An Encoding-Based Privacy-Preserving Security Control Strategy Under Stealthy Attacks

Jian Liu, *Member, IEEE*, Shuailong Wang, Lijuan Zha, Jinliang Liu, *Senior Member, IEEE*, and Engang Tian, *Senior Member, IEEE*

***Abstract*—This paper focuses on the privacy-preserving security control issue for cyber-physical systems (CPSs) via an encoding-decoding communication scheme (EDCS). To considerably contemplate the delayed data acquisition and analysis, the integral measurement model is established, which is governed by the function related to system states within a certain period. The EDCS designed has a certain resistant to the non-ideal communication network with limited bandwidth capacity and fading channels. Then the controller is constructed by utilizing the decoding data. Furthermore, in the controller-to-actuator channel, assuming the stealthy false data injection attacks occur randomly and the injected pseudo data is associated with transmission data that has been eavesdropped. By virtue of deriving sufficient conditions, the CPS with EDCS can achieve input-to-state stability as well as the corresponding controller and observer gain parameters are acquired. Eventually, the effectiveness of the designed EDCS and control algorithm is illustrated by a case study involving an autonomous underwater vehicle system.**

***Index Terms*—Cyber-physical systems, encoding-decoding communication scheme, false data injection attacks, privacy-preserving strategy.**

I. Introduction

ENJOYING attractive advantages of immediacy, high-accuracy and scalability, cyber-physical systems (CPSs) have witnessed more attention on theory and practical industry, including vehicle platoon [1], smart grid systems [2] and teleoperation systems [3]. By integrating communication, computation and control, CPSs can realize the seamless interaction and integration of the physical realm and cyber realm. However, unpredictable risks may arise due to the vulnerability of communication networks. What needs to be elaborated is security of the network aspect and data privacy-preserving, which have become increasingly critical.

Malicious attacks can bring adverse impacts on system stability and mostly come with pecuniary losses. From the perspective of attack techniques, it can be divided into stealthy false data injection attacks (SFDIAs) [4] that inject malicious information and denial-of-service attacks [5] that exhaust network resources and cause system paralysis. These malicious attacks have raised concerns about the security of industrial CPSs. In real-world scenarios, the Ukrainian power grid was attacked by Blackenergy in 2015 [6] and an industrial control security system of a petrochemical plant in Saudi Arabia was hacked in 2017 [7], to name a just few. To address these concerns, Li et al. [8] give the secure control algorithm for time-varying multi-agent systems to defend against SFDIAs on sensor-to-control (S/C) and control-to-actuator (C/A) communication channels. Qiu et al. [9] establish a resilient control framework for CPSs in the presence of denial-of-service attacks. For the multi-bus DC microgrid, Xiao et al. [10] develop a resilient copperative control scheme to defend against SFDIAs. As a result, exploring the security control strategy for CPSs that focus on the SFDIAs is of paramount significance.

Since the vulnerability of communication networks in terms of being monitored and attacked, the privacy-preserving of transmission data has become a crucial issue in reality. As an effective privacy-preserving strategy, the encoding-decoding communication scheme (EDCS) can manipulate transmitted data by virtue of the uniform quantization procedure. It is precisely the encoding process that limited resources can be saved and the original data can not be directly monitored by attackers, which realizes information security. Due to these attractive advantages, presently, some existing results [11], [12] have demonstrated the availability of the EDCS for networked systems. More specially, by virtue of the finite-level uniform quantizer, Han et al. [13] design a group of encoder and decoder for each agent, which can effectively achieve privacy-preserving. Realizing the same importance of S/C and C/A channel security, Dong et al. [14] further expand such the EDCS to sensor and actuator sides to investigate the zero-error tracking issue. Different from the above decoding scheme, a novel EDCS has been adopted in the communication channel, which carries out the decoding

Received 9 September 2024; revised 1 January 2025 and 22 January 2025; accepted 10 February 2025. Date of publication 13 February 2025; date of current version 3 March 2025. This work was supported by the National Natural Science Foundation of China under Grant 62001210, Grant 62273174, Grant 62373252, and Grant 61973152. *(Corresponding author: Jinliang Liu.)*

Jian Liu and Shuailong Wang are with the School of Computer and Artificial Intelligence, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: liujian@nufe.edu.cn; 1120220517@stu.nufe.edu.cn).

Lijuan Zha is with the School of Science, Nanjing Forestry University, Nanjing 210037, China (e-mail: zhalijuan@njfu.edu.cn).

Jinliang Liu is with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: 003768@nuist.edu.cn).

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

Digital Object Identifier 10.1109/TICPS.2025.3542039

process with the benefit of encoding alphabets [15]. Among these existing EDCSs, the communication channel is generally assumed to be ideal, that is, the signal will not be affected by external attacks or attention. The EDCS developed, if not adequately considered, may be no longer applicable. Therefore, we endeavor to design a suitable EDCS and security control strategy to resist attention and external attacks.

In the practical communication environment, bandwidth limitation, path loss and shadowing may cause a loss of signal integrity. Furthermore, actual measurements are related to current physical state and measurement outputs over a period of time, which is so-called *integral measurements* [16]. Note that sensors are invisibly assumed to be non-destructive in the majority of existing works. Unfortunately, in synchrotron radiation [17], material mechanics [18] and electronic chemistry [19], such an assumption has certain limitations. Therefore, Shen et al. [20] establish the model of integral measurements by introducing an indicator function. Utilizing such a model, Geng et al. [21] investigate the Tobit Kalman filter issue for the linear system with sensor failures and scheduling protocols. Nevertheless, the security control problem of CPSs with privacy-preserving scheme and integral measurements has not been adequately explored. This promotes our current investigation.

Motivated by previous observations, this article focuses on the security control issue for CPSs with privacy-preserving scheme and SFDIAs. To sum up, the central contributions are three-fold.

1) An uniform quantization-assisted EDCS is provided to achieve data privacy-preserving in the non-ideal communication channel. Different from existing EDCSs that rely on the ideal control signal, an attenuation parameter is introduced in this EDCS, which achieves an excellent performance in the presence of stealthy attacks and fading channels.
2) An improved memory-assisted event-triggered scheme (MAETS) with memory threshold is designed and employed in the C/A channel. Different from [22], [23], this paper constructs a threshold with lower and upper bounds by leveraging historical buffer information, which can respond to unpredictably complicated communication scenarios and avoid high oscillation.
3) Associated with the designed MAETS, we extend the study to insecure C/A channels, which are monitored by attackers and injected with false information. Several sufficient conditions are deduced to guarantee the input-to-state stability (ISS) of the overall system.

The rest of this article is structured as below. The specific details of integral measurements and encoding-decoding procedure are given in Section II. Section III provides several sufficient conditions to guarantee the ISS of CPSs. Section IV presents simulation results and Section V concludes this paper.

Notations: The notation used here is fairly standard. $\mathbb{R}^n$ is the n dimensional Euclidean space. $\mathbb{Z}^+$ is a set of positive integers. I_n denotes the n-dimensional identity matrix. Y^T and Y^{-1} denote the transpose and inverse of matrix Y, respectively. $||\cdot||_\infty$ denotes the ∞-norm of the vector or matrix. $\lambda_{\min}(Y)$ and $\lambda_{\max}(Y)$ are the minimum and maximum eigenvalues of the matrix Y, respectively. $\mathrm{diag}\{\cdot\}$ is a block-diagonal matrix. In a real symmetry matrix $\begin{bmatrix} X & Y \\ (*) & Z \end{bmatrix}$, $(*)$ is the entries implied by symmetry. $\sup\{\cdot\}$ and $\inf\{\cdot\}$ stand for the supremum and infimum of the set, respectively.

II. Problem Formulation

A. System Model

For a nonlinear physical plant, consider the following discrete-time system with integral measurements:

$$\begin{cases} x(k+1) = Ax(k) + B\bar{u}(k) + Cg(x(k)) \\ y(k) = D\sum_{s=0}^{q} x(k-s), \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ stands the system state with the initial value $x(0) = x_0$ satisfying $||x_0||_2 \le \epsilon_0$, ϵ_0 is a known constant. $\bar{u}(k) \in \mathbb{R}^{n_u}$ denotes the control input signal after transmitted through the C/A network and $y(k) \in \mathbb{R}^{n_y}$ represents the integral measurement outputs. q is the time required for data collection. A, B, C, D are coefficient matrices with appropriate dimensions.

Assumption 1: [24] For $\forall k$, the nonlinear function $g(\cdot)$ with $g(0) = 0$ satisfies

$$||g(x_1) - g(x_2)||_2 \le ||G(x_1 - x_2)||_2, \tag{2}$$

where the matrix G with proper dimensions is known.

Remark 1: In practical implementations, due to delayed data collection and processing, the measurement output may be affected by system states over a previously certain interval. Therefore, actual measurement outputs of the discrete-time version is modeled as a summable form within the interval $[k-q,\ k]$. Moreover, such a model could be depicted as integral measurements and has been illustrated to have certain rationality and applicability [21].

