Privacy-Preserving Schemes of Distributed Sensor Networks with Dynamic Code

Peipei Chen[1], Yun Liu[1], and Wen Yang[1]

[1]East China University of Science and Technology

January 4, 2023

Abstract

In this letter, we consider the privacy-preserving strategies of the distributed state estimator over wireless sensor networks. Aiming at an eavesdropper who can intercept the data transmitted on the communication channel, we design a simple preserving scheme to encode the transmitted data by using system dynamics and history estimates. To analyze the privacy-preserving performance, we use the gap between the values deciphered by the eavesdropper and decoded by the sensor as the privacy index to evaluate the degree of robust privacy protection. Finally, we provide some simulations to illustrate the effectiveness of the proposed preserving schemes.

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

SPECIAL ISSUE ARTICLE

Privacy-Preserving Schemes of Distributed Sensor Networks with Dynamic Code†

Peipei Chen | Yun Liu | Wen Yang*

[1]School of Information Science and Engineering, East China University of Science and Technology, Shanghai, China

Correspondence
*Wen Yang, School of Information Science and Engineering, East China University of Science and Technology, Shanghai, 200237, China. Email: weny@ecust.edu.cn

Abstract

In this letter, we consider the privacy-preserving strategies of the distributed state estimator over wireless sensor networks. Aiming at an eavesdropper who can intercept the data transmitted on the communication channel, we design a simple preserving scheme to encode the transmitted data by using system dynamics and history estimates. To analyze the privacy-preserving performance, we use the gap between the values deciphered by the eavesdropper and decoded by the sensor as the privacy index to evaluate the degree of robust privacy protection. Finally, we provide some simulations to illustrate the effectiveness of the proposed preserving schemes.

KEYWORDS:
Distributed state estimator; eavesdropping; dynamic encoding; privacy protection

1 Introduction

In recent years, Wireless Sensor Networks (WSNs)[1] are in widespread use in smart cities, intelligent manufacturing, and other key infrastructures. As WSNs are applied to industrial and critical infrastructures, security in the calculation process is one of the significantly important issues[2]. In distributed networks, the data exchanged between sensor nodes usually contains private information, such as location, income, etc. Once the data is eavesdropped, the participants will be subject to other attacks[3]. Considering the needs mentioned above, research related to various privacy-preserving schemes against eavesdropping attacks[4] has been quite active in recent years.

Cryptography and information security theory are two traditional privacy-preserving approaches[5]. Multi-party computation[6] is an important technology of cryptography that solves the problem of two or more users in a mutually distrustful multi-user network. Homomorphic encryption is a further refinement of secure multiparty computation[7,8]. The work[9] proposed a fully homomorphic encryption scheme with encryption depth optimization, which can simplify the re-encryption process and improve the efficiency of the fully homomorphic encryption scheme. Differential privacy[10] is a method of information security theory, which is realized by data distortion. Dwork initially proposed this concept[11], i.e., the attacker cannot distinguish the encryption results of different plaintexts. The work[12] solved the problem of privacy-aware machine learning by using the protection scheme combining differential privacy and ADMM algorithm with disturbance.

The traditional schemes cost much computing resources, which are not conducive to applications in practical industry. Therefore, the development of technologies to design a lightweight scheme that supports important infrastructure from eavesdropping is an issue of considerable urgency. In this letter, we explore the possibility of using model knowledge of physical processes to design secrecy encoding. The sensors communicate via acknowledgment signals (ACKs) on the feedback channel. In the distributed system, it will affect the performance of the estimator when the encoding scheme brings noise to the estimate of the sensor. With the encoding scheme proposed in this letter, the sensor can decode completely without introducing any noise to the estimate, which means the scheme can extremely guarantee the performance of the estimator and achieve robust privacy protection. Different from the existing preserving methods, the proposed encoding scheme does not include complicated calculation processes and can be deployed easily in practical applications.

†This work was supported in part by the National Natural Science Foundation of China under Grant (62122026,61973123), the projects sponsored by the Programme of Introducing Talents of Discipline to Universities (the 111 Project) under Grant B17017, Shuguang Program supported by Shanghai Education Development Foundation and Shanghai Municipal Education Commission, the Fundamental Research Funds for the Central Universities, Special project of military civilian integration development in Shanghai under Grant (2019-jmrh1-kj25).

