Distributed Kalman Filtering with Privacy against Honest-but-Curious Adversaries

Ashkan Moradi*, Naveen K. D. Venkategowda†, Sayed Pouria Talebi*, and Stefan Werner*
*Department of Electronic Systems, Norwegian University of Science and Technology, Trondheim, Norway
E-mail: {ashkan.moradi, pouria, stefan.werner}@ntnu.no .
†Linköping University, Norrköping, Sweden, E-mail: naveen.venkategowda@liu.se.

***Abstract*—This paper proposes a privacy-preserving distributed Kalman filter (PP-DKF) to protect the private information of individual network agents from being acquired by honest-but-curious (HBC) adversaries. The proposed approach endows privacy by incorporating noise perturbation and state decomposition. In particular, the PP-DKF provides privacy by restricting the amount of information exchanged with decomposition and concealing private information from adversaries through perturbation. We characterize the performance and convergence of the proposed PP-DKF and demonstrate its robustness against perturbation. The resulting PP-DKF improves agent privacy, defined as the mean squared estimation error of private data at the HBC adversary, without significantly affecting the overall filtering performance. Several simulation examples corroborate the theoretical results.**

***Index Terms*—Estimation, privacy, information fusion, average consensus, distributed Kalman filtering, multiagent systems.**

I. Introduction

Distributed Kalman filters (DKFs) have gained increased attention due to their high accuracy and computational efficiency for learning and estimation tasks in multiagent systems [1]–[4]. In general, distributed Kalman filtering techniques are based on agents running local Kalman filters and consensus operations to fuse observation and state information [5]–[7]. Although local cooperation among agents in distributed settings facilitates the fusion process, it causes undesirable information disclosure. Thus, the vulnerability of distributed procedures to potential eavesdroppers turns privacy preservation into an urgent issue to tackle in many applications [8]–[10].

Various methods are present to address privacy issues in distributed consensus operations in the literature. Differential privacy (DP) techniques, for example, use uncorrelated noise sequences within information exchange protocols to protect individual information [10], [11]. Alternatively, more recent noise injection-based methods achieve a better privacy-accuracy trade-off by perturbing the information exchanged with noise [12]–[14]. Further, decomposition-based techniques provide privacy by restricting the amount of information that is shared with other agents [15], [16].

Using DP to protect individual data streams in a system theoretic context where sensor measurements are transmitted to a fusion center was first addressed in [17]. In [18], a general approach is presented to design a differentially private Kalman filter in both cases of perturbation before exchanging information with the fusion center as well as output perturbation that injects noise to the output of the Kalman filter. In addition, the authors in [19] demonstrate that combining the input signals before adding DP noises, except for privacy, enhances the Kalman filtering performance. The privacy-aware Kalman filter proposed in [20] partitions sensor measurements into private and public substates to maximize the estimation error of the private state and minimize that for the public state. Although most literature discusses centralized filtering settings with external adversaries [17]–[20], in the context of distributed filtering applications, honest-but-curious (HBC) adversaries use local information to infer private data. An HBC adversary is a network agent that participates in the filtering process, but is curious and tries to retrieve private information from other agents. Although literature includes studies related to privacy-preserving Kalman filtering techniques, no attention has been paid to a privacy-preserving framework for distributed Kalman filtering strategies.

This paper proposes a privacy-preserving distributed Kalman filter that incorporates both noise injection-based and decomposition-based average consensus techniques to achieve privacy against HBC adversaries. In the proposed PP-DKF, agents decompose their private information into public and private substates, where only the public substate is shared with neighbors. A noise sequence perturbs the public substate before being shared with neighbors to provide an additional layer of protection. The proposed PP-DKF enhances filtering performance when compared to DKFs employing contemporary privacy-preserving techniques, showing that the method is more robust to noise-injection. Additionally, the PP-DKF improves the privacy level for all agents, defined as the mean squared estimation error of private data at the adversary [21].

Mathematical Notations: Scalars, column vectors, and matrices are denoted by lowercase, bold lowercase, and bold uppercase letters, while $\mathbf{I}$, and $\mathbf{0}$ represent identity and zero matrices, respectively. The transpose and statistical expectation operators are denoted by $(\cdot)^{\mathrm{T}}$ and $\mathbb{E}\{\cdot\}$, while $\otimes$ denotes the matrix Kronecker product. The trace operator is denoted as $\mathsf{tr}(\cdot)$, $\mathsf{diag}(\mathbf{a})$ denotes diagonal matrix whose diagonals are the elements of vector $\mathbf{a}$, and the $\mathsf{Blockdiag}(\{\mathbf{A}_i\}_{i=1}^{N})$ represents a block diagonal matrix containing $\mathbf{A}_i$s on the main diagonal.

This work was supported in part by the Research Council of Norway.

II. Problem Formulation

We consider a set of N interconnected agents that is modeled as a graph $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$ with node set $\mathcal{N}$, representing agents, and edge set $\mathcal{E}$, representing communication links. The neighborhood of agent i is denoted by $\mathcal{N}_i$, with cardinality N_i. We revisit the classical DKF to track a dynamic system state through observations from a network of agents [2], [3], [6]. The state-space model is given by

$$\mathbf{x}_n = \mathbf{A}\mathbf{x}_{n-1} + \mathbf{v}_n \tag{1}$$

$$\mathbf{y}_{i,n} = \mathbf{H}_i\mathbf{x}_n + \mathbf{w}_{i,n} \tag{2}$$

where for time instant n and agent i, $\mathbf{A}$ denotes the state transition matrix, and $\mathbf{H}_i$ denotes the observation matrix, $\mathbf{y}_{i,n}$ is the local observation, and $\mathbf{w}_{i,n}$, $\mathbf{v}_n$, are observation and process noises, respectively. The process noise and observation noise are mutually independent white Gaussian sequences with covariance matrices $\mathbf{C}_{\mathbf{v}_n}$ and $\mathbf{C}_{\mathbf{w}_{i,n}}$, respectively. The proposed PP-DKF is based on the DKF in [5], which requires agents to share local estimates with neighbors and reach a network-wide consensus by local collaboration. Since the shared data includes private information, we propose a PP-DKF that safeguards the private information of individual agents from being estimated by HBC adversaries.

