by Liu *et al.* [17] for exploiting the temporal correlation present in the unknown parameter. In their scheme, instead of directly transmitting observations to the FC, the SNs collaborate and share their measurements and only a subset of SNs transmit their observations to the FC for final estimation. Both centralized and ADMM-based distributed robust transceiver designs were developed for a MIMO WSN by Liu *et al.* [18] either for minimizing the worst-case MSE subject to per-sensor power constraints, or alternatively, for minimizing the total power subject to a worst-case MSE constraint. Shirazinia [19] have proposed an interesting framework for the estimation of a correlated parameter in a coherent MAC-based massive MIMO WSN, assuming both perfect and imperfect channel state information (CSI) between each SN and the FC. Upon employing MMSE receive combining at the FC, two different precoder designs have been proposed. One focuses on minimizing the MSE subject to the total transmit power budget of the WSN, while the other focuses on minimizing the total transit power for a desired level of MSE performance. Moreover, the analysis therein has also been extended to scenarios associated with correlated noise and correlated channels between each SN and the FC. However, the authors did not consider distributed precoder design and quantized measurement transmission in their analysis. Another major limitation of WSNs is the limited bandwidth available for measurement transmission. Therefore, it is critical to use low-rate quantization for sensor measurements prior to their transmission. A brief review of research papers that address this problem is presented next.

Sun and Goyal [20] developed a distributed functional scalar quantization scheme, where the SNs initally collaborate among themselves followed by the transmission of their quantized observations to the FC. A novel sensor data reduction and quantization technique is developed by Msechu and Giannakis [21] which requires only a subset of the SNs to transmit their observations to the FC. Interestingly, the algorithm therein considers the estimation of both deterministic as well as random parameters. A block coordinate descent (BCD)-based iterative scheme is developed in [22] for joint quantization and power allocation that minimizes the MSE at the FC. Sani and Vosoughi [23], presented novel coupled and decoupled techniques for minimum MSE estimation subject to both power and bandwidth constraints. However, an orthogonal MAC is used in [22], [23], which leads to bandwidth inefficiency [6], since it requires a dedicated channel between each SN and the FC. Moreover, it also enhances the effect of observation noise. A novel sensor observation and quantization framework is developed in [24] for minimizing the energy consumption, using a convex approximation-based iterative scheme that results in near-optimal performance. Several researchers have also been intrigued by the problem of secure estimation in a WSN. The salient endeavours in this field are reviewed next.

The authors of [25], [26] developed novel distributed schemes for secure detection by considering a scenario, where an unauthorized agent attempts to eavesdrop on the communication between authorized nodes of the WSN. He *et al.* [27] derived an interesting linear TPC for ensuring that the FC can only interpret a public hypothesis but not the private hypothesis of each sensor. The TPCs are designed to guarantee that the probability of detecting the private hypotheses by the FC is always lower than the maximum tolerable threshold. Guo *et al.* [28] determined the optimal transmit power allocation strategies under a total network power constraint for MSE minimization at the FC together with a secrecy constraint at the Ev. A unique aspect of their work is that it considers various scenarios, such as multiple SNs having a single antenna each and a single SN with multiple antennas, for comprehensively analyzing the system performance. Guo *et al.* [29] also develop novel TPC schemes for outage minimization in presence of an Ev node in the network. An optimal parameter encoding technique is developed by Goken and Gezici [30] that uses a novel approach based on minimizing the conditional Cramer-Rao lower bound (CRLB) at the receiver, while ensuring that the MSE at the Ev is always higher than a minimum tolerable value. In several WSN applications, it is extremely important that the SNs do not openly transmit secure information such as their respective observation matrices etc. since these messages may potentially contain sensitive details pertaining to the code, location and timing, for example in radar sensor networks [31]–[33] and in smart agriculture [34]. Therefore, in these systems, it is crucial to design the sensor TPCs in a distributed style, thus avoiding the need for the SNs to communicate their individual channel state information (CSI), sensing model and noise statistics etc. In this regard, the scheme developed by Venkategowda and Werner [35] achieves precisely this objective via the development of an efficient procedure for distributed maximum consensus in the network while guaranteeing privacy. This protects sensitive information from being accessed by the adversarial nodes in the network. However, to the best of our knowledge, none of the contributions in the open literature develop a privacy-preserving framework for the estimation of a correlated vector parameter relying either on analog or on quantized measurement transmission. Hence this treatise develops distributed transmit beamforming schemes to fill this knowledge gap. Table-I boldly and explicitly contrasts our unique contributions to the literature and one should note that the aspects mentioned in rows 1, 4, 5 and 10 are exclusive to our work. The next subsection details the contributions of this work in a point-wise fashion.

B. Contributions

- The system model is initially developed for the estimation of a temporally correlated vector parameter relying on analog sensor measurement transmission. Subsequently, the pertinent transceiver design problem is formulated as a sum-MSE (SMSE) minimization, subject to individual sensor power constraints.
- An efficient closed-form solution is developed for the design of the individual sensor TPCs as well as for conceiving a low-complexity fusion rule at the FC. A dual consensus ADMM-based privacy-preserving framework is developed, wherein the sensors design their TPCs in a distributed fashion.
- Subsequently, a rate-distortion theory (RDT)-based optimal bit allocation scheme is developed for the optimal quantization of each sensor's measurement for exploiting the temporal correlation present in the parameter. This is followed by the development of closed-form expressions for the individual sensor TPCs that minimize the SMSE at the FC subject to individual sensor power constraints. Distributed privacy-preserving designs are also derived for this scenario.
- The Bayesian Cramer-Rao bound (BCRB) is developed for bounding the SMSE performance of the proposed distributed TPC designs. Finally, exhaustive simulation results are presented for characterizing the performance of the proposed designs for the various scenarios considered.

The rest of the paper is organized as follows. Section-II presents the system model and formulates the SMSE minimization problem for vector parameter estimation considering analog transmission. This is followed by the development of a privacy-preserving distributed framework for TPC design in Subsection-II-B. Furthermore, Subsection-II-C systematically develops our approach for the optimal bit allocation and quantization of the sensor measurements followed by the development of a privacy-preserving distributed TPC design. The BCRB is derived in Section-III followed by the simulation results in Section-IV, with Section-V summarizing our conclusions.

Notation: $\mathbf{x} \sim \mathcal{CN}[\mathbf{0}, \mathbf{\Sigma}]$ denotes a circularly symmetric complex Gaussian vector $\mathbf{x}$ in nature with mean zero and covariance matrix $\mathbf{\Sigma}$. The trace and statistical expectation operations are denoted by $\mathrm{Tr}[.]$ and $\mathbb{E}[.]$, respectively, while $(.)^*$, $(.)^T$, and $(.)^H$ denotes the conjugation, transpose and Hermitian operations. The symbol $\otimes$ represents the Kronecker product. The matrix $\mathbf{I}_N$ represents an identity matrix of size $N \times N$. The matrix $\mathbf{X} = \mathrm{diag}\left[\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N\right]$ denotes a block-diagonal matrix with the matrices $\mathbf{X}_n$, $1 \leq n \leq N$ on its principal diagonal. The (i, j)th element of any matrix $\mathbf{X}$ is denoted by $[\mathbf{X}]_{ij}$. The operation $\mathbf{x} = \mathrm{vec}(\mathbf{X})$ stacks the columns of the matrix $\mathbf{X} \in \mathbb{C}^{N \times N}$ to obtain the vector $\mathbf{x} \in \mathbb{C}^{N^2 \times 1}$. The operation $\mathbf{X} = \mathrm{vec}_t^{-1}(\mathbf{x})$ yields a matrix $\mathbf{X}$ with t rows and appropriate number of columns. $||\mathbf{X}||_F$ denotes the Frobenius norm of the matrix $\mathbf{X}$.

II. Privacy-Preserving Temporally Correlated Parameter Estimation

This section begins by describing our vector parameter sensing and estimation model in a MIMO-OFDM-based WSN, followed by the design of our DC-ADMM-based privacy-preserving TPC. The system transmitting analog measurements is considered next.

A. Analog measurement transmission

Consider a MIMO-OFDM-based WSN comprised of K SNs, each equipped with N_s transmit antennas (TAs) and an FC equipped with N_{fc} received antennas (RAs). Each SN observes/ senses the unknown P dimensional complex-valued temporally correlated source vector $\tilde{\mathrm{s}}$ of interest. The pth element of $\tilde{\mathrm{s}}(n)$ at the nth time instant, denoted by $\tilde{s}_p(n)$, $1 \leq p \leq P$, is a sample of a zero-mean temporally correlated wide sense stationary Gaussian random process with its power spectral density (PSD) denoted by $\Phi_p(f)$. Practical applications based on WSN require sensing of the physical quantities such as temperature, pressure, location etc., which naturally exhibit temporal correlation. Furthermore, it is common to model the measurements as random variables with a suitable distribution in order to incorporate the statistical characteristics of the parameter of interest. Our work models the measurements as a zero-mean temporally correlated wide sense stationary Gaussian random processes, which is one of the widely used models of a random process, in order to exploit the correlation for enhanced parameter estimation [15,16]. For example, in target tracking applications, while

TABLE I
BOLDLY AND EXPLICITLY CONTRASTING OUR CONTRIBUTIONS TO THE LITERATURE.

