An Output-Coding-Based Detection Scheme Against Replay Attacks in Cyber-Physical Systems

Haibin Guo, Zhong-Hua Pang, *Senior Member, IEEE*, Jian Sun, *Senior Member, IEEE*, and Jun Li

***Abstract*—This brief studies the detection problem of replay attacks against measurement data transmitted over the feedback channel of a cyber-physical system. In order to detect such replay attacks, an output coding scheme, where the control input is coded into the measurement output transmitted in the feedback channel, is proposed to make the output residuals between the normal and compromised cases significantly different, which thus triggers an alarm from an anomaly detector. The main advantage of this scheme is that the system performance in the normal situation is not affected compared with existing coding detection schemes, which is also the practical motivation of our work. In addition, the encoded measurement output is directly used to estimate the system state instead of setting a decoder. Both theoretical analysis and simulation results are provided to demonstrate the effectiveness of the proposed scheme.**

***Index Terms*—Cyber-physical systems (CPSs), replay attacks, attack detection, output coding.**

I. Introduction

CYBER-PHYSICAL systems (CPSs), which are the integration of computation, communication, and control, have drawn much attention. CPSs have been applied in various fields such as aerospace, smart grids, and intelligent transportation. Since data in a CPS are usually transmitted over a wire/wireless network, they are susceptible to be corrupted by malicious attackers. For instance, Stuxnet is a notorious malware that disrupted the CPSs [1]. Since then, the security of CPSs has attracted great attention [2], [3]. Typical cyber attacks against CPSs include denial of service (DoS) attacks [4]–[6] and deception attacks [7]–[9].

Manuscript received February 23, 2021; accepted March 1, 2021. Date of publication March 4, 2021; date of current version September 24, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61925303, Grant 62088101, Grant U20B2073, and Grant 61673023; in part by the National Key R&D Program of China under Grant 2018YFB1700100; in part by the Youth Talent Support Program of Beijing Municipality; and in part by the NCUT Yujie Talent Training Program. This brief was recommended by Associate Editor S. Li. *(Corresponding author: Jian Sun.)*

Haibin Guo and Jian Sun are with the State Key Laboratory of Intelligent Control and Decision of Complex Systems, School of Automation, Beijing Institute of Technology, Beijing 100081, China (e-mail: ghb199509@163.com; sunjian@bit.edu.cn).

Zhong-Hua Pang is with the Key Laboratory of Fieldbus Technology and Automation of Beijing, North China University of Technology, Beijing 100144, China (e-mail: zhonghua.pang@ia.ac.cn).

Jun Li is with the China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China (e-mail: ljfigo@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSII.2021.3063835.

Digital Object Identifier 10.1109/TCSII.2021.3063835

Deception attack mainly modifies the data transmitted over a network, while keeping it stealthy. In [7] and [8], an innovation-based linear stealthy attack strategy was proposed to maximize degradation of the remote estimation performance. In [9], a stealthy two-channel attack scheme was presented to disrupt the stability of the system while avoiding to be detected. In [10] and [11], an optimal switching data injection attack scheme was proposed to corrupt partial transmission channels. In order to detect false data injection (FDI) attacks, a coding matrix was employed in [12] to code the original measurement output to increase the estimation residual. In [13], an active data modification detection scheme was designed to detect two-channel stealthy FDI attack. In [14], a distributed fusion strategy was presented to expose FDI attacks. In [15], the authors studied the detection method against deception attacks on multi-sensor remote state estimation. And then, a Gaussian-mixture-model-based detection mechanism against integrity attacks was proposed in [16].

Replay attacks are a special class of deception attacks, which attempt to record the previous normal system data and then replay these data to replace the current data transmitted over the network [17]. Since replayed data are originated from the normal system, the encode-decode detection schemes against FDI attacks in [12] and [13] become invalid for replay attacks. To the best of our knowledge, there are two main detection mechanisms against replay attacks: 1) coding scheme [17], [18] and 2) watermarking scheme [19], [20]. In [17], an additional Gaussian noise was coded into the control input to detect replay attacks. However, this detection scheme would bring an adverse effect on the system performance in the normal situation, and the actuator would also be further burdened under noisy control commands. To remove such a drawback in [17], a stochastic coding scheme was proposed in [18], but it required that two same Gaussian noise sequences were generated at the sensor and controller sides. In [19], an additive watermarking scheme was presented to detect replay attacks, where a watermarking noise was injected into actuators, and thus there exists the same drawback as in [17]. In [20], a multiplicative watermarking scheme was designed, which included a watermark generator at the sensor side and an equalizing filter at the controller side. Although this watermarking scheme can overcome the drawback of the method in [19], it increased the complexity of the system operation.

