machines

MDPI

Article

Privacy-Preserving State Estimation with Application to Target Tracking

Yulong Wang [1], Yuman Li [2,*], Sen Wang [1] and Hong Lin [2]

[1] Faculty of Mechanical and Electrical Engineering, Kunming University of Science and Technology, Kunming 650032, China; wangyulong0823@126.com (Y.W.); wangsen0401@126.com (S.W.)
[2] Institute of Intelligence Science and Engineering, Shenzhen Polytechnic University, Shenzhen 518055, China; linhongzju@163.com
* Correspondence: liyuman@szpu.edu.cn

Abstract

This paper studies the design of a privacy-preserving optimal state estimator for discrete-time linear systems.Insome traditional methods, such as noise injection, privacy is protected by adding noise to observations and the resulting data is deceptive information. The features of the proposed privacy protection in this paper are twofold. (i) Privacy is protected without providing deceptive information, that is, the information of the resulting protected observations is authentic. The privacy protection consists of two steps. First, the direction deviation of the observations, rather than the raw observation, is computed. Then, this deviation is random and is not always transmitted to the estimator. (ii) An optimal estimator is designed with desired privacy-preserving degree. By tuning a privacy-protection parameter, a given privacy-preserving degree and an estimation accuracy upper bound can be achieved simultaneously. Finally, drone-tracking experiments are provided to demonstrate the effectiveness of the proposed method, and some comparisons with the existing methods are presented.

Keywords: state estimation; discrete-time linear systems; privacy protection; target tracking

1. Introduction

1.1. Research Background

Real-time state estimation serves as the foundation of target tracking [1,2] and path planning [3,4]. These technologies have become indispensable core components in various systems, including the Internet of Things [5], intelligent transportation [6], and industrial automation [7].

State estimation inherently necessitates information provision and sharing among all participating entities (i.e., the sensors in this paper), which introduces nontrivial privacy leakage risks [8]. In practical scenarios such as smart grids, medical monitoring, and intelligent transportation, the data furnished by these entities may lead to the disclosure of sensitive privacy, including household living habits, patients' physiological information, and individuals' travel trajectories. Target tracking, as one of the primary applications of state estimation, involves highly identity-linked trajectory data: overly precise trajectory details (e.g., commuting routes, consumption venues, and daily routines) can expose participants' occupations, living habits, social connections, and even health conditions. Worse still, in the context of data fusion, preliminary anonymization of trajectory data does not

Check for updates

Academic Editor: Dan Zhang

Received: 30 November 2025
Revised: 5 January 2026
Accepted: 16 January 2026
Published: 19 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

guarantee privacy, as specific individuals may still be re-identified via cross-reference with other datasets.

This privacy concern is particularly pronounced in UAV target tracking—our focus in this work. For civilian UAV applications (e.g., aerial photography, parcel delivery, power grid inspection, and environmental monitoring), rough trajectory information suffices for assessing general operational status. In contrast, overly accurate trajectory estimation may result in the leakage of operational site details and further facilitate malicious sabotage. Beyond trajectory-related risks, privacy threats also arise during data transmission: when measurement data is transmitted to remote state estimators via wireless networks, it can be intercepted by network eavesdroppers [9]. In systems with malicious nodes, attackers can reconstruct private information (e.g., target locations and behavioral patterns) by analyzing data from these nodes, posing severe threats to privacy and security [10,11].

Collectively, these privacy-related issues motivate us to study state estimation with privacy protection capabilities. Designing privacy-preserving mechanisms to protect participants' sensitive information is crucial for sustaining their willingness to share data, addressing a key concern raised by reviewers. Specifically, as shown in Figure 1, the estimator to be designed will achieve a balanced trade-off between privacy protection and estimation accuracy.

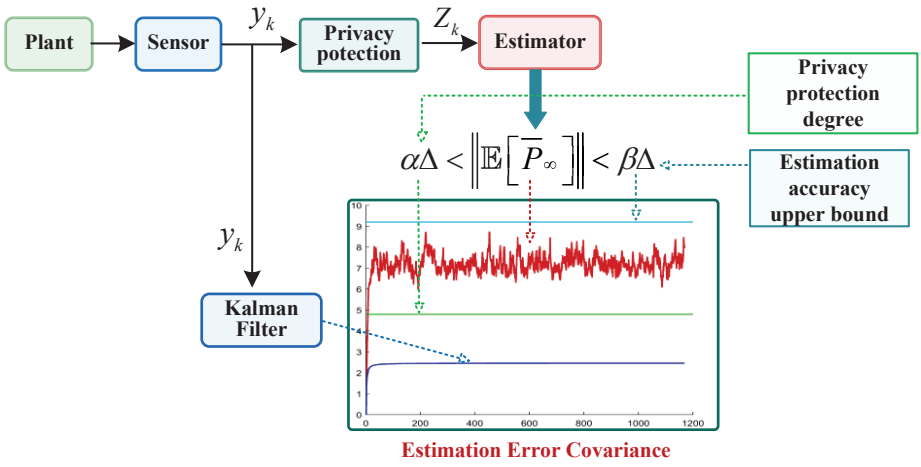


Figure 1. System with a privacy-preserving estimator.

1.2. Literature Review on State-Estimation-Related Privacy Protection

Data privacy protection can be implemented through multiple approaches [12,13], with suitable solutions selected based on specific privacy requirements. In state estimation scenarios, the core objects of privacy protection are system state data, involving three key entities: (1) data providers (sensor endpoints); (2) data recipients (estimators); and (3) third parties that exclude the aforementioned two entities. According to the objects to be protected, privacy protection methods can be broadly categorized into the following two types.

Type 1: Methods aimed at preventing third parties from accessing data. This category of methods focuses on blocking entities other than the data providers and intended receivers from obtaining valid system state data, with the core objective of achieving privacy protection through encryption or noise injection. For example, encoding parameters can be adjusted to ensure the confidentiality of state information [14]. Linear obfuscated encryption can be adopted to achieve lightweight and efficient data protection while maintaining estimation performance [15]. Encryption–decryption-based state estimators are designed to resist third-party eavesdropping attacks [16,17]. Somewhat homomorphic encryption [18] and fully homomorphic encryption [19] are utilized to support direct computation on

ciphertexts. Public key-based weighted innovation encoding is implemented to balance anti-eavesdropping capability and estimation performance [20]. Third-party information acquisition can be blocked by representing private information with numbers and indices [21], and encryption strategies are designed to protect signal transmission security [22]. Furthermore, noise injection also enables such protection; for instance, noise injection based on differential privacy [23], integrating noise into innovations to design privacy-preserving schemes for remote estimation [24], achieving distributed privacy protection by decomposing states and sharing noise-corrupted public sub-states [25], and dynamically selecting sensor transmission modes to maximize third-party estimation errors [26]. Integration applications of advanced encryption and learning technologies have also been reviewed [27]. Another study proposes a secure multi-party computation-based machine learning privacy protection framework, which avoids third-party access to original state data through distributed collaborative computing [28].

Type 2: Methods designed to prevent data recipients and third parties from obtaining accurate data. This category focuses on restricting both the receivers and third parties from acquiring the true system state. The core approach involves adopting noise-injection-based differential privacy techniques to reduce the accuracy of state data while ensuring data availability. For example, studies examine the conditions and properties of differential privacy and explore the trade-off between privacy and data utility [29]. A differential privacy-based "single-parameter defense" mechanism is proposed to prevent high-precision reconstruction of the true state via noise injection [30]. A data-privacy-preserving algorithm based on k-anonymity is designed to hide details of the true system state through attribute generalization and suppression [31]. Data perturbation is implemented via three-dimensional shearing statistical transformation to protect privacy by deforming state data [32]. Meanwhile, for multi-agent systems (MASs), differential privacy consensus algorithms suitable for different structures have been developed, such as those for general directed graphs [33], multivariable systems [34], and positive agents [35]. These algorithms prevent receivers and third parties from obtaining accurate state data while achieving system consensus.