B. Observer Structure

Having obtained integral measurement outputs $y(k)$, the following observer is adopted:

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + B\bar{u}(k) + Cg(\hat{x}(k)) + K(y(k) - \hat{y}(k)) \\ \hat{y}(k) = D\sum_{s=0}^{q} \hat{x}(k-s), \end{cases} \tag{3}$$

where $\hat{x}(k) \in \mathbb{R}^{n_x}$ is the estimated vector and satisfies $\hat{x}(0) = 0$, and K is the observer gain to be determined. It is noteworthy that the design of $\hat{y}(k)$ depends on the time interval q.

Defining $e(k) = x(k) - \hat{x}(k)$, the following error dynamics with integral measurements can be deduced by subtracting (3) from (1):

$$e(k+1) = Ae(k) + C\bar{g}(e(k)) - KD\sum_{s=0}^{q} e(k-s), \tag{4}$$

where $\bar{g}(e(k)) \triangleq g(x(k)) - g(\hat{x}(k))$. Then, setting $\bar{e}(k) = \begin{bmatrix} e^T(k) & e^T(k-1) & \cdots & e^T(k-q) \end{bmatrix}^T$, the compact form of above error dynamics (4) can be converted as:

$$\bar{e}(k+1) = (\mathscr{A} - \bar{K}\mathscr{D})\bar{e}(k) + \mathscr{C}f(\bar{e}(k)), \tag{5}$$

where

$$\mathscr{A}=\begin{bmatrix} A & 0 & \cdots & 0 & 0\\ I_{n_x} & 0 & \cdots & 0 & 0\\ 0 & I_{n_x} & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & I_{n_x} & 0 \end{bmatrix},\ \bar{K}=\begin{bmatrix} K\\ 0\\ \vdots\\ 0 \end{bmatrix},$$

$$\mathscr{D}=\begin{bmatrix} D & D & \cdots & D \end{bmatrix}, \mathscr{C}=\mathrm{diag}\{\mathrm{C},0,\ldots,0\},$$

$$f(\bar{e}(k))=\begin{bmatrix} \bar{g}^T(e(k)) & \bar{g}^T(e(k-1)) & \cdots & \bar{g}^T(e(k-q)) \end{bmatrix}^T.$$

C. Description of Encoding-Decoding Procedure

To strengthen the privacy-preserving and lighten the communication burden, the EDCS will be employed in the S/C channel. The data will be encoded before accessing the communication network and decoded after passing through the network. Before detailing the EDCS, the uniform quantization technique will be briefly introduced below.

Given positive parameters κ and integer p, the hyperrectangle $\mathcal{F}_\kappa=\{\varphi\in\mathbb{R}^{n_x}:||\varphi||_\infty\le\kappa, i=1,2,\ldots,n_x\}$ can be divided into p^{n_x} hyperrectangles $\mathscr{I}^1_{\iota_1}(\kappa)\times\mathscr{I}^1_{\iota_2}(\kappa)\times\cdots\times\mathscr{I}^{n_x}_{\iota_{n_x}}(\kappa)$, where $\iota_1,\iota_2,\ldots,\iota_{n_x}\in\{1,2,\ldots,p\}\triangleq\mathfrak{Q}$. The hyperrectangle $\mathscr{I}^i_m(\kappa)$ can be defined as:

$$\mathscr{I}^i_m(\kappa)\triangleq\{\varphi_i|-\kappa+2(j-1)\kappa/p\le\varphi_i<-\kappa+2m\kappa/p\}, \tag{6}$$

where $m\in\mathfrak{Q}$ and φ_i is the ith component of the vector φ. Furthermore, we obtain the center of the hyperrectangle $\mathscr{I}^1_{\iota_1}(\kappa)\times\mathscr{I}^2_{\iota_2}(\kappa)\times\cdots\times\mathscr{I}^{n_x}_{\iota_{n_x}}(\kappa)$ as:

$$\hbar_\kappa(\iota_1,\iota_2,\ldots,\iota_{n_x})\triangleq\begin{bmatrix} -\kappa+\frac{(2\iota_1-1)\kappa}{p}\\ -\kappa+\frac{(2\iota_2-1)\kappa}{p}\\ \vdots\\ -\kappa+\frac{(2\iota_{n_x}-1)\kappa}{p} \end{bmatrix}. \tag{7}$$

Then, there are unique integers $\iota_1,\iota_2,\ldots,\iota_{n_x}\in\mathfrak{Q}$ such that $\varphi\in\mathscr{I}^1_{\iota_1}(\kappa)\times\mathscr{I}^2_{\iota_2}(\kappa)\times\cdots\times\mathscr{I}^{n_x}_{\iota_{n_x}}(\kappa)$, which indicates

$$||\varphi-\hbar_\kappa(\iota_1,\iota_2,\ldots,\iota_{n_x})||_2\le\frac{\sqrt{n_x}\kappa}{p}. \tag{8}$$

Next, combining the above uniform quantization technique and analyzing at the encoding instant jh, the decoding error is denoted by $\varphi(jh)\triangleq\hat{x}(jh)-\vec{\chi}(jh)$, where h is the given encoding period and $\vec{\chi}(jh)$ is the auxiliary system state. Subsequently, the encoder and decoder can be designed below:

Encoder: For $\varphi(jh)\triangleq\hat{x}(jh)-\vec{\chi}(jh)\in\mathscr{I}^1_{\iota_1}(\kappa(jh))\times\mathscr{I}^2_{\iota_2}(\kappa(jh))\times\cdots\times\mathscr{I}^{n_x}_{\iota_{n_x}}(\kappa(jh))\subset\mathcal{F}_{\kappa(jh)}$, one knows that

$$\theta(jh)=\begin{bmatrix}\iota_1,\iota_2,\ldots,\iota_{n_x}\end{bmatrix}. \tag{9}$$

The auxiliary system state $\vec{\chi}(\cdot)$ and decoding value $\breve{\chi}(\cdot)$ are defined by

$$\begin{cases}\vec{\chi}(jh)=A\breve{\chi}(jh-1)+B\breve{u}(jh-1)+Cg(\breve{\chi}(jh-1))\\ \vec{\chi}(k)=\breve{\chi}(k), k\ne jh\\ \breve{u}(jh-1)=\bar{\beta}K_c\breve{\chi}(jh-1)\\ \vec{\chi}(0)=0\end{cases}$$

Decoder:

$$\begin{cases}\breve{\chi}(k+1)=A\breve{\chi}(k)+B\breve{u}(k)+Cg(\breve{\chi}(k)), k\ne jh-1\\ \breve{\chi}(jh)=\vec{\chi}(jh)+\hbar_\kappa(\iota_1,\iota_2,\ldots,\iota_{n_x})\\ \breve{u}(k)=\bar{\beta}K_c\breve{\chi}(k)\\ \breve{\chi}(0)=0,\end{cases} \tag{10}$$

where $\bar{\beta}$ and K_c are parameters to be defined later.

Remark 2: For purposes of achieving data privacy-preserving and mitigating the communication burden, we shall provide an improved EDCS against a backcloth of CPSs with fading channels. Firstly, such an EDCS utilizes the difference $\varphi(jh)$ rather than directly using estimation value $\hat{x}(jh)$ or state value, which reduces the size of transmitted data. Furthermore, compared with existing works in [25], [26], the nature of the periodic encoder diminishes the redundant transmission. To be specific, the data can be only encoded and transmitted at instants $h,2h,3h,\cdots$, and there is no data transmission in the remaining time.

Remark 3: In the existing EDCS, the update of encoding and decoding values rely on the control signal and precise *prediction* in [27]. Such a scheme, however, is no longer applicable when the control signal is contaminated by stealthy attacks and fading phenomena. By introducing an attenuation parameter and decoding values, we present the auxiliary control signal of the system. Hence, the EDCS (9) and (10) have been provided against SFDIAs and fading channels, which is more general than existing works.

D. Decoding Data-Based Controller and MAETS Design

With the aid of EDCS, the original data that threatens system performance can not be obtained by attackers. Besides, due to the presence of decoding errors and SFDIAs, the value received by the input terminal of the controller may not be the original value. The following decoding data-based controller can be designed:

$$u(k)=K_c\breve{\chi}(k), \tag{11}$$

where K_c represents the gain matrix to be determined.

In the C/A communication channel, an improved MAETS with a memory-assisted threshold and different weight coefficients has been employed to further utilize resources. Then, the sequence of triggered instant is deduced as

$$t_{n+1}=\inf_{k>t_n}\{\Delta(k,u(k),\xi_i(k))<0\}, \tag{12}$$

with the adopted function being

$$\Delta(k,u(k),\xi_i(k))=\delta(k)\frac{1}{m}\sum_{i=1}^{m}u^T(t_{n-i+1})\Phi u(t_{n-i+1})$$

$$-\sum_{i=1}^{m}\vartheta_i\xi_i^T(k)\Phi\xi_i(k), \tag{13}$$

where $m\in\mathbb{Z}^+$, $\delta(k)=\delta_M+(\delta_m-\delta_M)\frac{2}{\pi}atan\{\sigma||\sum_{i=1}^{m}u(k)-u(t_{n-i+1})||_2\}$, Φ and $\xi_i(k)=u(k)-u(t_{n-i+1})$ denote the number of the historical data packet, memory-assisted threshold, weight matrix and difference between the k instant and ith to last triggering time, respectively. In addition, weight coefficients satisfy $\sum_{i=1}^{m}\vartheta_i=1$ and $\vartheta_1\le\vartheta_2\le\cdots\le\vartheta_m$.

