Distributed Estimation in Multi-Agent Networks

Lalitha Sankar and H. Vincent Poor
Dept. of Electrical Engineering,
Princeton University, Princeton, NJ 08544.
{lalitha,poor}@princeton.edu

***Abstract*— A problem of distributed state estimation at multiple agents that are physically connected and have competitive interests is mapped to a distributed source coding problem with additional privacy constraints. The agents interact to estimate their own states to a desired fidelity from their (sensor) measurements which are functions of both the local state and the states at the other agents. For a Gaussian state and measurement model, it is shown that the sum-rate achieved by a distributed protocol in which the agents broadcast to one another is a lower bound on that of a centralized protocol in which the agents broadcast as if to a virtual CEO converging only in the limit of a large number of agents. The sufficiency of encoding using local measurements is also proved for both protocols.**

I. Introduction

We consider a network of K distributed agents in which each agent observes sensor measurements from a distinct part of a large interconnected physical network. Examples of such networks include cyber-physical systems, specifically the smart grid, in which an agent can be viewed as a regional operator whose power measurements are affected by those at other agents due to the physical grid connectivity. Agent k is interested in estimating the state (defined as a set of system parameters; for e.g., voltages and phases in the electric grid) of its local network from its measurements, Y_k, which are a function of both the local state X_k and the states X_l, $l \neq k$, $l, k \in \{1, 2, \ldots, K\}$ of other agents in the network where the states X_k are assumed to be independent of each other.

Estimating X_k at agent k with high fidelity requires the agents to interact and share data amongst themselves. While the estimate fidelity is crucial to the control decisions made by the agents, in many distributed systems, for competitive reasons, the agents wish to keep their state information private. This leads to a problem of *competitive privacy* which captures the tradeoff between the utility to the agent (estimate fidelity) that can be achieved via cooperation and the resulting privacy leakage (quantified via mutual information).

Mapping utility to distortion and privacy to leakage quantified via mutual information, one can abstract the competitive privacy problem as a distributed source coding problem with additional leakage constraints. The set of all achievable rate-fidelity-leakage tuples determines the utility-privacy tradeoff region. In [1], we introduced and studied this problem for a two-agent interactive system with Gaussian states and noisy Gaussian measurements. We proved that side-information (measurements at the other agent) aware Wyner-Ziv encoding [2] at each agent achieves both the minimal rate and the minimal leakage for every choice of fidelity (quantified via mean-squared distortion).

Even without additional privacy constraints, the problem of determining the set of all rate-distortion tuples in a multi agent network is related to the distributed source coding problem [3], [4] which remains open. Furthermore, for a relatively simpler setting obtained by assuming that a central entity, often referred to as a chief executive officer (CEO), wishes to estimate the states X_k, for all k, from the transmissions of all agents, we obtain a multi-variate (vector) Gaussian CEO problem which also remains open except for specific cases [5].

Circumventing these challenges, we focus on the rate-distortion-leakage behavior in the limit of large K for a *distributed protocol* in which each agent encodes its measurements taking into account the prior broadcasts of the other agents (henceforth referred to as *progressive encoding*) as well as the side-information at the other agents. We compare the performance of this protocol with a *centralized protocol* in which the agents broadcast their encoded messages as if to a virtual CEO. We consider a noisy Gaussian measurement model at each agent with the same level of interference from the states of the other agents. For this symmetric model, our results demonstrate that the sum-rate achieved by distributed protocol outperforms that for the centralized schemes with asymptotic convergence with K. We also prove the sufficiency of encoding local measurements for both protocols and present outer bounds for the per user rate and leakage.

The paper is organized as follows. We introduce the model and communication protocols in Section II. In Section III we develop the achievable rate-distortion-leakage tuples for both protocols as well as outer bounds. We conclude in Section IV.

II. Preliminaries

A. Model and Metrics

We consider a network of K agents such that, at any time instant i, $i = 1, 2, \ldots, n$, the measurement $Y_{k,i}$ at agent k, $k = 1, 2, \ldots, K$, is related to the states $X_{m,i}$, $m = 1, 2, \ldots, K$, at the agents as follows:

$$Y_{k,i} = X_{k,i} + \sum_{l=1, l\neq k}^{K} \sqrt{h} X_{l,i} + Z_{k,i}, \ k = 1, 2, \ldots, K, \quad (1)$$

where the state variables $X_{m,i} \sim \mathcal{N}(0, \sigma^2)$, for all m and i are assumed to be independent and identically distributed

The research was supported in part by the AFOSR under MURI Grant FA9550-09-1-0643 and in part by the NSF under Grant CCF-10-16671.