1.3. Limitations of the Existing Approaches and Motivation

In the scenario of preventing receivers and third parties from acquiring system state information, existing privacy-preserving methods exhibit notable limitations, which are elaborated as follows: (i) data perturbation techniques: Privacy protection is achieved by injecting noise into raw data, which essentially causes the information transmitted by data providers to deviate from the true system states and thus has the nature of information deception. (ii) Differential privacy techniques: The core objective is to protect the identifiability of individuals within group data. This category of methods is more suitable for group scenarios such as multi-agent systems, but it is difficult to adapt to the individual-oriented state estimation task focused on in this paper. (iii) *k*-anonymity techniques: Privacy protection is realized through non-deceptive strategies. However, this technology was originally designed for static databases, making it incompatible with the state estimation scenarios of dynamic systems. Moreover, it fails to guarantee the state estimation accuracy after privacy-preserving processing.

It can be seen from above that existing methods cannot simultaneously satisfy the following three requirements: (1) no transmission of deceptive information; (2) realization of dual privacy protection for both receivers and third parties; and (3) guarantee a privacy-preserving degree and estimation accuracy. Hence, this paper is dedicated to addressing this key issue, which constitutes the research motivation of this work.

1.4. Research Objectives and Main Contributions

The aforementioned limitations motivate us to consider the research objectives as follows: "Design a privacy-preserving method to prevent the system states and sensor observations from being precisely known to the estimator, and the privacy is not protected by providing deceptive information." The main contributions are summarized as follows:

- **A privacy protection method is proposed by providing authentic information, other than providing deceptive information.** First, the deviation between the observations and the predicted one is computed; then, the deviation is randomly transmitted to the estimator. Compared with those that provides deceptive information by adding noises, the provided deviation is authentic information.
- **An optimal estimation with a desired privacy protection degree is designed.** By using the sequential Kalman filtering, an optimal estimator is derived. Then, an approach is developed to simultaneously achieve a desired privacy-protection degree and estimation accuracy by tuning a privacy-protection parameter.

The rest of this paper is organized as follows. The system model and the research objectives are introduced in Section 2. A proposed privacy protection strategy is designed in Section 3. An optimal estimation with privacy protection is proposed in Section 4. Experiments are presented in Section 5 to verify the effectiveness of the proposed method. The conclusions are given in Section 6.

2. System Description and Research Objectives

In this section, first, the system considered is introduced, and then the definition of privacy protection is given. Finally, the research objectives are presented.

2.1. System Setup

Consider a discrete-time linear system as follows:

- **Plant:**

$$x_{k+1} = Ax_k + w_k \tag{1}$$

$$y_k = Cx_k + v_k \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state vector, has an initial condition $x_0 \sim \mathcal{N}(\overline{x}_0, P_0)$, $y_k \in \mathbb{R}^q$ is the observation, and $w_k \in \mathbb{R}^n$ and $v_k \in \mathbb{R}^q$ are Gaussian white noises with zero means and variances $Q \geq 0$ and $R \geq 0$, respectively.

- **Privacy Protection:** Let $\Theta(\cdot)$ be a mapping that transmits the processed observations to the estimator:

$$z_k \triangleq \Theta(y_k).$$

The specific mapping process will be given in Equation (5) in the following Section 3.2.

- **Privacy-Preserving Estimator:** The optimal estimation $\widehat{x}_k$ is defined as, based on the process information $Z_k \triangleq \{z_1, \ldots, z_k\}$, $\widehat{x}_k$ is the one that minimizes, it is well known that the optimal estimate is

$$P_k \triangleq \mathbb{E}[(x_k - \widehat{x}_k)(x_k - \widehat{x}_k)'|Z_k] \tag{3}$$

The estimation error covariance P_k and the prediction error covariance (PEC) $\overline{P}_k = AP_{k-1}A' + Q$ are used to assess the estimation uncertainty.

The following assumptions are made: (A, C) is observable, and $(A, Q^{1/2})$ is controllable; w_k, v_k, and x_0 are mutually independent. R is a diagonal matrix.

Remark 1 (**Diagonal matrix *R***). *It is an assumption that R is a diagonal matrix. If R is not a diagonal matrix, by eigenvalue decomposition, one can obtain* $R = u\Lambda u'$, *where u is an orthogonal matrix and* Λ *is a diagonal matrix containing the eigenvalues of R. Then,* $y_k^* = uy_k$ *and* $C^* = uC$ *instead* y_k *and C. Then,* $y_k^* = C^* x_k + v_k^*$ *with* $v_k^* = uv_k$, *where* $v_k^* \sim \mathcal{N}(0, \Lambda)$.

2.2. Research Objectives

The research objectives include two parts:

(i) Determine the appropriate definition of privacy and then design a privacy protection method.

(ii) Design an optimal state estimator with a desired privacy-protection degree and estimation accuracy.

3. Design of Privacy Protection Method

In this section, we first give some privacy-related definitions. Based on them, we design a privacy protection Method.

3.1. Definitions on Privacy

Privacy protection refers to preventing the system states from being precisely estimated by the estimator. In other words, the estimation uncertainty should be larger than a certain degree. It is well known that the least estimation uncertainty can be obtained by Kalman filtering. Denote the PEC of the Kalman filtering by $\overline{P}_k^{\mathsf{kf}}$, which is convergent; denote its limit by $\overline{P}_\infty^{\mathsf{kf}}$. In this paper, we use the following quantity Δ as the **estimation uncertainty benchmark:**

$$\Delta \triangleq \|\overline{P}_\infty^{\mathsf{kf}}\|.$$

For an estimator, denote its prediction error covariance (PEC) by $\overline{P}_k$. Define its averaged estimation uncertainty from a long-term perspective, when it exists, as follows:

$$\mathbb{E}[\overline{P}_\infty] \triangleq \limsup_{k \to +\infty} \mathbb{E}[\overline{P}_k].$$

Definition 1 (**privacy-protection degree**). *An estimator is called to have a privacy-protection degree* α, *if*

$$\alpha\Delta \leq \|\mathbb{E}[\overline{P}_\infty]\|, \ \ \alpha > 1.$$

It is clear that state estimates with too large estimation uncertainty are often considered meaningless. Then, a definition on estimation accuracy upper bound is given as follows:

Definition 2 (**estimation accuracy**). *An estimator is called to have an estimation accuracy* β, *if*

$$\|\mathbb{E}[\overline{P}_\infty]\| \leq \beta\Delta, \ \ \beta > 1.$$

3.2. Design of a Privacy Protection Method

Before designing the privacy protection method, some notations are given as follows. The measurement Equation (2) can be rewritten as

$$y_k = \begin{bmatrix} y_k^{[1]} \\ y_k^{[2]} \\ \vdots \\ y_k^{[q]} \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_q \end{bmatrix} x_k + \begin{bmatrix} v_k^{[1]} \\ v_k^{[2]} \\ \vdots \\ v_k^{[q]} \end{bmatrix}$$

where $C \triangleq (c_1,\ c_2,\ \ldots,\ c_q)'$, $c_i \in \mathbb{R}^{1\times n}$, $v_k^{[i]} \sim \mathcal{N}(0,\sigma_i)$, and $R = \mathrm{diag}(\sigma_1,\ldots,\sigma_q)$.

The privacy-protection method, which consists of two parts as shown in Figure 2, is introduced as follows:

- *Direction deviation:* Denote the state perdition by $\overline{x}_k$ and the predicted observation by $\overline{y}_k^{[i]} = c_i\overline{x}_k$. According to the direction deviation $y_k^{[i]} - \overline{y}_k^{[i]}$, a quantity $e_k^{[i]}$ is determined as follows:

$$e_k^{[i]} = \begin{cases} +1, & y_k^{[i]} - \overline{y}_k^{[i]} \geq 0, \\ -1, & y_k^{[i]} - \overline{y}_k^{[i]} < 0. \end{cases}$$