Remark 4: As shown in (13), the historical data information, including historical triggering instants and corresponding values, can be recorded and stored for utilization in determining the next triggering instant. Furthermore, this paper employs different weight coefficients to describe the general fact that the newly collected data is more important than the past ones. Different from the fixed threshold or traditional threshold only using current data, the summable gap and parameter σ are utilized to avoid high oscillation. The MAETS in (13) would degrade into the normal MAETS when $m=1$.

Next, from the practical attack perspective, unpredictable and hazardous SFDIAs are frequently adopted by attackers. Ideally, the signal received by the physical plant is sent with the assistance of the communication network. Nevertheless, a series of induced-phenomena can lead to the partial fading of signals in the C/A channel. Therefore, in the closed-loop system (1), the following control signal received by the target plant can be given:

$$\bar{u}(k)=\beta(t_n)(u(t_n)+\varepsilon(t_n)\varsigma(t_n)), \tag{14}$$

where $\varepsilon(t_n)\in\{0,1\}$ is a random variable characterized by the Bernoulli process. The random variable $\beta(\cdot)\in[\beta_\dagger,\beta^\dagger]$ is the fading channel coefficient and obeys the uniform distribution. Apparently, the probability distribution of $\varepsilon(\cdot)$ is $\bar{\varepsilon}\in[0,1]$. The expectation and variance of $\beta(\cdot)$ are $\bar{\beta}=(\beta_\dagger+\beta^\dagger)/2$ and $\tilde{\beta}^2=(\beta^\dagger-\beta_\dagger)^2/12$, respectively. $\varsigma(t_n)$ is the false information satisfying

$$\varsigma^T(t_n)\varsigma(t_n)\le u^T(t_n)Y^TYu(t_n), \tag{15}$$

where Y is a known matrix.

Remark 5: The partial fading of signals and external attacks are considered in the C/A channel. It is worth noting that no matter what factors cause deviation of the control signal, the EDCS in [27] is not applicable.

For subsequent analysis, the following definitions as a criterion for system detectability and stability are given.

Definition 1: [28] The nonlinear system (1) is detectable if there exist families of encoder-decoder pairs in (9) with an encoding alphabet $\mathfrak{H}$ of size $\mathfrak{X}$, such that

$$\lim_{k\to\infty}||x(k)-\breve{\chi}(k)||_2=0$$

holds for all solutions of the system.

Definition 2: [29] Consider the following system:

$$x(k+1)=\mathscr{F}(x(k),\varpi(k)),$$

where $x(k)$ denotes the system state, $\varpi(k)$ represents the exogenous signal. The above system is ISS if there exist a $\mathcal{KL}$ function $\ell(\cdot,\cdot)$ and a $\mathcal{K}$ class function $\wp(\cdot)$, such that

$$\ell(||\nu_0||_2,k)+\wp(||\varpi(k)||_\infty)\ge||\nu(k)||_2,$$

where $||\varpi(k)||\triangleq\sup_k\{||\varpi(k)||\}$.

III. Main Results

In this position, several sufficient conditions are presented to ensure that the closed-loop system (1) is detectable and ISS by using the Lyapunov function. Therefore, the following lemmas are given first before proceeding with the main results.

Lemma 1: Consider the nonlinear system (1) with EDCS, fading channels and SFDIAs. Given the scalar $\varrho_1>0$, if there exist a scalar $\nu_1>0$, matrix K_c and a positive definite matrix P satisfying

$$\Pi_1=\begin{bmatrix}\Pi_{11}^1 & \Pi_{12}^1 & \Pi_{13}^1 & \Pi_{14}^1\\ (*) & \Pi_{22}^1 & \Pi_{23}^1 & \Pi_{24}^1\\ (*) & (*) & \Pi_{33}^1 & \Pi_{34}^1\\ (*) & (*) & (*) & \Pi_{44}^1\end{bmatrix}<0 \tag{16}$$

where

$$\begin{aligned}
\Pi_{11}^1 &\triangleq -(1+\varrho_1)P+\nu_1\tilde{G}^T\tilde{G}+\tilde{A}^TP\tilde{A}+\bar{\beta}(\tilde{A}^TP\bar{\tilde{B}}\tilde{K}_c\\
&\quad+\tilde{K}_c^T\bar{\tilde{B}}^TP\tilde{A})+\tilde{K}_c^T(\bar{\beta}^2\bar{\tilde{B}}^TP\bar{\tilde{B}}+\tilde{\beta}^2\tilde{B}^TP\tilde{B})\tilde{K}_c\\
&\quad+\delta_M\tilde{K}_c^T\Phi\tilde{K}_c+\tilde{K}_c^TY^TY\tilde{K}_c,\\
\Pi_{12}^1 &\triangleq (\tilde{A}+\bar{\beta}\bar{\tilde{B}}\tilde{K}_c)^TP\tilde{C},\\
\Pi_{13}^1 &\triangleq -(\bar{\beta}\tilde{A}+\bar{\beta}^2\bar{\tilde{B}}\tilde{K}_c)^TP\tilde{B}I_1+\frac{\delta_M}{m}\tilde{K}_c^T\Phi I_2\\
&\quad-\tilde{K}_c^TY^TYI_1,\\
\Pi_{14}^1 &\triangleq (\bar{\beta}\bar{\varepsilon}\tilde{A}+\tilde{\beta}^2\bar{\varepsilon}\tilde{B}\tilde{K}_c+\bar{\beta}^2\bar{\varepsilon}\bar{\tilde{B}}\tilde{K}_c)^TP\tilde{B},\\
\Pi_{22}^1 &\triangleq -\nu_1I_{2n_x}+\tilde{C}^TP\tilde{C},\\
\Pi_{23}^1 &\triangleq -\bar{\beta}\tilde{C}^TP\tilde{B}I_1,\\
\Pi_{24}^1 &\triangleq \bar{\beta}\bar{\varepsilon}\tilde{C}^TP\tilde{B},\\
\Pi_{34}^1 &\triangleq -\check{\beta}\bar{\varepsilon}I_1^T\tilde{B}^TP\tilde{B},\\
\Pi_{33}^1 &\triangleq (\frac{\delta_M}{m}I_m-\bar{\vartheta})\bar{\Phi}+I_1^TY^TYI_1+\check{\beta}I_1^T\tilde{B}^TP\tilde{B}I_1,\\
\Pi_{44}^1 &\triangleq -I_{n_u}+\check{\beta}\bar{\varepsilon}\tilde{B}^TP\tilde{B},\\
\check{\beta} &\triangleq \bar{\beta}^2+\tilde{\beta}^2,\\
\tilde{A} &\triangleq diag\{A,A\},\\
\tilde{B} &\triangleq \begin{bmatrix}B^T & 0\end{bmatrix}^T,\\
\bar{\tilde{B}} &\triangleq \begin{bmatrix}0 & B^T\end{bmatrix}^T,\\
\tilde{K}_c &\triangleq \begin{bmatrix}0 & K_c\end{bmatrix},
\end{aligned}$$

$$\tilde{C} \triangleq diag\{C, C\},$$
$$\tilde{G} \triangleq diag\{G, G\},$$
$$I_1 \triangleq \begin{bmatrix} I_{n_u} & 0 & \cdots & 0 \end{bmatrix},$$
$$I_2 \triangleq \begin{bmatrix} I_{n_u} & I_{n_u} & \cdots & I_{n_u} \end{bmatrix},$$
$$\bar{\Phi} \triangleq diag\{\Phi, \Phi, \ldots, \Phi\},$$
$$\bar{\vartheta} \triangleq diag\{\vartheta_1, \vartheta_2, \ldots, \vartheta_m\}.$$

Then one can obtain

$$||\tilde{d}(k+1)||_2 < \tau_1 ||\tilde{d}(k)||_2, \tag{17}$$

where $\tau_1 \triangleq \sqrt{\frac{(1+\varrho_1)\lambda_{\max}(P)}{\lambda_{\min}(P)}}$.

Proof: The proof is given in Appendix A.