(i.i.d.) and are also independent of the i.i.d. noise variables $Z_{k,i} \sim \mathcal{N}(0,1)$. The coefficient $h > 0$ is assumed to be fixed for all time and known at all agents. We assume that the k^{th} agent observes a sequence of n measurements $Y_k^n = [Y_{k,1}\ Y_{k,2}\ \ldots\ Y_{k,n}]$, for all k, prior to communications.

Utility: For the continuous Gaussian distributed state and measurements, a reasonable metric for utility at the k^{th} agent is the mean square error D_k between the original and the estimated state sequences X_k^n and $\hat{X}_k^n$, respectively.

Privacy: The measurements at each agent in conjunction with the quantized data shared by the other agents while enabling accurate estimation also leaks information about the other agents' states. We capture this leakage using mutual information.

B. Communication Protocol

We assume that each agent broadcasts a function of its measurements (*distributed procotol*) to all agents and they do so in a round-robin fashion. We assume that all agents encode in one of the following two ways: i) *local encoding* in which each agent quantizes only its measurements; or ii) *progressive encoding* in which each agent encodes and transmits taking into account both its measurements and prior communications from other agents. In both cases, the agents transmit at a rate that takes into account the correlated measurements and prior communications of other agents.

To better understand the advantage of the above distributed procotol, we also consider the case where the agents broadcast as if communicating with a virtual central operator, say CEO, henceforth referred to as the *centralized protocol*. This may be viewed as the case in which the computing power at the agents is limited and the CEO shares with each agent its received messages (which are then decoded at each agent). For either protocol, the encoding can be either local or progressive. Let $I_p \in \{0,1\}$ and $I_{enc} \in \{0,1\}$ be random variables that denote the choice of protocols and encodings such that $I_p = 1$ and $I_p = 0$ for the distributed and centralized protocol, respectively, and $I_{enc} = 1$ and $I_{enc} = 0$ for the progressive and local encoding, respectively.

Formally, the encoder at agent k maps its measurements to an index set $\mathcal{J}_k$ where

$$\mathcal{J}_k \equiv \{1, 2, \ldots, J_k\},\ k = 1, 2, \ldots, K, \tag{2}$$

is the index set at the k^{th} agent for mapping the measurement sequence, and the prior communications (progressive encoding), via the encoder f_k, $k = 1, 2, \ldots K$, defined as

$$f_k : \mathcal{Y}_k^n \times I_{enc} \cdot \textstyle\prod_{l=1}^{k-1} \mathcal{J}_l \to \mathcal{J}_k, \tag{3}$$

such that at the end of the K broadcasts, one from each agent, the decoding function F_k at the k^{th} agent (or the CEO) is a mapping from the received message sets (both protocols) and the measurements (the distributed procotol) to that of the reconstructed sequence denoted as

$$F_k : \mathcal{J}_1 \times \ldots \times \mathcal{J}_K \times (\mathcal{Y}_k^n \cdot I_p) \to \hat{\mathcal{X}}_k^n, \quad k = 1, 2, \ldots, K. \tag{4}$$

Let M_k denotes the size of J_k. The expected distortion D_k at the k^{th} agent is given by

$$D_k = \frac{1}{n}\mathbb{E}\left[\sum_{i=1}^{n}\left(X_{k,i} - \hat{X}_{k,i}\right)^2\right],\ k = 1, 2, \ldots K, \tag{5}$$

The privacy leakage, $L_k^{(l)}$, about state k at agent l, $l \neq k$, is given by

$$L_k^{(l)} = \frac{1}{n} I\left(X_k^n; J_1, J_2, \ldots, J_K, Y_l^n\right),\ \text{for all } k \neq l. \tag{6}$$

The communication rate of the k^{th} agent is denoted by

$$R_k = n^{-1} \log_2 M_k, k = 1, 2, \ldots, K. \tag{7}$$

Definition 1: The utility-privacy tradeoff region is the set of all $(D_1, \ldots, D_k, L_1^{(2)}, \ldots, L_1^{(K)}, \ldots, L_K^{(1)}, \ldots, L_K^{(K-1)})$ for which there exists a coding scheme given by (2)-(4) with parameters $(n, K, M_1, M_2, D_1+\epsilon, \ldots, D_K+\epsilon, L_1+\epsilon, \ldots, L_K+\epsilon)$ for n sufficiently large such that $\epsilon \to 0$ as $n \to \infty$.

