Privacy-Preserving Distributed Estimation Over Sensor Networks With Multistrategy Injection Attacks: A Chaotic Encryption Scheme

Lijuan Zha, Jinzhao Miao, Jinliang Liu, *Senior Member, IEEE*, Engang Tian, *Senior Member, IEEE*, and Chen Peng, *Senior Member, IEEE*

***Abstract*—This article explores the distributed set-membership state estimation problem over sensor networks (SNs) with chaotic encrypted privacy-preserving scheme and multistrategy injection attacks (MIAs). Since potential eavesdroppers in communication networks may intercept the transmitted measurement signals, chaotic encryption is adopted as a privacy-preserving scheme to protect the system state information from being revealed. The measurement signals are encrypted before transmission and decrypted upon reception by the remote estimator. A newly devised attack model is developed to characterize the injection attacks, which occur randomly and involve a combination of multiple attack strategies. By employing matrix inequality techniques, a unified set-membership estimation scheme is developed when both the privacy-preserving scheme and the MIAs coexist. Subsequently, based on the sufficient condition of constraining the estimation error within an ellipsoidal range, an optimization problem is formulated to achieve the optimal estimation performance at each time step, along with the development of a recursive algorithm for computing the required estimator parameters. Finally, simulation is provided to verify the set-membership estimation approach under the chaotic encryption scheme.**

***Index Terms*—Chaotic encryption, multistrategy injection attacks (MIAs), privacy-preserving scheme, sensor networks (SNs), state estimation.**

Received 16 November 2024; revised 13 March 2025; accepted 6 April 2025. Date of publication 25 April 2025; date of current version 18 June 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62273174, Grant 62373252, and Grant 62441310; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20230063; and in part by the Startup Foundation for Introducing Talent of NUIST under Grant 2024r063. This article was recommended by Associate Editor P. Fierens. *(Corresponding author: Jinliang Liu.)*

Lijuan Zha is with the School of Science, Nanjing Forestry University, Nanjing 210037, China (e-mail: zhalijuan@vip.163.com).

Jinzhao Miao is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: miaojinzhao2022@163.com).

Jinliang Liu is with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: liujinliang@vip.163.com).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Chen Peng is with the School of Mechatronic Engineering and Automation, Department of Automation, Shanghai University, Shanghai 200444, China (e-mail: c.peng@shu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2025.3560404.

Digital Object Identifier 10.1109/TSMC.2025.3560404

I. Introduction

RECENTLY, sensor networks (SNs) have garnered considerable attention because of their widespread applications in various domains, e.g., industrial automation, power grids, traffic control, and mobile robots [1], [2], [3]. SNs consists of numerous distributed sensor nodes, each node is capable of sharing data with other nodes through the network. As one of the most common practical problems within the domain of signal processing, distributed state estimation on SNs has garnered significant attention from researchers owing to its notable advantages in robustness, adaptability, and flexibility [4], [5], [6].

The primary advantage of distributed estimation over SNs lies in the accuracy and stability of estimation through collaboration and information fusion among nodes [7], [8], [9]. In distributed estimation, each individual node conducts local estimation of the target state utilizing its own measured state information. Nodes exchange estimation results and measurement data through the network to collectively accomplish the state estimation task [10], [11], [12]. Up to this point, numerous researchers have achieved some accomplishments in investigating the issue of distributed estimation in SNs. A novel distributed estimator based on indicator functions is developed in [7] by combining energy harvesting and intermittent information exchange in SNs. In [13], distributed recursive estimation problem of multirate systems in SNs is explored, utilizing the FlexRay protocol for scheduling communication among the sensors. Distributed estimation of SNs with measurement noise is investigated in [14], employing a dynamic event-triggered scheme to alleviate resource constraints. However, there has been relatively little attention paid to the issue of privacy preserving in SNs, which stands as the key impetus for this article.

SNs typically involve sensitive information due to their application scenarios and deployment environments [15]. For instance, surveillance systems in smart homes and biometric data in health monitoring devices, may contain sensitive information such as personal identities, location details, and health conditions [16]. To mitigate the risk of sensitive information leakage and enhance data confidentiality, it is essential to implement privacy protection for critical data in SNs [17]. Currently, some progress has been made in addressing the issue of encrypting privacy data in networked systems. In [18], a distributed dispatch method is developed

to protect the data privacy in microgrids, employing a random state decomposition method to forestall the disclosure of confidential power information. A dynamic key-driven encryption scheme for privacy-preserving sampling data is investigated in [19], along with the proposal of a distributed proportional-integral observer applicable to vehicular network-physical systems. In [20], a novel privacy-preserving scheme is proposed that involves injecting artificial noise into measurement signals for encryption, and a new metric is established for security assessment of signal transmission. Although the encryption technology used in the aforementioned paper can prevent malicious adversaries from eavesdropping on private data, in open network environments, there is a significant likelihood that malicious adversaries may simultaneously initiate other network attacks. Therefore, this article introduces a chaotic encryption scheme to encrypt sensitive data, which can simultaneously mitigating data tampering caused by network attacks during the transmission process.

Note that the existing distributed privacy protection methods, such as homomorphic encryption and differential privacy have been widely applied [21]. However, they still face significant limitations in practical deployment. For instance, the high computational complexity and storage overhead associated with homomorphic encryption often make it challenging to apply it on resource-constrained sensor nodes [22]. Moreover, homomorphic encryption incurs considerable energy and bandwidth consumption in large-scale distributed SNs, which makes its deployment difficult in dynamic, resource limited environments [23]. Differential privacy, on the other hand, requires the addition of noise, directly impacting data accuracy and subsequently reducing the precision of estimation results in distributed estimation tasks [21]. In contrast, chaotic addition exploits the strong dependence of chaotic sequences on their initial conditions, along with their inherent unpredictability, to establish an efficient and lightweight encryption scheme. The computational complexity of the chaotic encryption algorithm are typically $O(\mathcal{L}+\mathcal{M})$, where $\mathcal{L}$ represents the length of the chaotic sequence and $\mathcal{M}$ denotes the size of the data to be encrypted. In contrast, homomorphic encryption schemes often involve computationally intensive operations such as modular exponentiation or polynomial arithmetic, typically resulting in a complexity of at least $O(\mathcal{M}\log\mathcal{M})$ or higher. Due to its significantly lower computational overhead, chaotic encryption is well-suited for resource-constrained sensor nodes, enabling distributed estimation while maintaining data privacy [24]. Additionally, chaotic encryption performs encryption and decryption through XOR operations, thereby protecting privacy without compromising estimation accuracy. This characteristic makes chaotic encryption-based privacy protection schemes better suited for application scenarios that demand high-precision estimation. For now, in [25], the application of chaotic encryption algorithm for the secure transmission of privacy data in industrial control systems is explored. The dynamical characteristics of a multiwing chaotic system are investigated in [24], and the application of chaotic encryption is implemented in practical problems. However, there remains a research gap regarding chaos encryption-based privacy-preserving schemes over SNs. Therefore, designing a chaos encryption-based distributed privacy-preserving scheme for deployment in SNs holds significant security importance.

Given that eavesdropping attacks often occur alongside other network attacks in the open network environment, in addition to potential eavesdroppers, other attacks may also pose threats to the system security. Frequently occurring network attacks include deception attacks, false data injection (FDI) attacks [26], [27], [28], DoS attacks [29], [30], replay attacks [31], and so on. The FDI attacks, which are notable for their prominence in both stealthiness and destructiveness, have garnered attention from some researchers [32]. In [33], the security estimation is investigated where the joint attacks on estimator and communication channel are addressed with resource limitations. The FDI attacks strategy for tampering with partial sensor measurement data is proposed in [34], and sufficient conditions for maintaining the stealthiness of FDI attacks are derived. Intermittent FDI attacks in cyber-physical systems are investigated in [35] to reduce the impact of actuator attacks on the system posterior estimation error. However, the vast majority of current research findings on FDI attacks rely on the assumption of a certain attack strategy. In order to enhance the success rate of their attacks, malicious attackers often employ FDI attacks that involve multiple strategies rather than relying on single strategy. Attack signals may exhibit adaptive or highly targeted characteristics, with attackers continually adjusting their strategies based on system feedback. For improving the stability and robustness of estimation systems, establishing a comprehensive model of FDI attacks that can primarily captures the randomness of strategy combinations is necessary. The proposed multistrategy injection attacks (MIAs) in this article will incorporate different FDI attacks simulation methods [26], [27], [28] to achieve multistrategy attacks in the simulation section. This is another prominent highlight of this article.

