Encrypted Finite-Horizon Energy-to-Peak State Estimation for Time-Varying Systems Under Eavesdropping Attacks: Tackling Secrecy Capacity

Lei Zou, Zidong Wang, *Fellow, IEEE,* Bo Shen, Hongli Dong, and Guoping Lu

***Abstract*—This paper is concerned with the problem of finite-horizon energy-to-peak state estimation for a class of networked linear time-varying systems. Due to the inherent vulnerability of the network-based communication, the measurement signals transmitted over a communication network might be intercepted by potential eavesdroppers. To avoid the information leakage, by resorting to an artificial-noise-assisted method, we develop a novel encryption-decryption scheme to ensure that the transmitted signal is composed of the raw measurement and an artificial-noise term. A special evaluation index named secrecy capacity is employed to assess the information security of signal transmissions under the developed encryption-decryption scheme. The purpose of the addressed problem is to design an encryption-decryption scheme and a state estimator such that: 1) the desired secrecy capacity is ensured; and 2) the required finite-horizon l_2–l_∞ performance is achieved. Sufficient conditions are established on the existence of the encryption-decryption mechanism and the finite-horizon state estimator. Finally, simulation results are proposed to show the effectiveness of our proposed encryption-decryption-based state estimation scheme.**

***Index Terms*—Eavesdropping, encryption-decryption scheme, energy-to-peak state estimation, artificial-noise-assisted technique, finite-horizon state estimation.**

Abbreviations and Notations

ADV	Artificial disturbance vector
ANT	artificial-noise term
EDS	Encryption-decryption scheme
FHEtP	Finite-horizon energy-to-peak
$\mathbb{R}^{p\times q}$	The set of all $p\times q$ real matrices
$\mathbb{R}^p$	The p-dimensional Euclidean space
$\mathscr{P}>\mathscr{Q}$	$\mathscr{P}-\mathscr{Q}$ is positive definite
$\mathscr{P}\geq\mathscr{Q}$	$\mathscr{P}-\mathscr{Q}$ is positive semi-definite
$\mathscr{M}^T$	The transpose of $\mathscr{M}$
$\mathscr{M}^{-1}$	The inverse matrix of $\mathscr{M}$
$\lambda_{\min}\{\mathscr{A}\}$	The minimum eigenvalue of $\mathscr{A}$
$\lambda_{\max}\{\mathscr{A}\}$	The maximum eigenvalue of $\mathscr{A}$
$\mathrm{Prob}\{s\}$	The occurrence probability of the event "s"
$\mathbb{E}\{x\}$	The expectation of the stochastic variable x
$\mathrm{diag}\{\cdots\}$	The block-diagonal matrix
$\|a\|$	The Euclidean norm of the vector a
I	The identity matrix with compatible dimensions
0	The zero matrix with compatible dimensions
$\delta(a)$	The Kronecker delta function that equals 1 if $a=0$ and equals 0 otherwise
l_2([0,N]; $\mathbb{R}^q$)	The space of square-summable q-dimensional vector functions over the interval $[0,N]$

I. Introduction

As one of the fundamental research topics in the fields of signal processing and control, the state estimation problem has stirred considerable research interest from both academia and industry, and a large number of state estimation strategies have been developed for different systems and different performance specifications, see e.g. [1]–[9]. Among others, the energy-to-peak state estimation, also known as l_2-l_∞ state estimation, has shown to be an effective technique to ensure a relatively small estimation error under the effects of energy-bounded noises [10]–[12]. In the context of energy-to-peak state estimation, most existing results have been concerned with the time-invariant systems. Nevertheless, in practical applications, it is quite common that the system parameters are time-varying for a variety of reasons (e.g. the operating point shifting, temperature fluctuation, and graduate aging of system components). Accordingly, the finite-horizon energy-to-peak (FHEtP) state estimation issue for time-varying systems, aiming to achieve a desired *transient* performance over a given finite horizon, has begun to gain some initial attention [13], [14].

This work was supported in part by the National Natural Science Foundation of China under Grants 62273087, 61933007, 62273088, U21A2019 and 62073180, the Shanghai Pujiang Program of China under Grant 22PJ1400400, the Program of Shanghai Academic/Technology Research Leader of China under Grant 20XD1420100, the European Union's Horizon 2020 Research and Innovation Programme under Grant 820776 (INTEGRADDE), the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany. (*Corresponding author: Zidong Wang.*)

L. Zou and B. 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).

Z. Wang is with the College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China, and is also with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom (Email: Zidong.Wang@brunel.ac.uk).

H. Dong is with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China, the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Northeast Petroleum University, Daqing 163318, China, and the Sanya Offshore Oil & Gas Research Institute, Northeast Petroleum University, Sanya 572024, China. (Email: shiningdhl@vip.126.com)

G. Lu is with the School of Electrical Engineering, Nantong University, Nantong 226019, China. (Email: lu.gp@ntu.edu.cn)

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: DOI10.1109/JAS.2023.123393,

The past several decades have witnessed the growing popularity of networked systems as a result of their distinct advantages (e.g. easy installation and low cost) and successful applications in various fields. Nevertheless, it is worth noting that the employment of communication networks would give rise to the so-called network-induced phenomena (e.g. packet dropouts, signal quantizations, packet disorders, cyber-attacks, and fading measurements), and hence damage the reliability and integrity of the transmitted measurement signals. As such, it is imperative to consider the networked state estimation problems in the presence of various network-induced phenomena. Along this direction, a great deal of remarkable research results have been available in the literature see e.g. [15]–[21] and the references therein. For example, an unbiasedness-constrained least squares state estimator has been developed in [22] for a class of time-varying stochastic systems with missing measurements under the Round-Robin protocol.

On another research frontier, the network-associated security has been attracting a growing research interest due primarily to the ever-increasing system complexities and safety demand [23], [24]. For networked systems, the security issue mainly arises from the inherent vulnerability of the network-based communication technique, i.e., the signal transmissions over shared communication channels are prone to the cyber-attacks and information leakage. It should be pointed out that the network-associated security issue would pose additional challenges to the design of networked state estimation schemes. More specifically, when it comes to the case of cyber-attacks, the malicious attackers might launch miscellaneous attacks to interfere with the signal transmissions over communication networks, thereby giving rise to the deteriorated estimation performance or the damage of entire system. To deal with such an issue, a rich body of results has been reported in the literature, see e.g. [25]–[29] and the references therein.

Generally speaking, information leakage refers to the phenomenon that certain confidential information is revealed to the unauthorized parties, e.g. eavesdroppers. In networked state estimation problems, the potential eavesdroppers might infer the private information of the system through overhearing the transmitted signals over communication networks. There is no doubt that the phenomenon of information leakage poses serious threats to the so-called *information security* and may lead to severe losses. In this sense, it is practically meaningful to investigate the secure state estimation issue in the presence of potential eavesdroppers, and some elegant results have appeared in the literature, see e.g. [30]–[35]. For instance, a state-secrecy encoding scheme has been developed in [32] to preserve the information security of the remote state estimation procedure in the presence of an eavesdropper. In [30], an optimal encryption scheduling scheme has been designed to protect the system privacy and guarantee the estimation performance.

It is worth noting that there are mainly two mechanisms to deal with the secure state estimation issues against eavesdropping, namely, the transmission-scheduling-based mechanism [30], [36]–[38] and the encryption-decryption-based mechanism [32], [39]. For the former one, a notable result has been presented in [37], where the security issue of the networked state estimation is addressed by using a dynamic transmission scheduling policy for the sensor measurements. For the latter one, the security of signal transmissions is protected by encrypting the original plaintext into ciphertext based on the preset secret key. In general, the encryption-decryption-based mechanism can achieve a satisfactory information security when the secret key is sufficiently safe. Nevertheless, it should be pointed out that the corresponding results on the FHEtP state estimation problem against eavesdropping have been rarely reported, which motivates us to shorten such a gap.

Summarizing the discussions made so far, in this paper, we strive to challenge the FHEtP state estimation problem in the presence of eavesdroppers by using the encryption-decryption-based mechanism. Two essential challenges are identified as follows: 1) how to design the FHEtP state estimator under the effect of encryption-decryption-based mechanism? and 2) how to design the encryptor parameters and thus guarantee the desired information security? In response to these identified challenges, the primary novelties of this research are highlighted as follows: *1) the FHEtP state estimation issue is, for the first time, considered for time-varying systems in the presence of eavesdroppers; 2) an artificial-noise-assisted encryption-decryption scheme (EDS) is developed to guarantee the information security of the network-based signal transmissions; and 3) the desired time-varying estimator parameter, derived in terms of the solutions to certain recursive linear matrix inequalities, is suitable for online computations.*

The rest of this work is outlined as follows. In Section II, we first introduce the framework of the encryption-decryption-based communication mechanism, and then formulate the FHEtP state estimation problem for networked systems against eavesdropping. In Section III, an EDS is designed to preserve the information security of the transmitted data. Moreover, the desired time-varying estimator parameter is obtained by resorting to certain recursive linear matrix inequalities. A simulation example is given in Section IV to illustrate the effectiveness of the developed EDS and FHEtP state estimation algorithm. Finally, some conclusions are drawn in Section V.

II. Problem Formulation and Preliminaries

A. Plant and encryption mechanism

In this research, we focus our attention on the networked state estimation issue (as shown in Fig. 1), where the signal transmissions might be intercepted by potential eavesdroppers.

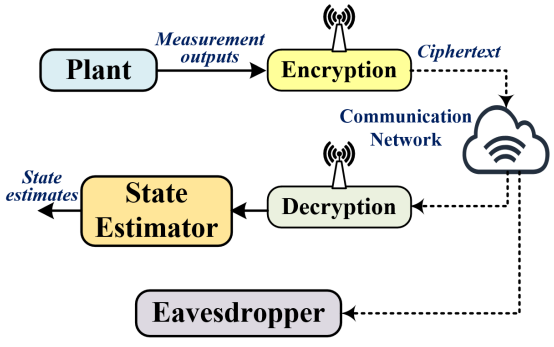

Fig. 1: Networked state estimation with an eavesdropper.

