Secure Adaptive-Event-Triggered Filter Design With Input Constraint and Hybrid Cyber Attack

Jinliang Liu, *Member, IEEE*, Yuda Wang, Jinde Cao, *Fellow, IEEE*, Dong Yue, *Senior Member, IEEE*, and Xiangpeng Xie, *Member, IEEE*

***Abstract*—The problem of secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack is investigated in this article. First, a new model of hybrid cyber attack, which considers a deception attack, a replay attack, and a denial-of-service (DoS) attack, is established for filter design. Second, an adaptive event-triggered scheme is applied to the filter design to save the limited communication resource. In addition, a novel adaptive-event-triggered filtering error model is established with the consideration of hybrid cyber attack and input constraint. Moreover, based on the Lyapunov stability theory and linear matrix inequality technique, sufficient conditions are obtained to guarantee the augmented system stability, and the parameters of the designed filter are presented with explicit forms. Finally, the proposed method is validated by simulation examples.**

***Index Terms*—Adaptive event-triggered scheme, deception attacks, denial-of-service (DoS) attacks, hybrid cyber attack, secure filtering.**

I. Introduction

AS A CLOSED-LOOP feedback control system, the networked control system (NCS) uses a communication network to exchange the measured signals. It has the advantages of convenient information resource sharing, fewer connections, simple installation and maintenance, low cost, etc. Because of the above advantages, networked systems can solve problems that traditional control systems cannot solve, such as multiagent [1]–[3]; remote control of teleoperation robots [4], [5]; and other fields [6]–[8] in harsh environments. That is why scholars pay so much attention to the relevant control areas of NCSs [9], [10]. Presently, the main research contents of networked systems include transmission mechanism design, security control and filtering, input and output constraints, etc. In practical applications, due to the influence of material quality and external environment, if the input or output of components exceeds a certain limit, it may cause component damage, system performance reduction, or even instability. Therefore, considering input constraint can protect components and maintain good performance of the system to a large extent. In view of this, the problem of state restriction has attracted much attention from scholars [11]–[14].

The introduction of the network brings many benefits to a control system, which makes networked systems a research hotspot. However, with the introduction of the network, the problem of network resource constraints caused by hardware and technology comes along. If the system runs smoothly, abundant unnecessary sampled data enter the network, thus wasting limited network resources. In order to solve this problem, the event-triggered scheme has been proposed which only allows data to be transmitted when the trigger condition is satisfied. Under this scheme, the transmission frequency of sampled data is reduced, which can save the network resources effectively. In view of this, the event-triggered scheme is widely studied [15]–[20]. For instance, Yue *et al.* [17] proposed a new event-triggered scheme, in which the implementation of the event generator only requires supervision of state. Considering the merits and drawbacks of the time-triggered and event-triggered mechanisms, a hybrid-triggered scheme is studied in [21]–[23]. Due to the triggering condition of the event-triggered scheme is preset, it cannot adapt to the changing system conditions. In view of this, an adaptive event-triggered scheme is first proposed for nonlinear networked interconnected control systems in [24], which can dynamically change triggering conditions rather than presupposing triggering conditions. Afterward, an adaptive event-triggered scheme and its application have been widely studied, and many achievements have been obtained [25]–[30].

With the in-depth application of networked systems, not only the problem of resource constraints has been studied but also the problem of security has attracted a lot of attention. According to the different attack targets, there are sensor attack [31], actuator attack [32], network attack [33], and so on. In recent years, the network attack has been a hot topic of research. There are several kinds of common

Manuscript received July 15, 2019; revised March 24, 2020; accepted June 14, 2020. Date of publication July 13, 2020; date of current version August 4, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61973152 and Grant 61903182; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20171481; in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 19KJA510005; and in part by the Qing Lan Project. This article was recommended by Associate Editor J. Qiu. *(Corresponding authors: Jinliang Liu; Dong Yue.)*

Jinliang Liu and Yuda Wang are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: liujinliang@vip.163.com; wangyd1996@163.com).

Jinde Cao is with the School of Mathematics, Southeast University, Nanjing 210096, China, and also with the Research Center for Complex Systems and Network Sciences, Southeast University, Nanjing 210096, China (e-mail: jdcao@seu.edu.cn).

Dong Yue and Xiangpeng Xie are with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: medongy@vip.163.com; xiexiangpeng1953@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2020.3003752.

Digital Object Identifier 10.1109/TCYB.2020.3003752

cyber attacks, such as deception [34]–[36], replay [37]–[39], denial-of-service (DoS) attack [40], etc. The deception attack, as the most common attack, usually replaces the real data of the system with carefully forged data to achieve certain purposes of the attacker. Another common cyber attack is the replay attack, which maliciously reproduces transmitted data to influence system operation. In addition, DoS attacks can also have a great impact on the system. Attackers prevent measurements from reaching their destination by executing DoS attacks, which can pose a huge threat to the system. However, it should be pointed out that although a lot of research has been done on network attacks, few studies have considered multiple attacks at the same time.

Taking the effects of the deception attack into account, Ding *et al.* [35] investigated the security control problem for a stochastic nonlinear system. In [39], the resilient networked control systems subject to replay attacks were studied. With the consideration of nonperiodic DoS attacks, the resilient event-based controller design for NCSs was investigated in [40]. However, it should be pointed out that although a lot of results like [35], [39], and [40] have been done on network attacks, few studies have considered multiple attacks. Inspired by that, a hybrid cyber attack is considered in this article, which contains deception, replay, and DoS attacks at the same time. Moreover, in order to better solve the problem of resource constraints, an adaptive event-triggered scheme is proposed and introduced into the NCS based on the scheme in [17]. As far as we know, although there exist some research results on event-triggered control and estimation, few results consider the impacts of network attacks and input constraints on the system. The innovation points of this article are summarized as follows.

1) Different from the existing literature, a novel unified model of hybrid attacks is first proposed, which considers deception, replay, and DoS attacks at the same time.
2) Based on the event-triggered scheme, a novel adaptive event-triggered filtering error model is first established with the consideration of a hybrid cyber attack and input constraint.
3) Based on the above error system model, the problem of filter design for networked systems with a hybrid cyber attack and input constraint is studied for the first time.

