Arbitrarily Strong Utility-Privacy Trade-off in Decentralized Linear Estimation

Chong Xiao Wang, Student Member, IEEE, Yang Song, Wee Peng Tay, Senior Member, IEEE

Abstract—Each agent in a network makes a local observation that is linearly related to a set of public and private parameters. The agents send their observations to a fusion center to allow it to estimate the public parameters. To prevent leakage of the private parameters, each agent first sanitizes its local observation using a local privacy mechanism before transmitting it to the fusion center. We investigate the utility-privacy trade-off in terms of the Cramér-Rao lower bounds for estimating the public and private parameters. We study the class of privacy mechanisms given by linear compression and noise perturbation, and derive necessary and sufficient conditions for achieving arbitrarily strong utility-privacy trade-off in a decentralized agent network for both the cases where prior information is available and unavailable, respectively. We also provide a method to find the maximum estimation privacy achievable without compromising the utility and propose an alternating algorithm to optimize the utility-privacy trade-off in the case where arbitrarily strong utility-privacy trade-off is not achievable.

Index Terms—Estimation privacy, inference privacy, Cramér-Rao lower bound, decentralized network, multi-agent.

I. INTRODUCTION

The increasing number of multifarious sensing and monitoring applications installed in mobile phones, offices and public facilities has led to the proliferation of various services based on network data analytics [1]–[4]. Due to the limited data that a single sensor or agent can observe because of its geographical placement or location, agent type and computation capabilities, decentralized agent networks [5]–[13] are often deployed to overcome the insufficiency of data retrieved from a single agent. Agent fusion or sense-making is then used to combine the sensory data derived from disparate sources to reduce the inference uncertainty. However, aggregation of data poses a higher risk of privacy leakage. For example, social network users in a community may share their personal opinions or experiences about different products over time. While the aggregated data can be useful feedback for a company to improve its own product, with a database recording the preferences of each user for multiple products over a period of time, one can infer personal traits and other sensitive attributes like the gender and income level of a user. Furthermore, studies [14] have shown that information from a user’s friends on a social network can accurately reveal the user’s marital status, location, sexual orientation or political affiliation. Therefore, it is imperative that data from each source is sanitized to reduce privacy leakage before revealing it to the public.

In this paper, we consider a decentralized network where each source, node or agent (for convenience, we call this an agent throughout the paper) makes a noisy observation, which is linearly related to a set of system parameters. A set of public and private parameters are defined to be linear maps of the system parameters. We assume a decentralized\(^1\) estimation scheme is used where the agents send their observations to a fusion center to allow it to infer the public parameter with high fidelity [15]–[18]. The agents however want to keep the private parameters secret. To achieve this, each agent sanitizes its observation before sending to the fusion center. In this paper, we consider two sanitization methods: linear compression and noise perturbation. Since a trusted third-party who can help perturb the agent observations in a centralized manner does not exist or is impractical in many applications, a decentralized sanitization scheme is considered where each agent performs its local sanitization independently.

A. Related Work

We can classify privacy into two types: data privacy and inference privacy [19]–[22]. Data privacy often refers to protecting access to the raw data while inference privacy refers to the prevention of illegitimately inferring sensitive information [19], [23]. Homomorphic encryption is a classical method for data privacy [24]. However, such an approach is unable to hide the sensitive information contained in the encrypted data. Differential privacy [25], [26] ensures the indistinguishability of the query records in a database. However, differential privacy only deals with a source alphabet with finite support, and thus does not apply to the privacy in estimation theory. The other privacy metrics that have been extensively used in inference privacy include mutual information (entropy) privacy, average information leakage and maximum information leakage [27]. The privacy we consider in this paper belongs to the category of inference privacy.

Privacy-preserving estimation and detection from a single data source or agent has been well-studied by using information-theoretic approaches. The paper [28] presented an information-theoretic framework that ensures the utility of the

\(^1\)Following most of the literature, the term “decentralized” refers to the agents sending summation information instead of their raw observations to a fusion center.
data source while providing necessary privacy guarantees in a database associated with a statistical model. The following works are based on a general privacy statistical framework: Two random variables \( (X, Y) \) are assumed to be associated with a given joint distribution, and a user observes \( Y \) and wants to disclose to another user as much information about \( Y \) as possible while limiting the amount of information revealed about \( X \) [29]. To achieve that, the data is transformed before being disclosed, according to a probabilistic privacy mapping. The paper [23] introduced two privacy metrics, namely average information leakage and maximum information leakage, and showed that optimal privacy-accuracy trade-off can be cast as modified rate-distortion problems. In [30], [31], the authors formulated the privacy-utility trade-off in terms of the smallest normalized minimum mean-squared error. Furthermore, the references [32], [33] characterized the fundamental performance limits of privacy-ensuring mechanisms from an estimation theoretic perspective, and developed data-driven privacy mechanisms that provide estimation-theoretic guarantees [34]. The papers [35], [36] introduced a log-loss metric to measure privacy and utility and linked the privacy funnel method to the information bottleneck method [37]. In [38]–[41], the authors investigated the utility-privacy trade-off quantified by mutual information in smart metering using a rate-distortion approach. All the above-mentioned works only deal with single entry data and do not generalize immediately to the decentralized multi-agent setting. One of the underlying presumptions of these works is that a single user owns the data, while this paper considers the case where data is distributed among multiple users.

Several papers have addressed the issue of privacy protection under the hypothesis testing framework in a multi-agent system from different perspectives. The papers [42], [43] investigated the privacy leakage problem in an eavesdropped distributed hypothesis test network from the Bayesian detection perspective. Under a similar decentralized detection framework, the papers [19], [19]–[21] proposed a nonparametric learning approach to design local privacy mappings to distort each agent’s observation, thus preventing the fusion center from using its received information to accurately infer the private hypothesis. The paper [44] considered ways to achieve robust information privacy for a set of private hypotheses while [45] proposed a multi-layer agent network where non-linear fusion is applied. In contrast to these papers, which focus on the protection of a private hypothesis in a hypothesis testing framework, we consider in this paper the privacy protection of a set of parameters in a parameter estimation framework. An example is in the deployment of various body sensors (agents) for evaluating a user’s health condition [46]. With the raw observations sent from the sensors, a service provider can not only analyze the user’s health condition but can also infer some sensitive information about the user such as her location and personal preferences. Therefore, preserving the privacy of certain sensitive parameters associated with the sensor data is an important requirement.

The references [31], [38] proposed to add random noise to perturb raw measurements, while [47]–[53] investigated the use of compressive linear mappings that transform the raw measurements to a lower dimensional space. Preserving the privacy of individual entries of a database with constrained additive noise was considered in [54] where a measure of privacy using the Fisher information matrix [55] was developed. These works did not explore the connection between adding random noise and compressive linear transformations as privacy mechanisms. In this paper, one of our contributions is to clarify the relationship between these two mechanisms.

**B. Our Contributions**

In this paper, we consider the case where agents in a network send sanitized observations to a fusion center to allow it to infer a set of public parameters, while preventing it from estimating a set of private parameters better than a predefined accuracy. Our main contributions are the following:

1) We make explicit the relationship between additive random noise and linear compression as privacy mechanisms under the Cramér-Rao lower bound (CRLB) privacy framework. We show that the CRLBs for estimating the private parameters under the linear compression mechanism form the boundary of the set of CRLBs under noise perturbation.

2) We introduce the notion of arbitrarily strong utility-privacy trade-off, and derived necessary and sufficient conditions under which this is achievable. In addition, we propose a method to find the maximum privacy that can be attained while maintaining perfect utility under a constraint on the noise perturbation power.

3) In the case where arbitrarily strong utility-privacy trade-off is not achievable, we propose an alternating optimization algorithm to find a sanitization to achieve an optimal utility-privacy trade-off.

A preliminary version of this work was presented in [56] in which the noise perturbation method was used to protect the private parameters, while allowing the inference of the public parameters. The present paper delves into the analysis of the privacy and utility trade-off in decentralized agent networks and clarifies the relationship between noise perturbation and linear compression. New theoretical insights and methods are also presented.

The rest of this paper is organized as follows. In Section II, we present our problem formulation and assumptions. Arbitrarily strong utility-privacy trade-off and maximum privacy under perfect utility are investigated in Section IV. In Section V, we propose an alternating optimization method. In Section VI, we present numerical simulation results and conclude in Section VII.

