Securing the Distributed Kalman Filter Against Curious Agents

Ashkan Moradi[1], Naveen K. D. Venkategowda[2], Sayed Pouria Talebi[1] and Stefan Werner[1]
[1]Department of Electronic Systems, Norwegian University of Science and Technology, Trondheim, Norway
[2]Linköping University, Norrköping, Sweden
E-mail: {ashkan.moradi, pouria, stefan.werner}@ntnu.no, naveen.venkategowda@liu.se

***Abstract*—Distributed filtering techniques have emerged as the dominant and most prolific class of filters used in modern monitoring and surveillance applications, such as smart grids. As these techniques rely on information sharing among agents, user privacy and information security have become a focus of concern. In this manuscript, a privacy-preserving distributed Kalman filter (PP-DKF) is derived that maintains privacy by decomposing the information into public and private substates, where only a perturbed version of the public substate is shared among neighbors. The derived PP-DKF provides privacy by restricting the amount of information exchanged with state decomposition and conceals private information by injecting a carefully designed perturbation sequence. A thorough analysis is performed to characterize the privacy-accuracy trade-offs involved in the distributed filter, with privacy defined as the mean squared estimation error of the private information at the honest-but-curious agent. The resulting PP-DKF improves the overall filtering performance and privacy of all agents compared to distributed Kalman filters employing contemporary privacy-preserving average consensus techniques. Several simulation examples corroborate the theoretical results.**

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

I. Introduction

Distributed Kalman filtering algorithms became popular for learning and estimation in multiagent systems [1], [2] due to their high accuracy and computational efficiency [3]–[5]. In general, distributed Kalman filtering techniques are based on agents of a sensor network implementing local Kalman filtering operations using their observed data. Agents then employ consensus techniques to fuse local and neighbor estimates [6]–[8]. However, the local interactions between agents in distributed filtering settings raise concerns regarding privacy and demands for secure distributed filtering [9], [10]. Although local cooperation among agents in distributed filtering facilitates the fusion process, it causes undesirable information disclosures [11]. This vulnerability of distributed filters to potential adversaries has made privacy preservation one of the most pressing subjects in many applications [12]–[18].

The literature contains various methods to address the privacy issues in distributed consensus operations. For example, differential privacy techniques inject uncorrelated noise sequences into information exchange procedures to provide privacy for individual information [13], [14]. In addition, the more recent noise injection-based average consensus techniques achieve an improved privacy-accuracy trade-off by perturbing the information exchanged with noise [15]–[17]. Decomposition-based privacy-preserving techniques, on the other hand, are based on altering the amount of information shared with other agents [19], [20].

In particular, privacy in a system theoretic context, where sensor measurements are transmitted to a fusion center, was first addressed in [9]. The work therein considers the notion of privacy characterized by differential privacy, which protects individual data streams. Subsequently, the work in [21] presents a general approach to design a differentially private Kalman filter in both cases of perturbation before exchanging information with fusion center and output perturbation that injects noise to the output of the Kalman filter. The authors in [22] show that adequately combining the input signals before adding the differential privacy noise can improve the Kalman filter performance.

The privacy-aware centralized Kalman filter proposed in [23] partitions sensor measurements into private and public substates to maximize the estimation error of the private portion while minimizing the estimation error of the public substate. The works in [9], [21]–[23] mainly consider a centralized filtering setting with external adversaries; however, in the context of distributed filtering applications, honest-but-curios adversaries employ local information to infer private data. An honest-but-curious adversary is a legitimate network agent taking part in the filtering process but is curious and attempts to retrieve the private information of other agents. Although considerable research has been devoted to privacy in centralized Kalman filtering solutions, the dilemma of privacy-preserving distributed Kalman filters against honest-but-curious agents has not been appropriately addressed.

In this paper, a privacy-preserving distributed Kalman filtering solution is derived. The derived framework draws upon the ideas from both noise injection and decomposition-based average consensus strategies. In this setting, agents decompose their acquired information into public and private substates, sharing only the perturbed version of their public substate with their neighbors. The private substate evolves internally and will not be shared with neighbors. This process is designed to provide enhanced privacy, defined as the mean squared estimation error of private data at the honest-but-curious agent [24]. In comparison to distributed Kalman filters employing con-

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

temporary privacy-preserving average consensus techniques, the PP-DKF derived here exhibits higher robustness against injected noise and accomplishes the filtering process with enhanced performance. The contribution of the work also includes a rigorous mathematical analysis of the convergence and performance of the derived PP-DKF, and formulating a closed-form expression for agent privacy in the presence of an honest-but-curious adversary.

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 $\mathsf{tr}(\cdot)$, matrix $\mathsf{diag}(\mathbf{a})$ 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. A white Gaussian sequence $\mathbf{x}(k)$ with covariance $\mathbf{\Sigma}$ is represented as $\mathbf{x}(k) \sim \mathscr{N}(\mathbf{0}, \mathbf{\Sigma})$.

II. Problem Formulation

We consider a set of N interconnected agents concerned with a common task. The agents and their connections are 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, denoted by $\mathcal{N}_i$, is the set of agents that agent i receives information from, which does not include agent i itself. The cardinality of the set $\mathcal{N}_i$ is denoted by N_i.