Feature	[15]	[21]	[23]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[35]	**Proposed**
OFDM-WSN												✓
Scalar parameter estimation	✓			✓			✓	✓	✓			✓
Vector parameter estimation		✓	✓		✓	✓						✓
Coherent MAC												✓
Frequency selective channel												✓
Analog Measurement transmission	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓
Quantized measurement transmission		✓	✓									✓
Distributed estimation	✓										✓	✓
Privacy-preserving				✓							✓	✓
Temporal correlation												✓
Individual power constraints			✓									✓

the position of a target changes over time, the current position has a bearing on the subsequent positions. Therefore, the time dependence between measurements, as well as the uncertainty and measurement errors can be incorporated via the correlated wide sense stationary Gaussian random process model. This paves the way for developing various interesting frameworks that enhance the estimation performance and result in efficient resource utilization in WSN. The time domain observation vector $\widetilde{\mathbf{z}}_k(n) \in \mathbb{C}^{N_s \times 1}$ of the kth SN at the nth time instant can be modeled as

$$\widetilde{\mathbf{z}}_k(n) = \mathbf{C}_k \tilde{\mathbf{s}}(n) + \widetilde{\mathbf{w}}_k(n), \tag{1}$$

where $\mathbf{C}_k \in \mathbb{C}^{N_s \times P}$ denotes the measurement matrix of the kth SN and $\widetilde{\mathbf{w}}_k(n) \sim \mathcal{CN}(\mathbf{0}, \widetilde{\mathbf{\Sigma}}_k) \in \mathbb{C}^{N_s \times 1}$ represents the measurement noise. At the kth SN, upon concatenating the measurements $\widetilde{\mathbf{z}}_k(n)$ over N time instants, one obtains

$$\widetilde{\mathbf{Z}}_k = \mathbf{C}_k \widetilde{\mathbf{S}} + \widetilde{\mathbf{W}}_k, \tag{2}$$

where the different matrices $\widetilde{\mathbf{Z}}_k \in \mathbb{C}^{N_s \times N}$, $\widetilde{\mathbf{S}} \in \mathbb{C}^{P \times N}$ and $\widetilde{\mathbf{W}}_k \in \mathbb{C}^{N_s \times N}$ are defined as

$$\widetilde{\mathbf{Z}}_k = [\widetilde{\mathbf{z}}_k(0), \widetilde{\mathbf{z}}_k(1) \ldots, \widetilde{\mathbf{z}}_k(N-1)] \tag{3}$$

$$\widetilde{\mathbf{S}} = [\tilde{\mathbf{s}}(0), \tilde{\mathbf{s}}(1), \ldots, \tilde{\mathbf{s}}(N-1)] \tag{4}$$

$$\widetilde{\mathbf{W}}_k = [\widetilde{\mathbf{w}}_k(0), \widetilde{\mathbf{w}}_k(1), \ldots, \widetilde{\mathbf{w}}_k(N-1)]. \tag{5}$$

Subsequently, taking the N-point row-wise normalized fast Fourier transform (FFT) of the measurement matrix $\widetilde{\mathbf{Z}}_k$ yields its frequency domain (FD) counterpart as

$$\mathbf{Z}_k = \widetilde{\mathbf{Z}}_k \mathbf{\Upsilon} = \mathbf{C}_k \widetilde{\mathbf{S}} \mathbf{\Upsilon} + \widetilde{\mathbf{W}}_k \mathbf{\Upsilon} = \mathbf{C}_k \mathbf{S} + \mathbf{W}_k, \tag{6}$$

where $\mathbf{\Upsilon} \in \mathbb{C}^{N \times N}$ represents the normalized FFT matrix with its (i,j)th entry defined as $\frac{1}{\sqrt{N}} e^{\frac{-2\pi i j}{N}}$. Using (6), the FD observation vector corresponding to the kth SN on the mth subcarrier can be written as

$$\mathbf{z}_k(m) = \mathbf{C}_k \mathbf{s}(m) + \mathbf{w}_k(m), \tag{7}$$

where the vectors $\mathbf{s}(m) \sim \mathcal{CN}[\mathbf{0}, \mathbf{\Sigma}_s(m)] \in \mathbb{C}^{P \times 1}$ and $\mathbf{w}_k(m) \sim \mathcal{CN}[\mathbf{0}, \mathbf{\Sigma}_k(m)] \in \mathbb{C}^{N_s \times 1}$ represent the frequency domain source vector and the kth SN's measurement noise vector, respectively. Furthermore, the frequency domain parameter and observation noise covariance matrices denoted by $\mathbf{\Sigma}_s(m)$ and $\mathbf{\Sigma}_k(m)$, respectively, are given as

$$\mathbf{\Sigma}_s(m) = \text{diag}\left[\Phi_1(f_m), \Phi_2(f_m), \ldots, \Phi_P(f_m)\right] \tag{8}$$

$$\mathbf{\Sigma}_k(m) = \sigma_k^2 \mathbf{I}_{N_s}, \tag{9}$$

where $f_m = \frac{m}{N}$, $0 \leq m \leq N-1$ and σ_k^2 denotes the variance of the kth observation noise vector. Next, one can employ the matrix $\mathbf{F}_k(m) \in \mathbb{C}^{N_s \times N_s}$ to precode the observation vector $\mathbf{z}_k(m)$, which can be represented as

$$\check{\mathbf{z}}_k(m) = \mathbf{F}_k(m)\mathbf{z}_k(m) = \mathbf{F}_k(m)\mathbf{C}_k\mathbf{s}(m) + \mathbf{F}_k(m)\mathbf{w}_k(m).$$

The above step is performed at each SN k in the WSN for each subcarrier m. Next, these precoded measurements are transmitted to the FC over a coherent MAC in the MIMO-OFDM based WSN. At the FC, the FFT-based demodulation is applied to the received vector to obtain the FD vector $\mathbf{y}(m) \in \mathbb{C}^{N_{fc} \times 1}$ corresponding to subcarrier m, as

$$\begin{aligned}\mathbf{y}(m) = &\sum_{k=1}^{K} \mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k\mathbf{s}(m) + \sum_{k=1}^{K} \mathbf{G}_k(m)\mathbf{F}_k(m) \\ &\mathbf{w}_k(m) + \mathbf{v}_{fc}(m),\end{aligned} \tag{10}$$

where the matrix $\mathbf{G}_k(m) \in \mathbb{C}^{N_{fc} \times N_s}$ represents the FD MIMO channel between the kth SN and the FC for the mth subcarrier, while $\mathbf{v}_{fc}(m) \sim \mathcal{CN}[\mathbf{0}, \mathbf{\Sigma}_v] \in \mathbb{C}^{N_{fc} \times 1}$ denotes the FC noise. Let the RC matrix $\mathbf{A}(m) \in \mathbb{C}^{P \times N_{fc}}$ be used for generating the estimate $\widehat{\mathbf{s}}(m) = \mathbf{A}^H(m)\mathbf{y}(m)$ on the mth subcarrier and SMSE can be formulated as shown in (11). The SMSE objective function of (11) is non-convex in nature, in addition to being non-separable in terms of the optimization variables $\{\mathbf{F}_k(m)\}_{k=1}^K$ and $\mathbf{A}(m)$ for each subcarrier m. Hence, the following estimation constraint can be employed to simplify the transceiver design problem at the FC

$$\sum_{k=1}^{K} \mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k = \gamma_m \mathbf{D}(m), 0 \leq m \leq N-1, \tag{12}$$

where the matrix $\mathbf{D}(m) \in \mathbb{C}^{N_{fc} \times P}$ denotes a known matrix, while the quantity γ_m represents the TPC gain to be optimized for each subcarrier m. This also results in a simple fusion rule at the FC, i.e., $\mathbf{A}^H(m) = \frac{1}{\gamma_m}\mathbf{D}^\dagger(m)$ for each subcarrier m. Upon exploiting the property $\text{vec}(\mathbf{XYZ}) = \left(\mathbf{Z}^T \otimes \mathbf{X}\right)\text{vec}(\mathbf{Y})$, for any suitable matrices $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$, one can rewrite the estimation constraint in (12) as

$$\sum_{k=1}^{K} \mathbf{E}_k(m)\mathbf{f}_k(m) = \mathbf{E}(m)\mathbf{f}(m) = \gamma_m \text{vec}\left[\mathbf{D}(m)\right] = \mathbf{h}(m), \tag{13}$$

$$\mathrm{SMSE} = \sum_{m=0}^{N-1} \mathbb{E}\left[\mathrm{Tr}\left[\left[\mathbf{A}^H(m)\mathbf{y}(m) - \mathbf{s}(m)\right]\left[\mathbf{A}^H(m)\mathbf{y}(m) - \mathbf{s}(m)\right]^H\right]\right] = \sum_{m=0}^{N-1} \mathrm{Tr}\Bigg[\mathbf{A}^H(m)\boldsymbol{\Sigma}_v(m)\mathbf{A}(m) + \boldsymbol{\Sigma}_s(m) - \mathbf{A}^H(m) \left(\sum_{k=1}^{K}\mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k\right)\boldsymbol{\Sigma}_s(m) - \boldsymbol{\Sigma}_s(m)\left(\sum_{k=1}^{K}\mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k\right)^H \mathbf{A}(m) + \mathbf{A}^H(m)\sum_{k=1}^{K}\mathbf{G}_k(m)\mathbf{F}_k(m)\boldsymbol{\Sigma}_k(m)\mathbf{F}_k^H(m)\mathbf{G}_k^H(m) \mathbf{A}(m) + \mathbf{A}^H(m)\left(\sum_{k=1}^{K}\mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k\right)\boldsymbol{\Sigma}_s(m)\left(\sum_{k=1}^{K}\mathbf{G}_k(m)\mathbf{F}_k(m)\mathbf{C}_k\right)^H \mathbf{A}(m)\Bigg]. \tag{11}$$

for each subcarrier m. The different matrices $\mathbf{E}_k(m) \in \mathbb{C}^{N_{fc}P\times N_{fc}N_s}$, $\mathbf{E}(m) \in \mathbb{C}^{KN_{fc}P\times N_{fc}N_s}$, $\mathbf{f}(m) \in \mathbb{C}^{KN_s^2\times 1}$ are defined as

$$\begin{aligned}\mathbf{E}_k(m) &= \left[\mathbf{C}_k^T \otimes \mathbf{G}_k(m)\right]\\ \mathbf{E}(m) &= \left[\mathbf{E}_1(m), \mathbf{E}_2(m), \ldots, \mathbf{E}_K(m)\right]\\ \mathbf{f}(m) &= [\mathbf{f}_1^T(m), \mathbf{f}_2^T(m), \ldots, \mathbf{f}_K^T(m)]^T,\end{aligned}$$

and the vector $\mathbf{h}(m) = \gamma_m \mathrm{vec}\left[\mathbf{D}(m)\right] \in \mathbb{C}^{N_{fc}P\times 1}$. One can also write the cumulative estimation constraint for all the subcarriers as

$$\mathbf{E}\mathbf{f} = \mathbf{h}, \tag{14}$$

where the matrices $\mathbf{E} \in \mathbb{C}^{NN_{fc}P\times NN_{fc}N_s}$, $\mathbf{f}_k \in \mathbb{C}^{NN_s^2\times 1}$, $\mathbf{f} \in \mathbb{C}^{KNN_s^2\times 1}$ and $\mathbf{h} \in \mathbb{C}^{NN_{fc}P\times 1}$ are defined as

$$\begin{aligned}\mathbf{E} &= \mathrm{diag}[\mathbf{E}(0), \mathbf{E}(1), \ldots, \mathbf{E}(N-1)] = [\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_K]\\ \mathbf{f}_k &= [\mathbf{f}_k^T(0), \mathbf{f}_k^T(1), \ldots, \mathbf{f}_k^T(N-1)]^T\\ \mathbf{f} &= [\mathbf{f}_1^T, \mathbf{f}_2^T, \ldots, \mathbf{f}_K^T]^T\\ \mathbf{h} &= [\mathbf{h}^T(0), \mathbf{h}^T(1), \ldots, \mathbf{h}^T(N-1)]^T.\end{aligned}$$