**Notations:** We use \( \mathbb{R} \) to denote the set of real numbers, and \( \mathbb{S}_n^+ \), \( \mathbb{S}_n^{-} \) to denote the set of \( n \times n \) positive semi-definite matrices and positive definite matrices, respectively. We use \( \uparrow \) to represent matrix transpose. The notation \( \mathbf{0}_N \) is the \( N \times N \) zero matrix, and \( \mathbf{I}_N \) is an \( N \times N \) identity matrix. We write \( A \succeq B \) if \( A - B \) is positive semi-definite, while \( A \succ 0 \) means \( A \) is positive definite. We use \( \text{diag}(\cdot) \) to denote the block diagonal operation and \( \text{Tr}(\cdot) \) the trace operation. We use \( [P]_{P \times Q} \) to denote the sub-matrix of the matrix \( P \) consisting of the entries \( P(i, j) \) for all \( i, j \in P \times Q \) and use \( [P]_{-, Q} \) and
The observation model for agent $u$ each individual agent. to all agents' observations achieves a higher accuracy than from its local observation $y$. However, the agents also want to prevent the fusion $x$ based on its own observation $y_i$.

In this paper, we consider the case where the fusion center aims to estimate $u = Ux \in \mathbb{R}^U$, where $U \in \mathbb{R}^{U \times L}$ and $U > 0$, based on information it receives from all agents in the network. However, the agents also want to prevent the fusion center from inferring a set of private parameters $g_i = G_i x \in \mathbb{R}^{G_i}$, where $G_i \in \mathbb{R}^{G_i \times L}$, $i = 1, \ldots, S$. We assume that at least one $G_i$, $i = 1, \ldots, S$, is non-zero. Otherwise, our problem formulation reduces to the case without privacy consideration.

For example, if $U$ is the diagonal matrix with 1’s on the diagonal at the row indices in the index set $P \subset \{1, \ldots, L\}$ and zero everywhere else, then $u = [x]_P$ consists of the components of $x$ indexed by $P$ and we obtain the system formulation in [53].

Stacking up all agents’ measurements, we have

$$y = Hx + n,$$

where $H = [H_1, \ldots, H_S] ^\top \in \mathbb{R}^{N \times L}$, $n = [n_1, \ldots, n_S] ^\top \in \mathbb{R}^N$, and $N = \sum_{i=1}^S N_i$.

Let $S_k = \{\sum_{i=1}^{k-1} N_i + 1, \ldots, \sum_{i=1}^{k} N_i\}$ be the index set corresponding to agent $k$. Note that the measurement noise $n_i$ and $n_j$ for any two different agents $i$ and $j$ are not necessarily independent of each other. We assume that $n \sim \mathcal{N}(0, \Sigma)$, where the block diagonal part of $\Sigma$ is equal to $\text{diag}(\Sigma_1, \ldots, \Sigma_S)$ and the off-diagonal entries are the noise correlations between agents.

To protect the private parameters $\{g_i : i = 1, \ldots, S\}$ from being inferred by the fusion center based on the collective measurements, each agent sanitizes its local observation before transmitting to the fusion center. Let $T(y) = [T_1(y_1)^\top, \ldots, T_S(y_S)^\top]^\top$ denote the sanitized information received at the fusion center, where $T$ belongs to a predefined class of sanitization mechanisms. We measure the utility and privacy by the CRLBs for estimating the public parameter $u$ and private parameters $\{g_i : i = 1, \ldots, S\}$, respectively. Denoting the CRLBs of the system variable $x$ before sanitization as $P_x$ and after sanitization as $\tilde{P}_x$, the CRLBs for the public parameter $u$ before and after sanitization at the agents are

$$P_u = U_{u} P_{x} U_{u} ^\top,$$

$$\tilde{P}_u = U_{\tilde{u}} \tilde{P}_{\tilde{x}} U_{\tilde{u}} ^\top,$$

respectively. Similarly, the CRLBs for the private parameter $g_i$ before and after sanitization at the agents are

$$P_{g_i} = G_i P_x G_i ^\top,$$

$$\tilde{P}_{g_i} = G_i \tilde{P}_{\tilde{x}} G_i ^\top,$$

respectively.

The quantity $\text{Tr}(P_u)$ gives a lower bound for the sum error variance for estimating every component of $u$. For each sanitization function $T$, we define the system utility function for the public parameter $u$ as

$$u(T) = 1 - \frac{\text{Tr}(\tilde{P}_u)}{\text{Tr}(P_u)},$$

which is the negative of the percentage increase in sum error variance lower bound for estimating $u$ due to privacy sanitization. We define the system privacy function for the private parameter $g_i$, $i = 1, \ldots, S$, as

$$p_i(T) = \frac{\text{Tr}(\tilde{P}_{g_i})}{\text{Tr}(P_{g_i})} - 1,$$

which is the percentage increase in sum error variance lower bound for estimating $g_i$ due to privacy sanitization. Since $T$ can be viewed as part of the estimation procedure, we have $\tilde{P}_x \succeq P_x$. Therefore, $u(T) \leq 0$ and $p_i(T) \geq 0$ for all $T$. The utility and privacy functions as defined are thus intuitive: perturbation on the measurement decreases the utility and increases the privacy. Our goal is to

$$\max_T u(T),$$

s.t. $p_i(T) \geq \epsilon_i$, $i = 1, \ldots, S$,  

where $\epsilon_i \geq 0$ is called the privacy threshold for agent $i$. We summarize the notations introduced so far in Table I for the reader’s convenience.

### III. Decentralized Privacy-Preserving Transformation

In this section, we study two sanitization schemes $T$ that are widely used in the privacy literature: 1) linear compression that reduces the dimension of the measurements [49], and 2) noise perturbation that adds random noise to the measurements [40]. We derive the relationship between these two schemes under CRLB-based privacy criteria like that in (3). We show that the noise perturbation scheme is equivalent to linear compression in an asymptotic sense.

To prevent the fusion center or potential adversarial agents from inferring the set of private parameters $g_1, \ldots, g_S$ through the measurement $y$, we consider an affine transformation $T_i : [P]_Q$.
\(\mathbb{R}^N_i \rightarrow \mathbb{R}^M_i\) where \(M_i \leq N_i\) to sanitize the measurement of agent \(i\) to obtain:

\[
T_i(y_i) = C_i y_i + \xi_i = \tilde{H}_i x_i + \tilde{n}_i + \xi_i,
\]

where \(C_i \in \mathbb{R}^{M_i \times N_i}\) is the compression matrix and \(\xi_i \in \mathbb{R}^{M_i}\) is a perturbation noise with \(\xi_i \sim N(0, \Theta_i)\). We also have \(\tilde{H}_i = C_i H_i \in \mathbb{R}^{M_i \times L}\), \(\tilde{n}_i = C_i n_i \in \mathbb{R}^{M_i}\), and \(\tilde{\xi}_i \sim N(0, \Theta_i)\) with \(\tilde{\xi}_i = C_i \xi_i\). By collecting all the perturbed measurements, the measurement model at the fusion center can be summarized as follows:

\[
T(y) = C y + \xi = \tilde{H}_x x + \tilde{n} + \xi,
\]

where \(T(y) = [T_1(y_1)^T, \ldots, T_S(y_S)^T]^T \in \mathbb{R}^M\), \(\tilde{H} = CH\), \(M = \sum_{i=1}^{S} M_i\), \(\tilde{n} \sim N(0, \Theta)\) and \(\tilde{\xi} \sim N(0, \Theta)\). Note that the global sanitization function \(T\) is composed of independent local sanitization functions \(T_1, \ldots, T_S\), the \(i\)-th of which applies a local compression matrix \(C_i\) and additive noise \(\xi_i\) with covariance \(\Theta_i\), to the \(i\)-th agent’s measurement \(y_i\). Both the global compression matrix \(C\) and additive noise covariance matrix \(\Theta\) have block diagonal form. There is no message exchange between agents during the sanitization process as this is prone to privacy attacks.