We revisit the classical distributed Kalman filtering problem of tracking a dynamic system state through observations from a network of agents [3], [4], [7]. The state-space model representing the state vector evolution and local observation function 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, $\mathbf{A}$ denotes the state transition matrix and $\mathbf{H}_i$ is the ith agent observation matrix. For time instant n and agent i, $\mathbf{y}_{i,n}$ is the local observation, while $\mathbf{w}_{i,n}$ and $\mathbf{v}_n$ are observation and process noises, respectively. The process and observation noises are zero-mean Gaussian sequences with joint covariance matrices given by

$$\mathbb{E}\left\{\begin{bmatrix}\mathbf{v}_n\\ \mathbf{w}_{i,n}\end{bmatrix}\begin{bmatrix}\mathbf{v}_l^{\mathrm{T}} & \mathbf{w}_{j,l}^{\mathrm{T}}\end{bmatrix}\right\} = \begin{bmatrix}\mathbf{C}_{\mathbf{v}_n} & \mathbf{0}\\ \mathbf{0} & \mathbf{C}_{\mathbf{w}_{i,n}}\delta_{i,j}\end{bmatrix}\delta_{n,l}$$

where $\delta_{n,l}$ denotes the Kronecker delta function. The proposed PP-DKF is implemented based on the distributed Kalman filter (DKF) in [6] that requires agents to exchange local estimates with neighbors, and through local collaboration, to reach a network-wide consensus. Since the shared data includes private information, we propose a PP-DKF that prevents an honest-but-curious adversaries from estimating the private information of individual agents. An honest-but-curious agent is a legitimate agent of the network that is curious about private data from other agents.

III. Privacy-Preserving Distributed Kalman Filter

Considering the framework established in the distributed Kalman filtering [6], each agent implements a model update as

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

where for agent i and time instant n, $\hat{\mathbf{x}}_{i,n|n-1}$ and $\hat{\mathbf{x}}_{i,n|n}$ are the respective *a priori* and *a posteriori* estimates of the state vector. The ith agent error covariance information at time instant n is denoted by $\mathbf{M}_{i,n|n-1}$ which following the centralized Kalman filter operations in [7] is updated as

$$\mathbf{M}_{i,n|n}^{-1} = \mathbf{M}_{i,n|n-1}^{-1} + \sum_{j\in\mathcal{N}}\mathbf{H}_j^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_{j,n}}^{-1}\mathbf{H}_j = \frac{1}{N}\sum_{j\in\mathcal{N}}\mathbf{\Gamma}_{j,n}. \tag{4}$$

The expression in (4) can be approximated through average consensus filters (ACFs) after a local update as

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

The local covariance information $\mathbf{\Gamma}_{i,n}$ is not considered private, and it can be shared among neighbors to update the *a posteriori* covariance information. To this end, the covariance information $\mathbf{M}_{i,n|n}^{-1}$ is updated via an ACF by averaging the local covariance information $\mathbf{\Gamma}_{i,n}$ among neighbors. The ACF operations is represented with the following schematic [6]:

$$\mathbf{S}_{i,n}(k) \leftarrow \boxed{\text{ACF}} \leftarrow \{\forall j \in \mathcal{N}_i \cup i : \mathbf{S}_{j,n}(0)\}$$

where $\mathbf{S}_{j,n}(0)$, $j \in \mathcal{N}_i \cup i$ are the initial inputs to the ACF at node i, and $\mathbf{S}_{i,n}(k)$ is the output at node i after k iterations. The iterative operation of the consensus filter is given by

$$\mathbf{S}_{i,n}(k) = q_{ii}\mathbf{S}_{i,n}(k-1) + \sum_{j\in\mathcal{N}_i} q_{ij}\mathbf{S}_{j,n}(k-1)$$

where $\mathbf{Q} = [q_{ij}]$ is a doubly stochastic consensus weight matrix [25]. It is assumed that the conditions for convergence of $\mathbf{M}_{i,n|n}$ for all agents are satisfied (see [6]).

The updated covariance information is employed to calculate an intermediate state estimate update using the sensors observation 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 $\mathbf{M}_{i,n|n}^{-1}$ is used to formulate the update gain $\mathbf{G}_{i,n} = N\mathbf{M}_{i,n|n}\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_{i,n}}^{-1}$. To improve the state estimation, agents share their intermediate state estimate $\boldsymbol{\psi}_{i,n}$ with their neighbors to reach the average consensus. The intermediate state estimate, $\boldsymbol{\psi}_{i,n}$, reveals information regarding the observations and current state vector of an agent, which is considered private. Thus, to avoid information disclosure, the average consensus of intermediate state estimates should be implemented in a privacy-preserving manner. To this end, a privacy-preserving average consensus mechanism is designed to protect the intermediate state estimates while having minimal impact on the filtering process.