III. Main Results

We use the following proposition, lemma, and function definition in the sequel to compute the achievable distortions and rates.

Proposition 1: For (column) vectors $\underline{A}$ and $\underline{B}$, let $K_{\underline{AA}} = var\left(\underline{A}\right) = E\left[\left(\underline{A} - E\left[\underline{A}\right]\right)\left(\underline{A}^T - E\left[\underline{A}^T\right]\right)\right]$ and $K_{\underline{AB}} = E\left[\left(\underline{A} - E\left[\underline{A}\right]\right)\left(\underline{B}^T - E\left[\underline{B}^T\right]\right)\right]$ denote the covariance and cross-correlation matrices, respectively. The conditional variance $E[var(\underline{A}|\underline{B})]$ is then given as $E[var(\underline{A}|\underline{B})] = K_{\underline{AA}} - K_{\underline{AB}}K_{\underline{BB}}^{-1}K_{\underline{AB}}^T$.

Lemma 1: For a $K \times K$ symmetric Toeplitz matrix whose diagonal entries are all a, and off-diagonal entries are all b the determinant is $(a + (K-1)\,b)\,(a-b)^{(K-1)}$.

Proof: The determinant is obtained by the following two operations: i) add columns 2-K to column 1, and ii) subtract row 1 from each of the remaining rows. ∎

Definition 2: For some α, $\beta \in \mathcal{R}^+$, the function $f_1(k, c) \equiv \alpha + (k-2)\,\beta - (k-1)\,c$ varies over $k \in [1, K]$ and $c \in \mathcal{R}^+$.

A. Distortion

We assume that each agent has the same distortion constraint D. The distortion D at each agent ranges from a minimum achieved when it has perfect access to the measurements at all agents to a maximum achieved when it estimates using only its own measurements. From the symmetry of the model in (1), the minimal (resp. maximal) distortion achieved at each agent is the same. Let $D_{\min}$ and $D_{\max}$ denote the minimal and maximal distortions, respectively, at each agent. For the Gaussian model considered here with minimum mean square error (MSE) constraints, we have

$$D_{\min} = E\left[var(X_1|Y_1Y_2\ldots Y_K)\right],\ \text{and} \tag{8}$$

$$D_{\max} = E\left[var(X_1|Y_1)\right]. \tag{9}$$

We now determine $D_{\min}$ and $D_{\max}$. Let

$$\alpha \equiv E(Y_l^2) = \sigma_X^2 \left(1 + h\left(K-1\right)\right) + 1, \text{ for all } l \quad (10a)$$

$$\beta \equiv E(Y_l Y_k) = \sigma_X^2 \left(2\sqrt{h} + h\left(K-2\right)\right), \ l \neq k. \quad (10b)$$

Note that for large K, $\alpha \rightarrow h\left(K-1\right)\sigma_X^2$, and $\beta \rightarrow h\left(K-2\right)\sigma_X^2$.

Computation of $D_{\max}$: Expanding (9), we obtain

$$D_{\max} = E\left[var(X_1|Y_1)\right] = \sigma_X^2\left(1 - \frac{\sigma_X^2}{\alpha}\right). \quad (11)$$

For large K, $D_{\max} \rightarrow \sigma_X^2$.