From (2) and (3), we can express the utility and privacy function with respect to (w.r.t.) \(C\) and \(\Theta\) as

\[
u(C, \Theta) = 1 - \text{Tr}\left( U \tilde{P}_x(C, \Theta) U^T \right)/\text{Tr}(U P_x U^T),
\]

\[
p_i(C, \Theta) = \text{Tr}\left( G_i \tilde{P}_x(C, \Theta) G_i^T \right)/\text{Tr}(G_i P_x G_i^T) - 1,
\]

where

\[
\tilde{P}_x(C, \Theta) = \tilde{J}_x(C, \Theta)^{-1} = \left( J_0 + H^T C^T (CRC^T + \Theta)^{-1} C H \right)^{-1}.
\]

Here, \(J_0\) is the Fisher Information Matrix (FIM) of any prior information. We let \(J_0 = 0\), if no prior information is available. There is no loss in generality if we restrict compression matrices \(C_i\), to be square matrices, i.e., we consider \((C, \Theta)\) to be chosen from the following sanitization parameter set

\[
\mathcal{C} = \left\{ (C, \Theta) \mid C = \text{diag}(C_1, \ldots, C_S) \in \mathbb{R}^{N \times N}, \right.
\]

\[
\Theta = \text{diag}(\Theta_1, \ldots, \Theta_S), \quad C_i \in \mathbb{R}^{N_i \times N_i}, \Theta_i \in \mathbb{S}^{N_i}, i = 1, \ldots, S\}.
\]

This is because the perturbed CRLE remains unaltered by padding a non-square \(C\) and \(\Theta\) with zeroes: \(\tilde{J}_x(C, \Theta) = \tilde{J}_x(C, \Theta)\), where \(\tilde{C} = \begin{bmatrix} C & 0 \\ 0 & 0 \end{bmatrix}, \tilde{\Theta} = \begin{bmatrix} \Theta & 0 \\ 0 & 0 \end{bmatrix}\) and \(0\) and \(0^T\) are \((N - M) \times N\) and \(M \times (N - M)\) zero matrices respectively. In the following, we prove some properties of \(\tilde{J}_x(C, \Theta)\) with the domain \(\mathcal{C}\). We consider the metric spaces \(\mathbb{R}^{N \times N} \times \mathbb{S}^N\) and \(\mathbb{S}^L\) endowed with the Frobenius norm so that \(C\) is a subset of \(\mathbb{R}^{N \times N} \times \mathbb{S}^N\) and \(P_x(\cdot)\) is a mapping from \(\mathbb{R}^{N \times N} \times \mathbb{S}^N\) to \(\mathbb{S}^L\). Notions of metric properties like continuity are defined w.r.t. these metric spaces.

**Lemma 1.** Let \((C, \Theta) \in \mathcal{C}\), where \(C \in \mathbb{R}^{N \times N}\) and \(\Theta \in \mathbb{S}^{N \times N}\).

(i) \(\tilde{J}_x(C, \Theta)\) is a continuous function on \(\mathcal{C}\).

(ii) Suppose \(A\) is either a unitary matrix or an invertible block diagonal matrix. Then, we have \(\tilde{J}_x(AC, \Theta) = \tilde{J}_x(C, A^T \Theta A)\).

**Proof:** The first claim follows immediately from (6). For the second claim, suppose first that \(A\) is unitary. We then have

\[
\tilde{J}_x(AC, \Theta) = J_0 + H^T C^T (ACRC^T + \Theta)^{-1} C H
\]

\[
= J_0 + H^T C^T (CRC^T + \Theta)^{-1} C H
\]

\[
= \tilde{J}_x(C, A^T \Theta A).
\]

The proof for the case where \(A\) is an invertible block diagonal matrix is similar and the proof is complete.

**Proposition 1.**

(i) Let \(A = \begin{bmatrix} \tilde{J}_x(I_N, \Theta) : (I_N, \Theta) \end{bmatrix} \in \mathcal{C}\)

and \(B = \begin{bmatrix} \tilde{J}_x(C, \Theta) : (C, \Theta) \end{bmatrix} \in \mathcal{C}\). Then, \(B \backslash A\) is the boundary of \(A\).

(ii) For any \((C, \Theta) \in \mathcal{C}\), there exists \((C', A_b) \in \mathcal{C}\), where \(A_b\) is a diagonal matrix with \([A_b]_{i,i} \in \{0, 1\}\), for all \(i \geq 1\), such that

\[
\tilde{P}_x(C', A_b) = \tilde{P}_x(C, \Theta).
\]

**Proof:**
(i) Since \( A \subset B \), it suffices to show that for any \( B \in \mathbb{B} \), there exists a sequence in \( A \) that converges to \( B \). From Lemma 1(ii), we have \( \tilde{J}_x(C, \Theta) = \tilde{J}_x(I_N, C^T \Theta C) \) with \( \tilde{J}_x(I_N, C^T \Theta C) \in A \) if \( C \) is invertible. On the other hand, if \( C \) is a singular matrix, we let the eigendecomposition of \( C = QAQ^{-1} \), where \( Q \) is the square matrix whose columns are the eigenvector, and \( A \) is the diagonal matrix whose diagonal elements are the corresponding eigenvalues. Denote \( A = \text{diag}(A', 0_A) \) with \( A' \) containing all the non-zero eigenvalues and an appropriate \( A \). From Lemma 1(ii), we have

\[
\tilde{J}_x(C, \Theta) = \tilde{J}_x(QAQ^{-1}, \Theta) = \tilde{J}_x(AQ^{-1}, \Theta'),
\]

where \( \Theta' = Q^T \Theta Q \). For any \( \lambda > 0 \), let \( A_\lambda = \text{diag}(\lambda A', 0_A) \), which is an invertible diagonal matrix. From Lemma 1(ii), we have

\[
\tilde{J}_x(A_\lambda Q^{-1}, \Theta') = \tilde{J}_x(I_N, (A_\lambda Q^{-1})^T \Theta' A_\lambda Q^{-1}) \in A,
\]

whose left-hand side converges to the right-hand side of (8) as \( \lambda \to 0 \) since \( \tilde{J}_x \) is continuous by Lemma 1(i). The proof is now complete.

(ii) Let the eigendecomposition of \( \Theta = QAQ^T \). The diagonal matrix \( A \) can be written as \( A_+^{1/2} A_0 A_+^{1/2} \), where \( A_+ \) and \( A_0 \) are diagonal matrices with \( [A_+]_{i,i} = [A_0]_{i,i} \), \( [A_+]_{i,i} = 1 \) when \( [A_0]_{i,i} > 0 \), and \( [A_+]_{i,i} = 1 \), \( [A_0]_{i,i} = 0 \) when \( [A_0]_{i,i} = 0 \). Two applications of Lemma 1(ii) gives us \( \tilde{J}_x(C, \Theta) = \tilde{J}_x(C', A_0) \), where \( C' = A_+^{1/2} Q^T C \) is a block diagonal matrix since \( Q \). \( A_+ \) and \( A_0 \) are all block diagonal matrices. Thus \( (C', A_0) \in C \) and the claim follows.

Proposition 1(ii) shows that the power of the additive noise can be normalized by the compression matrix when sanitizing the data. On the other hand, Proposition 1(i) shows that adding only noise can approximate linear compression arbitrarily well in terms of the estimation error covariance, but this requires arbitrarily large noise power. Therefore, perturbation noise by itself cannot replace linear compression in a practical system. Without loss of generality, we set the compression matrix \( C = I_N \) in the sequel as we can always normalize the noise by a compression matrix to obtain the same utility and privacy trade-off. We now rewrite the optimization problem (P0) as

\[
\begin{align*}
\max_{(I_N, \Theta) \in C} u(I_N, \Theta),
\text{s.t. } & p_i(I_N, \Theta) \geq \epsilon_i, i = 1, \ldots, S. \quad (P1)
\end{align*}
\]

Note that for (P1) to be feasible when \( J_0 \neq 0_L \), the privacy threshold \( \epsilon_i \) should satisfy \( \epsilon_i \leq \epsilon_i^{\text{max}} \), where

\[
\epsilon_i^{\text{max}} = \text{Tr} \left( G_i J_0^{-1} G_i^T \right) / \text{Tr} \left( G_i P_x G_i^T \right) - 1,
\]

for \( G_i \neq 0 \), and \( \epsilon_i^{\text{max}} = 0 \) if \( G_i = 0 \). This is because the prior information (as quantified by its FIM \( J_0 \)) already leaks privacy and any sanitization cannot achieve a higher level of privacy than this. When \( J_0 = 0_L \), we have \( \epsilon_i^{\text{max}} = \infty \) if \( G_i \neq 0 \) and \( 0 \) otherwise.

The following useful expressions can be derived by using the binomial inverse theorem and Woodbury matrix identity (see Appendix A for details).

1. No prior information, i.e., \( J_0 = 0_L \), we have

\[
\tilde{P}_x(I_N, \Theta) = P_x + \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^T,
\]

where \( \Phi = R^{-1} - R^{-1} H P_x H^T R^{-1} \) is a degenerate matrix and \( \Psi = P_x H^T R^{-1} \).

2. With prior information, i.e., \( J_0 > 0_L \), we have

\[
\tilde{P}_x(I_N, \Theta) = P_0 - P_0 H^T (\Phi^{-1} + \Theta)^{-1} H P_0
\]

\[
= P_x + \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^T,
\]

where \( P_0 = J_0^{-1} \), \( \Phi = (H P_0 H^T + R)^{-1} \), and \( \Psi = P^0 H^T \Phi \).

