This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

Secure Recursive State Estimation of Networked Systems Against Eavesdropping: A Partial-Encryption-Decryption Method

Lei Zou, Zidong Wang, Bo Shen, and Hongli Dong

***Abstract*—This paper addresses the problem of secure recursive state estimation for a networked linear system, which may be vulnerable to interception of transmitted measurement data by eavesdroppers. To effectively protect information security, an encryption-decryption-based communication scheme can be used, but encrypting all the measurement data from sensors can result in significant computational costs. To address this issue, a partial-encryption-decryption (PED) mechanism is proposed to enhance information security with relatively low computational costs. In this mechanism, only part of the transmitted measurement signals are encrypted, and the remaining signals are transmitted directly to the estimator. A Jordan-canonical-form-based approach is developed to select the appropriate parameter for the PED mechanism, and recursive formulas for the state estimator are designed based on the principle of minimum mean squared error. Sufficient conditions are derived to guarantee the ultimate boundedness of the estimation error variance matrix. Finally, the proposed PED-based recursive state estimation scheme is evaluated through two simulation examples to demonstrate its effectiveness.**

***Index Terms*—Recursive state estimation, eavesdropping, encryption-decryption scheme, minimum mean squared error, ultimate boundedness analysis**

Notations

$\rho(\mathcal{P})$	The spectral radius of the matrix $\mathcal{P}$
$\mathcal{B}\backslash\mathcal{A}$	The relative complement of $\mathcal{A}$ with respect to $\mathcal{B}$
$\mathbb{R}^p$	The p-dimensional Euclidean space
$\mathscr{P} \geq \mathscr{Q}$	$\mathscr{P} - \mathscr{Q}$ is positive semi-definite
$\mathscr{P} > \mathscr{Q}$	$\mathscr{P} - \mathscr{Q}$ is positive definite
$\mathscr{M}^T$	The transpose of $\mathscr{M}$
$\mathscr{M}^{-1}$	The inverse matrix of $\mathscr{M}$
$\lambda_{\max}\{\mathscr{A}\}$	The maximum eigenvalue of $\mathscr{A}$
$\lambda_{\min}\{\mathscr{A}\}$	The minimum eigenvalue of $\mathscr{A}$
$\mathrm{Prob}\{s\}$	The occurrence probability of the event "s"
$\mathbb{E}\{x\}$	The expectation of the stochastic variable x
$\mathbb{E}\{x\|y\}$	The expectation of x conditional on y
$\mathrm{rank}(A)$	The rank of a matrix A
I	The identity matrix with compatible dimensions
0	The zero matrix with compatible dimensions
$\mathrm{diag}\{\ldots\}$	The block-diagonal matrix
$\lfloor a \rfloor$	The largest integer less than or equal to a
$\mathrm{mod}(a, b)$	The unique nonnegative remainder on division of a by positive integer b

This work was supported in part by the National Natural Science Foundation of China under Grants 62273087, 61933007, 62273088 and U21A2019, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany. (*Corresponding author: Bo Shen.*)

Lei Zou and Bo Shen are with the College of Information Science and Technology, Donghua University, Shanghai 201620, China, and are also with the Engineering Research Center of Digitalized Textile and Fashion Technology, Ministry of Education, Shanghai 201620, China. (Emails: zouleicup@gmail.com; Bo.Shen@dhu.edu.cn).

Zidong Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom (Email: Zidong.Wang@brunel.ac.uk).

Hongli Dong is with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China, and is also with the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Northeast Petroleum University, Daqing 163318. (Email: shiningdhl@vip.126.com)

I. INTRODUCTION

In recent decades, networked systems have become increasingly prevalent in industrial communities due to the perceived benefits of network-based communication [3], [13], [18], [24], [34]. Unlike conventional point-to-point communication, networked systems transmit data through channel-sharing communication, and this type of communication can have a significant impact on signal transmission behavior, leading to network-induced effects that pose additional challenges to analysis and synthesis of networked systems [9], [37]. State estimation (SE), as a crucial research topic in control and signal processing, is essential for the information perception of dynamic systems. Accordingly, considerable research effort has been dedicated to developing SE techniques for a variety of networked systems over the last few decades, see [11], [15], [25], [35], [38], [41] and their respective references.

Recursive state estimation (RSE) for networked systems has garnered significant research attention due to its wide suitability and outstanding performance in many industrial applications [28], [30], making it one of the mostly investigated issues. Based on the estimation performance requirements, RSE schemes have been divided into three categories, namely, minimum-variance SE [31], [39], set-membership SE [22], [46], and finite-horizon $\mathcal{H}_\infty$ SE [19], [27]. For example, an event-based distributed set-membership SE strategy has been developed in [36] for time-varying nonlinear systems over sensor networks, and a recursive state estimator has been constructed in [29] for networked discrete-time systems with packet dropouts. Recently, extensive research attention has been given to the RSE problem under cyber-attacks, resulting in rapid development in the field [2], [4], [6], [12], [23].

Eavesdropping is one of the most frequently occurring cyber-attacks in practical networked systems. Due to the openness of the communication, potential eavesdroppers can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

hijack the communication links to infer private data, posing serious threats to the information security of networked systems [21], [44]. Therefore, protecting private information from eavesdropping in networked SE problems is of great significance. Representative results regarding the protection of information security in networked SE issues have been reported in the literature, as seen in [7], [45]. From a technical standpoint, privacy-preserving schemes can be divided into two categories: transmission-scheduling-based schemes [14], [17] and encryption-decryption schemes (EDSs) [32], [40]. In the framework of a transmission-scheduling-based scheme, a specific mechanism is dedicatedly designed to schedule signal transmissions to degrade the SE performance for potential eavesdroppers.

In the framework of an EDS, the prescribed secret key is used to transform the raw signal into encrypted data before transmission, thereby making it impossible for potential eavesdroppers to recover the raw signal from the encrypted data and achieve information security during signal transmissions. Compared with the transmission-scheduling-based scheme, the EDS can achieve better information security if the secret key is sufficiently safe. However, encryption algorithms in cryptography can lead to high consumption in computational resources at the signal transmitters [8], [26], [33], which greatly affects the real-time implementation of signal collection. Obviously, such encryption-induced effects can have a significant impact on the corresponding SE issues. Nevertheless, the networked SE problem subject to the encryption-induced effects has not received sufficient attention due to the complicated behaviors caused by the encryption process, and this motivates our current research.

In this paper, we focus our attention on the RSE problem of networked systems against eavesdropping under the effects of EDS. The challenges are outlined as follows:

1) how to preserve the information security by designing the suitable encryption-decryption mechanism with relatively low computational cost?
2) how to design the recursive state estimator under the encryption-induced effects? and
3) how to analyze the ultimate boundedness of the SE error variance?

Regarding the above identified challenges, the main contributions of this article are summarized as follows:

1) a novel partial-encryption-decryption (PED) mechanism is designed to achieve the desired information security while alleviating the computational cost in the signal transmitter,
2) an RSE strategy is developed in the sense of minimum mean squared error (MMSE) subject to the effects induced by the encryption process and packet dropouts, and
3) the ultimate boundedness is analyzed for the resultant SE error variance.

The remainder of this paper is organized as follows. In Section II, the PED-based RSE problem is formulated for networked systems against eavesdropping. In Section III, the desired encryptor parameter is devised to protect the information security. Then, the recursive formulas for the state estimator are proposed according to the principle of MMSE. Moreover, sufficient conditions are established to ensure the ultimate boundedness of the resultant SE error variance. Two simulation examples are provided in Section IV to demonstrate the effectiveness of the proposed PED-based RSE scheme. Finally, the conclusion of our investigation is drawn in Section V.

II. Problem formulation and preliminaries

A. The plant and encryption-decryption mechanism

Consider a networked SE problem where the signal transmissions over the communication channel are overheard by an eavesdropper. The plant under consideration is a linear discrete-time system of the following form:

$$\begin{cases} x_{k+1} = Ax_k + \omega_k \\ y_k = Cx_k + \nu_k \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^n$ and $y_k \in \mathbb{R}^m$ are, respectively, the system state and measurement output at time instant k; $\omega_k \in \mathbb{R}^p$ and $\nu_k \in \mathbb{R}^m$ denote the process noise and measurement noise, respectively; and A and C are real-valued parameter matrices of appropriate dimensions. Without loss of generality, in this paper, it is assumed that $AA^T > 0$.

Remark 1: The assumption that $AA^T > 0$ is quite reasonable for practical engineering. In real-world applications, the plant (1) is always derived by discretizing certain continuous-time linear time-invariant system. Specifically, consider the following continuous-time linear time-invariant system

$$d\vec{x}(t) = \vec{A}\vec{x}(t)dt + d\vec{\omega}(t)$$

where $\vec{x}(t) \in \mathbb{R}^n$ is the state vector, and $\vec{\omega}(t)$ stands for a zero-mean Wiener process (Brownian motion). By discretizing the above system subject to a sampling period $\mathcal{T}$ and letting $x_k \triangleq \vec{x}(k\mathcal{T})$, we can derive a discrete-time linear time-invariant system of the form (1), in which the parameter A is calculated by $A = e^{\vec{A}\mathcal{T}}$. Obviously, such a matrix A is invertible and satisfies $AA^T > 0$.

The initial state x_0, the measurement noise ν_k and the process noise ω_k are mutually uncorrelated Gaussian vectors and have the following statistical properties:

$$\mathbb{E}\{\omega_k\} = 0,\ \mathbb{E}\{\nu_k\} = 0,\ \mathbb{E}\{x_0\} = \bar{x}_0,\ \mathbb{E}\{\omega_k\omega_k^T\} = Q,$$
$$\mathbb{E}\{(x_0 - \bar{x}_0)(x_0 - \bar{x}_0)^T\} = X_0,\ \mathbb{E}\{\nu_k\nu_k^T\} = R$$

where $X_0 > 0$ and $Q > 0$ are known matrices, $R > 0$ is a known diagonal matrix, and $\bar{x}_0 \in \mathbb{R}^n$ is a known vector. Actually, the condition that R is a diagonal matrix is not a restrictive assumption. Consider the case that R is not a diagonal matrix. Obviously, the matrix R can be rewritten as $R = P\bar{R}P^T$ by using the eigen-decomposition technique, where P is an invertible matrix, and $\bar{R}$ is a diagonal matrix composed of the eigenvalues of R. Then, by constructing a new measurement output $\hat{y}_k \triangleq P^{-1}y_k$, it is easy to observe that $\hat{y}_k = P^{-1}y_k = P^{-1}Cx_k + \bar{\nu}_k$ where $\bar{\nu}_k \triangleq P^{-1}\nu_k$. Apparently, the new noise vector $\bar{\nu}_k$ satisfies the condition $\mathbb{E}\{\bar{\nu}_k\bar{\nu}_k^T\} = P^{-1}RP^{-T} = \bar{R}$. Hence, such a reformulated measurement noise vector falls into the case that $\mathbb{E}\{\bar{\nu}_k\bar{\nu}_k^T\}$ is a known diagonal matrix.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

In this paper, the encryption mechanism is utilized to protect the information security of the signal transmission procedure, where the measurement data is first transformed into encrypted data (i.e., ciphertext) before being transmitted. A decryption mechanism is adopted at the state estimator side to recover the measurement data from the received ciphertext. Such encryption-decryption-based communication schemes have been widely utilized in various industrial applications. However, encryption on the measurement data will inevitably result in heavy computational costs, which lead to certain computation and communication overheads. For example, in the well-known RSA encryption mechanism, the ciphertext κ for the plaintext (i.e., the original measurement data) is calculated using the following procedure:

$$\kappa = \psi^{\vartheta} \bmod \chi$$

where ψ is the integer corresponding to the plaintext, ϑ and χ are *very large positive integers*. The integer pair (ϑ, χ) is referred to as the public key for the RSA encryption.

In practice, RSA keys are typically 1024 to 4096 bits long. The huge computational cost of such an encryption mechanism restricts the corresponding usage in many real-time tasks. Note that the computational cost of the encryption process depends largely on the *dimension* of the measurement data. Inspired by [26], in this paper, a PED mechanism is introduced in the signal transmission process to enhance the information security while alleviating the computational cost in the signal transmitter. Different from the traditional encryption-decryption mechanism where the whole measurement data should be processed, the PED mechanism proposed in this paper only needs to encrypt part of the transmitted measurement data and thereby reduces the on-line computational cost in the signal transmitter. Considering the limited computational cost in the signal transmitter, without loss of generality, we assume that only $\bar{m}$ entries in y_k will be encrypted by the encryption mechanism simultaneously. The remained $m - \bar{m}$ entries in y_k will be transmitted directly to the state estimator over the communication network.

The PED mechanism utilized in this paper is implemented according to the following steps:

PED Process:

Step 1. Let the value of $\bar{m}$ (i.e., the number of encrypted entries in y_k) be given. Divide the measurement output y_k into two parts, namely $y_{1,k}$ and $y_{2,k}$. Here, $y_{1,k} \in \mathbb{R}^{\bar{m}}$ denotes the selected measurement data to be encrypted.