The structure of this article is organized as follows. By considering the influence of the hybrid cyber attack and introducing an adaptive event-triggered scheme, a filtering error system model is established in Section II. In Section III, based on the Lyapunov stability theory, a secure adaptive-event-triggered filter is designed. Then, the designed filter performance is validated by an illustrative example in Section IV. The conclusion is provided in Section V.

Notation: Throughout this article, $\mathbb{R}_n$ denotes the n-dimensional Euclidean space; S^{T} stands for transpose of matrix S; for real matrix S, $S > 0$ means that S is a real symmetric positive-definite matrix; 0 and I represent the zero matrix and identity matrix with compatible dimensions, respectively; and $(*)$ stands for a term that is induced by symmetry.

II. System Modeling

In this article, a secure adaptive-event-triggered filtering problem with input constraint and hybrid cyber attack is investigated. Consider the following linear system:

$$\begin{cases} \dot{x}(t) = Ax(t) + B\omega(t) \\ y(t) = Cx(t) \\ z(t) = Lx(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}_n$ is the state vector, $z(t)$ is the output vector to be estimated, $\omega(t)$ represents the external disturbance, and $y(t)$ is the measurement of the sensor. Matrices A, B, C, and L are constant matrices.

The purpose of this article is to design the following filter:

$$\begin{cases} \dot{x}_f(t) = A_f x_f(t) + B_f \tilde{y}(t) \\ z_f(t) = C_f x_f(t) \end{cases} \tag{2}$$

where $x_f(t)$ is the filter state; $\tilde{y}(t)$ is the real input of the filter; and $z_f(t)$ is the estimation of $z(t)$. A_f, B_f, and C_f are the parameter matrices of the filter to be designed.

As we all know, the state information of plant is measured by a sensor. However, due to the influence of its own hardware and environment, data transmitted by the sensor is often limited. In this article, the following restriction function is considered:

$$\bar{y}(t) = \begin{cases} y_{\max}, & \text{if } y(t) > y_{\max} \\ y(t), & \text{if } -y_{\max} \le y(t) \le y_{\max} \\ -y_{\max}, & \text{if } y(t) < -y_{\max}. \end{cases} \tag{3}$$

Then, similar to [23], the signal can be separated as

$$\bar{y}(t) = y(t) - \varrho(y(t)) \tag{4}$$

where the nonlinear function $\varrho(y(t))$ satisfies the following condition for $\mu \in (0, 1)$:

$$\mu y^{\mathrm{T}}(t) y(t) \ge \varrho^{\mathrm{T}}(y(t)) \varrho(y(t)). \tag{5}$$

Remark 1: In practical applications, there always exists constraint of the input and output signals by the influence of hardware materials and environment. If the input or output exceeds a certain limit, it will cause damage to the components themselves and influence the system performance. To avoid that, a kind of secure adaptive-event-triggered filter with input constraint is designed in this article.

By taking the limited network resources into account, inspired by [24], an adaptive event-triggered scheme is adopted to solve resource constraints. Under this scheme, the triggering instants are as follows:

$$\begin{aligned} t_{k+1}h = t_k h + \inf_{q \ge 1} \big\{ & qh | e^{\mathrm{T}}(t_k h) \Omega e(t_k h) \\ & - \phi(t) y^{\mathrm{T}}\big(t_k^q h\big) \Omega y\big(t_k^q h\big) \ge 0 \big\} \end{aligned} \tag{6}$$

where $t_k h$ represents the triggering instant; h represents the sampling period; Ω is a weight of triggering condition; $t_k^q h = t_k h + qh$; $e(t_k h) = y(t_k h) - y(t_k h + qh)$ represents the threshold error; $q = 1, 2, \ldots$, and $\phi(t)$ is a triggering parameter satisfying the following adaptive law:

$$\dot{\phi}(t) = \frac{\eta}{\phi(t)} \left(\frac{1}{\phi(t)} - \pi \right) e^{\mathrm{T}}(t) \Omega e(t) \tag{7}$$

with $\eta > 0$, $\pi > 0$, and $0 < \phi(t) \le 1$.

Remark 2: Considering that the existing event-triggered scheme cannot well meet the needs of rapidly changing systems, an adaptive event-triggered scheme which is determined by a varying threshold $\phi(t)$ is introduced. It can adjust the release frequency by changing the threshold parameter under the adaptive law (7). Moreover, when the system is stable, according to the adaptive law (7), $\phi(t)$ will maintain a constant which means it turns to the traditional event-triggered scheme. Particularly, if $\phi(t) \equiv 0$, the adaptive event-triggered scheme turns to the time-triggered scheme.

Remark 3: It can be seen from the adaptive triggering condition in (6) that the trigger parameter is not a preset constant as traditional ones. Instead, it satisfies an adaptive law in (7), which depends on the state error of the latest data and present data. In this case, measurements can be more reasonably transmitted in the network.

Remark 4: If set $\eta = 0$ in (7), then $\dot{\phi}(t) = 0$, the triggering instants in (6) can be changed as

$$t_{k+1}h = t_k h + \inf_{q\geq 1}\{qh | e^{\mathrm{T}}(t_k h)\Omega e(t_k h) - \bar{\phi} y^{\mathrm{T}}(t_k^q h)\Omega y(t_k^q h) \geq 0\}$$

where $0 < \bar{\phi} \leq 1$. That means the adaptive triggering condition reduces to the conventional ones (such as in [17] and [18]).

Similar to the analysis in [17], the interval $[t_k h+\mu_{t_k}, t_{k+1}h+\mu_{t_{k+1}})$ can be divided into several subintervals, which can be expressed as $[t_k h+\mu_{t_k}, t_{k+1}h+\mu_{t_{k+1}}) = \bigcup_{j=0}^{\theta}[t_k^j h+\mu_{t_k}, t_k^j h+h+\mu_{t_{k+1}})$. μ_{t_k} are the corresponding network-induced delay, and $\theta = t_{k+1} - t_k - 1$. Define $d(t) = t - t_k^q h$, and it is easy to get the range of $d(t)$ as $0 \leq \mu_{t_k} \leq d(t) \leq h + d_{t_{k+q+1}} \triangleq d_M$.