III. Privacy-Preserving Distributed Kalman Filter

Based on the proposed DKF in [5], the proposed PP-DKF tracks a dynamic system state by updating the local model given by

$$\begin{aligned}\hat{\mathbf{x}}_{i,n|n-1} &= \mathbf{A}\hat{\mathbf{x}}_{i,n-1|n-1}\\ \mathbf{M}_{i,n|n-1} &= \mathbf{A}\mathbf{M}_{i,n-1|n-1}\mathbf{A}^T + \mathbf{C}_{\mathbf{v}_n}\end{aligned} \tag{3}$$

where, for agent i, $\hat{\mathbf{x}}_{i,n|n-1}$ and $\hat{\mathbf{x}}_{i,n|n}$ are the respective *a priori* and *a posteriori* state vector estimates and the covariance information of agent i, at time instant n is denoted by $\mathbf{M}_{i,n|n-1}$. Following the centralized Kalman filter in [6], the local covariance information of agent i at time instant n is updated as

$$\mathbf{\Gamma}_{i,n} = \mathbf{M}^{-1}_{i,n|n-1} + N\mathbf{H}_i^T\mathbf{C}^{-1}_{\mathbf{w}_{i,n}}\mathbf{H}_i. \tag{4}$$

Updating the covariance information requires sharing the local covariance $\mathbf{\Gamma}_{i,n}$ to reach the average consensus among agents as $\mathbf{M}^{-1}_{i,n|n} = \frac{1}{N}\sum_{i\in\mathcal{N}}\mathbf{\Gamma}_{i,n}$. The local covariance is not considered as private information and it can be implemented in a distributed manner by employing an average consensus filter (ACF) with K consensus iterations as

$$\mathbf{M}^{-1}_{i,n|n} = \mathbf{\Gamma}_{i,n}(K) \leftarrow \boxed{\text{ACF}} \leftarrow \{\forall j \in \mathcal{N}_i : \mathbf{\Gamma}_{j,n}(0) = \mathbf{\Gamma}_{j,n}\}$$

where the operation at each consensus iteration k is given as $\mathbf{\Gamma}_{i,n}(k) = q_{ii}\mathbf{\Gamma}_{i,n}(k-1) + \sum_{j\in\mathcal{N}_i} q_{ij}\mathbf{\Gamma}_{j,n}(k-1)$ with consensus weights satisfying $q_{ii} + \sum_{j\in\mathcal{N}_i} q_{ij} = 1$ for each agent i. It is assumed that the conditions for convergence of $\mathbf{M}_{i,n|n}$ for all agents are satisfied, as given in [5]. The updated covariance is then used to evolve the intermediate state vector estimate of agent i at time instant n as

$$\boldsymbol{\psi}_{i,n} = \hat{\mathbf{x}}_{i,n|n-1} + \mathbf{G}_{i,n}\left(\mathbf{y}_{i,n} - \mathbf{H}_i\hat{\mathbf{x}}_{i,n|n-1}\right) \tag{5}$$

where $\mathbf{G}_{i,n} = N\mathbf{M}_{i,n|n}\mathbf{H}_i^T\mathbf{C}^{-1}_{\mathbf{w}_{i,n}}$ is the local gain. Subsequently, the state vector estimate needs to reach the average consensus among agents as $\hat{\mathbf{x}}_{i,n|n} = \frac{1}{N}\sum_{i\in\mathcal{N}}\boldsymbol{\psi}_{i,n}$, which requires agents to share their intermediate state vector estimate $\boldsymbol{\psi}_{i,n}$ among neighbors. Since $\boldsymbol{\psi}_{i,n}$ includes private information, it needs to be protected from adversaries.

To reach the average consensus of intermediate state vector estimates, the PP-DKF instructs each agent i to decompose its initial information $\mathbf{r}_{i,n}(0) = \boldsymbol{\psi}_{i,n}$ into public and private substates $\boldsymbol{\alpha}_{i,n}(0)$ and $\boldsymbol{\beta}_{i,n}(0)$, respectively. The initial substates are chosen such that $\boldsymbol{\alpha}_{i,n}(0) + \boldsymbol{\beta}_{i,n}(0) = 2\mathbf{r}_{i,n}(0)$ is satisfied [15]. The public substate $\boldsymbol{\alpha}_{i,n}$ is shared with neighbors, while the private substate $\boldsymbol{\beta}_{i,n}$ evolves internally without being observed by neighbors. We perturb the public substate before sharing with neighbors with a noise sequence $\boldsymbol{\omega}_i(k)$ at the ith agent and kth consensus iteration in order to further protect the private information. The designed noise structure is

$$\boldsymbol{\omega}_i(k) = \phi^k\boldsymbol{\nu}_i(k) - \phi^{k-1}\boldsymbol{\nu}_i(k-1), \ \ \forall k \geq 1 \tag{6}$$

where $\boldsymbol{\omega}_i(0) = \boldsymbol{\nu}_i(0)$, $\boldsymbol{\nu}_i(k) \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$ is an independent and identically distributed Gaussian sequence for each $i \in \mathcal{N}$, and $\phi \in (0,1)$ is a common constant. As a result, each agent i updates its substates at the kth consensus iteration by injecting (6) into the public substate before sharing with the neighbors as follows:

$$\begin{cases}\boldsymbol{\alpha}_{i,n}(k+1) = & \boldsymbol{\alpha}_{i,n}(k) + \varepsilon\displaystyle\sum_{j\in\mathcal{N}_i} w_{ij}\left(\tilde{\boldsymbol{\alpha}}_{j,n}(k) - \boldsymbol{\alpha}_{i,n}(k)\right)\\ & +\varepsilon\mathbf{U}_i\left(\boldsymbol{\beta}_{i,n}(k) - \boldsymbol{\alpha}_{i,n}(k)\right)\\ \boldsymbol{\beta}_{i,n}(k+1) = & \boldsymbol{\beta}_{i,n}(k) + \varepsilon\mathbf{U}_i\left(\boldsymbol{\alpha}_{i,n}(k) - \boldsymbol{\beta}_{i,n}(k)\right)\end{cases} \tag{7}$$