Computation of $D_{\min}$: Expanding (8), we have

$$D_{\min} = E\left[var(X_1|Y_1 Y_2 \ldots Y_K)\right] \quad (12)$$

$$= \frac{|E\left[var(X_1 Y_2 \ldots Y_K|Y_1)\right]|}{|E\left[var(Y_2 \ldots Y_K|Y_1)\right]|} \quad (13)$$

where the simplification in (13) results from the assumption of jointly Gaussian random variables. Applying Lemma 1, for

$$c_1 = \sigma_X^2 - \sigma_X^4/\alpha, \ c_2 = \sigma_X^2\left(\sqrt{h} - \beta/\alpha\right), \quad (14)$$

$$c_3 = \alpha - \beta^2/\alpha, \text{ and } c_4 = \beta - \beta^2/\alpha, \quad (15)$$

we obtain the minimum distortion $D_{\min}$ as

$$D_{\min} = D_{\max}\left(1 - \frac{\left(K-1\right)\frac{\sigma_X^2\left(\sqrt{h}-\beta/\alpha\right)^2}{\left(1-\sigma_X^2/\alpha\right)}}{f_1\left(K, \beta^2/\alpha\right)}\right). \quad (16)$$

Remark 1: For $K \rightarrow \infty$, $D_{\min} \rightarrow D_{\max}(1-(1-\sqrt{h})^2/h)$.

B. Distributed Protocol

A general coding strategy for this distributed source coding problem needs to take into account: a) the order of agent broadcasts; b) multiple encoding possibilities at each agent depending on whether the received data is used alongwith local measurements in encoding; c) exploiting the correlated measurements at other agents in broadcasting just sufficient data for other agents to achieve their distortions; and d) multiple rounds of interactions. We present a distributed encoding scheme with a single round of communication (for simplicity of analysis) in which the agents broadcast in order (the source permutation choice is irrelevant due to the symmetry of the model). The local and progressive coding schemes differ in including the received data in encoding at each agent, while the centralized and distributed protocols differ in whether they exploit the correlated measurements at the other agents.

The achievable distortion D in general depends on the encoding scheme chosen. Let R_k and $\tilde{R}_k$ denote the rates for the local and progessive encoding schemes, respectively. We first consider the progressive encoding scheme in which each agent broadcasts (to all other agents) a noisy function of both its measurements and prior communications. More precisely, agent k maps its measurement and prior communication sequences to one among a set of $2^{n\tilde{R}_k}$ $\tilde{U}_k^n$ sequences chosen to satisfy the distortion constraints. The $\tilde{U}_k^n$ sequences are generated via an i.i.d distribution of $\tilde{U}_{k,i}$ for all i such that $\tilde{U}_{1,i} = Y_{1,i} + Q_{1,i}$ and for all $k > 1$, $\tilde{U}_{k,i} = Y_{k,i} + \sum_{l=1}^{k-1} a_{k,l}\tilde{U}_{l,i} + Q_{k,i}$ where $a_{k,l} \in \mathcal{R}$, and $Q_{k,i} \sim N\left(0, \sigma_Q^2\right)$ is independent of $Y_{k,i}$ for all $k = 1, 2, \ldots, K$, and $i = 1, 2, \ldots, n$.

The achievable distortion D at agent k as a result of estimating its state using both its measurements Y_k^n and the received sequences $\tilde{U}_l^n$, for all $l \neq k$, is such that $D \in [D_{\min}, D_{\max}]$ where $D_{\max}$ is achieved when $U_l^n = 0$ for all l and $D = D_{\min}$ for $\sigma_Q^2 = 0$. On the other hand, for the local encoding scheme, let $U_{k,i} = Y_{k,i} + Q_{k,i}$, for all k and i, such that agent k maps *only* its measurement sequences to one among a set of 2^{nR_k} U_k^n sequences chosen to satisfy the distortion constraints.

Theorem 1: The sets $\mathcal{D}$ of all achievable distortions D for the local and progressive encoding schemes for the distributed protocol are the same.

Proof: For Gaussian codebooks and Gaussian measurements and from symmetry of the model, the distortion D at each agent is given by

$$D = \mathbb{E}\left[var\left(X_1|Y_1\tilde{U}_1\tilde{U}_2\tilde{U}_3\ldots\tilde{U}_K\right)\right] \quad (17)$$

$$= \mathbb{E}\left[var\left(X_1|Y_1U_1U_2U_3\ldots U_K\right)\right] \in [D_{\min}, D_{\max}] \quad (18)$$

where in (17) we have used that fact that $\tilde{U}_1 = U_1$, and conditioned on U_1,it suffices to condition on U_2, and similarly for the remaining U_k, $k > 2$. ■