In order to address eavesdropping attacks by potential adversaries in communication networks, as well as random FDI attacks with multiple attack strategies, a privacy-preserving scheme based on chaotic encryption and decryption is proposed for ensuring the privacy of critical data containing system state information over SNs. The unique features of this article are summarized as follows:

1) A new distributed set-membership estimation (DSME) scheme over SNs is proposed, which takes into account the chaotic encryption privacy-preserving scheme and multiple attack strategies. Through the use of recursive matrix inequalities (RMIs), the estimation errors are restricted within a specified ellipsoidal range and the optimal estimator gain matrices are achieved through the minimization of the constraint matrix.
2) In order to safeguard the confidentiality of sensitive data in communication networks, a privacy-preserving scheme based on chaotic encryption and decryption is utilized, which defends against potential eavesdropping attacks and safeguards the confidentiality of the system state information.
3) Compared to the existing FDI attacks model [26], [27], [28], a MIAs model is proposed to reflect more realistic adversarial behaviors, which

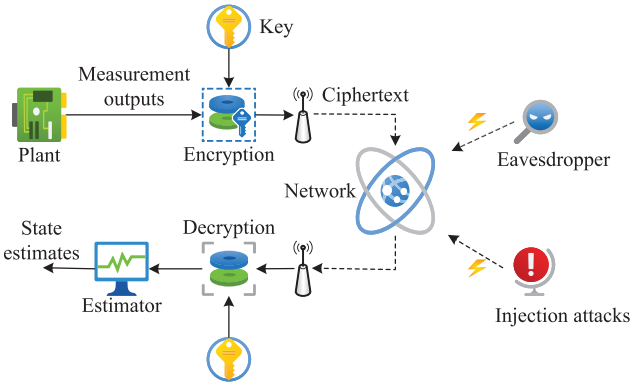

Fig. 1. Networked state estimation with eavesdropper and MIAs.

incorporates a combination of attack strategies and introduces a higher level of unpredictability and stealth.

Notation: $\mathbb{R}^n$ stands for the n-dimensional Euclidean space. $\mathbb{R}^{n\times m}$ denotes the set of $n \times m$ real matrices. M^{T} represents the transpose of the matrix M. $\|\cdot\|$ denotes the Euclidean norm. diag$\{\cdot\}$ represents the diagonal matrix. I and $\mathbf{0}$ represent the identity matrix and zero matrix of compatible dimension, respectively. $\mathbb{E}\{z\}$ means the expectation of the stochastic variable z. $z_1 \oplus z_2$ stands for the Exclusive OR (XOR) operations between z_1 and z_2. $z_1 \circ z_2$ denotes the Hadamard product and represents the element-wise multiplication of two matrices or vectors of the same dimension.

II. Problem Formulation

The communication topology of the SNs with N nodes in this article is described by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with the set of nodes $\mathcal{V} = \{1, 2, \ldots, N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ and the non-negative adjacency matrix $\mathcal{A} = [a_{ij}]_{N\times N}$. The edges of $\mathcal{G}$ are represented by ordered pairs (i, j), where $(i, j) \in \mathcal{E}$ indicating that node i can receive information from node j, and node j is referred to as one of the neighbors of node i. Define $\mathcal{N}_i = \{j \in \mathcal{V} | (i, j) \in \mathcal{E}\}$ as the set of all neighbors of node i.

A. System Model

Consider the state estimation problem illustrated in Fig. 1, the encrypted measurement signal may be intercepted by potential eavesdroppers and subjected to random occurrences of MIAs. The time-varying system with N spatially distributed sensors that represents the plant under investigation is characterized by

$$\begin{cases} x(k+1) = A(k)x(k) + B(k)\omega(k) \\ y_i(k) = C_i(k)x(k) + D_i(k)v_i(k), \quad i \in \mathcal{V} \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the system state and $y_i(k) \in \mathbb{R}^{n_y}$ is the measurement output of the ith sensor. $\omega(k) \in \mathbb{R}^{n_\omega}$ and $v_i(k) \in \mathbb{R}^{n_v}$ are the process and measurement noises, respectively. $A(k)$, $B(k)$, $C_i(k)$, and $D_i(k)$ are known matrices with appropriate dimensions.

Assumption 1: The unknown noise $\omega(k)$ and $v_i(k)$ are bounded and constrained within the following ellipsoids

$$\mathcal{W}(k) = \left\{\omega(k) : \omega(k)^{\mathrm{T}} W^{-1}(k)\omega(k) \le 1\right\} \tag{2}$$

$$\mathcal{V}(k) = \left\{v_i(k) : v_i^{\mathrm{T}}(k) V_i^{-1}(k) v_i(k) \le 1\right\} \tag{3}$$

where $W(k) > 0$ and $V_i(k) > 0$ are known matrices.

B. Privacy-Preserving Scheme

Generally, measurement output is transmitted to the remote estimator through a secure and reliable network. However, because of the inherent openness and susceptibility of the network, there exists the leakage risk of measurement data that may be intercepted by potential eavesdroppers when being transmitted to the remote estimator via the communication network. Therefore, a privacy-preserving scheme based on chaotic encryption and decryption is adopted during signal transmission to safeguard the privacy of measurement data.

Before transmitting measurement data to the remote estimator, the plaintext $y_i(k)(i \in \mathcal{V})$ is encrypted through employing chaotic encryption-decryption technique. Similarly to [36], the detailed steps of chaotic encryption are described below:

Generate chaotic sequences $\tilde{s}_i(k)$ as keys by employing the following Logistic Equation:

$$s(t+1) = E_i(k)s(t)(1 - s(t)) \tag{4}$$

where the parameter $E_i(k) \in [3.58, 4]$ and $s(0) = \bar{s}_i(0)$.

After iterating the chaotic system (4) $\tilde{t}$ times, set the key $\tilde{s}_i(k) = [s^{\mathrm{T}}(\tilde{t}), s^{\mathrm{T}}(\tilde{t}-1), \ldots, s^{\mathrm{T}}(\tilde{t}-n_y+1)]^{\mathrm{T}}$. Since XOR operations in chaotic encryption can only be performed on integers, it is necessary to scale up the measurement output $y_i(k)$ and the chaotic key $\tilde{s}_i(k)$ to eliminate the decimal component.

The process of chaotic encryption is formalized as follows:

$$\tilde{y}_i(k) = \Pi_i(-d)((\Pi_i(d)y_i(k)) \oplus (\Pi_i(d+2)\tilde{s}_i(k))) \tag{5}$$

where $\tilde{y}_i(k)$ represents the generated ciphertext, and $\Pi_i(d) = \mathrm{diag}_{n_y}\{10^d\}$ is the amplification matrix with encryption accuracy d.

After the remote estimator receives the actual ciphertext signal $\bar{y}_i(k)$, execute the decryption operation to obtain the measurement output $y_i(k)$. By employing the same chaotic system, initial condition, and iteration count, it is possible to obtain the identical chaotic keys $\tilde{s}_i(k)$ as used during encryption. The decryption process can be expressed as follows:

$$\hat{y}_i(k) = \Pi_i(-d)((\Pi_i(d)\bar{y}_i(k)) \oplus (\Pi_i(d+2)\tilde{s}_i(k))) \tag{6}$$

where $\hat{y}_i(k)$ denotes the decrypted plaintext of the measurement output $y_i(k)$.

Remark 1: Chaotic encryption scheme involves employing unpredictability sequences $s(t)$ generated by Logistic (4) as chaotic keys. Small variations in initial conditions $s(0)$ or parameters $E_i(k)$ can generate completely different chaotic sequences $s(t)$, making it nearly impossible for the attacker to obtain the chaotic key $\tilde{s}_i(k)$ when $s(0)$ and $E_i(k)$ are unknown. Chaotic encryption achieves secure communication by performing XOR operations between plaintext and chaotic sequences to generate ciphertext. Owing to the highly unpredictable characteristic of the generated chaotic sequence $\tilde{s}_i(k)$, the quest for effective cracking strategies becomes arduous, thereby enhancing the security of the measurement data $y_i(k)$.