The main contributions of this letter are as follows:

1. A privacy-preserving scheme of the distributed network is provided, which is based on system dynamics and the past estimates. The condition, in which the scheme guarantees perfect privacy protection, is derived.
2. The estimation offset of the eavesdropper and the sensor is proved to increase with the eavesdropper missing the ACK signal. The suggested scheme is easily implemented when the sensor receives the ACK signal, which is more desirable in engineering applications.

The remainder of this letter is organized as follows. In Section 2, some preliminary knowledge are expounded. In Section 3, a dynamic encoding framework is designed for the eavesdropper monitoring the communication channels, and the performance of privacy-preserving scheme is analyzed. Simulation experiments are conducted in Section 4. Finally, the summary of the letter is given in Section 5.

2 Problem Formulation

2.1 System Model

Consider a linear discrete time-invariant system as:

$$x(k+1) = Ax(k) + w(k), \tag{1}$$

where $x(k) \in \mathbb{R}^m$ is the system state vector at time k, $A \in \mathbb{R}^{m\times m}$ is the system matrix and $w(k) \in \mathbb{R}^m$ is the process noise. Assume that $w(k)$ and the initial state $x(0)$ are independent zero-mean Gaussian random vectors with covariances $Q > 0$ and $\Pi_0 > 0$, respectively.

The wireless sensor network consisting of n sensors is exploited to measure $x(k)$. The measurement equation of the ith sensor is given by:

$$y_i(k) = H_i x(k) + v_i(k), \tag{2}$$

where $y_i(k) \in \mathbb{R}^m$ is the measurement of the ith sensor, $H_i \in \mathbb{R}^{m\times m}$ is the measurement matrix and $v_i(k) \in \mathbb{R}^m$ is the measurement noise. Assume that $v_i(k)$ are mutually uncorrelated white Gaussian noises with covariance matrix $R_i > 0$ and are independent with $x(0)$ and $w(k)$ for $\forall k \geq 0$. The sensor network is modeled as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{D})$ with a set of nodes $\mathcal{V} = \{1, 2, \dots, n\}$ and a set of edges $\mathcal{D} \subset \mathcal{V} \times \mathcal{V}$. The edge $(i, j) \in \mathcal{D}$ represents the communication link. The in-neighbors of the ith sensor are denoted by $N_i = \{j : (i, j) \in \mathcal{D}\}$. Let $d_i = |N_i|$ represents the number of in-neighbors of sensor i. We assume the system is unstable.

Assumption 1. The system (1) is assumed to be unstable, and its spectral radius is $\rho(A) = \max_i |\lambda_i(A)| > 1$.

We consider the following distributed state estimator[13] for sensor i:

$$\hat{x}_i(k+1) = A\hat{x}_i(k) + K_p^i(k)[y_i(k) - H_i\hat{x}_i(k)] - \varepsilon A \sum_{j\in N_i} \Big(\hat{x}_i(k) - \hat{x}_j(k)\Big), \tag{3}$$

where $\hat{x}_i(k)$ is the estimate of sensor i at time step k, ε is the consensus gain in the range of $(0, 1/\Delta)$, $\Delta = \max_i\{d_i\}$. $K_p^i(k)$ is the estimator gain.

The cross-estimation error covariance are given by:

$$\begin{aligned} P_{ij}(k+1) = {} & [A - K_p^i(k)H_i]P_{ij}(k)[A - K_p^i(k)H_i]^T + Q + K_p^i(k)R_{ij}K_p^j(k)^T \\ & + \varepsilon^2 A \sum_{s\in N_i}\sum_{r\in N_j} [P_{ij}(k) + P_{sr}(k) - P_{sj}(k) - P_{ir}(k)]A^T \\ & + \varepsilon[A - K_p^i(k)H_i] \sum_{r\in N_j} [P_{ij}(k) - P_{ir}(k)]A^T \\ & + \varepsilon A \sum_{s\in N_i} [P_{ij}(k) - P_{sj}(k)][A - K_p^i(k)H_i]^T. \end{aligned} \tag{4}$$

By minimizing the estimation error covariance $P_i(k)$, the optimal estimator gain is given by:

$$K_p^{i*}(k) = A\Big\{P_i(k) + \varepsilon \sum_{r\in N_i} [P_{ri}(k) - P_i(k)]\Big\} H_i^T [H_i P_i(k) H_i^T + R_i]^{-1}, \tag{5}$$

where $r \in N_i$, $r = 1, 2, \dots, n$, $i \neq r$.