Then, the signal transmitted to network can be expressed as

$$\hat{y}(t) = \bar{y}(t - d(t)) + e(t). \tag{8}$$

When the data are transmitted by the network, a deception attack is considered first. It is assumed that the deception attack signal $f(\cdot)$ which satisfies Assumption 1 can completely replace the normal transmission data in this article. In order to show its randomness, a Bernoulli variable $\alpha(t)$ satisfying $\mathbb{E}\{\alpha(t)\} = \bar{\alpha}$ and $\mathbb{E}\{(\alpha(t) - \bar{\alpha})^2\} = \theta_1^2$ is introduced. Then, the data transmitted under the deception attack can be represented as

$$y_1(t) = (1 - \alpha(t))f(y(t - \tau(t))) + \alpha(t)\hat{y}(t) \tag{9}$$

where $\hat{y}(t)$ represents the data transmitted to the network, as defined in (8).

Assumption 1 [23]: For a real constant matrix F, the signal of the deception attack $f(y(t))$ satisfies

$$\|f(y(t))\|_2 \leq \|Fy(t)\|_2. \tag{10}$$

Remark 5: In (9), a nonlinear function is used to represent the deception attack signals and a Bernoulli variable $\alpha(t)$ is utilized to indicate whether the deception attack occurs or not. When $\alpha(t) = 1$, then the deception attack does not occur and the data transmitted is $y_1(t) = \hat{y}(t)$; when $\alpha(t) = 0$, that means the deception attack occurs and the data transmitted are replaced as $y_1(t) = f(y(t - \tau(t)))$.

Then, a replay attack is considered next. When the replay attack occurs, the data transmitted will be replaced by past data. In order to show the uncertainty of attack occurrence, similarly, variable $\beta(t)$ satisfying the Bernoulli distribution is introduced. Then, the signal transmitted in the network can be rewritten as

$$y_2(t) = (1 - \beta(t))y_r(t) + \beta(t)y_1(t) \tag{11}$$

where $y_r(t) = \hat{y}(t - r(t))$ is the replay signal, and $r(t)$ represents that the replayed data are the data transmitted in previous $r(t)$ seconds. $\mathbb{E}\{\beta(t)\} = \bar{\beta}$, $\mathbb{E}\{(\beta(t) - \bar{\beta})^2\} = \theta_2^2$. It should be pointed that the data stolen by attackers are often within a certain period of time, that is, $r(t)$ has an upper bound r_M. Then, we have $0 < r(t) \leq r_M$.

Assumption 2 [41]: The transmission data are assumed to be stored from instant t_0 to current instant t, and then the data of an arbitrary instant from the sequence are selected for replay.

Finally, a DoS attack is taken into consideration when the communication network transmits the measurement signals. When the DoS attack is active, no signal can be transmitted to the filter; when the DoS attack is sleeping, the signal is transmitted to the filter normally. In view of this, the data transmitted suffering the DoS attack can be represented as

$$y_3(t) = \begin{cases} y_2(t), & t \in [a_n, l_n) \\ 0, & t \in [l_n, a_{n+1}) \end{cases} \tag{12}$$

where a_n is used to represent the start time of the DoS attack when it enters sleeping for the nth time. s_n indicates the duration of the nth sleeping. l_n is the ending instant of the nth sleeping, that is, $l_n = a_n + s_n$. The condition $0 \leq a_0 < a_1 < l_1 < a_2 < l_2 < \cdots < l_n$ is satisfied.

Assumption 3 [42]: Assume that there exist uniform bounds on the lengths of the DoS sleeping and active periods, respectively

$$\begin{cases} s_{\min} \leq \inf_{n\in\mathbb{N}}\{s_n\} \\ b_{\max} \geq \sup_{n\in\mathbb{N}}\{a_n - l_{n-1}\}. \end{cases} \tag{13}$$

Assumption 4 [43]: Define $l(t)$ as the number of DoS attack sleep/active transitions during the interval $[0, t)$. For given real number $\nu_1 \geq 0$, $\varpi > h$, the DoS frequency $l(t)$ satisfies the following condition:

$$l(t) \leq \nu_1 + \frac{t}{\varpi}. \tag{14}$$

Combining (9), (11), and (12), the real input of filter can be obtained

$$\tilde{y}(t) = \begin{cases} (1 - \beta(t))y_r(t) + \beta(t)(1 - \alpha(t))f(y(t - \tau(t))) \\ \quad + \alpha(t)\beta(t)\hat{y}(t), & t \in [a_n, l_n) \\ 0, & t \in [l_n, a_{n+1}). \end{cases} \tag{15}$$

Remark 6: In this article, it is assumed that hybrid cyber attacks occur in the following order: deception → replay → DoS attack. In fact, the order of hybrid cyber attacks is uncertain in most cases; however, hybrid cyber attacks in other orders can also be modeled in the similar way described above. In practical applications, we can use the attack detection methods to determine whether the attacks occur and its sequence, and then adjust the corresponding control strategies.

By combining (2), (4), (8), and (15), one can obtain

$$\dot{x}_f(t) = \begin{cases} A_f x_f(t) + B_f\{(1-\beta(t))y_r(t) + (1-\alpha(t))\beta(t) \\ \qquad \times f(y(t-\tau(t))) + \alpha(t)\beta(t) \\ \qquad (Cx(t-d(t)) + e(t) - \varrho(y(t-d(t)))\} \\ \qquad t \in [a_n, l_n) \\ 0, \qquad t \in \big[l_n, a_{n+1}). \end{cases} \tag{16}$$

Define $\xi(t) = \begin{bmatrix} x(t) \\ x_f(t) \end{bmatrix}$, $\bar{z}(t) = z(t) - z_f(t)$, then one can have the filtering error system

$$\begin{cases} \dot{\xi}(t) = \begin{cases} \bar{A}\xi(t) + \bar{B}\omega(t) + (1-\beta(t))\bar{E}H\xi(t-r(t)) \\ + (1-\beta(t))\bar{E}e(t-r(t)) + (1-\alpha(t))\beta(t) \\ \times \bar{E}f(y(t-\tau(t))) + \alpha(t)\beta(t)\bar{C}(H\xi(t-d(t)) + e(t)) \\ - \alpha(t)\beta(t)\bar{E}\varrho(y(t-d(t))), \quad t \in [a_n, l_n) \\ \bar{A}\xi(t) + \bar{B}\omega(t), \qquad\qquad t \in \big[l_n, a_{n+1}) \end{cases} \\ \xi(t) = \varphi(t), \qquad t \in [-h, 0) \\ \bar{z}(t) = \bar{L}\xi(t) \end{cases} \tag{17}$$

where $\bar{A} = \begin{bmatrix} A & 0 \\ 0 & A_f \end{bmatrix}$, $\bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$, $\bar{C} = \begin{bmatrix} 0 \\ B_f C \end{bmatrix}$, $H = \begin{bmatrix} I & 0 \end{bmatrix}$, $\bar{E} = \begin{bmatrix} 0 \\ B_f \end{bmatrix}$, $\bar{L} = \begin{bmatrix} L & -C_f \end{bmatrix}$.