Finally, through a simple rearrangement of terms, the cumulative constraint in (14) can be recast as

$$\sum_{k=1}^{K}\mathbf{E}_k\mathbf{f}_k = \mathbf{h}. \tag{15}$$

It is now possible to decouple the resultant SMSE expression corresponding to each sensor, which can eventually be used for developing a distributed implementation using the DC-ADMM algorithm, as discussed next in detail. Substituting the estimation constraint of (12) into (11), and exploiting the property $\mathrm{Tr}\left(\mathbf{X}^H\mathbf{Y}\mathbf{Z}\mathbf{W}\right) = \mathrm{vec}(\mathbf{X})^H\left(\mathbf{W}^T \otimes \mathbf{Y}\right)\mathrm{vec}(\mathbf{Z})$ along with the result $\mathrm{Tr}(\mathbf{X}\mathbf{Y}) = \mathrm{Tr}(\mathbf{Y}\mathbf{X})$, the expression for the SMSE therein reduces to

$$\begin{aligned}\mathrm{SMSE} &= \sum_{m=0}^{N-1}\sum_{k=1}^{K}\mathrm{Tr}\Big[\mathbf{G}_k(m)\mathbf{F}_k(m)\boldsymbol{\Sigma}_k(m)\mathbf{F}_k^H(m)\mathbf{G}_k^H(m)\Big]\\ &+ \sum_{m=0}^{N-1}\frac{\sigma_m^2}{\gamma_m^2}\\ &= \sum_{k=1}^{K}\sum_{m=0}^{N-1}\mathbf{f}_k^H(m)\boldsymbol{\Psi}_k(m)\mathbf{f}_k(m) + \sum_{m=0}^{N-1}\frac{\sigma_m^2}{\gamma_m^2}\\ &= \sum_{k=1}^{K}\mathbf{f}_k^H\boldsymbol{\Psi}_k\mathbf{f}_k + \sum_{m=0}^{N-1}\frac{\sigma_m^2}{\gamma_m^2},\end{aligned} \tag{16}$$

where we have $\sigma_m^2 = \mathrm{Tr}\left[\mathbf{A}^H(m)\boldsymbol{\Sigma}_v(m)\mathbf{A}(m)\right]$ for each subcarrier m. Furthermore, the matrices $\boldsymbol{\Psi}_k(m) \in \mathbb{C}^{N_s^2\times N_s^2}$ and $\boldsymbol{\Psi}_k \in \mathbb{C}^{NN_s^2\times NN_s^2}$ are defined as

$$\begin{aligned}\boldsymbol{\Psi}_k(m) &= \left[\boldsymbol{\Sigma}_k(m) \otimes \mathbf{G}_k^H(m)\mathbf{G}_k(m)\right]\\ \boldsymbol{\Psi}_k &= \mathrm{diag}\left[\boldsymbol{\Psi}_k(0), \boldsymbol{\Psi}_k(1), \ldots, \boldsymbol{\Psi}_k(N-1)\right].\end{aligned}$$

The average transmit power of the kth SN corresponding to all the subcarriers is defined as $\sum_{m=0}^{N-1}\mathbb{E}\left[||\mathbf{F}_k(m)\mathbf{z}_k(m)||^2\right]$, which can further be simplified as

$$\begin{aligned}&\sum_{m=0}^{N-1}\mathrm{Tr}\Big[\mathbf{F}_k(m)\mathbb{E}\left[\mathbf{z}_k(m)\mathbf{z}_k^H(m)\right]\mathbf{F}_k^H(m)\Big]\\ &= \sum_{m=0}^{N-1}\mathrm{Tr}\Big[\mathbf{F}_k^H(m)\mathbf{R}_k(m)\mathbf{F}_k(m)\Big]\\ &= \sum_{m=0}^{N-1}\mathbf{f}_k^H(m)\boldsymbol{\Pi}_k(m)\mathbf{f}_k(m) = \mathbf{f}_k^H\boldsymbol{\Pi}_k\mathbf{f}_k,\end{aligned} \tag{17}$$

where we have $\mathbf{R}_k(m) = \left[\mathbf{C}_k\boldsymbol{\Sigma}_s(m)\mathbf{C}_k^H + \boldsymbol{\Sigma}_k(m)\right] \in \mathbb{C}^{N_s\times N_s}$, $\boldsymbol{\Pi}_k(m) = \left[\mathbf{R}_k(m) \otimes \mathbf{I}_P\right] \in \mathbb{C}^{N_sP\times N_sP}$, and $\boldsymbol{\Pi}_k = \mathrm{diag}\left[\boldsymbol{\Pi}_k(0), \boldsymbol{\Pi}_k(1), \ldots, \boldsymbol{\Pi}_k(N-1)\right] \in \mathbb{C}^{NN_sP\times NN_sP}$. Hence, the optimization problem for designing the optimal SMSE TPCs subject to individual SN power constraints is formulated as

$$\begin{aligned}&\underset{\{\mathbf{f}_k\}_{k=1}^{K},\gamma}{\text{minimize}} \quad \sum_{k=1}^{K}\mathbf{f}_k^H\boldsymbol{\Psi}_k\mathbf{f}_k + \sum_{m=0}^{N-1}\frac{\sigma_m^2}{\gamma_m^2}\\ &\text{subject to} \quad \mathbf{f}_k^H\boldsymbol{\Pi}_k\mathbf{f}_k \le \mathcal{P}_k,\ 1 \le k \le K, \text{ and (15).}\end{aligned} \tag{18}$$

The above optimization problem can be solved using the Karush-Kuhn-Tucker (KKT) framework [36], and the Lagrangian function is given by

$$\begin{aligned}\mathcal{L}(\mathbf{f}_k, \gamma_m, \boldsymbol{\beta}_k, \varepsilon_k) &= \sum_{k=1}^{K}\mathbf{f}_k^H\boldsymbol{\Psi}_k\mathbf{f}_k + \sum_{m=0}^{N-1}\frac{\sigma_m^2}{\gamma_m^2}\\ &+ \boldsymbol{\beta}_k^H\left(\sum_{k=1}^{K}\mathbf{E}_k\mathbf{f}_k - \mathbf{h}\right) + \varepsilon_k\left(\mathbf{f}_k^H\boldsymbol{\Pi}_k\mathbf{f}_k - \mathcal{P}_k\right),\end{aligned} \tag{19}$$

where $\boldsymbol{\beta}_k \in \mathbb{C}^{NN_{fc}P\times 1}$ and $\varepsilon_k \in \mathbb{C}$ are the dual variables corresponding to the equality and inequality constraints, respectively, for each SN k. Upon exploiting the first-order optimality KKT condition, the optimal TPC vector $\mathbf{f}_k^{\mathrm{opt}}$ is formulated as

$$\mathbf{f}_k^{\mathrm{opt}} = -\frac{1}{2}\left[\boldsymbol{\Psi}_k + \varepsilon_k^{\mathrm{opt}}\boldsymbol{\Pi}_k\right]^{-1}\mathbf{E}_k^H\boldsymbol{\beta}^{\mathrm{opt}}. \tag{20}$$

For each SN k, the dual variable $\varepsilon_k^{\mathrm{opt}}$ can be obtained via solving the equation

$$\left|\left|\mathbf{\Pi}_k^{\frac{1}{2}}\left[\mathbf{\Psi}_k+\varepsilon_k^{\mathrm{opt}}\mathbf{\Pi}_k\right]^{-1}\mathbf{E}_k\boldsymbol{\beta}^{\mathrm{opt}}\right|\right|_2^2=4\mathcal{P}_k, \tag{21}$$

using the procedure mentioned in [37, App. A], while, the optimal TPC gain γ_m^{opt} for each subcarrier m can be derived as

$$\gamma_m^{\mathrm{opt}}=\left(\frac{2\sigma_m^2}{\Re\{\boldsymbol{\beta}_k^H\mathbf{h}\}}\right)^{1/3}. \tag{22}$$

The equivalent dual optimization problem for (18) can be formulated as

$$\begin{aligned}&\underset{\boldsymbol{\beta_k}}{\text{minimize}} && \sum_{k=1}^{K}\boldsymbol{\beta}_k^H\mathbf{E}_k\left[\mathbf{\Psi}_k+\varepsilon_k\mathbf{\Pi}_k\right]^{-1}\mathbf{E}_k^H\boldsymbol{\beta}_k+\frac{4}{K}\Re\left[\boldsymbol{\beta}_k^H\mathbf{h}\right]\\&\text{subject to} && \boldsymbol{\beta}_k=\boldsymbol{\beta}\ \forall\ k=1,2,\cdots,K.\end{aligned} \tag{23}$$

The DC-ADMM framework [38] is now invoked for solving the above optimization problem. Let $\boldsymbol{\psi}_k$ denote the dual variable corresponding to the kth consensus constraint. The closed-form solution of $\boldsymbol{\beta}_k^{(i+1)}\in\mathbb{C}^{NN_{fc}K\times 1}$, $\boldsymbol{\beta}^{(i+1)}\in\mathbb{C}^{NN_{fc}K\times 1}$, and $\boldsymbol{\psi}_k^{(i+1)}\in\mathbb{C}^{NN_{fc}K\times 1}$ in the ith iteration can be formulated as

$$\boldsymbol{\beta}_k^{(i+1)}=\mathbf{Q}_k^{-1}\left[\frac{\rho}{2}\boldsymbol{\beta}^i-\frac{\boldsymbol{\psi}_k^i}{2}-\frac{2\mathbf{h}}{K}\right], \tag{24}$$

$$\boldsymbol{\beta}^{(i+1)}=\frac{1}{K}\sum_{k=1}^{K}\boldsymbol{\beta}_k^{(i+1)}, \tag{25}$$

$$\boldsymbol{\psi}_k^{(i+1)}=\boldsymbol{\psi}_k^i+\rho\left[\boldsymbol{\beta}_k^{(i+1)}-\boldsymbol{\beta}^{(i+1)}\right], \tag{26}$$

where we have $\mathbf{Q}_k=\left[\mathbf{E}_k\left[\mathbf{\Psi}_k+\varepsilon_k\mathbf{\Pi}_k\right]^{-1}\mathbf{E}_k^H+\frac{\rho}{2}\mathbf{I}_{NN_{fc}K}\right]\in\mathbb{C}^{NN_{fc}K\times NN_{fc}K}$. In every ADMM iteration, the computational complexity of evaluating the precoder vector $\mathbf{f}_k^{\mathrm{opt}}$, individual dual variable $\boldsymbol{\beta}_k$ and global dual variable $\boldsymbol{\beta}$ using (20), (24) and (25) is of order $\mathcal{O}\left[(NN_s^2)^3+(NN_{fc}N_s)^3\right]$, for each SN k. Next, the privacy-preserving distributed framework is developed and described in detail.