Before sharing the intermediate state estimate with neighbors, the ith agent decomposes the initial state $\boldsymbol{\psi}_{i,n}(0) =$

$\boldsymbol{\psi}_{i,n}$ into public and private substates $\boldsymbol{\alpha}_{i,n}(0)$ and $\boldsymbol{\beta}_{i,n}(0)$, satisfying $\boldsymbol{\alpha}_{i,n}(0) + \boldsymbol{\beta}_{i,n}(0) = 2\boldsymbol{\psi}_{i,n}(0)$, [19]. The public substate, $\boldsymbol{\alpha}_{i,n}$, is shared with neighbors, while the private substate, $\boldsymbol{\beta}_{i,n}$, evolves internally and will not be observed by neighbors. Although the private substate remains invisible to neighbors, it directly affects the evolution of the public substate. To provide an additional protection layer to the initial state of agent i, we perturb its public substate, at the kth consensus iteration, by noise sequence $\boldsymbol{\omega}_i(k)$. The perturbation-noise is a zero-mean Gaussian sequence, mutually and temporally independent among different agents, with time-dependent covariance such that

$$\boldsymbol{\omega}_i(k) \sim \mathscr{N}(\mathbf{0}, \sigma_k^2 \mathbf{I}), \ \ \forall i = 1, 2, \cdots, N. \tag{6}$$

In order to guarantee the convergence of the overall PP-DKF operations, the variance σ_k^2 is chosen to be exponentially decaying with respect to the consensus iteration k [10], [15]. Thus, as the number of consensus iterations increases, the shared data of the ith agent converges toward the average consensus value, which is common among all agents. Hence, regarding the perturbation sequence (6), the PP-DKF injects noise with higher variance to the initial substates, while substates approaching the average consensus value are perturbed with less noise. The substate updates at each agent, and consensus iteration k, are given by

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

where $\tilde{\boldsymbol{\alpha}}_{j,n}(k) = \boldsymbol{\alpha}_{j,n}(k) + \boldsymbol{\omega}_j(k)$ is the received information from the jth neighbor, $w_{ij}(k)$ denotes the interaction weight between agent i and j at consensus iteration k, and $\mathbf{U}_i(k) \triangleq \mathsf{diag}(\mathbf{u}_i(k))$ is a diagonal matrix containing the ith agent's coupling weight vector $\mathbf{u}_i(k) \in \mathbb{R}^m$ with independent elements that controls the level of contribution of each substate in the updating procedure. The consensus parameter ε resides in the range $(0, 1/(\Delta + 1)]$ where $\Delta \triangleq \max_{i \in \mathcal{N}} N_i$. For $k = 0$, all weights $w_{ij}(0)$ and each elements of $\mathbf{u}_i(0)$ are allowed to be arbitrarily chosen from the set of all real numbers, while satisfying $w_{ij}(0) = w_{ji}(0), \ \forall i, j$. For $k > 0$, a scalar $\eta \in (0, 1)$ is required, such that all non-zero $w_{ij}(k)$ and all elements of $\mathbf{u}_i(k)$ reside in the range $[\eta, 1)$, [19]. The operations of the proposed PP-DKF at each agent are summarized in Algorithm 1.

To investigate the convergence of the derived privacy-preserving ACF operations to the exact average consensus value, one can show that the sum of all substates is constant, asymptotically [19]. 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

$$\boldsymbol{\zeta}_n(k) = \boldsymbol{\zeta}_n(0) + \varepsilon \sum_{i=1}^{N} d_{ii} \left(\sum_{l=1}^{k-1} \boldsymbol{\omega}_i(l) \right). \tag{8}$$

Algorithm 1 Privacy-Preserving Distributed Kalman Filter

Initialization: For each agent $i \in \mathcal{N}$

$\hat{\mathbf{x}}_{i,0|0} = \mathbb{E}\{\mathbf{x}_0\}$

$\mathbf{M}_{i,0|0} = \mathbb{E}\left\{(\mathbf{x}_0 - \mathbb{E}\{\mathbf{x}_0\})(\mathbf{x}_0 - \mathbb{E}\{\mathbf{x}_0\})^{\mathrm{T}}\right\}$

Model update:

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

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

Measurement update:

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

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

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

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

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

Privacy-Preserving Mechanism:

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

Generate $\{\boldsymbol{\omega}_i(k), k = 0, 1, \cdots, K\}$ based on (6)

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

for $k = 1$ **to** 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 for

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

where d_{ii} is a diagonal element of matrix $\mathbf{D} \triangleq \mathsf{diag}(\{\sum_{j \in \mathcal{N}_i} w_{ij}\}_{i=1}^{N})$, to simplify the analysis, we assume that the interaction weights are time-invariant. 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 sense which is

$$\lim_{k \to \infty} \mathbb{E}\{\boldsymbol{\zeta}_n(k) - \boldsymbol{\zeta}_n(0)\} = \mathbf{0}. \tag{9}$$

Due to the connected network assumption and considering that $\boldsymbol{\alpha}_{i,n}(0) + \boldsymbol{\beta}_{i,n}(0) = 2\boldsymbol{\psi}_{i,n}(0)$, the ith agent substates, $\boldsymbol{\alpha}_{i,n}$ and $\boldsymbol{\beta}_{i,n}$, converge to the desired average consensus value [19], i.e.,

$$\lim_{k \to \infty} \mathbb{E}\{\boldsymbol{\alpha}_{i,n}(k)\} = \lim_{k \to \infty} \mathbb{E}\{\boldsymbol{\beta}_{i,n}(k)\} = \frac{1}{N} \sum_{i=1}^{N} \boldsymbol{\psi}_{i,n}(0).$$

In practice, due to the finite number of consensus iterations, the convergence in (9) is achieved with a bounded variance that reduces the average consensus accuracy. In the next section, we analyze the impact of this consensus error on the overall performance and convergence conditions of the proposed PP-DKF.