By considering the observation model \( y = H x + n, \Psi \) in (9) is the same as the minimum mean square error estimation matrix. By regarding \( P_0 \) as the predicted estimate covariance, \( \Psi \) and \( \Phi^{-1} \) in (11) are equivalent to the Kalman gain and innovation covariance, respectively. The equations (9) and (11) under both the cases where prior information is available and unavailable have meaningful interpretations: the first term of both equations is the CRLB without perturbation while the second term is the increased CRLB caused by noise perturbation.

IV. ARBITRARILY STRONG PRIVACY WITH PERFECT UTILITY

In this section, we derive necessary and sufficient conditions for achieving perfect utility and arbitrarily strong privacy when prior information is available and unavailable, respectively. Furthermore, we formulate the problem of achieving maximal privacy under perfect utility as a linear matrix inequality optimization.

**Definition 1.** We say that arbitrarily strong utility-privacy trade-off (ASUP) is achievable if for any non-negative \( \epsilon_i \leq \epsilon_i^{\text{max}}, i = 1, \ldots, S \), there exists \( (C, \Theta) \in C \) such that \( u(C, \Theta) < 0 \) and \( p_i(C, \Theta) \geq \epsilon_i \) for all \( i = 1, \ldots, S \).

While achieving perfect utility (by taking \( T \) to be \( (I_N, 0_N) \)) and arbitrarily strong privacy (by taking \( T \) to be \( (0_N, 0_N) \)) are easy, achieving both at the same time is difficult or infeasible. Therefore, it is of interest to know when ASUP is achievable. In the following, we derive necessary and sufficient conditions for ASUP under both the cases where prior information is available and unavailable.

A. **Achieving ASUP**

We provide necessary and sufficient conditions to achieve ASUP in Theorem 1 for the case \( J_0 = 0_L \), and in Theorem 2 for the case \( J_0 > 0_L \). Moreover, we provide a method to construct the noise covariance to achieve ASUP inside the proofs (if ASUP is feasible). We start with the following two preliminary lemmas.

**Lemma 2.** For matrices \( A \in \mathbb{R}^{M \times N}, B \in \mathbb{S}^N \) and a sequence of pairwise commuting matrices \( (S_n)_{n \geq 1} \) where each \( S_n \in \mathbb{S}^N_+ \), we have

\[
\lim_{n \to \infty} \text{Tr} \left( A (S_n + B)^{-1} A^T \right) = 0,
\]
if and only if
\[ \lim_{n \to \infty} \text{Tr} \left( A S_n^{-1} A^T \right) = 0. \]

Proof: See Appendix B.

Lemma 3. For matrices \( A \in \mathbb{R}^{M_1 \times N} \) and \( B \in \mathbb{R}^{M_2 \times N} \) such that \( M_1, M_2 \leq N \), there exists \( S \in \mathbb{S}^N \) such that \( \text{Tr}(A S A^T) = 0 \) and
\[ \lim_{n \to \infty} \text{Tr} \left( B \left( nS + \frac{1}{n}I_N \right)^{-1} B^T \right) = 0, \]
if and only if \( AB^T = 0 \).

Proof: See Appendix C.

Theorem 1. Suppose \( J_0 = 0_L \). Recall \( \Psi \) and \( \Phi \) as defined after (9). For \( k \in \{1, \ldots, S\} \), let \( \Xi_k = \left[ U[\Psi]_{i, s_k} \right]_{[\Phi]_{s_k, s_k}} \). There exists \( \Theta \in \mathbb{S}^N \) such that ASUP is achievable if and only if there exists at least an agent \( k \in \{1, \ldots, S\} \) such that

(i) \( N_k > \text{rank}(\Xi_k) \),
(ii) there does not exist any matrix \( P \) such that \( P \Xi_k = G_j[\Psi]_{j, s_k} \), \( \forall j = 1, \ldots, S \).

Proof: Note that condition (i) is equivalent to
\[ \text{Null} \left( [\Phi]_{s_k, s_k} \right) \cap \text{Null} \left( U[\Psi]_{i, s_k} \right) \neq \{0\}, \]
and condition (ii) is equivalent to
\[ \text{Null} \left( [\Phi]_{s_k, s_k} \right) \cap \text{Null} \left( U[\Psi]_{i, s_k} \right) \not\subseteq \text{Null} \left( G_j[\Psi]_{j, s_k} \right), \forall j = 1, \ldots, S. \]

We first show the necessity of conditions (i) and (ii). From (2) and (9), perfect utility \( u(I_N, \Theta) = 0 \) is obtained only if
\[ \text{Tr} \left( U[\Psi] (I_N + \Theta \Phi)^{-1} \Theta \Phi^T U^T \right) = 0. \]

Since the left-hand side (LHS) of the above equation is a continuous function \( \text{w.r.t.} \ \Theta \), the above equation can be expressed as
\[ \lim_{n \to \infty} \text{Tr} \left( U[\Psi] \left( \Theta + \frac{1}{n}I_N \right)^{-1} \Theta \Phi \Phi^T U^T \right) = 0. \]

From Lemma 2, this is equivalent to
\[ \lim_{n \to \infty} \text{Tr} \left( U[\Psi] (\Theta + \frac{1}{n}I_N)^{-1} \Psi^T U^T \right) = 0, \]
or
\[ \text{Tr} \left( U[\Psi] \Theta \Psi^T U^T \right) = 0. \]

Therefore, \( u(I_N, \Theta) = 0 \) only if \( U[\Psi] \Theta = 0 \). Following that, \( U[\Psi]_{i, s_k} \Theta = 0, \forall i = 1, \ldots, S \) since \( \Theta = \text{diag}(\Theta_1, \ldots, \Theta_S) \). From the rank-nullity theorem, this implies that \( \Theta_i = 0_{N_i} \) for an agent \( i \) with rank \( U[\Psi]_{i, s_k} = N_i \). Since at least one \( G_i \neq 0 \) for \( i = 1, \ldots, S \), to achieve any level of privacy, there must exist at least an agent \( k \) with rank \( U[\Psi]_{i, s_k} < N_k \) with \( U[\Psi]_{i, s_k} \) having a non-trivial null space. Let \( \Theta \) be such that \( \Theta_k \neq 0_{N_k} \) and
\[ U[\Psi]_{i, s_k} \Theta_k = 0. \]

Since \( p_j(I_N, \Theta) \) is a non-decreasing function \( \text{w.r.t.} \ \Theta \), arbitrarily strong privacy is achieved only if for all \( j = 1, \ldots, S \),
\[ \lim_{n \to \infty} p_j(I_N, n\Theta) = \infty. \]

From (3) and (9), the LHS of the above statement (15) is equivalent to
\[ \lim_{n \to \infty} \text{Tr} \left( G_j[\Psi] (I_N + n\Theta \Phi)^{-1} n\Theta \Psi \Psi^T G_j^T \right) = \lim_{n \to \infty} \text{Tr} \left( G_j[\Psi] \left( \left( n\Theta + \frac{1}{n}I_N \right)^{-1} + \Phi \right)^{-1} \Psi \Psi^T G_j^T \right) = \lim_{n \to \infty} \sum_{i=1}^{N} \alpha_i(n, j) \lambda_i(n), \]
where
\[ T(n) = \left( \left( n\Theta + \frac{1}{n}I_N \right)^{-1} + \Phi \right)^{-1}, \lambda_i(n) \] is the \( i \)-th eigenvalue of \( T(n) \) with \( v_i(n) \) being the corresponding unit eigenvector, and \( \alpha_i(n, j) = \| G_j[\Psi] v_i(n) \|^2 \). Therefore, (15) holds only if for each \( j = 1, \ldots, S \), there exists an index \( i_j \) such that \( n \to \infty \lambda_i(n) = \infty \) with corresponding eigenvectors \( v_i(n) \notin \text{Null}(G_j[\Psi]) \). Since \( G_j[\Psi] \) has finite rank, by passing to a subsequence if necessary, there exists a unit vector \( w_j \notin \text{Null}(G_j[\Psi]) \) such that
\[ \lim_{n \to \infty} w_j^T (T(n))^{-1} w_j = 0. \]

We then have
\[ \lim_{n \to \infty} w_j^T \left( n\Theta + \frac{1}{n}I_N \right)^{-1} w_j = 0, \]
\[ w_j^T \Phi w_j = 0. \]

Since \( \Theta_k \neq 0_{N_k} \), (16) holds only if \( w_j^\prime = [w_j]_{s_k} \notin \text{Null}(G_j[\Psi]) \), \( w_j^\prime = 0 \), such that
\[ \lim_{n \to \infty} w_j^\prime T \left( n\Theta_k + \frac{1}{n}I_N \right)^{-1} w_j^\prime = 0, \]
\[ \left[ \Phi \right]_{s_k, s_k} w_j^\prime = 0. \]

From Lemma 3, both (14) and (17) hold only if \( w_j^\prime \in \text{Null}(U[\Psi]_{i, s_k}) \). Therefore, conditions (i) and (ii) are necessary for ASUP.