B. Privacy-preserving algorithm

Considering the WSN as an undirected graph $\mathcal{G}=(\mathcal{V},\mathcal{C})$, where the SNs in the network form the set of vertices denoted by $\mathcal{V}=\{1,2,\ldots,K\}$, while the set of edges $\mathcal{C}$ provides information regarding the communication links between the different SNs in the network. The neighbourhood information of the kth SN is given by the set $\mathcal{N}_k$. The adjacency matrix $\mathcal{D}$ of the WSN is defined as $[\mathcal{D}]_{ij}=1$, if i and j belongs to the $\mathcal{C}$, and 0 otherwise.

Initially, the FC determines the neighbourhood information for each SN k in the network so that $\mathcal{N}_k\cup\{k\}\not\subseteq\mathcal{N}_l\cup\{l\}$, where $k\neq l$. The weight matrix $\mathbf{B}$ that provides the information about the weight to be assigned to the messages received from a specific SN is also provided by the FC to each individual SN in the WSN. This matrix is defined as $\mathbf{B}=\frac{1}{K-1}\left[\mathcal{D}+\mathrm{diag}\left[\{K-1-|\mathcal{N}_k|\}_{k=1}^{K}\right]\right]$. It is important to note that the weight matrix $\mathbf{B}$ is selected for ensuring that its eigenvalues are arranged as $\lambda_1>\lambda_2>\ldots>\lambda_K$, with $\lambda_1=1$ and $\lambda_k<1$ for $k=2,\ldots,K$, where $\mathbf{B1}=\mathbf{1}$.

We then employ the privacy-preserving algorithm of [12] in every iteration of the DC-ADMM, where the initial state of the kth SN is set as $\boldsymbol{\zeta}_k(0)=\boldsymbol{\beta}_k^{(i+1)}$. Next, the kth SN generates the noise vector $\boldsymbol{\upsilon}_k(j)$ according to the distribution $\mathcal{CN}\left[\mathbf{0},\xi\mathrm{diag}\left[\boldsymbol{\zeta}_k(j)\right]\right]$, where ξ denotes the privacy parameter. As seen, the privacy parameter ξ is a scalar value that directly affects the variance of the perturbation noise vector $\mathbf{v}$. Hence, the value of the privacy parameter ξ can be directly tuned to obtain the required privacy levels at different agents. Additionally, the noise $\boldsymbol{\upsilon}_k(j)$ also satisfies the property that $\mathbb{E}\left[\boldsymbol{\upsilon}_k(j)\boldsymbol{\upsilon}_l(\tilde{j})\right]=\mathbf{0}$ for all $k\neq l$ and $j\neq\tilde{j}$. Furthermore, the kth SN generates the noise $\boldsymbol{\pi}_k(j)$ as

$$\boldsymbol{\pi}_k(j)=\phi^j\boldsymbol{\upsilon}_k(j)-\phi^{(j-1)}\boldsymbol{\upsilon}_k(j-1), \tag{27}$$

where the quantity ϕ satisfies $0<\phi<1$. The noise $\boldsymbol{\pi}_k(j)$ is used for perturbing the kth SN's original message $\boldsymbol{\zeta}_k(j)$ to obtain $\boldsymbol{\zeta}_k^+(j)=\boldsymbol{\zeta}_k(j)+\boldsymbol{\pi}_k(j)$. Subsequently, it communicates the perturbed message $\boldsymbol{\zeta}_k^+(j)$ with the neighbouring SNs and updates its local state as

$$\boldsymbol{\zeta}_k(j+1)=b_{kk}\boldsymbol{\zeta}_k^+(j)+\sum_{l\in\mathcal{N}_k}b_{kl}\boldsymbol{\zeta}_l^+(j), \tag{28}$$

where $\mathbf{B}_{kl}=b_{kl}$ represents the weight applied to the message obtained from the lth sensor. For each SN k, it follows that

$$\lim_{j\to\infty}\boldsymbol{\zeta}_k(j)=\boldsymbol{\beta}^{(i+1)}=\frac{1}{K}\sum_{k=1}^{K}\boldsymbol{\beta}_k^{(i+1)}. \tag{29}$$

This proves that even when the SNs can only share perturbed messages with each other, consensus can still be achieved in the network. In the end, each SN determines its own TPC vector using (20) and the value of γ_m^{opt} can be obtained using (22). This further leads to the expression for the optimal RC matrix $\mathbf{A}(m)$ formulated as $\mathbf{A}(m)=\frac{1}{\gamma_m^{\mathrm{opt}}}\mathbf{D}^{\dagger}$ for each subcarrier m. A succinct summary of the privacy-preserving distributed system design procedure is given in Algorithm 1. Next, it is demonstrated that the proposed algorithm is indeed of privacy-preserving nature.

Without loss of generality, assume that the Kth SN in the WSN is a malicious node, which is trying to infer the initial states of the other SNs in the network. The malicious SN K can determine the maximum likelihood estimate of $\boldsymbol{\mu}_k^{(i+1)}$, where $k\neq K$, provided that it also possesses the information $\mathcal{I}(j)=\left\{\boldsymbol{\zeta}_K(0),\boldsymbol{\zeta}_{l_1}^+(j),\ldots,\boldsymbol{\zeta}_{l_{|\mathcal{N}_K|}}^+(j)\right\}$ from its neighbouring SNs. The neighbourhood of the Kth SN is represented by the set $\mathcal{N}_K=\left\{l_1,\ldots,l_{|\mathcal{N}_K|}\right\}$. Let the covariance matrix of the estimation error of the kth SN in the WSN be denoted by $\mathbf{M}_k$. The following theorem states the key result of the proposed work.

Theorem 1: The proposed distributed beamforming design is of privacy-preserving nature, i.e., $\mathrm{Tr}\left[\mathbf{M}_k\right]>0$, for $k=1,2,\ldots,K-1$, and asymptotically reaches the optimal solution in the mean square sense, yielding:

$$\lim_{j\to\infty}\mathbb{E}\left|\left|\boldsymbol{\zeta}_k(j)-\boldsymbol{\beta}^{(i+1)}\right|\right|=\mathbf{0},\ \forall\ k. \tag{30}$$

Algorithm 1 Privacy-preserving distributed beamforming for the estimation of a correlated vector parameter

```
**At the FC**:
For each SN$k$ in the WSN, find its neighbourhood using $\mathcal{N}_k \cup \{k\} \nsubseteq \mathcal{N}_l \cup \{l\}$, where $k \neq l$.
Determine the weight matrix $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_K]$ and provide the quantities $\mathcal{N}_k$ and $\mathbf{b}_k$ as a feedback to each SN $k$ in the WSN.
Initialize $0 < \psi < 1$, $\{\varepsilon_k^{(0)}\}_{k=1}^{K}$=0, $\{\boldsymbol{\phi}_k^{(0)}\}_{k=1}^{K} = \mathbf{0}$ and $\boldsymbol{\beta}_k^{(0)} = \mathbf{0}$.
**At each SN** $k$:
**for** $i = 0, 1, 2, \ldots$ **do**
    Compute $\boldsymbol{\beta}_k^{(i+1)}$ from (24) and $\varepsilon_k^{(i+1)}$ using (21)
    Set $\boldsymbol{\zeta}_k^{(0)} = \boldsymbol{\beta}_k^{(i+1)}$ and $\boldsymbol{\upsilon}_k(-1) = \mathbf{0}$
    **for** $j = 0, 1, 2, \ldots$ **do**
        Generate $\boldsymbol{\upsilon}_k(j) \sim \mathcal{CN}(\mathbf{0}, \xi \mathrm{diag}[\boldsymbol{\zeta}_k])$
        Determine $\boldsymbol{\pi}_k(j)$=$\phi^j \boldsymbol{\upsilon}_k(j) - \phi^{(j-1)} \boldsymbol{\upsilon}_k(j-1)$
        Next, calculate $\boldsymbol{\zeta}_k^{+}(j) = \boldsymbol{\zeta}_k(j) + \boldsymbol{\pi}_k(j)$.
        Receive $\boldsymbol{\zeta}_k^{+}(j)$ from neighbours
        Update $\boldsymbol{\zeta}_k(j+1) = b_{kk}\boldsymbol{\zeta}_k^{+}(j) + \sum_{l \in \mathcal{N}_j} b_{kl}\boldsymbol{\zeta}_l^{+}(j)$
    **end for**
    Update $\boldsymbol{\beta}^{(i+1)} = \boldsymbol{\zeta}_k(j+1)$ and $\boldsymbol{\phi}^{(i+1)}$ using (26)
**end for**
Forward $\gamma_m^{\mathrm{opt}}$ for each $m$ to FC and derive $\mathbf{F}_k$ from $\mathbf{f}_k$ for each SN $k$ in the WSN.
```

This implies that

$$\lim_{j\to\infty} \mathbb{E}\left[\sum_{m_1=1}^{j}\sum_{m_2=1}^{j} \boldsymbol{\pi}_k(m_1)\boldsymbol{\pi}_k^H(m_2)\right] = \mathbf{0} \quad \forall\ k. \tag{31}$$

Proof: Enforcing the condition that each SN k in the network should satisfy $\mathcal{N}_k \cup \{k\} \nsubseteq \mathcal{N}_l \cup \{l\}$, where $k \neq l$, implies that the initial condition of the SN k can't be inferred by any other SN l. Hence, the proposed distributed TPC design is privacy-preserving in nature. Next, we demonstrate the convergence of the proposed design to the optimal solution.