In view of the analysis above, the coding scheme is relatively simple and easy to implement compared with the watermarking scheme. Therefore, a novel output coding based

detection scheme for replay attacks is proposed in this brief, which codes the measurement output with the control input at the plant side. Compared with [17] and [18], the main advantages of the proposed scheme are summarized as follows: 1) the system performance is not affected in the normal situation where there are no replay attacks and 2) the encoded measurement output is directly employed in the estimator instead of establishing a specific decoder to decode it.

Notation: Throughout this brief, $\mathbb{R}^n$ is the n-dimensional Euclidean space. $X \geq 0$ and $X > 0$ denote a positive semi-definite matrix and a positive definite matrix, respectively. X^T is the transpose of X. $\mathcal{N}(\mu, \Sigma)$ stands for a Gaussian distribution with the mean μ and the covariance matrix Σ. $\mathbb{E}\{X\}$ represents the expectation of a random variable X. I_m is an m-dimensional identity matrix.

II. Problem Formulation

A. System Model

Consider a linear discrete-time system described by

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

$$y(k) = Cx(k) + \nu(k), \tag{2}$$

where $x(k) \in \mathbb{R}^n$, $y(k) \in \mathbb{R}^m$, and $u(k) \in \mathbb{R}^l$ are the system state, measurement output, and control input, respectively; and $\omega(k) \in \mathbb{R}^n$ and $\nu(k) \in \mathbb{R}^m$ denote process noise and measurement noise, which are zero-mean i.i.d Gaussian noises with covariance matrices $Q \geq 0$ and $R > 0$, respectively. The initial state $x(0) \sim \mathcal{N}(0, \Pi_0)$ with $\Pi_0 \geq 0$, which is independent of $\omega(k)$ and $\nu(k)$ for all $k \geq 0$. It is assumed that (A, C) is observable, (A, B) is controllable, and the system operates in a steady state during the attack.

B. Control Law Based on Kalman Filter

To estimate the system state, the following Kalman filter is employed:

$$\hat{x}(k+1|k) = A\hat{x}(k) + Bu(k), \tag{3}$$

$$\hat{x}(k) = \hat{x}(k|k-1) + K\big(y(k) - C\hat{x}(k|k-1)\big), \tag{4}$$

where $\hat{x}(k|k-1)$ and $\hat{x}(k)$ are the *a priori* and *a posteriori* estimates of the state $x(k)$, and the Kalman filter gain matrix satisfies

$$K \triangleq PC^T(CPC^T + R)^{-1}, \tag{5}$$

where $P \geq 0$ is the unique solution of $X = AXA^T + Q - AXC^T(CXC^T + R)^{-1}CXA^T$. Then a state feedback control law is designed as

$$u(k) = L\hat{x}(k), \tag{6}$$

where L is the controller gain.

Remark 1: Due to the presence of the process and measurement noises, the Kalman filter in (3) and (4) is utilized to estimate the system state. Then based on the state estimate, the control law (6) is performed. To ensure the resulting closed-loop system stable, it is needed that the matrices $A + BL$ and $(I - KC)A$ are stable.

C. Anomaly Detector

To monitor the operation state of the system, a residual-based χ^2 detector, which is widely used to detect system anomalies [21], [22], is incorporated at the controller side.

Define the output residual

$$z(k) \triangleq y(k) - C\hat{x}(k|k-1), \tag{7}$$

and the residual covariance satisfies

$$\Sigma_z \triangleq \lim_{k \to +\infty} \mathbb{E}\{z(k)z(k)^T\} = CPC^T + R. \tag{8}$$

The detection criterion is given in the following form:

$$g(k) = \sum_{i=k-J+1}^{k} z(i)^T \Sigma_z^{-1} z(i) \underset{H_1}{\overset{H_0}{\lessgtr}} \tau, \tag{9}$$

where J is the window size of detection, and τ is the threshold. If $g(k)$ is greater than τ, the detector triggers an alarm.