For the convenience of analysis, some lemmas are introduced as follows.

Lemma 1 [21]: For any vectors a, $b \in \mathbb{R}_n$, and positive-definite matrix $S \in \mathbb{R}_{n\times n}$, the following inequality holds:

$$2a^{\mathrm{T}}b \le a^{\mathrm{T}}Sa + b^{\mathrm{T}}S^{-1}b. \tag{18}$$

Lemma 2 [23]: For given positive-definite matrices R, P and scalar γ, the following inequality holds:

$$-PR^{-1}P \le -2\gamma P + \gamma^2 R. \tag{19}$$

III. Main Results

In this section, sufficient conditions to ensure the mean-square exponential stability for system (17) are obtained. Then, on this basis, a filter is designed under an adaptive event-triggered scheme and hybrid attack. The main results are presented as follows.

Theorem 1: For given positive scalars λ_i, ς_i (i=1,2), γ, $\bar{\alpha}$, $\bar{\beta}$, sampling period h, DoS parameters $s_{\min}$, $b_{\max}$, ν_1, ϖ, and matrices F, and filter parameters A_f, B_f, C_f, system (17) is exponentially mean-square stable if there exist $\Omega > 0$, $P_i > 0$, $Q_{i1} > 0$, $R_{i1} > 0$, $Q_{i2} > 0$, $R_{i2} > 0$, $Q_{i3} > 0$, $R_{i3} > 0$, and matrices J_i, M_i, Z_i, N_i, U_i and V_i $(i = 1, 2)$ with appropriate dimensions, such that for $i = 1, 2$, $j = 1, 2, 3$ the following inequalities hold:

$$\Phi_i = \begin{bmatrix} \Upsilon_{i1} & (*) & (*) & (*) \\ \Upsilon_{i2} & \Upsilon_{i3} & (*) & (*) \\ \Upsilon_{i4} & 0 & \Upsilon_{i5} & (*) \\ \Upsilon_{i6} & 0 & 0 & \Upsilon_{i7} \end{bmatrix} < 0 \tag{20}$$

$$\frac{2\varsigma_1 s_{\min} - 2(\varsigma_1+\varsigma_2)h - 2\varsigma_2 b_{\max} - \ln(\lambda_1\lambda_2)}{\varpi} > 0 \tag{21}$$

$$P_1 \le \lambda_2 P_2 \tag{22}$$

$$P_2 \le \lambda_1 e^{2(\varsigma_1+\varsigma_2)h} P_1 \tag{23}$$

$$Q_{ij} \le \lambda_{3-i} Q_{(3-i)j} \tag{24}$$

$$R_{ij} \le \lambda_{3-i} R_{(3-i)j} \tag{25}$$

where the elements of the matrix Φ_i are given in Appendix A.

Proof: See Appendix B. ∎

In Theorem 1, sufficient conditions guaranteeing the exponentially mean-square stability for argument filtering system have been obtained. In the following, an adaptive-event-triggered filter with input constraint and hybrid cyber attack is designed on the basis of Theorem 1.

Theorem 2: For given positive scalars λ_i, ς_i $(i = 1, 2)$, γ, $\bar{\alpha}$, $\bar{\beta}$, sampling period h, DoS parameters $s_{\min}$, $b_{\max}$, ν_1, ϖ, matrices F, system (17) is exponentially mean-square stable if there exist $\hat{A}_f$, $\hat{B}_f$, $\hat{C}_f$, Ω, $P_{i1} > 0$, $\bar{P}_{i3} > 0$, $\hat{Q}_{i1} > 0$, $\hat{R}_{i1} > 0$, $\hat{Q}_{i2} > 0$, $\hat{R}_{i2} > 0$, $\hat{Q}_{i3} > 0$, $\hat{R}_{i3} > 0$, S_i, $\hat{J}_i$, $\hat{M}_i$, $\hat{Z}_i$, $\hat{N}_i$, $\hat{U}_i$ and $\hat{V}_i$ $(i = 1, 2)$ with appropriate dimensions, such that for $i = 1, 2$, $j = 1, 2, 3$ the following linear matrix inequalities and conditions (21)–(23) hold:

$$\hat{\Phi}_i = \begin{bmatrix} \hat{\Upsilon}_{i1} & (*) & (*) & (*) \\ \Upsilon_{i2} & \Upsilon_{i3} & (*) & (*) \\ \hat{\Upsilon}_{i4} & 0 & \hat{\Upsilon}_{i5} & (*) \\ \hat{\Upsilon}_{i6} & 0 & 0 & \hat{\Upsilon}_{i7} \end{bmatrix} < 0 \tag{26}$$

$$P_{i1} - \bar{P}_{i3} > 0 \tag{27}$$

$$S_i \hat{Q}_{ij} S_i^{\mathrm{T}} \le \lambda_{3-i} \hat{Q}_{(3-i)j} \tag{28}$$

$$S_i \hat{R}_{ij} S_i^{\mathrm{T}} \le \lambda_{3-i} \hat{R}_{(3-i)j} \tag{29}$$

where the elements of the matrix $\hat{\Phi}_i$ are given in Appendix C.

Moreover, the parameters of the designed filter can be obtained

$$\begin{cases} A_f = \hat{A}_f \bar{P}_{13}^{-1} \\ B_f = \hat{B}_f \\ C_f = \hat{C}_f \bar{P}_{13}^{-1}. \end{cases} \tag{30}$$

Proof: See Appendix D. ∎

IV. Simulation Examples

In this section, the effectiveness of the designed method is validated by the following examples. A tunnel diode circuit system is considered to prove the effectiveness of the designed filter in Example 1. Moreover, in Example 2, a numerical example is used to demonstrate the effectiveness of the design filter.