To this end, let the matrices $\boldsymbol{\Xi}(j) \in \mathbb{C}^{NN_{fc}K \times K}$, $\boldsymbol{\Pi}(j) \in \mathbb{C}^{NN_{fc}K \times K}$, and $\mathbf{V}(j) \in \mathbb{C}^{NN_{fc}K \times K}$ be defined as

$$\boldsymbol{\Xi}(j) = [\boldsymbol{\zeta}_1(j), \boldsymbol{\zeta}_2(j), \ldots, \boldsymbol{\zeta}_K(j)], \tag{32}$$

$$\boldsymbol{\Pi}(j) = [\boldsymbol{\pi}_1(j), \boldsymbol{\pi}_2(j), \ldots, \boldsymbol{\pi}_K(j)], \tag{33}$$

$$\mathbf{V}(j) = [\mathbf{V}_1(j), \mathbf{V}_2(j), \ldots, \mathbf{V}_K(j)]. \tag{34}$$

Then the cumulative update equation can be written as

$$\boldsymbol{\Xi}^T(j+1) = \mathbf{B}\left[\boldsymbol{\Xi}^{+}(j)\right]^T = \mathbf{B}\left[\boldsymbol{\Xi}(j) + \boldsymbol{\Pi}(j)\right]^T. \tag{35}$$

Let $\bar{\mathbf{B}} = \mathbf{B} - \frac{\mathbf{1}\mathbf{1}^T}{K}$. Using the result

$$\frac{\mathbf{1}\mathbf{1}^T}{K}\mathbf{B} = \frac{\mathbf{1}\mathbf{1}^T}{K} = \mathbf{B}\frac{\mathbf{1}\mathbf{1}^T}{K}, \tag{36}$$

it is easy to see that the following equalities hold

$$\mathbf{B}^m(\mathbf{B} - \mathbf{I}) = \bar{\mathbf{B}}^m(\mathbf{B} - \mathbf{I}) \tag{37}$$

$$\mathbf{B}^m - \frac{\mathbf{1}\mathbf{1}^T}{K} = \bar{\mathbf{B}}^m\left(\mathbf{I} - \frac{\mathbf{1}\mathbf{1}^T}{K}\right). \tag{38}$$

Then, (35) simplifies to

$$\begin{aligned}\boldsymbol{\Xi}^T(j+1) &= \mathbf{B}^{j+1}\boldsymbol{\Xi}^T(0) + \sum_{t=0}^{j}\mathbf{B}^{j+1-t}\boldsymbol{\Pi}^T(t), \\ &= \mathbf{B}^{j+1}\boldsymbol{\Xi}^T(0) + \phi^j\mathbf{B}\mathbf{V}^T(j) + \sum_{t=0}^{j-1}\phi^t\mathbf{B}^{j-t}(\mathbf{B} - \mathbf{I})\mathbf{V}^T(t).\end{aligned} \tag{39}$$

Let the matrix $\mathbf{X} \in \mathbb{C}^{KNN_{fc}P \times K}$ be defined by concatenating the vector $\boldsymbol{\beta}$, K times as

$$\mathbf{X} = [\boldsymbol{\beta}, \boldsymbol{\beta}, \ldots, \boldsymbol{\beta}]. \tag{40}$$

Furthermore, defining $\mathbf{X}^T = \frac{\mathbf{1}\mathbf{1}^T}{K}\boldsymbol{\Xi}^T(0)$ yields the error matrix $\mathbf{C} = \boldsymbol{\Xi}(j) - \mathbf{X}^i$ and its expression is given as

$$\begin{aligned}\mathbf{C}^T(j+1) =& \bar{\mathbf{B}}^{j+1}\mathbf{C}^T(0) + \phi^j\mathbf{B}\mathbf{V}^T(j) \\ &+ \sum_{t=0}^{j-1}\phi^t\bar{\mathbf{B}}^{j-t}(\mathbf{B} - \mathbf{I})\mathbf{V}^T(t).\end{aligned} \tag{41}$$

One can now demonstrate that we have $\lim_{j\to\infty}\mathbb{E}\left[||\mathbf{C}(j+1)||_F^2\right] = 0$ as shown below:

$$\begin{aligned}&\lim_{j\to\infty}\mathbb{E}\left[||\mathbf{C}(j+1)||_F^2\right] = \lim_{j\to\infty}\mathbb{E}\left[\mathrm{Tr}\left[\mathbf{C}^H(j+1)\mathbf{C}(j+1)\right]\right] \\ &= \mathrm{Tr}\Bigg[\bar{\mathbf{B}}^{j+1}\mathbf{C}^T(0)\mathbf{C}^*(0)\left(\bar{\mathbf{B}}^{j+1}\right)^T + \phi^{2j}\mathbf{B}\mathbf{V}^T(j)\mathbf{V}^*(j)\mathbf{B}^H \\ &\left(\sum_{t=0}^{j-1}\phi^t\bar{\mathbf{B}}^{j-t}(\mathbf{B} - \mathbf{I})\mathbf{V}^T(t)\right)\left(\sum_{t=0}^{j-1}\phi^t\bar{\mathbf{B}}^{j-t}(\mathbf{B} - \mathbf{I})\mathbf{V}^T(t)\right)^H\Bigg].\end{aligned} \tag{42}$$

As $j \to \infty$, since all the eigenvalues of $\bar{\mathbf{B}}$ are less than 1 and ϕ satisfies the condition $0 < \phi < 1$, it can be deduced from the above equation that

$$\lim_{j\to\infty}\mathbb{E}\left[||\mathbf{C}(j+1)||_F^2\right] = 0. \tag{43}$$

Thus, it follows that

$$\lim_{j\to\infty}\left|\left|\boldsymbol{\zeta}_k(j) - \boldsymbol{\beta}^{(i+1)}\right|\right| = 0,\ \forall\ k.$$

Furthermore, multiplying Eq.(35) with $\mathbf{1}^T$ at both sides, one obtains

$$\mathbf{1}^T\boldsymbol{\Xi}^T(j+1) = \mathbf{1}^T\mathbf{B}\left[\boldsymbol{\Xi}(j) + \boldsymbol{\Pi}(j)\right]^T = \mathbf{1}^T\boldsymbol{\Xi}^T(j) + \mathbf{1}^T\boldsymbol{\Pi}(j)^T.$$

Next, defining $\mathbf{U}(j) = [\mathbf{u}_1^T(j); \mathbf{u}_1^T(j); \ldots; \mathbf{u}_K^T(j)] = \sum_{t=0}^{j}\boldsymbol{\Pi}(t)$ and using $\mathbf{1}^T\boldsymbol{\Xi}^T(0) = \mathbf{1}^T\mathbf{X}^T$, the above equation can be recast as

$$\mathbf{1}^T\boldsymbol{\Xi}^T(j+1) = \mathbf{1}^T\boldsymbol{\Xi}^T(0) + \mathbf{1}^T\mathbf{U}(j)^T = \mathbf{1}^T\tilde{\boldsymbol{\beta}}^T + \mathbf{1}^T\mathbf{U}(j)^T. \tag{44}$$

From (43), it follows that

$$\lim_{j\to\infty}\mathbb{E}\left[\left(\sum_{k=1}^{K}\mathbf{u}_k(j)\right)\left(\sum_{k=1}^{K}\mathbf{u}_k(j)\right)^H\right] = \mathbf{0}. \tag{45}$$

Furthermore, since the noise $\boldsymbol{\pi}_k$ is independent across the SNs, one may conclude that $\mathbb{E}\left[\mathbf{u}_m(j)\mathbf{u}_n(j)^H\right] = \mathbf{0}$. This implies that

$$\lim_{j\to\infty} \mathbb{E}\left[\mathbf{u}_k(j)\mathbf{u}_k^H(j)\right] = \mathbf{0} \quad \forall \ k. \tag{46}$$

Finally, it may be concluded that

$$\lim_{j\to\infty} \mathbb{E}\left[\sum_{m_1=1}^{j}\sum_{m_2=1}^{j} \boldsymbol{\pi}_k(m_1)\boldsymbol{\pi}_k^H(m_2)\right] = \mathbf{0} \quad \forall \ k.$$

■

1) Privacy-limit calculation: We now derive the privacy limit offered by the proposed privacy-preserving distributed beamforming algorithm. Without loss of generality, assume that the Kth SN acts as an Ev and desires to infer the initial conditions of its neighbouring SNs during each ADMM iteration.

To this end, upon generalizing Theorem 3 of [12], we let the matrix $\widetilde{\mathbf{B}} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}$ be defined as $\widetilde{\mathbf{B}} = \mathbf{B}(1:K-1, 1:K-1) \otimes \mathbf{I}_{NN_{fc}P}$, which is obtained by removing the Kth column and row of the matrix $\mathbf{B}$. Furthermore, let $\boldsymbol{\mathcal{B}} = \left(\mathbf{I}_{NN_{fc}P(K-1)} - \widetilde{\mathbf{B}}\right)^{-1} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}$, and $\mathbf{T} = \left[\mathbf{e}_{l_1} \otimes \mathbf{I}_{NN_{fc}P}, \mathbf{e}_{l_2} \otimes \mathbf{I}_{NN_{fc}P}, \ldots, \mathbf{e}_{l_{|\mathcal{N}_k|}} \otimes \mathbf{I}_{NN_{fc}P}\right]^T \in \mathbb{C}^{NN_{fc}P|\mathcal{N}_k|\times NN_{fc}P(K-1)}$, where $\mathbf{e}_k \in \mathbb{R}^{K-1\times 1}$ represents a vector with its kth element equal to 1 and the remaining elements zero. In addition, let the matrices

$$\mathbf{L}_j = \xi \mathrm{diag}\left(\left[\boldsymbol{\zeta}_1^T(j), \boldsymbol{\zeta}_2^T(j), \ldots, \boldsymbol{\zeta}_{K-1}^T(j)\right]^T\right) \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}, \tag{47}$$

$$\mathbf{U}_j = \mathbf{T}^T\left(\mathbf{T}\mathbf{L}_j\mathbf{T}^T\right)^{-1}\mathbf{T} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}, \tag{48}$$

$$\mathbf{V}_j = \mathbf{I}_{NN_{fc}P(K-1)} - \mathbf{L}_j^{\frac{1}{2}}\mathbf{U}_j\mathbf{L}_j^{\frac{1}{2}} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}, \tag{49}$$

$$\mathbf{H}_j = \boldsymbol{\mathcal{B}}\mathbf{U}_j\boldsymbol{\mathcal{B}} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}. \tag{50}$$