IV. Performance Evaluation

To provide an intuitive analysis and a proper insight into the effects of incorporating the privacy-preserving operations, we consider the equivalent network of $2N$ agents so that each private substate corresponds to an agent only attached to its peer in the original network with the same observation parameters, $\mathbf{y}_{i,n}$, $\mathbf{H}_i$, and $\mathbf{C}_{\mathbf{w}_i}$ (see Fig. 1). It is assumed that agents initialize the privacy-preserving steps with equal

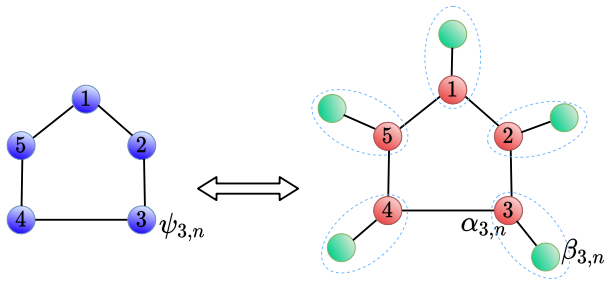

Fig. 1. A ring network topology with $N = 5$ nodes.

substates, so that the intermediate estimation error of agents in the decomposed network is expressed as

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

Following the made assumption on the initial substates, $\boldsymbol{\alpha}_{i,n}(0) = \boldsymbol{\beta}_{i,n}(0) = \boldsymbol{\psi}_{i,n}$, the intermediate estimation error of each agent $i \in \{1, 2, \cdots, 2N\}$, employing the local observation in (2), is formulated as

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

Substituting (1) into (10) and after some algebraic manipulation, we have

$$\begin{aligned}\boldsymbol{\epsilon}_{i,n} =& \left(\mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_i}^{-1}\mathbf{H}_i\right)\mathbf{A}\boldsymbol{\epsilon}_{i,n-1|n-1}\\ &+ \left(\mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_i}^{-1}\mathbf{H}_i\right)\mathbf{v}_n - \mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_i}^{-1}\mathbf{w}_{i,n}.\end{aligned} \tag{11}$$

where $\boldsymbol{\epsilon}_{i,n-1|n-1} = \mathbf{x}_{n-1} - \hat{\mathbf{x}}_{i,n-1|n-1}$. Considering the block row vectors organizing all error terms as

$$\begin{aligned}\boldsymbol{\mathcal{E}}_n =&[\boldsymbol{\epsilon}_{1,n}^{\mathrm{T}}, \cdots, \boldsymbol{\epsilon}_{2N,n}^{\mathrm{T}}]^{\mathrm{T}}\\ \boldsymbol{\mathcal{E}}_{n-1|n-1} =&[\boldsymbol{\epsilon}_{1,n-1|n-1}^{\mathrm{T}}, \cdots, \boldsymbol{\epsilon}_{2N,n-1|n-1}^{\mathrm{T}}]^{\mathrm{T}}\end{aligned}$$

the network-wide state vector estimation error of the state-decomposed network, $\boldsymbol{\mathcal{E}}_{n|n}$, which is the stacked error after the privacy-preserving average consensus operations in (7) with k consensus iterations, is expressed by

$$\boldsymbol{\mathcal{E}}_{n|n} = \mathbf{G}^k\boldsymbol{\mathcal{E}}_n + \sum_{s=1}^{k}\mathbf{G}^{s-1}\boldsymbol{\mathcal{B}}\boldsymbol{\omega}(k-s). \tag{12}$$

The stacked perturbation sequences is denoted by $\boldsymbol{\omega}(k) = \left[\boldsymbol{\omega}_1^{\mathrm{T}}(k), \cdots, \boldsymbol{\omega}_N^{\mathrm{T}}(k)\right]^{\mathrm{T}}$, while $\boldsymbol{\mathcal{B}} = [\varepsilon\mathbf{W}, \mathbf{0}]^{\mathrm{T}} \otimes \mathbf{I}$, and $\mathbf{G}$ is a doubly stochastic matrix given by

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

with $\mathbf{M} \triangleq (\mathbf{I} - \varepsilon(\mathbf{D} - \mathbf{W})) \otimes \mathbf{I} - \varepsilon\mathbf{U}$. The interaction and coupling weight matrices for the entire network are denoted by $\mathbf{W}(k) \triangleq [w_{ij}(k)]$ and $\mathbf{U}(k) = \mathsf{Blockdiag}(\{\mathbf{U}_i(k)\}_{i=1}^N)$, respectively. To simplify the state vector error analysis, we assume that the interaction and coupling weight matrices are time-invariant. Alternatively, (12) can be expressed as

$$\begin{aligned}\boldsymbol{\mathcal{E}}_{n|n} =&\boldsymbol{\mathcal{P}}\boldsymbol{\mathcal{E}}_{n-1|n-1} + \boldsymbol{\mathcal{Q}}\boldsymbol{\Upsilon}_n - \boldsymbol{\Omega}_n\\ &+ \sum_{s=1}^{k}\mathbf{G}^{s-1}\boldsymbol{\mathcal{B}}\boldsymbol{\omega}(k-s)\end{aligned} \tag{13}$$

where

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

with $\mathbf{P}_i = \mathbf{I} - N\mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_i}^{-1}\mathbf{H}_i$ and $\mathbf{Q}_i = \mathbf{M}_i\mathbf{H}_i^{\mathrm{T}}\mathbf{C}_{\mathbf{w}_i}^{-1}$. Following the definition, $\mathbf{P}_i$ is stable and since $\mathbf{G}$ is doubly stochastic, the block matrix $\boldsymbol{\mathcal{P}}$ is stable; therefore, 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 (12) yields