Computation of D: Using the independence of the quantization noise Q_k for all k, as well as the independence of Q_k and X_k, we have $E\left[U_k U_l\right] = E\left[Y_k Y_l\right] = \beta$ for all $l \neq k$ and $E\left[U_k^2\right] = E\left[Y_k^2\right] + E\left[Q_k^2\right] = \alpha + \sigma_Q^2$. Thus, D is obtained in a manner analogous to the calculation of $D_{\min}$ with the replacement of c_3 by $c_3 + \sigma_Q^2$. Thus, we have

$$D = D_{\max}\left(1 - \frac{\left(K-1\right)\frac{\sigma_X^2\left(\sqrt{h}-\beta/\alpha\right)^2}{\left(1-\sigma_X^2/\alpha\right)}}{f_1\left(K, \frac{\beta^2}{\alpha}\right) + \sigma_Q^2}\right). \quad (19)$$

Rate Computation: We consider a round-robin protocol in which agent 1 broadcasts a quantized function of its measurements and prior communications at a rate which takes into account all the side information at all other agents. Thus, the rate $\tilde{R}_1$ required is the maximal of the rates required to each agent and is given by

$$\tilde{R}_1 \geq I(\tilde{U}_1; Y_1) - \min\left(I(\tilde{U}_1; Y_2), \ldots, I(\tilde{U}_1; Y_K)\right) \quad (20a)$$

$$= I(U_1; Y_1) - I(U_1; Y_2) = R_1 \quad (20b)$$

where (20b) follows from the symmetry of the measurement model, the fact that $\tilde{U}_1 = U_1$, and R_1 is the minimal rate required at agent 1 for the local scheme. Next, agent 2 analogously broadcasts a function of its measurements at a

rate R_2 given by

$$\tilde{R}_2 \geq I(\tilde{U}_2; Y_2\tilde{U}_1) - \min_{l\in\{1,\ldots,K\},l\neq 2} I(\tilde{U}_2; Y_l\tilde{U}_1) \quad (21a)$$

$$= I(\tilde{U}_2; Y_2|\tilde{U}_1) - \min_{l\in\{1,\ldots,K\},l\neq 2} I(\tilde{U}_2; Y_1|\tilde{U}_1) \quad (21b)$$

$$= I(U_2; Y_2) - I(U_2; Y_1) = R_2 \quad (21c)$$

where (21c) follows from $h(\tilde{U}_2|Y_1\tilde{U}_1) - h(\tilde{U}_2|Y_2\tilde{U}_1) = h(U_2|Y_1) - h(U_2|Y_2)$ since $U_2 - Y_2 - U_1$ form a Markov chain and due to the symmetry of the model. It can be verified easily that the bound in (21c) is the minimal rate R_2 for the local encoding scheme. One can similarly show that the rate at which agent 3 broadcasts is

$$\tilde{R}_3 \geq I(\tilde{U}_3; Y_3\tilde{U}_1\tilde{U}_2) - \min_{l\in\{1,\ldots,K\},l\neq 3} I(\tilde{U}_3; Y_1\tilde{U}_1\tilde{U}_2) \quad (22a)$$

$$= I(U_3; Y_3) - I(U_3; Y_1U_2) = R_3 \quad (22b)$$

where we have used the fact that $U_3 - Y_3 - U_1U_2$ and $U_1 - Y_1 - U_3$ form Markov chains. Generalizing we have, for all $k > 1$,

$$\tilde{R}_k = R_k \geq I(U_k; Y_k) - I(U_k; Y_1U_1 \ldots U_{k-1}), \quad (23a)$$

where the bound in (23a) is the minimal rate at which agent k is required to broadcast when it only encodes Y_k^n.

Calculation of Leakage: For the proposed progressive encoding, the leakage of the state of agent k at any other agent $j \neq k$, for all such k, j, is bounded as

$$L_k^{(j)} = \frac{1}{n} I(X_k^n; Y_j^n J_1 J_2 \ldots J_K),\ j \neq k \quad (24a)$$

$$\geq I(X_1; Y_2\tilde{U}_1 \ldots \tilde{U}_K) = I(X_1; Y_2U_1 \ldots U_K) \quad (24b)$$

$$= \frac{1}{2}\log\left(\frac{\alpha f_1\left(K, \beta^2/\alpha\right)}{\left(\alpha - \sigma_X^2\right) f_1\left(K, c_5\right)}\right) \quad (24c)$$

where (24b) is a result of the model symmetry, the code construction and typicality arguments and is omitted for brevity. The bound in (24c) follows from the relation of the code constructions for the two encoding schemes and $c_5 = (\beta - \sqrt{h}\sigma_x^2)^2 \Big/ \left(\alpha - \sigma_x^2\right) + h\sigma_X^2$.