where $\tilde{\boldsymbol{\alpha}}_{j,n}(k) = \boldsymbol{\alpha}_{j,n}(k) + \boldsymbol{\omega}_j(k)$ is the received information from the jth neighbor and $\varepsilon \in (0, 1/(\Delta+1)]$ with $\Delta \triangleq \max_{i\in\mathcal{N}} N_i$ is the consensus parameter. The interaction weight is denoted by w_{ij}, while $\mathbf{U}_i \triangleq \mathsf{diag}(\mathbf{u}_i)$ is a diagonal matrix containing the the coupling weight vector of the ith agent. The coupling weight vector $\mathbf{u}_i \in \mathbb{R}^m$ contains independent elements that control the level of contribution of each substate in the updating procedure. In addition, we require a scalar $\eta \in (0,1)$, such that all nonzero $w_{ij} = w_{ji}$ and all elements of $\mathbf{u}_i$ reside in the range $[\eta, 1)$, [15]. After repeating the steps in (7) for a sufficient number of iterations, say K iterations, the local state estimate, $\hat{\mathbf{x}}_{i,n|n}$, is updated as $\hat{\mathbf{x}}_{i,n|n} = \boldsymbol{\alpha}_{i,n}(K)$ for all $i \in \mathcal{N}$. The operations of the proposed PP-DKF is summarized in Algorithm 1.

Theorem 1: The privacy-preserving average consensus operations in Algorithm 1 converges to the exact average consensus value, asymptotically.

$$\lim_{k\to\infty}\mathbb{E}\{\boldsymbol{\alpha}_{i,n}(k)\} = \lim_{k\to\infty}\mathbb{E}\{\boldsymbol{\beta}_{i,n}(k)\} = \frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\psi}_{i,n}. \tag{8}$$

Proof: To show the convergence of the derived privacy-preserving ACF operations to the exact average consensus value, we first show that the sum of all substates is constant,

Algorithm 1: Privacy-Preserving Distributed Kalman Filter

Model update: For each $i \in \mathcal{N}$

$\hat{\mathbf{x}}_{i,n|n-1} = \mathbf{A}\hat{\mathbf{x}}_{i,n-1|n-1}$

$\mathbf{M}_{i,n|n-1} = \mathbf{A}\mathbf{M}_{i,n-1|n-1}\mathbf{A}^T + \mathbf{C}_{\mathbf{v}_n}$

$\mathbf{\Gamma}_{i,n} = \mathbf{M}^{-1}_{i,n|n-1} + N\mathbf{H}_i^T\mathbf{C}^{-1}_{\mathbf{w}_{i,n}}\mathbf{H}_i$

$\mathbf{M}^{-1}_{i,n|n} \leftarrow \boxed{\text{ACF}} \leftarrow \{\forall j \in \mathcal{N}_i : \mathbf{\Gamma}_{j,n}\}$

$\mathbf{G}_{i,n} = N\mathbf{M}_{i,n|n}\mathbf{H}_i^T\mathbf{C}^{-1}_{\mathbf{w}_{i,n}}$

$\boldsymbol{\psi}_{i,n} = \hat{\mathbf{x}}_{i,n|n-1} + \mathbf{G}_{i,n}\left(\mathbf{y}_{i,n} - \mathbf{H}_i\hat{\mathbf{x}}_{i,n|n-1}\right)$

Set $\mathbf{r}_{i,n}(0) = \boldsymbol{\psi}_{i,n}$

Privacy-Preserving ACF:

Select $\boldsymbol{\alpha}_{i,n}(0)$ and set $\boldsymbol{\beta}_{i,n}(0) = 2\mathbf{r}_{i,n}(0) - \boldsymbol{\alpha}_{i,n}(0)$

Share $\tilde{\boldsymbol{\alpha}}_{i,n}(0) = \boldsymbol{\alpha}_{i,n}(0) + \boldsymbol{\omega}_i(0)$

for $k = 1, \ldots, K$ **do**

  Receive $\tilde{\boldsymbol{\alpha}}_{j,n}(k-1)$, $\forall j \in \mathcal{N}_i$

  Update $\boldsymbol{\alpha}_{i,n}(k)$ and $\boldsymbol{\beta}_{i,n}(k)$, as given in (7)

  Share $\tilde{\boldsymbol{\alpha}}_{i,n}(k) = \boldsymbol{\alpha}_{i,n}(k) + \boldsymbol{\omega}_i(k)$

end

$\hat{\mathbf{x}}_{i,n|n} = \boldsymbol{\alpha}_{i,n}(K)$

asymptotically [15]. The sum of all substates at the kth iteration is defined as $\boldsymbol{\zeta}_n(k) \triangleq \sum_{i=1}^{N}(\boldsymbol{\alpha}_{i,n}(k) + \boldsymbol{\beta}_{i,n}(k))$ where

$$\boldsymbol{\zeta}_n(k) = \boldsymbol{\zeta}_n(0) + \varepsilon \sum_{i=1}^{N}\sum_{l=1}^{k-1} d_i\, \boldsymbol{\omega}_i(l).$$

with $d_i = \sum_{j\in\mathcal{N}_i} w_{ij}$. Given the zero mean and decaying covariance properties of the designed noise (6), $\boldsymbol{\zeta}_n(k)$ converges to $\boldsymbol{\zeta}_n(0)$ in the mean square sense which is $\lim_{k\to\infty}\mathbb{E}\{\|\boldsymbol{\zeta}_n(k) - \boldsymbol{\zeta}_n(0)\|^2\} = \mathbf{0}$. Subsequently, due to the connected network assumption and considering that $\boldsymbol{\alpha}_{i,n}(0) + \boldsymbol{\beta}_{i,n}(0) = 2\boldsymbol{\psi}_{i,n}$, the ith agent substates, $\boldsymbol{\alpha}_{i,n}$ and $\boldsymbol{\beta}_{i,n}$, converge to the desired average consensus value [15], as in (8). ■