Lemma 2: Consider the error dynamics (4) under integral measurements. Give the scalar $\varrho_2 \in (0,1)$, assuming there exist a scalar $\nu_2 > 0$ and a positive definite matrix Q satisfying

$$\bar{\Pi}_2 = \begin{bmatrix} \bar{\Pi}_2^{11} & 0 & \bar{\Pi}_2^{13} \\ (*) & -\nu_2 I_{(q+1)n_x} & \mathscr{C}^T Q \\ (*) & (*) & -Q \end{bmatrix} < 0 \tag{18}$$

where $\bar{\Pi}_2^{11} \triangleq \nu_2 \bar{G}^T \bar{G} - (1-\varrho_2)Q$, $\bar{\Pi}_2^{13} \triangleq \mathscr{A}^T Q - \mathscr{D}^T(k)\tilde{K}^T$, $\bar{G} = diag\{Q, Q, \ldots, Q\}$.

Furthermore, the desired observer gain can be denoted by $\bar{K} = Q^{-1}\tilde{K}$. Then, select any positive integer h that fits $0 < \tau_2 < 1$ where $\tau_2 \triangleq \sqrt{\frac{(1-\varrho_2)^h \lambda_{\max}(Q)}{\lambda_{\min}(Q)}}$. In addition, one has

$$||\bar{e}(k+h)||_2 < \sqrt{\frac{(1-\varrho_2)^h \lambda_{\max}(Q)}{\lambda_{\min}(Q)}} ||\bar{e}(k)||_2. \tag{19}$$

Proof: The proof is given in Appendix B.

Lemma 3: The EDCS procedure (6)–(10) satisfies the following constraint:

$$||\hat{x}(jh) - \vec{\chi}(jh)||_\infty \leq \kappa(jh), \ j = 1, 2, \cdots \tag{20}$$

where $\kappa(jh)$ is defined by

$$\begin{cases} \kappa(h) \triangleq & \tau_2 \epsilon_0 + \tau_1^h \epsilon_0 \\ \kappa((j+1)h) \triangleq & \tau_2^{j+1}\epsilon_0 + \tau_1^h \tau_2^j \epsilon_0 + \tau_1^h \frac{\sqrt{n_x}}{p} \kappa(jh). \end{cases} \tag{21}$$

Proof: The proof is given in Appendix C.

Remark 6: Notice that Lemma 1 provides the relationship of the system state and decoder state and Lemma 2 proves that the error dynamics with integral measurements are convergent. Then, with the output of Lemmas 1 and 2, the boundedness of the encoding data is proved in Lemma 3 and we have provided upper bounds on the first encoding time and remaining encoding time, although the integral measurements lead to a relatively conservative outcome.

In what follows, we present that the system (1) is detectable and ISS, whose proof utilizes results of the above lemmas.

Theorem 1: The parameter τ_1 is defined in Lemma 1, as well as n_x is introduced in the target plant (1). Given positive scalars h and p, the system (1) is detectable under the EDCS, SFDIAs and fading channels if satisfying:

$$\tau_1^h \frac{\sqrt{n_x}}{p} < 1. \tag{22}$$

Proof: Recalling the definition of τ_2 in Lemma 2 and the definition of $\kappa(jh)$ in Lemma 3, based on Lemma 1 and (22), we can conclude that

$$\lim_{j\to\infty} \kappa(jh) = 0. \tag{23}$$

Then, one has

$$\begin{aligned} &||x(jh) - \breve{\chi}(jh)||_2 \\ &\leq ||\hat{x}(jh) - \vec{\chi}(jh) - \hbar_{\kappa(jh)}(\iota_1, \iota_2, \ldots, \iota_{n_x})||_2 \\ &\quad + ||x(jh) - \hat{x}(jh)||_2 \\ &\leq \tau_2^j \epsilon_0 + \tfrac{\sqrt{n_x}}{p}\kappa(jh). \end{aligned} \tag{24}$$

Consequently, we have $\lim_{j\to\infty} ||x(jh) - \breve{\chi}(jh)||_2 = 0$. Moreover, we can obtain from Lemma 1 that $||x(k) - \breve{\chi}(k)||_2 \leq \tau_1^{k-jh} ||x(jh) - \breve{\chi}(jh)||_2$ at non-encoding instants $k \in (jh, (j+1)h)$. Then, we obtain $\lim_{k\to\infty} ||x(k) - \breve{\chi}(k)||_2 = 0$, which means the physical plant (1) is detectable. That's the end of the proof.■

In what follows, the ISS of nonlinear system can be analyzed by resorting to linear matrix inequalities. Denoting decoding error $v(k) = \breve{\chi}(k) - x(k)$, it yields that $\breve{\chi}(k) = x(k) + v(k)$. In light of the (11) and (14), the controller is converted as

$$\bar{u}(k) = \beta(t_n)(K_c(x(k) + v(k)) - \xi_1(k) + \varepsilon(t_n)\varsigma(t_n)). \tag{25}$$

Consequently, the target plant can be deduced that

$$\begin{aligned} &x(k+1) = (A + \beta(t_n)BK_c)x(k) + Cg(x(k)) \\ &+\beta(t_n)(BK_c v(k) - B\xi_1(k) + \varepsilon(t_n)B\varsigma(t_n)). \end{aligned} \tag{26}$$

The decoding errors $v(k)$ are bounded by means of Lemma 1 and Theorem 1. In what follows, the stability of the discrete-time system (1) will be proved according to Definition 2 under the fading control signal and stealthy attacks.

Theorem 2: For given $\bar{\epsilon} \in [0,1]$, $\beta_\dagger, \beta^\dagger, \delta_M$ and m, the ISS of decoding data-based system (26) under EDCS, SFDIAs and MAETS can be guaranteed if there exist positive scalars μ_1 and ν_1, matrices K_c, and positive definite matrices W, P and $\mathcal{Z}$ such that

$$\Theta = \begin{bmatrix} \Theta_{11} & \Theta_{12} & \Theta_{13} & \Theta_{14} & \Theta_{15} \\ (*) & \Theta_{22} & \Theta_{23} & \Theta_{24} & \Theta_{25} \\ (*) & (*) & \Theta_{33} & \Theta_{34} & \Theta_{35} \\ (*) & (*) & (*) & \Theta_{44} & \Theta_{45} \\ (*) & (*) & (*) & (*) & \Theta_{55} \end{bmatrix} < 0 \tag{27}$$

$$\Pi_1 = \begin{bmatrix} \Pi_{11}^1 & \Pi_{12}^1 & \Pi_{13}^1 & \Pi_{14}^1 \\ (*) & \Pi_{22}^1 & \Pi_{23}^1 & \Pi_{24}^1 \\ (*) & (*) & \Pi_{33}^1 & \Pi_{34}^1 \\ (*) & (*) & (*) & \Pi_{44}^1 \end{bmatrix} < 0 \tag{28}$$

where

$$\begin{aligned} \Theta_{11} \triangleq & -W + A^T W A + \bar{\beta}(A^T W B K_c + K_c^T B^T W A) \\ & + \check{\beta} K_c^T B^T W B K_c + \mu_1 G^T G + \delta_M K_c^T \Phi K_c \end{aligned}$$

$$+K_c^TY^TYK_c,$$

$$\Theta_{12}\triangleq(A+\bar{\beta}BK_c)^TWC,\Theta_{55}\triangleq-I_{n_u}+\check{\beta}\bar{\varepsilon}B^TWB,$$

$$\Theta_{13}\triangleq\bar{\beta}A^TWBK_c+\check{\beta}K_c^TB^TWBK_c+\delta_MK_c^T\Phi K_c+K_c^TY^TYK_c,$$

$$\Theta_{14}\triangleq-(\bar{\beta}A+\check{\beta}BK_c)^TWBI_1-\frac{\delta_M}{m}K_c^T\Phi I_1-K_c^TY^TYI_1,$$

$$\Theta_{15}\triangleq\bar{\beta}\bar{\varepsilon}A^TWB+\check{\beta}\bar{\varepsilon}K_c^TB^TWB,$$

$$\Theta_{22}\triangleq-\mu_1I_{n_x}+C^TWC,\Theta_{23}\triangleq\bar{\beta}C^TWBK_c,$$

$$\Theta_{24}\triangleq-\bar{\beta}C^TWBI_1,\Theta_{25}\triangleq\bar{\beta}\bar{\varepsilon}C^TWB,$$

$$\Theta_{33}\triangleq-\mathcal{Z}+\check{\beta}K_c^TB^TWBK_c+\delta_MK_c^T\Phi K_c+K_c^TY^TYK_c,$$

$$\Theta_{34}\triangleq-\check{\beta}K_c^TB^TWBI_1-K_c^T\frac{\delta_M}{m}\Phi I_1-K_c^TY^TYI_1,$$

$$\Theta_{35}\triangleq\check{\beta}\bar{\varepsilon}K_c^TB^TWB,\Theta_{45}\triangleq-\check{\beta}\bar{\varepsilon}I_1^TB^TWB,$$

$$\Theta_{44}\triangleq\check{\beta}I_1^TB^TWBI_1+(\frac{\delta_M}{m}I_m-\bar{\vartheta})\bar{\Phi}+I_1^TY^TYI_1.$$