  The directional deviation $e_k^{[i]}$, rather than the raw observation $y_k^{[i]}$, is transmitted to the estimator. In this way, the real spatial observation $y_k^{[i]}$ cannot be exactly known by the estimator.
- *Random transmission:* Let $\gamma_k^{[i]}$ be an i.i.d. Bernoulli random variable with

$$\Pr\{\gamma_k^{[i]} = 1\} = \lambda. \tag{4}$$

  $e_k^{[i]}$ is transmitted from the sensor to the estimator when $\gamma_k^{[i]} = 1$. In this way, the deviation information $e_k^{[i]}$ cannot be known by the estimator at every time step. That is,

$$z_k^{[i]} = \begin{cases} e_k^{[i]}, & \gamma_k^{[i]} = 1 \\ \emptyset, & \gamma_k^{[i]} = 0, \end{cases}$$

  where $\gamma_0^{[i]} = 0$, nothing is received at i-th entry, which is denoted by an empty set $\emptyset$. Then, the mapping $\Theta(y_k)$ can be written as

$$z_k = \Theta(y_k) = [z_k^{[1]},\ldots,z_k^{[q]}]'. \tag{5}$$

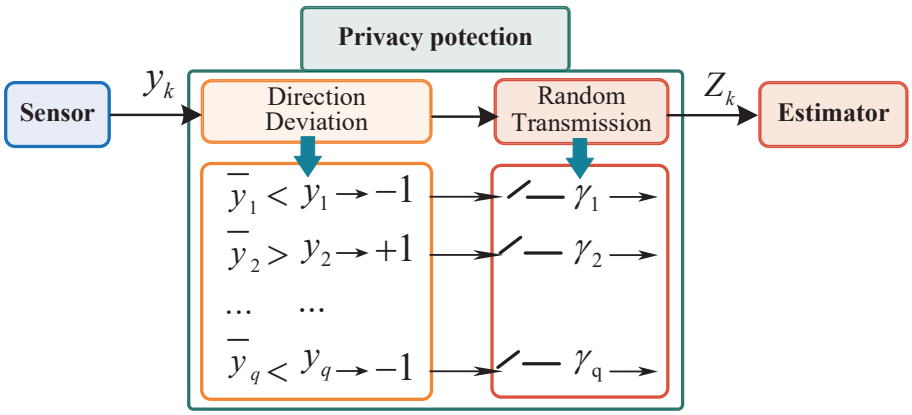


Figure 2. Privacy protection method.

4. Design of Privacy-Protection-Based Optimal Estimator

Based on the privacy-protection method, an optimal state estimator for the system in Equations (1) and (2) is developed by the sequential Kalman filtering technique in the following Theorem 1.

4.1. Design of Optimal Estimator

A preliminary result for proving Theorem 1 is given as follows.

Lemma 1. *Let*

$$Q(\delta) \triangleq \int_{\delta}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\Big(-\frac{t^2}{2}\Big)dt.$$

Then,

$$\int_{-\infty}^{+\infty} \delta Q\Big(-\frac{c}{\sigma}\delta\Big)\mathcal{N}_{\delta}(0,m)d\delta = \frac{mc^{'}}{\sqrt{2\pi}\sqrt{cmc^{'}+\sigma^2}}$$

Proof. By the definition of $\mathcal{N}_{\delta}(0,m)$, and using the method of integration by parts, we obtain

$$\begin{aligned}
&\int_{-\infty}^{+\infty} \delta Q\Big(-\frac{c\delta}{\sigma}\Big)\frac{\exp[-\frac{1}{2}\delta^{'}(m)^{-1}\delta]}{\sqrt{2\pi m}}d\delta \\
&= 0 - \int_{-\infty}^{+\infty} \frac{m}{\sqrt{2\pi m}} \exp\big(-\frac{\delta^{'}\delta}{2m}\big)\frac{c^{'}}{\sigma\sqrt{2\pi}} \exp\big(-\frac{\delta^{'}cc^{'}\delta}{2\sigma^2}\big)d\delta \\
&= \frac{c^{'}\sqrt{m}}{2\pi\sigma}\int_{-\infty}^{+\infty} \exp\Big(-\frac{\delta^{'}(\sigma^2+cmc^{'})\delta}{2m\sigma^2}\Big)d\delta \\
&= \frac{\sqrt{2/\pi}mc^{'}}{2\sqrt{cmc^{'}+\sigma^2}}.
\end{aligned}$$

The proof is completed. □

Theorem 1 (Privacy-Preserving Optimal Estimator). *Based on the privacy-protection method, the optimal estimator can be computed as follows:*

$$\begin{aligned}
\overline{x}_k &= A\widehat{x}_{k-1} \\
\overline{P}_k &= AP_{k-1}A' + Q
\end{aligned}$$

Initial conditions: $\widehat{x}_k^{[0]} = \overline{x}_k$ *and* $m_k^{[0]} = \overline{P}_k$.

For $i = 1$ *to* q,

$$K_k^{[i]} = \sqrt{2/\pi}m_k^{[i-1]}c_i^{'} \cdot (c_i m_k^{[i-1]}c_i^{'} + \sigma_i)^{-1/2} \tag{6}$$

$$\widehat{x}_k^{[i]} = \widehat{x}_k^{[i-1]} + \gamma_k^{[i]}K_k^{[i]}e_k^{[i]} \tag{7}$$

$$m_k^{[i]} = m_k^{[i-1]} - \gamma_k^{[i]}K_k^{[i]}(K_k^{[i]})^{'} \tag{8}$$

End for

$$\widehat{x}_k = \widehat{x}_k^{[q]} \qquad P_k = m_k^{[q]}$$

Proof. It is clear that Equations (7) and (8) hold when $\gamma_k^{[i]} = 0$. Hence, we consider the case that $\gamma_k^{[i]} = 1$ in the following.

We first compute $\widehat{x}_k^{[1]}$, and the others can be computed similarly.

Define $E_{k-1} \triangleq \Big\{(e_1^{[1]} \cdots e_1^{[q]}) \cup \cdots \cup (e_{k-1}^{[1]} \cdots e_{k-1}^{[q]})\Big\}$.

$$\begin{aligned}
\widehat{x}_k^{[1]} &\triangleq \mathbb{E}[x_k \mid E_{k-1}, e_k^{[1]}] \\
&= \int_{-\infty}^{+\infty} x_k\, p(x_k \mid E_{k-1}, e_k^{[1]})dx_k.
\end{aligned} \tag{9}$$

Then, $p(x_k \mid E_{k-1}, e_k^{[1]})$ is calculated using Bayes' rule

$$p(x_k \mid E_{k-1}, e_k^{[1]}) = \frac{p(e_k^{[1]} \mid x_k, E_{k-1}) \cdot p(x_k \mid E_{k-1})}{p(e_k^{[1]} \mid E_{k-1})}. \tag{10}$$

Calculate each factor in (10) separately. Note that the value of $e_k^{[1]}$ is ± 1.

$$\begin{aligned} \Pr\{e_k^{[1]} = \pm 1 \mid x_k, E_{k-1}\} &= \Pr\{v_k^{[1]} \gtrless [c_1(\hat{x}_k^{[0]} - x_k)] \mid x_k\} \\ &= Q\Big(\pm \frac{c_1(\hat{x}_k^{[0]} - x_k)}{\sigma_1} \Big). \end{aligned} \tag{11}$$

$$\begin{aligned} \Pr\{e_k^{[1]} = \pm 1 \mid E_{k-1}\} &= \Pr\{\bar{y}_k^{[1]} \gtrless \bar{y}_k^{[0]} \mid E_{k-1}\} \\ &= \frac{1}{2}. \end{aligned} \tag{12}$$

Assume that the prior probability is a Gaussian distribution. Then,

$$p(x_k \mid E_{k-1}, e_k^{[1]}) = \mathcal{N}(\hat{x}_k^{[0]}, m_k^{[0]}). \tag{13}$$

We first prove the case of $e_k^{[1]} = 1$. Substituting (10)–(13) into (9), we obtain

$$\hat{x}_k^{[1]} = 2 \int_{-\infty}^{+\infty} x_k \mathcal{N}(\hat{x}_k^{[0]}, m_k^{[0]}) Q\Big[\frac{c_1(\hat{x}_k^{[0]} - x_k)}{\sigma_1} \Big] dx_k. \tag{14}$$

Let $\delta_k = x_k - \hat{x}_k^{[0]}$. Then, we can write Equation (14) as

$$\hat{x}_k^{[1]} = \hat{x}_k^{[0]} + 2 \int_{-\infty}^{+\infty} \delta_k Q\Big[\frac{-c_1 \delta_k}{\sigma_1} \Big] \frac{\exp(-\frac{1}{2} \delta_k' (m_k^{[0]})^{-1} \delta_k)}{\sqrt{2\pi m_k^{[0]}}} d\delta_k \tag{15}$$

$$\begin{aligned} &= \hat{x}_k^{[0]} + \frac{(\sqrt{2/\pi} m_k^{[0]} c_1')}{\sqrt{c_1 m_k^{[0]} c_1' + \sigma_1^2}} \\ &= \hat{x}_k^{[0]} + K_k^{[1]}, \end{aligned} \tag{16}$$

where Equation (16) is obtained by using Lemma 1.