Theorem 2: It is sufficient to encode the local measurements at each agent in the distributed protocol.

Theorem 2 follows directly from the fact that for Gaussian encoding, from (18), (23a), and (24c), we have that the set of all rate-distortion-leakage tuples achieved by the local and progressive encoding schemes is the same.

The sum-rate of the distributed scheme $R_{sum}^{Dist} = \sum_{k=1}^K R_k$ can be simplified as

$$R_{sum}^{Dist} = h\left(U_2U_3 \ldots U_K|Y_1\right) + h(U_1|Y_2) - \frac{K}{2}\log\left(2\pi e\sigma_Q^2\right) \quad (25a)$$

$$= \frac{K}{2}\log\left(\frac{\alpha + \sigma_Q^2 - \beta}{\sigma_Q^2}\right) + \frac{1}{2}\log\left(\frac{\left(\alpha + \sigma_Q^2 - \frac{\beta^2}{\alpha}\right)}{\left(\alpha + \sigma_Q^2 - \beta\right)}\right) \quad (25b)$$

$$+ \frac{1}{2}\log\left(\left(f_1\left(K, \beta^2/\alpha\right) + \sigma_Q^2\right)/\left(\alpha + \sigma_Q^2 - \beta\right)\right)$$

where (25b) is obtained from (25a) by determining $|E\left[var\left(\underline{U}_K|Y_1\right)\right]|$ where $\underline{U}_{K-1} = \left[U_2\ U_3\ \ldots\ U_K\right]^T$ denotes a column vector of length $(K-1)$. By expanding $E\left[var\left(\underline{U}_{K-1}|Y_1\right)\right]$ using Proposition 1, one can verify that $|E\left[var\left(\underline{U}_K|Y_1\right)\right]|$ simplifies to finding the determinant of the $(K-1)\times(K-1)$ Toeplitz matrix with diagonal and off diagonal entries $\alpha + \sigma_Q^2 - \frac{\beta^2}{\alpha}$ and $\beta - \frac{\beta^2}{\alpha}$, respectively, which from Lemma 1 is given by $f_1\left(K, \beta^2/\alpha\right)\left(\alpha + \sigma_Q^2 - \beta\right)^{(K-2)}$. One can similarly show that $E\left[var\left(U_1|Y_2\right)\right] = \alpha + \sigma_Q^2 - \beta^2/\alpha$.

In the limit of $K \to \infty$, $(K-2)\beta - (K-1)\frac{\beta^2}{\alpha} \to 0$, $\alpha - \beta^2/\alpha \to h$, $\alpha - \beta \to h$, and therefore, the second and third log terms in (25b) scale as $\log(K)$. Thus, in the limit, the per agent rate $R = R_{sum}^{Dist}/K$ is given by

$$\lim_{K\to\infty} R = \frac{1}{2}\log\left(\frac{\alpha + \sigma_Q^2 - \beta}{\sigma_Q^2}\right). \quad (26)$$

C. Distributed vs. Centralized

We now compare the distributed protocol to a centralized protocol in which each agent broadcasts at a rate intended for a (virtual) CEO, and thus, is oblivious of the correlated measurements at the other agents. Here again, the agents can use a progressive encoding scheme analogously to the distributed protocol. As in the distributed protocol, here too one can show that a local encoding scheme suffices, in which agent k generates a codebook U_k^n whose entries $U_{k,i}$ are generated in an i.i.d fashion such that $U_{k,i} = Y_{k,i} + Q_{k,i}$, $Q_{k,i}$ is independent of $Y_{k,i}$ and $Q_{l,i}$, for all $l \neq k$, for all k, and for all i. The compression rates are bounded as follows. First, agent 1 transmits its quantized measurements at a rate R_1 such that for error-free decoding of U_1^n at the decoder, we require

$$R_1 \geq I\left(U_1; Y_1\right). \quad (27)$$

Agent 2 takes into account the knowledge of U_1^n at all agents and broadcasts at a rate

$$R_2 \geq I\left(U_2; Y_2\right) - I\left(U_2; U_1\right). \quad (28)$$

Note that the agents broadcast taking into account the prior transmissions (as if to a CEO) but not the side information at the other agents. Continuing similarly, we have for all $k \geq 2$,

$$R_k \geq I\left(U_2; Y_k\right) - I\left(U_k; U_1U_2 \ldots U_{k-1}\right). \quad (29)$$