Remark 2: It is known that $g(k)$ in (9) follows a χ^2 distribution with mJ degrees of freedom. The null hypotheses H_0 means that the system is operating normally, while the alternative hypotheses H_1 denotes that the system is under attack. The selection condition of the threshold τ subject to the false alarm rate (FAR) is given as follows:

$$\tau \geq \chi_\alpha, \tag{10}$$

where α is the upper bound of FAR.

D. Replay Attack

It is assumed that the attacker starts to record measurement data at time $k - D$, meanwhile replaying those recorded data into the feedback channel instead of current data at time k. The recorded data sequence is denoted as $Y_D \triangleq \{y(k-D), y(k-D+1), \ldots, y(k-1)\}$, where D denotes the length of Y_D.

Define

$$y'(k) \triangleq y(k-D), \tag{11}$$

and the replay attack model is

$$y^a(k) = y'(k). \tag{12}$$

Remark 3: From [17, Th. 2], under the replay attack (12), the residual of the compromised system is

$$z^a(k) = z(k-D) - C(A+BL)\mathscr{A}^{k-1}\Delta\hat{x}^a(0), \tag{13}$$

where $\mathscr{A} \triangleq (I - KC)(A + BL)$, and $\Delta\hat{x}^a(0) = \hat{x}^a(0) - \hat{x}(0-D)$. If the matrix $\mathscr{A}$ is stable, $z^a(k)$ will converge to $z(k-D)$ that is the residual of the normal system. This implies that the detector (9) cannot detect the replay attack.

From the above discussions, the main work in this study is that an output-coding-based detection scheme is designed to achieve two objects: 1) detect the replay attacks and 2) ensure the normal system performance when no replay attacks occur.

III. Design of Attack Detection Scheme

In this section, a detection scheme based output coding is proposed in detail for replay attacks, as shown in Fig. 1.

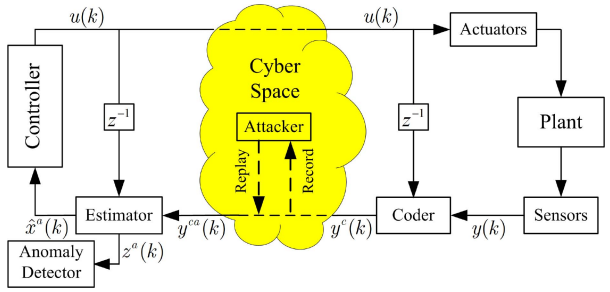

Fig. 1. A Closed-loop CPS under replay attacks.

A. Coding Scheme

At the plant side, the measurement output is encoded as

$$y^c(k) = y(k) + C\Gamma u(k-1), \tag{14}$$

where Γ is the coding matrix to be designed, which is transmitted to the controller side through networks.

When the encoded measurement output $y^c(k)$ is received at the controller side, it is directly employed to estimate the system state using the same coding matrix Γ as in (14) by the following Kalman filter:

$$\hat{x}(k+1|k) = A\hat{x}(k) + Bu(k), \tag{15}$$
$$\hat{y}^c(k|k-1) = C\hat{x}(k|k-1) + C\Gamma u(k-1), \tag{16}$$
$$\hat{x}(k) = \hat{x}(k|k-1) + K\big(y^c(k) - \hat{y}^c(k|k-1)\big). \tag{17}$$

Then, the residual $z^c(k)$ under this coding scheme is obtained as

$$\begin{aligned} z^c(k) &= y^c(k) - \hat{y}^c(k|k-1) \\ &= y(k) + C\Gamma u(k-1) - (C\hat{x}(k|k-1) + C\Gamma u(k-1)) \\ &= z(k). \end{aligned} \tag{18}$$