According to symmetry, the derivation for the cases $e_k^{[1]} = -1$ is the same as that for the case $e_k^{[1]} = 1$. It is easy to obtain that for $e_k^{[1]} = -1$, $\hat{x}_k^{[1]} = \hat{x}_k^{[0]} - K_k^{[1]}$. Consequently,

$$\hat{x}_k^{[1]} = \hat{x}_k^{[0]} + K_k^{[1]} e_k^{[1]}, \tag{17}$$

where $K_k^{[1]} = \sqrt{2/\pi} m_k^{[0]} {c_1}' \cdot (c_1 m_k^{[0]} {c_1}' + \sigma_1)^{-1/2}$. Hence, Equation (7) holds.

Then, Equation (8) is proved as follows:

$$\begin{aligned} m_k^{[1]} &= \mathbb{E}[(x_k - \hat{x}_k^{[0]} - e_k^{[1]} K_k^{[1]}) \cdot (x_k - \hat{x}_k^{[0]} - e_k^{[1]} K_k^{[1]})'] \\ &= m_k^{[0]} + K_k^{[1]} (K_k^{[1]})' \mathbb{E}[(e_k^{[1]})^2] - 2 K_k^{[1]} \mathbb{E}[e_k^{[1]} x_k'], \end{aligned} \tag{18}$$

where the first equality follows from the definition, and in the second equality, $m_k^{[0]} \triangleq \mathbb{E}[(x_k - \widehat{x}_k^{[0]}) \cdot (x_k - \widehat{x}_k^{[0]})']$ was used. The last term in Equation (18) can be obtained by noting that $\Pr\{e_k^{[1]} = \pm 1 | E_{k-1}\} = 1/2$, and then using the total probability.

$$\begin{aligned} \mathbb{E}[e_k^{[1]} x_k'] &= \frac{1}{2}\mathbb{E}[x_k' | e_k^{[1]} = 1] - \frac{1}{2}\mathbb{E}[x_k' | e_k^{[1]} = -1] \\ &= \frac{1}{2}(K_k^{[1]})' - \frac{1}{2}[-(K_k^{[1]})'] \\ &= (K_k^{[1]})'. \end{aligned} \tag{19}$$

Substituting Equation (19) into Equation (18) and noting that $\mathbb{E}\left[(e_k^{[1]})^2\right] = 1$, we obtain

$$m_k^{[1]} = m_k^{[0]} - K_k^{[1]}(K_k^{[1]})'. \tag{20}$$

Thus, Equation (8) holds for $i = 1$.

For a given $p(x_k | E_{k-1})$, when $e_k^{[1]}$ is available, how to use $e_k^{[1]}$ to update $\{\widehat{x}_k^{[0]}, m_k^{[0]}\}$ to $\{\widehat{x}_k^{[1]}, m_k^{[1]}\}$ is derived above. By using the sequential Kalman filtering technique, it is known that the derivations for updating $\{\widehat{x}_k^{[i-1]}, m_k^{[i-1]}\}$ to $\{\widehat{x}_k^{[i]}, m_k^{[i]}\}$ with $e_k^{[i]}$ are the same as the derivations above. Hence, by replacing $\{[0]$ and $[1]\}$ with $\{[i-1]$ and $[i]\}$ in Equations (7) and (8), we will obtain $\{\widehat{x}_k^{[i]}, m_k^{[i]}\}$, which are the same as in Equations (7) and (8). The proof is completed. □

4.2. Determine Privacy-Protection Degree and Estimation Accuracy

In the following, we will introduce how to design an optimal state estimator with a privacy-protection degree α and estimation accuracy β, that is,

$$\alpha\Delta \leq \|\mathbb{E}[\overline{P}_\infty]\| \leq \beta\Delta.$$

To achieve joint optimization of privacy protection and estimation accuracy, the error covariance must be constrained within a bounded interval.

In Theorem 1, $\widehat{x}_k$ and P_k are computed by the Sequential Kalman Filtering (SKF) technique, and the advantage is that it only deals with the same dimension data $e_k^{[i]}$ when $\gamma_k^{[i]} = 1$, without considering all $e_k^{[i]}$ and processing matrices operations. However, an analytical equation for P_k and $\overline{P}_k$, rather than Equation (8) in the For-End loop, will facilitate the analysis of estimation performance. Hence, a recursive equation for $\overline{P}_k$ is obtained in the following Lemma 2.

Lemma 2. *$\overline{P}_k$ in Theorem 1 can be expressed as follows:*

$$\overline{P}_{k+1} = A\left(\overline{P}_k^{-1} + H'\Gamma_k H\right)^{-1} A' + Q, \tag{21}$$

where $H \triangleq \sqrt{\frac{\pi}{2}R'}C$, $C \triangleq (c_1, c_2, \ldots, c_q)'$, $\Gamma_k \triangleq \mathrm{diag}(\gamma_k^{[1]}, \ldots, \gamma_k^{[q]})$, $R \triangleq \mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_q)$.

Proof. Let $\widetilde{\gamma}_k^{[i]} \triangleq \frac{2}{\pi}\gamma_k^{[i]}$. It has been shown in Equation (8) in [36] that the Riccati-like Equation (8) can be rewritten as

$$(m_k^{[i]}) = (m_k^{[i-1]})^{-1} + \widetilde{\gamma}_k^{[i]} c_i' \sigma_i^{-1} c_i. \tag{22}$$

By summing up the above equations from $i = 0$ to $i = q$ and then eliminating the same quantities $(m_k^{[i-1]})^{-1}$ from $i = 1$ to $q - 1$, we have

$$P_k = (m_k^{[q]}) = (m_k^{[0]})^{-1} + \sum_{i=1}^{q} \widetilde{\gamma}_k^{[i]} c_i' \sigma_i^{-1} c_i. \tag{23}$$

Note that $\gamma_k^{[i]} = \gamma_k^{[i]} * \gamma_k^{[i]}$ due to $\gamma_k^{[i]} = 0$ or 1.

$$\sum_{i=1}^{q} \widetilde{\gamma}_k^{[i]} c_i' \sigma_i^{-1} c_i = \frac{2}{\pi} \sum_{i=1}^{q} \gamma_k^{[i]} c_i' \sigma_i^{-1} \gamma_k^{[i]} c_i,$$

where

$$\begin{aligned}
\sum_{i=1}^{q} \gamma_k^{[i]} c_i' \sigma_i^{-1} \gamma_k^{[i]} c_i = & \begin{bmatrix} \gamma_k^{[1]} & 0 & \dots & 0 \\ 0 & \gamma_k^{[2]} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & \gamma_k^{[q]} \end{bmatrix} \begin{bmatrix} c_1' \\ \vdots \\ c_q' \end{bmatrix} \\
& \times \begin{bmatrix} \sigma_1^{-1} & 0 & \dots & 0 \\ 0 & \sigma_2^{-1} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & \sigma_q^{-1} \end{bmatrix} \times \begin{bmatrix} \gamma_k^{[1]} & 0 & \dots & 0 \\ 0 & \gamma_k^{[2]} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & \gamma_k^{[q]} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_q \end{bmatrix} \\
= & (\Gamma_k C)' R^{-1} (\Gamma_k C).
\end{aligned}$$

Let $\overline{R} = \frac{\pi R}{2}$. Both $\overline{R}^{-1/2}$ and Γ_k are diagonal matrices, and thus $\Gamma_k \overline{R}^{-1/2} = \overline{R}^{-1/2} \Gamma_k$ and $\Gamma_k \Gamma_k = \Gamma_k$ hold. Then,

$$\begin{aligned}
P_k &= \overline{P}_k^{-1} + (\Gamma_k C)' \overline{R}^{-1} (\Gamma_k C) \\
&= \overline{P}_k^{-1} + (\overline{R}^{-1/2} C)' \overline{R}^{-1/2} \Gamma_k \overline{R}^{-1/2} C) \\
&= (\overline{P}_k^{-1} + H' \Gamma_k H)^{-1}.
\end{aligned}$$

The proof is completed. □

To study the lower and upper bounds of $\overline{P}_k$, two functions are defined as follows:

$$f(X, \lambda) \triangleq (1 - \lambda)^n AXA' + Q \tag{24}$$

$$\phi(X, \lambda) \triangleq AXA' + Q - AXC'(T \otimes (CXC' + I_n))^{-1} CXA' \tag{25}$$

where $T = \mathbf{1}\mathbf{1}' + D_\lambda^{-1} I_n$, $\mathbf{1}$ is a column vector with all components equal to 1, $D_\lambda \triangleq \dfrac{\lambda}{1 - \lambda}$.