Remark 2: Since XOR operations are performed on binary numbers, it is necessary to convert both the ciphertext and plaintext into binary form before encryption and decryption. Moreover, since decimals cannot be directly converted into binary, it is essential to convert the measurement data $y_i(k)$, $\bar{y}_i(k)$ and chaotic sequence $\tilde{s}_i(k)$ into integers beforehand. By establishing the data precision d of the estimator, the diagonal matrix $\Pi_i(d)$ is constructed to convert plaintext and ciphertext into integer matrices.

C. Multistrategy Injection Attacks

In an insecure network environment, compared to eavesdropping attacks, more commonly occurring are FDI attacks aimed at disrupting system performance. One of the central focuses of this article is to devise estimation strategies that ensure robust estimation performance subject to FDI attacks. Considering the potential for various false signals generated by different FDI attacks in actual scenarios, the MIAs model integrated with multiple attack strategies is designed as

$$\bar{y}_i(k) = \tilde{y}_i(k) + \mu_i(k)\sum_{l=1}^{q}\xi_{i,l}(k)\lambda_l(k) \tag{7}$$

where $\lambda_l(k)$ represents the false signal injected by the attacker. $\mu_i(k)$ and $\xi_{i,l}(k)$ are Bernoulli random variables with the expectation $\bar{\mu}_i$ and $\bar{\xi}_{i,l}$, respectively, which satisfy

$$\sum_{l=1}^{q}\xi_{i,l}(k) = 1, \quad \sum_{l=1}^{q}\bar{\xi}_{i,l} = 1.$$

Considering the occurrence process of MIAs in practical scenarios and the need for MIAs to avoid detection, the fluctuation range of the false signals $\lambda_l(k)(l = 1, 2, \ldots, q)$ is restricted as follows:

$$\lambda_l^{\mathrm{T}}(k)\lambda_l(k) \le \tilde{y}_i^{\mathrm{T}}(k)\vartheta^{\mathrm{T}}\vartheta\tilde{y}_i(k) \tag{8}$$

where ϑ represents the known boundary matrix.

Remark 3: The Bernoulli variable $\mu_i(k)$ has two possible values, 0 and 1, which can intuitively represent the occurrence or nonoccurrence of attacks. The parameter $\bar{\mu}_i$ denotes the probability of attacks occurring in the complex network environment. Utilizing Bernoulli variable allows for flexible modeling and depiction of the likelihood of attacks occurring in various scenarios.

Remark 4: The Bernoulli variable $\xi_{i,l}(k)$ is employed to represent the occurrence of FDI attacks $\lambda_l(k)$. When $\xi_{i,l}(k) = 1$ and all other $\xi_{i,\iota}(k) = 0(\iota = 1, 2, \ldots, q$ and $\iota \neq l)$, it represents the occurrence of the lth type of FDI attacks. Through adjusting the value of $\bar{\xi}_{i,l}$, the occurrence frequency of FDI attacks can be regulated.

Remark 5: Compared with some existing FDI attacks with single attack strategy in [26], [27], [28], the proposed MIAs can model various attack behaviors to more realistically replicate attack scenarios in actual network environments. In practical scenarios, attackers may employ a combination of various attack strategies in a dynamic and coordinated manner to increase the difficulty of system detection. The MIAs model describes this complexity by allowing random combinations of different attack strategies, enhancing the unpredictability of attacks and thereby better reflecting real-world attack scenarios in distributed SNs.

Remark 6: Compared to existing MIAs models in [37] and [38], our approach employs two Bernoulli-distributed random variables $\mu_i(k)$ and $\xi_{i,l}(k)$ to model potential attacks in distributed sensor systems, providing a more flexible and realistic representation of adversarial behavior. Unlike previous MIAs models that use a fixed injection matrix, our method utilizes Bernoulli-distributed random variables $\xi_{i,l}(k)$ to simulate the selective injection of false signals by the attacker into different sensor nodes, making it more consistent with real-world attack scenarios. Moreover, instead of imposing direct constraints on false signals as in existing MIAs models in [37], [38], our approach constrains the range of false signals based on measurement data in (8), leading to a more reasonable and practical security framework.

D. Distributed Estimator Design

In view of the privacy-preserving scheme and MIAs, the following distributed estimator is devised for system (1):

$$\hat{x}_i(k+1) = L_i(k)\hat{x}_i(k) + \sum_{j\in\mathcal{N}_i}a_{ij}K_{ij}(k)\big(\hat{y}_j(k) - C_j(k)\hat{x}_i(k)\big) \tag{9}$$

where $\hat{x}_i(k)$ is the estimation of $x(k)$, $L_i(k)$, and $K_{ij}(k)$ are estimator gain matrix to be designed.

Denote the estimation error as $e_i(k) = x(k) - \hat{x}_i(k)$. Recalling (1) and (9), we obtain

$$\begin{aligned} e_i(k+1) = {} & A(k)x(k) + B(k)\omega(k) - L_i(k)\hat{x}_i(k) \\ & - \sum_{j\in\mathcal{N}_i}a_{ij}K_{ij}(k)\big(C_j(k)e_i(k) + D_j(k)v_j(k) \\ & + \mu_j(k)\Big(\tilde{\lambda}_j(k)\oplus\tilde{s}_j(k)\Big)\big) \end{aligned} \tag{10}$$

where

$$\tilde{\lambda}_j(k) = \sum_{l=1}^{q}\xi_{j,l}(k)\lambda_l(k).$$

To simplify the notations, we define

$$\begin{aligned} e(k) &= \mathrm{col}_N\{e_i(k)\}, \quad \tilde{x}(k) = \mathbf{1}_N\otimes x(k) \\ \tilde{\omega}(k) &= \mathbf{1}_N\otimes\omega(k), \quad \hat{x}(k) = \mathrm{col}_N\{\hat{x}_i(k)\} \\ L(k) &= \mathrm{diag}_N\{L_i(k)\}, \quad K(k) = \big[a_{ij}K_{ij}(k)\big]_{N\times N} \\ C(k) &= \mathrm{diag}_N\{C_i(k)\}, \quad D(k) = \mathrm{diag}_N\{D_i(k)\} \\ v(k) &= \mathrm{col}_N\{v_i(k)\}, \quad \mu(k) = \mathrm{diag}_N\{\mu_i(k)I_{n_x}\} \\ \bar{\lambda}(k) &= \mathrm{col}_N\{\tilde{\lambda}_i(k)\oplus\tilde{s}_i(k)\}. \end{aligned}$$

From (10), we can have

$$\begin{aligned} e(k+1) = {} & (I_N\otimes A(k))\tilde{x}(k) + (I_N\otimes B(k))\tilde{\omega}(k) \\ & - L(k)\hat{x}(k) - K(k)C(k)\mathbf{1}_{Nn_x}\circ e(k) \\ & - K(k)D(k)v(k) - K(k)\mu(k)\bar{\lambda}(k). \end{aligned} \tag{11}$$

Assumption 2: For known matrix $P(0) > 0$, the initial estimation error $e(0)$ satisfies

$$e_i^{\mathrm{T}}(0)P^{-1}(0)e_i(0) \le 1, \quad i = 1, 2, \ldots, N. \tag{12}$$

Definition 1 [14]: The system (1) under the privacy-preserving scheme and MIAs are considered to achieve the DSME, if the estimation error $e_i(k)(i = 1, 2, \ldots, N)$ is confined within certain elliptical region. Specifically, for the error dynamics (10) and positive matrix sequences $P(k)$, there exist sufficient conditions such that $e_i(k)$ satisfies

$$\Psi(k) = e_i^{\mathrm{T}}(k)P^{-1}(k)e_i(k) \leq 1. \tag{13}$$

III. Main Results

In this section, considering privacy-preserving scheme and MIAs, a new distributed estimator of form (9) will be proposed. The adequate prerequisites for fulfilling the designed estimator will be established based on a set of RMIs. Afterward, an algorithm is presented to calculate $L_i(k)$ and $K_{ij}(k)$ in the presence of privacy-preserving scheme and MIAs. We will start by presenting several lemmas that will aid in the subsequent derivation.