Remark 4: To detect the replay attack, a Gaussian noise was encoded into the control input $u(k)$ in [17]. As a result, even for a normal system without replay attacks, the control performance would be degraded. Moreover, the actuator would be further burdened with more frequent actions. In addition, for the stochastic coding detection scheme proposed in [18], two random signal generators were established at the plant and controller sides, respectively, and further, the two generators needed a specific mechanism to generate the same random coding signal to encode and decode the measurement output at each time instant. However, the proposed coding detection scheme uses the same coding matrix at the plant and controller sides, which thus is easy to implement for CPSs in practice. Furthermore, it can be found that with (14) and (16), the Eqs. (15) and (17) are the same as (3) and (4), respectively, which implies that for a normal system without replay attacks, the control performance will not be affected.

B. Design of Coding Matrix Γ

Under the coding scheme (14), the corresponding attack signal (12) becomes

$$y^{ca}(k) = y^{c\prime}(k), \tag{19}$$

where $y^{c\prime}(k) = y'(k) + C\Gamma u'(k-1)$ denotes the data recorded by the attacker.

In this brief, for the theoretical analysis, the recorded data sequence Y_D can be regarded as the output of a virtual system with the same parameters as the normal system. The virtual system is described by

$$x'(k+1) = Ax'(k) + Bu'(k) + \omega'(k), \tag{20}$$
$$y^{c\prime}(k) = Cx'(k) + v'(k) + C\Gamma u'(k-1), \tag{21}$$

where $x'(k) \triangleq x(k-D)$, $u'(k) \triangleq u(k-D)$, $\omega'(k) \triangleq \omega'(k-D)$, and $v'(k) \triangleq v(k-D)$.

The corresponding Kalman filter satisfies

$$\hat{x}'(k+1|k) = A\hat{x}'(k) + Bu'(k), \tag{22}$$
$$\hat{y}^{c\prime}(k|k-1) = C\hat{x}'(k|k-1) + C\Gamma u'(k-1), \tag{23}$$
$$\hat{x}'(k) = \hat{x}'(k|k-1) + K(y^{c\prime}(k) - \hat{y}^{c\prime}(k|k-1)), \tag{24}$$

and the corresponding control law is

$$u'(k) = L\hat{x}'(k). \tag{25}$$

With (21) and (23), the residual in the virtual system is

$$\begin{aligned} z^{c\prime}(k) &= y^{c\prime}(k) - \hat{y}^{c\prime}(k|k-1) \\ &= z'(k) \\ &= z(k-D). \end{aligned} \tag{26}$$

Remark 5: From (26), it is obvious that the residual $z^{c\prime}(k)$ in the virtual system follows the same distribution as that of the residual $z(k)$ in the normal system, except a D-step shift backward.

Under the replay attack (19), the coded prediction output in the compromised system is given as

$$\hat{x}^a(k+1|k) = A\hat{x}^a(k) + Bu^a(k), \tag{27}$$
$$\hat{y}^{ca}(k|k-1) = C\hat{x}^a(k|k-1) + C\Gamma u^a(k-1), \tag{28}$$
$$\hat{x}^a(k) = \hat{x}^a(k|k-1) + K(y^{ca}(k) - \hat{y}^{ca}(k|k-1)), \tag{29}$$

where $u^a(k) = L\hat{x}^a(k)$.

Then, combining (19), (23) and (28), the residual in the compromised system is

$$\begin{aligned} z^{ca}(k) &= y^{ca}(k) - \hat{y}^{ca}(k|k-1) \\ &= (y^{c\prime}(k) - \hat{y}^{c\prime}(k|k-1)) - (\hat{y}^{ca}(k|k-1) - \hat{y}^{c\prime}(k|k-1)) \\ &= z'(k) - C[(\hat{x}^a(k|k-1) - \hat{x}'(k|k-1)) \\ &\qquad + \Gamma(u^a(k-1) - u'(k-1))] \\ &= z'(k) - C(A + BL + \Gamma L)(\hat{x}^a(k-1) - \hat{x}'(k-1)) \\ &= z'(k) - C\mathscr{C}\Delta\hat{x}^a(k-1), \end{aligned} \tag{30}$$

where $\mathscr{C} \triangleq A + BL + \Gamma L$, and $\Delta\hat{x}^a(k) \triangleq \hat{x}^a(k) - \hat{x}'(k)$.