IV. Performance Evaluation

With the equivalent network model of $2N$ agents, each private substate corresponds to an agent only attached to its peer in the original network, we evaluate the effects of incorporating privacy-preserving operations on the filtering performance. It is assumed that the imaginary agents have the same observation parameters, $\mathbf{y}_{i,n}$, $\mathbf{H}_i$, and $\mathbf{C}_{\mathbf{w}_i}$, with their original peers. We also assume that agents start privacy-preserving steps with equal substates, $\boldsymbol{\alpha}_{i,n}(0) = \boldsymbol{\beta}_{i,n}(0) = \boldsymbol{\psi}_{i,n}$, so that their intermediate estimation error is equal to

$$\begin{aligned}\boldsymbol{\epsilon}_{i,n} =& \mathbf{x}_n - \boldsymbol{\alpha}_{i,n}(0) \qquad i = 1, \cdots, N\\ \boldsymbol{\epsilon}_{i,n} =& \mathbf{x}_n - \boldsymbol{\beta}_{i-N,n}(0) \quad i = N+1, \cdots, 2N\end{aligned}$$

Based on the local observation in (2) and substituting the intermediate state in (5), the intermediate estimation error of each agent, $\boldsymbol{\epsilon}_{i,n} = \mathbf{x}_n - \boldsymbol{\psi}_{i,n}$, is formulated as

$$\begin{aligned}\boldsymbol{\epsilon}_{i,n} =& \mathbf{x}_n - \hat{\mathbf{x}}_{i,n|n-1} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{H}_i\left(\mathbf{x}_n - \hat{\mathbf{x}}_{i,n|n-1}\right)\\ &- N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{w}_{i,n} \qquad (9)\\ =& \left(\mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{H}_i\right)\mathbf{A}\boldsymbol{\epsilon}_{i,n-1|n-1} \qquad (10)\\ &+ \left(\mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{H}_i\right)\mathbf{v}_n - \mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{w}_{i,n}.\end{aligned}$$

where $\boldsymbol{\epsilon}_{i,n-1|n-1} = \mathbf{x}_{n-1} - \hat{\mathbf{x}}_{i,n-1|n-1}$. Assuming the stacked vectors organizing all error terms as $\boldsymbol{\mathcal{E}}_n \triangleq [\boldsymbol{\epsilon}^{\mathrm{T}}_{1,n}, \cdots, \boldsymbol{\epsilon}^{\mathrm{T}}_{2N,n}]^{\mathrm{T}}$ and $\boldsymbol{\mathcal{E}}_{n-1|n-1} \triangleq [\boldsymbol{\epsilon}^{\mathrm{T}}_{1,n-1|n-1}, \cdots, \boldsymbol{\epsilon}^{\mathrm{T}}_{2N,n-1|n-1}]^{\mathrm{T}}$, the network-wide state vector estimation error, $\boldsymbol{\mathcal{E}}_{n|n}$, which is the stacked error after the privacy-preserving ACF operations in (7) with k consensus iterations, is formulated as

$$\begin{aligned}\boldsymbol{\mathcal{E}}_{n|n} =& \mathbf{G}^k\boldsymbol{\mathcal{E}}_n + \phi^{k-1}\boldsymbol{\mathcal{B}}\boldsymbol{\nu}(k-1)\\ &+ \sum_{s=2}^{k}\phi^{k-s}\left(\mathbf{G}^{s-1} - \mathbf{G}^{s-2}\right)\boldsymbol{\mathcal{B}}\boldsymbol{\nu}(k-s)\end{aligned} \qquad (11)$$

where $\boldsymbol{\nu}(k) = [\boldsymbol{\nu}_1^{\mathrm{T}}(k), \cdots, \boldsymbol{\nu}_N^{\mathrm{T}}(k)]^{\mathrm{T}}$, $\boldsymbol{\mathcal{B}} = [\varepsilon\mathbf{W}, \mathbf{0}]^{\mathrm{T}} \otimes \mathbf{I}$, and $\mathbf{G}$ is a doubly stochastic matrix given by

$$\mathbf{G} = \begin{bmatrix}\mathbf{M} & \varepsilon\mathbf{U}\\ \varepsilon\mathbf{U} & \mathbf{I} - \varepsilon\mathbf{U}\end{bmatrix} \qquad (12)$$

with $\mathbf{M} \triangleq (\mathbf{I}_N - \varepsilon(\mathbf{D} - \mathbf{W})) \otimes \mathbf{I} - \varepsilon\mathbf{U}$, $\mathbf{U} = \mathsf{Blockdiag}(\{\mathbf{U}_i\}_{i=1}^N)$, $\mathbf{D} = \mathsf{diag}(\{d_i\}_{i=1}^N)$, and $\mathbf{W}$ as the interaction weight matrix consisting all weights w_{ij}. Substituting the network-wide intermediate state vector estimation error $\boldsymbol{\mathcal{E}}_n$ from (10) into (11) results

$$\begin{aligned}\boldsymbol{\mathcal{E}}_{n|n} =& \boldsymbol{\mathcal{P}}\boldsymbol{\mathcal{E}}_{n-1|n-1} + \boldsymbol{\theta}_n - \boldsymbol{\mu}_n + \phi^{k-1}\boldsymbol{\mathcal{B}}\boldsymbol{\nu}(k-1)\\ &+ \sum_{s=2}^{k}\phi^{k-s}\left(\mathbf{G}^{s-1} - \mathbf{G}^{s-2}\right)\boldsymbol{\mathcal{B}}\boldsymbol{\nu}(k-s)\end{aligned} \qquad (13)$$

where $\boldsymbol{\mathcal{P}} = \mathbf{G}^k\mathsf{Blockdiag}(\{\mathbf{P}_i\mathbf{A}\}_{i=1}^{2N})$ and