We next prove sufficiency by constructing a \( \Theta_k \) that yields ASUP as illustrated in Fig. 1. For any \( \epsilon_j = 1 \), choose an eigenvalue \( \lambda_j \) of \( \Theta_k \) to be arbitrarily large and its corresponding eigenvector \( v_j \) to satisfy
\begin{align*}
(a) & \ v_j \in \text{Null}(\left[ \Phi \right]_{s_k, s_k}), \\
(b) & \ v_j \in \text{Null}(U[\Psi]_{i, s_k}), \\
(c) & \ v_j \notin \text{Null}(G_j[\Psi]_{j, s_k}), \forall j = 1, \ldots, S. 
\end{align*}

The existence of \( v_j \) is guaranteed by condition i and ii (it may not be unique). Let \( \Theta_i = 0_{s_i} \) for all \( i \neq k \). By reversing the arguments used in the necessity proof, it can be verified
that such $\Theta = \text{diag}(\Theta_1, \ldots, \Theta_S)$ leads to ASUP. The proof is now complete.

Theorem 1 implies that ASUP is achievable when $J_0 \succ 0_L$ as long as one agent in the network satisfies certain conditions. As an illustration, consider the special case $H \in \mathbb{R}^{L \times L}$, where $\Psi$ turns out to be $H^{-1}$ and $\Phi$ becomes $0_N$. Then from (9), the perturbed CRLB for estimating $x$ can be written as

$$\mathbf{P}_x(I_N, \Theta) = \mathbf{P}_x + H^{-1}\Theta(H^\top)^{-1}$$

$$= \mathbf{P}_x + \sum_{i=1}^S \left[H^{-1}\right]_{S_i} \Theta_i \left[(H^\top)^{-1}\right]_{S_i}^\top,$$

which is linear in the perturbation noise covariance $\Theta_i$ of each agent $i$. Recall that $u = Ux$ and $g_i = G_i x$. It can be seen that if there is one row in $U \left[H^{-1}\right]_{S_i}$ not in the row space of $G_i \left[H^{-1}\right]_{S_i}$, agent $i$ can use arbitrarily large noise power in the corresponding row of $\Theta_i$, so that the estimation error of $g_i$ becomes arbitrarily large while the estimation error of $u$ remains unchanged. Theorem 1 generalizes this result to any $H$.

**Theorem 2.** Suppose $J_0 \succ 0_L$. ASUP is achievable if and only if

$$U \left[\Psi_{i, S_i} \mid H_{S_i} \right] G^\top = 0,$$

(19)

for every agent $i = 1, \ldots, S$, where $G = [G_1^\top, \ldots, G_S^\top]^\top \in \mathbb{R}^{G \times L}$.

**Proof:** From (11), perfect utility $u(I_N, \Theta) = 0$ requires

$$\text{Tr} \left(U \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^\top U^\top \right) = 0.$$

Applying Lemma 2 and the same argument in the proof of Theorem 1, the above statement holds if and only if

$$\text{Tr} \left(U \Psi \Theta \Psi^\top U^\top \right) = 0.$$

(20)

Arbitrarily strong privacy requires the existence of $\Theta$ such that

$$\lim_{n \to \infty} p_j(I_N, n\Theta) = c_j^{\text{max}}, \quad \forall j = 1, \ldots, S,$$

From (10), the above equation can be written as

$$\lim_{n \to \infty} \text{Tr} \left(\mathbf{G}^\top \mathbf{H}^{-1} + n\Theta + \frac{1}{n} I_N \right)^{-1} \mathbf{H}^\top \mathbf{G}^\top = 0.$$

Since the LHS of the above statement is a continuous function w.r.t. $\Theta$, it is equivalent to

$$\lim_{n \to \infty} \text{Tr} \left(\mathbf{G}^\top \mathbf{H}^{-1} + \frac{1}{n} I_N \right)^{-1} \mathbf{H}^\top \mathbf{G}^\top = 0.$$

From Lemma 2, we have equivalently,

$$\lim_{n \to \infty} \text{Tr} \left(\mathbf{G}^\top \mathbf{H}^{-1} \left(n\Theta + \frac{1}{n} I_N \right)^{-1} \mathbf{H}^\top \mathbf{G}^\top \right) = 0.$$

(21)

Rewriting the perfect utility condition (20) and the arbitrarily strong privacy condition (21) in terms of $\Theta_i$, $i = 1, \ldots, S$, yields

$$\sum_{i=1}^S \text{Tr} \left(U \left[\Psi_i_{S_i} \mid \Theta_i \right] \Psi_i^\top U^\top \right) = 0,$$

$$\lim_{n \to \infty} \sum_{i=1}^S \text{Tr} \left(\mathbf{G}^\top \mathbf{H}^\top \left(n\Theta_i + \frac{1}{n} I_N \right)^{-1} \mathbf{H}^\top \mathbf{G}^\top \right) = 0.$$

The proof of necessity now follows by applying Lemma 3 to the above statements. To show sufficiency, we can follow the method in Appendix C to construct $\Theta$ as illustrated in Fig. 2. The theorem is now proved.

---

**Fig. 1.** ASUP sanitization flowchart when $J_0 = 0_L$. Agent $k$ chooses a basis of the row space of $U \left[\Psi \mid \cdot \right]_{S_k}$, denoted as $\mathcal{V}_k$.

Agent $k$ chooses a vector $v$ from $\mathcal{V}$ such that $v \notin \text{Null} (G \mid \Psi, \cdot)$.

Agent $k$ chooses $v$ as one of the eigenvector of $\Theta_k$ and its corresponding eigenvalue to be sufficiently large and let the other eigenvalues be 0.

Agent $k$ generates a noise $\xi_k \sim \mathcal{N}(0, \Theta_k)$ and add the noise to its measurement.

---

**Fig. 2.** ASUP sanitization flowchart when $J_0 \succ 0_L$.

Agent $k$ chooses a basis of the row space of $U \left[\Psi \mid \cdot \right]_{S_k}$, denoted as $\mathcal{V}_k$.

Agent $k$ chooses a basis of the row space of $\mathbf{G} \left[P_0 \mid \mathbf{H}^\top \right]_{S_k}$, denoted as $\mathcal{V}_k$.

Agent $k$ chooses $\mathcal{V}_1$ and $\mathcal{V}_2$ as the eigenvectors of $\Theta_k$ and their corresponding eigenvalues be sufficiently large and 0, respectively, and let the other eigenvalues be 0.

Agent $k$ generates a noise $\xi_k \sim \mathcal{N}(0, \Theta_k)$ and add the noise to its measurement.

Note that $\Psi \mathbf{H}^\top \mathbf{P}_0$ is the reduced estimate covariance for $x$ w.r.t. the prior estimate covariance $\mathbf{P}_0$ after agents observe $y$. We may consider $\left[\Psi \mid \cdot \right]_{S_k} \mathbf{H}^\top \mathbf{P}_0$ in condition (19) as the reduced estimate covariance for agent $i$ to observe $y_i$. Theorem 2 gives the condition for each agent $i = 1, \ldots, S$, to be able to decrease this reduced estimate covariance to its minimum for the private parameter $g_i = G_i x$ without affecting the reduced estimate covariance for the public parameter $u = Ux$.

We note that the privacy function is bounded when $J_0 \succ 0_L$ because $J_0 \succ 0_L$ provides prior information about every
The achievable privacy is the cumulative result of the noise perturbation applied by each agent. Since the privacy contributed by each agent is bounded when \( J_0 > 0_L \), the maximum privacy is only obtained when all the agents offer their maximum privacy. This is different from the case \( J_0 = 0_L \), where the privacy each agent can contribute is unbounded. Therefore, we can rely on one agent to provide arbitrarily strong privacy in Theorem 1. This explains why \( \text{ASUP} \) for \( J_0 = 0_L \) requires only one agent while \( \text{ASUP} \) for \( J_0 > 0_L \) requires every agent. In the case where only a set of agents satisfy the condition given in Theorem 2 when \( J_0 > 0_L \), we still can apply the sanitization method in Fig. 2 to these nodes. However, as a consequence, we will obtain perfect utility but not arbitrarily strong privacy. In what follows we give an example in which condition (19) in Theorem 2 holds.