Theorem 1: For the system in (1) and (2), using the detection criterion (9) and the coding scheme (14), if the coding matrix Γ is designed to make the matrix

$$\mathscr{B} \triangleq (I - KC)(A + BL) - KC\Gamma L \tag{31}$$

unstable, the replay attack (19) can be detected successfully; otherwise, it cannot be detected.

Proof: Substituting (27) and (28) into (29) yields

$$\begin{aligned} \hat{x}^a(k) &= \hat{x}^a(k|k-1) + K(y^{ca}(k) - \hat{y}^{ca}(k|k-1)) \\ &= (I - KC)\hat{x}^a(k|k-1) - KC\Gamma u^a(k-1) + Ky^{ca}(k) \end{aligned}$$

$$= [(I - KC)(A + BL) - KC\Gamma L]\hat{x}^a(k-1) + Ky^{c\prime}(k)$$
$$= \mathscr{B}\hat{x}^a(k-1) + Ky^{c\prime}(k). \quad (32)$$

With (22)-(24), a similar equation to (32) is also obtained for $\hat{x}'(k)$ as follows:

$$\hat{x}'(k) = \hat{x}'(k|k-1) + K(y^{c\prime}(k) - \hat{y}^{c\prime}(k|k-1))$$
$$= \mathscr{B}\hat{x}'(k-1) + Ky^{c\prime}(k). \quad (33)$$

Subtracting (33) from (32) gives

$$\Delta\hat{x}^a(k) \triangleq \hat{x}^a(k) - \hat{x}'(k)$$
$$= (\mathscr{B}\hat{x}^a(k-1) + Ky^{c\prime}) - (\mathscr{B}\hat{x}'(k-1) + Ky^{c\prime})$$
$$= \mathscr{B}\Delta\hat{x}^a(k-1)$$
$$= \mathscr{B}^k\Delta\hat{x}^a(0), \quad (34)$$

where $\Delta\hat{x}^a(0) = \hat{x}^a(0) - \hat{x}'(0)$. $\hat{x}^a(0)$ denotes the state estimate at the instant that replay attacks are launched, and $\hat{x}'(0) = \hat{x}(-D)$ is the state estimate at the past D instant. Generally, $\hat{x}^a(0)$ is not equal to $\hat{x}(-D)$. That is, $\Delta\hat{x}^a(0) \neq 0$.

Substituting (34) into (30) yields

$$z^{ca}(k) = z'(k) - C\mathscr{C}\mathscr{B}^{k-1}\Delta\hat{x}^a(0). \quad (35)$$

If the matrix $\mathscr{B}$ is unstable, the last term of (35) will diverge, which leads to

$$\lim_{k\to+\infty} g^{ca}(k) = \lim_{k\to+\infty} \sum_{i=k-J+1}^{k} z^{ca}(i)^T \Sigma_z^{-1} z^{ca}(i)$$
$$= +\infty. \quad (36)$$

From (36), it is clear that the replay attack can be detected successfully.

If $\mathscr{B}$ is stable, the last term of (35) will tend to zero, and it is obtained from (35) that

$$\lim_{k\to+\infty} z^{ca}(k) = z'(k), \quad (37)$$

and with (26), the detection criterion (36) becomes

$$\lim_{k\to+\infty} g^{ca}(k) = \lim_{k\to+\infty} \sum_{i=k-J+1}^{k} z'(i)^T \Sigma_z^{-1} z'(i)$$
$$= \lim_{k\to+\infty} \sum_{i=k-D-J+1}^{k-D} z(i)^T \Sigma_z^{-1} z(i), \quad (38)$$

which indicates that the replay attack (19) cannot be detected. The proof is completed. ■

IV. Simulation Results

To verify the effectiveness of the proposed attack detection scheme, the servo motor system (SMS) in [9] is considered for simulation study. The output and input of the SMS are angle position and input voltage, respectively. For the sampling period 0.04s, its model is in form of (1) and (2) with parameters

$$A = \begin{bmatrix} 1.2998 & -0.4341 & 0.1343 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$
$$C = \begin{bmatrix} 3.5629 & 2.7739 & 1.0121 \end{bmatrix}.$$