2.2 Channel Model

Communication between the jth sensor and the ith sensor is unreliable, i.e., packet drop may occur. Communication is simultaneously not secure due to the existence of the eavesdropper. The transmitted model between the jth sensor and the ith sensor is shown in Fig. 1. The output of the jth sensor is denoted by $z_j(k) \in \mathbb{R}^m$. There are two transmitted channels. The first is the authorized channel, denoted by $\theta_{ij}(k)$, which is the input of the ith sensor. The other is the unauthorized channel, denoted as $\theta_{ij}^e(k)$, which is intercepted by the eavesdropper. Assume that $\gamma_{ij}(k)$ and $\gamma_{ij}^e(k)$ are independent of the process noise $w(k)$ and

the measurement noise $v_i(k)$, and independent of each other. In addition, the ith sensor can reliably send the ACK signals back to the jth sensor via the feedback channel. If ACK=1, it represents the sensor i succeeds in receiving, otherwise, it fails. Thus, the jth sensor knows what is the latest received message from the ith sensor for $\forall k > 0$.

A binary variable $\gamma_{ij}(k)$ with Bernoulli distribution is used to indicate whether sensor i successfully receives data from sensor j, i.e., if $\gamma_{ij}(k) = 1$, the reception is successful; otherwise, the reception is a failure. The input of the ith sensor is expressed as:

$$\theta_{ij}(k) = \begin{cases} z_j(k), & \text{if } \gamma_{ij}(k) = 1, \\ \delta, & \text{if } \gamma_{ij}(k) = 0, \end{cases} \tag{6}$$

where δ represents a number close to zero, i.e., no information is transmitted.

We denote the outcome of the eavesdropper's packet interception as $\gamma^e_{ij}(k) \in \{0, 1\}$. When $\gamma^e_{ij}(k) = 1$, then the interception is successful. Otherwise, the interception is a failure. Thus, the input of the eavesdropper is expressed as:

$$\theta^e_{ij}(k) = \begin{cases} z_j(k), & \text{if } \gamma^e_{ij}(k) = 1, \\ \delta_e, & \text{if } \gamma^e_{ij}(k) = 0, \end{cases} \tag{7}$$

where δ_e represents no information input.

2.3 Encoding Process

In this letter, we suppose that the system knows the existence of the eavesdropper. To ensure the data privacy, sensor j encodes and sends a weighted version of the current state estimate $\hat{x}_j(k)$ as $\hat{x}_j(k) - A^{k-t_k}\hat{x}_j(t_k)$, where $\hat{x}_j(t_k)$ is the reference state of the encoded information. Specifically, the state-secrecy code is introduced to encode the jth sensor's current state estimate.

Definition 1 (State-Secrecy Code)**.** Consider the system matrix A satisfying Assumption 1, a state-secrecy code is yielded by the following time-varying linear operation:

$$z_j(k) = \hat{x}_j(k) - A^{k-t_k}\hat{x}_j(t_k), \tag{8}$$

where t_k is the reference time, defined by:

$$t_k = max\{t : 0 \le t < k, \gamma_{ij}(k) = 1\}. \tag{9}$$

The initial value of t_k is $\{-1\}$, and $\hat{x}_j(-1) = 0$.

Remark 1. The encoding scheme mentioned above refers to the encoding structure in Anastasios's paper[14]. Unlike Anastasios's work, the scheme proposed in this paper encodes the interactive information between sensors. We consider the privacy protection of the distributed sensor network, which applies more widely and has higher scalability and flexibility. Design and analysis of preserving schemes for the distributed network are more complicated due to data exchange between sensors. We improve the encoding scheme to satisfy the confidentiality of the distributed system and analyse the influence of interception rate on the performance of estimator. Furthermore, the encoding scheme proposed in this paper will not degrade the accuracy of the estimate at each time step.