$$\begin{aligned}\boldsymbol{\theta}_n &= \mathbf{G}^k\mathsf{Blockdiag}(\{\mathbf{P}_i\}_{i=1}^{2N})[\mathbf{v}_n^{\mathrm{T}}, \cdots, \mathbf{v}_n^{\mathrm{T}}]^{\mathrm{T}}\\ \boldsymbol{\mu}_n &= \mathbf{G}^k\mathsf{Blockdiag}(\{\mathbf{Q}_i\}_{i=1}^{2N})[\mathbf{w}_{1,n}^{\mathrm{T}}, \cdots, \mathbf{w}_{2N,n}^{\mathrm{T}}]^{\mathrm{T}}\end{aligned}$$

with $\mathbf{P}_i = \mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}\mathbf{H}_i$ and $\mathbf{Q}_i = \mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}^{-1}_{\mathbf{w}_i}$. Since $\mathbf{P}_i$ is stable and $\mathbf{G}$ is doubly stochastic, the block matrix $\boldsymbol{\mathcal{P}}$ is stable; thus, the statistical expectation of any vector norm for $\boldsymbol{\mathcal{E}}_{n|n}$ converges to a stabilizing value, as $n \to \infty$. Taking the statistical expectation of (13) yields

$$\mathbb{E}\{\boldsymbol{\mathcal{E}}_{n|n}\} = \boldsymbol{\mathcal{P}}\mathbb{E}\{\boldsymbol{\mathcal{E}}_{n-1|n-1}\} = \boldsymbol{\mathcal{P}}^n\mathbb{E}\{\boldsymbol{\mathcal{E}}_{0|0}\}.$$

Since $\boldsymbol{\mathcal{P}}$ is stable, we have $\lim_{n\to\infty}\mathbb{E}\{\boldsymbol{\mathcal{E}}_{n|n}\} = 0$ that indicates the steady-state estimates are unbiased regardless of their initializing values or perturbation sequences.

The second-order statistics of all agents is formulated by defining $\boldsymbol{\Sigma}_n = \mathbb{E}\{\boldsymbol{\mathcal{E}}_{n|n}\boldsymbol{\mathcal{E}}^{\mathrm{T}}_{n|n}\}$ and given by

$$\begin{aligned}\boldsymbol{\Sigma}_n =& \boldsymbol{\mathcal{P}}\boldsymbol{\Sigma}_{n-1}\boldsymbol{\mathcal{P}}^{\mathrm{T}} + \mathbb{E}\{\boldsymbol{\theta}_n\boldsymbol{\theta}_n^{\mathrm{T}}\} + \mathbb{E}\{\boldsymbol{\mu}_n\boldsymbol{\mu}_n^{\mathrm{T}}\}\\ &+ \sum_{s=2}^{k}\phi^{2(k-s)}\boldsymbol{\mathcal{T}}_s + \phi^{2(k-1)}\boldsymbol{\mathcal{B}}\mathbf{C}_{\boldsymbol{\nu}}\boldsymbol{\mathcal{B}}^{\mathrm{T}}\end{aligned} \qquad (14)$$

with $\mathbf{C}_{\boldsymbol{\nu}} = \mathbb{E}\{\boldsymbol{\nu}(s)\boldsymbol{\nu}^{\mathrm{T}}(s)\}$ at each consensus iteration s and $\boldsymbol{\mathcal{T}}_s = \left(\mathbf{G}^{s-1} - \mathbf{G}^{s-2}\right)\boldsymbol{\mathcal{B}}\mathbf{C}_{\boldsymbol{\nu}}\boldsymbol{\mathcal{B}}^{\mathrm{T}}\left(\mathbf{G}^{s-1} - \mathbf{G}^{s-2}\right)^{\mathrm{T}}$. Since $\mathbf{G}$ is doubly stochastic and $\boldsymbol{\mathcal{P}}$ is stable, $\boldsymbol{\Sigma}_n \to \boldsymbol{\Sigma}$ as $n \to \infty$, where $\boldsymbol{\Sigma}$ is the solution of the discrete-time Lyapunov equation in (14). Compared with the non-private approach, the effect of injected noise is manifested as a rise in the steady-state mean square error (MSE) of Algorithm 1. In the next section, we examine the performance of the derived framework to preserve agent privacy.

V. Privacy Analysis

We consider an HBC agent that can access the interaction weights and exchanged information of its neighbors. To benchmark the privacy of the derived PP-DKF, we consider the MSE associated with the estimates of the initial states $\boldsymbol{\psi}_n = [\boldsymbol{\psi}_{1,n}^{\mathrm{T}}, \cdots, \boldsymbol{\psi}_{N,n}^{\mathrm{T}}]^{\mathrm{T}}$ at the HBC agent as a privacy metric. Without loss of generality, we assume that the Nth agent is an HBC agent that attempts to estimate the initial states of all agents using the accessible information set $\mathcal{I}(k) = \{\boldsymbol{\alpha}_{N,n}(k), \boldsymbol{\beta}_{N,n}(k), \boldsymbol{\omega}_N(k), \mathbf{u}_N, w_{Nj}, \tilde{\boldsymbol{\alpha}}_{j,n}(k) : \forall j \in \mathcal{N}_N\}$ at each consensus iteration k. We introduce the observation vector $\mathbf{y}_n(k)$ that includes the accessible information transferred to the HBC agent at each iteration k as

$$\mathbf{y}_n(k) = \mathbf{C}\mathbf{z}_n(k) + \mathbf{C}_\alpha \boldsymbol{\omega}(k) \tag{15}$$

where $\mathbf{C} \triangleq [\mathbf{C}_\alpha, \mathbf{C}_\beta]$ with $\mathbf{C}_\beta = [\mathbf{0}, \mathbf{e}_N]^{\mathrm{T}} \otimes \mathbf{I}$ and $\mathbf{C}_\alpha = [\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_{N_N}}, \mathbf{e}_N]^{\mathrm{T}} \otimes \mathbf{I}$. The canonical basis $\mathbf{e}_i \in \mathbb{R}^N$ is a vector with 1 in the ith entry and zeros elsewhere, while $\mathbf{z}_n(k) \triangleq [\boldsymbol{\alpha}_n^{\mathrm{T}}(k), \boldsymbol{\beta}_n^{\mathrm{T}}(k)]^{\mathrm{T}}$ with the network-wide agent substate vectors given as

$$\begin{aligned}\boldsymbol{\alpha}_n(k) &\triangleq [\boldsymbol{\alpha}_{1,n}^{\mathrm{T}}(k), \cdots, \boldsymbol{\alpha}_{N,n}^{\mathrm{T}}(k)]^{\mathrm{T}} \\ \boldsymbol{\beta}_n(k) &\triangleq [\boldsymbol{\beta}_{1,n}^{\mathrm{T}}(k), \cdots, \boldsymbol{\beta}_{N,n}^{\mathrm{T}}(k)]^{\mathrm{T}}.\end{aligned}$$