Lemma 1 [39]: The quadratic functions $Z_l(\varsigma)(\varsigma \in \mathbb{R}^{n_\varsigma})$ are $Z_l(\varsigma) = \varsigma^{\mathrm{T}} V_l \varsigma$, $(l = 0, 1, \ldots, \tilde{q})$ with $V_l^{\mathrm{T}} = V_l$. Then

$$Z_1(\varsigma) \leq 0, \ldots, Z_{\tilde{q}}(\varsigma) \leq 0 \longrightarrow Z_0(\varsigma) \leq 0 \tag{14}$$

holds if there exist $\beta_1 > 0, \ldots, \beta_{\tilde{q}} > 0$ such that

$$V_0 - \sum_{l=1}^{\tilde{q}} \beta_l V_l \leq 0. \tag{15}$$

Theorem 1: Let positive-definite matrix $P(k)$ be given, considering the privacy-preserving scheme and MIAs, for system (1) and the estimator (9), the estimation error constraint condition (13) is achieved if there exist matrices $L_i(k)$, $K_{ij}(k)$, positive scalars $\sigma_{1,i}(k)$, $\sigma_2(k)$, $\sigma_{3,i}(k)$, and $\sigma_{4,i}(k)$ such that for $j = 1, 2, \ldots, N$

$$\begin{bmatrix} -\Theta(k) & * \\ \Phi_j \Omega(k) & -P(k+1) \end{bmatrix} \leq 0 \tag{16}$$

where

$$\begin{aligned}
\Theta(k) = \mathrm{diag}\Bigg\{ & 1 - \sigma_2(k) - \sum_{i=1}^{N} \big(\sigma_{1,i}(k) + \sigma_{3,i}(k) \\
& + 3\sigma_{4,i}(k)\delta\Lambda_{1,i}(k)\big) \\
& \sum_{i=1}^{N} \big(\sigma_{1,i}(k)\Phi_i - 3\sigma_{4,i}(k)\delta\tilde{\Lambda}_{2,i}(k)\big) \\
& \sigma_2(k)\Delta(k), \quad \sum_{i=1}^{N} \big(\sigma_{3,i}(k)\Gamma_i(k) \\
& - 3\sigma_{4,i}(k)\delta\tilde{\Lambda}_{3,i}(k)\big), \quad \sum_{i=1}^{N} \sigma_{4,i}(k)\Phi_i \Bigg\} \\
\Lambda_{1,i}(k) = {} & \hat{x}_i^{\mathrm{T}}(k) C_i^{\mathrm{T}}(k) \vartheta^{\mathrm{T}} \vartheta C_i(k) \hat{x}_i(k) + \tilde{s}_i^{\mathrm{T}}(k) \vartheta^{\mathrm{T}} \vartheta \tilde{s}_i(k) \\
\tilde{\Lambda}_{\ell,i}(k) = {} & \mathrm{diag}\{\underbrace{0, \ldots, 0}_{i-1}, \Lambda_{\ell,i}(k), \underbrace{0, \ldots, 0}_{N-i}\}, \ \ell = 2, 3 \\
\Lambda_{2,i}(k) = {} & R^{\mathrm{T}}(k) C_i^{\mathrm{T}}(k) \vartheta^{\mathrm{T}} \vartheta C_i(k) R(k) \\
\Lambda_{3,i}(k) = {} & D_i^{\mathrm{T}}(k) \vartheta^{\mathrm{T}} \vartheta D_i(k), \quad \Delta(k) = \mathrm{diag}_N\{W^{-1}(k)\} \\
\Gamma_i(k) = {} & \mathrm{diag}\{\underbrace{0, \ldots, 0}_{i-1}, V_i^{-1}(k), \underbrace{0, \ldots, 0}_{N-i}\}
\end{aligned}$$

$$\begin{aligned}
\Phi_j = {} & \mathrm{diag}\{\underbrace{0, \ldots, 0}_{j-1}, I, \underbrace{0, \ldots, 0}_{N-j}\}, \quad \bar{\mu} = \mathrm{diag}_N\{\bar{\mu}_i I_{n_x}\} \\
\Omega(k) = {} & \begin{bmatrix} \Omega_1(k) & \Omega_2(k) & \Omega_3(k) & K(k)D(k) & K(k)\bar{\mu} \end{bmatrix} \\
\Omega_1(k) = {} & \big(I_N \otimes A(k) - L(k)\big)\hat{x}(k) \\
\Omega_2(k) = {} & I_N \otimes (A(k)R(k)) - \mathrm{diag}\big\{K(k)C(k) \\
& \times (\mathbf{1}_N \otimes R(k))\big\} \\
\Omega_3(k) = {} & I_N \otimes B(k).
\end{aligned}$$

Proof: This theorem is demonstrated by employing mathematical induction. First, it is evident from Assumption 2 that $\mathbb{E}\{\Psi(0)\} \leq 1$ holds true. Then, assume that $\mathbb{E}\{\Psi(k)\} \leq 1$ is true, it is required to demonstrate the validity of $\mathbb{E}\{\Psi(k+1)\} \leq 1$.

Applying Cholesky Decomposition to $P(k)$, we can have $P(k) = R(k)R^{\mathrm{T}}(k)$, where $R(k) > 0$ is a lower triangular matrix. Referring to [40], there exists $\zeta_i(k)$ satisfying $\|\zeta_i(k)\| \leq 1$ such that

$$e_i(k) = R(k)\zeta_i(k). \tag{17}$$

Furthermore, (17) is equivalent to

$$x(k) = \hat{x}_i(k) + R(k)\zeta_i(k). \tag{18}$$

Define $\zeta(k) = \mathrm{col}_N\{\zeta_i(k)\}$, it follows from (18) that

$$\tilde{x}(k) = \hat{x}(k) + (I_N \otimes R(k))\zeta(k). \tag{19}$$

Substituting (19) into (11) yields

$$\begin{aligned}
e(k+1) = {} & \big(I_N \otimes A(k) - L(k)\big)\hat{x}(k) + (I_N \otimes B(k))\tilde{\omega}(k) \\
& + (I_N \otimes A(k))(I_N \otimes R(k))\zeta(k) \\
& - K(k)C(k)\mathbf{1}_{Nn_x} \circ \big((I_N \otimes R(k))\zeta(k)\big) \\
& - K(k)D(k)v(k) - K(k)\mu(k)\bar{\lambda}(k) \\
= {} & \big(I_N \otimes A(k) - L(k)\big)\hat{x}(k) + (I_N \otimes B(k))\tilde{\omega}(k) \\
& + \big(I_N \otimes (A(k)R(k))\big)\zeta(k) \\
& - K(k)C(k)(\mathbf{1}_N \otimes R(k)) \circ \zeta(k) \\
& - K(k)D(k)v(k) - K(k)\mu(k)\bar{\lambda}(k) \\
= {} & \big(I_N \otimes A(k) - L(k)\big)\hat{x}(k) + (I_N \otimes B(k))\tilde{\omega}(k) \\
& + \big(I_N \otimes (A(k)R(k)) - \mathrm{diag}\big\{K(k)C(k) \\
& \times (\mathbf{1}_N \otimes R(k))\big\}\big)\zeta(k) - K(k)D(k)v(k) \\
& - K(k)\mu(k)\bar{\lambda}(k).
\end{aligned} \tag{20}$$

By denoting

$$\eta(k) = \begin{bmatrix} \mathbf{1}_{n_x}^{\mathrm{T}} & \zeta^{\mathrm{T}}(k) & \tilde{\omega}^{\mathrm{T}}(k) & v^{\mathrm{T}}(k) & \bar{\lambda}^{\mathrm{T}}(k) \end{bmatrix}^{\mathrm{T}}.$$

Equation (20) can be rewritten as

$$\mathbb{E}\big\{e(k+1)\big\} = \Omega(k)\eta(k). \tag{21}$$

Based on (13) and (21), one has

$$\mathbb{E}\big\{\Psi(k+1)\big\} = \eta^{\mathrm{T}}(k)\Omega^{\mathrm{T}}(k)\Phi_j^{\mathrm{T}} P^{-1}(k+1)\Phi_j\Omega(k)\eta(k). \tag{22}$$

Therefore, $\mathbb{E}\{\Psi(k+1)\} \leq 1$ is equivalent to

$$\eta^{\mathrm{T}}(k)\Upsilon(k)\eta(k) \leq 0 \tag{23}$$

where $\Upsilon(k) = \Omega^{\mathrm{T}}(k)\Phi_j^{\mathrm{T}} P^{-1}(k+1)\Phi_j\Omega(k) - \mathcal{E}$ and $\mathcal{E} = \mathrm{diag}\{1, 0, 0, 0, 0\}$.