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: DOI10.1109/JAS.2023.123393,

The plant under consideration is modeled by the following linear time-varying system with time delay defined on the finite horizon $[0, N]$:

$$\begin{cases} x_{k+1} = A_k x_k + E_k x_{k-\tau} + B_k \omega_k \\ y_k = C_k x_k + D_k \nu_k \\ z_k = M_k x_k \\ x_i = \psi_{-i}, \quad i = -\tau, -\tau+1, \cdots, 0 \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^n$, $y_k \in \mathbb{R}^m$ and $z_k \in \mathbb{R}^p$ stand for, respectively, the system state vector, the measurement output and the signal to be estimated. $\omega_k \in l_2([0, N]; \mathbb{R}^q)$ and $\nu_k \in l_2([0, N]; \mathbb{R}^r)$ represent, respectively, the process noise and measurement noise. τ is a known constant positive scalar. A_k, B_k, C_k, D_k, E_k and M_k are known time-varying matrices with appropriate dimensions.

In traditional scenarios, the state estimates are generated based on the received measurements that are directly transmitted over the communication network. Nevertheless, owing primarily to the inherent vulnerability of the network-based communication, the transmitted measurement signals might be intercepted by the potential eavesdroppers [37], [39]. To protect the information security, as shown in Fig. 1, an encryption-decryption-based communication scheme is employed to preserve the privacy of the measurement data during the signal transmission process.

Specifically, the encryption-decryption-based communication scheme can be divided into the following three steps. First, an encryptor is utilized to transform the original measurement data (i.e., the original plaintext) into the encrypted data (i.e., the ciphertext). Then, the encrypted data is transmitted over the communication network. Finally, a decryptor is employed at the state estimator side to re-transform the received encrypted data into the decrypted one (which might be slightly different from the original measurement data). Under such a scheme, the information security is protected in the sense that the potential eavesdropper is unable to acquire the accurate state information based on the transmitted ciphertext.

To begin with, let us introduce the following encryption scheme by utilizing a special noise injection mechanism.

Encryption scheme: For any $k \geq 0$, the ciphertext $\bar{y}_k$ is generated by

$$\bar{y}_k = \mathcal{E}(y_k) \triangleq y_k + S\Phi(\xi_k)\eta_k \tag{2}$$

where $S \in \mathbb{R}^{m\times m}$ is an orthogonal matrix and referred to as the secret key. $\Phi(\xi_k) \triangleq \mathrm{diag}\{\delta(1-\xi_k), \delta(2-\xi_k), \cdots, \delta(m-\xi_k)\}$ denotes a parameter-dependent matrix in which $\xi_k \in \{1, 2, \cdots, m\}$ is an artificial random scalar. Note that $\{\xi_k\}_{k\geq 0}$ is a sequence of independent and identically distributed (i.i.d.) random variables with the occurrence probabilities $\mathrm{Prob}\{\xi_k = i\} = p_i$ ($i = 1, 2, \cdots, m$). $\eta_k \in \mathbb{R}^m$ is an artificial disturbance vector (ADV) to be designed. In this research, the secret key S is known to the remote state estimator but unknown to the eavesdropper.

Actually, the encryption mechanism (2) is a *stochastic mapping*, where a special artificial-noise term (ANT) $S\Phi(\xi_k)\eta_k$ is introduced to protect the information security. It should be pointed out that the artificial-noise-assisted scheme has shown to be an effective method to enhance the information security against eavesdropping [40]–[42]. For the encryption mechanism (2), the *unpredictability* of the artificial random variable ξ_k and the ADV η_k can greatly reduce the risk of information leakage.

Rewriting the secrete key as $S \triangleq \begin{bmatrix} s_1 & s_2 & \cdots & s_m \end{bmatrix}$, the ANT can be reformulated as $S\Phi(\xi_k)\eta_k = \eta_{\xi_k,k} s_{\xi_k}$, where $\eta_{\xi_k,k}$ represents the ξ_k-th element of the vector η_k. It is obvious that the artificial random variable ξ_k denotes the direction vector from the secret key S, and the ADV η_k determines the encryption strength of the encryption mechanism. As such, the scalar $\eta_{\xi_k,k}$ with a relatively large value will give rise to a significant difference between the original measurement data y_k and the encrypted data $\bar{y}_k$, thereby misleading the potential eavesdropper in an effective way.

B. Decryption mechanism and state estimator

In this subsection, we shall introduce the following decryption mechanism to "remove" the effects of the ANT.

Decryption scheme: Based on the received ciphertext $\bar{y}_k$ ($k \geq 0$) and the secret key S, the decrypted measurement data (i.e., $\vec{y}_k$) is generated through the following calculations:

$$\begin{cases} \vec{\xi}_k = \arg\min\limits_i \mathcal{F}_k(\Phi(i)) \\ \vec{y}_k = S(I - \Phi(\vec{\xi}_k))S^T \bar{y}_k \end{cases} \tag{3}$$

where $\vec{\xi}_k$ stands for the estimate of ξ_k, $\vec{y}_k$ denotes the decrypted measurement data, and $\mathcal{F}_k(\Phi(i))$ is the decryption function to be designed.

According to the encryption-decryption mechanism introduced in (2) and (3), we are now in a position to deal with the issue of information security. To this end, by resorting to the instantaneous received signal-to-noise ratios (SNRs) [43], the so-called *secrecy capacity* is mathematically defined as follows [44]:

$$\mathcal{C}_k = \begin{cases} \log_2(1+\vec{\mu}_k) - \log_2(1+\bar{\mu}_k), & \text{if } \vec{\mu}_k > \bar{\mu}_k \\ 0, & \text{if } \vec{\mu}_k \leq \bar{\mu}_k \end{cases}$$

where $\vec{\mu}_k$ and $\bar{\mu}_k$ are, respectively, the instantaneous received SNRs at the legitimate receiver (i.e., the state estimator) and the eavesdropper. As discussed in [43], a sufficiently large secrecy capacity can guarantee the security of the network-based communication.

The SNR is defined as the ratio between the power of the signal and the power of noise. In this paper, it is assumed that there is no channel noise in the process of signal transmission. Letting $\varepsilon_k \triangleq y_k - \vec{y}_k$ be the encryption-decryption error, the values of $\vec{\mu}_k$ and $\bar{\mu}_k$ can be calculated as follows:

$$\begin{cases} \vec{\mu}_k \triangleq \dfrac{\|y_k\|^2}{\|y_k - \vec{y}_k\|^2} = \dfrac{\|y_k\|^2}{\|\varepsilon_k\|^2}, \\ \bar{\mu}_k \triangleq \dfrac{\|y_k\|^2}{\|y_k - \bar{y}_k\|^2} = \dfrac{\|y_k\|^2}{\|S\Phi(\xi_k)\eta_k\|^2}. \end{cases}$$

As discussed in [39], the SNR is an important index to reflect the signal transmission performance. A lower SNR for the eavesdropper would effectively prevent the eavesdropper from obtaining real observations through the network-based

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: DOI10.1109/JAS.2023.123393,

communication. A sufficiently large secrecy capacity means that the SNR for the state estimator is much higher than the SNR for the eavesdropper. In this paper, the secrecy capacity is adopted to evaluate the information security in the signal transmission process.

Remark 1: It can be observed from (3) that the constructed EDS would result in certain encryption-decryption errors (i.e., ε_k) on the measurement data, thereby degrading the estimation performance. In this sense, the enhancement of information security against eavesdropping is at the expense of a slight performance degradation in terms of state estimation.

In this paper, based on the values of $\vec{\xi}_k$ and $\vec{y}_k$, the proposed time-varying state estimator is of the following structure:

$$\begin{cases} \hat{x}_{k+1} = A_k\hat{x}_k + E_k\hat{x}_{k-\tau} + L_k(\vec{\xi}_k)\big(\vec{y}_k - \vec{\Phi}(\vec{\xi}_k)C_k\hat{x}_k\big) \\ \hat{z}_k = M_k\hat{x}_k \\ \hat{x}_i = 0, \quad i = -\tau, -\tau+1, \cdots, 0 \end{cases} \tag{4}$$

where $\vec{\Phi}(\vec{\xi}_k) \triangleq S(I - \Phi(\vec{\xi}_k))S^T$, $\hat{z}_k$ and $\hat{x}_k$ represent, respectively, the estimates of z_k and x_k. $L_k(\vec{\xi}_k)$ is a parameter-dependent time-varying estimator parameter to be designed.

We are now ready to introduce the main purposes of this research:

1) Design the ADV η_k and the decryption function $\mathcal{F}_k(\cdot)$ such that the secrecy capacity is greater than a given threshold α (i.e., $\mathcal{C}_k > \alpha$) for all $k \geq 0$.
2) Design the time-varying estimator parameter L_k such that the following finite-horizon l_2-l_∞ estimation performance requirement

$$\begin{aligned} &\sup_{k\in[0,N]} \mathbb{E}\{\|z_k - \hat{z}_k\|^2\} \\ &\leq \gamma^2\bigg(\sum_{k=0}^{N}\big(\|\omega_k\|^2 + \|\nu_k\|^2\big) \\ &\quad + \sum_{i=-\tau}^{0}(x_i - \hat{x}_i)^T Q_{-i}(x_i - \hat{x}_i)\bigg) \end{aligned} \tag{5}$$

holds for all nonzero noises $\nu_k$and ω_k, where $\gamma > 0$ denotes the energy-to-peak performance index (or the prescribed l_2-l_∞ disturbance attenuation level), Q_{-i} ($i = -\tau, -\tau+1, \cdots, 0$) are the given weighting matrices satisfying $Q_i > 0$.

III. Main Results

A. Design of the decryption function

In this paper, the required finite-horizon l_2-l_∞ performance is independent from the ANT $S\Phi(\xi_k)\eta_k$. In this regard, we shall design the decryption function $\mathcal{F}_k(\cdot)$ such that $\vec{\xi}_k = \xi_k$ and remove the effects of the ANT $S\Phi(\xi_k)\eta_k$ in the estimation process.