3 Main Results

In this paper, we aim to design a lightweight encoding scheme for the distributed sensor network. The scheme promises a robust confidentiality against the eavesdropper. Meanwhile, we try to achieve the best performance of the distributed estimation and degrade the estimate performance of the eavesdropper. We use the error $e_j(k)$ between the value $\tilde{x}_j(k)$ decoded by the sensor and the value $\tilde{x}^e_j(k)$ deciphered by the eavesdropper, called decoding information error, as a measurement of privacy-preserving

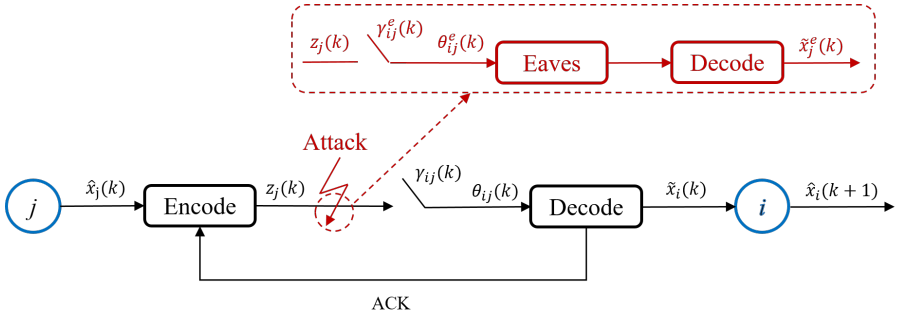

Figure 1 The jth sensor transmits the encoded version $z_j(k)$ of the current state estimate over the channel. Packet drop may occur between sensors, denoted as $\gamma_{ij}(k)$. They might be intercepted by the eavesdropper, denoted as $\gamma^e_{ij}(k)$.The state estimate of sensor i is denoted by $\hat{x}_i(k+1)$. The information deciphered by the eavesdropper is denoted by $\tilde{x}^e_j(k)$. The feedback channel transmits the ACK signal which is the current package reception status of sensor i.

Table 1 Example for State-Secrecy Code.

k	0	1	2	3
$\gamma_{ij}(k)$	1	1	0	1
$\gamma^e_{ij}(k)$	1	1	1	0
t_k	-1	0	1	1
t_{ek}	-1	0	1	2
$z_j(k)$	$\hat{x}_j(0)$	$\hat{x}_j(1) - A\hat{x}_j(0)$	$\hat{x}_j(2) - A\hat{x}_j(1)$	$\hat{x}_j(3) - A^2\hat{x}_j(1)$

performance.

$$e_j(k) = \tilde{x}^e_j(k) - \tilde{x}_j(k), \tag{10}$$

We define $E = \{e_j(k_0), e_j(k_1), \dots, e_j(k_n)\}$. Then, we have the following definition of privacy protection.

Definition 2 (Perfect Privacy Protection)**.** Consider the system (1) and (2), the distributed state estimator (3) and channel models (6) and (7), an encoding scheme achieves perfect privacy protection if and only if the following conditions hold when $\gamma_{ij}(k) = 1$.

1. The performance of the distributed state estimator is same as the case without the privacy-preserving scheme.
2. The decoding information error $e_j(k)$ diverges.

Assuming that the eavesdropper is passive and knows the model of the estimator and the encoding scheme. All system and noise parameters A, H, Q, R, and Π_0 are available to the sensors and the eavesdropper. Note that the sensors are utterly ignorant of the interception rate of the eavesdropper $\gamma^e_{ij}(k)$.

We first define the eavesdropper's reference time t_{ek} to be the time of the most recent successful interception by the eavesdropper before k as:

$$t_{ek} = max\{t : 0 \le t < k, \gamma^e_{ij}(k) = 1\}, \tag{11}$$

where the initial value of t_{ek} is $\{-1\}$.

The eavesdropper cannot obtain the ACK signals, but it knows the encoding scheme, i.e., the eavesdropper knows the form of $z_j(k)$ but not t_k. In order to decipher packets, the eavesdropper obtains t_{ek} according to $\gamma^e_{ij}(k)$. When the eavesdropper intercepts packet $z_j(k)$, it recovers $\hat{x}_j(k)$ by adding $A^{k-t_{ek}}\hat{x}_j(t_{ek})$ and then updates t_{ek} to k. We observe that the eavesdropper cannot decipher $\hat{x}_j(k)$ when $t_k \neq t_{ek}$. Thus, as long as $\gamma_{ij}(k)$ and $\gamma^e_{ij}(k)$ are not exactly same, the eavesdropper's estimation error will turn larger. After receiving a new packet $\hat{x}_j(k) - A^{k-t_k}\hat{x}_j(t_k)$, the ith sensor can recover $\hat{x}_j(k)$ by adding $A^{k-t_k}\hat{x}_j(t_k)$. It confirms the reference time and the reference state through the ACK signals. Then the ith sensor notifies the ith sensor to update t_k to k, and update $\hat{x}_j(k)$ as the reference state for the next transmission. It means that no information is missed at the side of the sensor.