From $\|\zeta_i(k)\| \leq 1$, it can be deduced that

$$\eta^{\mathrm{T}}(k)\Xi_{1,i}(k)\eta(k) \leq 0 \tag{24}$$

where $\Xi_{1,i}(k) = \mathrm{diag}\{-1, \Phi_i, 0, 0, 0\}$.

Noting Assumption 1, we have

$$\eta^{\mathrm{T}}(k)\Xi_2(k)\eta(k) \leq 0 \tag{25}$$

and

$$\eta^{\mathrm{T}}(k)\Xi_{3,i}(k)\eta(k) \leq 0 \tag{26}$$

where $\Xi_2(k) = \mathrm{diag}\{-1, 0, \Delta(k), 0, 0\}$ and $\Xi_{3,i}(k) = \mathrm{diag}\{-1, 0, 0, \Gamma_i(k), 0\}$.

According to (1), (5), and (8), one has

$$\begin{aligned}\mathbb{E}\Big\{&\big(\tilde{\lambda}_i(k) \oplus \tilde{s}_i(k)\big)^{\mathrm{T}}\big(\tilde{\lambda}_i(k) \oplus \tilde{s}_i(k)\big)\Big\}\\ &\leq \delta y_i^{\mathrm{T}}(k)\vartheta^{\mathrm{T}}\vartheta y_i(k) + \delta\tilde{s}_i^{\mathrm{T}}(k)\vartheta^{\mathrm{T}}\vartheta\tilde{s}_i(k)\\ &\leq 3\delta\Lambda_{1,i}(k) + 3\delta\zeta_i^{\mathrm{T}}(k)\Lambda_{2,i}(k)\zeta_i(k)\\ &\quad + 3\delta v_i^{\mathrm{T}}(k)\Lambda_{3,i}(k)v_i(k)\end{aligned} \tag{27}$$

where δ is the scaling factor induced by XOR operations.

Then, it follows from (27) that:

$$\eta^{\mathrm{T}}(k)\Xi_{4,i}(k)\eta(k) \leq 0 \tag{28}$$

where

$$\Xi_{4,i}(k) = \mathrm{diag}\Big\{-3\delta\Lambda_{1,i}(k), -3\delta\tilde{\Lambda}_{2,i}(k), 0, -3\delta\tilde{\Lambda}_{3,i}(k), \Phi_i\Big\}.$$

In light of the aforementioned discussion and Lemma 1, in order to facilitate the proof, we construct the following matrix inequality:

$$\begin{aligned}\Upsilon(k) &- \sum_{i=1}^{N}\sigma_{1,i}(k)\Xi_{1,i}(k) - \sigma_2(k)\Xi_2(k)\\ &- \sum_{i=1}^{N}\sigma_{3,i}(k)\Xi_{3,i}(k) - \sum_{i=1}^{N}\sigma_{4,i}(k)\Xi_{4,i}(k) \leq 0.\end{aligned} \tag{29}$$

For the convenience of subsequent calculations, (29) is transformed into the following equivalent inequality:

$$\Omega^{\mathrm{T}}(k)\Phi_j^{\mathrm{T}}P^{-1}(k+1)\Phi_j\Omega(k) - \Theta(k) \leq 0. \tag{30}$$

By employing Schur Complement, we can obtain that (30) is ensured by (16). In view of (24), (25), (26), (28), and (30), it follows from Lemma 1 that $\Upsilon(k) \leq 0$. Therefore, from (23), one can get $\mathbb{E}\{\Psi(k+1)\} \leq 1$. The proof is now completed.

Remark 6: Each bit of a binary number can only be 0 or 1. The result of XOR operations may be a binary number with all bits equal to 1. This means that the result of XOR operations on two binary numbers may be larger than either of the operands. Since the number of bits in both operands is finite, the size of the operation result is also limited. In other words, the operation result is a limited multiple of the operands. Therefore, a scaling factor δ is established to represent the upper bound of the operation result. The scaling factor can be obtained by deriving the theoretical maximum value through the calculation principles of XOR operations. Alternatively, an exact value of δ can be obtained by collecting data from actual problems.

Algorithm 1: Calculation of Gains $L_i(k)$ and $K_{ij}(k)$

Input: System parameter matrices $A(k)$, $B(k)$, $C_i(k)$ and $D_i(k)$; boundary matrices $W(k)$ and $V_i(k)$; chaotic encryption parameters ϑ, $\tilde{s}_i(k)$ and δ; attack parameter $\bar{\mu}_i$;
Output: $L_i(k)$, $K_{ij}(k)$;
for $k = 1$ *to* T **do**
  Initialize symbolic variables $P(k)$, $\sigma_{1,i}(k)$, $\sigma_2(k)$, $\sigma_{3,i}(k)$ and $\sigma_{4,i}(k)$;
  Obtain $R(k)$ by applying Cholesky Decomposition to $P(k)$;
  Calculating matrices $\Theta(k)$ and $\Omega(k)$;
  solve $L_i(k)$ and $K_{ij}(k)$ with LMI (16) by the LMI toolbox in MATLAB;
end

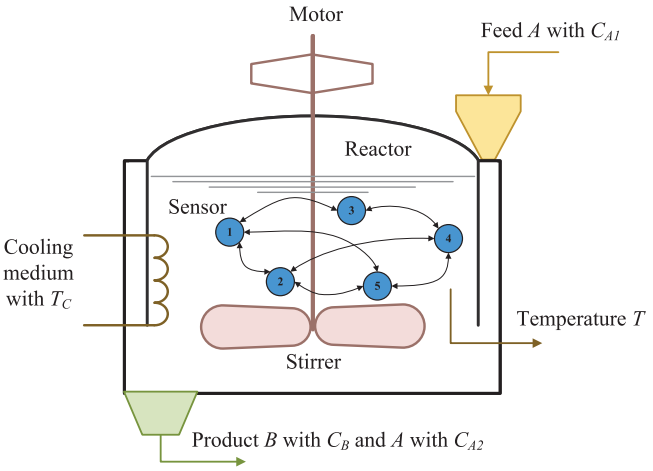

Fig. 2. Physical structure of the CSTR.

Theorem 2: Consider the system (1) with MIAs, the privacy-preserving scheme, and the estimator (9). A sequence of minimized $\{P(k)\}_{k\geq 0}$ is provided by solving the following optimization problem:

$$\min_{P(k+1),L_i(k),K_{ij}(k),\sigma_{1,i}(k),\sigma_2(k),\sigma_{3,i}(k),\sigma_{4,i}(k)} \mathrm{tr}\{P(k+1)\} \tag{31}$$

subject to the constraint condition (16), then $L_i(k)$, $K_{ij}(k)$, positive scalars $\sigma_{1,i}(k)$, $\sigma_2(k)$, $\sigma_{3,i}(k)$, and $\sigma_{4,i}(k)$ can be derived. Accordingly, the optimal estimator gains in (9) can be obtained.

Based on the optimization problem (31) proposed in Theorem 2, the following Algorithm 1 are summarized for calculating the estimator gain matrices $L_i(k)$ and $K_{ij}(k)$ in the DSME scheme.

IV. Illustrative Example

In this section, we implement the proposed DSME method on an industrial nonisothermal continuous stirred tank reactor (CSTR), validating its effectiveness through simulation results. The CSTR is a chemical reactor where reactants are stirred nonisothermally in the tank, and the reaction process occurs discretely, not continuously. The control system of CSTR

typically includes temperature sensors, stirrers, heating or cooling devices, as well as systems for adding reactants and collecting products. Fig. 2 depicts the schematic diagram of the CSTR physical structure. The inflow substance of the CSTR is a chemical substance A with concentration C_{A1}. The effluent is a mixture of reactant A with concentration C_{A2} and desired product B with concentration C_B. T and T_C represent the temperature inside the reactor and the temperature of the cooling medium, respectively.