The resulting sum rate $R_{sum}^{CEO} = \sum_{k=1}^K R_k$ can be simplified as

$$R_{sum}^{CEO} = \sum\nolimits_{k=1}^K I(U_k; Y_k) - \sum\nolimits_{k=2}^K I(U_k; U_1 \ldots U_{k-1}) \quad (30)$$

$$= h\left(U_K, U_{K-1} \ldots U_1\right) - \frac{K}{2}\log\left(2\pi e\sigma_Q^2\right) \quad (31)$$

$$= \frac{K}{2}\log\left(\frac{\left(\alpha + \sigma_Q^2 - \beta\right)}{\sigma_Q^2}\right) + \frac{1}{2}\log\left(\frac{\left(\alpha + \sigma_Q^2 + (K-1)\beta\right)}{\left(\alpha + \sigma_Q^2 - \beta\right)}\right). \quad (32)$$

Thus, the rate on average per user is $R^{CEO} = R^{CEO}_{sum}/K$ which converges in the limit of a large number of agents K to

$$\lim_{K\to\infty} R^{CEO} = \frac{1}{2}\log\left(\frac{(\alpha+\sigma_Q^2-\beta)}{\sigma_Q^2}\right). \quad (33)$$

Comparing (25b) and (32), we can verify that for every choice of σ_Q^2, and hence D, $R^{CEO}_{sum} > R^{Dist}_{sum}$. Furthermore, one can also show that the leakage at each agent for the centralized protocol is the same as the distributed protocol in (24) and is the same for both the local and progressive encoding schemes. The following theorem summarizes our results.

Theorem 3: The average per user rate of the centralized protocol is strictly lower bounded by that for the distributed protocol and converges to this lower bound only in the limit of large K.

D. Outer Bounds

From the symmetry of the model, it suffices to bound the rate R_1 of agent 1 as

$$R_1 \geq \frac{1}{n}H(J_1) \geq \frac{1}{n}I(Y_1^n; J_1|Y_2^nY_3^n\dots Y_K^n) \quad (34)$$

$$\geq h\left(Y_1|Y_2\dots Y_K\right) - \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|\hat{X}_{2,i}Y_{2,i}\dots Y_{K,i}) \quad (35)$$

$$\geq h\left(Y_1|Y_2\dots Y_K\right) - \frac{1}{2}\log(2\pi e\Sigma) \quad (36)$$

where (35) results from the fact that $\hat{X}_2^n,\dots\hat{X}_K^n$ can be estimated from $J_1, Y_2^n,\dots Y_K^n$, and that conditioning on only one of the estimates is a lower bound on R_1, and (36) results from using the fact that a jointly Gaussian distribution maximizes the differential entropy for a fixed variance, from the concavity of the log function for $\Sigma \equiv E\left[var\left(Y_1|\hat{X}_1Y_2Y_3\dots Y_K\right)\right]$. For jointly Gaussian $\left(Y_1,\dots,Y_K,\hat{X}_2\right)$, we can write

$$\hat{X}_2 = Y_2 + \textstyle\sum_{l=1,l\neq 2}^{K} bY_l + Z \quad (37)$$

where $Z \sim N\left(0,\sigma_Z^2\right)$ is independent of Y_k for all k, and from symmetry, we choose the same scaling constant b in (37). For $g \equiv E[\left(\hat{X}_2 - Y_2 - bY_3\dots - bY_K\right)^2] = b^2/\left(b^2\alpha+\sigma_Z^2\right)$, $c_1 = \beta^2 g$, and $c_2 = c_1 + (\beta-\beta\alpha g)^2/\left(\alpha-\alpha^2 g\right)$, we obtain