Step 2. Transform the selected measurement data $y_{1,k}$ into ciphertext by using the given encryption algorithm (e.g. the widely adopted RSA algorithm). Then, transmit the ciphertext to the state estimator via the communication network.

Step 3. Recover the measurement data from the received ciphertext by using the corresponding decryption algorithm.

Let $\vec{\xi} \triangleq \{\xi_i\}_{i=1,2,\ldots,\bar{m}}$ be the index set of the selected entries in y_k to be encrypted, where $\xi_i \in \{1, 2, \ldots, m\}$ and $\xi_i \neq \xi_j$ for all $i \neq j$. In other words, the selected measurement data $y_{1,k}$ can be described as follows:

$$y_{1,k} \triangleq \begin{bmatrix} y_k^T(\xi_1) & y_k^T(\xi_2) & \ldots & y_k^T(\xi_m) \end{bmatrix}^T$$

where $y_k^T(\xi_i)$ represents the ξ_i-th entry in y_k. Here, the value of the set $\vec{\xi}$ is regarded as the designing parameter for the PED mechanism. For notation simplicity, we let

$$\Phi(\vec{\xi}) \triangleq \begin{bmatrix} \mathbf{e}^T(\xi_1) & \mathbf{e}^T(\xi_2) & \ldots & \mathbf{e}^T(\xi_{\bar{m}}) \end{bmatrix}^T,$$

in which

$$\mathbf{e}(\xi_i) \triangleq \left[\underbrace{0 \;\; 0 \;\; \ldots \;\; 0}_{\xi_i - 1} \;\; 1 \;\; \underbrace{0 \;\; 0 \;\; \ldots \;\; 0}_{m - \xi_i} \right].$$

Obviously, by letting $\hat{\xi} \triangleq \{1, 2, \ldots, m\} \setminus \vec{\xi}$, we have

$$\begin{cases} y_{1,k} = \Phi(\vec{\xi}) y_k \\ y_{2,k} = \Phi(\hat{\xi}) y_k \end{cases}.$$

According to the above discussion, the networked SE process with PED mechanism can be shown by Fig. 1.

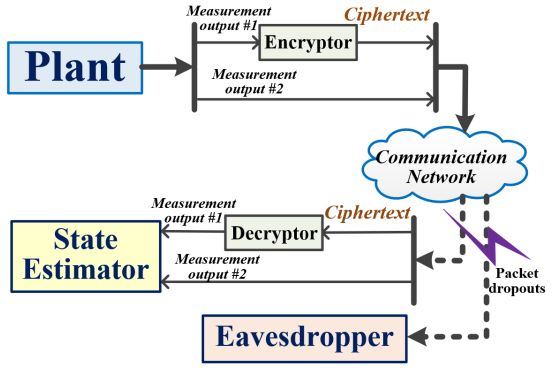

Fig. 1: Networked SE with partially encrypted measurements

We are now in a position to introduce the effects induced by the encryption process and network-based communication. Before introducing the encryption process, let us introduce the following assumption on the encryption mechanism.

Assumption 1: The elapsed time of the encryption process on the data $y_{1,k}$ is d. The encryption on $y_{1,k}$ can be implemented only when the encryption on the previous data is completed. Furthermore, the first encrypted measurement data is $y_{1,0}$.

It is easy to observe from Assumption 1 that: 1) the measurement signal $y_{1,k}$ will only be encrypted at time instants $\{0, d, 2d, 3d, \ldots\}$, 2) the encryption on the measurement signal $y_{1,ld}$ $(\forall l \in \{0, 1, 2, \ldots\})$ will be completed at time instant $(l+1)d$ (due to the elapsed time of the encryption process), and 3) the measurement signals $\{y_{1,k}\}_{ld<k<(l+1)d}$ $(\forall l = 0, 1, \ldots)$ (which are generated during the encryption process) will be "discarded". Without loss of generality, let the generated ciphertext at time instant ld be β_{ld}. Then, the time instants of the encryption process on the measurement signal $y_{1,ld}$ are described in Fig. 2.

As shown in Fig. 2, we can conclude that

$$\beta_{ld} = \mathrm{En}(y_{1,(l-1)d}), \quad l = 1, 2, \ldots$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

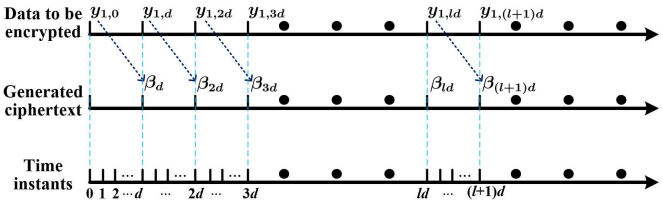

Fig. 2: Time instants of the encryption process

where $\mathrm{En}(\cdot)$ represents the encryption mechanism. Accordingly, the transmitted data at time instant k (which is represented by $\bar{\beta}_k$) is described as follows:

$$\bar{\beta}_k = \begin{cases} y_{2,k}, & \text{if } \mathrm{mod}(k,d) \neq 0 \\ \begin{bmatrix} \beta_k \\ y_{2,k} \end{bmatrix}, & \text{if } \mathrm{mod}(k,d) = 0 \end{cases}$$

In this paper, it is assumed that the signal transmissions over the communication network would suffer from the effects of packet dropouts, which can be described by a sequence of independent and identically distributed (i.i.d.) random variables $\{\gamma_k\}_{k\geq 0}$. More specifically, γ_k equals to 1 if the signal is successfully transmitted at time instant k and zero otherwise. The corresponding occurrence probabilities are $\mathrm{Prob}\{\gamma_k = 1\} = \bar{\gamma}$ and $\mathrm{Prob}\{\gamma_k = 0\} = 1 - \bar{\gamma}$.

Let $\mathrm{De}(\cdot)$ be the decryption mechanism and $\bar{y}_k$ be the received measurement data of the state estimator at time instant k. Under the effects of packet dropouts, we have

$$\begin{aligned} \bar{y}_k &= \begin{cases} \emptyset, & \text{if } \gamma_k = 0 \\ y_{2,k}, & \text{if } \gamma_k = 1 \text{ and } \mathrm{mod}(k,d) \neq 0 \\ \begin{bmatrix} \mathrm{De}(\beta_k) \\ y_{2,k} \end{bmatrix}, & \text{if } \gamma_k = 1 \text{ and } \mathrm{mod}(k,d) = 0 \end{cases} \\ &= \begin{cases} \emptyset, & \text{if } \gamma_k = 0 \\ y_{2,k}, & \text{if } \gamma_k = 1 \text{ and } \mathrm{mod}(k,d) \neq 0 \\ \begin{bmatrix} y_{1,k-d} \\ y_{2,k} \end{bmatrix}, & \text{if } \gamma_k = 1 \text{ and } \mathrm{mod}(k,d) = 0 \end{cases} \end{aligned} \tag{2}$$

where the last step follows from the fact that $\mathrm{De}(\beta_{ld}) = \mathrm{De}(\mathrm{En}(y_{1,(l-1)d})) = y_{1,(l-1)d}$.

Remark 2: Encryption is recognized as one of the most effective ways to protect information security. In the context of cryptography, encryption stands for the process that transforms the representation of the original information into the encrypted message based on the "secret key". By doing so, only authorized parties (i.e., those with knowledge of the secret key) can infer the original information from the encrypted message through decryptors, thereby preserving private information from information leakage. Generally speaking, the strength of the encryption process is described by the length of the secret key. However, a secret key with a long length would result in a high computational cost. In practice, the length of the secret key can be adjusted to attain a tradeoff between information security and computational cost.

B. The information security and recursive state estimator

In this subsection, we shall first discuss the information security of the networked SE issue shown in Fig. 1. Let us start the discussion with a brief review of the *detectability*.

Definition 1: [16] A linear time-invariant system is *detectable* if and only if all the unstable states of the system are observable.

As shown in Fig. 1, an eavesdropper can acquire the transmitted signals from the communication channel and estimate the system states. *In this paper, it is assumed that the eavesdropper is incapable of recovering the measurement data from the cyphertext.* Accordingly, only partial measurement data (i.e., $y_{2,k}$) can be used for SE on the eavesdropper side. Specifically, the ciphertext provides *no information* to the eavesdropper.

According to the above discussions, it is easy to see that the SE issue from the eavesdropper side is considered for the following system:

$$\begin{cases} x_{k+1} = Ax_k + \omega_k \\ y_{2,k} = \Phi(\hat{\xi})Cx_k + \Phi(\hat{\xi})\nu_k \end{cases} \tag{3}$$

The purpose of the eavesdropper is to estimate the system state based on the available measurements $\mathcal{I}_{e,k} \triangleq \{\breve{y}_0, \breve{y}_1, \ldots, \breve{y}_k\}$, where

$$\breve{y}_k = \begin{cases} \emptyset, & \text{if } \gamma_{e,k} = 0 \\ y_{2,k}, & \text{if } \gamma_{e,k} = 1 \end{cases},$$

and $\gamma_{e,k}$ governs the random nature of the packet dropouts for the signal transmissions during the eavesdropping process.

To protect the information security of the networked SE process, in this paper, we would like to select the suitable set $\vec{\xi}$ such that the linear time-invariant system (3) is *undetectable*. By doing so, it is nearly impossible for the eavesdropper to derive an accurate estimate of the system state, even if $\gamma_{e,k} = 1$ holds for all $k \geq 0$ (i.e., all the transmitted signals are successfully received by the eavesdropper).

Next, let us consider the SE issue for the user side. Considering the measurement data received by the estimator, in this paper, the MMSE state estimate $\hat{x}_{k|k}$ at the user side is calculated by the following scheme:

$$\begin{aligned} \hat{x}_{k|k} &= \arg\min_{\hat{x}} \mathbb{E}\{(\hat{x} - x_k)^T(\hat{x} - x_k)|\mathcal{I}_k\}, \\ &= \mathbb{E}\{x_k|\mathcal{I}_k\}, \end{aligned} \tag{4}$$

where $\mathcal{I}_k \triangleq \{\bar{y}_i | i \leq k, \bar{y}_i \neq \emptyset\}$ represents the available measurements set.

We are now ready to present the three main objectives of this paper as follows.

- Design the value of the set $\vec{\xi}$ such that the linear time-invariant system (3) is undetectable.
- Design the recursive formulas to calculate the desired state estimate $\hat{x}_{k|k}$ according to the SE scheme (4).
- Analyze the boundedness of the SE error variance $\mathbb{E}\{(\hat{x}_{k|k} - x_k)(\hat{x}_{k|k} - x_k)^T\}$.

III. Main results

A. Design of the set $\vec{\xi}$

According to the plant (1), we can derive the following Jordan canonical form by using the similarity transformation. Without loss of generality, we assume that the matrix A has

r distinct eigenvalues $\{\lambda_i\}_{i=1,2,\ldots,r}$. Then, there exists an invertible matrix $\mathcal{T} \in \mathbb{R}^{n\times n}$ such that

$$\begin{cases} \chi_{k+1} = J\chi_k + \mathcal{B}\omega_k \\ y_k = G\chi_k + \nu_k \end{cases} \tag{5}$$

where

$$\chi_k \triangleq \mathcal{T}x_k,\ \mathcal{B} \triangleq \mathcal{T},\ J \triangleq \mathcal{T}A\mathcal{T}^{-1} = \mathrm{diag}\{J_1, J_2, \ldots, J_r\},$$
$$G \triangleq C\mathcal{T}^{-1} = \begin{bmatrix} G_1 & G_2 & \ldots & G_r \end{bmatrix},$$
$$G_i \triangleq \begin{bmatrix} G_{i,1} & G_{i,2} & \ldots & G_{i,\alpha_i} \end{bmatrix},\ G_{i,j} \triangleq \begin{bmatrix} g_{i,j}^{(1)} & g_{i,j}^{(2)} & \ldots \end{bmatrix},$$
$$J_i \triangleq \begin{bmatrix} J_{i,1} & & \\ & \ddots & \\ & & J_{i,\alpha_i} \end{bmatrix},\quad J_{i,j} \triangleq \begin{bmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_i \end{bmatrix},$$

and α_i denotes the geometric multiplicity of the eigenvalue λ_i.

Before proceeding further, we introduce the following lemma.

Lemma 1: [47] The linear time-invariant system (5) is observable if and only if

$$\mathrm{rank}\left(\Phi(\hat{\xi}) \begin{bmatrix} g_{i,1}^{(1)} & g_{i,2}^{(1)} & \ldots & g_{i,\alpha_i}^{(1)} \end{bmatrix}\right) = \alpha_i,\ \forall 1 \le i \le r.$$

For notation simplicity, we define

$$\Lambda \triangleq \big\{\lambda | \lambda \in \{\lambda_i\}_{i=1,2,\ldots,r}, \rho(A) \ge 1\big\},$$
$$\mathcal{G}_i \triangleq \begin{bmatrix} g_{i,1}^{(1)} & g_{i,2}^{(1)} & \ldots & g_{i,\alpha_i}^{(1)} \end{bmatrix}.$$

Based on the definition of Λ, we have the following proposition.