Proof: Construct the following Lyapunov function:

$$V(k)=x^T(k)Wx(k). \tag{29}$$

Denote $\eta_3(k)=\begin{bmatrix}x^T(k) & g^T(k) & v^T(k) & \bar{\xi}^T(k) & \varsigma^T(t_n)\end{bmatrix}^T$. Taking the Assumption 1, MAETS (13) and attack energy (15) into account, one has

$$\begin{aligned}&E\{\Delta V(k)\}=E\{V(k+1)-V(k)\}\\&\le E\{-x^T(k)Wx(k)+(x(k+1))^TWx(k+1)\\&+\mu_1(x^T(k)G^TGx(k)-g^T(x(k))g(x(k)))\\&+\Delta(k,u(k),\xi_i(k))+(u^T(t_n)Y^TYu(t_n)\\&-\varsigma^T(t_n)\varsigma(t_n))+v^T(k)\mathcal{Z}v(k)-v^T(k)\mathcal{Z}v(k)\}\\&=\eta_3^T(k)\Theta\eta_3(k)+v^T(k)\mathcal{Z}v(k).\end{aligned} \tag{30}$$

According to (27), one knows that $\Theta<0$. Then, we can obtain $\Delta V(k)\le-\lambda_{\min}(-\Theta)||x(k)||_2^2+\lambda_{\max}(\mathcal{Z})||v(k)||_2^2$. The networked system (26) is ISS by selecting

$$\begin{aligned}\vartheta(||v(k)||_2)&=\lambda_{\max}(\mathcal{Z})||v(k)||_2^2,\\\phi_1(||x(k)||_2)&=\lambda_{\min}(W)||x(k)||_2^2,\\\phi_2(||x(k)||_2)&=\lambda_{\max}(W)||x(k)||_2^2,\\\phi_3(||x(k)||_2)&=\lambda_{\min}(-\Theta)||x(k)||_2^2.\end{aligned}$$

Letting $\ell(||x(0)||_2,k)=\phi_1^{-1}(\psi^k\phi_2(||x(0)||_2))$ and $\wp=\phi_1^{-1}(\phi_2(\phi_3^{-1}(\vartheta(||v(k)||_2))))$, we obtain that

$$\begin{aligned}\ell(||x(0)||_2,k)&=\sqrt{\frac{\psi^k\lambda_{\max}(W)||\epsilon_0||_2^2}{\lambda_{\min}(W)}},\\\wp(||v(k)||_2)&=\sqrt{\frac{\lambda_{\max}(\mathcal{Z})\lambda_{\max}(W)||v(k)||_2^2}{\zeta\lambda_{\min}(-\Theta)\lambda_{\min}(W)}},\end{aligned} \tag{31}$$

where $\zeta\in(0,1)$. Then, one has

$$||x(k)||_2\le\ell(||x(0)||_2,k)+\wp(||v(k)||_2). \tag{32}$$

The proof is completed.■

Theorem 3: For given $\bar{\epsilon}\in[0,1],\beta_\dagger,\beta^\dagger,\delta_M$ and m, the ISS of decoding data-based system (26) under SFDIAs, EDCS and MAETS can be guaranteed if there exist positive scalars μ_1 and ν_1, positive definite matrices W,P,X,L and $\mathcal{Z}$, and real-valued matrix $\tilde{K}_c,\breve{K}_c$ such that

$$\bar{\Theta}=\begin{bmatrix}\bar{\Theta}_1 & \bar{\Theta}_2\\(*) & \bar{\Theta}_4\end{bmatrix}<0 \tag{33}$$

$$\bar{\Pi}_1=\begin{bmatrix}\bar{\Pi}_{11}^1 & \bar{\Pi}_{12}^1\\(*) & \bar{\Pi}_{22}^1\end{bmatrix}<0 \tag{34}$$

with $K_c=\bar{X}^{-1}\vec{K}_c$ and $\bar{X}^T=\mathcal{Q}^{-1}S^{-1}US\mathcal{Q}$, where the parameters are presented in Appendix C.

Proof: Drawing support from Schur complement lemma and (27), we have the following condition:

$$\tilde{\Theta}=\begin{bmatrix}\bar{\Theta}_1 & \tilde{\Theta}_2\\(*) & \tilde{\Theta}_4\end{bmatrix}<0 \tag{35}$$

where

$$\tilde{\Theta}_2\triangleq\begin{bmatrix}\tilde{\Theta}_{11}^2 & \tilde{\beta}K_c^TB^T & \bar{\Theta}_{13}^2 & \bar{\Theta}_{14}^2\\C^T & 0 & 0 & 0\\\bar{\beta}K_c^TB^T & \tilde{\beta}K_c^TB^T & \bar{\Theta}_{33}^2 & \bar{\Theta}_{34}^2\\-\bar{\beta}I_1^TB^T & -\tilde{\beta}I_1^TB^T & 0 & 0\\-\bar{\beta}\bar{\varepsilon}B^T & -\tilde{\beta}\bar{\varepsilon}B^T & 0 & 0\end{bmatrix},$$

$\tilde{\Theta}_{11}^2\triangleq A^T+\bar{\beta}K_c^TB^T,\tilde{\Theta}_4\triangleq-diag\{W^{-1},W^{-1},\aleph,I_{n_u}\}$.

Pre-multiplying and post-multiplying (35) by $\mathscr{X}=diag\{I_{n_x},I_{n_x},I_{n_x},I_m,I_{n_u},X,X,I_{n_u},I_{n_u}\}$ and $\mathscr{X}^T$, it yields that

$$\breve{\Theta}=\begin{bmatrix}\bar{\Theta}_1 & \breve{\Theta}_2\\(*) & \breve{\Theta}_4\end{bmatrix}<0 \tag{36}$$

where

$$\breve{\Theta}_2\triangleq\begin{bmatrix}\breve{\Theta}_{11}^2 & \tilde{\beta}K_c^TB^TX^T & \bar{\Theta}_{13}^2 & \bar{\Theta}_{14}^2\\C^TX & 0 & 0 & 0\\\bar{\beta}K_c^TB^TX^T & \tilde{\beta}K_c^TB^TX^T & \bar{\Theta}_{33}^2 & \bar{\Theta}_{34}^2\\\bar{\Theta}_{41}^2 & \bar{\Theta}_{42}^2 & 0 & 0\\\bar{\Theta}_{51}^2 & \bar{\Theta}_{52}^2 & 0 & 0\end{bmatrix},$$

$\breve{\Theta}_{11}^2\triangleq A^TX+\bar{\beta}K_c^TB^TX^T$,

$\breve{\Theta}_4\triangleq-diag\{XW^{-1}X^T,XW^{-1}X^T,\aleph,I_{n_u}\}$.

In light of the singular value decomposition (SVD) lemma in [30], we can obtain that $B^TX^T=\bar{X}^TB^T$ with $\bar{X}^T=\mathcal{Q}^{-1}S^{-1}US\mathcal{Q}$, where $B^T=\mathcal{Q}[S\ 0]R^T$ and $X^T=R\begin{bmatrix}U & 0\\0 & V\end{bmatrix}R^T$. In addition, if there exist a non-singular matrix X, the following inequality holds $(W-X)W^{-1}(W-X)^T\ge0$, which has $W-X-X^T\ge-XW^{-1}X^T$.

Furthermore, the sufficient condition (34) can be guaranteed by (28) employing the same treatment, which is omitted here for brevity. Then, the proof is completed.■

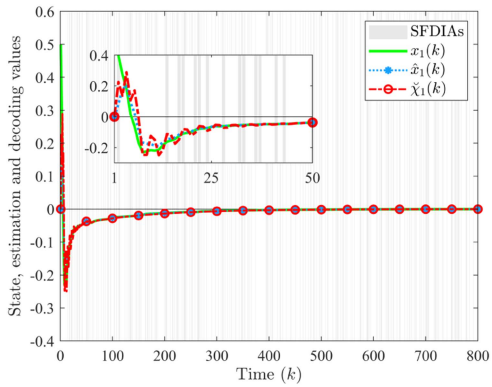

Fig. 1. The curves of state $x_1(k)$, estimate $\hat{x}_1(k)$ and decoding data $\check{\chi}_1(k)$ under SFDIAs.

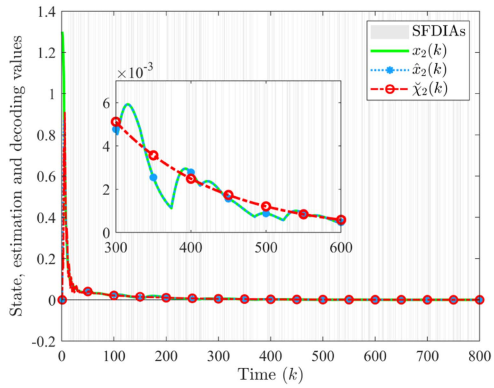

Fig. 2. The curves of state $x_2(k)$, estimate $\hat{x}_2(k)$ and decoding data $\check{\chi}_2(k)$ under SFDIAs.