Due to constraints arising from operating conditions, reactant properties, and potential interference with the reaction process, direct measurement of concentrations within CSTR is difficult in the majority of cases. The common solution involves applying signal processing techniques based on available measurement data of CSTR to estimate concentrations. In [14] and [41], an exploration is undertaken regarding the state estimation and H_∞ filtering associated with CSTR model.

The state matrix of the discretized and linearized state-space model of the CSTR draws inspiration from [14] and [41], and given by

$$\begin{bmatrix} x^{(1)}(k+1) \\ x^{(2)}(k+1) \end{bmatrix} = \begin{bmatrix} 0.9719 & -0.0013 \\ -0.0340 & 0.8628 \end{bmatrix} \begin{bmatrix} x^{(1)}(k) \\ x^{(2)}(k) \end{bmatrix} \tag{32}$$

where $x^{(1)}(k)$ and $x^{(2)}(k)$ are the output concentration and the reactor temperature, respectively.

In practical scenarios, fluctuations in the internal temperature of the reactor or fouling of the cooling medium may potentially impact the CSTR system to a certain extent. Thus, we consider the parameter matrix sequences of the CSTR to be time-varying and can be represented in the following form:

$$A(k) = \begin{bmatrix} 0.9719 & -0.0013 \\ -0.0340 & 0.8628 + 0.2\sin(k) \end{bmatrix}$$
$$B(k) = \begin{bmatrix} 0.1 + 0.1\sin(k) \\ 0.3 \end{bmatrix}.$$

The time-varying parameters of the measurement model for the CSTR system is given by

$$C_i(k) = \begin{bmatrix} 0 & 1 + 0.2\sin(k) + 0.05i \end{bmatrix}$$
$$D_i(k) = 0.1 + 0.1\sin(i+k), \quad i = 1, 2, \ldots, 5.$$

In this example, $N = 5$ sensors are deployed with an interactive topology as illustrated in Fig. 2 to collaboratively estimate the state of the CSTR system. To enhance the security and confidentiality capabilities of the chaotic encryption scheme, time-varying parameters $E_i(k) = 0.21\sin(0.5i + 0.8k) + 3.79$ are employed. The initial values for the chaotic sequences $s(t)$ are set as $\bar{s}_1(0) = 0.32$, $\bar{s}_2(0) = 0.34$, $\bar{s}_3(0) = 0.56$, $\bar{s}_4(0) = 0.71$, and $\bar{s}_5(0) = 0.84$. When the Logistic (4) generates the chaotic sequences, the iteration count is $\tilde{t} = 300$ and the encryption accuracy is $d = 8$. The expectations of MIAs occurrence probability are taken as $\bar{\mu}_i = 0.2$. It is assumed that there are 3 attack strategies, that is $q = 3$. Set the expectations for occurrence probability of each attack strategy to $\bar{\xi}_1 = 0.3$, $\bar{\xi}_2 = 0.3$, and $\bar{\xi}_3 = 0.4$. The generation methods of false signals $\lambda_l(k)$ in each attack strategy are as follows:

$$\lambda_1(k) = \sin(0.1k\pi) + e^{0.5 - \frac{1}{(0.1k)^2}}$$

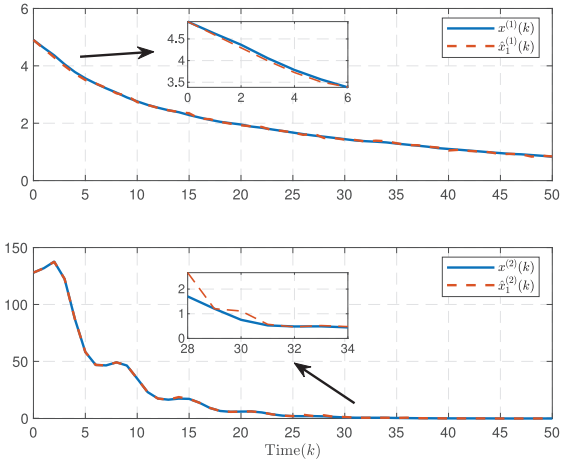

Fig. 3. System state $x(k)$ and the its estimation $\hat{x}_1(k)$.

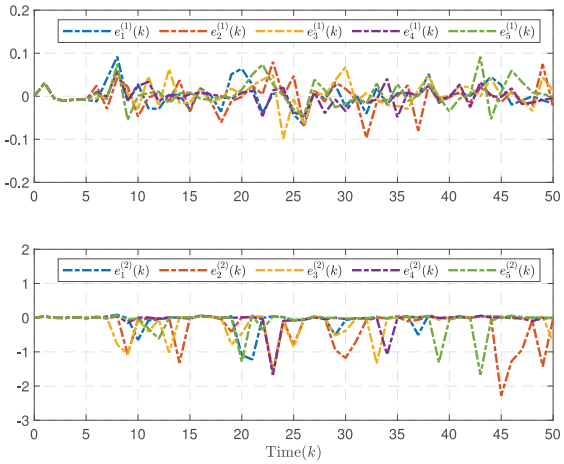

Fig. 4. Estimate errors $e_i(k)$.

$$\lambda_2(k) = 4.5e^{(-0.01k-1)}|\sin(2\pi\tilde{y}_i(k))|$$
$$\lambda_3(k) = 2 + 0.5\sin(k)$$

where $\lambda_1(k)$, $\lambda_2(k)$, and $\lambda_3(k)$ are the false signal generation methods adopted in references [42], [43], and [26], respectively.

The initial concentration of reactant A is set as 4.9 mod/L, and the initial temperature is set as 128 $^{\mathrm{C}}$. The other initial conditions are selected as $\hat{x}_1(0) = [4.8\ 129]^{\mathrm{T}}$, $\hat{x}_2(0) = [5.0\ 131]^{\mathrm{T}}$, $\hat{x}_3(0) = [5.1\ 132]^{\mathrm{T}}$, $\hat{x}_4(0) = [4.8\ 130]^{\mathrm{T}}$, $\hat{x}_5(0) = [5.2\ 127]^{\mathrm{T}}$, and $P(0) = \mathrm{diag}\{40, 40\}$.

The simulation results are demonstrated in Figs. 3–7. The system state $x(k)$ and its estimation $\hat{x}_1(k)$ are displayed in Fig. 3. As shown in Fig. 4, the estimation errors $e_i(k)$ remain consistently within an acceptable range, which demonstrates that the designed estimator can estimate the system state $x(k)$.

In order to examine the impact of privacy-preserving scheme utilizing chaotic encryption on measurement signals $y_i(k)$, Fig. 5 depicts a comparison of measurement signals before and after encryption. The signals before encryption $y_i(k)$ differs significantly from signals after encryption $\tilde{y}_i(k)$, exhibiting no apparent regularity. This indicates that the chaotic encryption

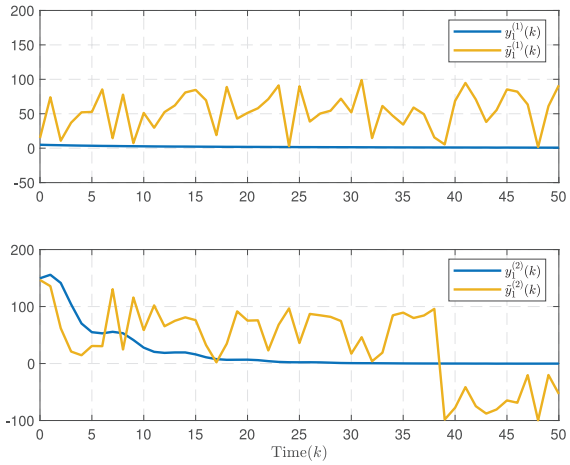

Fig. 5. Comparison of measurement signals before and after encryption.

scheme effectively prevents malicious adversaries from eavesdropping on the measurement.