Construct two matrix sequences as follows:

$$\begin{aligned}
\overline{P}_{k+1}^{L} &= \phi(\overline{P}_k^{L}, \lambda) \\
\overline{P}_{k+1}^{U} &= f(\overline{P}_k^{U}, \lambda)
\end{aligned}$$

with $\overline{P}_1^L = \overline{P}_1^U = \overline{P}_1$. When $\overline{P}_k^L$ and $\overline{P}_k^U$ convergent, their limits are a function of λ, which are denoted as

$$\overline{P}^L(\lambda) \triangleq \lim_{k\to+\infty} \overline{P}_{k+1}^L = \lim_{k\to+\infty} \phi(\overline{P}_k^L, \lambda)$$
$$\overline{P}^U(\lambda) \triangleq \lim_{k\to+\infty} \overline{P}_{k+1}^U = \lim_{k\to+\infty} f(\overline{P}_k^U, \lambda).$$

The following theorem shows how to determine λ to satisfy the specified privacy protection requirement.

Remark 2 (**Stability of the Proposed Estimator**). *Denote $\{\delta_j\}, 1 \le j \le n$ as the set of n eigenvalues of A. Denote $k(A)$ as the set of all eigenvalues of A whose absolute values are greater than 1, and $r(A)$ as the product of all the elements of $k(A)$, that is, $k(A) \triangleq \{\delta_j \mid |\delta_j| > 1,\ 1 \le j \le n\}$, $r(A) \triangleq \prod_{\delta_j \in k(A)} |\delta_j|$. Let $(\overline{\lambda}) = 1 - \lambda$. If $(\overline{\lambda})^n = r(A)^{-2}$, then the estimator is stable [36].*

Theorem 2 (**Estimation with Privacy Protection**). *For given privacy protection degree α and estimation accuracy β with $\beta > \alpha > 1$, there exists a transmission rate λ as in Equation (4), such that the following requirement holds:*

$$\alpha\Delta < \|\mathbb{E}[\overline{P}_\infty]\| < \beta\Delta$$

Proof. We first prove that there exist unique λ_a and λ_b, such that

$$\|\overline{P}^U(\lambda_b)\| = \beta\Delta \tag{26}$$
$$\|\overline{P}^L(\lambda_a)\| = \alpha\Delta. \tag{27}$$

It is well known that the function of $\phi(X, \lambda)$ in Equation (25) is monotonically decreasing with respect to λ. Note that $\overline{P}^L(\lambda) = \phi(\overline{P}_k^L(\lambda))$ will tend to $+\infty$ as $\lambda \to 0$. It is clear that there exists a unique λ_b such that $\|\overline{P}^U(\lambda_b)\| = \beta\Delta$. The existence of a unique λ_a can be proved in the same way above.

For $\overline{P}_k$ in Equation (21), it has been reported in Proposition 1 and Lemma 1 in [36] that the following fact holds:

$$\overline{P}^L(\lambda) \le \|\mathbb{E}[\overline{P}_\infty]\| \le \overline{P}^U(\lambda). \tag{28}$$

By Equations (26) and (27), when

$$\lambda_a < \lambda < \lambda_b,$$

$\|\overline{P}^U(\lambda_b)\| = \beta\Delta$ and $\|\overline{P}^L(\lambda_a)\| = \alpha\Delta$. Then, we have $\alpha\Delta < \|\mathbb{E}[\overline{P}_\infty]\| < \beta\Delta$.

The proof is completed. □

5. Experiments and Comparison with Existing Methods

In this section, we first present numerical simulations to validate the theoretical results of this paper, including comparisons with other methods; then, we apply the proposed estimator to a real UAV system for practical verification.

5.1. Experiment for Tracking a Drone

In this section, the effectiveness of the proposed privacy-preserving state estimation is verified by tracking a drone in a laboratory, as shown in Figure 3.

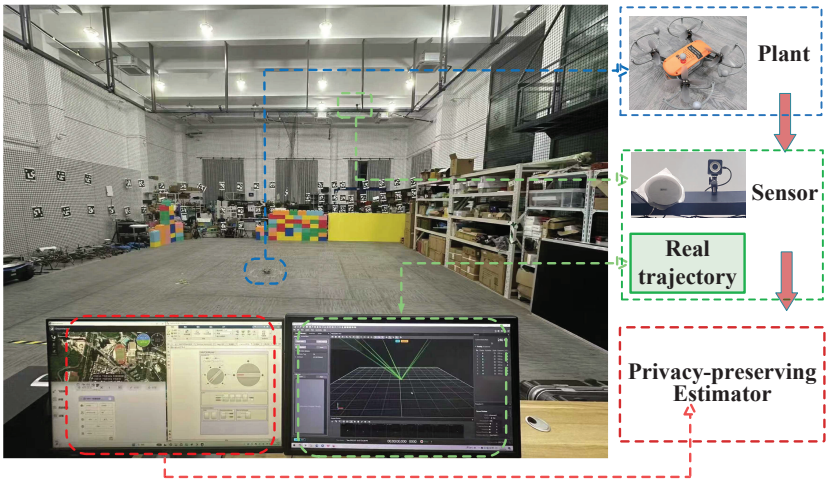


Figure 3. Laboratory with high−precision motion capture cameras for tracking drones.

Given the core importance of UAV trajectory privacy protection discussed in Section 1, this section experimentally validates the effectiveness and applicability of the proposed privacy-preserving method for UAV target tracking. As shown in the trajectory estimation results, the method can accurately infer the UAV's general flight direction; this accuracy suffices for scenarios requiring only the UAV's rough flight path and operation duration. Meanwhile, preset estimation deviations are imposed on the precise trajectory, thus protecting the privacy of sensitive UAV trajectory data.

The motion equation of the drone is the following:

$$A = \begin{bmatrix} 1 & t & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & t & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & t \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$R = 0.2I_3$, $Q = \mathrm{diag}(Q^*, Q^*, Q^*)$, where

$$Q^* = \begin{bmatrix} \frac{(t)^4}{4}\sigma^2 & \frac{(t)^3}{2}\sigma^2 \\ \frac{(t)^3}{2}\sigma^2 & (t)^2\sigma^2 \end{bmatrix},$$

with $t = 0.1$ and $\sigma = 1$.

Determine λ to achieve $\alpha\Delta \leq \|\mathbb{E}[\overline{P}_\infty]\| \leq \beta\Delta$: for the above system, the PEC of Kalman filtering converges to $\overline{P}_\infty^{\mathrm{kf}}$, and $\Delta = \|\overline{P}_\infty^{\mathrm{kf}}\| = 2.3$. For given privacy-protection degree $\alpha = 2$ and estimation accuracy $\beta = 4$, that is, $2\Delta \leq \|\mathbb{E}[\overline{P}_\infty]\| \triangleq \|\limsup_{k\to+\infty} \mathbb{E}[\overline{P}_k]\| \leq 4\Delta$. It is easy to obtain that $\lambda_a = 0.625$ and $\lambda_b = 0.760$. According to Theorem 2, the above requirement of privacy protection can be achieved by letting $\lambda = 0.7$, and the corresponding results for privacy protection are shown in Figure 4.