IV. Numerical Example

In this section, numerical results are presented to highlight the applicability of the designed security control strategy in an autonomous underwater vehicle (AUV) system as in [31] and [32]. Take the sampling period of $T = 0.1s$ and then parameter values of the discrete-time system can be obtained as [31]:

$$A = \begin{bmatrix} 0.861 & -0.021 & 0.003 \\ 0.1 & 0.909 & -0.027 \\ 0 & 0.1 & 1 \end{bmatrix},$$

$$B = \begin{bmatrix} -0.089 & -0.135 & 0 \end{bmatrix}^T, \ D = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

In this example, we set $Cf(x)$ as a vector where all elements are 0. Therefore, with the initial state $x(0) = [0.5; 1.3; -1.5]$, $\varrho_1 = 0.3$ and $\varrho_2 = 0.85$, the values of τ_1 and τ_2 can be solved by Lemmas 1 and 2 as 1.1807 and 0.8076. Defining the positive scalars $h = 2$ and $p = 20$, as stated in Theorem 1, the sufficient condition (22) can be satisfied and calculated as $\tau_1^h \frac{\sqrt{n_x}}{p} = 0.1207$. The attack probability, lower and upper bounds of the fading parameter are selected as $\bar{\varepsilon} = 0.3$, $\beta_\dagger = 0.6$ and $\beta^\dagger = 0.9$. Furthermore, the parameters for MAETS are chosen as $\Phi = 10, \vartheta_1 = 0.6, \vartheta_2 = 0.2, \vartheta_3 = 0.2, \sigma = 100, \delta_m = 0.01$ and $\delta_M = 0.05$. The following gain parameters of the observer and controller can be obtained by solving linear matrix inequalities: $K = \begin{bmatrix} 0.0653 & 0.0016 \\ 0.1762 & -0.0145 \\ 0.0552 & 0.1869 \end{bmatrix}$,

$K_c = \begin{bmatrix} 1.1512 & 1.3368 & -0.0972 \end{bmatrix}$.

As the setting of the aforementioned parameters, the simulation results are presented in Figs. 1-5, in which Figs. 1-3 plot the state trajectories of the AUV, Fig. 4 depicts the errors of observer and decoder, and Fig. 5 shows the control input, curve of threshold and event-based interval with improved MAETS and normal MAETS. From Figs. 1-3, the observer with integral measurements can track the system state well. In addition, it can be clearly seen from time 1 to 50 in Fig. 1 that decoding value $\check{\chi}$ can track the system state only by leveraging the differential, which can achieve the data privacy-preserving. The moments of SFDIAs are characterized by gray areas. Furthermore, in

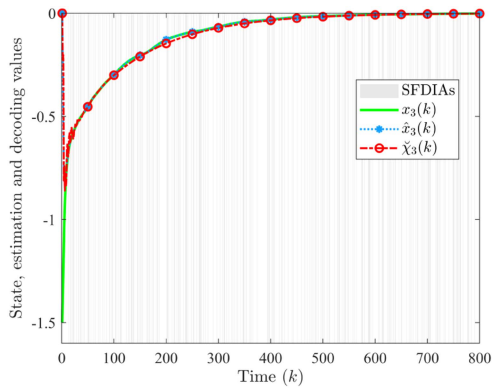

Fig. 3. The curves of state $x_3(k)$, estimate $\hat{x}_3(k)$ and decoding data $\check{\chi}_3(k)$ under SFDIAs.

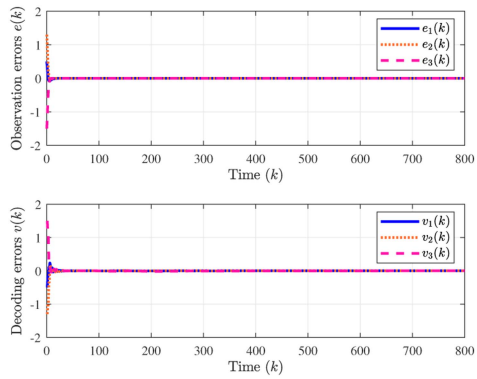

Fig. 4. The observation errors $e(k)$ and decoding errors $v(k)$.

increasing time, the considered system still achieves ISS without the absence of SFDIAs and integral measurements, which shows the availability of the security control algorithm.

Fig. 4 depicts that the observation and decoding errors are quickly eliminated by the designed control strategy around 20 and 40 time instants, respectively. Fig. 5(a) describes the control input under ideal networks and attacks. Intuitively, the threshold will evolve adaptively along with the different control signals and triggering instants in Fig. 5(b). Following the trajectory of

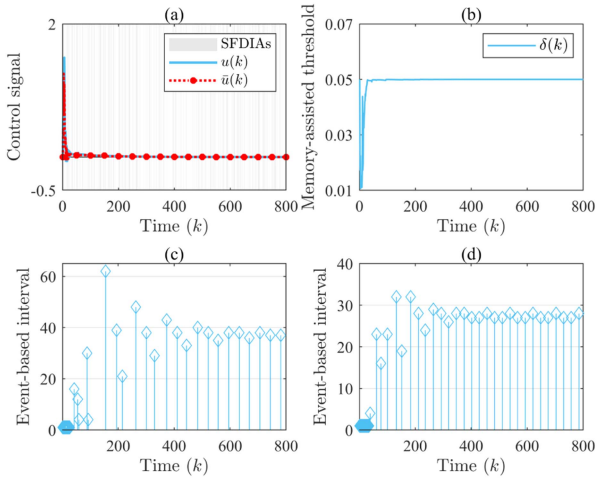

Fig. 5. (a) The control signals under ideal and attacks; (b) Memory-assisted threshold; (c) Triggering instants of improved MAETS; (d) Triggering instants of normal MAETS [33].

the adjustable threshold, there are several distinct fluctuations, mainly due to the prosperous transmission of data at those times. To further verify the superiority of the MAETS, the results of comparing to the threshold without historical information support in [33] are provided in Fig. 5(c)–(d). 6.38% of sampling data can be released in this paper, while the normal MAETS in [33] reached 8.13%. Apparently, the effectiveness and availability of the designed control method can be confirmed again.

V. Conclusion

This paper is dedicated to the security control strategy for the CPS with integral measurements to resist stochastic SFDIAs. The measurement output model is concretely formulated under the unsuspected influence of integral measurements. In the S/C channel, the EDCS has been effectively utilized to realize privacy-preserving and mitigate the communication burden by virtue of the uniform quantization strategy. Therefore, a secure controller has been designed based on decoding information. Furthermore, an improved MAETS with a memory-assisted threshold has been put forward to deploy on the insecure C/A channel, which is susceptible to interference from SFDIAs. Therefore, the corresponding gains of the observer and controller can be acquired and several sufficient criteria for satisfying the system ISS. Eventually, the simulation results are conducted to illustrate the superiority and availability of the security control method. In future research, how to extend this result to more complicated communication circumstances is an interesting topic.

Appendix A
The Proof of Lemma 1

Proof: Denoting $d(k) = x(k) - \breve{\chi}(k)$, obviously, we can get

$$\begin{aligned} d(k+1) &= Ad(k) + C\tilde{g}(d(k)) + B(\bar{u}(k) - \breve{u}(k)) \\ &= Ad(k) + C\tilde{g}(d(k)) + B((\beta(t_n) - \bar{\beta})K_c\breve{\chi}(k) \\ &\quad - \beta(t_n)\xi_1(k) + \beta(t_n)\varepsilon(t_n)\varsigma(t_n)), \end{aligned} \tag{37}$$

where $\tilde{g}(d(k)) = g(x(k)) - g(\breve{\chi}(k))$.

Then, by virtue of the vector augmentation technology, denoting $\tilde{d}(k) = \begin{bmatrix} d^T(k) & \breve{\chi}^T(k) \end{bmatrix}^T$, one has

$$\begin{aligned} \tilde{d}(k+1) &= (\tilde{A} + (\beta(t_n) - \bar{\beta})\tilde{B}\tilde{K}_c + \bar{\beta}\bar{\tilde{B}}\tilde{K}_c)\tilde{d}(k) + \tilde{C}\bar{\tilde{g}}(k) \\ &\quad - \beta(t_n)\tilde{B}I_1\bar{\xi}(k) + \beta(t_n)\varepsilon(t_n)\tilde{B}\varsigma(t_n), \end{aligned} \tag{38}$$

where $\bar{\tilde{g}}(k) \triangleq \begin{bmatrix} \tilde{g}^T(d(k)) & g^T(\breve{\chi}(k)) \end{bmatrix}^T$, $\bar{\xi}(k) = [\xi_1^T(k)$ $\xi_2^T(k)$ $\cdots$ $\xi_m^T(k)]^T$. Construct the following Lyapunov function:

$$V(k) = \tilde{d}^T(k)P\tilde{d}(k). \tag{39}$$

Then, define $\eta_1(k) = \begin{bmatrix} \tilde{d}^T(k) & \bar{\tilde{g}}^T(k) & \bar{\xi}^T(k) & \varsigma^T(t_n) \end{bmatrix}^T$ and $\Delta V(k) = V(k+1) - V(k)$. According to (2) (13) and (15), we can derive

$$\begin{aligned} &E\{\Delta V(k) - \varrho_1 V(k)\} \\ &\le E\{-(1+\varrho_1)\tilde{d}^T(k)P\tilde{d}(k) + (\tilde{d}(k+1))^T P\tilde{d}(k+1) \\ &\quad + \nu_1(\tilde{d}^T(k)\tilde{G}^T\tilde{G}\tilde{d}(k) - \bar{\tilde{g}}^T(k)\bar{\tilde{g}}(k)) - (\varsigma^T(t_n)\varsigma(t_n) \\ &\quad - u^T(t_n)Y^TYu(t_n)) + \Delta(k, u(k), \xi_i(k))\} \\ &= \eta_1^T(k)\Pi_1\eta_1(k). \end{aligned} \tag{40}$$