To evaluate the effectiveness of the chaotic encryption algorithm in randomizing data and enhancing information concealment, information entropy is introduced as a key metric. Proposed by Shannon in information theory, entropy serves as a fundamental measure of uncertainty or randomness in a dataset. It quantifies the average amount of information contained in a data source, where higher entropy values indicate greater uncertainty and lower redundancy. Theoretically, an effective encryption algorithm should maximize information entropy, ensuring that the encrypted data exhibits a highly random distribution, thereby resisting statistical analysis and cryptographic attacks. The calculation of information entropy is based on probability distributions. The Shannon entropy is mathematically defined as

$$H(Z) = -\sum_{\kappa=1}^{\kappa_z} p(z_\kappa)\log_2 p(z_\kappa) \tag{33}$$

where Z is a set of encrypted variables, z_κ represents possible values of Z, $p(z_\kappa)$ is the probability of occurrence of z_κ, κ_z represents the total number of distinct values that Z can take. $H(Z)$ represents the average amount of information contained in a data source under the probability distribution $p(z_\kappa)$.

Table I presents the information entropy of the measurement data $y_i(k)$ before encryption and the encrypted data $\tilde{y}_i(k)$. It can be observed that the entropy values of the encrypted data are significantly higher than those of the original data. This indicates that the encryption process effectively increases data uncertainty and randomness, thereby enhancing security. A higher entropy value suggests that the encrypted data is more uniformly distributed over its possible range, making it more challenging for an adversary to extract meaningful information. Consequently, the results validate the effectiveness of the proposed chaotic encryption algorithm in enhancing data obfuscation and privacy protection.

As depicted in Fig. 6, compared to single strategy attacks, MIAs exhibit more irregular signal fluctuations with significantly greater variations in the amplitude and frequency of the

TABLE I
INFORMATION ENTROPY OF DATA BEFORE AND AFTER ENCRYPTION

	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$
$y_i(k)$	2.4910	2.4896	2.4985	2.4910	2.4821
$\tilde{y}_i(k)$	5.8569	5.8736	5.8569	5.8173	5.8547

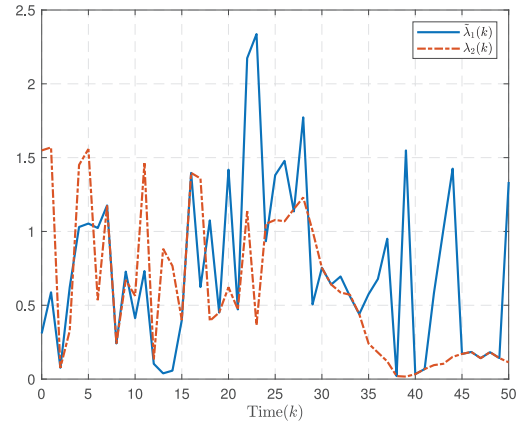

Fig. 6. Comparison between MIAs and single strategy attacks.

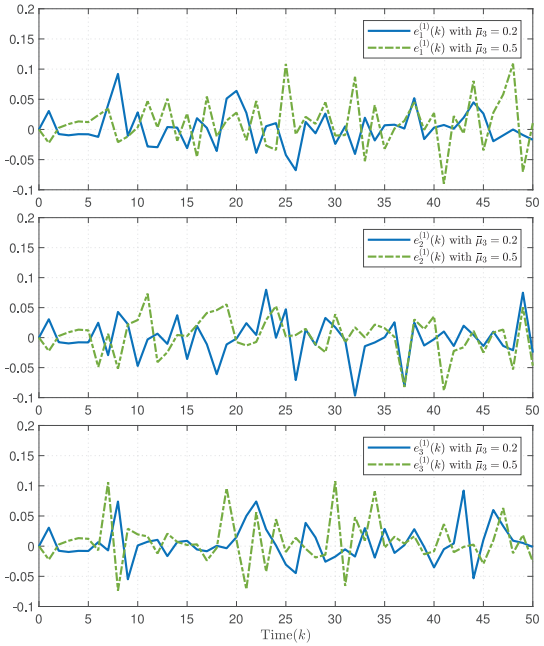

Fig. 7. $e_i(k)$ with different MIAs occurrence probability.

attack signals. This variability arises from the random combination of multiple attack strategies, making it challenging for the system to adapt to and predict the attack patterns, resulting in larger and more unstable estimation errors. The comparison in Fig. 6 demonstrates the advantages of MIAs over single strategy attacks in terms of destructiveness and stealth.

In order to evaluate the influence of MIAs on estimation performance, the expectations of MIAs occurrence probability are taken as $\bar{\mu}_i = 0.2$ and $\bar{\mu}_i = 0.5$, respectively. Fig. 7 displays the estimation error $e_i(k)$ subject to MIAs with different occurrence probability, which illustrates that the

escalation in MIAs probability leads to results in a further increase in $e_i(k)$. Based on the aforementioned simulation results, it is evident that the designed DSME method performs effectively under the privacy-preserving scheme and in the presence of MIAs.

V. Conclusion

This article delves into the problem of distributed state estimation over SNs, considering a privacy-preserving scheme with chaotic encryption and the impact of MIAs. To safeguard against the leakage of system important data, a privacy-preserving scheme incorporating chaotic encryption is employed to counteract potential eavesdroppers lurking within the communication network. The MIAs is proposed to model malicious attacks targeting privacy data, which involves randomly injecting various false signals into encrypted privacy data during transmission. A unified DSME scheme that takes into account privacy-preserving scheme and MIAs is developed, which constrains the estimation errors within a specific elliptical range. To achieve optimal estimation performance, an optimization algorithm for computing the required estimator gain matrix is proposed. In the future, to better accommodate a wider range of application environments, further optimization of encryption algorithms and the integration of differential privacy protection techniques will be explored in resource-constrained scenarios.

References

[1] J. Liu et al., "Frame-dilated convolutional fusion network and GRU-based self-attention dual-channel network for soft-sensor modeling of industrial process quality indexes," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 9, pp. 5989–6002, Sep. 2022.

[2] H. Geng, Z. Wang, L. Ma, Y. Cheng, and Q.-L. Han, "Distributed filter design over sensor networks under try-once-discard protocol: Dealing with sensor-bias-corrupted measurement censoring," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 54, no. 5, pp. 3032–3043, May 2024.

[3] Y. Mo, L. Xing, and J. Jiang, "Modeling and Analyzing linear wireless sensor networks with backbone support," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3912–3924, Oct. 2020.

[4] T. O. Olasupo and C. E. Otero, "The impacts of node orientation on radio propagation models for airborne-deployed sensor networks in large-scale tree vegetation terrains," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 256–269, Jan. 2020.

[5] H. Zheng, W. Guo, and N. Xiong, "A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2315–2327, Dec. 2018.

[6] C.-Y. Chang, Y.-T. Chin, C.-C. Chen, and C.-T. Chang, "Impasse-aware node placement mechanism for wireless sensor networks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 48, no. 8, pp. 1225–1237, Aug. 2018.

[7] W. Chen, Z. Wang, D. Ding, X. Yi, and Q.-L. Han, "Distributed state estimation over wireless sensor networks with energy harvesting sensors," *IEEE Trans. Cybern.*, vol. 53, no. 5, pp. 3311–3324, May 2023.

[8] A. Basit, M. Tufail, and M. Rehan, "Event-triggered distributed state estimation under unknown parameters and sensor saturations over wireless sensor networks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1772–1776, Mar. 2022.

[9] C. Xu, D. He, and H. Du, "Event-triggered distributed moving horizon estimation for smart sensor networks with fading channels and constraints," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–12, Sep. 2023.

[10] C. Gao, Z. Wang, J. Hu, Y. Liu, and X. He, "Consensus-based distributed state estimation over sensor networks with encoding-decoding scheme: Accommodating bandwidth constraints," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4051–4064, Nov./Dec. 2022.

[11] H. Song, H. Yao, P. Shi, D. Zhang, and L. Yu, "Distributed secure state estimation of multi-sensor systems subject to two-channel hybrid attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 1049–1058, 2022.

[12] Y. Xie, S. Ding, F. Yang, L. Wang, and X. Xie, "Probabilistic-constrained distributed set-membership estimation over sensor networks: A dynamic periodic event-triggered approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4444–4457, Nov./Dec. 2022.

[13] Y. Shen, Z. Wang, H. Dong, G. Lu, and F. E. Alsaadi, "Distributed recursive state estimation for a class of multi-rate nonlinear systems over wireless sensor networks under FlexRay protocols," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1551–1563, May/Jun. 2023.

[14] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 1, pp. 171–183, Jan. 2019.