Before introducing the design of $\mathcal{F}_k(\cdot)$, we first consider the input-output model for the plant (1) and the ciphertext $\bar{y}_k$. Letting $\bar{x}_k \triangleq \begin{bmatrix} x_k^T & x_{k-1}^T & \cdots & x_{k-\tau}^T \end{bmatrix}^T$, the plant (1) and the ciphertext $\bar{y}_k$ can be rewritten as follows:

$$\begin{cases} \bar{x}_{k+1} = \bar{A}_k\bar{x}_k + \bar{B}_k\omega_k \\ \bar{y}_k = \bar{C}_k\bar{x}_k + D_k\nu_k + S\Phi(\xi_k)\eta_k \end{cases} \tag{6}$$

where $\bar{C}_k \triangleq \begin{bmatrix} C_k & 0 & 0 & \cdots & 0 \end{bmatrix}$ and

$$\bar{A}_k \triangleq \begin{bmatrix} A_k & 0 & \cdots & 0 & E_k \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I & 0 \end{bmatrix}, \bar{B}_k \triangleq \begin{bmatrix} B_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \bar{x}_0 \triangleq \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_\tau \end{bmatrix}.$$

Now, let us recall the definition of uniform observability and introduce some necessary assumptions which will be utilized in the derivation of main results.

Definition 1: [45] Let the time-varying matrices $\bar{C}_k$ and $\bar{A}_k$ be given. The matrix pair $(\bar{A}_k, \bar{C}_k)$ is said to be uniformly observable if there exist two positive scalars $\underline{\aleph}$, $\bar{\aleph}$ and an integer $\bar{N} > 0$ such that the following condition is satisfied for any $0 \leq k \leq N - \bar{N}$:

$$\underline{\aleph} I \leq \mathcal{M}_{k+\bar{N},k} \leq \bar{\aleph} I$$

where

$$\begin{aligned} \mathcal{M}_{k+\bar{N},k} &\triangleq \sum_{i=k}^{k+\bar{N}} \Psi_{i,k}^T \bar{C}_i^T \bar{C}_i \Psi_{i,k}, \\ \Psi_{i,k} &\triangleq \begin{cases} \bar{A}_{i-1}\bar{A}_{i-2}\cdots\bar{A}_k, & \text{if } i > k \\ I, & \text{if } i = k \end{cases}. \end{aligned}$$

Assumption 1: The matrix pair $(\bar{A}_k, \bar{C}_k)$ is uniformly observable with the known positive scalars $\underline{\aleph}$, $\bar{\aleph}$ and integer $\bar{N}$.

Assumption 2: Consider the time-varying matrices $\bar{C}_k^{[i]} \triangleq \bar{\Phi}(i)\bar{C}_k$ in which $\bar{\Phi}(i) \triangleq (I - \Phi(i))S^T$. The following inequalities hold for all $0 \leq k \leq N - \bar{N}$:

$$\big(\bar{C}_k^{[i]}\big)^T \bar{C}_k^{[i]} \geq \varpi \bar{C}_k^T \bar{C}_k, \quad i = 0, 1, \cdots, m$$

where ϖ is a known positive constant.

Assumption 3: The values of the initial system state $\bar{x}_0$ and the energy-bounded disturbances (e.g. ν_k and ω_k) satisfy the following conditions:

$$\|\bar{x}_0\| \leq \chi, \quad \|\omega_k\| \leq \bar{\omega}, \quad \|\nu_k\| \leq \bar{\nu},$$

where χ, $\bar{\nu}$ and $\bar{\omega}$ are known positive constants.

Based on Assumptions 1-2, the input-output model for the plant (1) and the ciphertext $\bar{y}_k$ is constructed in the following proposition.

Proposition 1: Consider the time-varying system (6). Under Assumptions 1-2, for any $i \in \{0, 1, \cdots, m\}$, the encrypted measurement sequence $\{\bar{y}_k\}_{k\geq 0}$ satisfies the following condition

$$\begin{cases} \mathcal{J}_{k+1}(\Phi(i)) = \mathcal{L}_{k+1}(\Phi(i)), & \text{if } k \geq \bar{N} \\ \bar{\Phi}(i)\bar{y}_{k+1} = \bar{\Phi}(i)\bar{h}_{k+1}, & \text{if } k < \bar{N} \end{cases} \tag{7}$$

where

$$F_k \triangleq \begin{bmatrix} \bar{C}_{k-\bar{N}}^{[\xi_{k-\bar{N}}]} \\ \bar{C}_{k-\bar{N}+1}^{[\xi_{k-\bar{N}+1}]}\Psi_{k-\bar{N}+1,k-\bar{N}} \\ \vdots \\ \bar{C}_k^{[\xi_k]}\Psi_{k,k-\bar{N}} \end{bmatrix}, \quad o_k \triangleq S\Phi(\xi_k)\eta_k,$$

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: DOI10.1109/JAS.2023.123393,

$$\mathcal{J}_{k+1}(\Phi(i)) \triangleq \bar{\Phi}(i)\bar{y}_{k+1} - \sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\bar{y}_{k-\bar{N}+j},$$

$$\mathcal{L}_{k+1}(\Phi(i)) \triangleq \bar{\Phi}(i)\hbar_{k+1} - \sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\hbar_{k-\bar{N}+j},$$

$$\hbar_i \triangleq \vec{\omega}_i + D_i\nu_i + o_i, \quad \vec{\omega}_i \triangleq \bar{C}_i \sum_{s=k-\bar{N}}^{i-1} \Psi_{i-1,s}\bar{B}_s\omega_s,$$

$$\bar{\hbar}_j \triangleq \bar{C}_j\Psi_{j,0}\bar{x}_0 + \bar{C}_j\sum_{i=0}^{j-1}\Psi_{j-1,i}\bar{B}_i\omega_i + D_j\nu_j + o_j,$$

$$H_{j,k+1}^{[i]} \triangleq \bar{C}_{k+1}^{[i]}\Psi_{k+1,k-\bar{N}}\big(F_k^TF_k\big)^{-1} \times \big(\bar{C}_{k-\bar{N}+j}^{[\xi_{k-\bar{N}+j}]}\Psi_{k-\bar{N}+j,k-\bar{N}}\big)^T, \quad (j=0,1,\cdots,\bar{N})$$

with $\sum_{s=k-\bar{N}}^{k-\bar{N}-1}(\,\cdot\,) = 0$.

Proof: We first consider the case $k \geq \bar{N}$. According to Assumptions 1-2, it is clear that

$$\begin{aligned} F_k^TF_k &= \sum_{i=k-\bar{N}}^{k}\Psi_{i,k-\bar{N}}^T\big(\bar{C}_i^{[\xi_i]}\big)^T\bar{C}_i^{[\xi_i]}\Psi_{i,k-\bar{N}} \\ &\geq \varpi\sum_{i=k-\bar{N}}^{k}\Psi_{i,k-\bar{N}}^T\bar{C}_i^T\bar{C}_i\Psi_{i,k-\bar{N}} \geq \varpi\underline{\aleph}I, \end{aligned}$$

which means that the time-varying matrix $F_k^TF_k$ is invertible.

Define the following time-varying matrices $H_{k+1}^{[i]}$ $(i = 1,2,\cdots,m)$:

$$\begin{aligned} H_{k+1}^{[i]} &\triangleq \begin{bmatrix} H_{0,k+1}^{[i]} & H_{1,k+1}^{[i]} & \cdots & H_{\bar{N},k+1}^{[i]} \end{bmatrix} \\ &= \bar{C}_{k+1}^{[i]}\Psi_{k+1,k-\bar{N}}\big(F_k^TF_k\big)^{-1}F_k^T. \end{aligned}$$

Then, it follows from the definition of $H_{k+1}^{[i]}$ that

$$H_{k+1}^{[i]}F_k = \bar{C}_{k+1}^{[i]}\Psi_{k+1,k-\bar{N}},$$

which means that

$$\sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{C}_{k-\bar{N}+j}^{[\xi_{k-\bar{N}+j}]}\Psi_{k-\bar{N}+j,k-\bar{N}} = \bar{C}_{k+1}^{[i]}\Psi_{k+1,k-\bar{N}}. \quad (8)$$

Post-multiplying (8) by $\bar{x}_{k-\bar{N}}$, we have

$$\begin{aligned} &\sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{C}_{k-\bar{N}+j}^{[\xi_{k-\bar{N}+j}]}\Psi_{k-\bar{N}+j,k-\bar{N}}\bar{x}_{k-\bar{N}} \\ &= \sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\bar{C}_{k-\bar{N}+j}\Psi_{k-\bar{N}+j,k-\bar{N}}\bar{x}_{k-\bar{N}} \\ &= \bar{\Phi}(i)\bar{C}_{k+1}\Psi_{k+1,k-\bar{N}}\bar{x}_{k-\bar{N}}. \end{aligned} \quad (9)$$

Note that

$$\begin{aligned} &\bar{y}_{k-\bar{N}+j} - D_{k-\bar{N}+j}\nu_{k-\bar{N}+j} - o_{k-\bar{N}+j} \\ &= \bar{C}_{k-\bar{N}+j}\bar{x}_{k-\bar{N}+j} \\ &= \bar{C}_{k-\bar{N}+j}\Bigg(\Psi_{k-\bar{N}+j,k-\bar{N}}\bar{x}_{k-\bar{N}} \\ &\quad + \sum_{s=k-\bar{N}}^{k-\bar{N}+j-1}\Psi_{k-\bar{N}+j-1,s}\bar{B}_s\omega_s\Bigg) \\ &= \bar{C}_{k-\bar{N}+j}\Psi_{k-\bar{N}+j,k-\bar{N}}\bar{x}_{k-\bar{N}} + \vec{\omega}_{k-\bar{N}+j}, \end{aligned}$$

from which we have

$$\begin{aligned} &\sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\bar{C}_{k-\bar{N}+j}\Psi_{k-\bar{N}+j,k-\bar{N}}\bar{x}_{k-\bar{N}} \\ &= \sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\Big(\bar{y}_{k-\bar{N}+j} - D_{k-\bar{N}+j}\nu_{k-\bar{N}+j} \\ &\quad - o_{k-\bar{N}+j} - \vec{\omega}_{k-\bar{N}+j}\Big), \end{aligned} \quad (10)$$

and

$$\begin{aligned} &\bar{\Phi}(i)\bar{C}_{k+1}\Psi_{k+1,k-\bar{N}}\bar{x}_{k-\bar{N}} \\ &= \bar{\Phi}(i)\big(\bar{y}_{k+1} - D_{k+1}\nu_{k+1} - o_{k+1} - \vec{\omega}_{k+1}\big). \end{aligned} \quad (11)$$