According to (16) and Schur complement lemma, it is apparent to find that $\Delta V(k) - \varrho_1 V(k) < 0$ and then $||d(k+1)||_2 \le ||\tilde{d}(k+1)||_2 < \tau_1||\tilde{d}(k)||_2$, which completes the proof.■

Appendix B
The Proof of Lemma 2

Select the Lyapunov function as

$$V(k) = \bar{e}^T(k)Q\bar{e}(k). \tag{41}$$

Similar to Lemma 1, letting $\eta_2(k) = \begin{bmatrix} \bar{e}^T(k) & f^T(\bar{e}(k)) \end{bmatrix}^T$, it follows that

$$\begin{aligned} &E\{\Delta(k) + \varrho_2 V(k)\} \\ &\quad = E\{-(1-\varrho_2)\bar{e}^T(k)Q\bar{e}(k) + \bar{e}^T(k+1)Q\bar{e}(k+1)\} \\ &\quad \le \eta_2^T(k)\Pi_2\eta_2(k), \end{aligned} \tag{42}$$

where $\Pi_2 \triangleq \begin{bmatrix} \Pi_2^{11} & \Pi_2^{12} \\ (*) & \Pi_2^{22} \end{bmatrix}$, $\Pi_2^{12} \triangleq (\mathscr{A} - \bar{K}\mathscr{D}(k))^T Q\mathscr{C}$, $\Pi_2^{22} \triangleq -\nu_2 I_{(q+1)n_x} + \mathscr{C}^T Q\mathscr{C}$, $\Pi_2^{11} \triangleq (\mathscr{A} - \bar{K}\mathscr{D}(k))^T Q(\mathscr{A} - \bar{K}\mathscr{D}(k)) + \nu_2\bar{G}^T\bar{G} - (1-\varrho_2)Q$.

In light of the (42) and Schur complement lemma, one derives that $V(k+1) < (1-\varrho_2)V(k)$. Moreover, it yields that $V(k+h) < (1-\varrho_2)V(k+h-1) < \cdots < (1-\varrho_2)^h V(k)$ and $||\bar{e}(k+h)||_2 < \tau_2||\bar{e}(k)||_2$, which completes the proof.■

APPENDIX C
THE PROOF OF LEMMA 3

Proof: Using mathematical induction to prove this lemma. Firstly, according to Lemma 2, we acquire $||e(k+h)||_2 \leq ||\bar{e}(k+h)||_2 < \tau_2||\bar{e}(k)||_2$. Then, for $j=1$, it yields that

$$\begin{aligned} &||\hat{x}(h)-\vec{\chi}(h)||_2 \\ &\leq ||x(h)-\vec{\chi}(h)||_2+||\hat{x}(h)-x(h)||_2 \leq \cdots \leq \tau_1^h\epsilon_0+\tau_2\epsilon_0 \end{aligned} \tag{43}$$

which guarantees $||\hat{x}(h)-\chi(h)||_\infty \leq \kappa(h)$.

Secondly, assuming $i=2,3,\ldots,j$ all meet the $||\hat{x}(ih)-\vec{\chi}(ih)||_\infty \leq \kappa(ih)$, then for $i=j+1$, we have

$$\begin{aligned} &||\hat{x}((j+1)h)-\vec{\chi}((j+1)h)||_2 \\ &\quad\leq ||x((j+1)h)-\vec{\chi}((j+1)h)||_2+||\hat{x}((j+1)h) \\ &\qquad -x((j+1)h)||_2 \\ &\quad\leq \cdots \\ &\quad\leq \tau_2^{j+1}\epsilon_0+\tau_1^h\tau_2^j\epsilon_0+\tau_1^h\frac{\sqrt{n_x}}{p}\kappa(jh) \end{aligned} \tag{44}$$

which clearly implies $||\hat{x}((j+1)h)-\vec{\chi}((j+1)h)||_\infty \leq \kappa((j+1)h)$. That's the end of the proof.

APPENDIX D
THE PARAMETERS OF THEOREM 3

$$\bar{\Theta}_1 \triangleq \begin{bmatrix} -W+\mu_1\tilde{}G^TG & 0 & 0 & \bar{\Theta}_{14}^1 & 0 \\ (*) & -\mu_1 I_{n_x} & 0 & 0 & 0 \\ (*) & (*) & -\mathcal{Z} & \bar{\Theta}_{34}^1 & 0 \\ (*) & (*) & (*) & \bar{\Theta}_{44}^1 & 0 \\ (*) & (*) & (*) & (*) & \bar{\Theta}_{55}^1 \end{bmatrix},$$

$$\bar{\Theta}_2 \triangleq \begin{bmatrix} \bar{\Theta}_{11}^2 & \bar{\Theta}_{12}^2 & \bar{\Theta}_{13}^2 & \bar{\Theta}_{14}^2 \\ C^TX & 0 & 0 & 0 \\ \bar{\Theta}_{31}^2 & \bar{\Theta}_{32}^2 & \bar{\Theta}_{33}^2 & \bar{\Theta}_{34}^2 \\ \bar{\Theta}_{41}^2 & \bar{\Theta}_{42}^2 & 0 & 0 \\ \bar{\Theta}_{51}^2 & \bar{\Theta}_{52}^2 & 0 & 0 \end{bmatrix},$$

$$\bar{\Theta}_{14}^1 \triangleq -\frac{\delta_M}{m}K_c^T\Phi I_1-K_c^TY^TYI_1, \bar{\Theta}_{11}^2 \triangleq A^TX+\bar{\beta}\vec{K}_c^TB^T,$$

$$\bar{\Theta}_{34}^1 \triangleq -\frac{\delta_M}{m}K_c^T\Phi I_1-K_c^TY^TYI_1, \bar{\Theta}_{12}^2 \triangleq \tilde{\beta}\vec{K}_c^TB^T,$$

$$\bar{\Theta}_{44}^1 \triangleq (\frac{\delta_M}{m}I_m-\bar{\vartheta})\bar{\Phi}+I_1^TY^TYI_1, \bar{\Theta}_{13}^2 \triangleq \sqrt{\delta_M}K_c^T,$$

$$\bar{\Theta}_{55}^1 = -I_{n_u}+\check{\beta}(\bar{\varepsilon}-\bar{\varepsilon}^2)B^TWB\bar{\Theta}_{14}^2 \triangleq K_c^TY^T,$$

$$\bar{\Theta}_{31}^2 \triangleq \bar{\beta}\vec{K}_c^TB^T, \bar{\Theta}_{32}^2 \triangleq \tilde{\beta}\vec{K}_c^TB^T, \bar{\Theta}_{33}^2 \triangleq \sqrt{\delta_M}K_c^T,$$

$$\bar{\Theta}_{34}^2 \triangleq K_c^TY^T, \bar{\Theta}_{41}^2 \triangleq -\bar{\beta}I_1^TB^TX, \bar{\Theta}_{42}^2 \triangleq -\tilde{\beta}I_1^TB^TX,$$

$$\bar{\Theta}_{51}^2 \triangleq -\bar{\beta}\bar{\varepsilon}B^TX, \bar{\Theta}_{52}^2 \triangleq -\tilde{\beta}\bar{\varepsilon}B^TX, \aleph \triangleq \Phi^{-1},$$

$$\bar{\Theta}_5 \triangleq diag\{\mathscr{W},\mathscr{W},-\aleph,-I_{n_u}\}, \mathscr{W} \triangleq W-X-X^T,$$

$$\bar{\Pi}_{11}^1 \triangleq \begin{bmatrix} \Gamma_{11}^1 & 0 & \Gamma_{13}^1 & 0 \\ (*) & -\nu_1 I_{2n_x} & 0 & 0 \\ (*) & (*) & \Gamma_{33}^1 & 0 \\ (*) & (*) & (*) & \Gamma_{44}^1 \end{bmatrix},$$

$$\bar{\Pi}_{12}^1 \triangleq \begin{bmatrix} \Gamma_{11}^2 & \Gamma_{12}^2 & \Gamma_{13}^2 & \Gamma_{14}^2 \\ \tilde{C}^TL & 0 & 0 & 0 \\ \Gamma_{31}^2 & \Gamma_{32}^2 & 0 & 0 \\ \Gamma_{41}^2 & \Gamma_{42}^2 & 0 & 0 \end{bmatrix},$$