The information decoded by the ith sensor is given by:

$$\tilde{x}_j(k) = \theta_{ij}(k) + A^{k-t_k}\tilde{x}_j(t_k). \tag{12}$$

The information deciphered by the eavesdropper is given by:

$$\tilde{x}^e_j(k) = \theta^e_{ij}(k) + A^{k-t_{ek}}\tilde{x}^e_j(t_{ek}). \tag{13}$$

Example 1 Suppose that for $k = 0, 1, 2, 3$, in the first three rows of Table 1 show the channel outcomes. The last five rows show the reference times of sensors and the eavesdropper, the output of sensor j, and the information decoded by sensor i and deciphered by the eavesdropper, respectively. Notice that the reference time t_{ek} of the eavesdropper and t_k of the sensor are inconsistent at time $k = 3$. Thus, the eavesdropper cannot recover $\hat{x}_j(k)$ after time $k = 3$. Then, the decoding information error $e_j(k)$ will gradually divergent.

Assuming that $\gamma_{ij}(k) \neq \gamma^e_{ij}(k)$ occurs at time k_0 and $\gamma_{ij}(k)$ is always equal to $\gamma^e_{ij}(k)$ for $k > k_0$, which is the worst case for the estimator but the best case for the eavesdropper. The following lemma will certify the above intuitive statements.

Lemma 1 (Worst Case Analysis)**.** Consider the system (1) with measurement equation (2), the distributed state estimator (3), channel model (6) and (7), and the encoding scheme (8). If the following two events both occur for some $k_0 > 0$,

$$\mathcal{X} = \{\gamma_{ij}(k) \neq \gamma^e_{ij}(k), \text{ for some } k_0 \ge 0\}, \tag{14}$$

$$\mathcal{Y} = \{\gamma_{ij}(k) = \gamma^e_{ij}(k), \text{ for all } k \ge k_0 + 1\}. \tag{15}$$

Then for $k \ge k_0$ in $\mathcal{X} \cap \mathcal{Y}$, we have:

$$e_j(k) = \begin{cases} A^{k-t_k}e_j(t_k), & \text{if } \gamma_{ij}(k) = 1, \\ 0, & \text{if } \gamma_{ij}(k) = 0. \end{cases} \tag{16}$$

Proof. Suppose event $\mathcal{X}$ occurs at time k_0, the interception rate of the eavesdropper equals the reception rate of sensor i for $k > k_0$. We have $\gamma_{ij}(k) = \gamma^e_{ij}(k)$ for $k > k_0$. Define the event:

$$\mathcal{W} = \{\gamma_{ij}(k) = \gamma^e_{ij}(k) = 1\}.$$

Case I:For $k > k_0$, $\gamma_{ij}(k) = \gamma^e_{ij}(k) = 1$.
Suppose event $\mathcal{W}$ occurs for the first time at time $k_1 > k_0$, and $t_k = t_{k1}, t_{ek} = t_{ek1}$. The information encoded by sensor j is:

$$z_j(k_1) = \hat{x}_j(k_1) - A^{k_1 - t_{k1}} \hat{x}_j(t_{k1}).$$

The decoding information error is:

$$e_j(k_1) = \tilde{x}^e_j(k_1) - \tilde{x}_j(k_1) = -A^{k_1 - t_{k1}} \hat{x}_j(t_{k1}) + A^{k_1 - t_{ek1}} \hat{x}_j(t_{ek1}).$$

We can deduce similarly the following conclusions by mathematical induction. Suppose the nth occurrence of event $\mathcal{W}$ at time $k_n > k_0$, and $t_k = t_{ek} = k_{n-1}$, where k_{n-1} is the time when event $\mathcal{W}$ last occurred. The decoding information error is:

$$e_j(k_n) = \tilde{x}^e_j(k_n) - \tilde{x}_j(k_n) = A^{k_n - k_{n-1}} e_j(k_{n-1}).$$

Case II: For $k > k_0$, $\gamma_{ij}(k) = \gamma^e_{ij}(k) = 0$.