The estimated value of $\mathbf{z}_n(0)$, i.e., $\hat{\mathbf{z}}_n(0) \triangleq [\hat{\boldsymbol{\alpha}}_n^{\mathrm{T}}(0), \hat{\boldsymbol{\beta}}_n^{\mathrm{T}}(0)]^{\mathrm{T}}$, is then used to estimate the initial state of the agents as $\hat{\boldsymbol{\psi}}_n = \frac{1}{2}(\hat{\boldsymbol{\alpha}}_n(0) + \hat{\boldsymbol{\beta}}_n(0))$. Substituting the network-wide substate update equations in (7) into (15) results

$$\mathbf{y}_n(k) = \mathbf{C}\mathbf{G}^k \mathbf{z}_n(0) + \mathbf{C}_\alpha \sum_{t=0}^{k-1} \boldsymbol{\mathcal{C}}_{k-1-t} \mathbf{B} \boldsymbol{\omega}(t) + \mathbf{C}_\alpha \boldsymbol{\omega}(k) \tag{16}$$

where $\boldsymbol{\mathcal{C}}_k = \begin{bmatrix}\mathbf{I} & \mathbf{0}\end{bmatrix} \mathbf{G}^k \begin{bmatrix}\mathbf{I} & \mathbf{0}\end{bmatrix}^{\mathrm{T}}$ and $\mathbf{B} = \varepsilon \mathbf{W} \otimes \mathbf{I}$. Since $\boldsymbol{\nu}(k)$ is a zero-mean i.i.d. sequence, the accumulated observation of the HBC agent set-up at consensus iteration k, $\tilde{\mathbf{y}}_n(k) = \sum_{t=0}^{k} \mathbf{y}_n(t)$, is simplified as

$$\tilde{\mathbf{y}}_n(k) = \mathbf{C}(\mathbf{I} - \mathbf{G})^{k+1}(\mathbf{I} - \mathbf{G})^{-1} \mathbf{z}_n(0) + \mathbf{C}_\alpha \tilde{\boldsymbol{\nu}}(k) \tag{17}$$

where $\tilde{\boldsymbol{\nu}}(k) = \sum_{t=0}^{k-1} \phi^t \boldsymbol{\mathcal{C}}_{k-1-t} \mathbf{B} \boldsymbol{\nu}(t) + \phi^k \boldsymbol{\nu}(k)$. Stacking all the available accumulated observations at each consensus iteration k in a vector, $\bar{\mathbf{y}}_n(k) = [\tilde{\mathbf{y}}_n^{\mathrm{T}}(0), \ldots, \tilde{\mathbf{y}}_n^{\mathrm{T}}(k)]^{\mathrm{T}}$, gives

$$\bar{\mathbf{y}}_n(k) = \mathbf{H}(k)\mathbf{z}(0) + \mathbf{F}(k)\bar{\boldsymbol{\nu}}(k) \tag{18}$$

where $\mathbf{H}(k) = (\mathbf{I} \otimes \mathbf{C})[\mathbf{H}_0^{\mathrm{T}}, \mathbf{H}_1^{\mathrm{T}}, \ldots, \mathbf{H}_k^{\mathrm{T}}]^{\mathrm{T}}$ with $\mathbf{H}_k = \sum_{t=0}^{k} \mathbf{G}^t$, $\bar{\boldsymbol{\nu}}(k) = [\boldsymbol{\nu}^{\mathrm{T}}(0), \cdots, \boldsymbol{\nu}^{\mathrm{T}}(k)]^{\mathrm{T}}$, and

$$\mathbf{F}(k) = \begin{bmatrix} \mathbf{C}_\alpha & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{C}_\alpha \boldsymbol{\mathcal{C}}_0 \mathbf{B} & \phi \mathbf{C}_\alpha & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{C}_\alpha \boldsymbol{\mathcal{C}}_{k-1} \mathbf{B} & \phi \mathbf{C}_\alpha \boldsymbol{\mathcal{C}}_{k-2} \mathbf{B} & \cdots & \phi^k \mathbf{C}_\alpha \end{bmatrix}.$$

With the perfect observation matrix $\mathbf{H}(k)$ available, the estimate of initial substates $\mathbf{z}_n(0)$ could be modeled as

$$\hat{\mathbf{z}}_n(0) = \mathbf{H}^{\dagger}(k)(\mathbf{H}(k)\mathbf{z}_n(0) + \mathbf{F}(k)\bar{\boldsymbol{\nu}}(k)) \tag{19}$$

where $\mathbf{H}^{\dagger}(k)$ is the Moore–Penrose pseudoinverse of $\mathbf{H}(k)$. However, since the HBC agent does not have access to the coupling weight matrix $\mathbf{U}$, it has to estimate the observation matrix $\mathbf{H}(k)$. Following the estimation procedure in [22], the HBC agent estimates the coupling weight matrix as $\hat{\mathbf{U}} = \mathbf{U} + \boldsymbol{\Delta}_{\mathbf{U}}$ where $\boldsymbol{\Delta}_{\mathbf{U}}$ shows its uncertainty to determine the coupling weight matrix $\mathbf{U}$.