Then, it follows from (9)-(11) that

$$\begin{aligned} &\bar{\Phi}(i)\big(\bar{y}_{k+1} - D_{k+1}\nu_{k+1} - o_{k+1} - \vec{\omega}_{k+1}\big) \\ &= \sum_{j=0}^{\bar{N}} H_{j,k+1}^{[i]}\bar{\Phi}(\xi_{k-\bar{N}+j})\Big(\bar{y}_{k-\bar{N}+j} - D_{k-\bar{N}+j}\nu_{k-\bar{N}+j} \\ &\quad - o_{k-\bar{N}+j} - \vec{\omega}_{k-\bar{N}+j}\Big). \end{aligned} \quad (12)$$

According to the definitions of $\mathcal{J}_{k+1}(\cdot)$, $\mathcal{L}_{k+1}(\cdot)$ and $\hbar_i$, it follows from (12) that the following equality holds for all $i = 1,2,\cdots,m$:

$$\mathcal{J}_{k+1}(\Phi(i)) = \mathcal{L}_{k+1}(\Phi(i)). \quad (13)$$

Next, let us move on to consider the case $-1 \leq k < \bar{N}$. Obviously, it follows directly from (6) that

$$\bar{x}_{k+1} = \Psi_{k+1,0}\bar{x}_0 + \sum_{s=0}^{k}\Psi_{k,s}\bar{B}_s\omega_s,$$

which implies that

$$\begin{aligned} \bar{\Phi}(i)\bar{y}_{k+1} &= \bar{\Phi}(i)\bar{C}_{k+1}\Psi_{k+1,0}\bar{x}_0 + \bar{\Phi}(i)\bar{C}_{k+1}\sum_{s=0}^{k}\Psi_{k,s}\bar{B}_s\omega_s \\ &\quad + \bar{\Phi}(i)D_{k+1}\nu_{k+1} + \bar{\Phi}(i)o_{k+1} \\ &= \bar{\Phi}(i)\bar{\hbar}_{k+1}. \end{aligned} \quad (14)$$

The proof is now complete. ■

Remark 2: It should be noted that the condition (7) is an input-output model reflecting the relationship between the ciphertext $\bar{y}_k$ and the external inputs (i.e., the process noise ω_k, the measurement noise ν_k and the ADV η_k). Accordingly, the sequences $\{\bar{y}_k\}_{k\geq 0}$ can be utilized to evaluate the effects induced by the external inputs, thereby contributing to the identification of ξ_k.

In what follows, we are going to design the decryption function $\mathcal{F}_k(\Phi(i))$ such that the equality $\vec{\xi}_k = \xi_k$ holds for all $k \geq 0$.

Theorem 1: Under Assumptions 1-3, design the decryption function $\mathcal{F}_k(\Phi(i))$ as follows:

$$\mathcal{F}_k(\Phi(i)) \triangleq \begin{cases} \|\bar{\mathcal{J}}_k(\Phi(i))\|, & \text{if } k \geq \bar{N}+1 \\ \|\bar{\Phi}(i)\bar{y}_k\|, & \text{if } k < \bar{N}+1 \end{cases} \quad (15)$$

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: DOI10.1109/JAS.2023.123393,

where

$$\bar{\mathcal{J}}_k(\Phi(i)) \triangleq \bar{\Phi}(i)\bar{y}_k - \sum_{j=0}^{\bar{N}} H_{j,k}^{[i]}\bar{\Phi}(\vec{\xi}_{k-\bar{N}+j-1})\bar{y}_{k-\bar{N}+j-1}.$$

Then, the condition $\vec{\xi}_k = \xi_k$ holds for all $k \geq 0$ if $|\eta_{i,k}| > \max\{\bar{\eta}, \hat{\eta}\}$, $\forall i \in \{1, 2, \cdots, m\}$, where

$$\bar{\eta} \triangleq 2\left(\zeta_{\bar{N}+1} + \sum_{j=0}^{\bar{N}} \frac{\bar{c}^2\bar{a}^{\bar{N}+j+1}}{\varpi\underline{\aleph}}\zeta_j\right),\ \bar{a} \triangleq \max_{0\leq k\leq N}\{\|\bar{A}_k\|\},$$

$$\hat{\eta} \triangleq \begin{cases} 2\big(\bar{c}\chi + \zeta_{\bar{N}}\big), & \text{if } \bar{a} \leq 1 \\ 2\big(\bar{c}\bar{a}^{\bar{N}}\chi + \zeta_{\bar{N}}\big), & \text{if } \bar{a} > 1 \end{cases},\ \bar{b} \triangleq \max_{0\leq k\leq N}\{\|\bar{B}_k\|\},$$

$$\bar{c} \triangleq \max_{0\leq k\leq N}\{\|\bar{C}_k\|\},\ \ \bar{d} \triangleq \max_{0\leq k\leq N}\{\|D_k\|\},$$

$$\zeta_j \triangleq \bar{c}\sum_{s=0}^{j-1}\bar{a}^s\bar{b}\bar{\omega} + \bar{d}\bar{\nu}, \quad (j = 0, 1, \cdots, \bar{N}+1).$$

Proof: To begin with, let us consider the norms of $\mathcal{L}_{k+1}(\Phi(i))$ and $\bar{\Phi}(i)\bar{h}_{k+1}$.

Case 1: $i = \xi_{k+1}$. In this case, we have $\bar{\Phi}(i)o_{k+1} = 0$.

According to the definitions of $\bar{a}$, $\bar{b}$ and $\bar{c}$, we are easy to verify that, for any $k \geq \bar{N}$, the condition $F_k^T F_k \geq \varpi\mathcal{M}_{k,k-\bar{N}} \geq \varpi\underline{\aleph}I$ holds, which implies that

$$\|H_{j,k+1}^{[i]}\| \leq \frac{\bar{c}^2\bar{a}^{\bar{N}+j+1}}{\varpi\underline{\aleph}} \tag{16}$$

holds for any $i \in \{1, 2, \cdots, m\}$. Furthermore, it can be obtained from the definition of $\vec{\omega}_i$ that

$$\|\vec{\omega}_{k-\bar{N}+j}\| \leq \bar{c}\sum_{s=0}^{j-1}\bar{a}^s\bar{b}\bar{\omega}. \tag{17}$$

Accordingly, noting that $\|\bar{\Phi}(i)\| \leq 1$, it follows from (16)-(17) that the following condition

$$\begin{aligned}
&\big\|\mathcal{L}_{k+1}(\Phi(i))\big\| \\
&\leq \|\vec{\omega}_i\| + \|D_i\nu_i\| + \sum_{j=0}^{\bar{N}}\|H_{j,k+1}^{[i]}\|\big(\|\vec{\omega}_{k-\bar{N}+j}\| \\
&\quad + \|D_{k-\bar{N}+j}\nu_{k-\bar{N}+j}\|\big) \\
&\leq \bar{c}\sum_{s=0}^{\bar{N}}\bar{a}^s\bar{b}\bar{\omega} + \bar{d}\bar{\nu} + \sum_{j=0}^{\bar{N}}\frac{\bar{c}^2\bar{a}^{\bar{N}+j+1}}{\varpi\underline{\aleph}}\left(\bar{c}\sum_{s=0}^{j-1}\bar{a}^s\bar{b}\bar{\omega} + \bar{d}\bar{\nu}\right) \\
&= \zeta_{\bar{N}+1} + \sum_{j=0}^{\bar{N}}\frac{\bar{c}^2\bar{a}^{\bar{N}+j+1}}{\varpi\underline{\aleph}}\zeta_j = 0.5\bar{\eta}
\end{aligned} \tag{18}$$

holds if $\bar{\Phi}(\xi_{k-\bar{N}+j})o_{k-\bar{N}+j} = 0$ $(j = 0, 1, \cdots, \bar{N})$.

On the other hand, for any $k < \bar{N}$, it is obvious that

$$\|\bar{\Phi}(i)\bar{h}_{k+1}\| \leq \|\bar{h}_{k+1}\| \leq \bar{c}\bar{a}^{k+1}\chi + \zeta_{k+1} \leq 0.5\hat{\eta}. \tag{19}$$

Case 2: $i \neq \xi_{k+1}$. In this case, we have $\bar{\Phi}(i)o_{k+1} \neq 0$.

Noting that

$$\bar{\Phi}(i)o_{k+1} = (I - \Phi(i))\Phi(\xi_{k+1})\eta_{k+1} = \Phi(\xi_{k+1})\eta_{k+1},$$

we have

$$\begin{aligned}
&\big\|\mathcal{L}_{k+1}(\Phi(i))\big\| \\
&\geq \|\Phi(\xi_{k+1})\eta_{k+1}\| - \Bigg(\|\vec{\omega}_i\| + \sum_{j=0}^{\bar{N}}\|H_{j,k+1}^{[i]}\|\big(\|\vec{\omega}_{k-\bar{N}+j}\| \\
&\quad + \|D_{k-\bar{N}+j}\nu_{k-\bar{N}+j}\|\big) + \|D_i\nu_i\|\Bigg) \\
&> \max\{\bar{\eta}, \hat{\eta}\} - 0.5\bar{\eta} \geq 0.5\bar{\eta}, \quad k \geq \bar{N}
\end{aligned} \tag{20}$$

and

$$\|\bar{\Phi}(i)\bar{h}_{k+1}\| > 0.5\hat{\eta}, \quad k < \bar{N}. \tag{21}$$

In what follows, by resorting to the *mathematical induction*, we will prove the assertion that $\vec{\xi}_k = \xi_k$ holds for all $0 \leq k \leq N$.