Example 1: As shown in Fig. 1, a tunnel diode circuit system is considered, which can be expressed as follows:

$$\begin{cases} C\dot{V}_C(t) = -\frac{V_C(t)}{R_D} + i_L(t) \\ L\dot{i}_L(t) = -V_C(t) - R_E i_L(t) + \omega(t). \end{cases}$$

Let $x(t) = \begin{bmatrix} x_1(t) & x_2(t) \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} V_C(t) & i_L(t) \end{bmatrix}^{\mathrm{T}}$, then the circuit system can be expressed as

$$\dot{x}(t) = \begin{bmatrix} -\frac{1}{CR_D} & -\frac{1}{C} \\ \frac{1}{L} & -\frac{R_E}{L} \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ \frac{1}{L} \end{bmatrix} + \omega(t).$$

Consider the circuit system in Fig. 1 with $C = 2$ F, $R_E = 2\ \Omega$, $L = 1000$ mH, and $R_D = 2\ \Omega$. Set the system parameters to $h = 0.1$ s, $s_{\min} = 2$, $b_{\max} = 3$, $\bar{\alpha} = 0.2$, $\bar{\beta} = 0.3$, $\lambda_1 = \lambda_2 = 1.01$, $\varsigma_1 = 0.46$, $\varsigma_2 = 0.4$, $d_M = 0.1$, $\tau_M = 0.08$, $r_M = 0.11$, $\gamma = 2$, $\mu = 0.16$, and $e_1 = e_2 = 3$.

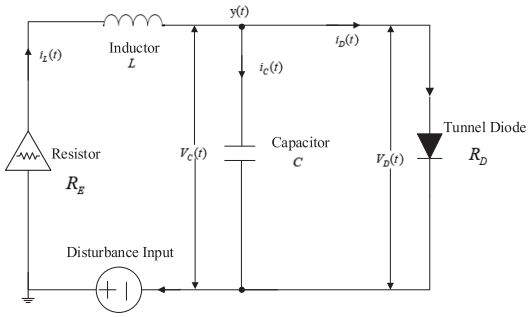


Fig. 1. Structure of the tunnel diode circuit system.

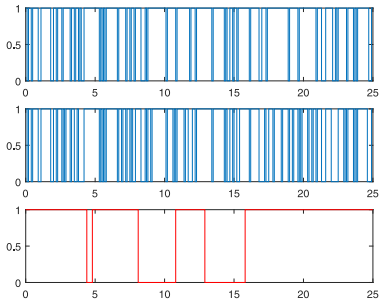
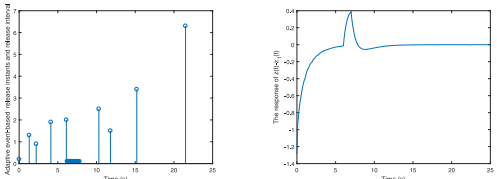


Fig. 2. Occurrence instants of deception, replay, and DoS attacks in Example 1.



(a) (b)

Fig. 3. Release instants, intervals, and filtering error in Example 1. (a) Release instants and intervals. (b) Filtering error.

The disturbance signal is described as

$$\omega(t) = \begin{cases} 1, & 6 \le t \le 7 \\ 0, & \text{else} \end{cases}$$

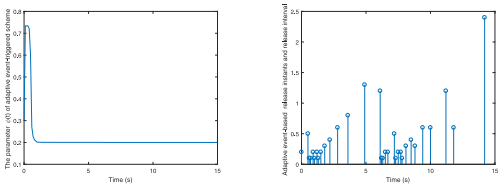
and the deception attack signal is selected as $f(y(t)) = \tanh(0.15y(t))$.

By using Theorem 2, the designed parameters of filter can be acquired

$$\begin{cases} A_f = \begin{bmatrix} -0.0254 & -2.0152 \\ -0.4233 & -26.8053 \end{bmatrix} \\ B_f = \begin{bmatrix} 0.9870 & -0.5781 \end{bmatrix}^{\mathrm{T}} \\ C_f = \begin{bmatrix} -0.0050 & -0.2376 \end{bmatrix}. \end{cases}$$

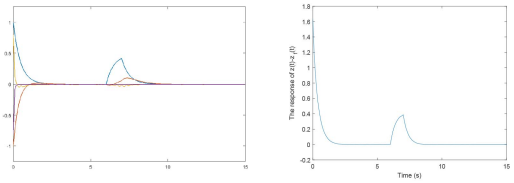
Set the initial condition $x(0) = \begin{bmatrix} 1 & 0.4 \end{bmatrix}^{\mathrm{T}}$, $x_f(0) = \begin{bmatrix} 0.9 & 0.3 \end{bmatrix}^{\mathrm{T}}$, the following figures can be obtained.

Fig. 2 shows the Bernoulli distributed variable for the deception attack, replay attack, and occurrence of DoS attack, respectively. Release instants and intervals under the adaptive event-triggered scheme are shown in Fig. 3(a). Fig. 3(b) shows the filtering error of the filter designed under the adaptive event-triggered scheme and hybrid attack, which illustrates the validity of the designed method.



(a) (b)

Fig. 4. Adaptive event-triggered scheme in Example 2. (a) Parameter $\phi(t)$ of the adaptive event-triggered scheme. (b) Release instants and intervals.



(a) (b)

Fig. 5. $x(t)$, $x_f(t)$, and the filtering error in Example 2. (a) $x(t)$ and $x_f(t)$. (b) Filtering error.

Example 2: The following system (1) is considered:

$$A = \begin{bmatrix} -2.1 & 0.1 \\ 1 & -2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ -0.2 \end{bmatrix}$$
$$C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad L = \begin{bmatrix} 1 & -0.5 \end{bmatrix}.$$

Consider the disturbance signal described as

$$\omega(t) = \begin{cases} 1, & 6 \le t \le 7 \\ 0, & \text{else} \end{cases}$$

and the deception attack signal is selected as

$$f(y(t)) = \tanh(0.15y(t)).$$

Checking Assumption 1, one can see that if the nonlinearity upper bound is $F = 0.15$, the condition (10) is satisfied.