1. When $\gamma_{ij}(k) = \gamma^e_{ij}(k) = 0, t_k = t_{k0}, t_{ek} = t_{ek0}$, for $k_0 < k < k_1$, $\theta_{ij}(k) = \delta, \theta^e_{ij}(k) = \delta_e$. The decoding information error is:

$$e_j(k) = \tilde{x}^e_j(k) - \tilde{x}_j(k) = A^{k - t_{ek0}} \hat{x}_j(t_{ek0}) - A^{k - t_{k0}} \hat{x}_j(t_{k0}),$$

   which is the initial value of $e_j(k)$.
2. When $t_k = t_{ek}$ for $k > k_1$, the decoding information error is:

$$e_j(k) = \tilde{x}^e_j(k) - \tilde{x}_j(k) = 0.$$

□

By Lemma 1, one can easily deduce Theorem 1.

Theorem 1. Consider the system (1) with measurement equation (2), the distributed state estimator (3) and channel model (6) and (7), if

$$\mathbb{P}\{\gamma_{ij}(k) \neq \gamma^e_{ij}(k), \text{ for some } k \geq 0\} = 1, \tag{17}$$

the encoding scheme (8) achieves perfect privacy protection. And the decoding information error grows unbounded when event $\{\gamma_{ij}(k) \neq \gamma^e_{ij}(k)\}$ occurs at time k_0, i.e., $e_j(k)$ is divergent, where $e_j(k)$ is defined in (10), and we suppose (A, E) is detectable.

Note that the system is unstable, i.e., $\rho(A) > 1$. The necessary and sufficient condition, where matrix A is convergent, is $\rho(A) < 1$. We can easily deduce that the error $e_j(k)$ is divergent. Hence, even in the worst case for the estimator, there is an unbounded error between the information obtained by the eavesdropper and the state estimate of the sensor.

4 Simulations

To illustrate the effectiveness of the proposed privacy-preserving scheme, we present several simulation experiments to verify the privacy-preserving performance.

Consider a wireless sensor network composed of $n = 50$ sensors. The system parameters are as follows:

$$A = \begin{bmatrix} 1.01 & 0 \\ 0 & 1.01 \end{bmatrix}, H_i = \begin{bmatrix} 2 + 2\xi_i & 0 \\ 0 & 2 + 2\xi_i \end{bmatrix}, Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where $\xi_i \in (0, 1], \forall i$, and $\varepsilon = 0.1$. Moreover, $\gamma_{ij}(k)$ is the reception rate of the sensors with $P\{\gamma_{ij}(k) = 1\} = 0.9$ and $P\{\gamma_{ij}(k) = 0\} = 0.1$. The mean-squared error $P_e(k)$ of the eavesdropper is expressed by:

$$P_e(k) = [\tilde{x}^e_j(k) - x(k)][\tilde{x}^e_j(k) - x(k)]^T \tag{18}$$

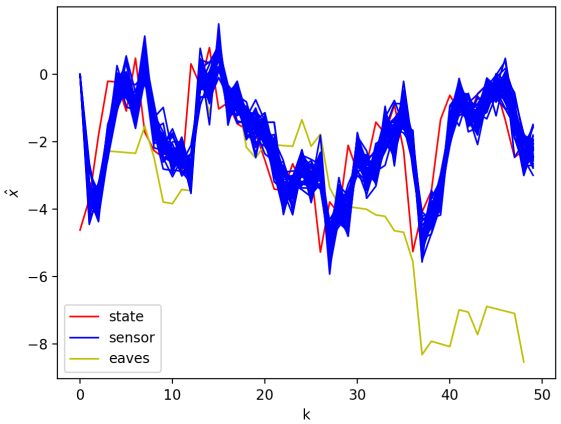

Figure 2 Tracking performance of the distributed estimator with encoding scheme.

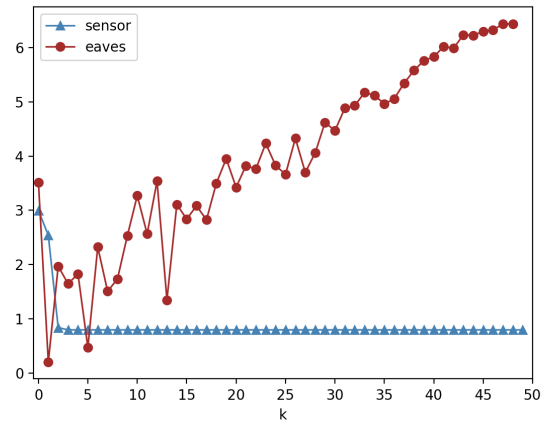

Figure 3 Trace of covariance of the proposed estimator and eavesdropper.