[15] L. Zhou, C. Ge, S. Hu, and C. Su, "Energy-efficient and privacy-preserving data aggregation algorithm for wireless sensor networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3948–3957, May 2020.

[16] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 100–114, 2020.

[17] L. Shi, W. X. Zheng, Q. Liu, Y. Liu, and J. Shao, "Privacy-preserving distributed iterative Localization for wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 70, no. 11, pp. 11628–11638, Nov. 2023.

[18] W. Chen, Z. Wang, H. Dong, J. Mao, and G.-P. Liu, "Privacy-preserving distributed economic dispatch of microgrids over directed networks via state decomposition: A fast consensus algorithm," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 4092–4102, Mar. 2024.

[19] D. Pan, D. Ding, X. Ge, Q.-L. Han, and X.-M. Zhang, "Privacy-preserving platooning control of vehicular cyber–physical systems with saturated inputs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 4, pp. 2083–2097, Apr. 2023.

[20] L. Zou, Z. Wang, B. Shen, H. Dong, and G. Lu, "Encrypted finite-horizon energy-to-peak state estimation for time-varying systems under eavesdropping attacks: Tackling secrecy capacity," *IEEE/CAA J. Automatica Sinica*, vol. 10, no. 4, pp. 985–996, Apr. 2023.

[21] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for Industrial Internet of Things: Opportunities, applications, and challenges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10430–10451, Jul. 2021.

[22] K. Teranishi, T. Sadamoto, and K. Kogiso, "Input–output history feedback controller for encrypted control with leveled fully homomorphic encryption," *IEEE Trans. Control Netw. Syst.*, vol. 11, no. 1, pp. 271–283, Mar. 2024.

[23] A. Hosseingholizadeh, F. Rahmati, M. Ali, H. Damadi, and X. Liu, "Privacy-preserving joint data and function homomorphic encryption for cloud software services," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 728–741, Jan. 2024.

[24] H. Lin et al., "An extremely simple multiwing chaotic system: Dynamics analysis, encryption application, and hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12708–12719, Dec. 2021.

[25] A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma, "Chaotic encryption applied to optical Ethernet in industrial control systems," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 12, pp. 4876–4886, Dec. 2019.

[26] X.-G. Guo, P.-M. Liu, Z.-G. Wu, D. Zhang, and C. K. Ahn, "Hybrid event-triggered group consensus control for heterogeneous Multiagent systems with TVNUD faults and stochastic FDI attacks," *IEEE Trans. Autom. Control*, vol. 68, no. 12, pp. 8013–8020, Dec. 2023.

[27] X. Li, C. K. Ahn, W. Zhang, and P. Shi, "Asynchronous event-triggered-based control for stochastic networked Markovian jump systems with FDI attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 9, pp. 5955–5967, Sep. 2023.

[28] Y. Yang, X. Wang, Y. Li, S. Gorbachev, and D. Yue, "Adaptive resilient tracking control with dual-terminal dynamic-triggering for a linear multi-agent system against false data injection attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 9, pp. 1–12, 2023.

[29] S. Hu, X. Ge, Y. Li, X. Chen, X. Xie, and D. Yue, "Resilient load frequency control of multi-area power systems under DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 936–947, 2023.

[30] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, and J. Cao, "Outlier-resistant distributed filtering over sensor networks under dynamic event-triggered schemes and DoS attacks," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 1152–1162, 2025.

[31] Y. Yu, W. Yang, W. Ding, and J. Zhou, "Reinforcement learning solution for cyber-physical systems security against replay attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2583–2595, 2023.

[32] L. Zha, J. Miao, J. Liu, X. Xie, and E. Tian, "State estimation for delayed Memristive neural networks with multichannel round-robin protocol and multimodal injection attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 54, no. 6, pp. 3738–3748, Jun. 2024.
[33] W. Xu, Z. Wang, L. Hu, and J. Kurths, "State estimation under joint false data injection attacks: Dealing with constraints and insecurity," *IEEE Trans. Autom. Control*, vol. 67, no. 12, pp. 6745–6753, Dec. 2022.
[34] Z.-H. Pang, L.-Z. Fan, Z. Dong, Q.-L. Han, and G.-P. Liu, "False data injection attacks against partial sensor measurements of networked control systems," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 69, no. 1, pp. 149–153, Jan. 2022.
[35] G. Chen, Y. Zhang, S. Gu, and W. Hu, "Resilient state estimation and control of cyber-physical systems against false data injection attacks on both actuator and sensors," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 500–510, Mar. 2022.
[36] L. Min, P. Fei, Q. Shuisheng, and C. Yanfeng, "Implementation of a new chaotic encryption system and synchronization," *J. Syst. Eng. Electron.*, vol. 17, no. 1, pp. 43–47, 2006.
[37] Y. Yang, Y. Niu, and J. Lam, "Security interval type-2 fuzzy sliding mode control under multistrategy injection attack: Design, analysis, and optimization," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 9, pp. 2943–2955, Sep. 2023.
[38] H. Zhao, J. Ma, and Q. Xu, "Security sliding mode control of Lur'e switched systems subject to multi-strategy injection attack," *J. Franklin Inst.*, vol. 361, no. 17, 2024, Art. no. 107187.
[39] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA, USA: SIAM Studies Appl. Math., 1994.
[40] L. El Ghaoui and G. Calafiore, "Robust filtering for discrete-time systems with bounded noise and parametric uncertainty," *IEEE Trans. Autom. Control*, vol. 46, no. 7, pp. 1084–1089, Jul. 2001.
[41] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1148–1159, Apr. 2019.
[42] B. Chen, Y. Tan, Z. Sun, and L. Yu, "Attack-resilient control against FDI attacks in Cyber-physical systems," *IEEE/CAA J. Automatica Sinica*, vol. 9, no. 6, pp. 1099–1102, Jun. 2022.
[43] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

Lijuan Zha received the Ph.D. degree in control science and engineering from Donghua University, Shanghai, China, in 2018.

From 2017 to 2024, she was an Associate Professor with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China. From 2018 to 2023, she was a Postdoctoral Research Associate with the School of Mathematics, Southeast University, Nanjing. She is currently an Associate Professor with the College of Science, Nanjing Forestry University, Nanjing. Her current research interests include networked control systems, neural networks, and complex dynamical systems.

Jinzhao Miao received the B.S. degree in computer science and technology from the Nanjing University of Finance and Economics, Nanjing, China, in 2020, where he is currently pursuing the M.S. degree in computer science and technology with the College of Information Engineering.

His research interests include networked control systems, complex networks, and neural networks.

Jinliang Liu (Senior Member, IEEE) received the Ph.D. degree in control theory and control engineering from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011.

He was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from December 2013 to June 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from October 2016 to October 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from November 2017 to January 2018. From June 2011 to May 2023, he was an Associate Professor and then a Professor with the Nanjing University of Finance and Economics, Nanjing. In June 2023, he joined the Nanjing University of Information Science and Technology, Nanjing, where he is currently a Professor with the School of Computer Science. His research interests include networked control systems, complex dynamical networks, and time delay systems.

Engang Tian (Senior Member, IEEE) received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with The Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. He has published more than 100 papers in refereed international journals. His research interests include networked control systems, cyber attack, as well as nonlinear stochastic control and filtering.

Chen Peng (Senior Member, IEEE) received the M.Sc. degree in coal preparation and Ph.D. degree in control theory and control engineering from the China University of Mining Technology, Xuzhou, China, in 1999 and 2002, respectively.

From September 2002 to August 2004, he was a Postdoctoral Research Fellow of Applied Math with Nanjing Normal University, Nanjing, China. From November 2004 to January 2005, he was a Research Associate with The University of Hong Kong, Hong Kong. From July 2006 to August 2007, he was a Visiting Scholar with the Queensland University of Technology, Brisbane, QLD, Australia. From September 2010 to August 2012, he was a Postdoctoral Research Fellow with Central Queensland University, Rockhampton, QLD, Australia. He is currently a Professor with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. His current research interests include networked control systems, multiagent systems, power systems, and interconnected systems.

Dr. Peng was named a Highly Cited Researcher in 2020, 2021, and 2022 by Clarivate Analytics. He is an Associate Editor for a number of international journals, including the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Information Sciences*, and *Transactions of the Institute of Measurement and Control*.