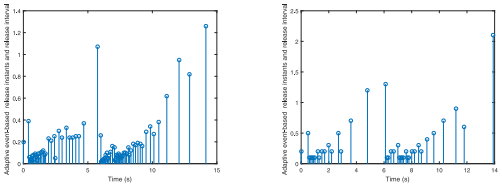
Set the system parameters to $h = 0.1$ s, $s_{\min} = 2$, $b_{\max} = 3$, $\bar{\alpha} = 0.2$, $\bar{\beta} = 0.3$, $\lambda_1 = \lambda_2 = 1.01$, $\varsigma_1 = 0.46$, $\varsigma_2 = 0.4$, $d_M = 0.05$, $\tau_M = 0.08$, $r_M = 0.06$, $\gamma = 2$, $\mu = 0.16$, and $e_1 = e_2 = 3$.

Then, the filter parameters can be acquired by using Theorem 2

$$\begin{cases} \bar{P}_{13} = \begin{bmatrix} 0.9865 & -0.9102 \\ -0.9102 & -2.9232 \end{bmatrix} \\ \hat{A}_f = \begin{bmatrix} -12.6588 & 0.7785 \\ -0.6137 & -14.9601 \end{bmatrix} \\ \hat{B}_f = \begin{bmatrix} -1.2303 & -0.1701 \end{bmatrix}^{\mathrm{T}} \\ \hat{C}_f = \begin{bmatrix} -0.2016 & -0.0466 \end{bmatrix}. \end{cases}$$

The initial condition is assumed that $x(0) = \begin{bmatrix} 1 & -1 \end{bmatrix}^{\mathrm{T}}$, $x_f(0) = \begin{bmatrix} 0.9 & -0.9 \end{bmatrix}^{\mathrm{T}}$, one can obtain the following figures by simulation.

Variations in parameters of the adaptive event triggering mechanism are shown in Fig. 4(a). In Fig. 4(b), release time intervals under the adaptive event-triggered scheme are presented. The filtered signal and actual signal are shown in Fig. 5(a). Moreover, the filtering error when the filter is subjected to the hybrid attack is shown in Fig. 5(b).



(a) (b)

Fig. 6. Release instants and intervals with different sampling period h. (a) Release instants and intervals with $h = 0.01$ s. (b) Release instants and intervals with $h = 0.1$ s.

TABLE I
INFLUENCE OF THE ADAPTIVE PARAMETER π WITH $\phi(0) = 0.4$

π	π=4	π=5	π=9
$\phi(n)$	$\phi(n) \to 0.27$	$\phi(n) \to 0.2$	$\phi(n) \to 0.11$
packages transmitted	$30/151$	$45/151$	$81/151$

From Fig. 4(b), one can see that at the beginning of the system operation, the measurement data are released frequently due to the instability of the system, and the release intervals are small. When the system is stable, the release decreases instantaneously until the disturbance in the 6th second causes the data to be transmitted again frequently. This proves that the adaptive event-triggered scheme can save the communication resources effectively. From Fig. 5(a) and (b), it can be seen that the filter designed is still effective even with disturbance and hybrid attack.

By setting different sampling period h, the data release can be seen in Fig. 6.

It can be seen from Fig. 6 that with the increase of the sampling periods h, the number of data triggered under the same trigger parameter decreases. When the system is stable, the number of data triggered is basically close. Therefore, before the system is stabilized, the larger the sampling period h is, the better the effect of saving network resources will be obtained.

By setting different adaptive parameter π, the data records are obtained in Table I.

It can be seen from Table I that with the increase of the selected value of the adaptive parameter π, the smaller the trigger parameter $\phi(t)$ becomes after the system is stable, and the more packets are transmitted in the network. Therefore, in the actual system, we should set the corresponding adaptive parameters according to the system requirements, in order to achieve the best effect. In addition, it should be noted that when $\pi = 2.5$ and $\phi(n) \equiv 0.4$, the adaptive event-triggered scheme degenerates into the event-triggered scheme.

V. CONCLUSION

The secure adaptive-event-triggered filtering with hybrid cyber attack and input constraint is investigated in this article. To save the limited network and power resources, an adaptive event-triggered scheme is introduced. Then, by taking the influence of the hybrid cyber attack into account, a novel filtering error model with the adaptive event-triggered scheme and input constraint is established. Sufficient conditions to guarantee the system stability is obtained by using the Lyapunov stability theory. Moreover, the filter parameters are obtained by utilizing the linear matrix inequality technique. Finally, simulation examples are given to verify the effectiveness of the proposed method. In the future, security control problems for the cyber–physical systems under the adaptive event-triggered scheme and hybrid cyber attack will be studied.

APPENDIX A
ELEMENTS OF MATRIX Υ_i IN THEOREM 1

$$\Upsilon_{11} = \Psi_1 + \Gamma_1 + \Gamma_1^{\mathrm{T}},\ \Upsilon_{21} = \Psi_2 + \Gamma_2 + \Gamma_2^{\mathrm{T}}$$

$$\Gamma_i = [J_i + N_i + U_i \quad -J_i + M_i \quad -M_i \quad -N_i + Z_i \quad -Z_i \quad -U_i + V_i \quad -V_i]$$

$$\Psi_1 = \begin{bmatrix} \Lambda_1 & (*) & (*) & (*) & (*) \\ \Lambda_2 & \Lambda_3 & (*) & (*) & (*) \\ 0 & 0 & \Lambda_4 & (*) & (*) \\ \Lambda_5 & 0 & 0 & \Lambda_6 & (*) \\ \Lambda_7 & 0 & 0 & 0 & \Lambda_8 \end{bmatrix}$$

$$\Lambda_1 = 2\varsigma_1 P_1 + P_1\bar{A} + \bar{A}^{\mathrm{T}}P_1 + Q_{11} + Q_{12} + Q_{13}$$

$$\Lambda_2 = \bar{\alpha}\bar{\beta}H^{\mathrm{T}}\bar{C}^{\mathrm{T}}P_1, \quad \Lambda_3 = \bar{C}^{\mathrm{T}}H^{\mathrm{T}}\Omega H\bar{C}$$