Initial step. For $0 \leq k \leq \bar{N}$, it is immediately concluded from (15), (19) and (21) that

$$\begin{cases} \mathcal{F}_k(\Phi(i)) = \|\bar{\Phi}(i)\bar{y}_k\| = \|\bar{\Phi}(i)\bar{h}_k\| > 0.5\hat{\eta}, & \text{if } i \neq \xi_k \\ \mathcal{F}_k(\Phi(i)) = \|\bar{\Phi}(i)\bar{y}_k\| = \|\bar{\Phi}(i)\bar{h}_k\| \leq 0.5\hat{\eta}, & \text{if } i = \xi_k \end{cases},$$

which implies that

$$\vec{\xi}_k = \arg\min_i \mathcal{F}_k(\Phi(i)) = \xi_k. \tag{22}$$

Inductive step. Note that the assertion $\vec{\xi}_k = \xi_k$ holds for all $0 \leq k \leq \bar{N}$. Then, assuming that $\vec{\xi}_k = \xi_k$ holds for all $k \leq \kappa$ where $\kappa > \bar{N}$, we are going to show that $\vec{\xi}_{\kappa+1} = \xi_{\kappa+1}$.

From the definition of $\mathcal{F}_k(\Phi(i))$, it is obvious that

$$\begin{aligned}
\mathcal{F}_{\kappa+1}(\Phi(i)) &= \|\bar{\mathcal{J}}_{\kappa+1}(\Phi(i))\| = \|\mathcal{J}_{\kappa+1}(\Phi(i))\| \\
&= \|\mathcal{L}_{\kappa+1}(\Phi(i))\|.
\end{aligned}$$

Then, it follows from (18) and (20) that

$$\begin{cases} \mathcal{F}_{\kappa+1}(\Phi(i)) = \|\mathcal{L}_{\kappa+1}(\Phi(i))\| > 0.5\bar{\eta}, & \text{if } i \neq \xi_{\kappa+1} \\ \mathcal{F}_{\kappa+1}(\Phi(i)) = \|\mathcal{L}_{\kappa+1}(\Phi(i))\| \leq 0.5\bar{\eta}, & \text{if } i = \xi_{\kappa+1} \end{cases}, \tag{23}$$

which means that

$$\vec{\xi}_{\kappa+1} = \arg\min_i \mathcal{F}_{\kappa+1}(\Phi(i)) = \xi_{\kappa+1}. \tag{24}$$

We can now conclude that $\vec{\xi}_k = \xi_k$ holds for all $0 \leq k \leq N$, which completes the proof. ■

Remark 3: Up to now, we have designed the decryption function $\mathcal{F}_k(\cdot)$ and analyzed the value of $\vec{\xi}_k$ in Theorem 1. It can be observed that the scalars $\eta_{i,k}$ $(i = 1, 2, \cdots, m)$ with large values will contribute to the correct identification of ξ_k, i.e., $\vec{\xi}_k = \xi_k$.

B. Design of the ADV η_k

In this subsection, we will design the ADV η_k based on the condition established in Theorem 1 (i.e., $|\eta_{i,k}| > \max\{\bar{\eta}, \hat{\eta}\}$) and the requirement on the secrecy capacity (i.e., $\mathcal{C}_k > \alpha$). The design of sequence $\{\eta_k\}_{k\geq 0}$ is detailed through the following theorem.

Theorem 2: Given the threshold $\alpha < 1$ for the secrecy capacity, design the ADV η_k as follows:

$$\eta_k = \max\{\max\{\bar{\eta}, \hat{\eta}\}, \rho_k\}\mathbf{1}_m + \epsilon_k \tag{25}$$

where

$$\rho_k \triangleq \frac{\|y_k\|}{\sqrt{2^{1-\alpha} - 1}}, \quad \epsilon_k \triangleq \begin{bmatrix}\epsilon_{1,k} & \epsilon_{2,k} & \cdots & \epsilon_{m,k}\end{bmatrix}^T,$$

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: DOI10.1109/JAS.2023.123393,

and $\epsilon_{i,k}$ ($i = 1, 2, \cdots, m$) are arbitrary positive numbers. Then, the conditions $\vec{\xi}_k = \xi_k$ and $\mathcal{C}_k > \alpha$ hold for all $k \geq 0$.

Proof: First, it follows from Theorem 1 and (25) that $|\eta_{i,k}| > \max\{\bar{\eta}, \hat{\eta}\}$, which implies that $\vec{\xi}_k = \xi_k$ holds for all $k \geq 0$.

Considering the decrypted measurement data $\vec{y}_k$, one has

$$\begin{aligned}\vec{y}_k &= S(I - \Phi(\vec{\xi}_k))S^T\bar{y}_k \\ &= S(I - \Phi(\vec{\xi}_k))S^T\big(y_k + S\Phi(\xi_k)\eta_k\big) \\ &= y_k - S\Phi(\vec{\xi}_k)S^T y_k + S(I - \Phi(\vec{\xi}_k))\Phi(\xi_k)\eta_k,\end{aligned}$$

from which we conclude that

$$\vec{y}_k = y_k - S\Phi(\vec{\xi}_k)S^T y_k \tag{26}$$

holds if $\vec{\xi}_k = \xi_k$. Moreover, the decrypted measurement data is independent from the ADV η_k if $\vec{\xi}_k = \xi_k$.

From (25) and Theorem 1, we have obtained that $\vec{\xi}_k = \xi_k$. Then, it follows from (26) that

$$\varepsilon_k = y_k - \vec{y}_k = S\Phi(\vec{\xi}_k)S^T y_k,$$

which implies that

$$\begin{aligned}\vec{\mu}_k &= \frac{\|y_k\|^2}{\|\varepsilon_k\|^2} = \frac{\|y_k\|^2}{\|S\Phi(\vec{\xi}_k)S^T y_k\|^2} \\ &\geq \frac{\|y_k\|^2}{\|S\Phi(\vec{\xi}_k)S^T\|^2\|y_k\|^2} = \frac{1}{\|S\Phi(\vec{\xi}_k)S^T\|^2} \\ &= \frac{1}{\lambda_{\max}\{S\Phi(\vec{\xi}_k)S^T\}} \geq 1.\end{aligned} \tag{27}$$

On the other hand, the value of $\bar{\mu}_k$ is calculated by

$$\bar{\mu}_k = \frac{\|y_k\|^2}{\|S\Phi(\xi_k)\eta_k\|^2} = \frac{\|y_k\|^2}{\eta^2_{\xi_k,k}\|s_{\xi_k}\|^2}. \tag{28}$$

Noting that $S^T S = I = \big[s_i^T s_j\big]_{m\times m}$, it is easy to find that $\|s_i\|^2 = 1$ holds for all $i = 1, 2, \cdots, m$. Hence, it follows from (25) and (28) that

$$\bar{\mu}_k = \frac{\|y_k\|^2}{\eta^2_{\xi_k,k}} < \frac{\|y_k\|^2}{\rho_k^2} = 2^{1-\alpha} - 1. \tag{29}$$

In light of the definition about the secrecy capacity, we derive that

$$\mathcal{C}_k = \log_2(1 + \vec{\mu}_k) - \log_2(1 + \bar{\mu}_k) > 1 - \log_2(2^{1-\alpha}) = \alpha. \tag{30}$$

The proof is now complete. ■

Remark 4: From the design process of the ADV η_k in Theorem 2, it is not difficult to see that a vector ϵ_k with relatively large norm leads to the improvement of the secrecy capacity. Nevertheless, such a "big" vector would amplify the value of the ciphertext $\bar{y}_k$, thereby increasing the communication burden. As such, in practical applications, the proper upper bounds on the positive numbers $\epsilon_{i,k}$ should be selected to achieve a tradeoff between the secrecy capacity and communication burden.

C. Design of the estimator parameter $L_k(\vec{\xi}_k)$

Based on the designed decryption function and ADV, the estimation error dynamics can be characterized via the following parameter-dependent time-varying system:

$$\begin{cases} e_{k+1} = \big(A_k - L_k(\vec{\xi}_k)\vec{\Phi}(\vec{\xi}_k)C_k\big)e_k + E_k e_{k-\tau} \\ \qquad\quad + B_k\omega_k - L_k(\vec{\xi}_k)\vec{\Phi}(\vec{\xi}_k)D_k\nu_k \\ \tilde{z}_k = M_k e_k \end{cases} \tag{31}$$

where $e_k \triangleq x_k - \hat{x}_k$ is the estimation error and $\tilde{z}_k \triangleq z_k - \hat{z}_k$ stands for the output estimation error.

In what follows, we shall present sufficient conditions to ensure the desired estimation performance in the following theorem.

Theorem 3: Given the estimation error dynamics (31) and the parameter-dependent time-varying estimator gain $L_k(\vec{\xi}_k)$, under Assumptions 1-3, the required finite-horizon l_2-l_∞ estimation performance is achieved if there exist positive definite matrices R_k ($-\tau \leq k \leq N$) and $P_{i,k}$ ($i = 1, 2, \cdots, m$, $0 \leq k \leq N$) satisfying the following recursive matrix inequalities

$$\Theta_{i,k} \triangleq \begin{bmatrix} \underline{\Theta}_{11} & \underline{\Theta}_{12} & \underline{\Theta}_{13} & \underline{\Theta}_{14} \\ * & \underline{\Theta}_{22} & \underline{\Theta}_{23} & \underline{\Theta}_{24} \\ * & * & \underline{\Theta}_{33} & \underline{\Theta}_{34} \\ * & * & * & \underline{\Theta}_{44} \end{bmatrix} < 0 \tag{32}$$

and the constraints

$$P_{i,0} \leq \gamma^2 Q_0, \quad R_{-j} \leq \gamma^2 Q_j, \quad (j = 0, 1, \cdots, \tau) \tag{33}$$

$$P_{i,k} \geq M_k^T M_k \tag{34}$$

for all $i = 1, 2, \cdots, m$, where $\bar{P}_{k+1} \triangleq \sum_{j=1}^m p_j P_{j,k+1}$ and

$$\begin{aligned}
&\underline{\Theta}_{11} \triangleq \mathcal{A}_{i,k}^T\bar{P}_{k+1}\mathcal{A}_{i,k} + R_k - P_{i,k}, \\
&\underline{\Theta}_{12} \triangleq \mathcal{A}_{i,k}^T\bar{P}_{k+1}E_k, \\
&\underline{\Theta}_{13} \triangleq \mathcal{A}_{i,k}^T\bar{P}_{k+1}B_k, \\
&\underline{\Theta}_{14} \triangleq -\mathcal{A}_{i,k}^T\bar{P}_{k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k, \\
&\underline{\Theta}_{22} \triangleq E_k^T\bar{P}_{k+1}E_k - R_{k-\tau}, \\
&\mathcal{A}_{i,k} \triangleq A_k - L_k(\vec{\xi}_k)\vec{\Phi}(i)C_k, \\
&\underline{\Theta}_{24} \triangleq -E_k^T\bar{P}_{k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k, \\
&\underline{\Theta}_{33} \triangleq B_k^T\bar{P}_{k+1}B_k - \gamma^2 I, \\
&\underline{\Theta}_{34} \triangleq -B_k^T\bar{P}_{k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k, \\
&\underline{\Theta}_{23} \triangleq E_k^T\bar{P}_{k+1}B_k, \\
&\underline{\Theta}_{44} \triangleq D_k^T\vec{\Phi}(i)L_k^T(\vec{\xi}_k)\bar{P}_{k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k - \gamma^2 I.
\end{aligned}$$

Proof: First, define the following Lyapunov-like function:

$$V_k \triangleq e_k^T P_{i,k} e_k + \sum_{j=k-\tau}^{k-1} e_j^T R_j e_j,$$

where $i \triangleq \vec{\xi}_k$.