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

Once again, 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 recursive expression of the state vector estimation error in (13), is used to formulate the second-order statistics of all agents, denoted by $\boldsymbol{\Sigma}_n = \mathbb{E}\{\boldsymbol{\mathcal{E}}_{n|n}\boldsymbol{\mathcal{E}}_{n|n}^{\mathrm{T}}\}$, as

$$\boldsymbol{\Sigma}_n = \boldsymbol{\mathcal{P}}\boldsymbol{\Sigma}_{n-1}\boldsymbol{\mathcal{P}}^{\mathrm{T}} + \boldsymbol{\mathcal{Q}}\mathbf{C}_{\boldsymbol{\Upsilon}}\boldsymbol{\mathcal{Q}}^{\mathrm{T}} + \mathbf{C}_{\boldsymbol{\Omega}} + \boldsymbol{\mathcal{T}} \tag{14}$$

where $\mathbf{C}_{\boldsymbol{\Upsilon}} = \mathbb{E}\{\boldsymbol{\Upsilon}_n\boldsymbol{\Upsilon}_n^{\mathrm{T}}\}$, $\mathbf{C}_{\boldsymbol{\Omega}} = \mathbb{E}\{\boldsymbol{\Omega}_n\boldsymbol{\Omega}_n^{\mathrm{T}}\}$, and with respect to the noise sequence (6), we have

$$\boldsymbol{\mathcal{T}} = \sum_{s=1}^{k}\sigma_{k-s}^2\mathbf{G}^{s-1}\boldsymbol{\mathcal{B}}\boldsymbol{\mathcal{B}}^{\mathrm{T}}\left(\mathbf{G}^{s-1}\right)^{\mathrm{T}}.$$

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). The effect of injected noise is manifested in terms of $\boldsymbol{\mathcal{T}}$, which increases the steady-state mean squared error (MSE) of Algorithm 1 compared to the non-private approach. In the next section, we analyze the performance of the derived framework to preserve agent privacy.

V. Privacy Analysis

We consider an honest-but-curious agent that can access the interaction weights and information shared by its neighbors. To benchmark the privacy of the derived PP-DKF, we consider the MSE associated with the estimates of the initial states $\boldsymbol{\psi}_{i,n}(0)$ at the honest-but-curious agent, as privacy measure. Without loss of generality, it is assumed that the Nth agent is an honest-but-curious agent that employs a maximum likelihood (ML) estimator to estimate the initial states of all agents, $\boldsymbol{\psi}_n(0) = [\boldsymbol{\psi}_{1,n}^{\mathrm{T}}, \cdots, \boldsymbol{\psi}_{N,n}^{\mathrm{T}}]^{\mathrm{T}}$, at time instant n. The honest-but-curious agent has access to the following information set at consensus iteration k

$$\begin{aligned}\mathcal{I}(k) = \{&\boldsymbol{\alpha}_{N,n}(k), \boldsymbol{\beta}_{N,n}(k), \boldsymbol{\omega}_N(k), u_N(k),\\ &w_{Nj}(k), \tilde{\boldsymbol{\alpha}}_{j,n}(k) : \forall j \in \mathcal{N}_N\}.\end{aligned} \tag{15}$$

Proposition 1. *Suppose an honest-but-curious agent has access to messages shared by its neighbors and their corresponding interaction weights. If every agent has at least one regular agent in the neighborhood, an honest-but-curious agent cannot infer private information of any other agent in the network.*

Proof: The proof follows from Theorem 2 in [19] by showing that an arbitrary change in the initial information of the jth agent, $\boldsymbol{\psi}_{j,n}$ to $\bar{\boldsymbol{\psi}}_{j,n}$, remains indistinguishable from the honest-but-curious agent. ∎

In the worst case, the honest-but-curious agent also accesses the interaction and coupling weights of the entire network, thereafter it can construct an ML estimator to estimate the private information of the other agents. To construct an ML estimator, we introduce the observation vector $\mathbf{y}_n(k)$ that includes the accessible information transferred from the neighbors to the honest-but-curious agent at each iteration k as

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

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

$$\mathbf{C}_\alpha = \left[\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_{N_N}}, \mathbf{e}_N\right]^{\mathrm{T}} \otimes \mathbf{I}.$$

The canonical basis $\mathbf{e}_i$ 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

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

The estimated value of $\mathbf{z}_n(0) \triangleq [\boldsymbol{\alpha}_n^{\mathrm{T}}(0), \boldsymbol{\beta}_n^{\mathrm{T}}(0)]^{\mathrm{T}}$ is employed to estimate agent initial states as $\hat{\boldsymbol{\psi}}_n(0) = \frac{1}{2}(\hat{\boldsymbol{\alpha}}_n(0) + \hat{\boldsymbol{\beta}}_n(0))$.