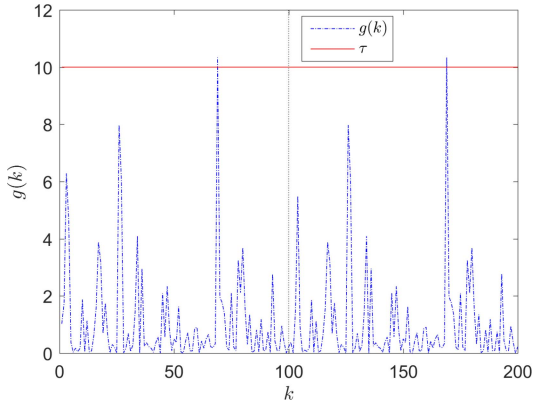

Fig. 2. Simulation result for the coding scheme with a stable $\mathscr{B}$.

The covariances of process noise $\omega(k)$ and measurement noise $\nu(k)$ are given as

$$Q = 0.0001I_3, \quad R = 0.01.$$

Using (5), the Kalman filter gain K is calculated as

$$K = \begin{bmatrix} 0.0896 \\ 0.0764 \\ 0.0251 \end{bmatrix},$$

and the controller gain L is set as

$$L = \begin{bmatrix} -1.1573 & 0.5689 & -0.0950 \end{bmatrix}.$$

The upper bound of FAR and the detection threshold are chosen as $\alpha = 1.0\%$ and $\tau = 10$, respectively. Suppose that the attacker injects replay attacks at the time interval $k \in [100, 200]$. Two simulation cases are conducted: 1) the coding scheme with a stable matrix $\mathscr{B}$, and 2) the coding scheme with an unstable matrix $\mathscr{B}$.

A. $\mathscr{B}$ Is Stable

The coding matrix is chosen as

$$\Gamma = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T.$$

Then the matrix $\mathscr{B}$ is

$$\mathscr{B} = \begin{bmatrix} 0.6106 & -0.3736 & 0.0893 \\ 1.3988 & -0.4331 & 0.0426 \\ 0.1310 & 0.8578 & 0.0140 \end{bmatrix},$$

whose eigenvalues are

$$\text{eig}(\mathscr{B}) = \{0.3448, \quad -0.0767 \pm 0.5093\text{i}\}.$$

It is obvious that all eigenvalues of matrix $\mathscr{B}$ are within the unit circle, i.e., the matrix $\mathscr{B}$ is stable. The simulation result is shown in Fig. 2, which indicates that the detection criterion $g(k)$ of the compromised system is almost lower than the threshold τ under the FAR 1.0% during the attack time interval $k \in [100, 200]$. This means that the replay attack keeps stealthy when the matrix $\mathscr{B}$ is stable.

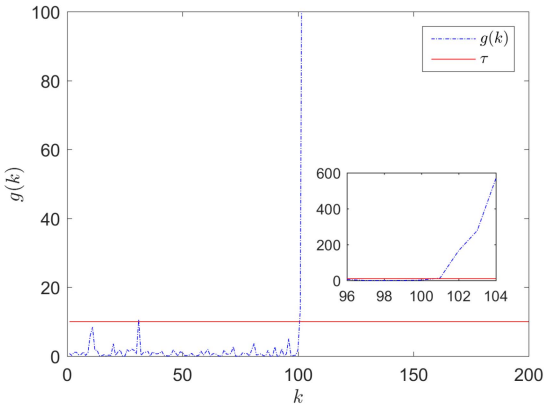

Fig. 3. Simulation result for the coding scheme with an unstable $\mathscr{B}$.