Calculating the difference of V_k (i.e., $\Delta V_k \triangleq V_{k+1} - V_k$), we have

$$\begin{aligned}&\Delta V_k \\ &= e_{k+1}^T P_{i,k+1} e_{k+1} - e_k^T(P_{i,k} - R_k)e_k - e_{k-\tau}^T R_{k-\tau} e_{k-\tau}\end{aligned}$$

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: DOI10.1109/JAS.2023.123393,

$$= \begin{bmatrix} e_k \\ e_{k-\tau} \\ \omega_k \\ \nu_k \end{bmatrix}^T \begin{bmatrix} \vec{\Theta}_{11} & \vec{\Theta}_{12} & \vec{\Theta}_{13} & \vec{\Theta}_{14} \\ * & \vec{\Theta}_{22} & \vec{\Theta}_{23} & \vec{\Theta}_{24} \\ * & * & \vec{\Theta}_{33} & \vec{\Theta}_{34} \\ * & * & * & \vec{\Theta}_{44} \end{bmatrix} \begin{bmatrix} e_k \\ e_{k-\tau} \\ \omega_k \\ \nu_k \end{bmatrix} + \gamma^2\|\omega_k\|^2 + \gamma^2\|\nu_k\|^2 \tag{35}$$

where

$$\begin{aligned}
&\bar{i} \triangleq \vec{\xi}_{k+1},\\
&\vec{\Theta}_{11} \triangleq \mathcal{A}_{i,k}^T P_{\bar{i},k+1}\mathcal{A}_{i,k} + R_k - P_{i,k},\\
&\vec{\Theta}_{12} \triangleq \mathcal{A}_{i,k}^T P_{\bar{i},k+1}E_k,\\
&\vec{\Theta}_{34} \triangleq -B_k^T P_{\bar{i},k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k,\\
&\vec{\Theta}_{14} \triangleq -\mathcal{A}_{i,k}^T P_{\bar{i},k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k,\\
&\vec{\Theta}_{13} \triangleq \mathcal{A}_{i,k}^T P_{\bar{i},k+1}B_k,\\
&\vec{\Theta}_{23} \triangleq E_k^T P_{\bar{i},k+1}B_k,\\
&\vec{\Theta}_{24} \triangleq -E_k^T P_{\bar{i},k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k,\\
&\vec{\Theta}_{33} \triangleq B_k^T P_{\bar{i},k+1}B_k - \gamma^2 I,\\
&\vec{\Theta}_{22} \triangleq E_k^T P_{\bar{i},k+1}E_k - R_{k-\tau},\\
&\vec{\Theta}_{44} \triangleq D_k^T\vec{\Phi}(i)L_k^T(\vec{\xi}_k)P_{\bar{i},k+1}L_k(\vec{\xi}_k)\vec{\Phi}(i)D_k - \gamma^2 I.
\end{aligned}$$

By noticing that $\bar{P}_{k+1} \triangleq \sum_{j=1}^m p_j P_{j,k+1} = \mathbb{E}\{P_{\bar{i},k+1}\}$, it follows from (32) and (35) that

$$\begin{aligned}
\mathbb{E}\{\Delta V_k|\mathbb{I}\} &= \begin{bmatrix} e_k \\ e_{k-\tau} \\ \omega_k \\ \nu_k \end{bmatrix}^T \Theta_{i,k} \begin{bmatrix} e_k \\ e_{k-\tau} \\ \omega_k \\ \nu_k \end{bmatrix} + \gamma^2\|\omega_k\|^2 + \gamma^2\|\nu_k\|^2\\
&\le \gamma^2\|\omega_k\|^2 + \gamma^2\|\nu_k\|^2
\end{aligned} \tag{36}$$

where $\mathbb{I} \triangleq \{i, e_k, e_{k-\tau}, \omega_k, \nu_k\}$. Hence, we have $\mathbb{E}\{\Delta V_k\} \le \gamma^2\|\omega_k\|^2 + \gamma^2\|\nu_k\|^2$, which implies that

$$\begin{aligned}
\mathbb{E}\{V_k\} - \mathbb{E}\{V_0\} &= \sum_{j=0}^{k-1}\mathbb{E}\{\Delta V_j\} \le \gamma^2\sum_{j=0}^{k-1}\big(\|\omega_k\|^2 + \|\nu_k\|^2\big)\\
&\le \gamma^2\sum_{j=0}^{N}\big(\|\omega_k\|^2 + \|\nu_k\|^2\big).
\end{aligned} \tag{37}$$

According to the conditions (33) and (34), we are not difficult to conclude that

$$\begin{aligned}
\sup_{k\ge 0}\mathbb{E}\{\|\tilde{z}_k\|^2\} &\le \mathbb{E}\{V_k\} \le \gamma^2\sum_{j=0}^{N}\big(\|\omega_k\|^2 + \|\nu_k\|^2\big) + \mathbb{E}\{V_0\}\\
&\le \gamma^2\sum_{j=0}^{N}\big(\|\omega_k\|^2 + \|\nu_k\|^2\big) + \sum_{i=-\tau}^{0} e_i^T Q_{-i} e_i,
\end{aligned}$$

which indicates that the required finite-horizon l_2-l_∞ estimation performance is achieved. The proof is now complete. ■

Up to now, sufficient conditions have been derived in Theorem 3 to guarantee the required finite-horizon l_2-l_∞ estimation performance for the plant (1) and the proposed EDS. Next, we shall proceed to design the parameter-dependent time-varying estimator gain matrix $L_k(\vec{\xi}_k)$.

Corollary 1: Given the estimation error described by the dynamical system (31), under Assumptions 1-3, the required finite-horizon l_2-l_∞ estimation performance is achieved if there exist positive definite matrices $P_{i,k}$ ($i = 1, 2, \cdots, m$, $0 \le k \le N+1$), R_k ($-\tau \le k \le N$) and real-valued matrices $\mathcal{L}_{i,k}$ satisfying the following recursive matrix inequalities

$$\bar{\Theta}_{i,k} \triangleq \begin{bmatrix} \bar{\Theta}_{11} & 0 & 0 & 0 & \bar{\Theta}_{15} \\ * & \bar{\Theta}_{22} & 0 & 0 & \bar{\Theta}_{25} \\ * & * & \bar{\Theta}_{33} & 0 & \bar{\Theta}_{35} \\ * & * & * & \bar{\Theta}_{44} & \bar{\Theta}_{45} \\ * & * & * & * & \bar{\Theta}_{55} \end{bmatrix} < 0 \tag{38}$$

and the constraints (33)-(34), where

$$\begin{aligned}
&\bar{\Theta}_{11} \triangleq R_k - P_{i,k},\\
&\bar{\Theta}_{15} \triangleq \big(\bar{P}_{k+1}A_k - \mathcal{L}_{i,k}\vec{\Phi}(i)C_k\big)^T,\\
&\bar{\Theta}_{22} \triangleq -R_{k-\tau},\\
&\bar{\Theta}_{35} \triangleq B_k^T\bar{P}_{k+1},\\
&\bar{\Theta}_{33} \triangleq -\gamma^2 I,\\
&\bar{\Theta}_{44} \triangleq -\gamma^2 I,\\
&\bar{\Theta}_{45} \triangleq -D_k^T\vec{\Phi}(i)\mathcal{L}_{i,k}^T,\\
&\bar{\Theta}_{55} \triangleq -\bar{P}_{k+1},\\
&\bar{\Theta}_{25} \triangleq E_k^T\bar{P}_{k+1}.
\end{aligned}$$

Moreover, the desired time-varying estimator gain parameter at time instant k is calculated as follows:

$$L_k(\vec{\xi}_k) = \bar{P}_{k+1}^{-1}\mathcal{L}_{\hat{i},k} \tag{39}$$

where $\hat{i} \triangleq \vec{\xi}_k$.

Proof: By using the Schur Complement Lemma, the proof is straightforward based on Theorem 3, and thus omitted here for brevity. ■

Remark 5: By now, we have handled the design issues of the EDS and the FHEtP state estimator. To guarantee the required finite-horizon energy-to-peak performance, a parameter-dependent time-varying state estimation algorithm and a measurement-data-based decryption function $\mathcal{F}_k(\cdot)$ have been constructed to decouple the estimation error from the ANT $S\Phi(\xi_k)\eta_k$. Then, the ADV η_k has been designed to achieve the desired secrecy capacity, under which the satisfactory information security can be ensured. Compared with the existing literature, the main novelty of this research can be emphasized from the following three aspects: 1) this paper has made one of the first attempts to deal with the FHEtP state estimation issue in the presence of eavesdroppers; 2) a novel encryption-decryption-based communication scheme has been constructed to ensure the desired secrecy capacity; and 3) an input-output-model-based method has been developed to design the decryption function and the ADV sequence.

IV. An Illustrative Example

In this section, an illustrative example is provided to examine the effectiveness and correctness of our proposed FHEtP state estimation algorithm as well as the EDS.