**Example 1.** Suppose \( [H]_{S:\gamma} = H_0 \in \mathbb{R}^{(N/S) \times L} \), for all \( i = 1, \ldots, S \), and the measurement noise is white, i.e., \( R = \sigma^2 I_N \). In this case, we can verify that for some \( \Psi_0 \in \mathbb{R}^{N \times (N/S)} \), \( [\Psi]_{S:\gamma} = \Psi_0 \), for all \( i = 1, \ldots, S \). When \( U\Psi_0 H_0 P_0 G^\top = 0 \), condition (19) is satisfied. Note that \( \Psi_0 H_0 P_0 \) is the reduced estimate covariance of \( \mathbf{x} \) after agent \( i \) observes \( y_i \). Following that, \( U\Psi_0 H_0 P_0 G^\top \) can be interpreted as the reduced estimate cross-covariance between the public parameter \( \mathbf{u} \) and the private parameters \( \mathbf{g}_1, \ldots, \mathbf{g}_S \), which need to be uncorrelated to make ASUP feasible.

**B. Maximum privacy under perfect utility**

When discussing ASUP, we allow the power of the perturbation noise to be arbitrarily large so that the privacy function can exceed arbitrarily large privacy thresholds. In most practical applications, there is a power constraint on the perturbation noise that can be added (if we normalize the noise as discussed immediately before (P1), this translates into a constraint on the dynamic range of the compression mechanism.). We consider the following optimization:

\[
\max_{(I_N, \Theta) \in \mathcal{C}} \sum_{i=1}^S p_i(I_N, \Theta), \quad \text{s.t.} \quad u(I_N, \Theta) = 0, \quad \text{Tr} (\Theta_i) \leq \delta_i, \quad \text{for} \quad i = 1, \ldots, S,
\]

where \( \delta_i > 0 \) is the maximum total power available to agent \( i \). In the following, we show how to reformulate (22) as a convex optimization problem with linear matrix inequality (LMI) constraints.

Recall from Theorems 1 and 2 that \( u(I_N, \Theta) = 0 \) (perfect utility) under both the cases \( J_0 = 0_L \) and \( J_0 > 0_L \) is achievable if and only if

\[
\text{Tr} (U\Psi_0 \Theta \Psi^\top U^\top) = 0.
\]

By introducing an auxiliary variable \( Z \in \mathbb{R}^L \), (22) can be cast as

\[
\max_{(I_N, \Theta) \in \mathcal{C}} \sum_{i=1}^S p_i(I_N, \Theta), \quad \text{s.t.} \quad Z \leq P_x(I_N, \Theta), \quad \text{Tr} (U\Psi_0 \Theta \Psi^\top U^\top) = 0, \quad \text{diag} \left( \left( \text{Tr} (\Theta_i) \right)^2 \right) \leq \text{diag} \left( \left( \delta_i \right)^2 \right).
\]

Note that the maximization will force \( Z \) to achieve its upper bound.

In the case \( J_0 = 0_L \), we need the following form of the perturbed CRLB before transforming the first constraint of (23) into a LMI. Let the column vectors of \( \tilde{H} \) be a basis of \( \text{Null} (H^\top) \) and let \( K = [K_1^\top, K_2^\top]^\top = [H, \tilde{H}]^{-1} \) with \( K_1 \in \mathbb{R}^{L \times N} \). We obtain from (6)

\[
\tilde{P}_x(I_N, \Theta) = \left( H^\top (R + \Theta)^{-1} H \right)^{-1}
\]

\[
= \left( \left( K^\top \right)^{-1} \left( R + \Theta \right)^{-1} K \right)_{\mathcal{L}, \mathcal{L}}^{-1}
\]

\[
= \left( \left( K(R + \Theta)K^\top \right)_{\mathcal{L}, \mathcal{L}} \right)^{-1}
\]

\[
= K_1 \tilde{\Theta} K_1^\top - K_1 \tilde{\Theta} K_2 \left( K_2 \tilde{\Theta} K_2^\top \right)^{-1} K_2 \tilde{\Theta} K_1^\top,
\]

where \( \tilde{\Theta} = R + \Theta \), \( \mathcal{L} = \{1, \ldots, L\} \) and the last equation is a consequence of the block matrix inversion. Substituting the above expression into the first constraint of (23) and using the Schur complement, the constraint can be cast as the following LMI:

\[
\begin{bmatrix}
K_1(\Theta + R)K_1^\top & K_1(\Theta + R)K_2^\top \\
K_2(\Theta + R)K_1^\top & K_2(\Theta + R)K_2^\top
\end{bmatrix}
+ \begin{bmatrix}
Z & 0 \\
0 & 0_{N-L}
\end{bmatrix}
\succeq 0_N.
\]

Similarly, in the case \( J_0 > 0_L \), by substituting (10) into the first constraint of (23), it can be linearized as

\[
\begin{bmatrix}
P_0 - Z & P_0 H^\top \\
HP_0 & \Phi^{-1} + \Theta
\end{bmatrix}
\succeq 0_{N+L}.
\]

The above formulations can then be solved by using standard semi-definite programming techniques [57].

![Fig. 3. Sanitization procedure.](image-url)

Together with the results in Theorems 1 and 2, one may proceed to design the sanitization mechanism at each agent as illustrated in Fig. 3: one first checks if the necessary and sufficient conditions for achieving ASUP are satisfied. If so and if there is no power constraint, we can use the steps outlined in Figs. 1 and 2 to choose the sanitization mappings.
If there is a power constraint, we solve (23). On the other hand, if ASUP is not achievable, we propose an alternating optimization procedure to solve (P1) in the following section.

V. ALTERNATING OPTIMIZATION

In this section, we propose an algorithm to solve (P1) for both the cases where information is available and unavailable. Because $\Theta$ is restricted to be a block diagonal matrix and the utility and privacy functions are non-linear w.r.t. $\Theta$, it is difficult to directly solve the optimization problem (P1) using standard optimization tools. We propose to optimize (P1) w.r.t. $\Theta_1, \ldots, \Theta_S$, sequentially and in an alternating fashion, instead of $\Theta$. We show that optimizing (P1) over $\Theta_i$ is a convex problem, which can be solved by semi-definite programming [57].

To proceed, we need to do a trivial relaxation by assuming $\Theta$ is invertible. Then both the perturbed CRLBs when $J_0 = 0_L$ and $J_0 > 0_L$ in (9) and (11) can be written as

$$
\tilde{P}_x(I_N, \Theta) = P_x + \Psi (\Theta^{-1} + \Phi)^{-1} \Psi^T,
$$

where $\Psi$ and $\Phi$ refer to their respective definitions when prior information is available or unavailable. Therefore, the optimization procedure to solve (P1) in the following section.

Both the cases where information is available and unavailable.

We propose to optimize (P1) w.r.t. $\Theta_i, \ldots, \Theta_S$, sequentially and in an alternating fashion, instead of $\Theta$. We show that optimizing (P1) over $\Theta_i$ is a convex problem, which can be solved by semi-definite programming [57].

At the $i$-th sequence, we treat $\Theta_i$ as a constant and optimize (P1) over $\Theta_i$. This optimization problem can be formulated as

$$
\max_u u(\Theta_i) \\
\text{s.t. } p_j(\Theta_i) \geq \epsilon_j, \forall j = 1, \ldots, S,
$$

which can be re-cast as a semidefinite programming problem by introducing $Z = (\Theta_i + \Omega)^{-1}$ to obtain:

$$
\min_{Z} \frac{\tr (\Gamma \cdot Z)}{Z} \\
\text{s.t. } \tr (\Gamma_j \cdot Z) \geq \epsilon_j', \forall j = 1, \ldots, S,
$$

where $\epsilon'_j = (\epsilon_j - \Delta_{pj}) \cdot \tr (G_j P_x G_j^T) - \Delta_{pj}$.

We propose to optimize (P1) over $\Theta_i, \ldots, \Theta_S$ sequentially over multiple iterations. The algorithm is summarized in Algorithm 1.

Algorithm 1 Alternating optimization

Initialize: $\Theta_i^0 = 0_{N_i}, i = 1, \ldots, S$ at iteration 0.

Output: $\Theta^k$, $i = 1, \ldots, S$ at iteration $k$.