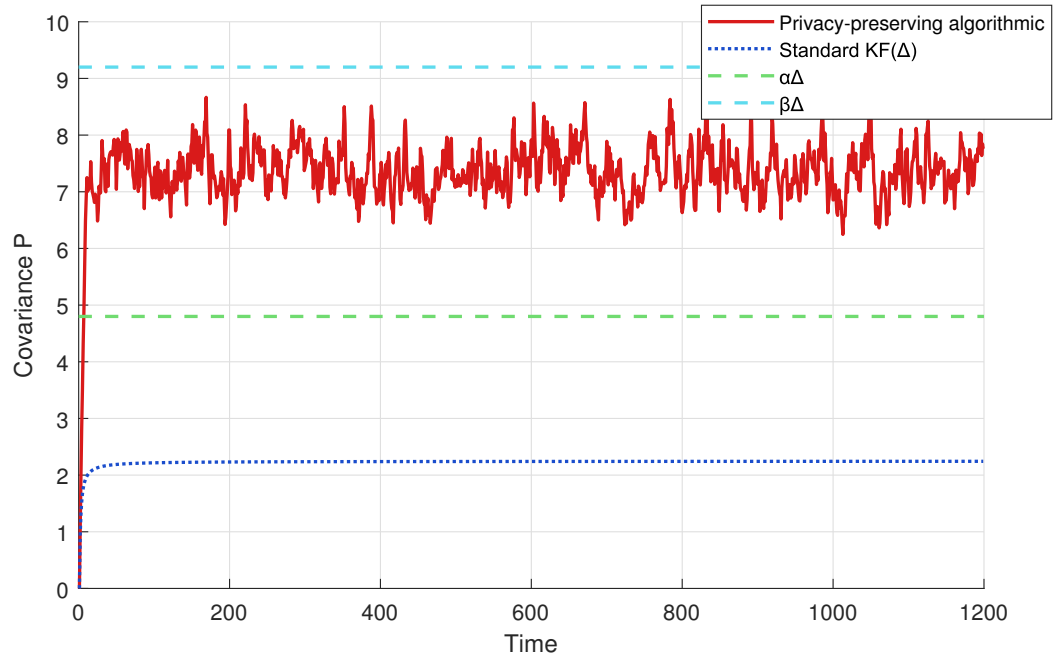


Figure 4. Relationship between privacy protection degree, estimation accuracy, $\|E[\overline{P}_k]\|$, and $\|\overline{P}_\infty^{\mathrm{kf}}\|$.

Trajectory tracking by the privacy-preserving estimator: The real trajectory of the drone captured by high-precision motion capture cameras is presented in Figure 5. Both the real and the estimated trajectories are presented in Figure 6. It shows that the tendency of the estimated trajectories is close to the real one, but the distance between the real one and the estimated one is greater than a certain value, which is related to the privacy protection degree; thus, the privacy protection method prevents the position of the drone from being precisely known to the estimator.

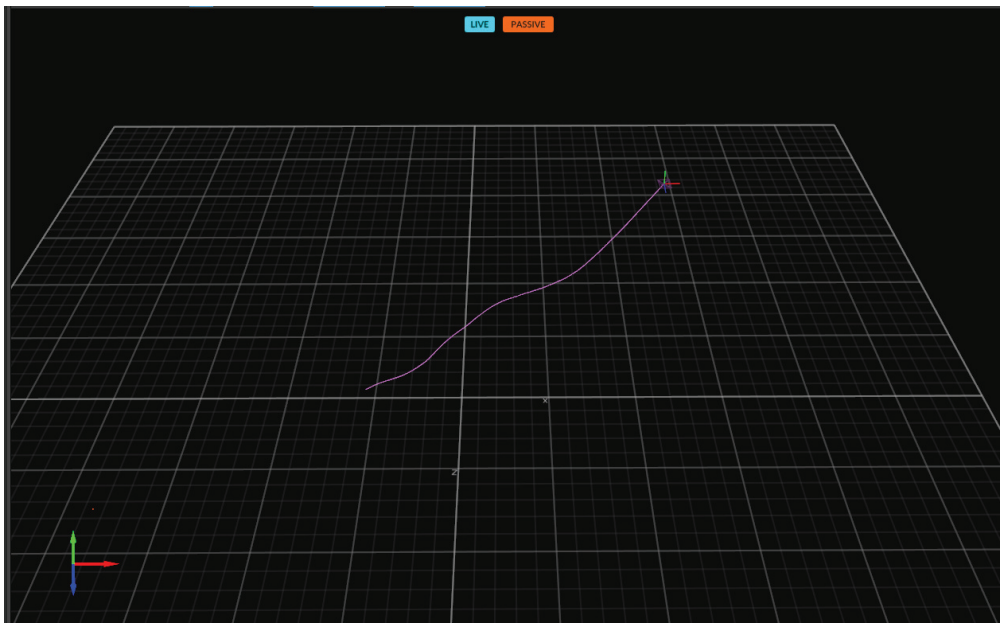


Figure 5. Real trajectories of the drone obtained by the motion capture cameras.

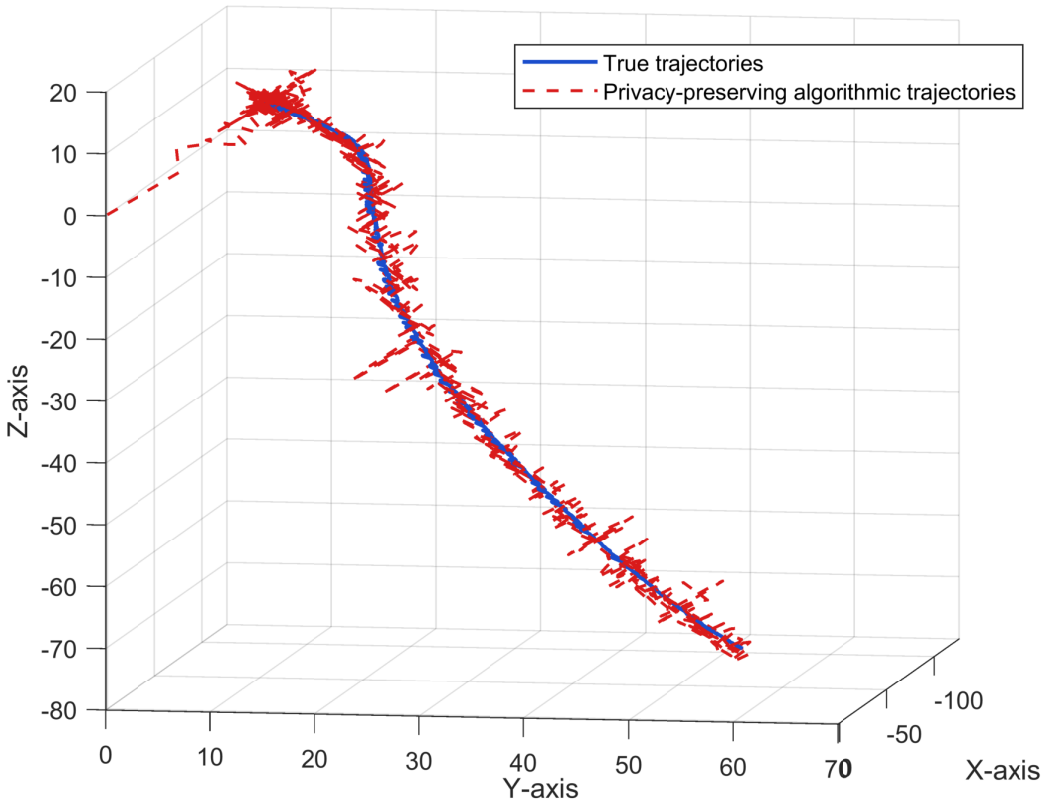
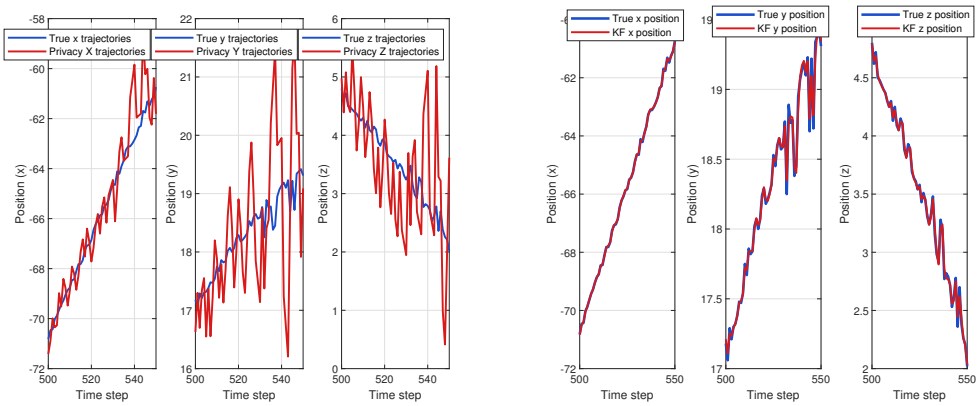


Figure 6. Tracking of the drone by the proposed privacy−preserving estimator.