$$\Gamma_{11}^1 \triangleq -(1+\varrho_1)P+\nu_1\tilde{G}^T\tilde{G}, \Gamma_{11}^2 = \tilde{A}^TL+\bar{\beta}\check{K}_c^T\bar{\tilde{B}}^T,$$

$$\Gamma_{13}^1 \triangleq -\frac{\delta_M}{m}\tilde{K}_c^T\Phi^TI_1-\tilde{K}_c^TY^TYI_1, \Gamma_{12}^2 \triangleq \tilde{\beta}\check{K}_c^T\tilde{B}^T,$$

$$\Gamma_{33}^1 \triangleq (\frac{\delta_M}{m}I_m-\bar{\vartheta})\bar{\Phi}+I_1^TY^TYI_1, \Gamma_{13}^2 \triangleq \sqrt{\delta_M}\tilde{K}_c^T,$$

$$\Gamma_{44}^1 \triangleq -I_{n_u}+\check{\beta}(\bar{\varepsilon}-\bar{\varepsilon}^2)\tilde{B}^TP\tilde{B}, \Gamma_{14}^2 \triangleq \tilde{K}_c^TY^T,$$

$$\Gamma_{31}^2 \triangleq -\bar{\beta}I_1^T\tilde{B}^TL, \Gamma_{32}^2 \triangleq -\tilde{\beta}I_1^T\tilde{B}^TL, \Gamma_{41}^2 \triangleq \bar{\beta}\bar{\varepsilon}\tilde{B}^TL$$

$$\Gamma_{42}^2 \triangleq \tilde{\beta}\bar{\varepsilon}\tilde{B}^TL, \bar{\Pi}_{22}^1 \triangleq diag\{\mathscr{P},\mathscr{P},-\aleph,-I_{n_u}\},$$

$$\mathscr{P} \triangleq P-L-L^T.$$

REFERENCES

[1] P. Zhang, "Joint optimization of platoon control and resource scheduling in cooperative vehicle-infrastructure system," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 6, pp. 3629–3646, Jun. 2023.

[2] F. Sangoleye, E. E. Tsiropoulou, and S. Papavassiliou, "Dynamic risk management for demand response in multi-utility smart grids," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 98–107, 2024.

[3] L. Hu, J. Huang, S. Hao, S. Liu, J. Lu, and B. Chen, "Finite-time switching resilient control for networked teleoperation system with time-varying delays and random DoS attacks," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 232–243, 2024.

[4] Y. Liu and L. Cheng, "Relentless false data injection attacks against Kalman-filter-based detection in smart grid," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 3, pp. 1238–1250, Sep. 2022.

[5] J. Liu, Y. Dong, L. Zha, X. Xie, and E. Tian, "Reinforcement learning-based tracking control for networked control systems with DoS attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 4188–4197, 2024.

[6] S. Kim, K.-J. Park, and C. Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1534–1573, thirdquarter 2022.

[7] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, 2020.

[8] X.-M. Li, Q. Zhou, P. Li, H. Li, and R. Lu, "Event-triggered consensus control for multi-agent systems against false data-injection attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1856–1866, May 2020.

[9] X. Qiu, W. Meng, J. Xu, and Q. Yang, "Reduced-order observer-based resilient control for MASs with time-varying delay against DoS attacks," *IEEE Trans. Ind. Cyber- Phys. Syst.*, vol. 2, pp. 51–59, 2024.

[10] F. Xiao, S. Liu, B. Wei, F. Fang, and J. Qin, "Resilient cooperative control of multiple DC microgrids with interconnection networks against cyber attacks," *IEEE Trans. Ind. Cyber- Phys. Syst.*, vol. 3, pp. 116–126, 2025.

[11] S. Zhang, L. Ma, and X. Yi, "Model-free adaptive control for nonlinear multi-agent systems with encoding-decoding mechanism," *IEEE Trans. Signal Inf. Process. Networks*, vol. 8, pp. 489–498, 2022.

[12] J. Zhou, W. Ding, and W. Yang, "A secure encoding mechanism against deception attacks on multisensor remote state estimation," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1959–1969, 2022.

[13] Y. Han, C. Li, W. Zhang, and H. G. Ahmad, "Impulsive consensus of multiagent systems with limited bandwidth based on encoding–decoding," *IEEE Trans. Cybern.*, vol. 50, no. 1, pp. 36–47, Jan. 2020.

[14] D. Shen and C. Zhang, "Zero-error tracking control under unified quantized iterative learning framework via encoding–decoding method," *IEEE Trans. Cybern.*, vol. 52, no. 4, pp. 1979–1991, Apr. 2022.
[15] J. Sun, B. Shen, and L. Zou, "Ultimately bounded state estimation for nonlinear networked systems with constrained average bit rate: A buffer-aided strategy," *IEEE Trans. Signal Process.*, vol. 72, pp. 1865–1876, 2024.
[16] A. Gopalakrishnan, N. S. Kaisare, and S. Narasimhan, "Incorporating delayed and infrequent measurements in extended Kalman filter based nonlinear state estimation," *J. Process Control*, vol. 21, no. 1, pp. 119–129, 2011.
[17] E. V. Markov and O. M. Mikhailov, "Integral measurements of the color of nanodimensional radiators," *Meas. Techn.*, vol. 57, pp. 990–996, 2014.
[18] H. R. Moran, "An experimental study of the thermohydraulic characteristics of flow boiling in horizontal pipes: Linking spatiotemporally resolved and integral measurements," *Appl. Thermal Eng.*, vol. 194, 2021, Art. no. 117085.
[19] M. Martins, "A setup for integral measurements of multiple scattering angular distributions by 10- to 100-keV electrons," *Radiat. Phys. Chem.*, vol. 200, 2022, Art. no. 110381.
[20] Y. Shen, Z. Wang, B. Shen, and F. E. Alsaadi, "H_∞ state estimation for multi-rate artificial neural networks with integral measurements: A switched system approach," *Inf. Sci.*, vol. 539, pp. 434–446, 2020.
[21] H. Geng, Z. Wang, L. Zou, A. Mousavi, and Y. Cheng, "Protocol-based Tobit Kalman filter under integral measurements and probabilistic sensor failures," *IEEE Trans. Signal Process.*, vol. 69, pp. 546–559, 2021.
[22] L. Li, Y. Zhang, and T. Li, "Memory-based event-triggered output regulation for networked switched systems with unstable switching dynamics," *IEEE Trans. Cybern.*, vol. 52, no. 11, pp. 12429–12439, Nov. 2022.
[23] L. Yao, X. Huang, Z. Wang, and H. Shen, "Memory-based event-triggered control of Markov jump systems under hybrid cyber attacks: A switching-like adaptive law," *IEEE Trans. Automat. Sci. Eng.*, vol. 21, no. 4, pp. 6347–6357, Oct. 2024.
[24] W. Fan, W. Zidong, L. Jinling, and L. Xiaohui, "Recursive distributed filtering for two-dimensional shift-varying systems over sensor networks under stochastic communication protocols," *Automatica*, vol. 115, 2020, Art. no. 108865.
[25] C. Gao, Z. Wang, J. Hu, Y. Liu, and X. He, "Consensus-based distributed state estimation over sensor networks with encoding-decoding scheme: Accommodating bandwidth constraints," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4051–4064, Nov./Dec. 2022.
[26] X. Lu, Y. Jia, Y. Fu, and F. Matsuno, "Finite-level quantized min-consensus control based on encoding-decoding," *IEEE Trans. Cybern.*, vol. 53, no. 11, pp. 6788–6802, Nov. 2023.
[27] J.-Y. Li, Z. Wang, R. Lu, and Y. Xu, "Partial-nodes-based state estimation for complex networks with constrained bit rate," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1887–1899, Apr.–Jun. 2021.
[28] L. Wang, Z. Wang, Q.-L. Han, and G. Wei, "Synchronization control for a class of discrete-time dynamical networks with packet dropouts: A coding–decoding-based approach," *IEEE Trans. Cybern.*, vol. 48, no. 8, pp. 2437–2448, Aug. 2018.
[29] Z.-P. Jiang and Y. Wang, "Input-to-state stability for discrete-time nonlinear systems," *Automatica*, vol. 37, no. 6, pp. 857–869, 2001.
[30] J. Liu, E. Gong, L. Zha, E. Tian, and X. Xie, "Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 11, pp. 3853–3865, Nov. 2023.
[31] L. Xu, H. Zhu, K. Guo, Y. Gao, and C. Wu, "Output-based secure control under false data injection attacks," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 43–50, 2024.
[32] J. Petrich and D. J. Stilwell, "Model simplification for AUV pitch-axis control design," *Ocean Eng.*, vol. 37, no. 7, pp. 638–651, 2010.
[33] E. Tian and C. Peng, "Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, Nov. 2020.