The plant under consideration is modeled by the system (1) where the corresponding parameters are given as follows:

$$A_k = \begin{bmatrix} 0.1 + 0.01\sin(0.3k) & 0.1 & 0.1 \\ 0 & 0.2 + 0.1\cos(0.1k) & 0.1 \\ -0.6 & 0 & -0.7 \end{bmatrix},$$

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: DOI10.1109/JAS.2023.123393,

$$E_k = \begin{bmatrix} 0 & 0.5 & -0.6 \\ 0.8 & -0.2 & -0.4 \\ 0.3 & 0.6 & 0.4 \end{bmatrix}, B_k = \begin{bmatrix} 0.2 \\ -0.3 \\ 0.1 + \frac{\cos(0.1k)}{10} \end{bmatrix}, \tau = 1,$$
$$C_k = \begin{bmatrix} -0.06 & -0.08 & -0.14 \\ -0.08 & 0.06 & -0.02 \\ 0.1 & 0.1 & 0.2 \end{bmatrix}, D_k = \begin{bmatrix} 0.1 \\ 0.1 \\ 0 \end{bmatrix}, M_k = 0.5I.$$

It is clear that the time-varying parameters satisfy

$$\bar{a} = \max_{0\le k\le N}\{\bar{A}_k\} = 1.4881, \quad \bar{b} = \max_{0\le k\le N}\{\bar{B}_k\} = 0.4123,$$
$$\bar{c} = \max_{0\le k\le N}\{\bar{C}_k\} = 0.3, \quad \bar{d} = \max_{0\le k\le N}\{D_k\} = 0.1414.$$

The measurement disturbance and process disturbance are, respectively, set to be $\nu_k = 0.4\sin(0.3k)$ and $\omega_k = 0.1\sin(k)$. The energy-to-peak performance index is set as $\gamma = 0.8$. The secret key S and the occurrence probabilities p_i $(i = 1, 2)$ are set to be

$$S = \begin{bmatrix} -0.6 & -0.8 & 0 \\ -0.8 & 0.6 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad p_1 = p_3 = 0.3, \quad p_2 = 0.4.$$

Clearly, S is an orthogonal matrix.

Based on the given parameters, it can be verified that Assumptions 1-2 hold by letting $\varpi = 0.28$, $\bar{N} = 5$ and $\underline{\aleph} = 0.0166$. Moreover, the threshold for the secrecy capacity is selected to be $\alpha = 0.5$. Calculating the sequence $\{\eta_k\}_{k\ge 0}$ based on Theorem 2 and designing the decryption function $\mathcal{F}_k(\Phi(i))$ according to (15), the corresponding trajectories of ξ_k and $\vec{\xi}_k$ are depicted in Fig. 2. It can be observed that our developed decryption mechanism is able to identify the value of ξ_k exactly.

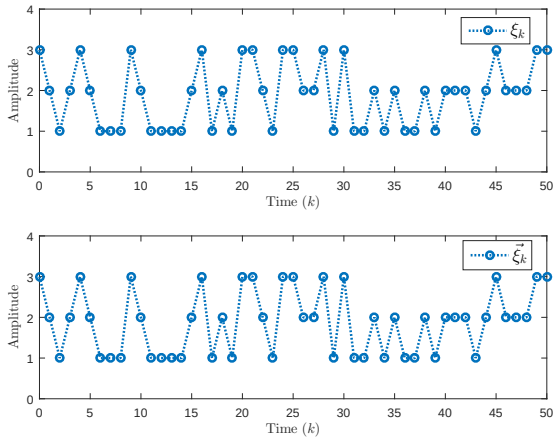

Fig. 2: The values of $\{\xi_k\}_{0\le k\le N}$ and $\{\vec{\xi}_k\}_{0\le k\le N}$.

The detailed simulation results are given in Figs. 3-7. Among them, Figs. 3-5 plot the state trajectories and their corresponding estimates under the designed time-varying state estimator (4). Fig. 6 shows the trajectory of $\mathcal{C}_k$, which implies that the resultant secrecy capacity is greater than the given threshold α. Fig. 7 displays the trajectory of $\|\tilde{z}_k\|^2$, from which we can see that the desired finite-horizon l_2-l_∞ estimation performance is satisfied. All the simulation results confirm that the main objectives of this paper are achieved.

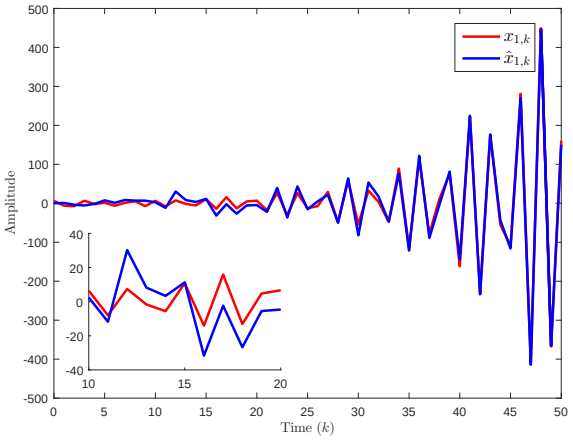

Fig. 3: The values of $\{x_{1,k}\}_{0\le k\le N}$ and $\{\hat{x}_{1,k}\}_{0\le k\le N}$.

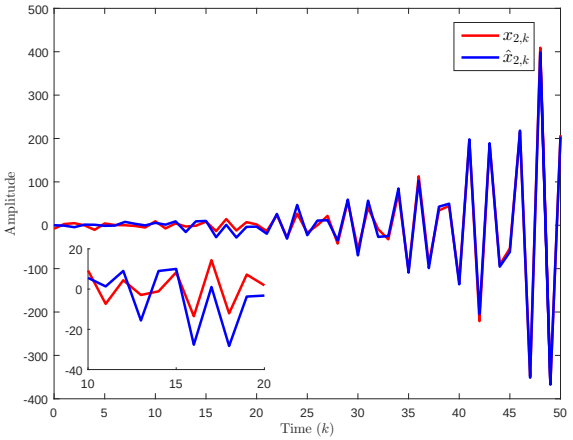

Fig. 4: The values of $\{x_{2,k}\}_{0\le k\le N}$ and $\{\hat{x}_{2,k}\}_{0\le k\le N}$.

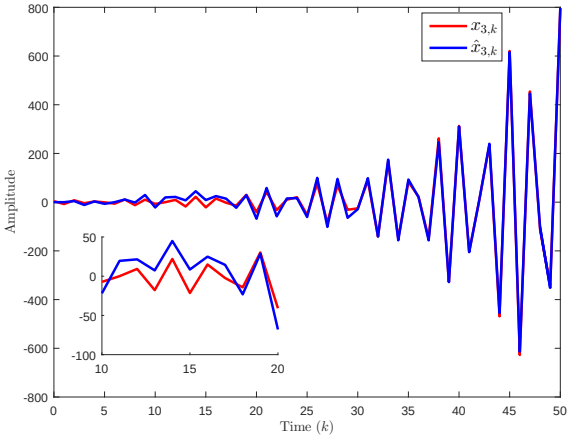

Fig. 5: The values of $\{x_{3,k}\}_{0\le k\le N}$ and $\{\hat{x}_{3,k}\}_{0\le k\le N}$.

V. Conclusion

In this article, we have addressed the FHEtP state estimation problem for linear time-varying systems in the presence of eavesdroppers. A novel artificial-noise-assisted encryptor has been developed to enhance the information security against

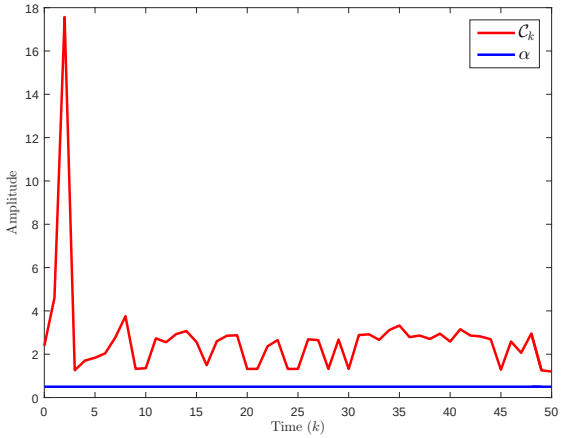

Fig. 6: The values of $\{\mathcal{C}_k\}_{0\leq k\leq N}$.

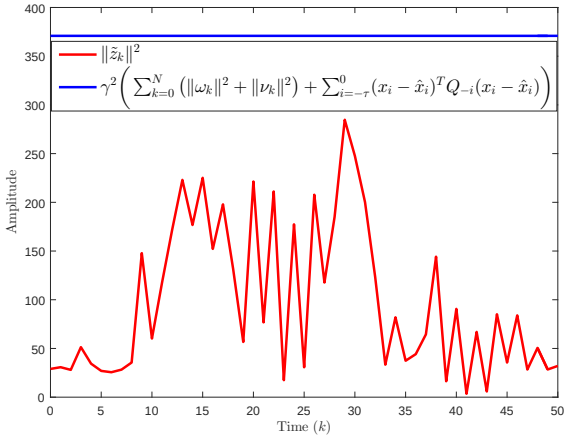

Fig. 7: The trajectory of the output estimation error $\|\tilde{z}_k\|^2$.

eavesdropping, under which the raw measurement signals are transformed into the ciphertexts before being transmitted. In addition, particular attention has been devoted to the design of the decryption function and the time-varying estimator gain parameter. Finally, the correctness and effectiveness of our derived results have been demonstrated through a numerical simulation example. Some interesting topics for future study include: 1) the secure state estimation issue for networked nonlinear systems against eavesdropping [46], [47]; and 2) the fusion state estimator design for networked systems in the presence of an eavesdropper [48].

REFERENCES

[1] D. Ciuonzo, A. Aubry, and V. Carotenuto, Rician MIMO channel- and jamming-aware decision fusion, *IEEE Transactions on Signal Processing*, vol. 65, no. 15, pp. 3866–3880, 2017.

[2] R. Caballero-Águila, A. Hermoso-Carazo and J. Linares-Pérez, Covariance-based fusion filtering for networked systems with random transmission delays and non-consecutive losses, *International Journal of General Systems*, vol. 46, no. 7, pp. 752-771, 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] X. Chen and Q. Song, State estimation for quaternion-valued neural networks with multiple time delays, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2278–2287, Nov. 2019.