The estimation results of the proposed estimator and the Kalman filter are presented in Figure 7a,b, respectively. It can be seen from these results that Kalman filtering provides precise estimation of the position, which sometimes are not expected by the system. Hence, the privacy-preserving estimator provides a less, but sufficiently, accurate estimate.



(**a**) (**b**)

Figure 7. (**a**) Target tracking in $x - y - z$ directions by the proposed privacy-preserving estimator. (**b**) Target tracking in $x - y - z$ directions by Kalman filter.

5.2. Comparison with the Existing Methods

As introduced in Section 1, some privacy-preserving methods have been developed for state estimation. In this section, we make a comparison among them, and conduct a numerical simulation to show the estimation results of them.

Some key aspects of the state-estimation-related privacy-preserving methods are presented in the following table.

Table 1 presents the characteristics of state estimation privacy protection methods across various dimensions: (i) "Retention of Authentic Information" measures whether the accuracy of original data is preserved. Only differential privacy methods cannot retain this (as they introduce noise to interfere with original data), while the others can. (ii) "Adjustable Estimation Performance" refers to the ability to tailor state estimation accuracy as needed. Only the method proposed in this paper supports this capability, while the others do not. (iii) "Observation Data Protection" evaluates whether privacy is safeguarded for observers. Only the data encryption method does not protect observers (covering only transmission or storage phases), while the others do. (vi) "Computational Complexity" reflects resource consumption. The proposed method, differential privacy, and anti-eavesdropping approaches exhibit LOW complexity (using basic operations like vector manipulations and simple noise addition). Data encryption requires HIGH complexity (involving complex cryptographic operations such as polynomial ring operations for homomorphic encryption and bilinear pairings for attribute-based encryption).

Table 1. Privacy-preserving methods in state estimation.

Privacy-Preserving Methods	True Information	Tunable Estimation Performance	Protection of Observations	Computational Complexity
Proposed method in this paper	✓	✓	✓	LOW
Differential privacy [23,30]	×	×	✓	LOW
Eavesdrop [37]	✓	×	✓	LOW
Data encryption [18]	✓	×	×	HIGH

Numerical simulation is based on the following equations of motion:

$$A = \begin{bmatrix} 1.01 & -0.02 \\ 0.02 & 0.98 \end{bmatrix}, \quad Q = \begin{bmatrix} 1.35 & 0.1 \\ 0.1 & 1.35 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$R = 0.35I_2$.

For the aforementioned system, we systematically compared the proposed algorithm, anti-eavesdropping techniques, and cryptographic methods. Figure 8 illustrates the evolution of covariance over time steps for the three approaches. The data encryption method achieves covariance (consistent with KF) but only protects the data transmission process. This approach fails to constrain the state estimation accuracy of the estimator and does not provide privacy protection for the receiver. Although anti-eavesdropping techniques demonstrate stronger convergence and superior privacy protection capabilities, their estimation accuracy is fixed, lacking flexibility for adjustment. In contrast, the algorithm proposed in this paper achieves dynamic adaptation between privacy protection and estimation accuracy by adjusting the transmission probability λ, while simultaneously preventing observers from obtaining precise information.

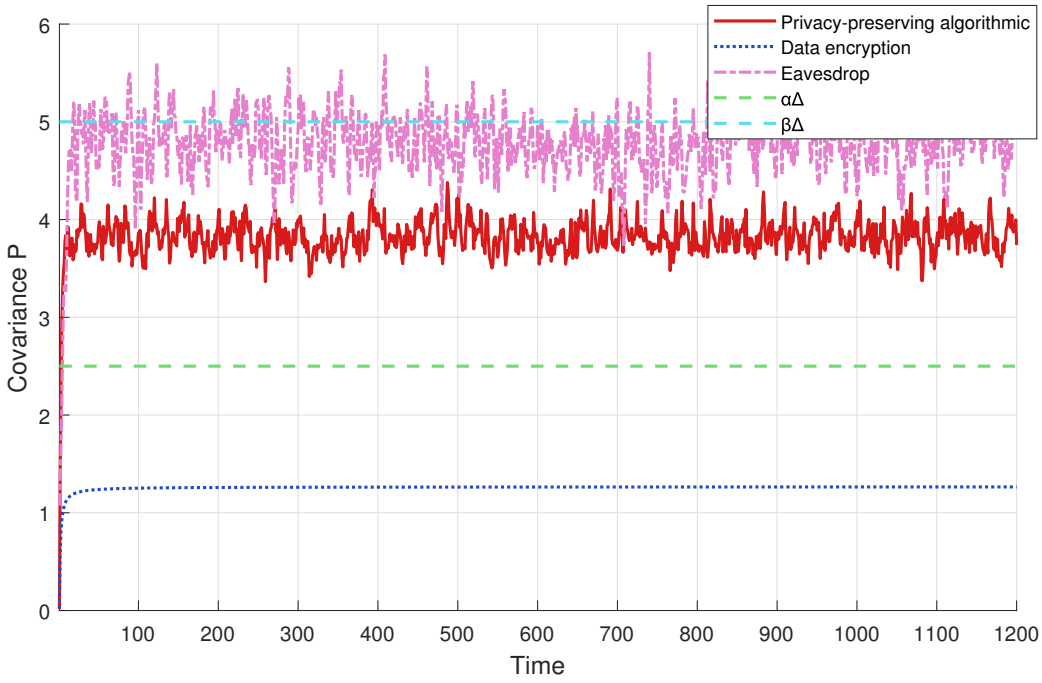


Figure 8. Simulation variance comparison.

6. Conclusions

This paper proposes a privacy protection strategy that combines direction deviation and random transmission. This method ensures that the true measurement values of the sensor will not be precisely disclosed to the estimator, thereby protecting the privacy of system state as well as the observations. The drone-tracking experiments have demonstrated the effectiveness of the proposed method. Future research will focus on extending this method to nonlinear systems and multi-agent systems with distributed privacy-preserving estimation methods.

Author Contributions: Conceptualization, H.L.; Methodology, Y.L.; Validation, S.W.; Formal analysis, Y.W. and H.L.; Investigation, S.W.; Writing—original draft, Y.W.; Writing—review & editing, Y.L. and H.L.; Supervision, S.W. and H.L.; Funding acquisition, H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by Research Projects of Department of Education of Guangdong Province (2025KTSCX251), in part by Shenzhen Polytechnic University Research Fund (602331015PQ), in part by Shenzhen Major Science and Technology Project (KCXFZ20240903093923031), and in part by 2025 College-Level Doctoral Fund Project of Guangzhou Nanfang College (2025BQ104).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Notations

$\mathcal{N}_x(\mu, P)$	Random variable x follows a Gaussian probability density function (pdf) with mean μ and covariance P. $\mathcal{N}(\mu, P)$ is used when the random variable is clear from the context.
$x \sim \mathcal{N}(\mu, P)$	Random variable x follows a Gaussian pdf $\mathcal{N}(\mu, P)$.
$p(\cdot)$, $p(\cdot\|\cdot)$	pdf and conditional pdf, respectively.
$\mathbb{E}[\cdot]$	Mathematical expectation.

$\|\cdot\|$	The norm of a matrix.
$Pr(\cdot)$	Probability measure.
$(A)_{ij}$	The element of matrix A in the i-th column and the j-th low.
$A \otimes B$	The Hadamard product of matrices A and B is a matrix with its elements computed as $(A \otimes B)_{ij} = (A)_{ij}(B)_{ij}$.
I_n	An n-th dimensional identity matrix.