Proposition 1: The linear time-invariant system (3) is undetectable if and only if there exists a positive integer $i \in \Lambda$ such that

$$\mathrm{rank}\big(\Phi(\hat{\xi})\mathcal{G}_i\big) < \alpha_i. \tag{6}$$

Proof: The proof follows readily from Definition 1 and Lemma 1, and is therefore omitted here for space saving. ■

Corollary 1: The linear time-invariant system (3) is undetectable if there exist a positive integer $i \in \Lambda$ such that $\mathrm{rank}\big(\Phi(\hat{\xi})\big) < \alpha_i$.

Proof: The proof is straightforward based on Proposition 1, and is thus omitted here for brevity. ■

Remark 3: We have now completed the design of the set $\vec{\xi}$ based on the Jordan canonical form of the plant. As previously mentioned, the encryption process inevitably incurs a certain computational cost, which is largely dependent on the number of elements in the set $\vec{\xi}$ (i.e., the value of $\bar{m}$). To minimize the computational cost of the encryption process, the value of the integer $\bar{m}$ can be determined by solving the constrained optimization problem of minimizing $\bar{m}$ subject to the feasibility of $\mathrm{rank}\big(\Phi(\hat{\xi})\mathcal{G}_i\big) < \alpha_i$ for certain $\hat{\xi}$ and $i \in \Lambda$. Note that for any $\bar{m} \in \{1, 2, \ldots, m\}$, the number of possible combinations $(\hat{\xi}, i)$ is limited. Hence, the above constrained optimization problem can be easily solved by the enumeration method.

B. Design of the MMSE estimator

Before further proceeding, the following lemmas are introduced, which will be used later.

Lemma 2: [1] Let X and Y be random vectors with a jointly Gaussian distribution. Then, the conditional distribution of X given Y is of the expectation

$$\mathbb{E}\{X|Y\} = \mathbb{E}\{X\} + \Sigma_{XY}\Sigma_Y^{-1}(Y - \mathbb{E}\{Y\}) \tag{7}$$

and conditional variance

$$\begin{aligned} &\mathbb{E}\{(X - \mathbb{E}\{X\})(X - \mathbb{E}\{X\})^T|Y\} \\ &= \Sigma_X - \Sigma_{XY}\Sigma_Y^{-1}\Sigma_{YX} \end{aligned} \tag{8}$$

where $\Sigma_X \triangleq \mathbb{E}\{(X - \mathbb{E}\{X\})(X - \mathbb{E}\{X\})^T\}$ and $\Sigma_{XY} \triangleq \mathbb{E}\{(X - \mathbb{E}\{X\})(Y - \mathbb{E}\{Y\})^T\}$.

Lemma 3: [1] Suppose that X, Y_1, Y_2, …, Y_k are jointly distributed with Y_1, Y_2, …, Y_k mutually uncorrelated, i.e., $\Sigma_{Y_iY_j} = 0$ for $i \ne j$. Then, we have

$$\mathbb{E}\{X|Y_1, Y_2, \ldots, Y_k\} = \sum_{i=1}^{k} \mathbb{E}\{X|Y_i\} - (k-1)\mathbb{E}\{X\}. \tag{9}$$

Lemma 4: [1] Let $Z_k \triangleq \{z_k\}_{k\ge 0}$ be a Gaussian random sequence. Define $\tilde{z}_0 \triangleq z_0 - \mathbb{E}\{z_0\}$, $\tilde{z}_k \triangleq z_k - \mathbb{E}\{z_k|Z_{k-1}\}$ and $\tilde{Z}_k \triangleq \{\tilde{z}_k\}_{k\ge 0}$. Then, with w and Z_k jointly distributed, we have

$$\mathbb{E}\{w|Z_k\} = \mathbb{E}\{w|\tilde{Z}_k\} = \sum_{l=0}^{k} \mathbb{E}\{w|\tilde{z}_l\}$$

provided $\mathbb{E}\{w\} = 0$.

We can now proceed with designing the MMSE estimator in a recursive form. Let us first consider the case where $\mathrm{mod}(k, d) \ne 0$. The following theorem proposes the corresponding estimator design.

Theorem 1: For the case that $\mathrm{mod}(k, d) \ne 0$ or $k = 0$, the MMSE state estimate $\hat{x}_{k|k}$ can be calculated according to the following recursions:

$$\begin{cases} \hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1}, \\ \hat{x}_{k|k} = \hat{x}_{k|k-1} + \gamma_k\tilde{\Sigma}_k\Sigma_{\tilde{y}_k}^{-1}\tilde{y}_k \\ \hat{x}_{0|-1} = \bar{x}_0 \end{cases} \tag{10}$$

where

$$e_{k|k-1} \triangleq x_k - \hat{x}_{k|k-1},\quad \Sigma_{e_{k|k-1}} \triangleq \mathbb{E}\{e_{k|k-1}e_{k|k-1}^T|\gamma_0^{k-1}\},$$
$$\hat{x}_{k-i|k-j} \triangleq \mathbb{E}\{x_{k-i}|\mathcal{I}_{k-j}\},\ \gamma_0^k \triangleq \begin{bmatrix} \gamma_0 & \gamma_1 & \ldots & \gamma_k \end{bmatrix}^T,$$
$$\begin{aligned} \Sigma_{\tilde{y}_k} &\triangleq \mathbb{E}\{\tilde{y}_k\tilde{y}_k^T|\gamma_0^k\} \\ &= \Phi(\hat{\xi})C\Sigma_{e_{k|k-1}}C^T\Phi^T(\hat{\xi}) + \Phi(\hat{\xi})R\Phi^T(\hat{\xi}), \end{aligned}$$
$$\tilde{\Sigma}_k \triangleq \mathbb{E}\{(x_k - \mathbb{E}\{x_k\})\tilde{y}_k^T|\gamma_0^k\} = \Sigma_{e_{k|k-1}}C^T\Phi^T(\hat{\xi}),$$
$$\tilde{y}_k \triangleq \gamma_k\big(\bar{y}_k - \mathbb{E}\{\bar{y}_k|\mathcal{I}_{k-1}\}\big) = \gamma_k(\bar{y}_k - \Phi(\hat{\xi})C\hat{x}_{k|k-1}).$$

Furthermore, the values of $\{\Sigma_{e_{k|k-1}}\}_{k\ge 1}$ can be calculated recursively according to the following difference equations:

$$\begin{cases} \Sigma_{e_{k|k-1}} = A\Sigma_{e_{k-1|k-1}}A^T + Q \\ \Sigma_{e_{k|k}} = \Sigma_{e_{k|k-1}} - \gamma_k\tilde{\Sigma}_k\Sigma_{\tilde{y}_k}^{-1}\tilde{\Sigma}_k^T \\ \Sigma_{e_{0|-1}} = X_0 \end{cases} \tag{11}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

in which $e_{k|k} \triangleq x_k - \hat{x}_{k|k}$ and $\Sigma_{e_{k|k}} \triangleq \mathbb{E}\{e_{k|k}e_{k|k}^T|\gamma_0^k\}$.

Proof: First, it is easy to observe from the definition of $\bar{y}_k$ that $\mathcal{I}_k$ is consisted of the available measurements (i.e. $\{y_{1,id}\}_{0\le i<\lfloor k/d\rfloor}$ and $\{y_{2,i}\}_{0\le i\le k}$). Since the initial state x_0, the measurement noise ν_k and the process noise ω_k are mutually uncorrelated Gaussian vectors, it is easy to conclude that $\bar{y}_k$ is a Gaussian vector whose statistical property depends on the value of $\mathrm{mod}(k,d)$, which indicates that $\mathcal{I}_k$ is a sequence of Gaussian vectors.

According to the definition of $\mathcal{I}_k$, it is observed that

$$\mathcal{I}_k = \begin{cases} \mathcal{I}_{k-1}, & \text{if } \gamma_k = 0 \\ \mathcal{I}_{k-1} \cup \{y_{2,k}\}, & \text{if } \gamma_k = 1 \end{cases}.$$

According to the MMSE estimation scheme (4), we have

$$\hat{x}_{k|k} = \mathbb{E}\{x_k|\mathcal{I}_k\} = \begin{cases} \mathbb{E}\{x_k|\mathcal{I}_k\}, & \text{if } \gamma_k = 1 \\ \mathbb{E}\{x_k|\mathcal{I}_{k-1}\}, & \text{if } \gamma_k = 0 \end{cases}. \tag{12}$$

Consider the case that $\gamma_k = 1$ and define $w_k \triangleq x_k - \mathbb{E}\{x_k\}$. It is obvious that $\mathbb{E}\{w_k\} = 0$. Then, it follows from Lemma 4 that

$$\begin{aligned} &\mathbb{E}\{x_k|\mathcal{I}_k\} - \mathbb{E}\{x_k\} = \mathbb{E}\{w_k|\mathcal{I}_k\} = \mathbb{E}\{w_k|\tilde{\mathcal{I}}_k\} \\ =&\mathbb{E}\{x_k|\tilde{\mathcal{I}}_k\} - \mathbb{E}\{x_k\}, \end{aligned}$$

which implies that $\mathbb{E}\{x_k|\mathcal{I}_k\} = \mathbb{E}\{x_k|\tilde{\mathcal{I}}_k\}$. Subsequently, it follows from (12) that

$$\begin{aligned} \hat{x}_{k|k} &= \begin{cases} \mathbb{E}\{x_k|\mathcal{I}_k\}, & \text{if } \gamma_k = 1 \\ \mathbb{E}\{x_k|\mathcal{I}_{k-1}\}, & \text{if } \gamma_k = 0 \end{cases} \\ &= \begin{cases} \mathbb{E}\{x_k|\tilde{\mathcal{I}}_k\}, & \text{if } \gamma_k = 1 \\ \mathbb{E}\{Ax_{k-1} + \omega_{k-1}|\mathcal{I}_{k-1}\}, & \text{if } \gamma_k = 0 \end{cases} \end{aligned} \tag{13}$$

where $\tilde{\mathcal{I}}_k \triangleq \{\tilde{y}_i | i \le k, \gamma_i \ne 0\}$. As shown in [1], it is obvious that the vectors in $\tilde{\mathcal{I}}_k$ are mutually uncorrelated. Then, considering the case that $\gamma_k = 1$, the following equalities can be easily achieved by using Lemma 3:

$$\begin{aligned} &\mathbb{E}\{x_k|\tilde{\mathcal{I}}_k\} = \sum_{i=1}^{k} \mathbb{E}\{x_k|\tilde{y}_i\} - (k-1)\mathbb{E}\{x_k\} \\ =&\sum_{i=1}^{k-1} \mathbb{E}\{x_k|\tilde{y}_i\} - (k-2)\mathbb{E}\{x_k\} + \mathbb{E}\{x_k|\tilde{y}_k\} - \mathbb{E}\{x_k\} \\ =&\mathbb{E}\{x_k|\tilde{\mathcal{I}}_{k-1}\} + \mathbb{E}\{x_k|\tilde{y}_k\} - \mathbb{E}\{x_k\} \\ =&\mathbb{E}\{x_k|\tilde{\mathcal{I}}_{k-1}\} + \mathbb{E}\{x_k|\tilde{y}_k\} - \mathbb{E}\{x_k\} \\ =&\hat{x}_{k|k-1} + \mathbb{E}\{x_k|\tilde{y}_k\} - \mathbb{E}\{x_k\}. \end{aligned}$$

Subsequently, it follows from Lemma 2, (1) and (12) that

$$\begin{aligned} \hat{x}_{k|k} &= \begin{cases} \mathbb{E}\{x_k|\mathcal{I}_k\}, & \text{if } \gamma_k = 1 \\ \mathbb{E}\{x_k|\mathcal{I}_{k-1}\}, & \text{if } \gamma_k = 0 \end{cases} \\ &= \begin{cases} \hat{x}_{k|k-1} + \tilde{\Sigma}_k\Sigma_{\tilde{y}_k}^{-1}\tilde{y}_k, & \text{if } \gamma_k = 1 \\ A\hat{x}_{k-1|k-1}, & \text{if } \gamma_k = 0 \end{cases}. \end{aligned} \tag{14}$$

Noting that

$$\hat{x}_{k|k-1} = \mathbb{E}\{Ax_{k-1} + \omega_{k-1}|\mathcal{I}_{k-1}\} = A\hat{x}_{k-1|k-1},$$

it can be concluded from (14) that

$$\begin{cases} \hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1}, \\ \hat{x}_{k|k} = \hat{x}_{k|k-1} + \gamma_k\tilde{\Sigma}_k\Sigma_{\tilde{y}_k}^{-1}\tilde{y}_k \end{cases}. \tag{15}$$

For the case that $\gamma_k = 1$, it is easy to observe from the definition of $\tilde{y}_k$ that

$$\tilde{y}_k = \Phi(\hat{\xi})Ce_{k|k-1} + \Phi(\hat{\xi})\nu_k,$$

which implies that

$$\begin{aligned} \tilde{\Sigma}_k &= \mathbb{E}\big\{(x_k - \mathbb{E}\{x_k\})(\Phi(\hat{\xi})Ce_{k|k-1} + \Phi(\hat{\xi})\nu_k)^T\big\} \\ &= \mathbb{E}\big\{(e_{k|k-1} + \hat{x}_{k|k-1})e_{k|k-1}^T C^T\Phi^T(\hat{\xi})\big\} \\ &= \Sigma_{e_{k|k-1}}C^T\Phi^T(\hat{\xi}), \end{aligned}$$

and

$$\Sigma_{\tilde{y}_k} = \Phi(\hat{\xi})C\Sigma_{e_{k|k-1}}C^T\Phi^T(\hat{\xi}) + \Phi(\hat{\xi})R\Phi^T(\hat{\xi}).$$