[5] J. Hu, C. Jia, H. Liu, X. Yi and Y. Liu, A survey on state estimation of complex dynamical networks, *International Journal of Systems Science*, vol. 52, no. 16, pp. 3351–3367, Dec. 2021.

[6] Q. Li, J. Liang and H. Qu, H_∞ estimation for stochastic semi-Markovian switching CVNNs with missing measurements and mode-dependent delays, *Neural Networks*, vol. 141, pp. 281–293, Sep. 2021.

[7] 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.

[8] Q. Song, S. Chen, Z. Zhao, Y. Liu and F. E. Alsaadi, Passive filter design for fractional-order quaternion-valued neural networks with neutral delays and external disturbance, *Neural Networks*, vol. 137, pp. 18–30, May 2021.

[9] L. Yu, Y. Liu, Y. Cui, N. D. Alotaibi, F. E. Alsaadi, Intermittent dynamic event-triggered state estimation for delayed complex networks based on partial nodes, *Neurocomputing*, vol. 459, pp. 59–69, Octagons

[10] Z.-M. Li, X.-H. Chang, K. Mathiyalagan and J. Xiong, Robust energy-to-peak filtering for discrete-time nonlinear systems with measurement quantization, *Signal Processing*, vol. 139, pp. 102–109, Oct. 2017.

[11] H. Shen, Z.-G. Wu and J. H. Park, Finite-time energy-to-peak filtering for Markov jump repeated scalar non-linear systems with packet dropouts, *IET Control Theory & Applications*, vol. 8, no. 16, pp. 1617–1624, Nov. 2014.

[12] L. Zou, Z. Wang, H. Dong and Q.-L. Han, Energy-to-peak state estimation with intermittent measurement outliers: the single-output case, *IEEE Transactions on Cybernetics*, vol. 52, no. 11, pp. 11504-11515, Nov. 2022.

[13] H. Liu, Z. Wang, W. Fei and J. Li, H_∞ and l_2–l_∞ state estimation for delayed memristive neural networks on finite horizon: the Round-Robin protocol, *Neural Networks*, vol. 132, pp. 121–130, Dec. 2020.

[14] J. Zhang, L. Ma, Y. Liu, M. Lyu, F. E. Alsaadi and Y. Bo, H_∞ and l_2–l_∞ finite-horizon filtering with randomly occurring gain variations and quantization effects, *Applied Mathematics and Computation*, vol. 298, pp. 171–187, Apr. 2017.

[15] Y. Chen, J. Ren, X. Zhao and A. Xue, State estimation of Markov jump neural networks with random delays by redundant channels, *Neurocomputing*, vol. 453, pp. 493–501, Sep. 2021.

[16] J. Hu, Z. Wang and G.-P. Liu, Delay compensation-based state estimation for time-varying complex networks with incomplete observations and dynamical bias, *IEEE Transactions on Cybernetics*, in press, DOI: 10.1109/TCYB.2020.3043283.

[17] B. Jiang, H. Dong, Y. Shen and S. Mu, Encoding-decoding-based recursive filtering for fractional-order systems, *IEEE/CAA Journal of Automatica Snica*, vol. 9, no. 6, pp. 1103–1106, Jun. 2022.

[18] N. Li, Q. Li and J. Suo, Dynamic event-triggered H_∞ state estimation for delayed complex networks with randomly occurring nonlinearities, *Neurocomputing*, vol. 421, pp. 97–104, Jan. 2021.

[19] L. Ma, Z. Wang, Y. Chen and X. Yi, Probability-guaranteed distributed filtering for nonlinear systems with innovation constraints over sensor networks, *IEEE Transactions on Control of Network Systems*, vol. 8, no. 2, pp. 951–963, Jun. 2021.

[20] Y. Niu, L. Sheng, M. Gao and D. Zhou, Dynamic event-triggered state estimation for continuous-time polynomial nonlinear systems with external disturbances, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 3962–3970, Jun. 2020.

[21] X.-M. Zhang, Q.-L. Han and B.-L. Zhang, An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems, *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 4-16, Feb. 2017.

[22] Y. Zhao, X. He, L. Ma and H. Liu, Unbiasedness-constrained least squares state estimation for time-varying systems with missing measurements under round-robin protocol, *International Journal of Systems Science*, vol. 53, no. 9, pp. 1925–1941, Jul. 2022.

[23] 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.

[24] X. Ge, F. Yang and Q.-L. Han, Distributed networked control systems: a brief overview, *Information Sciences*, vol. 380, pp. 117-131, Feb. 2017.

[25] J. Cheng, Y. Wu, Z.-G. Wu and H. Yan, Nonstationary filtering for fuzzy Markov switching affine systems with quantization effects and deception attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, in press, DOI: 10.1109/TSMC.2022.3147228.

[26] D. Ding, H. Liu, H. Dong and H. Liu, Resilient filtering of nonlinear complex dynamical networks under randomly occurring faults

and hybrid cyber-attacks, *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2341–2352, Jul.-Aug. 2022.
[27] H. Song, D. Ding, H. Dong and Q.-L. Han, Distributed maximum correntropy filtering for stochastic nonlinear systems under deception attacks, *IEEE Transactions on Cybernetics*, vol. 52, no. 5, pp. 3733–3744, May 2022.
[28] H. Xiao, D. Ding, H. Dong and G. Wei, Adaptive event-triggered state estimation for large-scale systems subject to deception attacks, *Science China Information Sciences*, vol. 65, no. 2, art. no. 122207, Feb. 2022.
[29] X. Ge, Q.-L. Han, M. Zhong and X.-M. Zhang, Distributed Krein space-based attack detection over sensor networks under deception attacks, *Automatica*, vol. 109, art. no. 108557, Nov. 2019.
[30] 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.
[31] K. Miao, W.-A. Zhang and X. Qiu, An adaptive unscented Kalman filter approach to secure state estimation for wireless sensor networks, *Asian Journal of Control*, in press, DOI: 10.1002/asjc.2783.
[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] W. Xu, G. Hu, D. W. C. Ho and Z. Feng, Distributed secure cooperative control under denial-of-service attacks from multiple adversaries, *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3458–3467, Aug. 2020.
[35] W. Yang, Z. Zheng, G. Chen, Y. Tang and X. Wang, Security analysis of a distributed networked system under eavesdropping attacks, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1254–1258, Jul. 2020.
[36] 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.
[37] 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.
[38] A. Tsiamis, K. Gatsis and G. J. Pappas, State estimation with secrecy against eavesdroppers, in *Proceedings of the 20th World Congress of the International-Federation-of-Automatic-Control (IFAC)*, vol. 50, no. 1, pp. 8385–8392, Jul. 2017.
[39] 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.
[40] A. S. Leong, A. Redder, D. E. Quevedo and S. Dey, On the use of artificial noise for secure state estimation in the presence of eavesdroppers, In *Proceedings of the 2018 European Control Conference*, Limassol, Cyprus, pp. 325–330, 2018.
[41] H.-M. Wang, C. Wang, D. W. K. Ng, M. H. Lee and J. Xiao, Artificial noise assisted secure transmission for distributed antenna systems, *IEEE Transactions on Signal Processing*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.
[42] D. Xu, X. Yan, B. Chen and L. Yu, Energy-constrained confidentiality fusion estimation against eavesdroppers, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 2, pp. 624–628, Feb. 2022.
[43] N. A. Sarker and M. F. Samad, Capacity and outage performance analysis of secure cooperative RF-FSO relaying system in the p-resence of multiple eavesdroppers, *Physical Communication*, vol. 49, art. no. 101477, Dec. 2021.
[44] M. Z. I. Sarkar and T. Ratnarajah, Enhancing security in correlated channel with maximal ratio combining diversity, *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6745–6751, Dec. 2012.
[45] K. Reif, S. Günther, E. Yaz and R. Unbehauen, Stochastic stability of the discrete-time extended Kalman filter, *IEEE Transactions on Automatic Control*, vol. 44, no. 4, pp. 714–728, Apr. 1999.
[46] J. Mao, Y. Sun, X. Yi, H. Liu and D. Ding, Recursive filtering of networked nonlinear systems: a survey, *International Journal of Systems Science*, vol. 52, no. 6, pp. 1110–1128, Apr. 2021.
[47] P. Zhang, Y. Yuan and L. Guo, Fault-tolerant optimal control for discrete-time nonlinear system subjected to input saturation: a dynamic event-triggered approach, *IEEE Transactions on Cybernetics*, vol. 51, no. 6, pp. 2956–2968, Jun. 2021.
[48] H. Geng, H. Liu, L. Ma and X. Yi, Multi-sensor filtering fusion meets censored measurements under a constrained network environment: advances, challenges and prospects, *International Journal of Systems Science*, vol. 52, no. 16, pp. 3410–3436, 2021.

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. 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*, and *International Journal of Control, Automation and Systems*; a Senior Member of *IEEE*; an Early Career Advisory Board Member of *IEEE/CAA Journal of Automatica Sinica*; a Member of *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 more than 700 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. He is currently a Professor with the College of Information Science and Technology, Donghua University. From 2009 to 2010, he was a Research Assistant with the Department of Electrical and Electronic Engineering, 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, Uxbridge, 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 has published around 60 papers 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 serves (or has served) as an Associate Editor or an Editorial Board Member for eight international journals, including Systems Science and Control Engineering, the Journal of the Franklin Institute, the Asian Journal of Control, Circuits, Systems, and Signal Processing, Neurocomputing, Assembly Automation, Neural Processing Letters, and Mathematical Problems in Engineering. He is a Program Committee Member for many international conferences.

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. Her current research interests include robust control and networked control systems.

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

Guoping Lu received the B.Sc. degree from the Department of Applied Mathematics, Chengdu University of Science and Technology, Chengdu, China, in 1984, and the M.Sc. and Ph.D. degrees in applied mathematics from the Department of Mathematics, East China Normal University, Shanghai, China, in 1989 and 1998, respectively.

He is currently a Professor with the School of Electrical Engineering, Nantong University, Jiangsu, China. His research interests include singular systems, multi-agent systems, networked control, and nonlinear signal processing.