1: while $k \leq \text{Max. number of iterations}$ do
2: for $i = 1$ to $S$ do
3: Compute $\epsilon'_j, \Gamma_u$ and $\Gamma_{pj}$ for all $j = 1, \ldots, S$.
4: Solve (P2) to obtain $\Theta_i^k$
5: Use $\Theta_i^k$ to update $\Theta_{i+1}^k, \ldots, \Theta_S^k$.
6: end for
7: end while

VI. NUMERICAL RESULTS

In the section, we investigate the impact of different parameters on the maximum privacy attainable under perfect
utility discussed in Section IV and verify the performance of Algorithm 1 proposed in Section V. The settings used for the simulations in this section are given in Table II unless otherwise stated. We do not impose the noise power constraint when retrieving the maximum privacy under perfect utility. Each data point shown in the figures is averaged over 100 independent experiments.

A. Maximum privacy under perfect utility

![Graph](image)

Fig. 4. The maximum privacy under perfect utility when no prior information is available. Because the maximum privacy can be unbounded, it is truncated when exceeding 100.

![Graph](image)

Fig. 5. The maximum privacy under perfect utility when prior information is available. The privacy at S = 0 stands for the maximum privacy threshold.

We vary the number S of the agents and the length U of the public parameter vector to investigate the impact of these parameters on the maximum privacy attainable under perfect utility. Recall that \( \epsilon_1^{\text{max}} = \infty \) when \( J_0 = 0_L \) while \( \epsilon_1^{\text{max}} \) is bounded when \( J_0 > 0_L \). From Fig. 4 with \( J_0 = 0_L \), it can be seen that the maximum privacy under perfect utility goes to infinity (ASUP is achieved) when \( S = 1 \). By examining the necessary and sufficient conditions for ASUP in Theorem 1, it is observed that a system with a smaller number of agents \( S \) is more likely to fulfill the ASUP conditions than a system with a larger \( S \) with all the other settings remaining the same. In Fig. 5 with \( J_0 > 0_L \), none of the maximum privacy obtained under perfect utility when \( S = 1, 2, 3, 4 \) is close to \( \epsilon_1^{\text{max}} \) (ASUP is not achieved). This can be elucidated from Theorem 2, where every agent is required to satisfy certain orthogonality conditions for ASUP to be achievable. Thus it is unlikely to generate a random system model to achieve ASUP. Furthermore, both Figs. 4 and 5 demonstrate a descending trend for the maximum privacy achievable as the number of agents \( S \) increases or the length of the public parameter vector \( u \) increases. To expound further on this, recall from Theorems 1 and 2 that perfect utility is achieved if and only if

\[
\text{Tr} \left( \sum_{i=1}^{S} U_i [\Psi_i], S_i \Theta_i [\Psi_i^\top U_i^\top] \right) = 0.
\]

Therefore, to obtain \( u (I_N, \Theta) = 0 \), a larger \( S \) or \( U \) is likely to force more agents to have \( \Theta_i = \Theta_U \). Thus a system with a larger \( S \) or \( U \) has less degrees-of-freedom for privacy perturbation when maintaining perfect utility compared to a system with a smaller \( S \) or \( U \).

B. Alternating optimization

By varying \( S \) and the privacy threshold \( \epsilon_1 \), Fig. 6 demonstrates the utility and privacy trade-off by using Algorithm 1 proposed in Section V. It is observed that the utility decreases as the privacy increases. Under the same setting, a larger number of agents deteriorates the utility. This is because each agent contains less measurements, thus giving less degrees-of-freedom for the optimization and leading to smaller utility. Furthermore, it can be seen that the optimal utility obtained by the algorithm is close to perfect utility when the privacy threshold \( \epsilon_1 \) is set to be less than the maximum privacy obtained under perfect utility. This implies that the algorithm proposed in Section V approximates the optimal solution well. Fig. 7 shows the convergence of the algorithm.

![Graph](image)

Fig. 6. The privacy and utility trade-off when \( S = 2, 3, 4 \), respectively, obtained by using the algorithm in Algorithm 1. The maximum privacy under perfect utility is marked.

VII. CONCLUSION

We defined utility and privacy using the CRLB and investigated the utility-privacy trade-off in a decentralized setting. We showed that the privacy mechanism of linear compression can be arbitrarily closely approximated by the privacy mechanism using noise perturbation, and we showed how to translate between these two mechanisms. Furthermore, we derived necessary and sufficient conditions for achieving arbitrarily strong utility-privacy trade-off, and developed methods to minimize privacy leakage while maintaining perfect utility under these conditions. When arbitrarily strong utility-privacy trade-off is not achievable, we proposed an alternating optimization
where $\Psi = P_2 H^T R^{-1}$ and $\Phi = R^{-1} - R^{-1} H P_2 H^T R^{-1} \in S^N$, (27) follows from the binomial inverse theorem, and (28) follows from the Woodbury matrix identity. Note that $\Phi$ is a degenerate matrix since by letting the singular value decomposition of $H^T R^{-1/2} = U \Sigma V^T$, we have

$$\Phi = R^{-1} - R^{-1} H P_2 H^T R^{-1} \equiv R^{-1} - R^{-1/2} H^{-1/2} \left( H^T R^{-1/2} R^{-1/2} H \right)^{-1} H^T R^{-1/2} R^{-1/2} = R^{-1/2} V \text{diag}(0_L, I_{N-L}) V^T R^{-1/2}. \quad (29)$$

On the other hand, if $J_0 > 0_L$, we obtain

$$\tilde{P}_x(I_N, \Theta) = \left( J_0 + H^T (R + \Theta)^{-1} H \right)^{-1} = P_0 - P_0 H^T \left( \Phi^{-1} + \Theta \right)^{-1} H P_0 \quad (30)$$

$$= P_0 - P_0 H^T \left( \Phi - \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi \right) H P_0 = P_0 - P_0 H^T \Phi H^T P_0 + P_0 H^T \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi H P_0 = \left( J_0 + H^T R^{-1} H \right)^{-1} + P_0 H^T \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi H P_0 = P_x + \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^T,$$

where $P_0 = J_0^{-1}$, $\Phi = (H_0 H^T + R)^{-1}$, $\Psi = P_0 H^T \Phi$. (30) follows from the Woodbury matrix identity, and (31) is a consequence of the binomial inverse theorem.

**APPENDIX A**

**DERIVATION OF (9) TO (11)**

If $J_0 = 0_L$, we have

$$\tilde{P}_x(I_N, \Theta) = \left( H^T (R + \Theta)^{-1} H \right)^{-1}$$

$$= \left( H^T \left( R^{-1} - R^{-1} (I_N + \Theta R^{-1})^{-1} \Theta R^{-1} \right) \right)^{-1} \quad (27)$$

$$= \left( H^T R^{-1} H - H^T R^{-1} (I_N + \Theta R^{-1})^{-1} \Theta R^{-1} \right)^{-1}$$

$$= P_x - P_x H^T R^{-1} \left( -I_N - \Theta R^{-1} \right)^{-1} \Theta R^{-1} H P_x$$

$$+ \Theta R^{-1} H P_2 H^T R^{-1} \left( -I_N - \Theta R^{-1} \right)^{-1} \Theta R^{-1} H P_x \quad (28)$$

$$= P_x + \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^T,$$

where $\Psi = P_2 H^T R^{-1}$ and $\Phi = R^{-1} - R^{-1} H P_2 H^T R^{-1} \in S^N$, (27) follows from the binomial inverse theorem, and (28) follows from the Woodbury matrix identity. Note that $\Phi$ is a degenerate matrix since by letting the singular value decomposition of $H^T R^{-1/2} = U \Sigma V^T$, we have

$$\Phi = R^{-1} - R^{-1} H P_2 H^T R^{-1} \equiv R^{-1} - R^{-1/2} H^{-1/2} \left( H^T R^{-1/2} R^{-1/2} H \right)^{-1} H^T R^{-1/2} R^{-1/2} = R^{-1/2} V \text{diag}(0_L, I_{N-L}) V^T R^{-1/2}. \quad (29)$$