An estimate of matrix $\mathbf{G}$ is obtained using uncertainty modeling above as $\hat{\mathbf{G}} = \mathbf{G} + \varepsilon \boldsymbol{\Delta}_{\mathbf{G}_1}$ where $\boldsymbol{\Delta}_{\mathbf{G}_1} = -\boldsymbol{\mathcal{L}}^{\mathrm{T}} \boldsymbol{\Delta}_{\mathbf{U}} \boldsymbol{\mathcal{L}}$ with $\boldsymbol{\mathcal{L}} = [-\mathbf{I}, \mathbf{I}]$. Employing the binomial expansion, the uncertainty of $\hat{\mathbf{G}}^k$ is simplified as $\hat{\mathbf{G}}^k = \mathbf{G}^k + \varepsilon \boldsymbol{\Delta}_{\mathbf{G}_k}$ where

$$\boldsymbol{\Delta}_{\mathbf{G}_k} = \sum_{t=1}^{k} \frac{k! \varepsilon^{t-1}}{(k-t)!t!} \mathbf{G}^{k-t} \boldsymbol{\Delta}_{\mathbf{G}_1}^t \quad \forall k \geq 2.$$

Thus, estimate of the observation matrix $\mathbf{H}(k)$ is formulated as $\hat{\mathbf{H}}(k) = \mathbf{H}(k) + \varepsilon \boldsymbol{\Delta}_{\mathbf{H}}(k)$ where $\boldsymbol{\Delta}_{\mathbf{H}}(k)$ denotes the uncertainty of the observation matrix, independent of $\mathbf{H}(k)$, and is computed as $\boldsymbol{\Delta}_{\mathbf{H}}(k) = (\mathbf{I} \otimes \mathbf{C})[\mathbf{0}, \boldsymbol{\Delta}_{\mathbf{G}_1}^{\mathrm{T}}, \ldots, \sum_{t=1}^{k} \boldsymbol{\Delta}_{\mathbf{G}_t}^{\mathrm{T}}]^{\mathrm{T}}$. Subsequently, the estimate of the initial substates in (19) is reformulated as $\hat{\mathbf{z}}_n(0) = \hat{\mathbf{H}}^{\dagger}(k)\bar{\mathbf{y}}_n(k)$ where $\hat{\mathbf{H}}^{\dagger}(k) = (\mathbf{H}(k) + \boldsymbol{\Delta}_{\mathbf{H}}(k))^{\dagger}$. The HBC agent is a legitimate agent of the network and knows the distribution of coupling weights. Given a negligible uncertainty in $\hat{\mathbf{H}}(k)$, the pseudo-inverse of $\hat{\mathbf{H}}(k)$ can be approximated by the first order Taylor expansion as $\hat{\mathbf{H}}^{\dagger}(k) \cong \mathbf{H}^{\dagger}(k)\left(\mathbf{I} - \varepsilon \boldsymbol{\Delta}_{\mathbf{H}}(k)\mathbf{H}^{\dagger}(k)\right)$ and subsequently, we have $\hat{\mathbf{z}}_n(0) = \left(\mathbf{H}^{\dagger}(k) - \varepsilon \mathbf{H}^{\dagger}(k)\boldsymbol{\Delta}_{\mathbf{H}}(k)\mathbf{H}^{\dagger}(k)\right)\mathbf{y}_n(k)$ which can be further simplified as

$$\hat{\mathbf{z}}_n(0) = \mathbf{z}_n(0) + \boldsymbol{\eta}(k) \tag{20}$$

with the estimation error of the initial substates

$$\begin{aligned}\boldsymbol{\eta}(k) =& \mathbf{H}^{\dagger}(k)\mathbf{F}(k)\bar{\boldsymbol{\nu}}(k) - \varepsilon \mathbf{H}^{\dagger}(k)\boldsymbol{\Delta}_{\mathbf{H}}(k)\mathbf{z}_n(0) \\ &- \varepsilon \mathbf{H}^{\dagger}(k)\boldsymbol{\Delta}_{\mathbf{H}}(k)\mathbf{H}^{\dagger}(k)\mathbf{F}(k)\bar{\boldsymbol{\nu}}(k).\end{aligned}$$

For the worst-case scenario, when the HBC agent knows the exact coupling weights of the entire network, i.e., $\boldsymbol{\Delta}_{\mathbf{U}} = \mathbf{0}$, the estimation error covariance $\mathbf{P}(k) = \mathbb{E}\{\boldsymbol{\eta}(k)\boldsymbol{\eta}^{\mathrm{T}}(k)\}$ is computed as

$$\mathbf{P}(k) = \sigma^2 \left(\mathbf{H}^{\mathrm{T}}(k)\left(\mathbf{F}(k)\mathbf{F}^{\mathrm{T}}(k)\right)^{-1}\mathbf{H}(k)\right)^{-1}. \tag{21}$$

As a result, the privacy of the jth agent, pertaining to estimate its initial information $\boldsymbol{\psi}_{j,n}$, is defined as

$$\mathcal{E}_j(k) \triangleq \mathrm{tr}\left((\mathbf{e}_j^{\mathrm{T}} \otimes \mathbf{I})\bar{\mathbf{P}}(k)(\mathbf{e}_j \otimes \mathbf{I})\right), \tag{22}$$

where $\bar{\mathbf{P}}(k) = \frac{1}{4}[\mathbf{I}, \mathbf{I}]\mathbf{P}(k)[\mathbf{I}, \mathbf{I}]^{\mathrm{T}}$.

VI. Numerical Results

We consider a connected network with $L = 5$ agents and edge set $\mathcal{E} = \{(1,2), (2,3), (3,4), (4,5), (5,1)\}$. The proposed PP-DKF is considered in a collaborative target tracking application as given in [5]. To illustrate the benefits of state-decomposition and noise perturbation, characterizing the PP-DKF, we also implemented a pure noise-injection-based privacy-preserving DKF (NIP-DKF), wherein the noise sequence in (6) perturbed the shared messages of the conventional DKF in [5]. If not stated otherwise, $K = 40$ consensus iterations and $\phi = 0.9$ are employed.

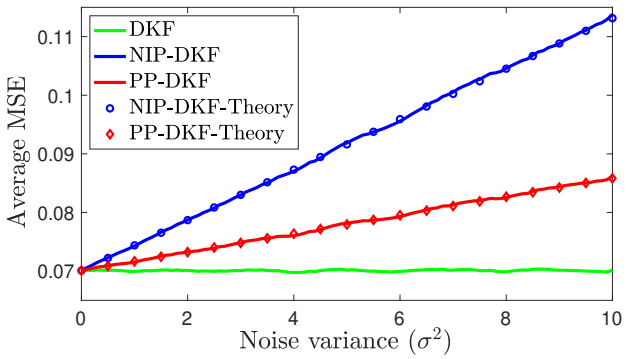

Fig. 1. Average MSE versus noise variance σ^2.