$$\Lambda_4 = \mathrm{diag}\left\{-e^{-2\varsigma_1 d_M}Q_{12}, 0, -e^{-2\varsigma_1\tau_M}Q_{11}\right\}$$

$$\Lambda_5 = \begin{bmatrix}\bar{\beta}_1 P_1\bar{C}H & 0 & \bar{\alpha}\bar{\beta}P_1\bar{C} & \bar{\beta}_1 P_1\bar{C}\end{bmatrix}^{\mathrm{T}}$$

$$\Lambda_6 = \mathrm{diag}\left\{C^{\mathrm{T}}H^{\mathrm{T}}\Omega HC, -e^{-2\varsigma_1\tau_M}Q_{13}, -\nu\Omega, -\nu\Omega\right\}$$

$$\Lambda_7 = \begin{bmatrix}\bar{\alpha}_1\bar{\beta}P_1\bar{E} & P_1\bar{B} & -\bar{\alpha}\bar{\beta}P_1\bar{E}\end{bmatrix}^{\mathrm{T}}, \quad \bar{\beta}_1 = 1 - \bar{\beta}$$

$$\Lambda_8 = \mathrm{diag}\left\{-I, -\gamma^2 I, -I\right\}, \quad \Upsilon_{13} = \mathrm{diag}\{-I, -I, -I\}$$

$$\Upsilon_{12} = \begin{bmatrix} \bar{L} & 0 & 0 & 0 & 0_{1\times 8} \\ 0 & 0 & 0 & FH & 0_{1\times 8} \\ 0 & \sqrt{\mu}C_1 & 0 & 0 & 0_{1\times 8} \end{bmatrix}$$

$$\Upsilon_{14} = \begin{bmatrix}\Lambda_9 & \Lambda_{10} & 0 & \Lambda_{11} & \Lambda_{12}\end{bmatrix}$$

$$\Lambda_9 = \begin{bmatrix}\bar{A}^{\mathrm{T}}P_1 & 0 & 0 & 0\end{bmatrix}^{\mathrm{T}}, \quad \theta_1 = \sqrt{\bar{\alpha}\bar{\alpha}_1}, \quad \theta_2 = \bar{\beta}\bar{\beta}_1$$

$$\Lambda_{10} = \begin{bmatrix}\Lambda_2 & \bar{\alpha}\theta_2\Lambda_{13} & \bar{\beta}\theta_1\Lambda_{13} & \theta_1\theta_2\Lambda_{13}\end{bmatrix}^{\mathrm{T}}$$

$$\Lambda_{11} = \begin{bmatrix} \bar{\beta}_1 P_1\bar{C}H & 0 & \bar{\alpha}\bar{\beta}P_1\bar{C} & \bar{\beta}_1 P_1\bar{C} \\ -\theta_2 P_1\bar{C}H & 0 & \bar{\alpha}\theta_2 P_1\bar{C} & -\theta_2 P_1\bar{C} \\ 0 & 0 & \theta_1\bar{\beta}P_1\bar{C} & 0 \\ 0 & 0 & \theta_1\theta_2 P_1\bar{C} & 0 \end{bmatrix}$$

$$\Lambda_{12} = \begin{bmatrix} \bar{\alpha}_1\bar{\beta}P_1\bar{E} & P_1\bar{B} & -\bar{\alpha}\bar{\beta}P_1\bar{E} \\ \bar{\alpha}_1\theta_2 P_1\bar{E} & 0 & -\bar{\alpha}\theta_2 P_1\bar{E} \\ -\theta_1\bar{\beta}P_1\bar{E} & 0 & -\theta_1\bar{\beta}P_1\bar{E} \\ -\theta_1\theta_2 P_1\bar{E} & 0 & -\theta_1\theta_2 P_1\bar{E} \end{bmatrix}$$

$$\Upsilon_{15} = \mathrm{diag}\left\{-P_1R_1^{-1}P_1, -P_1R_1^{-1}P_1, -P_1R_1^{-1}P_1 - P_1R_1^{-1}P_1\right\}, \quad f_1 = e^{-2\varsigma_1 h}$$

$$R_1 = \tau_M R_{11} + d_M R_{12} + r_M R_{13}, \quad f_2 = e^{2\varsigma_2 d_M}$$

$$R_2 = \tau_M R_{21} + d_M R_{22} + r_M R_{23}, \quad f_3 = e^{2\varsigma_2\tau_M}$$

$$\Upsilon_{17} = \mathrm{diag}\{-f_1R_{12}, -f_1R_{12}, -f_1R_{11}, -f_1R_{11} - f_1R_{13}, -f_1R_{13}\}$$

$$\Upsilon_{22} = \begin{bmatrix}\bar{L} & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$\Upsilon_{24} = \begin{bmatrix}P_2\bar{A} & 0 & 0 & 0 & 0 & 0 & P_2\bar{B}\end{bmatrix}$$

$$\Upsilon_{23} = -I, \quad \Upsilon_{25} = -P_2R_2^{-1}P_2$$

$$\Psi_2=\begin{bmatrix}\Lambda_{14} & (*) & (*) & (*) & (*) & (*)\\ 0 & 0 & (*) & (*) & (*) & \\ 0 & 0 & -f_2Q_{22} & (*) & (*) & (*)\\ 0 & 0 & 0 & 0 & (*) & (*)\\ 0 & 0 & 0 & 0 & -f_3Q_{21} & (*)\\ \bar{B}^{\mathrm{T}}P_2 & 0 & 0 & 0 & 0 & -\gamma^2 I\end{bmatrix}$$

$$\Upsilon_{i6}=\begin{bmatrix}J_i & M_i & N_i & Z_i & U_i & V_i\end{bmatrix}^{\mathrm{T}}$$

$$J_i^{\mathrm{T}}=\begin{bmatrix}J_{i1}^{\mathrm{T}} & J_{i2}^{\mathrm{T}} & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$M_i^{\mathrm{T}}=\begin{bmatrix}0 & M_{i2}^{\mathrm{T}} & M_{i3}^{\mathrm{T}} & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$N_i^{\mathrm{T}}=\begin{bmatrix}N_{i1}^{\mathrm{T}} & 0 & 0 & N_{i4}^{\mathrm{T}} & 0 & 0 & 0 & 0\end{bmatrix}$$