Since the information of the Nth agent is already known to the honest-but-curious agent, we reduce the state space dimension by removing all entries belonging to the Nth agent form the defined variables and find the estimation error covariance $\tilde{\mathbf{P}}(k)$ instead of $\mathbf{P}(k)$ as it satisfies

$$\mathbf{P}(k) = \begin{bmatrix} \tilde{\mathbf{P}}(k) & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & 0 \end{bmatrix}.$$

Accordingly, the reduced version of $\mathbf{C}$ and the observation vector $\mathbf{y}_n(k)$ can be expressed as $\tilde{\mathbf{C}} = [\tilde{\mathbf{C}}_\alpha, \tilde{\mathbf{0}}]$ and

$$\tilde{\mathbf{y}}_n(k) = \tilde{\mathbf{C}}\tilde{\mathbf{z}}_n(k) + \tilde{\mathbf{C}}_\alpha \tilde{\boldsymbol{\omega}}(k) \tag{16}$$

where

$$\tilde{\mathbf{z}}_n(k) = [\tilde{\boldsymbol{\alpha}}_n^{\mathrm{T}}(k), \tilde{\boldsymbol{\beta}}_n^{\mathrm{T}}(k)]^{\mathrm{T}}$$
$$\tilde{\mathbf{C}}_\alpha = [\tilde{\mathbf{e}}_{j_1}, \tilde{\mathbf{e}}_{j_2}, \cdots, \tilde{\mathbf{e}}_{j_{N_N}}]^{\mathrm{T}}.$$

Substituting the network-wide state update equations (7) in (16), gives

$$\tilde{\mathbf{y}}_n(k) = \tilde{\mathbf{C}}\tilde{\mathbf{G}}^k \tilde{\mathbf{z}}_n(0) + \tilde{\mathbf{C}}_\alpha \left(\sum_{t=0}^{k-1} \boldsymbol{\mathcal{C}}_{k-1-t} \tilde{\boldsymbol{\mathcal{B}}} \tilde{\boldsymbol{\omega}}(t) + \tilde{\boldsymbol{\omega}}(k) \right) \tag{17}$$

where $\tilde{\boldsymbol{\mathcal{B}}} = \varepsilon \tilde{\mathbf{W}} \otimes \mathbf{I}$, $\boldsymbol{\mathcal{C}}_k = \begin{bmatrix} \mathbf{I} & \mathbf{0} \end{bmatrix} \tilde{\mathbf{G}}^k \begin{bmatrix} \mathbf{I} & \mathbf{0} \end{bmatrix}^{\mathrm{T}}$, and

$$\tilde{\mathbf{G}} = \begin{bmatrix} \tilde{\mathbf{M}} & \varepsilon\tilde{\mathbf{U}} \\ \varepsilon\tilde{\mathbf{U}} & \mathbf{I} - \varepsilon\tilde{\mathbf{U}} \end{bmatrix}.$$

We can simplify the accumulated observation set of the honest-but-curious agent, up to consensus iteration k, as

$$\begin{bmatrix} \tilde{\mathbf{y}}_n(0) \\ \tilde{\mathbf{y}}_n(1) \\ \vdots \\ \tilde{\mathbf{y}}_n(k) \end{bmatrix} = \mathbf{H}(k)\tilde{\mathbf{z}}_n(0) + \mathbf{F}(k) \begin{bmatrix} \tilde{\boldsymbol{\omega}}(0) \\ \tilde{\boldsymbol{\omega}}(1) \\ \vdots \\ \tilde{\boldsymbol{\omega}}(k) \end{bmatrix} \tag{18}$$

where $\mathbf{H}(k) \triangleq [(\tilde{\mathbf{C}})^{\mathrm{T}}, (\tilde{\mathbf{C}}\tilde{\mathbf{G}})^{\mathrm{T}}, \cdots, (\tilde{\mathbf{C}}\tilde{\mathbf{G}}^k)^{\mathrm{T}}]^{\mathrm{T}}$ and

$$\mathbf{F}(k) = \begin{bmatrix} \tilde{\mathbf{C}}_\alpha & \mathbf{0} & \cdots & \mathbf{0} \\ \tilde{\mathbf{C}}_\alpha \boldsymbol{\mathcal{C}}_0 \tilde{\boldsymbol{\mathcal{B}}} & \tilde{\mathbf{C}}_\alpha & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\mathbf{C}}_\alpha \boldsymbol{\mathcal{C}}_{k-1} \tilde{\boldsymbol{\mathcal{B}}} & \tilde{\mathbf{C}}_\alpha \boldsymbol{\mathcal{C}}_{k-2} \tilde{\boldsymbol{\mathcal{B}}} & \cdots & \tilde{\mathbf{C}}_\alpha \end{bmatrix}. \tag{19}$$