To obtain a recursive form for the MMSE estimator, we shall consider the calculation of $\Sigma_{e_{k|k-1}}$. As shown in [1], it is obvious that

$$\begin{aligned} \Sigma_{e_{k|k-1}} &= A\Sigma_{e_{k-1|k-1}}A^T + Q, \\ \Sigma_{e_{k|k}} &= \Sigma_{e_{k|k-1}} - \gamma_k\Sigma_{e_{k|k-1}}C^T\Phi^T(\hat{\xi})\Sigma_{\tilde{y}_k}^{-1}\Phi(\hat{\xi})C\Sigma_{e_{k|k-1}}. \end{aligned}$$

The proof is now complete. ■

Now, we are in the position to consider the case of $\mathrm{mod}(k,d) = 0$, where the received measurement output is

$$\bar{y}_k = \begin{cases} \emptyset, & \text{if } \gamma_k = 0 \\ \begin{bmatrix} y_{1,k-d} \\ y_{2,k} \end{bmatrix}, & \text{if } \gamma_k = 1 \end{cases}$$

Evidently, the measurement data received at the previous time instant, i.e., $y_{1,k-d}$, can aid in improving the state estimate of x_{k-d}, which, in turn, can help "correct" the generated state estimates of $\{x_i\}_{i=k-d,k-d+1,\ldots,k-1}$. To generate the desired state estimates of x_k using these corrected state estimates, we introduce the following sets that describe the available measurements:

$$\begin{cases} \check{\mathcal{I}}_{k-d} \triangleq \mathcal{I}_{k-d} \cup \{\check{y}_{k-d}\}, \\ \check{\mathcal{I}}_{k-d+i} \triangleq \check{\mathcal{I}}_{k-d+i-1} \cup \{\check{y}_{k-d+i}\}, \quad i = 1,2,\ldots,d \end{cases}$$

where

$$\check{y}_{k-d} \triangleq \begin{cases} y_{1,k-d}, & \text{if } \gamma_k = 1 \\ \emptyset, & \text{if } \gamma_k = 0 \end{cases},$$

$$\check{y}_{k-d+i} \triangleq \begin{cases} y_{2,k-d+i}, & \text{if } \gamma_{k-d+i} = 1 \\ \emptyset, & \text{if } \gamma_{k-d+i} = 0 \end{cases}, \quad i = 1,2,\ldots,d.$$

Now, we shall consider the corrected state estimate of x_{k-d}. For notation simplicity, we define $\check{x}_{i|i} \triangleq \mathbb{E}\{x_i|\check{\mathcal{I}}_i\}$ for $i = k-d, k-d+1,\ldots,k$. In this paper, the corrected state estimate of x_{k-d} is calculated by the MMSE $\mathbb{E}\{x_{k-d}|\check{\mathcal{I}}_{k-d}\} = \check{x}_{k-d|k-d}$.

In light of definition of $\check{\mathcal{I}}_{k-d}$, the state estimate $\check{x}_{k-d|k-d}$ can be calculated in the following theorem.

Theorem 2: For the case that $\mathrm{mod}(k,d) = 0$ and $k > 0$, the value of $\check{x}_{k-d|k-d}$ can be calculated as follows:

$$\check{x}_{k-d|k-d} = \hat{x}_{k-d|k-d} + \gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d} \tag{16}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

where

$$\begin{aligned}\vec{y}_{1,k-d} &\triangleq \gamma_k\big(y_{1,k-d}-\mathbb{E}\{y_{1,k-d}|\mathcal{I}_{k-d}\}\big)\\ &=\gamma_k\big(y_{1,k-d}-\Phi(\vec{\xi})C\hat{x}_{k-d|k-d}\big),\\ \vec{\Sigma}_{k-d} &\triangleq \mathbb{E}\{(x_{k-d}-\mathbb{E}\{x_{k-d}\})\vec{y}_{1,k-d}^T|\gamma_0^k\}\\ &=\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi}),\\ \Sigma_{\vec{y}_{1,k-d}} &\triangleq \mathbb{E}\{\vec{y}_{k-d}\vec{y}_{k-d}^T|\gamma_0^k\}\\ &=\Phi(\vec{\xi})C\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi})+\Phi(\vec{\xi})R\Phi^T(\vec{\xi}).\end{aligned}$$

Furthermore, the value of the corresponding conditional variance matrix for $x_{k-d}-\check{x}_{k-d|k-d}$ can be calculated as follows:

$$\begin{aligned}\check{\Sigma}_{e_{k-d|k-d}} =&\Sigma_{e_{k-d|k-d}}-\gamma_k\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi})\\ &\times\Sigma_{\vec{y}_{1,k-d}}^{-1}\Phi(\vec{\xi})C\Sigma_{e_{k-d|k-d}}\end{aligned}\tag{17}$$

where

$$\check{\Sigma}_{e_{k-d|k-d}}\triangleq\mathbb{E}\{(x_{k-d}-\check{x}_{k-d|k-d})(x_{k-d}-\check{x}_{k-d|k-d})^T|\gamma_0^k\}.$$

Proof: According to the definition of $\check{x}_{k-d|k-d}$, it is observed from the definition of $\check{\mathcal{I}}_{k-d}$ that

$$\check{x}_{k-d|k-d}=\mathbb{E}\{x_{k-d}|\check{\mathcal{I}}_{k-d}\}=\hat{x}_{k-d|k-d}\tag{18}$$

if $\gamma_k=0$.

For the case of $\gamma_k=1$, it is concluded that $\check{\mathcal{I}}_{k-d}=\mathcal{I}_{k-d}\cup\{y_{1,k-d}\}$. Along the similar lines in the proof of Theorem 1, we have $\mathbb{E}\{x_{k-d}|\mathcal{I}_{k-d}\}=\mathbb{E}\{x_{k-d}|\tilde{\mathcal{I}}_{k-d}\}$, from which we observe that

$$\begin{aligned}\check{x}_{k-d|k-d}&=\mathbb{E}\big\{x_{k-d}|\mathcal{I}_{k-d}\cup\{y_{1,k-d}\}\big\}\\ &=\mathbb{E}\{x_{k-d}|\vec{y}_{1,k-d}\}+\mathbb{E}\{x_{k-d}|\tilde{\mathcal{I}}_{k-d}\}-\mathbb{E}\{x_{k-d}\}\\ &=\hat{x}_{k-d|k-d}+\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d}\end{aligned}\tag{19}$$

where $\tilde{\mathcal{I}}_{k-d}\triangleq\{\tilde{y}_0,\tilde{y}_1,\ldots,\tilde{y}_{k-d}\}$ with

$$\begin{aligned}&\vec{\Sigma}_{k-d}\\ &=\mathbb{E}\big\{(x_{k-d}-\mathbb{E}\{x_{k-d}\})(\Phi(\vec{\xi})Ce_{k-d|k-d}+\Phi(\vec{\xi})\nu_{k-d})^T\big\}\\ &=\mathbb{E}\big\{(e_{k-d|k-d}+\hat{x}_{k-d|k-d})e_{k-d|k-d}^TC^T\Phi^T(\vec{\xi})\big\}\\ &=\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi})\end{aligned}$$

and

$$\Sigma_{\vec{y}_{1,k-d}}=\Phi(\vec{\xi})C\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi})+\Phi(\vec{\xi})R\Phi^T(\vec{\xi}).$$

Summarizing the results derived so far, it is concluded that

$$\check{x}_{k-d|k-d}=\hat{x}_{k-d|k-d}+\gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d}.\tag{20}$$

Now, let us calculate the value of $\check{\Sigma}_{e_{k-d|k-d}}$ as follows:

$$\begin{aligned}&\check{\Sigma}_{e_{k-d|k-d}}\\ &=\mathbb{E}\{(x_{k-d}-\check{x}_{k-d|k-d})(x_{k-d}-\check{x}_{k-d|k-d})^T|\gamma_0^k\}\\ &=\mathbb{E}\{(e_{k-d|k-d}-\gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d})(e_{k-d|k-d}\\ &\quad-\gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d})^T|\gamma_0^k\}\\ &=\Sigma_{e_{k-d|k-d}}-\gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{\Sigma}_{k-d}^T\\ &=\Sigma_{e_{k-d|k-d}}-\gamma_k\Sigma_{e_{k-d|k-d}}C^T\Phi^T(\vec{\xi})\Sigma_{\vec{y}_{1,k-d}}^{-1}\Phi(\vec{\xi})C\Sigma_{e_{k-d|k-d}}.\end{aligned}$$

The proof is now complete. ■

The following corollaries, which can be easily obtained based on Theorem 2, are presented without proof to save space.

Corollary 2: For the case of $\mathrm{mod}(k,d)=0$, the values of $\{\check{x}_{i|i}\}_{i=k-d+1,k-d+2,\ldots,k}$ can be calculated as follows:

$$\begin{cases}\check{x}_{i|i-1}=A\check{x}_{i-1|i-1}\\ \check{x}_{i|i}=\check{x}_{i|i-1}+\gamma_i\check{\vec{\Sigma}}_i\check{\Sigma}_{\vec{y}_{2,i}}^{-1}\vec{y}_{2,i}\end{cases}\tag{21}$$

where

$$\begin{aligned}&\check{e}_{i|i-1}\triangleq x_i-\check{x}_{i|i-1},\quad \check{\Sigma}_{e_{i|i-1}}\triangleq\mathbb{E}\{\check{e}_{i|i-1}\check{e}_{i|i-1}^T|\gamma_0^k\},\\ &\check{\vec{\Sigma}}_i\triangleq\mathbb{E}\{(x_i-\mathbb{E}\{x_i\})\vec{y}_{2,i}^T|\gamma_0^k\}=\check{\Sigma}_{e_{i|i-1}}C^T\Phi^T(\hat{\xi}),\\ &\check{\Sigma}_{\vec{y}_{2,i}}\triangleq\mathbb{E}\{\vec{y}_{2,i}\vec{y}_{2,i}^T|\gamma_0^k\}=\Phi(\hat{\xi})\big(C\check{\Sigma}_{e_{i|i-1}}C^T+R\big)\Phi^T(\hat{\xi}),\\ &\vec{y}_{2,i}\triangleq\gamma_i(y_{2,i}-\mathbb{E}\{y_{2,i}|\check{\mathcal{I}}_{i-1}\})=\gamma_i(y_{2,i}-\Phi(\hat{\xi})C\check{x}_{i|i-1}).\end{aligned}$$

Furthermore, the values of $\{\check{\Sigma}_{e_{i|i-1}}\}_{i=k-d+1,k-d+2,\ldots,k}$ and $\{\check{\Sigma}_{e_{i|i}}\}_{i=k-d+1,k-d+2,\ldots,k}$ can be calculated recursively by using the following difference equations:

$$\begin{cases}\check{\Sigma}_{e_{i|i-1}}=A\check{\Sigma}_{e_{i-1|i-1}}A^T+Q\\ \check{\Sigma}_{e_{i|i}}=\check{\Sigma}_{e_{i|i-1}}-\gamma_i\check{\vec{\Sigma}}_i\check{\Sigma}_{\vec{y}_{2,i}}^{-1}\check{\vec{\Sigma}}_i^T\end{cases},\tag{22}$$

where $\check{e}_{i|i}\triangleq x_i-\check{x}_{i|i}$ and $\check{\Sigma}_{e_{i|i}}\triangleq\mathbb{E}\{\check{e}_{i|i}\check{e}_{i|i}^T|\gamma_0^k\}$.

Corollary 3: For the case of $\mathrm{mod}(k,d)=0$, the MMSE state estimate $\hat{x}_{k|k}$ and the corresponding conditional error variance matrices can be calculated as follows:

$$\begin{cases}\hat{x}_{k|k}=\mathbb{E}\{x_k|\mathcal{I}_k\}=\mathbb{E}\{x_k|\check{\mathcal{I}}_k\}=\check{x}_{k|k}\\ \Sigma_{e_{k|k}}=\check{\Sigma}_{e_{k|k}}\end{cases}.\tag{23}$$

Summarizing the above discussions, the detailed implementation of the whole estimation process can be described as follows:

Case 1: if $\mathrm{mod}(k,d)\neq0$ or $k=0$

$$\begin{cases}\hat{x}_{k|k-1}=A\hat{x}_{k-1|k-1},\\ \hat{x}_{k|k}=\hat{x}_{k|k-1}+\gamma_k\tilde{\Sigma}_k\Sigma_{\tilde{y}_k}^{-1}\tilde{y}_k\\ \hat{x}_{0|-1}=\bar{x}_0\end{cases}$$

where the computations of $\tilde{y}_k$, $\tilde{\Sigma}_k$ and $\Sigma_{\tilde{y}_k}$ are given in Theorem 1.