$$R_1 \geq \frac{1}{2}\log\left(\frac{f_1(K,\beta^2/\alpha)\,(\alpha-\beta)}{f_1\left(K-1,\beta^2/\alpha\right)}\right) \quad (38)$$

$$-\frac{1}{2}\log\left(\frac{f_1\left(K,c_2\right)}{f_1\left(K,c_1\right)}\left(\alpha-\alpha^2 g\right)\right) \quad (39)$$

where we have used the orthogonality of the minimum MSE estimate and the measurements, i.e., $E\left[\left(X_1-\hat{X}_1\right)Y_l\right]=0$, for all $l\neq 1$, and the distortion constraint in (5).

With $\hat{X}_2$ in (37), one can similarly bound $L_1^{(j)} = L_1^{(2)}$ (from symmetry), for all j, as

$$R_1 \geq \frac{1}{n}I(X_1^n; Y_2^nJ_1J_2\dots J_K) \quad (40)$$

$$\geq h\left(X_1\right) - \frac{1}{2}\log\left(2\pi eE\left[var\left(X_1|Y_2\hat{X}_2\right)\right]\right) \quad (41)$$

$$= \frac{1}{2}\log\left(q_1\Big/\left(\left(1-\sigma_X^2q_2^2\right)q_1 - \sigma_X^2\left(\sqrt{h}-q_2\right)^2\right)\right)$$

where $g_1 \equiv E\left[\left(\hat{X}_2-Y_2\right)^2\right] = \left(b^2\left(K-1\right)\alpha + \left(K-1\right)\left(K-2\right)b\beta/2 + \sigma_Z^{2-1}\right)^{-1}$,

$$q_1 \equiv \alpha - g_1b^2\beta^2\left(K-1\right)^2, \text{ and} \quad (42)$$

$$q_2 = g_1b^2\left(1+\left(K-2\right)\sqrt{h}\right)\beta\left(K-1\right). \quad (43)$$

Remark 2: Due to the lack of a pre-log factor K, the per-user rate R for the outer bound rapidly approaches 0 with K (relative to the inner bounds).

The rate R and leakage L_k (for any k) as a function of K are illustrated in Fig. 1 for $h = 0.5$ and $\sigma_Q^2 = 6$.

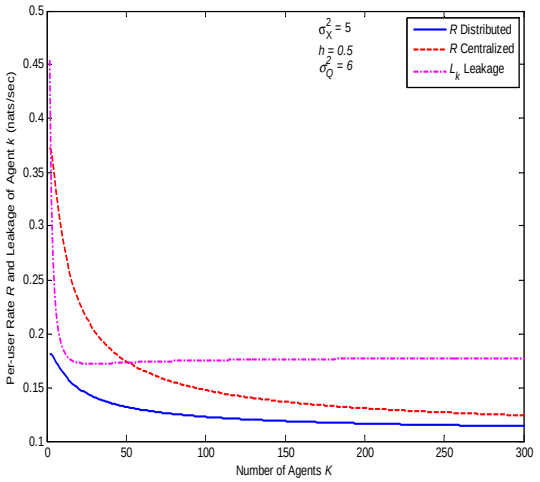

Fig. 1. Plot of per-user rate R and leakage L_k of any agent k vs. K.

IV. Concluding Remarks

We have introduced a distributed state estimation problem among K agents with fidelity and privacy constraints. We have shown that the sum-rate and per user rate achieved from a distributed protocol in which the agents directly interact taking into account the prior knowledge at all agents lower bounds those achieved by a centralized protocol with convergence for very large K. Tighter outer bounds that account for the distributed coding are much needed.

References

[1] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Proc. 2nd IEEE Intl. Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011.

[2] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[3] T. Berger, “Multiterminal source coding,” in *Information Theory Approach to Communications*, G. Longo, Ed. New York: Springer-Verlag, 1978.
[4] S. Tung, “Multiterminal rate-distortion theory,” Ph.D., Cornell University, Ithaca NY, USA, 1978.
[5] A. B. Wagner, S. Tavildar, and P. Viswanath, “Rate region of the quadratic gaussian two-encoder source-coding problem,” *IEEE Trans. Inform. Theory*, vol. 54, no. 5, pp. 1938 –1961, May 2008.