Let the eigenvalue decomposition of the matrix $\mathbf{H}_j$ be defined as

$$\mathbf{H}_j = \left[\mathbf{R}_{j,1}\ \mathbf{R}_{j,2}\right]\mathrm{diag}\left[\boldsymbol{\Lambda}_j,\ \mathbf{0}\right]\left[\mathbf{R}_{j,1}\ \mathbf{R}_{j,2}\right]^H, \tag{51}$$

where $\mathbf{R}_{j,2} \in \mathbb{R}^{NN_{fc}P(K-1)\times NN_{fc}P(K-|\mathcal{N}_K|-1)}$ contains the eigenvectors corresponding to zero eigenvalues. The privacy offered by the kth SN is defined as

$$\mathrm{Tr}\left[\mathbf{M}_k\right] = \mathrm{Tr}\left[\left[\mathbf{e}_k^T \otimes \mathbf{I}_{NN_{fc}P}\right]\mathbf{P}\left[\mathbf{e}_k \otimes \mathbf{I}_{NN_{fc}P}\right]\right], \tag{52}$$

where $\mathbf{P} = \lim_{j\to\infty}\mathbf{P}_j$ is obtained using the following recursive equation

$$\mathbf{P}_j = \mathbf{R}_{j,2}\left[\mathbf{R}_{j,2}^H\boldsymbol{\mathcal{B}}\mathbf{X}_j\boldsymbol{\mathcal{B}}\mathbf{R}_{j,2}\right]^{-1}\mathbf{R}_{j,2}^H. \tag{53}$$

The matrix $\mathbf{X}_{j+1} \in \mathbb{C}^{NN_{fc}P(K-1)\times NN_{fc}P(K-1)}$ is defined as

$$\mathbf{X}_{j+1} = \mathbf{X}_0 + \phi^{-2}\widetilde{\mathbf{B}}\left[\mathbf{X}_j^{+} - \mathbf{X}_j^{+}\left[\phi^2\mathbf{I} + \mathbf{X}_j^{+}\right]^{-1}\mathbf{X}_j^{+}\right], \tag{54}$$

where $\mathbf{X}_j^{+} = \mathbf{L}_j^{\frac{1}{2}}\mathbf{V}_j\mathbf{Y}_j\mathbf{V}_j\mathbf{L}_j^{\frac{1}{2}}$, and $\mathbf{X}_0 = \widetilde{\mathbf{B}}\mathbf{U}_0\widetilde{\mathbf{B}}$. The next section describes the procedure of our privacy-preserving distributed TPC design for a system transmitting quantized measurements.

C. Quantized vector transmission

Below, an RDT based optimal quantizer is conceived for the quantization of each SN's measurements, which exploits the temporal correlation inherent in the parameter vector s. To begin with, a zero-forcing (ZF) estimator is employed initially at the kth SN for eliminating the inter-parameter interference, followed by the quantization of the individual components of the FD observation vector $\mathbf{z}_k(m)$. The ZF-estimate of $\mathbf{z}_k(m)$ in (7) can be modeled as

$$\widehat{\mathbf{z}}_k(m) = \mathbf{s}(m) + \left[\mathbf{C}_k^H\mathbf{C}_k\right]^{-1}\mathbf{C}_k^H\mathbf{w}_k(m) = \mathbf{s}(m) + \mathbf{t}_k(m),$$

where $\mathbf{t}_k(m) \in \mathbb{C}^{P\times 1}$ is the effective noise after the ZF operation. Furthermore, without loss of generality, assuming $\boldsymbol{\Sigma}_k(m) = \sigma^2\mathbf{I}_{N_s}$, the noise $\mathbf{t}_k(m)$ follows the distribution $\mathbf{t}_k(m) \sim \mathcal{CN}\left(\mathbf{0}, \sigma^2\left[\mathbf{C}_k^H\mathbf{C}_k\right]^{-1}\right)$. Let the ith element of the ZF-estimate of $\widehat{\mathbf{z}}_k(m)$ be represented by $\widehat{z}_{k,i}(m)$, which is given by

$$\widehat{z}_{i,k}(m) = s_i(m) + t_{i,k}(m), \tag{55}$$

and its variance denoted by $\sigma_{i,k}^2(m)$ is formulated as

$$\sigma_{i,k}^2(m) = \mathbb{E}\left[|\widehat{z}_{i,k}(m)|^2\right] = \Phi_i(f_m) + \sigma_{t_{i,k}}^2(m), \tag{56}$$

where $\sigma_{t_{i,k}}^2(m) = \left[\sigma^2\left[\mathbf{C}_k^H\mathbf{C}_k\right]^{-1}\right]_{ii}$. As described in [7], using the results from RDT [39, Th. 10.3.2], the optimal number of bits $\alpha_{i,k}^{\mathrm{opt}}(m)$ to be allocated for the quantization of the Gaussian sample $\widehat{z}_{i,k}(m)$ is given as

$$\alpha_{i,k}^{\mathrm{opt}}(m) = \frac{A}{N} - \ln(4)\left[\left[\frac{1}{N}\sum_{m=0}^{N-1}\ln\left[\tilde{\sigma}_{i,k}^2(m)\right]\right] - \ln\left[\tilde{\sigma}_{i,k}^2(m)\right]\right], \tag{57}$$

where $\tilde{\sigma}_{i,k}^2(m) = \sigma_{i,k}^2(m)\ln(4)$ and A denotes the total bit-rate budget. The quantized version of $z_{i,k}(m)$, which is denoted by $z_{i,k}^q(m)$, can be modeled as

$$z_{i,k}^q(m) = z_{i,k}(m) + t_{i,k}^q(m) = s_i(m) + \bar{t}_{i,k}(m), \tag{58}$$

where we have $\bar{t}_{i,k}(m) = t_{i,k}(m) + t_{i,k}^q(m)$. The quantity $t_{i,k}^q(m)$ denotes the ensuing quantization noise that has a mean of zero and variance of $\sigma_{t,q}^2$. Furthermore, assuming that the quantity $t_{i,k}(m)$ and the quantization noise $t_{i,k}^q(m)$ are uncorrelated [40, Sec. 6.3], the variance of the effective noise $\bar{t}_{i,k}(m)$ can be expressed as

$$\sigma_{\bar{t}}^2(m) = \sigma_{t_{i,k}}^2(m) + \sigma_{t,q}^2. \tag{59}$$

Let $\bar{\mathbf{t}}_k(m) \in \mathbb{C}^{P\times 1}$ denote the stacked vector of effective noise terms $\bar{t}_{i,k}(m)$ having the covariance matrix $\boldsymbol{\Sigma}_{\bar{t}}(m)) = \mathrm{diag}\left[\sigma_{\bar{t}_{i,1}}^2(m), \sigma_{\bar{t}_{i,2}}^2(m), \ldots, \sigma_{\bar{t}_{i,p}}^2(m)\right] \in \mathbb{C}^{P\times P}$. The pertinent optimization problem of SMSE minimization using quantized measurements can be formulated similar to (18), with the matrix $\boldsymbol{\Psi}_k$ replaced by $\boldsymbol{\Psi}_{q,k}$ and the TPC vector $\mathbf{f}_k$ replaced by $\mathbf{f}_{q,k}$. Furthermore, we have $\boldsymbol{\Psi}_{q,k}(m) = \left[\boldsymbol{\Sigma}_{e,k}(m) \otimes \mathbf{G}_k^H(m)\mathbf{G}_k(m)\right] \in \mathbb{C}^{N_s^2\times N_s^2}$, where the matrix $\boldsymbol{\Psi}_{q,k} \in \mathbb{C}^{NN_s^2\times NN_s^2}$ is defined as

$$\boldsymbol{\Psi}_{q,k} = \mathrm{diag}\left[\boldsymbol{\Psi}_{q,k}(0), \boldsymbol{\Psi}_{q,k}(1), \ldots, \boldsymbol{\Psi}_{q,k}(N-1)\right].$$

The optimal TPC vector $\mathbf{f}_{q,k}^{\text{opt}}$ is formulated as

$$\mathbf{f}_{q,k}^{\text{opt}} = -\frac{1}{2}\left[\boldsymbol{\Psi}_{q,k} + \varepsilon_{q,k}^{\text{opt}}\boldsymbol{\Pi}_k\right]^{-1}\mathbf{E}_k^H\boldsymbol{\beta}_q^{\text{opt}}. \tag{60}$$

For each SN k, the dual variable $\varepsilon_k^{\text{opt}}$ can be obtained by solving equation [37, App. A]

$$\left\|\boldsymbol{\Pi}_k^{\frac{1}{2}}\left[\boldsymbol{\Psi}_{q,k} + \varepsilon_{q,k}^{\text{opt}}\boldsymbol{\Pi}_k\right]^{-1}\mathbf{E}_k\boldsymbol{\beta}_q^{\text{opt}}\right\|_2^2 = 4\mathcal{P}_k. \tag{61}$$

The DC-ADMM framework can be invoked once again to solve the above optimization problem and the closed-form solutions of the quantities $\boldsymbol{\beta}_{q,k}^{(i+1)}$, $\boldsymbol{\beta}_q^{(i+1)}$, and $\boldsymbol{\psi}_{q,k}^{(i+1)}$ during the ith DC-ADMM iteration may be expressed as

$$\boldsymbol{\beta}_{q,k}^{(i+1)} = \mathbf{Q}_{q,k}^{-1}\left[\frac{\rho}{2}\boldsymbol{\beta}_q^i - \frac{\boldsymbol{\psi}_{q,k}^i}{2} - \frac{2\mathbf{h}}{K}\right], \tag{62}$$

$$\boldsymbol{\beta}_q^{(i+1)} = \frac{1}{K}\sum_{k=1}^{K}\boldsymbol{\beta}_{q,k}^{(i+1)}, \tag{63}$$

$$\boldsymbol{\psi}_{q,k}^{(i+1)} = \boldsymbol{\psi}_{q,k}^i + \rho\left[\boldsymbol{\beta}_{q,k}^{(i+1)} - \boldsymbol{\beta}_q^{(i+1)}\right], \tag{64}$$

where we have $\mathbf{Q}_{q,k} = \left[\mathbf{E}_k\left[\boldsymbol{\Psi}_{q,k} + \varepsilon_{q,k}\boldsymbol{\Pi}_{q,k}\right]^{-1}\mathbf{E}_k^H + \frac{\rho}{2}\mathbf{I}_{NN_{fc}K}\right] \in \mathbb{C}^{NN_{fc}K\times NN_{fc}K}$ and $\boldsymbol{\psi}_{q,k}$ is the dual variable corresponding to the consensus constraint. The privacy-preserving distributed TPC procedure of this scenario can be obtained similar to Algorithm 1 upon replacing the quantities $\boldsymbol{\beta}_k$, $\boldsymbol{\beta}$, $\boldsymbol{\psi}_k$ by $\boldsymbol{\beta}_{q,k}$, $\boldsymbol{\beta}_q$, $\boldsymbol{\psi}_{q,k}$, respectively.