Subsequently, the error covariance of the ML estimator [26], to estimate $\tilde{\mathbf{z}}_n(0)$, with independent noise sequences is obtained by

$$\tilde{\mathbf{P}}(k) = \left(\mathbf{H}^{\mathrm{T}}(k) \left(\mathbf{F}(k) \tilde{\boldsymbol{\Gamma}}(k) \mathbf{F}^{\mathrm{T}}(k) \right)^{-1} \mathbf{H}(k) \right)^{-1} \tag{20}$$

where $\tilde{\boldsymbol{\Gamma}}(k) = \mathsf{diag}\left(\{\sigma_t^2 \mathbf{I}\}_{t=0}^{k} \right)$ contains the perturbation sequence covariances up to consensus iteration k. Since the accessible information of the honest-but-curious agent is expanding, the error covariance $\tilde{\mathbf{P}}(k)$ is monotonically non-increasing, i.e., for $k_1 \leq k_2$, we have $\tilde{\mathbf{P}}(k_2) \leq \tilde{\mathbf{P}}(k_1)$. This implies that error covariance matrix $\tilde{\mathbf{P}}(k)$ converges to a constant matrix $\tilde{\mathbf{P}} = \lim_{k\to\infty} \tilde{\mathbf{P}}(k)$. Let us assume

$$\tilde{\mathbf{P}} = \begin{bmatrix} \tilde{\mathbf{P}}_1 & \tilde{\mathbf{P}}_{12} \\ \tilde{\mathbf{P}}_{21} & \tilde{\mathbf{P}}_{22} \end{bmatrix},$$

then, the error covariance of the ML estimator to estimate $\tilde{\boldsymbol{\psi}}_n(0)$ is given by

$$\bar{\mathbf{P}} = \frac{1}{4} \left(\tilde{\mathbf{P}}_1 + \tilde{\mathbf{P}}_{12} + \tilde{\mathbf{P}}_{21} + \tilde{\mathbf{P}}_{22} \right).$$

Thus, the privacy metric of the ith agent, related to estimate its initial state $\boldsymbol{\psi}_{i,n}(0)$ by the honest-but-curious agent N is defined as

$$\mathcal{E}_i \triangleq \mathrm{tr}\left((\tilde{\mathbf{e}}_i^{\mathrm{T}} \otimes \mathbf{I}) \bar{\mathbf{P}} (\tilde{\mathbf{e}}_i \otimes \mathbf{I}) \right). \tag{21}$$

The derived privacy metric represents the ability of the privacy-preserving strategy to conceal the initial states from being estimated by the honest-but-curious agent. Several simulations verify the privacy performance of the proposed PP-DKF in the next section.

VI. Numerical Results

We consider a ring network topology with $N = 5$ agents shown in Fig. 1. The proposed PP-DKF is considered in a collaborative target tracking application. The state-space model is following the distributed Kalman filter in [6], where the state vector $\mathbf{x}_n = [X_n, Y_n, \dot{X}_n, \dot{Y}_n]^{\mathrm{T}}$ consists of the positions $\{X_n, Y_n\}$ and velocities $\{\dot{X}_n, \dot{Y}_n\}$ in the horizontal and vertical directions, respectively. For comparison purposes, we implement a pure noise-injection based privacy-preserving DKF (NIP-DKF), wherein the noise sequence in (6) perturbs

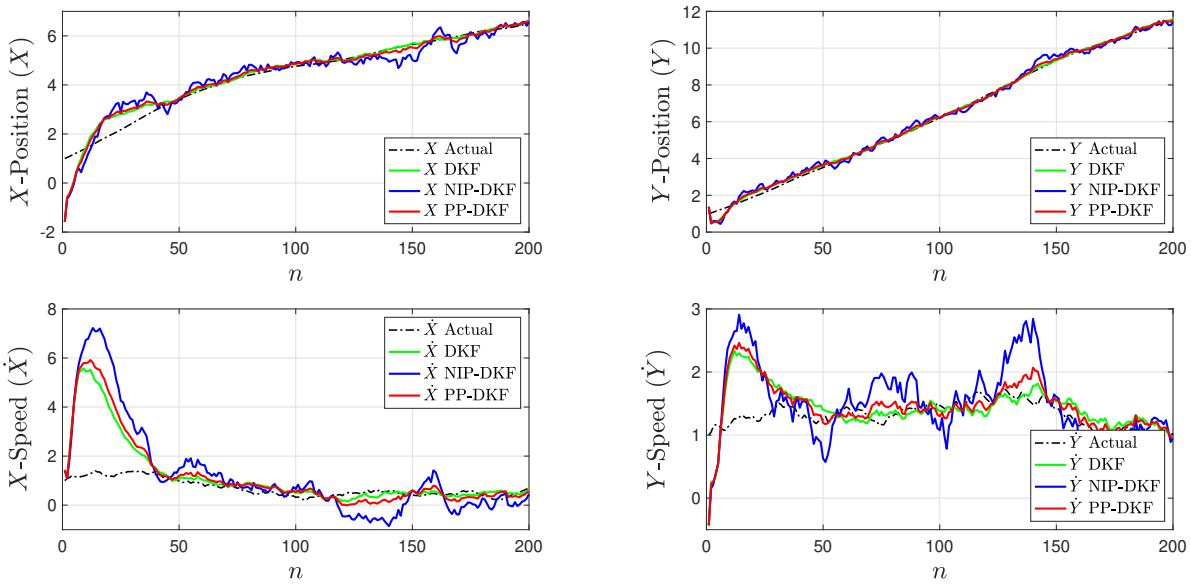

Fig. 2. Tracking performance of the derived PP-DKF with $K = 40$ consensus iterations and noise variance $\sigma^2 = 0.5$.