Case 2: if $\mathrm{mod}(k,d)=0$ and $k>0$

$$\begin{cases}\check{x}_{k-d|k-d}=\hat{x}_{k-d|k-d}+\gamma_k\vec{\Sigma}_{k-d}\Sigma_{\vec{y}_{1,k-d}}^{-1}\vec{y}_{1,k-d}\\ \check{x}_{i|i-1}=A\check{x}_{i-1|i-1},\quad k-d<i\le k\\ \check{x}_{i|i}=\check{x}_{i|i-1}+\gamma_i\check{\vec{\Sigma}}_i\check{\Sigma}_{\vec{y}_{2,i}}^{-1}\vec{y}_{2,i},\quad k-d<i\le k\\ \hat{x}_{k|k}=\check{x}_{k|k}\end{cases}$$

where the computations of $\vec{y}_{1,k-d}$, $\vec{\Sigma}_{k-d}$, $\Sigma_{\vec{y}_{1,k-d}}$, $\check{\vec{\Sigma}}_i$, $\check{\Sigma}_{\vec{y}_{2,i}}$ and $\vec{y}_{2,i}$ are given in Theorem 2 and Corollary 2.

Remark 4: It should be pointed out that the estimates at time instant $\{k-d+1,k-d+2,\ldots,k-1\}$ derived in Corollary 2 can be regarded as the "corrected" version of the estimates derived in Theorem 1. Actually, Theorem 1 calculates the *real-time* MMSE estimate at time instant k for the case that $\mathrm{mod}(k,d)\neq0$. For the case that $\mathrm{mod}(k,d)=0$, Theorem 2 and Corollary 2 calculate a sequence of MMSE estimates

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

$\{\check{x}_{i|i}\}_{i=k-d,k-d+1,\ldots,k}$, where $\{\check{x}_{i|i}\}_{i=k-d,k-d+1,\ldots,k-1}$ are regarded as the "updated" MMSE estimates at time instants $\{k-d, k-d+2, \ldots, k-1\}$, and $\check{x}_{k|k}$ is used to generate the *real-time* MMSE estimate at time instant k based on those updated MMSE estimates. Obviously, the derived results in Corollary 2 are actually the estimates for "historic states". Hence, although the results in Corollary 2 might be more accurate than the estimates derived in Theorem 1, Theorem 1 is of great importance from the aspect of real-time application.

Remark 5: By now, we have completed the design of the MMSE state estimator and derived the conditional one-step prediction error variance matrices $\{\Sigma_{e_{k|k-1}}\}_{k\geq 1}$ and conditional estimation error variance matrices $\{\Sigma_{e_{k|k}}\}_{k\geq 0}$, respectively. It should be pointed out that the values of $\{\Sigma_{e_{k|k-1}}\}_{k\geq 1}$ and $\{\Sigma_{e_{k|k}}\}_{k\geq 0}$ are dependent on the sequence $\{\gamma_k\}_{k\geq 0}$. To study the infinite-horizon property of the estimation error, it is reasonable to analyze ultimate boundedness of the estimation error variance matrix $\mathbb{E}\{e_{k|k}e_{k|k}^T\} = \mathbb{E}\{\Sigma_{e_{k|k}}\}$ with the consideration of the statistical distribution of the random variable sequence $\{\gamma_k\}_{k\geq 0}$.

C. Boundedness analysis of $\mathbb{E}\{\Sigma_{e_{k|k}}\}$

In this subsection, we are in a position to analyze the ultimate boundedness for the time-varying matrix $\mathbb{E}\{\Sigma_{e_{k|k}}\}$. According to the recursions proposed in (11), the following equalities hold for $\mathrm{mod}(k,d)\neq 0$ or $k=0$:

$$\begin{cases} \Sigma_{e_{k|k-1}} = A\Sigma_{e_{k-1|k-1}}A^T + Q \\ \Sigma^{-1}_{e_{k|k}} = \Sigma^{-1}_{e_{k|k-1}} + \gamma_k C^T\Phi^T(\hat{\xi})\big(\Phi(\hat{\xi})R\Phi^T(\hat{\xi})\big)^{-1}\Phi(\hat{\xi})C \end{cases}. \tag{24}$$

On the other hand, for the case of $\mathrm{mod}(k,d)=0$ and $k>0$, we have

$$\begin{cases} \check{\Sigma}^{-1}_{e_{k-d|k-d}} = \gamma_k C^T\Phi^T(\vec{\xi})\big(\Phi(\vec{\xi})R\Phi^T(\vec{\xi})\big)^{-1}\Phi(\vec{\xi})C \\ \qquad\qquad + \Sigma^{-1}_{e_{k-d|k-d}} \\ \check{\Sigma}^{-1}_{e_{i|i}} = \check{\Sigma}^{-1}_{e_{i|i-1}} + \gamma_i C^T\Phi^T(\hat{\xi})\big(\Phi(\hat{\xi})R\Phi^T(\hat{\xi})\big)^{-1}\Phi(\hat{\xi})C, \\ \qquad\qquad\qquad\qquad\qquad\qquad k-d<i<k \\ \check{\Sigma}_{e_{i|i-1}} = A\check{\Sigma}_{e_{i-1|i-1}}A^T + Q, \qquad k-d<i\leq k \\ \Sigma^{-1}_{e_{k|k}} = \check{\Sigma}^{-1}_{e_{k|k-1}} + \gamma_k C^T\Phi^T(\hat{\xi})\big(\Phi(\hat{\xi})R\Phi^T(\hat{\xi})\big)^{-1}\Phi(\hat{\xi})C \end{cases}. \tag{25}$$

Now, we focus our attention on the lower bounds of the time-varying matrix $\Sigma_{e_{k|k}}$.

Proposition 2: The following inequalities hold for any $k\geq 0$:

$$\Sigma_{e_{k|k}} \geq \underline{\phi}^{-1}I, \quad \check{\Sigma}_{e_{k|k}} \geq \underline{\phi}^{-1}I \tag{26}$$

where

$$\begin{aligned} &\underline{\hat{\phi}} \triangleq \min\{\lambda_{\min}\{X_0\}, \lambda_{\min}\{Q\}\}, \\ &\underline{\phi} \triangleq \underline{\hat{\phi}}^{-1} + 2\lambda^{-1}_{\min}\{R\}\lambda_{\max}\{C^TC\}. \end{aligned}$$

Proof: First, it is easy to see from the recursions (24) and (25) that

$$\begin{cases} \Sigma_{e_{k|k-1}} \geq \min\{\lambda_{\min}\{X_0\}, \lambda_{\min}\{Q\}\}I = \underline{\hat{\phi}}I \\ \check{\Sigma}_{e_{k|k-1}} \geq \lambda_{\min}\{Q\}I \geq \underline{\hat{\phi}}I \end{cases}. \tag{27}$$

Noting that $\Phi(\hat{\xi})\Phi^T(\hat{\xi}) = I$ and $\Phi^T(\hat{\xi})\Phi(\hat{\xi}) \leq I$, it is easy to see that

$$\begin{cases} \Phi^T(\vec{\xi})\big(\Phi(\vec{\xi})R\Phi^T(\vec{\xi})\big)^{-1}\Phi(\vec{\xi}) \leq \lambda^{-1}_{\min}\{R\}I \\ \Phi^T(\hat{\xi})\big(\Phi(\hat{\xi})R\Phi^T(\hat{\xi})\big)^{-1}\Phi(\hat{\xi}) \leq \lambda^{-1}_{\min}\{R\}I \end{cases}.$$

Then, it follows from the calculation of $\Sigma^{-1}_{e_{k|k}}$ that

$$\begin{aligned} \Sigma^{-1}_{e_{k|k}} &\leq \underline{\hat{\phi}}^{-1}I + \gamma_k C^T\Phi^T(\hat{\xi})\big(\Phi(\hat{\xi})R\Phi^T(\hat{\xi})\big)^{-1}\Phi(\hat{\xi})C \\ &\leq \underline{\hat{\phi}}^{-1}I + \gamma_k\lambda^{-1}_{\min}\{R\}C^TC < \underline{\phi}I, \end{aligned} \tag{28}$$

and

$$\begin{cases} \check{\Sigma}^{-1}_{e_{i|i}} \leq \check{\Sigma}^{-1}_{e_{i|i-1}} + \lambda^{-1}_{\min}\{R\}C^TC < \underline{\phi}I, \ k-d<i<k \\ \check{\Sigma}^{-1}_{e_{k-d|k-d}} \leq \Sigma^{-1}_{e_{k-d|k-d}} + \lambda^{-1}_{\min}\{R\}C^TC \leq \underline{\phi}I, \end{cases} \tag{29}$$

which implies that $\Sigma_{e_{k|k}} \geq \underline{\phi}^{-1}I$ and $\check{\Sigma}_{e_{k|k}} \geq \underline{\phi}^{-1}I$. The proof is now complete. ■

According to Proposition 2, we can easily obtain the following proposition.

Proposition 3: For two given positive integers $s\geq 1$ and $1\leq N\leq s$, the following condition holds:

$$\begin{aligned} \Sigma^{-1}_{e_{sd|sd}} \geq\ &\theta^{-Nd}(A^{-Nd})^T\Sigma^{-1}_{e_{(s-N)d|(s-N)d}}A^{-Nd} \\ &+ \theta^{-Nd}\mathcal{F}\big(\gamma^{sd}_{(s-N)d+1}\big) \end{aligned} \tag{30}$$

where

$$\begin{aligned} &\theta \triangleq 1 + \frac{\underline{\phi}\lambda_{\max}\{Q\}}{\lambda_{\min}\{AA^T\}},\ \mathcal{R}(\hat{\xi}) \triangleq \frac{C^T\Phi^T(\hat{\xi})\Phi(\hat{\xi})C}{\lambda_{\max}\{R\}}, \\ &\mathcal{F}\big(\gamma^{sd}_{(s-N)d+1}\big) \triangleq \sum_{i=0}^{Nd-1}\big(\gamma_{sd-i}(A^{-i})^T\mathcal{R}(\hat{\xi})A^{-i}\big) \\ &\qquad\qquad + \sum_{j=1}^{N}\gamma_{(s-j+1)d}(A^{-jd})^T\mathcal{R}(\vec{\xi})A^{-jd}. \end{aligned}$$

Proof: Considering the difference equations (24) and (25), one can infer that

$$\begin{cases} A\Sigma_{e_{k-1|k-1}}A^T \geq \underline{\phi}^{-1}AA^T \geq \underline{\phi}^{-1}\lambda_{\min}\{AA^T\}I \\ Q \leq \lambda_{\max}\{Q\}I \\ A\check{\Sigma}_{e_{k-1|k-1}}A^T \geq \underline{\phi}^{-1}AA^T \geq \underline{\phi}^{-1}\lambda_{\min}\{AA^T\}I \\ Q \leq \lambda_{\max}\{Q\}I \end{cases},$$

which implies that $\Sigma_{e_{k|k-1}} \leq \theta A\Sigma_{e_{k-1|k-1}}A^T$ and $\check{\Sigma}_{e_{k|k-1}} \leq \theta A\Sigma_{e_{k-1|k-1}}A^T$ hold for all $k\geq 1$. Then, it is concluded that

$$\begin{cases} \Sigma^{-1}_{e_{sd|sd}} \geq \theta^{-1}A^{-T}\check{\Sigma}^{-1}_{e_{sd-1|sd-1}}A^{-1} + \gamma_{sd}\mathcal{R}(\hat{\xi}) \\ \check{\Sigma}^{-1}_{e_{sd-1|sd-1}} \geq \theta^{-1}A^{-T}\check{\Sigma}^{-1}_{e_{sd-2|sd-2}}A^{-1} + \gamma_{sd-1}\mathcal{R}(\hat{\xi}) \\ \check{\Sigma}^{-1}_{e_{sd-2|sd-2}} \geq \theta^{-1}A^{-T}\check{\Sigma}^{-1}_{e_{sd-3|sd-3}}A^{-1} + \gamma_{sd-2}\mathcal{R}(\hat{\xi}) \\ \qquad\qquad\vdots \\ \check{\Sigma}^{-1}_{e_{sd-d|sd-d}} \geq \Sigma^{-1}_{e_{sd-d|sd-d}} + \gamma_{sd}\mathcal{R}(\vec{\xi}) \end{cases}. \tag{31}$$

According to (31), it is readily obtained that

$\Sigma^{-1}_{e_{sd|sd}}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

$$
\begin{aligned}
&\geq \theta^{-d}(A^{-d})^T\Sigma^{-1}_{e_{(s-1)d|(s-1)d}}A^{-d} + \sum_{i=0}^{d-1}\big(\theta^{-i}\gamma_{sd-i}(A^{-i})^T \\
&\quad \times \mathcal{R}(\hat{\xi})A^{-i}\big) + \gamma_{sd}\theta^{-d}(A^{-d})^T\mathcal{R}(\vec{\xi})A^{-d} \\
&\geq \cdots \\
&\geq \theta^{-Nd}\Bigg((A^{-Nd})^T\Sigma^{-1}_{e_{(s-N)d|(s-N)d}}A^{-Nd} + \sum_{i=0}^{Nd-1}\big(\gamma_{sd-i} \\
&\quad \times (A^{-i})^T\mathcal{R}(\hat{\xi})A^{-i}\big) + \sum_{j=1}^{N}\gamma_{(s-j+1)d}(A^{-jd})^T\mathcal{R}(\vec{\xi})A^{-jd}\Bigg) \\
&= \theta^{-Nd}(A^{-Nd})^T\Sigma^{-1}_{e_{(s-N)d|(s-N)d}}A^{-Nd} \\
&\quad + \theta^{-Nd}\mathcal{F}(\gamma^{sd}_{(s-N)d+1}).
\end{aligned} \tag{32}
$$

■

Now, we are ready to consider the ultimate boundedness of $\mathbb{E}\{\Sigma_{e_{k|k}}\}$. According to (24), it is easy to conclude that $\Sigma_{e_{sNd+i|sNd+i}} \leq \theta^i A^i \Sigma_{e_{sNd|sNd}(A^i)^T}$ for any $i > 0$, which implies that the ultimate boundedness of $\mathbb{E}\{\Sigma_{e_{k|k}}\}$ can be achieved if the matrix sequence $\{\mathbb{E}\{\Sigma_{e_{sNd|sNd}}\}\}_{s=0,1,\cdots}$ is ultimately bounded. Next, let us consider the boundedness of $\{\mathbb{E}\{\Sigma_{e_{sNd|sNd}}\}\}_{s=0,1,\cdots}$ in the following Theorem.