III. Bayesian Cramer Rao Bound (BCRB)

The BCRB is derived for benchmarking the performance of the proposed designs. The best estimation performance can be achieved when all the measurements corresponding to each sensor on each subcarrier are available with infinite precision at the FC. Hence, the overall stacked observation vector can be modeled as

$$\breve{\mathbf{z}} = \breve{\mathbf{C}}\breve{\mathbf{s}} + \breve{\mathbf{w}}, \tag{65}$$

where $\breve{\mathbf{z}} \in \mathbb{C}^{KlN\times 1}$, $\breve{\mathbf{C}} \in \mathbb{C}^{KlN\times NP}$, and $\breve{\mathbf{w}} \in \mathbb{C}^{KlN\times 1}$ are defined as

$$\breve{\mathbf{z}} = \left[\mathbf{z}_1^T(0), \mathbf{z}_1^T(1), \ldots, \mathbf{z}_K^T(N-1)\right]^T \tag{66}$$

$$\breve{\mathbf{C}} = \left[\mathbf{C}_1 \otimes \mathbf{I}_N, \mathbf{C}_2 \otimes \mathbf{I}_N, \ldots, \mathbf{C}_K \otimes \mathbf{I}_N\right]^T \tag{67}$$

$$\breve{\mathbf{w}} = \left[\mathbf{w}_1^T(0), \mathbf{w}_1^T(1), \ldots, \mathbf{w}_K^T(N-1)\right]^T. \tag{68}$$

Hence, the BCRB for the vector parameter estimation scenario can be evaluated as [41]

$$\text{BCRB} = \text{Tr}\left[\left[\boldsymbol{\Sigma}_s^{-1} + \breve{\mathbf{C}}^H\breve{\boldsymbol{\Sigma}}_w^{-1}\breve{\mathbf{C}}\right]^{-1}\right], \tag{69}$$

where the quantities $\boldsymbol{\Sigma}_s \in \mathbb{C}^{NK\times NK}$ and $\breve{\boldsymbol{\Sigma}}_w \in \mathbb{C}^{LNq\times LNq}$ denote the covariance matrices of the parameter vector $\breve{\mathbf{s}}$ and stacked observation noise vector $\breve{\mathbf{u}}$, respectively, which are defined as

$$\boldsymbol{\Sigma}_s = \text{diag}\left[\boldsymbol{\Sigma}(0), \boldsymbol{\Sigma}(1), \ldots, \boldsymbol{\Sigma}(N-1)\right] \tag{70}$$

$$\breve{\boldsymbol{\Sigma}}_w = \text{diag}\left[\boldsymbol{\Sigma}_{w,1}(0), \boldsymbol{\Sigma}_{w,2}(1), \ldots, \boldsymbol{\Sigma}_{w,K}(N-1)\right], \tag{71}$$

respectively. The next section presents the simulation results for characterizing the performance of the various designs proposed in this work.

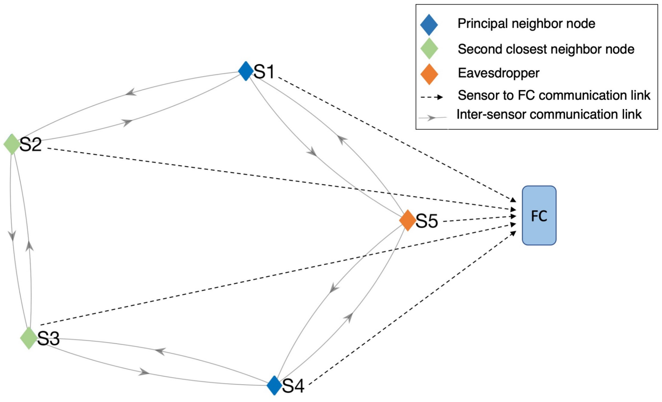

Principal neighbor node
Second closest neighbor node
Eavesdropper
Sensor to FC communication link
Inter-sensor communication link
S1
S2
S3
S4
S5
FC

Fig. 1. Scatter plot depicting the SN arrangement in the WSN considered.

Parameter	Value
Number of SNs (K)	5
Number of subcarriers N	32
Number of antennas at each SN (N_s)	3
Number of antennas at the FC (N_{fc})	3
Number of elements in the parameter vector P	3
Privacy parameter ξ	0.9
Observation SNR (SNR$_{\text{OB}}$)	-10 dB
SNR at the FC (SNR$_{\text{FC}}$)	20 dB

TABLE II
SUMMARY OF SYSTEM PARAMETERS

IV. Simulation Results

The simulation setup considered is as follows, which is also summarized in Table 1. The number of SNs K is set equal to 5, which are assumed to be deployed in a ring topology, so that every SN has two immediate neighboring SNs and two second-closest neighbor SNs. The immediate neighbor SNs are those SNs which are connected directly to the SN of interest while the second-closest neighbor SNs are the nodes which are connected directly to the immediate neighbors other than the SN of interest. The SNs positions are shown in Fig.1, where the 5th SN is acting as an Ev having SNs 1 and 4 as its immediate neighbors, while the SNs 2 and 4 are its second-closest neighbors. The number of subcarriers N at each SN is set to 32. The signal to noise ratio (SNR) at the FC, denoted by SNR$_{\text{FC}}$, is set to 20 dB, while the privacy parameter is $\xi = 0.9$. The observation SNR (SNR$_{\text{OB}}$) is equal to -10 dB. Due to the dearth of similar algorithms in the literature we are unable to show any performance comparison with the existing works. However, we have derived the BCRB, which serves as a lower bound for the performance of the decentralized parameter estimation schemes.

Fig. 2 shows the normalized SMSE (NSMSE) performance as a function of the SNR$_{\text{FC}}$ for both analog as well as quantized

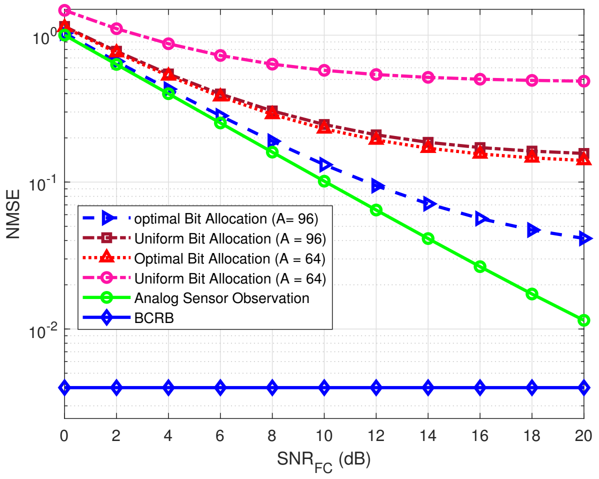


Fig. 2. NMSE versus SNR$_{\text{FC}}$ for the analog and quantizated transmission schemes for different values of the total bit-rate budget $\boldsymbol{A}$.

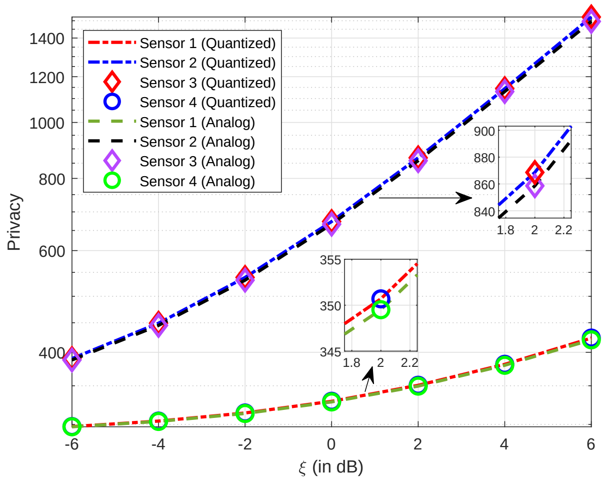


Fig. 3. Privacy offered by the WSN versus the privacy parameter $\boldsymbol{\xi}$ for the analog and quantized measurement transmission scenarios.

SN measurement transmission. It can be readily observed from the plot that the NSMSE performance of the quantized scenario improves as the bit-rate budget of quantization increases and it approaches that of the analog sensor observation transmission scenario with as few as 3 bits per subcarrier. It can also be deduced from the figure that the estimation performance improves upon increasing SNR$_{\text{FC}}$ and at high SNR$_{\text{FC}}$ the MSE performance of the analog measurement transmission scheme approaches the BCRB.

Fig. 3 quantifies the privacy performance of the different SNs in the WSN against the privacy parameter ξ using the procedure described in II-B.1. Since, $\text{Tr}\left[\mathbf{M}_k\right] > 0$, the proposed design is privacy-preserving in nature. The figure clearly evidences the fact that SNs 1 and 4, which are the immediate neighbours of the Ev, yield the same privacy, which is lower than that offered by second-closest neighbours namely SNs 2 and 3. The intuition behind this behaviour is that the immediate neighbours SNs 1 and 4 are directly communicating with the Ev and hence their information is less perturbed in comparison to the second-closest neighbours 2 and 3, which are not sharing their dual variable directly with the Ev and hence their privacy is improved. The privacy parameter ξ can be tuned to obtained the required privacy levels at different agents, as shown in Fig.3 . Observe that the privacy varies across the network depending on the relative placement of the adversary. Hence, ξ acts as a single parameter controlling the privacy across different agents.

Fig. 4 depicts the NSMSE performance as a function of the privacy parameter ξ for both analog as well as quantized SN measurement transmission in our sensor network. It can be readily observed from the plot that the NSMSE performance deteriorates as the value of the privacy parameter ξ increases, which demonstrates the trade-off between the privacy guarantee and the estimation accuracy. The reason behind this behaviour is that the privacy parameter ξ directly affects the variance of the noise to be added to the dual variable of each sensor, which leads to better privacy at the cost of eroded estimation performance. It can once again be seen from the figure that the NMSE of quantized measurements approaches the performance associated with ideal analog sensor measurement transmission, as the number of bits increases.