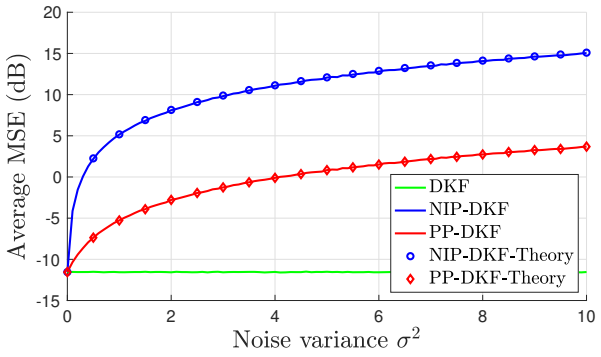

Fig. 3. Average filtering MSE versus injected noise variance σ^2.

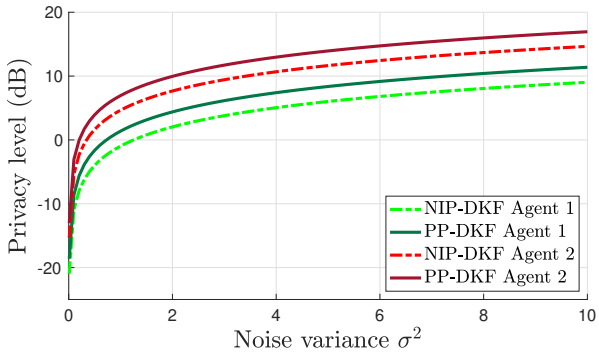

Fig. 4. Privacy metric $\mathcal{E}_i$ versus injected noise variance σ^2.

the shared messages of the conventional DKF [6]. Regarding the perturbation sequence assumptions in (6), we assume $\sigma_k^2 = \frac{\phi^{2k}}{N(k+1)}\sigma^2$ at each consensus iteration, where $\phi = 0.9$, and σ^2 is noise variance that controls the amount of the injected noise.

Fig. 2 shows the performance of the proposed PP-DKF to track the system state compared to the NIP-DKF and non-private distributed Kalman filter (DKF). The proposed PP-DKF performs as well as the non-private distributed Kalman filter and outperforms the NIP-DKF. This means that the estimate produced by PP-DKF is closer to the actual position and speed of the target compared to NIP-DKF. The higher accuracy of PP-DKF to track the position and speed of the target, verifying its robustness to the perturbation noise sequences.

Fig. 3 shows the average MSE of the distributed Kalman filter versus the noise variance parameter σ^2 with $K = 40$ consensus iterations. We see that the perturbation sequence degrades the performance of the privacy-preserving approaches, PP-DKF and NIP-DKF, compared to the conventional DKF [6]. We also see that the proposed PP-DKF significantly outperforms the NIP-DKF method by achieving lower MSE for a broad range of injected noise variances, indicating lower sensitivity of the PP-DKF to the noise variance than the NIP-DKF. This is because the proposed PP-DKF operates by partially obfuscating shared substates. At the same time, the NIP-DKF solution perturbs the entire state before sharing among neighbors, which was the motivation behind the design of our consensus framework.

Fig. 4 shows the privacy metric (21) for $K = 30$ consensus iterations versus the noise variance parameter σ^2, for all agents. We see that injecting a higher amount of noise results in higher privacy, where the privacy level of all agents is significantly improved under the proposed PP-DKF compared to the NIP-DKF. Due to the ring topology, agents 3 and 4 achieve the same privacy level as agents 2 and 1. The improved

privacy-accuracy trade-off under the PP-DKF is manifested by achieving lower MSE and higher privacy $\mathcal{E}_i$ for all agents compared to NIP-DKF.

VII. Conclusion

This paper proposed a privacy-preserving distributed Kalman filter that utilizes both decomposition-based and noise injection-based privacy-preserving average consensus techniques to protect network agents disclosing their private information. It provides a private distributed Kalman filter by restricting the amount of information exchanged with decomposition and concealing the private data from being estimated by adversaries with perturbation. The convergence and performance of the derived PP-DKF have been analyzed. The achieved privacy level of all agents, defined as the uncertainty of the honest-but-curious agent to estimate the initial state of other agents, has been characterized in the presence of an honest-but-curious agent. It has been shown that the proposed PP-DKF solution improves privacy and performance of the Kalman filtering operations compared to the DKF employing contemporary privacy-preserving techniques. Lastly, several simulations verified the obtained theoretical results.

References

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Multi-agent systems: A survey," *IEEE Access*, vol. 6, pp. 28 573–28 593, Jun. 2018.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

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

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

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

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

[10] 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.

[11] Q. Li, R. Heusdens, and M. G. Christensen, "Convex optimisation-based privacy-preserving distributed average consensus in wireless sensor networks," in *Proc. 45th IEEE Int. Conf. Acoust., Speech and Signal Process.*, 2020, pp. 5895–5899.

[12] 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.*, 2019, pp. 495–499.

[13] 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.

[14] 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, Jul. 2020.

[16] 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.

[17] 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.

[18] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

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

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

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

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

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

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

[25] L. Xiao, S. Boyd, and S.-J. Kim, "Distributed average consensus with least-mean-square deviation," *J. Parallel Distrib. Comput.*, vol. 67, no. 1, pp. 33–46, Jan. 2007.

[26] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, ser. Prentice Hall Signal Process. Ser. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.