B. $\mathscr{B}$ Is Unstable

In this simulation case, the coding matrix is set to be

$$\Gamma = \begin{bmatrix} 5 & 5 & 5 \end{bmatrix}^T,$$

and the matrix $\mathscr{B}$ is

$$\mathscr{B} = \begin{bmatrix} 3.6594 & -1.8723 & 0.3395 \\ 3.9962 & -1.7099 & 0.2557 \\ 0.9839 & 0.4385 & 0.0840 \end{bmatrix}.$$

The eigenvalues of matrix $\mathscr{B}$ are

$$\text{eig}(\mathscr{B}) = \{1.5950,\ 0.2192 \pm 0.4415\text{i}\},$$

which reveals that the matrix $\mathscr{B}$ is unstable. The simulation result is shown in Fig. 3. It can be seen that the detection criterion $g(k)$ of the compromised system becomes greater than the threshold τ after replay attacks are launched. That is, the proposed coding scheme can assist the anomaly detector to expose the replay attack successfully when the coding matrix Γ is chosen to make matrix $\mathscr{B}$ unstable. Furthermore, the controller gain L and the filter gain K are unchanged, which means that the proposed attack detection method can ensure the system performance in the normal situation.

V. Conclusion

This brief has investigated the detection problem of replay attacks in cyber-physical systems. An output-coding-based detection scheme, which codes the measurement output with the control input, has been proposed to detect the replay attacks. Through the theoretical analysis, the design principle of the coding matrix has been derived. Moreover, under the proposed attack detection scheme, the encoded output is directly utilized to estimate the system state in the remote controller, which can ensure the normal system performance when there is no replay attack. Finally, two cases of simulation results have been given to demonstrate the effectiveness of the proposed scheme.

It is noted that only the detection problem of replay attacks has been addressed for CPSs. As mentioned in [17], the only possible way to counter such an attack is to detect it when occurring. How to eliminate adverse effects of replay attacks is a very challenging problem, and there has been no relevant work addressing it to the best knowledge of authors. However, this is an interesting and practically important topic, which is worth exploring deeply in our future work by using, for example, time-delay system approach and optimization algorithms [23], [24].

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.
[2] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, Apr. 2019.
[3] S. Xu, Y. Xia, and H.-L. Shen, "Analysis of malware-induced cyber attacks in cyber-physical power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 12, pp. 3482–3486, Dec. 2020.
[4] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[5] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.
[6] J. Zhou, J. Shang, Y. Li, and T. Chen, "Optimal DoS attack against LQR control channels," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, early access, Oct. 1, 2020, doi: 10.1109/TCSII.2020.3028105.
[7] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, no. 89, pp. 117–124, 2018.
[8] Y.-G. Li and G. H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Inf. Sci.*, vol. 481, pp. 474–490, May 2019.
[9] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, May 2016.
[10] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3302–3312, Dec. 2018.
[11] G. Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3919–3926, Sep. 2020.
[12] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.
[13] Z.-H. Pang, L.-Z. Fan, J. Sun, K. Liu, and G.-P. Liu, "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Inf. Sci.*, vol. 546, pp. 192–205, Feb. 2021.
[14] L. Gao, B. Chen, and L. Yu, "Fusion-based FDI attack detection in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 8, pp. 1487–1491, Aug. 2020.
[15] Y. Li, L. Shi, and T. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 846–856, Sep. 2018.
[16] Z. Guo, D. Shi, D. E. Quevedo, and L. Shi, "Secure state estimation against integrity attacks: A Gaussian mixture model approach," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 194–207, Jan. 2019.
[17] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.
[18] D. Ye, T.-Y. Zhang, and G. Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack," *Inf. Sci.*, vol. 481, pp. 432–444, May 2019.
[19] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 93–109, Feb. 2015.
[20] R. M. G. Ferrari and A. M. H. Teixeira, "Detection and isolation of replay attacks through sensor watermarking," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7363–7368, 2017.
[21] R. K. Mehra and J. Peschon, "An innovations approach to fault detection and diagnosis in dynamic systems," *Automatica*, vol. 7, no. 5, pp. 637–640, 1971.
[22] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, no. 6, pp. 601–611, 1976.
[23] K. Liu, A. Selivanov, and E. Fridman, "Survey on time-delay approach to networked control," *Annu. Rev. Control*, vol. 48, pp. 57–79, Jul. 2019.
[24] A. H. Khan, X. Cao, S. Li, V. N. Katsikis, and L. Liao, "BAS-ADAM: An ADAM based approach to improve the performance of beetle antennae search optimizer," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 461–471, Mar. 2020.