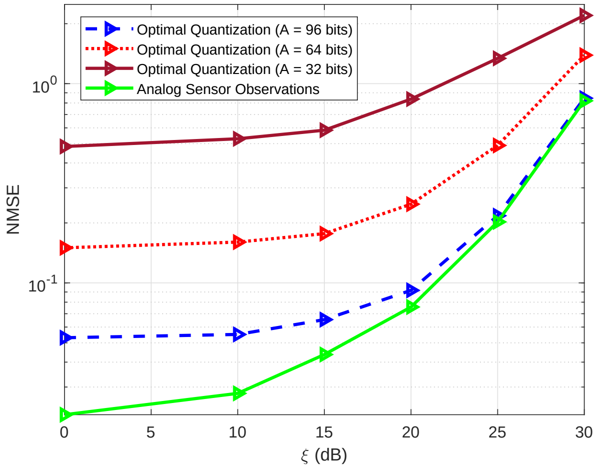


Fig. 4. NMSE versus the privacy parameter $\boldsymbol{\xi}$ for the analog and quantizated measurement transmission schemes for different values of the bit budget $\boldsymbol{A}$.

V. Conclusion

Novel DC-ADMM-based privacy-preserving distributed TPC designs were conceived for the estimation of a temporally correlated vector parameter relying on both analog as well as quantized measurement transmission. The privacy-preserving algorithm conceived ensures that each sensor's dual variable is transmitted in a secure fashion to the other SNs in the sensor network. Explicit theoretical guarantees were provided for characterizing the privacy-preserving nature of the design presented. The BCRB was also derived for benchmarking the MSE performance of the proposed distributed estimation technique. Finally, simulation results were provided for comprehensively characterizing the NMSE and privacy performance of the schemes conceived.

This work can be further extended to massive or mmWave MIMO WSNs, considering the availability of perfect and imperfect CSI. Furthermore, intelligent reflecting surface (IRS) can be harnessed for privacy-preserving distributed parameter estimation. As for application scenarios, both the IoTs ans its underwater counterpart [42] as well as unmanned aerial vehicle (UAV)-aided systems [43] might be considered.

References

[1] R. Lara, D. Benítez, A. Caamaño, M. Zennaro, and J. L. Rojo-Álvarez, “On real-time performance evaluation of volcano-monitoring systems with wireless sensor networks,” *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3514–3523, 2015.

[2] S. Amendola, G. Bovesecchi, A. Palombi, P. Coppa, and G. Marrocco, “Design, calibration and experimentation of an epidermal RFID sensor for remote temperature monitoring,” *IEEE Sensors Journal*, vol. 16, no. 19, pp. 7250–7257, 2016.

[3] K. Ma, Z. Li, P. Liu, J. Yang, Y. Geng, B. Yang, and X. Guan, “Reliability-constrained throughput optimization of industrial wireless sensor networks with energy harvesting relay,” *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13 343–13 354, 2021.

[4] J. J. Estrada-López, A. A. Castillo-Atoche, J. Vázquez-Castillo, and E. Sánchez-Sinencio, “Smart soil parameters estimation system using an autonomous wireless sensor network with dynamic power management strategy,” *IEEE Sensors Journal*, vol. 18, no. 21, pp. 8913–8923, 2018.

[5] B. Velusamy and S. C. Pushpan, “An enhanced channel access method to mitigate the effect of interference among body sensor networks for smart healthcare,” *IEEE Sensors Journal*, vol. 19, no. 16, pp. 7082–7088, 2019.

[6] J.-J. Xiao, S. Cui, Z.-Q. Luo, and A. J. Goldsmith, “Linear coherent decentralized estimation,” *IEEE Transactions on Signal Processing*, vol. 56, no. 2, pp. 757–770, 2008.

[7] K. P. Rajput, M. F. Ahmed, N. K. D. Venkategowda, A. K. Jagannatham, G. Sharma, and L. Hanzo, “Robust decentralized and distributed estimation of a correlated parameter vector in MIMO-OFDM wireless sensor networks,” *IEEE Transactions on Communications*, pp. 1–1, 2021.

[8] K. P. Rajput, Y. Verma, N. K. D. Venkategowda, A. K. Jagannatham, and P. K. Varshney, “Linear MMSE precoder combiner designs for decentralized estimation in wireless sensor networks,” in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6.

[9] A. S. Behbahani, A. M. Eltawil, and H. Jafarkhani, “Linear decentralized estimation of correlated data for power-constrained wireless sensor networks,” *IEEE Transactions on Signal Processing*, vol. 60, no. 11, pp. 6003–6016, 2012.

[10] Y. Liu, J. Li, and X. Lu, “Joint transceiver design for linear MMSE data fusion in coherent MAC wireless sensor networks,” *Information Fusion*, vol. 37, pp. 37–49, 2017.

[11] N. K. D. Venkategowda, H. Lee, and I. Lee, “Joint transceiver designs for MSE minimization in MIMO wireless powered sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5120–5131, 2018.

[12] Y. Mo and R. M. Murray, “Privacy preserving average consensus,” *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2017.

[13] K. P. Rajput, Y. Verma, N. K. D. Venkategowda, A. K. Jagannatham, and P. K. Varshney, “Robust linear transceiver designs for vector parameter estimation in MIMO wireless sensor networks under CSI uncertainty,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7347–7362, 2021.

[14] K. P. Rajput, A. Kumar, S. Srivastava, A. K. Jagannatham, and L. Hanzo, “Bayesian learning-based linear decentralized sparse parameter estimation in MIMO wireless sensor networks relying on imperfect CSI,” *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6236–6250, 2021.

[15] S. Khobahi, M. Soltanalian, F. Jiang, and A. L. Swindlehurst, “Optimized transmission for parameter estimation in wireless sensor networks,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 6, pp. 35–47, 2020.

[16] J. Akhtar and K. Rajawat, “Distributed sequential estimation in wireless sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 86–100, 2018.

[17] S. Liu, S. Kar, M. Fardad, and P. K. Varshney, “Optimized sensor collaboration for estimation of temporally correlated parameters,” *IEEE Transactions on Signal Processing*, vol. 64, no. 24, pp. 6613–6626, 2016.

[18] Y. Liu, J. Li, and H. Wang, “Robust linear beamforming in wireless sensor networks,” *IEEE Transactions on Communications*, vol. 67, no. 6, pp. 4450–4463, 2019.

[19] A. Shirazinia, S. Dey, D. Ciuonzo, and P. Salvo Rossi, “Massive MIMO for decentralized estimation of a correlated source,” *IEEE Transactions on Signal Processing*, vol. 64, no. 10, pp. 2499–2512, 2016.

[20] J. Z. Sun and V. K. Goyal, “Intersensor collaboration in distributed quantization networks,” *IEEE Transactions on Communications*, vol. 61, no. 9, pp. 3931–3942, 2013.

[21] E. J. Msechu and G. B. Giannakis, “Sensor-centric data reduction for estimation with WSNs via censoring and quantization,” *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 400–414, 2012.

[22] M. H. Chaudhary and L. Vandendorpe, “Power constrained linear estimation in wireless sensor networks with correlated data and digital modulation,” *IEEE Transactions on Signal Processing*, vol. 60, no. 2, pp. 570–584, Feb 2012.

[23] A. Sani and A. Vosoughi, “Distributed vector estimation for power- and bandwidth-constrained wireless sensor networks,” *IEEE Transactions on Signal Processing*, vol. 64, no. 15, pp. 3879–3894, 2016.

[24] Y. Zhou, C. Huang, T. Jiang, and S. Cui, “Wireless sensor networks and the Internet of Things: Optimal estimation with nonuniform quantization and bandwidth allocation,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3568–3574, Oct 2013.

[25] Z. Li and T. J. Oechtering, “Privacy-constrained parallel distributed Neyman-Pearson test,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 77–90, 2017.

[26] J. Guo, U. Rogers, X. Li, and H. Chen, “Secrecy constrained distributed detection in sensor networks,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 2, pp. 378–391, 2018.

[27] X. He, W. P. Tay, and M. Sun, “Privacy-aware decentralized detection using linear precoding,” in *2016 IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, 2016, pp. 1–5.

[28] X. Guo, A. S. Leong, and S. Dey, “Estimation in wireless sensor networks with security constraints,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 2, pp. 544–561, 2017.

[29] ——, “Distortion outage minimization in distributed estimation with estimation secrecy outage constraints,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 12–28, 2017.

[30] C. Göken and S. Gezici, “ECRB-based optimal parameter encoding under secrecy constraints,” *IEEE Transactions on Signal Processing*, vol. 66, no. 13, pp. 3556–3570, 2018.

[31] A. De Maio, S. De Nicola, Y. Huang, S. Zhang, and A. Farina, “Code design to optimize radar detection performance under accuracy and similarity constraints,” *IEEE Transactions on Signal Processing*, vol. 56, no. 11, pp. 5618–5629, 2008.

[32] Y. Huang, A. De Maio, and Z. S., *Semidefinite programming, matrix decomposition, and radar code design*. Cambridge University Press, 2009.

[33] C. Chen and P. P. Vaidyanathan, “MIMO radar waveform optimization with prior information of the extended target and clutter,” *IEEE Transactions on Signal Processing*, vol. 57, no. 9, pp. 3533–3544, 2009.

[34] J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan, and Y. Liu, “FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture,” *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17 430–17 438, 2021.

[35] N. K. D. Venkategowda and S. Werner, “Privacy-preserving distributed maximum consensus,” *IEEE Signal Processing Letters*, vol. 27, pp. 1839–1843, 2020.

[36] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[37] S. Serbetli and A. Yener, “Transceiver optimization for multiuser MIMO systems,” *IEEE Transactions on Signal Processing*, vol. 52, no. 1, pp. 214–226, 2004.

[38] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, “Distributed optimization and statistical learning via the alternating direction method of multipliers,” *Foundations and Trends® in Machine learning*, vol. 3, no. 1, pp. 1–122, 2011.

[39] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[40] B. Widrow and I. Kollár, *Quantization Noise: Roundoff Error in Digital Computation, Signal Processing, Control, and Communications*. Cambridge University Press, 2008.

[41] T. Kailath, A. H. Sayed, and B. Hasibi, *Linear Estimation*. Prentice Hall, New Jersey, 2000.

[42] M. Jahanbakht, W. Xiang, L. Hanzo, and M. Rahimi Azghadi, “Internet of underwater things and big marine data analytics—a comprehensive survey,” *IEEE Communications Surveys Tutorials*, vol. 23, no. 2, pp. 904–956, 2021.

[43] N. Cheng, S. Wu, X. Wang, Z. Yin, C. Li, W. Chen, and F. Chen, "AI for UAV-assisted IoT applications: A comprehensive review," *IEEE Internet of Things Journal*, pp. 1–1, 2023.