The eavesdropper intercepts on the communication channel and $\gamma_{ij}^{e}(k)$ is the interception rate of the eavesdropper with $P\{\gamma_{ij}^{e}(k) = 1\} = 0.6$ and $P\{\gamma_{ij}^{e}(k) = 0\} = 0.4$. As shown in Fig. 2, the blue curves correspond to 50 sensors, the red curve corresponds to the given target, and the yellow curve corresponds to the eavesdropper who eavesdrops on the communication channel. Although the encoding scheme proposed in this article is adopted, the sensors can track the unstable object state of system (1), and the tracking performance of the eavesdropper is poor. Furthermore, Fig. 3 shows that the estimation error $P_1(k)$ of the 1st sensor converges, and the mean-squared error $P_e(k)$ of the eavesdropper is divergent. This means that the encoding scheme does not affect the performance of the estimator, but it protects the information of the system from being leaked.

5 Conclusion

In this letter, we have developed a privacy-preserving scheme to avoid the eavesdropper deciphering the intercepted estimates, which only used system dynamics with low computation complexity. Then, we have provided the conditions for achieving perfect privacy protection, that is, the estimate of the eavesdropper deviates from the real state as the vital event occurring once. In the case that the eavesdropper intercepts the packet with a certain probability, we have provided an example to illustrate that the vital event can always occur in the first few moments regardless of the probability. It means that the proposed scheme can be easily deployed in practical applications.

References

1. Corti F, Laudani A, Lozito GM, Reatti A, Bartolini A, Ciani L. Model-Based Power Management for Smart Farming Wireless Sensor Networks. *IEEE Transactions on Circuits and Systems I: Regular Papers* 2022: 1-11.

2. Tuo M, Zhou X, Yang G, Fu N. An Approach for Safety Analysis of Cyber-Physical System Based on Model Transformation. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* 2016: 636-639.

3. Chen L, Yue D, Dou C, Chen J, Cheng Z. Study on attack paths of cyber attack in cyber-physical power systems. *IET Generation, Transmission & Distribution* 2020; 14(12): 2352-2360.

4. Han J, Chen L, Schneider S, Treharne H, Wesemeyer S. Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials. *IEEE Transactions on Dependable and Secure Computing* 2021; 18(4): 1836-1849.

5. Ogiela MR, Ogiela L, Ogiela U. Cryptographic Techniques in Advanced Information Management. *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* 2014: 254-257.

6. Mishra DK, Chandwani M. Arithmetic Cryptography Protocol for Secure Multi-party Computation. *Proceedings 2007 IEEE SoutheastCon* 2007: 22-22.

7. Cartlidge J, Smart NP, Talibi Alaoui Y. Multi-party computation mechanism for anonymous equity block trading: A secure implementation of turquoise plato uncross. *Intelligent Systems in Accounting, Finance and Management* 2021; 28(4): 239-267.

8. Chaudhary P, Gupta R, Singh A, Majumder P. Analysis and Comparison of Various Fully Homomorphic Encryption Techniques. *2019 International Conference on Computing, Power and Communication Technologies (GUCON)* 2019: 58-62.

9. Chen L, Ben H, Huang J. An Encryption Depth Optimization Scheme for Fully Homomorphic Encryption. *2014 International Conference on Identification, Information and Knowledge in the Internet of Things* 2014: 137-141.

10. Xue Q, Zhu Y, Wang J. Joint Distribution Estimation and Naïve Bayes Classification Under Local Differential Privacy. *IEEE Transactions on Emerging Topics in Computing* 2021; 9(4): 2053-2063.

11. Dwork C, Roth A. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer ence* 2014; 9(3-4): 211-407.

12. Wang X, Ishii H, Du L, Cheng P, Chen J. Privacy-Preserving Distributed Machine Learning via Local Randomization and ADMM Perturbation. *IEEE Transactions on Signal Processing* 2020; 68: 4226-4241.

13. Yang W, Yang C, Shi H, Shi L, Chen G. Stochastic link activation for distributed filtering under sensor power constraint. *Automatica* 2017; 75: 109-118.

14. Tsiamis A, Gatsis K, Pappas GJ. State-Secrecy Codes for Networked Linear Systems. *IEEE Transactions on Automatic Control* 2020; 65(5): 2001-2015.