Theorem 3: Given the occurrence probability $\bar{\gamma}$ and positive integer $N > 1$, calculate the sequence of positive scalars $\{\varpi_{s+1}\}_{s\geq 0}$ according to the following difference equation

$$
\begin{cases}
\varpi_{s+1} = \displaystyle\sum_{j\in\bar{\mathcal{O}}}\pi(j)\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\}\varpi_s + \sum_{j\in\mathcal{O}}\pi(j)\vartheta^{-1} \\
\varpi_0 = \lambda_{\max}\{X_0\}
\end{cases} \tag{33}
$$

where

$$
\begin{aligned}
&\mathcal{O} \triangleq \{\eta | \mathcal{F}(\eta) > 0, \eta \in \vec{\mathcal{O}}\},\ \vartheta \triangleq \min_{\eta\in\mathcal{O}}\big\{\lambda_{\min}\{\mathcal{F}(\eta)\}\big\}, \\
&\pi(j) \triangleq \theta^{\bar{N}}\Big(\bar{\gamma}^{(\mathbf{1}_{\bar{N}})^T\cdot j}(1-\bar{\gamma})^{(\mathbf{1}_{\bar{N}})^T\cdot(\mathbf{1}_{\bar{N}}-j)}\Big),\quad \bar{\mathcal{O}} \triangleq \vec{\mathcal{O}}\backslash\mathcal{O}, \\
&\vec{\mathcal{O}} \triangleq \left\{\begin{bmatrix}0\\0\\0\\\vdots\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\\vdots\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\\vdots\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\\vdots\\0\end{bmatrix}, \ldots, \begin{bmatrix}1\\1\\1\\\vdots\\1\end{bmatrix}\right\}.
\end{aligned}
$$

Then, the mathematical expectation of the time-varying matrix $\Sigma_{e_{s\bar{N}|s\bar{N}}}$ is bounded by

$$
\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\} \leq \varpi_s I, \qquad s = 0, 1, \ldots \tag{34}
$$

where $\bar{N} \triangleq Nd$. Furthermore, the value of ϖ_s converges exponentially to the steady value

$$
\varpi_\infty \triangleq \frac{\sum_{j\in\mathcal{O}}\pi(j)\vartheta^{-1}}{1-\sum_{j\in\bar{\mathcal{O}}}\pi(j)\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\}} \tag{35}
$$

if $\sum_{j\in\bar{\mathcal{O}}}\pi(j)\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\} < 1$.

Proof: To prove the assertion that $\mathbb{E}\{\Sigma_{e_{sN|sN}}\} \leq \varpi_s I$ holds for all $s = 0, 1, \ldots$, the mathematical induction is utilized as follows.

Initial Step: For $s = 0$, it is immediately known from the definition of (11) that

$$
\Sigma_{e_{0|0}} \leq \Sigma_{e_{0|-1}} = X_0 \leq \lambda_{\max}\{X_0\}I,
$$

which implies that $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\} \leq \varpi_s I$ holds for $s = 0$.

Inductive Step: Given the fact that $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\} \leq \varpi_s I$ holds for $s = 0$, we aim to show that $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\} \leq \varpi_s I$ holds for $s = i$ based on the condition $\mathbb{E}\{\Sigma_{e_{(i-1)\bar{N}|(i-1)\bar{N}}}\} \leq \varpi_{i-1}I$.

According to Proposition 3, it is concluded that

$$
\begin{aligned}
\Sigma^{-1}_{e_{i\bar{N}|i\bar{N}}} \geq{}& \theta^{-\bar{N}}(A^{-\bar{N}})^T\Sigma^{-1}_{e_{(i-1)\bar{N}|(i-1)\bar{N}}}A^{-\bar{N}} \\
&+ \theta^{-\bar{N}}\mathcal{F}\big(\gamma^{i\bar{N}}_{(i-1)\bar{N}+1}\big),
\end{aligned}
$$

from which we have

$$
\begin{aligned}
&\Sigma_{e_{i\bar{N}|i\bar{N}}} \\
&\leq \begin{cases}
\theta^{\bar{N}}A^{\bar{N}}\Sigma_{e_{(i-1)\bar{N}|(i-1)\bar{N}}}(A^{\bar{N}})^T, & \text{if } \gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \bar{\mathcal{O}} \\
\theta^{\bar{N}}\mathcal{F}^{-1}\big(\gamma^{i\bar{N}}_{(i-1)\bar{N}+1}\big), & \text{if } \gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \mathcal{O}
\end{cases}.
\end{aligned} \tag{36}
$$

Then, it follows from (36) that

$$
\begin{aligned}
&\mathbb{E}\big\{\Sigma_{e_{i\bar{N}|i\bar{N}}}\big\} = \mathbb{E}\big\{\mathbb{E}\big\{\Sigma_{e_{i\bar{N}|i\bar{N}}}\big|\gamma_0^{(i-1)\bar{N}}\big\}\big\} \\
&= \mathbb{E}\Bigg\{\sum_{\eta\in\vec{\mathcal{O}}}\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = \eta\big\}\Sigma^{*\eta}_{e_{i\bar{N}|i\bar{N}}}\Bigg\} \\
&\leq \mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \bar{\mathcal{O}}\big\}\theta^{\bar{N}}A^{\bar{N}}\mathbb{E}\big\{\Sigma_{e_{(i-1)\bar{N}|(i-1)\bar{N}}}\big\}(A^{\bar{N}})^T \\
&\quad + \mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \mathcal{O}\big\}\theta^{\bar{N}}\mathcal{F}^{-1}\big(\gamma^{i\bar{N}}_{(i-1)\bar{N}+1}\big) \\
&\leq \mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \bar{\mathcal{O}}\big\}\theta^{\bar{N}}A^{\bar{N}}\mathbb{E}\big\{\Sigma_{e_{(i-1)\bar{N}|(i-1)\bar{N}}}\big\}(A^{\bar{N}})^T \\
&\quad + \mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \mathcal{O}\big\}\theta^{\bar{N}}\vartheta
\end{aligned} \tag{37}
$$

where $\Sigma^{*\eta}_{e_{i\bar{N}|i\bar{N}}}$ represents the value of $\Sigma_{e_{i\bar{N}|i\bar{N}}}$ in the case that $\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = \eta$.

For the occurrence probabilities $\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \bar{\mathcal{O}}\big\}$ and $\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \mathcal{O}\big\}$, we observe that

$$
\begin{cases}
\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \bar{\mathcal{O}}\big\} = \displaystyle\sum_{j\in\bar{\mathcal{O}}}\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = j\big\} \\
\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} \in \mathcal{O}\big\} = \displaystyle\sum_{j\in\mathcal{O}}\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = j\big\}
\end{cases}.
$$

It should be pointed out that, for any vector $j \in \bar{\mathcal{O}}$ or $j \in \mathcal{O}$, the value of j is composed by the scalars 1 and 0. Obviously, the number of non-zero elements in the vector j can be calculated by $(\mathbf{1}_{\bar{N}})^T \cdot j$, and the number of zero elements in the vector j can be calculated by $(\mathbf{1}_{\bar{N}})^T\cdot(\mathbf{1}_{\bar{N}} - j)$. Subsequently, it is concluded that

$$
\begin{aligned}
&\sum_{j\in\bar{\mathcal{O}}}\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = j\big\} \\
&= \sum_{j\in\bar{\mathcal{O}}}\Big(\bar{\gamma}^{(\mathbf{1}_{\bar{N}})^T\cdot j}(1-\bar{\gamma})^{(\mathbf{1}_{\bar{N}})^T\cdot(\mathbf{1}_{\bar{N}}-j)}\Big),
\end{aligned}
$$

and

$$
\begin{aligned}
&\sum_{j\in\mathcal{O}}\mathrm{Prob}\big\{\gamma^{i\bar{N}}_{(i-1)\bar{N}+1} = j\big\} \\
&= \sum_{j\in\mathcal{O}}\Big(\bar{\gamma}^{(\mathbf{1}_{\bar{N}})^T\cdot j}(1-\bar{\gamma})^{(\mathbf{1}_{\bar{N}})^T\cdot(\mathbf{1}_{\bar{N}}-j)}\Big).
\end{aligned}
$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

Accordingly, it follows from (37) that

$$\begin{aligned}&\mathbb{E}\{\Sigma_{e_{i\bar{N}|i\bar{N}}}\}\\ &\leq \left(\sum_{j\in\bar{\mathcal{O}}}\pi(j)\varpi_{i-1}\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\}+\sum_{j\in\mathcal{O}}\pi(j)\vartheta^{-1}\right)I\\ &=\varpi_i I. \end{aligned}\tag{38}$$

Hence, by the induction, it is concluded that $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\}\leq \varpi_s I$ holds for all $s\geq 0$. Furthermore, it is easy to see that ϖ_s converges exponentially to the steady value ϖ_∞ if the condition $\sum_{j\in\bar{\mathcal{O}}}\pi(j)\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\}<1$ holds, where

$$\varpi_\infty=\frac{\sum_{j\in\mathcal{O}}\pi(j)\theta^{\bar{N}}\vartheta^{-1}}{1-\sum_{j\in\bar{\mathcal{O}}}\pi(j)\varpi_{i-1}\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\}}.$$

The proof is now complete. ■

Remark 6: So far, in Theorems 1-2, the secure RSE problem is tackled for a class of networked systems in the presence of eavesdroppers. A novel PED mechanism is developed to achieve the desired information security while alleviating the computational cost in the signal transmitter. The effects induced by the encryption process and packet dropouts are described using a parameter-dependent model. A dedicatedly designed MMSE estimator, which is implemented in a recursive manner, is developed to generate the desired state estimates under the effects of PED. Furthermore, in Theorem 3, special attention is paid to the ultimate boundedness analysis on the resultant time-varying estimation error variance matrix. It is worth mentioning that the corresponding ultimate boundedness analysis approach is different from the existing results concerning the Kalman filtering issues subject to packet dropouts (where the upper-bounds for the estimation error variance matrices are calculated based on the solutions to certain modified algebraic Riccati equations). In this paper, the upper-bound for the estimation error variance is calculated by using an inverse-matrix-based approach. Compared with the existing results (e.g. [4], [39]), the inverse-matrix-based approach proposed in this paper is implemented without solving certain matrix-valued equations, which provides a convenient way to calculate the upper-bound for $\mathbb{E}\{e_{k|k}e_{k|k}^T\}$.

Remark 7: This paper has presented a systematic investigation of the secure RSE issue against eavesdropping using a PED method. The research is novel in the following three aspects: 1) proposing a novel Jordan-canonical-form-based approach for designing the PED scheme to protect information security; 2) constructing a dedicatedly designed MMSE estimator to handle the effects induced by the PED mechanism; and 3) presenting sufficient conditions to guarantee the ultimate boundedness of the estimation error variance matrix.

IV. Illustrative Examples

In this section, the effectiveness and correctness of the proposed secure RSE algorithm and PED mechanism are verified through two illustrative examples.

Example 1: Consider a discrete-time system (1) with the following parameters:

$$A=\begin{bmatrix}1.01 & 0\\ 0.32 & 1.03\end{bmatrix},\ C=\begin{bmatrix}0.5 & 0\\ 1 & 1\end{bmatrix},\ Q=0.64I,$$

$$R=I,\ X_0=I,\ \bar{x}_0=\begin{bmatrix}0.8 & -0.7\end{bmatrix}^T.$$

It is easy to see that the matrix A has two distinct eigenvalues: $\lambda_1=1.01$ and $\lambda_2=1.03$. Furthermore, it is immediately known from the matrix A that

$$\Lambda=\{\lambda_1,\lambda_2\},\quad \mathcal{G}_1=\begin{bmatrix}0\\1\end{bmatrix},\quad \mathcal{G}_2=\begin{bmatrix}0.014\\-0.4193\end{bmatrix}.$$

As shown in [47], for $i\in\{1,2\}$, the geometric multiplicity of λ_i is $\alpha_i=n-\mathrm{rank}(\lambda_i I-A)=1$. Then, by setting $\vec{\xi}=2$, it can be derived that $\mathrm{rank}\big(\Phi(\hat{\xi})\mathcal{G}_1\big)=0<\alpha_1$, which implies that the linear time-invariant system (3) is undetectable.