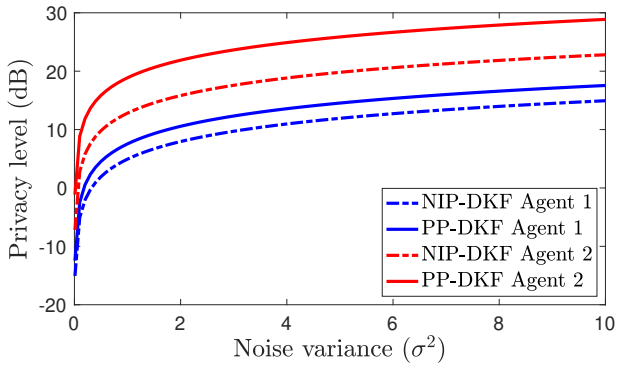

Fig. 2. Privacy metric $\mathcal{E}_j(k)$ versus noise variance σ^2.

Fig. 1 shows the average MSE of the various distributed Kalman filters versus the injected noise variance. We see that the PP-DKF has a better filtering performance than NIP-DKF and achieves an MSE close to the non-private DKF for a broad range of injected noise variances. Also, our theoretical prediction in (14) match the simulation results. The agent privacy $\mathcal{E}_j(k)$ in (22), considering the 5th agent as an HBC agent, is shown in Fig. 2. It shows that injecting more noise results in higher privacy and PP-DKF improves agent privacy compared to NIP-DKF settings. Because of the symmetric topology of the ring network, agents 3 and 4 achieve the same level of privacy as agents 2 and 1, respectively, so they are omitted from Fig.2.

VII. Conclusion

This paper proposed a privacy-preserving distributed Kalman filter that employs decomposition-based and noise injection-based privacy-preserving average consensus techniques to protect private information of agents. It restricts the amount of information exchanged with decomposition and conceals the private data from being estimated by adversaries with perturbation. The convergence and performance of the PP-DKF have been analyzed. Moreover, the achieved privacy level of each agent has been defined as the uncertainty of the honest-but-curious agent in estimating the initial state of other agents. It has been shown that the proposed PP-DKF solution improves privacy and performance of the Kalman filtering operations compared to the DKFs employing contemporary privacy-preserving consensus techniques. Lastly, several simulations verified the obtained theoretical results.

References

[1] V. Katewa, F. Pasqualetti, and V. Gupta, "On privacy vs. cooperation in multi-agent systems," *Int. J. of Control*, vol. 91, no. 7, pp. 1693–1707, Jul. 2018.

[2] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," in *Proc. 46th IEEE Conf. Decis. and Control*, 2007, pp. 5492–5498.

[3] F. S. Cattivelli and A. H. Sayed, "Diffusion strategies for distributed Kalman filtering and smoothing," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2069–2084, Sept. 2010.

[4] U. A. Khan and J. M. Moura, "Distributing the Kalman filter for large-scale systems," *IEEE Trans. Signal Process.*, vol. 56, no. 10, pp. 4919–4935, Oct. 2008.

[5] S. P. Talebi and S. Werner, "Distributed Kalman filtering and control through embedded average consensus information fusion," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4396–4403, Oct. 2019.

[6] R. Olfati-Saber, "Distributed Kalman filter with embedded consensus filters," in *Proc. 44th IEEE Conf. Decis. and Control*, 2005, pp. 8179–8184.

[7] R. Olfati-Saber, "Kalman-consensus filter: Optimality, stability, and performance," in *Proc. 48th IEEE Conf. Decis. and Control (CDC)*, 2009, pp. 7036–7042.

[8] J. He, L. Cai, P. Cheng, J. Pan, and L. Shi, "Distributed privacy-preserving data aggregation against dishonest nodes in network systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1462–1470, Apr. 2019.

[9] A. Moradi, N. K. Venkategowda, and S. Werner, "Coordinated data-falsification attacks in consensus-based distributed Kalman filtering," in *Proc. 8th IEEE Int. Workshop Comput. Advances Multi-Sensor Adaptive Process. (CAMSAP)*, 2019, pp. 495–499.

[10] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Trans. Signal Process.*, vol. 68, pp. 4069–4082, 2020.

[11] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.

[12] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[13] J. He, L. Cai, and X. Guan, "Preserving data-privacy with added noises: Optimal estimation and privacy analysis," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5677–5690, Aug. 2018.

[14] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan, "Privacy-preserving average consensus: privacy analysis and algorithm design," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 1, pp. 127–138, Mar. 2019.

[15] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, Nov. 2019.

[16] W. Wang, D. Li, X. Wu, and S. Xue, "Average consensus for switching topology networks with privacy protection," in *Proc. IEEE Chinese Automat. Congr. (CAC)*, 2019, pp. 1098–1102.

[17] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[18] J. Le Ny, "Differentially private Kalman filtering," in *Differential Privacy for Dynamic Data*. Springer, 2020, pp. 55–75.

[19] K. H. Degue and J. Le Ny, "On differentially private Kalman filtering," in *Proc. 5th IEEE Global Conf. Signal and Inf. Process. (GlobalSIP)*, 2017, pp. 487–491.

[20] Y. Song, C. X. Wang, and W. P. Tay, "Privacy-aware kalman filtering," in *Proc. 43rd IEEE Int. Conf. Acoust., Speech and Signal Process. (ICASSP)*, 2018, pp. 4434–4438.

[21] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," *ACM Comput. Surveys (CSUR)*, vol. 51, no. 3, pp. 1–38, Jun. 2018.

[22] C. Wang, E. K. Au, R. D. Murch, W. H. Mow, R. S. Cheng, and V. Lau, "On the performance of the mimo zero-forcing receiver in the presence of channel estimation error," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 805–810, Mar. 2007.