On the other hand, if $J_0 > 0_L$, we obtain

$$\tilde{P}_x(I_N, \Theta) = \left( J_0 + H^T (R + \Theta)^{-1} H \right)^{-1} = P_0 - P_0 H^T \left( \Phi^{-1} + \Theta \right)^{-1} H P_0 \quad (30)$$

$$= P_0 - P_0 H^T \left( \Phi - \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi \right) H P_0 \quad (31)$$

$$= P_0 - P_0 H^T \Phi H^T P_0 + P_0 H^T \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi H P_0$$

$$= \left( J_0 + H^T R^{-1} H \right)^{-1} + P_0 H^T \Phi (I_N + \Theta \Phi)^{-1} \Theta \Phi H P_0$$

$$= P_x + \Psi (I_N + \Theta \Phi)^{-1} \Theta \Psi^T,$$

where $P_0 = J_0^{-1}$, $\Phi = (H_0 H^T + R)^{-1}$, $\Psi = P_0 H^T \Phi$. (30) follows from the Woodbury matrix identity, and (31) is a consequence of the binomial inverse theorem.
Let $\lambda_i(n) > 0$ be the $i$-th eigenvalue of $S_n$, associated with a unit eigenvector $v_i$ (commuting matrices share the same eigenspaces). Let $\alpha_i = \|Av_i\|^2$. We obtain

$$0 = \lim_{n \to \infty} \text{Tr} \left( A (S_n + \mu I_N)^{-1} A^T \right) = \lim_{n \to \infty} \sum_{i=1}^{N} \frac{\alpha_i}{\lambda_i(n) + \mu},$$

hence either $\alpha_i = 0$ or $\lambda_i(n) \to \infty$ as $n \to \infty$ for each $i = 1, \ldots, N$, which implies

$$\lim_{n \to \infty} \text{Tr} \left( AS_n^{-1} A^T \right) = \lim_{n \to \infty} \sum_{i=1}^{N} \frac{\alpha_i}{\lambda_i(n)} = 0.$$

Combining the above result with (32), we obtain

$$\lim_{n \to \infty} \text{Tr} \left( A (S_n + B)^{-1} A^T \right) = 0 \quad \implies \quad \lim_{n \to \infty} \text{Tr} \left( AS_n^{-1} A^T \right) = 0.$$

The proof is now complete.

**APPENDIX C**

**PROOF OF LEMMA 3**

Let $\lambda_i \geq 0$ be the $i$-th eigenvalue of $S$, associated with a unit eigenvector $v_i$. We first note that

$$\text{Tr} (ASA^T) = \sum_{i=1}^{N} \lambda_i \|Av_i\|^2,$$

(33)

$$\lim_{n \to \infty} \text{Tr} \left( B \left(nS + \frac{1}{n} I_N\right)^{-1} B^T \right)$$

$$= \lim_{n \to \infty} \sum_{i=1}^{N} \frac{1}{n\lambda_i - 1/n} \|Bv_i\|^2.$$

(34)

We first prove necessity. If both (33) and (34) are $0$, $Av_i = 0$ if $\lambda_i \neq 0$, and $Bv_i = 0$ if $\lambda_i = 0$ for each $i = 1, \ldots, N$. This implies that $v_i$ is in the null space of either $A$, $B$ or both. Therefore, we have $AQQT^{\top} = 0$, where $Q = [v_1, \ldots, v_N]$ is a unitary matrix. Thus, $AB^T = 0$.

We next assume that $AB^T = 0$. Let $\{v_i \mid i = 1, \ldots, |B|\}$ be a basis of the row space of $B$ and $\{v_i \mid i = |B| + 1, \ldots, |A|\}$ be a basis of the row space of $A$, where $|A| = \text{rank}(A)$ and $|B| = \text{rank}(B)$. Let $\lambda_i > 0$ if $i = 1, \ldots, |B|$, else $\lambda_i = 0$. Let $S = Q \text{diag}(\lambda_i) Q^T$, where $Q = [v_1, \ldots, v_N]$ is a unitary matrix. It can be easily verified that such $S$ satisfies the lemma conditions, and the proof is complete.

**APPENDIX D**

**DERIVATION OF (25) AND (26)**

We show the steps to obtain the utility and privacy function w.r.t. $\overline{\sigma_i}$ described in Section V. Partition $\Phi_i$ as

$$\Phi_i = \begin{bmatrix} \Phi_i|_{N_i,N_i} & \Phi_i|_{N_i,N_{i+1}} \\ \Phi_i|_{N_{i+1},N_i} & \Phi_i|_{N_{i+1},N_{i+1}} \end{bmatrix},$$

where $[\Phi_i]|_{N_i,N_i} \in \mathbb{R}^{N_i \times N_i}$, $N_i = \{1, \ldots, N_i\}$, $N_{i+1} = \{N_i + 1, \ldots, N\}$. We have

$$\left( \text{diag}(\overline{\sigma_i}, \overline{\sigma_{i}}) + \Phi_i \right)^{-1} = \left[ \begin{bmatrix} \Phi_i|_{N_i,N_i} & \Phi_i|_{N_i,N_{i+1}} \\ \Phi_i|_{N_{i+1},N_i} & \Phi_i|_{N_{i+1},N_{i+1}} \end{bmatrix} + \overline{\sigma_i} + \Phi_i|_{N_{i+1},N_{i+1}} \right]^{-1}$$

$$= \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where

$$A_{11} = (\Phi_i|_{N_i,N_i} + \Phi_i|_{N_{i+1},N_i})^{-1},$$

$$A_{12} = -A_{11} \Phi_i|_{N_i,N_{i+1}},$$

$$A_{21} = -T \Phi_i|_{N_{i+1},N_i} A_{11},$$

$$A_{22} = T + \Phi_i|_{N_{i+1},N_i} A_{11} \Phi_i|_{N_{i+1},N_i},$$

$$\Omega = \Phi_i|_{N_i,N_i} - \Phi_i|_{N_i,N_{i+1}} T \Phi_i|_{N_{i+1},N_i}$$

and $T = (\Omega|_{N_{i+1},N_i} + \Phi_i|_{N_{i+1},N_i})^{-1}$. Therefore, we have

$$P_x(\overline{\sigma_i}) = P_x + \begin{bmatrix} \Phi_i|_{N_i,N_i} & \Phi_i|_{N_i,N_{i+1}} \\ \Phi_i|_{N_{i+1},N_i} & \Phi_i|_{N_{i+1},N_{i+1}} \end{bmatrix}$$

$$= P_x + \begin{bmatrix} \Phi_i|_{N_i,N_i} & \Phi_i|_{N_i,N_{i+1}} \\ \Phi_i|_{N_{i+1},N_i} & \Phi_i|_{N_{i+1},N_{i+1}} \end{bmatrix}$$

$$= P_x + [\Phi_i|_{N_i,N_i} A_{11} \Phi_i|_{N_i,N_{i+1}}]^{T} + \Phi_i|_{N_i,N_i} A_{21} \Phi_i|_{N_{i+1},N_i}$$

$$+ [\Phi_i|_{N_{i+1},N_i} A_{12} \Phi_i|_{N_{i+1},N_{i+1}}] + \Phi_i|_{N_{i+1},N_i} A_{22} \Phi_i|_{N_{i+1},N_{i+1}}.$$

Therefore, the utility and $j$-th privacy function can be written as

$$u(\overline{\sigma_i}) = -\text{Tr} \left( \Gamma_u \left( \overline{\sigma_i} + \Omega \right)^{-1} \right) / \text{Tr} (U P_x U^T) - \Delta_u,$$

$$p_j(\overline{\sigma_i}) = \text{Tr} \left( \Gamma_p \left( \overline{\sigma_i} + \Omega \right)^{-1} \right) / \text{Tr} (G_j P_x G_j^T) + \Delta_{p_j},$$

where $\Delta_{p_j}, \Delta_u, \Gamma_u, \Gamma_p$ are defined in Section V.

**REFERENCES**

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] B. C. Csajai, Z. Kemeny, G. Pedone, A. Kuti, and J. Vanzca, “Wireless multi-sensor networks for smart cities: A prototype system with statistical data analysis,” *IEEE Sensors J.*, vol. 17, no. 23, pp. 7667–7676, Dec. 2017.

[3] W. Tang, F. Ji, and W. P. Tay, “Estimating infection sources in networks using partial timestamps,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 3035–3049, Dec. 2018.

[4] J. Yang, X. Zhong, and W. P. Tay, “A dynamic Bayesian nonparametric model for blind calibration of sensor networks,” *IEEE Internet of Things J.*, vol. 5, no. 5, pp. 3942–3953, Oct. 2018.

[5] J-F. Chamberland and V. V. Veeravalli, “Decentralized detection in sensor networks,” *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 407–416, Feb. 2003.

[6] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, “Asymptotic performance of a censoring sensor network,” *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4191–4209, Nov. 2007.

[7] ______, “Data fusion trees for detection: Does architecture matter?” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4155–4168, Sep. 2008.

[8] O. P. Kreidl, J. N. Tsitsiklis, and S. I. Zoumpoulis, “On decentralized detection with partial information sharing among sensors,” *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1759–1765, Apr. 2011.