References

1. Cao, S.; Wang, T.; Li, T.; Fei, S. UAV Real-Time Target Detection and Tracking Algorithm Based on Improved KCF and YOLOv5s_MSES. *Machines* **2025**, *13*, 364. [CrossRef]
2. Sharghi, A.; Karimi, B.; Dehghan, S.M. Fixed-time adaptive multi-target tracking control in unknown nonlinear MIMO multi-agent systems using a distributed allocation algorithm. *Frankl. Open* **2025**, 100285.. [CrossRef]
3. Zhang, J.; Xu, Z.; Liu, H.; Zhu, X.; Lan, B. An Improved Hybrid Ant Colony Optimization and Genetic Algorithm for Multi-Map Path Planning of Rescuing Robots in Mine Disaster Scenario. *Machines* **2025**, *13*, 474. [CrossRef]
4. Huang, C.; Wang, T.; Wang, S.; Xu, J. Dynamic path planning for spacecraft rendezvous and approach based on hybrid honey badger algorithm. *J. Frankl. Inst.* **2025**, *362*, 107398. [CrossRef]
5. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
6. Zhang, J.; Mao, S.; Yang, L.; Ma, W.; Li, S.; Gao, Z. Physics-informed deep learning for traffic state estimation based on the traffic flow model and computational graph method. *Inf. Fusion* **2024**, *101*, 101971. [CrossRef]
7. Natarajan, R.; Reddy, S.; Bose, S.C.; Gururaj, H.; Flammini, F.; Velmurugan, S. Fault detection and state estimation in robotic automatic control using machine learning. *Array* **2023**, *19*, 100298. [CrossRef]
8. Dibaji, S.M.; Hussain, A.; Ishii, H. A tutorial on security and privacy challenges in CPS. In *Security and Resilience of Control Systems: Theory and Applications*; Springer: Cham, Switzerland, 2022; pp. 121–146.
9. Sivaraman, D.; Pillai, B.M.; Ongwattanakul, S.; Suthakorn, J. Adaptive polynomial predictive filter for sensor data estimation and prediction in interference environment. *IET Control Theory Appl.* **2025**, *19*, e12771. [CrossRef]
10. Sun, Q.; Qi, X.; Du, D.; Ren, X.; Fei, M. Event-triggered output feedback model predictive control for path following of autonomous vehicles under false data injection attacks. *IEEE Trans. Intell. Veh.* **2024**, *10*, 323–335. [CrossRef]
11. Skuta, A.; Steurer, P.; Hegenbart, S.; Hoch, R.; Loruenser, T. Towards privacy-preserving machine learning for energy prediction in industrial robotics: Modeling, evaluation and integration. *Machines* **2025**, *13*, 780. [CrossRef]
12. Binjubeir, M.; Ahmed, A.A.; Ismail, M.A.B.; Sadiq, A.S.; Khan, M.K. Comprehensive survey on big data privacy protection. *IEEE Access* **2019**, *8*, 20067–20079. [CrossRef]
13. Yang, P.; Xiong, N.; Ren, J. Data security and privacy protection for cloud storage: A survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
14. Yang, W.; Li, D.; Zhang, H.; Tang, Y.; Zheng, W.X. An encoding mechanism for secrecy of remote state estimation. *Automatica* **2020**, *120*, 109116. [CrossRef]
15. Shang, J.; Chen, T. Linear encryption against eavesdropping on remote state estimation. *IEEE Trans. Autom. Control* **2022**, *68*, 4413–4419. [CrossRef]
16. Gao, P.; Jia, C.; Zhou, A. Encryption–decryption-based state estimation for nonlinear complex networks subject to coupled perturbation. *Syst. Sci. Control Eng.* **2024**, *12*, 2357796. [CrossRef]
17. Yang, H.; Yan, H.; Li, Y.; Wen, P.; Yang, F. Secure zonotopic set-membership state estimation for multirate complex networks under encryption–decryption mechanism. *IEEE Trans. Autom. Control* **2023**, *69*, 5109–5124. [CrossRef]
18. Farokhi, F.; Shames, I.; Batterham, N. Secure and private control using semi-homomorphic encryption. *Control Eng. Pract.* **2017**, *67*, 13–20. [CrossRef]
19. Lu, Y.; Zhu, M. Privacy preserving distributed optimization using homomorphic encryption. *Automatica* **2018**, *96*, 314–325. [CrossRef]
20. Huang, J.; Gao, C.; He, X. Privacy-preserving state estimation with unreliable channels. *ISA Trans.* **2022**, *127*, 4–12. [CrossRef]
21. Yuan, H.; Yang, W.; Wang, J.; Ding, W. Privacy-Preserving State Estimation Under Quantized Innovation via the Exponential Mechanism. *IEEE Internet Things J.* **2025**, *12*, 41990–42000. [CrossRef]
22. Li, M.Q.; Chang, X.H. Finite-horizon quantized security output feedback control for time-varying cyber-physical systems: Based on encryption strategy. *J. Frankl. Inst.* **2025**, *362*, 108003. [CrossRef]
23. Wang, Y.; Lin, H.; Lam, J.; Kwok, K.W. Differentially private consensus and distributed optimization in multi-agent systems: A review. *Neurocomputing* **2024**, *597*, 127986. [CrossRef]

24. Liu, H.; Zou, J.; Ren, X.; Wang, X. A privacy-preserving approach against eavesdropping attacks on remote state estimation for cyber–physical systems. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *71*, 1221–1225. [CrossRef]
25. Si, K.; Li, P.; Yuan, Z.P.; Jiang, X.D.; Wei, Z.X. Privacy-Preserving Distributed Kalman Filtering Based on State Decomposition and Dynamic Mask. *IEEE Trans. Aerosp. Electron. Syst.* **2024**, *61*, 5839–5852. [CrossRef]
26. Zou, J.; Liu, H.; Liu, C.; Ren, X.; Wang, X. Optimal privacy-preserving transmission schedule against eavesdropping attacks on remote state estimation. *IEEE Control Syst. Lett.* **2024**, *8*, 538–543. [CrossRef]
27. Ramya, M.R.; Kumar, P.; Dhanasekaran, M.D.; Kumar, M.R.S.; Sharavan, S.A. A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques. *Frankl. Open* **2025**, *10*, 100223. [CrossRef]
28. Zhou, I.; Tofigh, F.; Piccardi, M.; Abolhasan, M.; Franklin, D.; Lipman, J. Secure multi-party computation for machine learning: A survey. *IEEE Access* **2024**, *12*, 53881–53899. [CrossRef]
29. Qin, S.; He, J.; Fang, C.; Lam, J. Differential private discrete noise-adding mechanism: Conditions, properties, and optimization. *IEEE Trans. Signal Process.* **2023**, *71*, 3534–3547. [CrossRef]
30. Ye, D.; Shen, S.; Zhu, T.; Liu, B.; Zhou, W. One parameter defense—Defending against data inference attacks via differential privacy. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1466–1480. [CrossRef]
31. Mahanan, W.; Chaovalitwongse, W.A.; Natwichai, J. Data privacy preservation algorithm with k-anonymity. *World Wide Web* **2021**, *24*, 1551–1561. [CrossRef]
32. Kumar, G.S.; Premalatha, K. Securing private information by data perturbation using statistical transformation with three dimensional shearing. *Appl. Soft Comput.* **2021**, *112*, 107819. [CrossRef]
33. Wang, Y.; Lam, J.; Lin, H. Differentially private average consensus with general directed graphs. *Neurocomputing* **2021**, *458*, 87–98. [CrossRef]
34. Wang, Y.; Lam, J.; Lin, H. Consensus of linear multivariable discrete-time multiagent systems: Differential privacy perspective. *IEEE Trans. Cybern.* **2022**, *52*, 13915–13926. [CrossRef]
35. Wang, Y.; Lam, J.; Lin, H. Differentially private average consensus for networks with positive agents. *IEEE Trans. Cybern.* **2023**, *54*, 3454–3467. [CrossRef]
36. Yang, C.; Zheng, J.; Ren, X.; Yang, W.; Shi, H.; Shi, L. Multi-sensor Kalman filtering with intermittent measurements. *IEEE Trans. Autom. Control* **2017**, *63*, 797–804. [CrossRef]
37. Tsiamis, A.; Gatsis, K.; Pappas, G.J. State estimation with secrecy against eavesdroppers. *IFAC-PapersOnLine* **2017**, *50*, 8385–8392. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.