In this paper, the occurrence probability of $\gamma_k=1$ is assumed to be $\bar{\gamma}=0.92$. The elapsed time of the encryption process is assumed to be $d=2$. Then, by using the MMSE estimator proposed in Section III-B, the simulation results about the estimation performance at the user side are shown in Figs. 3-4, which depict the true state trajectories and their corresponding estimates. Here, $x_k^{(i)}$ and $\hat{x}_{k|k}^{(i)}$ represent the i-th entry in x_k and $\hat{x}_{k|k}$, respectively.

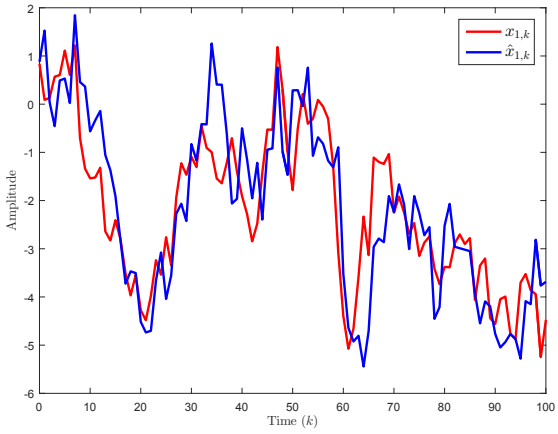

Fig. 3: The trajectories of $x_k^{(1)}$ and $\hat{x}_{k|k}^{(1)}$.

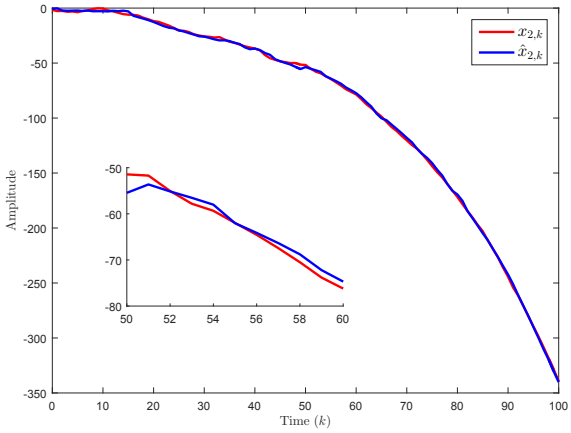

Fig. 4: The trajectories of $x_k^{(2)}$ and $\hat{x}_{k|k}^{(2)}$.

To verify the effectiveness of the PED scheme, we consider the case that the eavesdropper implements a standard Kalman filtering scheme based on its available measurements (i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

$\{y_{2,k}\}_{k\geq 0}$). Fig. 5 shows the trajectories of the estimation error for the user and eavesdropper, respectively. Obviously, the norm of the estimation error for the eavesdropper is divergent under the effects of our proposed PED mechanism. The simulation results confirm that the effectiveness and correctness of our proposed PED mechanism and SE scheme.

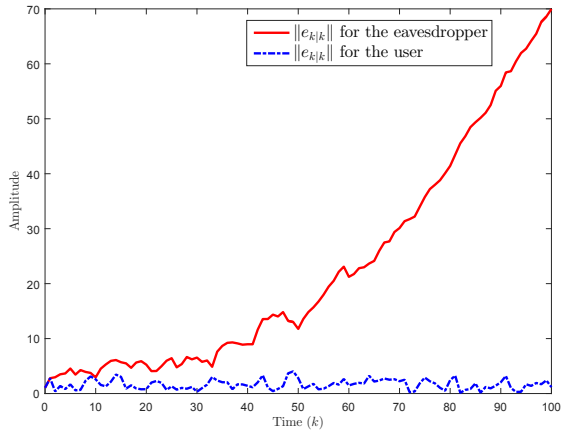

Fig. 5: The trajectories of $\|e_{k|k}\|$ for the user and eavesdropper.

Next, we conduct Monte Carlo simulations (with 100 steps and 200 runs) to verify the boundedness analysis on $\mathbb{E}\{\Sigma_{e_{k|k}}\}$. In this example, the value of N is set to be 1. According to the definition of $\mathcal{F}\big(\gamma^{sd}_{(s-N)d+1}\big)$, the set $\mathcal{O}$ can be derived as follows:

$$\mathcal{O} = \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\},$$

from which we observe that $\sum_{j\in\bar{\mathcal{O}}} \pi(j)\lambda_{\max}\{A^{\bar{N}}(A^{\bar{N}})^T\} = 0.9490 < 1$.

According to Theorem 3, the matrix $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\}$ is bounded by $\varpi_s I$ and the value of ϖ_s converges exponentially to a steady value. Fig. 6 plots the trajectories of the maximum eigenvalues and the minimum eigenvalues of $\frac{1}{200}\lambda_{\max}\{\sum_{i=1}^{200}\Sigma^{(i)}_{e_{s\bar{N}|s\bar{N}}}\}$ (where $\Sigma^{(i)}_{e_{s\bar{N}|s\bar{N}}}$ represents the value of $\Sigma_{e_{s\bar{N}|s\bar{N}}}$ in the i-th run), from which it can be observed that $\mathbb{E}\{\Sigma_{e_{s\bar{N}|s\bar{N}}}\}$ is bounded by ϖ_s and $\underline{\phi}^{-1}$.

Example 2: Let us now consider the application of our developed secure RSE scheme to the maneuvering target tracking problem. The maneuvering target is modeled by the following time-invariant system [5]:

$$x_{k+1} = \begin{bmatrix} 1 & T & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & T \\ 0 & 0 & 0 & 1 \end{bmatrix} x_k + \omega_k$$

where $x_k \triangleq \begin{bmatrix} p_x(k) & \dot{p}_x(k) & p_y(k) & \dot{p}_y(k) \end{bmatrix}^T$ is the state vector; $p_x(k)$ and $p_y(k)$ denote, respectively, the positions in dimensions x and y at time k; and T is the sampling period.

The initial state is set to be $x_0 = \begin{bmatrix} 10 & 0.2 & 8 & 0.8 \end{bmatrix}^T$, and the sampling period of the plant is $T = 0.2$. As proposed in

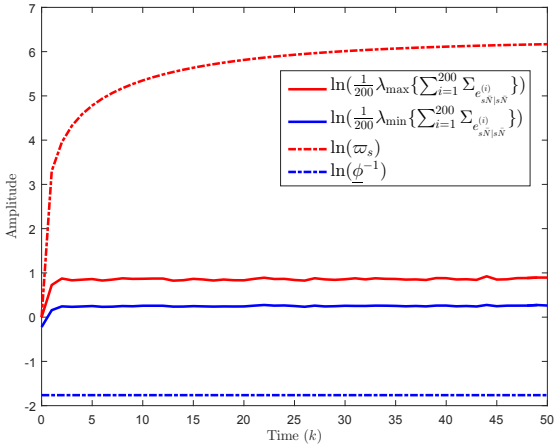

Fig. 6: The trajectories of $\ln(\frac{1}{200}\lambda_{\max}\{\sum_{i=1}^{200}\Sigma^{(i)}_{e_{k|k}}\})$ and $\ln(\frac{1}{200}\lambda_{\min}\{\sum_{i=1}^{200}\Sigma^{(i)}_{e_{k|k}}\})$.

[5], the variance of the process noise ω_k is given by

$$Q \triangleq \sigma^2_{accel} \begin{bmatrix} \frac{T^3}{3} & \frac{T^2}{2} & 0 & 0 \\ \frac{T^2}{2} & T & 0 & 0 \\ 0 & 0 & \frac{T^3}{3} & \frac{T^2}{2} \\ 0 & 0 & \frac{T^2}{2} & T \end{bmatrix}$$

where σ_{accel} is the acceleration standard deviation. In this example, the acceleration standard deviation is set to be $\sigma_{accel} = 2$.

The positions in dimensions x and y are measured by two radars, i.e.,

$$y_k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} x_k + \nu_k.$$

In this example, the values of X_0 and R are set to be

$$P_0 = \mathrm{diag}\{12, 9, 12, 14\}, \quad R = 0.81I.$$

The value of $\bar{\gamma}$ is assumed to be $\bar{\gamma} = 0.85$. The elapsed time of the encryption process is assumed to be $d = 2$.

It is obvious that the matrix A has only one eigenvalue $\lambda_1 = 1$. As shown in [47], the geometric multiplicity of λ_1 is determined by $\alpha_1 = n - \mathrm{rank}(\lambda_1 I - A) = 2$. Then, by selecting $\vec{\xi} = 1$, we have $\mathrm{rank}\big(\Phi(\hat{\xi})\big) < \alpha_1$, from which it can be concluded that the linear time-invariant system (3) is undetectable.

According to the system parameters and the value of $\vec{\xi}$, the simulation results about the MMSE state estimation are given in Fig. 7, which depicts the trajectories of the system states and the derived state estimates. Obviously, our developed SE scheme is capable of tracking the positions of the maneuvering target with satisfactory estimation accuracy.

To examine the effects of our proposed PED mechanism, we consider the case that the eavesdropper implements a standard Kalman filtering scheme based on its available measurements (i.e., $\{y_{2,k}\}_{k\geq 0}$). The corresponding simulation results are given in Fig. 8, from which it can be found that our proposed PED mechanism has largely degraded the estimation performance for the eavesdropper's estimator.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/TAC.2024.3512413, IEEE Transactions on Automatic Control

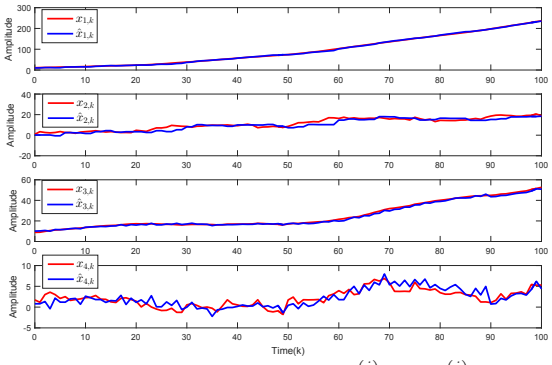

Fig. 7: The trajectories of $x_k^{(i)}$ and $\hat{x}_{k|k}^{(i)}$.

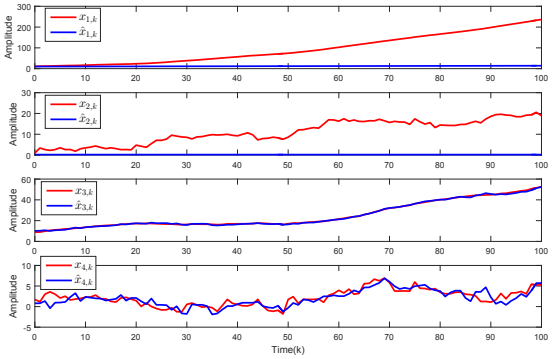

Fig. 8: The trajectories of the system states and their estimates for the eavesdropper.

V. CONCLUSION

In this paper, we have addressed the secure RSE problem of a class of networked systems under the presence of eavesdroppers. We have developed a novel PED mechanism to achieve the desired information security while reducing the computational cost at the signal transmitter. A parameter-dependent model has been constructed to describe the effects induced by the encryption process and packet dropouts. Subsequently, we have devised a dedicated MMSE estimator in a recursive manner to generate the desired state estimates under the effects of PED. We have also analyzed the ultimate boundedness of the resultant time-varying estimation error variance matrix. Finally, we have provided two numerical simulation examples to demonstrate the effectiveness of our proposed algorithm. Potential future research directions include investigating encryption-decryption-based SE problems for nonlinear systems [10], [42], [43] and studying the distributed SE problem against eavesdropping [20], [48].

REFERENCES

[1] B. D. Anderson and J. B. Moore, *Optimal Filtering*, Prentice-Hall, New York, 1979.

[2] C.-Z. Bai, V. Gupta and F. Pasqualetti, On Kalman filtering with compromised sensors: attack stealthiness and performance bounds, *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6641–6648, Dec. 2017.

[3] R. Caballero-Águila, A. Hermoso-Carazo, and J. Linares-Pérez, Networked fusion estimation with multiple uncertainties and time-correlated channel noise, *Information Fusion*, vol. 54, pp. 161-171, 2020.

[4] Y. H. Chang, Q. Hu and C. J. Tomlin, Secure estimation based Kalman Filter for cyber-physical systems against sensor attacks, *Automatica*, vol. 95, pp. 399–412, Sep. 2018.

[5] S. S. Dias and M. G. S. Bruno, Cooperative target tracking using decentralized particle filtering and RSS sensors, *IEEE Transactions on Signal Processing*, vol. 61, no. 14, pp. 3632-3646, Jul. 2013.

[6] D. Ding, Q.-L. Han, X. Ge and J. Wang, Secure state estimation and control of cyber-physical systems: A survey, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176-190, Jan. 2021.

[7] K. Ding, X. Ren, A. S. Leong, D. E. Quevedo and L. Shi, Remote state estimation in the presence of an active eavesdropper, *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 229–244, Jan. 2021.

[8] W. Ding, W. Yang, J. Zhou, L. Shi and G. Chen, Privacy preserving via secure summation in distributed Kalman filtering, *IEEE Transactions on Control of Network Systems*, vol. 9, no. 3, pp. 1481-1492, Sep. 2022.

[9] S. Feng, X. Li, S. Zhang, Z. Jian, H. Duan and Z. Wang, A review: state estimation based on hybrid models of Kalman filter and neural network, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2173682, 2023.

[10] Y. Feng, X. Li, D. Shi and D. Dai, An efficient robust model predictive control for nonlinear Markov jump systems with persistent disturbances using matrix partition, *International Journal of Systems Science*, vol. 54, no. 10, pp. 2118–2133, Jul. 2023.

[11] H. Gao, Y. Li, L. Yu and H. Yu, Collaborative-prediction-based recursive filtering for nonlinear systems with sensor saturation under duty cycle scheduling, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2247007, 2023.

[12] X. Ge, Q.-L. Han, M. Zhong and X. Zhang, Distributed Krein space-based attack detection over sensor networks under deception attacks, *Automatica*, vol. 109, art. no. 108557, Nov. 2019.

[13] F. Han, J. Liu, J. Li, J. Song, M. Wang and Y. Zhang, Consensus control for multi-rate multi-agent systems with fading measurements: the dynamic event-triggered case, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2158959, 2023.

[14] L. Huang, K. Ding, A. S. Leong, D. E. Quevedo and L. Shi, Encryption scheduling for remote state estimation under an operation constraint, *Automatica*, vol. 127, art. no. 109537, May 2021.

[15] Y. Jin, X. Ma, X. Meng and Y. Chen, Distributed fusion filtering for cyber-physical systems under Round-Robin protocol: a mixed H_2/H_∞ framework, *International Journal of Systems Science*, vol. 54, no. 8, pp. 1661–1675, Jun. 2023.

[16] H. Kwakernaak and R. Sivan, *Linear Optial Control Systems*, Wiley-Interscience, New York, 1972.

[17] A. S. Leong, D. E. Quevedo, D. Dolz and S. Dey, Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper, *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3732–3739, Sep. 2019.

[18] W. Li and F. Yang, Information fusion over network dynamics with unknown correlations: An overview, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, art. no. 100003, Jun. 2023.

[19] X.-M. Li, B. Zhang, P. Li, Q. Zhou and R. Lu, Finite-horizon H_∞ state estimation for periodic neural networks over fading channels, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 5, pp. 1450–1460, May 2020.

[20] X. Li and D. Ye, Dynamic event-triggered distributed filtering design for interval type-2 fuzzy systems over sensor networks under deception attacks, *International Journal of Systems Science*, vol. 54, no. 15, pp. 2875–2890, Nov. 2023.

[21] J. Liu, T. Yin, J. Cao, D. Yue and H. R. Karimi, Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 10, pp. 6544-6554, 2021.

[22] E. Mousavinejad, X. Ge, Q.-L. Han, T. J. Lim and L. Vlacic, An ellipsoidal set-membership approach to distributed joint state and sensor fault estimation of autonomous ground vehicles, *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 6, pp. 1107–1118, Jun. 2021.

[23] Z.-H. Pang, L.-Z. Fan, K. Liu and G.-P. Liu, Detection of stealthy false data injection attacks against networked control systems via active data modification, *Information Sciences*, vol. 546, pp. 192-205, 2021.

[24] Z.-H. Pang, T. Mu, F.-Y. Hou, Y. Shi and J. Sun, Two networked predictive control methods for output tracking of networked systems with plant-model mismatch, *International Journal of Systems Science*, vol. 54, no. 10, pp. 2073–2088, 2023.

[25] A. Rajagopal and S. Chitraganti, State estimation and control for networked control systems in the presence of correlated packet drops,

International Journal of Systems Science, vol. 54, no. 11, pp. 2352–2365, 2023.
[26] J. Shang and T. Chen, Linear encryption against eavesdropping on remote state estimation, *IEEE Transactions on Automatic Control*, vol. 68, no. 7, pp. 4413–4419, Jul. 2023.
[27] W. Shang, Y. Kang, H. Xi, Y. Xia and Y.-B. Zhao, Distributed H_∞-consensus filtering with sensor networks: a finite horizon solution, *IMA Journal of Mathematical Control and Information*, vol. 31, no. 1, pp. 33–49, Mar. 2014.
[28] Y. Shen and S. Sun, Distributed recursive filtering for multi-rate uniform sampling systems with packet losses in sensor networks, *International Journal of Systems Science*, vol. 54, no. 8, pp. 1729–1745, Jun. 2023.
[29] L. Shi, M. Epstein and R. M. Murray, Kalman filtering over a aacket-dropping network: a probabilistic perspective, *IEEE Transactions on Automatic Control*, vol. 55, no. 3, pp. 594–604, Mar. 2010.
[30] Y. S. Shmaliy, F. Lehmann, S. Zhao and C. K. Ahn, Comparing robustness of the Kalman, H_∞, and UFIR filters, *IEEE Transactions on Signal Processing*, vol. 66, no. 13, pp. 3447–3458, 2018.
[31] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla. M. I. Jordan and S. S. Sastry, Kalman filtering with intermittent observations, *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.
[32] A. Tsiamis, K. Gatsis and G. J. Pappas, State-secrecy codes for networked linear systems, *IEEE Transactions on Automatic Control*, vol. 65, no. 5, pp. 2001–2015, May 2020.
[33] L. Wang, X. Cao, H. Zhang, C. Sun and W. X. Zheng, Transmission scheduling for privacy-optimal encryption against eavesdropping attacks on remote state estimation, *Automatica*, vol. 137, art. no. 110145, Mar. 2022.
[34] Y. Wang, H.-J. Liu and H.-L. Tan, An overview of filtering for sampled-data systems under communication constraints, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 3, art. no. 100011, Sep. 2023.
[35] Y.-A. Wang, B. Shen, L. Zou and Q.-L. Han, A survey on recent advances in distributed filtering over sensor networks subject to communication constraints, *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, art. no. 100007, Jun. 2023.
[36] G. Wei, S. Liu, L. Wang and Y. Wang, Event-based distributed set-membership filtering for a class of time-varying non-linear systems over sensor networks with saturation effects, *International Journal of General Systems*, vol. 45, no. 5, pp. 532–547, Apr. 2016.
[37] P. Wen, X. Li, N. Hou and S. Mu, Distributed recursive fault estimation with binary encoding schemes over sensor networks, *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 417-427, 2022.
[38] Y. Xu, L. Yang, Z. Wang, H. Rao and R. Lu, State estimation for networked systems with Markov driven transmission and buffer constraint, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 12, pp. 7727-7734, Dec. 2021.
[39] C. Yang, J. Zheng, X. Ren, W. Yang, H. Shi and L. Shi, Multi-sensor Kalman filtering with intermittent measurements, *IEEE Transactions on Automatic Control*, vol. 63, no. 3, pp. 797–804, Mar. 2018.
[40] W. Yang, D. Li, H. Zhang, Y. Tang and W. X. Zheng, An encoding mechanism for secrecy of remote state estimation, *Automatica*, vol. 120, art. no. 109116, Oct. 2020.
[41] X. Yi, H. Yu, Z. Fang and L. Ma, Probability-guaranteed state estimation for nonlinear delayed systems under mixed attacks, *International Journal of Systems Science*, vol. 54, no. 9, pp. 2059–2071, Jul. 2023.
[42] Y. Yuan, X. Tang, W. Zhou, W. Pan, X. Li, H.-T. Zhang, H. Ding and J. Goncalves, Data driven discovery of cyber physical systems, *Nature Communications*, vol. 10, no. 1, pp. 1-9, 2019.
[43] T. Zhang, Q. Liu, J. Liu, Z. Wang and H. Li, Multiple-bipartite consensus for networked Lagrangian systems without using neighbours' velocity information in the directed graph, *Systems Science & Control Engineering*, vol. 11, no. 1, art. no. 2210185, 2023.
[44] Z. Zhang, P. Cheng, J. Wu and J. Chen, Secure state estimation using hybrid homomorphic encryption scheme, *IEEE Transactions on Control Systems Technology*, vol. 29, no. 4, pp. 1704–1720, Jul. 2021.
[45] B. Zhao, Y. Zhang and Z. Ding, Probabilistic transmission scheme for distributed filtering over randomly lossy sensor networks in the presence of eavesdropper, *IEEE Transactions on Control of Network Systems*, vol. 9, no. 2, pp. 800-810, Jun. 2022.
[46] Z. Zhao, Z. Wang, L. Zou, Y. Chen and W. Sheng, Zonotopic non-fragile set-membership fusion estimation for nonlinear systems under sensor resolution effects: boundedness and monotonicity, *Information Fusion*, vol. 105, art. no. 102232, May. 2024.
[47] D. Zheng, *Linear System Theory (Second Edition)*. Peking, P. R. China: Tsinghua University Press, 2002.
[48] 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 Journal of Automatica Sinica*, vol. 10, no. 4, pp. 985–996, Apr. 2023.

Lei Zou (Senior Member, IEEE) received the B.Sc. degree in automation from Beijing Institute of Petrochemical Technology, Beijing, China, in 2008, the M.Sc. degree in control science and engineering from China University of Petroleum (Beijing Campus), Beijing, China, in 2011 and the Ph.D degree in control science and engineering in 2016 from Harbin Institute of Technology, Harbin, China. From October 2013 to October 2015, he was a visiting Ph.D. student with the Department of Computer Science, Brunel University London, Uxbridge, U.K.

He is currently a Professor with the College of Information Science and Technology, Donghua University, Shanghai, China. His research interests include control and filtering of networked systems, moving-horizon estimation, state estimation subject to outliers, and secure state estimation.

Prof. Zou serves (or has served) as an Associate Editor for *Neurocomputing*, *International Journal of Systems Science*, *IEEE/CAA Journal of Automatica Sinica*, *IET Control Theory & Applications*, and *International Journal of Control, Automation and Systems*. He is a Senior Member of *IEEE* and *Chinese Association of Automation*, a Regular Reviewer of *Mathematical Reviews*, and a very active reviewer for many international journals.

Zidong Wang (Fellow, IEEE) received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, the M.Sc. degree in applied mathematics and the Ph.D. degree in electrical engineering both from Nanjing University of Science and Technology, Nanjing, China, in 1990 and 1994, respectively.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published a number of papers in international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for *International Journal of Systems Science*, the Editor-in-Chief for *Neurocomputing*, the Editor-in-Chief for *Systems Science & Control Engineering*, and an Associate Editor for 12 international journals, including IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, IEEE TRANSACTIONS ON NEURAL NETWORKS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, and IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS–PART C. He is a Member of the Academia Europaea, a Member of the European Academy of Sciences and Arts, an Academician of the International Academy for Systems and Cybernetic Sciences, a Fellow of the IEEE, a Fellow of the Royal Statistical Society, and a member of program committee for many international conferences.

Bo Shen (Senior Member, IEEE) received the B.Sc. degree in mathematics from Northwestern Polytechnical University, Xi'an, China, in 2003, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2011.

From 2009 to 2010, he was a Research Assistant with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong. From 2010 to 2011, he was a Visiting Ph.D. Student with the Department of Information Systems and Computing, Brunel University London, London, U.K. From 2011 to 2013, he was a Research Fellow (Scientific Co-Worker) with the Institute for Automatic Control and Complex Systems, University of Duisburg–Essen, Duisburg, Germany. He is currently a Professor with the College of Information Science and Technology, Donghua University. He has published around 100 articles in refereed international journals. His research interests include nonlinear control and filtering, stochastic control and filtering, as well as complex networks and neural networks.

Prof. Shen is a program committee member for many international conferences. He serves (or has served) as an Associate Editor or Editorial Board Member for eight international journals, including Systems Science and Control Engineering, Journal of The Franklin Institute, Asian Journal of Control, Circuits, Systems, and Signal Processing, Neurocomputing, Assembly Automation, Neural Processing Letters, and Mathematical Problems in Engineering.

Hongli Dong (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from the Harbin Institute of Technology, Harbin, China, in 2012.

From 2009 to 2010, she was a Research Assistant with the Department of Applied Mathematics, City University of Hong Kong, Hong Kong. From 2010 to 2011, she was a Research Assistant with the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong. From 2011 to 2012, she was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, London, U.K. From 2012 to 2014, she was an Alexander von Humboldt Research Fellow with the University of Duisburg–Essen, Duisburg, Germany. She is currently a Professor with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing, China. She is also the Director of the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Daqing, China. Her current research interests include robust control and networked control systems.

Prof. Dong is a very active reviewer for many international journals.