$$Z_i^{\mathrm{T}}=\begin{bmatrix}0 & 0 & 0 & Z_{i4}^{\mathrm{T}} & Z_{i5}^{\mathrm{T}} & 0 & 0 & 0\end{bmatrix}$$

$$U_i^{\mathrm{T}}=\begin{bmatrix}U_{i1}^{\mathrm{T}} & 0 & 0 & 0 & 0 & U_{i6}^{\mathrm{T}} & 0 & 0\end{bmatrix}$$

$$V_i^{\mathrm{T}}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & V_{i6}^{\mathrm{T}} & V_{i7}^{\mathrm{T}} & 0\end{bmatrix}$$

$$\Upsilon_{27}=\mathrm{diag}\{-R_{22},-R_{22},-R_{21},-R_{21},-R_{23},-R_{23}\}.$$

APPENDIX B
PROOF OF THEOREM 1

Choose the following Lyapunov functional:

$$\begin{aligned}V_i(t)=&\,\xi^{\mathrm{T}}(t)P_i\xi(t)+\int_{t-\tau_M}^{t}\xi^{\mathrm{T}}(s)\exp(\cdot)Q_{i1}\xi(s)ds\\&+\int_{t-d_M}^{t}\xi^{\mathrm{T}}(s)\exp(\cdot)Q_{i2}\xi(s)ds\\&+\int_{t-r_M}^{t}\xi^{\mathrm{T}}(s)\exp(\cdot)Q_{i3}\xi(s)ds\\&+\int_{-\tau_M}^{0}\int_{t+v}^{t}\dot{\xi}^{\mathrm{T}}(s)\exp(\cdot)R_{i1}\dot{\xi}(s)dsdv\\&+\int_{-d_M}^{0}\int_{t+v}^{t}\dot{\xi}^{\mathrm{T}}(s)\exp(\cdot)R_{i2}\dot{\xi}(s)dsdv\\&+\int_{-r_M}^{0}\int_{t+v}^{t}\dot{\xi}^{\mathrm{T}}(s)\exp(\cdot)R_{i3}\dot{\xi}(s)dsdv\end{aligned}\tag{31}$$

where $P_i>0$, $Q_{i1}>0$, $R_{i1}>0$, $Q_{i2}>0$, $R_{i2}>0$, $Q_{i3}>0$, $R_{i3}>0$, $\exp(\cdot)=e^{2(-1)^i\varsigma_i(t-s)}$, $\varsigma_i>0$, and

$$i=\begin{cases}1, & t\in[-h,0]\cup\left(\underset{n\in\mathbb{N}}{\cup}[a_n l_n)\right)\\ 2, & t\in\underset{n\in\mathbb{N}}{\cup}\left[l_n,a_{n+1}\right).\end{cases}$$

When $i=1$, by taking the derivative and mathematical expectation of (31), one can obtain

$$\begin{aligned}\mathbb{E}\{\dot{V}_1(t)\}\le&-2\varsigma_1V_1(t)+2\varsigma_1\xi^{\mathrm{T}}(t)P_1\xi(t)+2\mathbb{E}\{\xi^{\mathrm{T}}(t)P_1\dot{\xi}(t)\}\\&+\xi^{\mathrm{T}}(t)(Q_{11}+Q_{12}+Q_{13})\xi(t)+\mathbb{E}\{\dot{\xi}^{\mathrm{T}}(t)R_1\dot{\xi}(t)\}\\&-\xi^{\mathrm{T}}(t-d_M)e^{-2\varsigma_1h}Q_{12}\xi(t-d_M)\\&-\xi^{\mathrm{T}}(t-\tau_M)e^{-2\varsigma_1h}Q_{11}\xi(t-\tau_M)\\&-\xi^{\mathrm{T}}(t-r_M)e^{-2\varsigma_1h}Q_{13}\xi(t-r_M)\\&-\int_{t-\tau(t)}^{t}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{11}\dot{\xi}(s)ds\\&-\int_{t-\tau_M}^{t-\tau(t)}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{11}\dot{\xi}(s)ds\\&-\int_{t-d(t)}^{t}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{12}\dot{\xi}(s)ds\\&-\int_{t-d_M}^{t-d(t)}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{12}\dot{\xi}(s)ds\\&-\int_{t-r(t)}^{t}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{13}\dot{\xi}(s)ds\\&-\int_{t-r_M}^{t-r(t)}\dot{\xi}^{\mathrm{T}}(s)e^{-2\varsigma_1h}R_{13}\dot{\xi}(s)ds.\end{aligned}\tag{32}$$

Then, the following equalities can be obtained by using the free weighting matrix method:

$$\begin{aligned}2\rho(t)Z_1\left[\xi(t-\tau(t))-\xi(t-\tau_M)-\int_{t-\tau_M}^{t-\tau(t)}\dot{\xi}(s)ds\right]=0\\2\rho(t)N_1\left[\xi(t)-\xi(t-\tau(t))-\int_{t-\tau(t)}^{t}\dot{\xi}(s)ds\right]=0\\2\rho(t)M_1\left[\xi(t-d(t))-\xi(t-d_M)-\int_{t-d_M}^{t-d(t)}\dot{\xi}(s)ds\right]=0\\2\rho(t)J_1\left[\xi(t)-\xi(t-d(t))-\int_{t-d(t)}^{t}\dot{\xi}(s)ds\right]=0\\2\rho(t)V_1\left[\xi(t-r(t))-\xi(t-r_M)-\int_{t-r_M}^{t-r(t)}\dot{\xi}(s)ds\right]=0\\2\rho(t)U_1\left[\xi(t)-\xi(t-r(t))-\int_{t-r(t)}^{t}\dot{\xi}(s)ds\right]=0\end{aligned}\tag{33}$$

where Z_1, N_1, M_1, J_1, V_1, and U_1 are the introduced free weighting matrices, $\rho(t)=\begin{bmatrix}\rho_1(t) & \rho_2(t) & \rho_3(t)\end{bmatrix}^{\mathrm{T}}$, $\rho_1(t)=\begin{bmatrix}\xi^{\mathrm{T}}(t) & \xi^{\mathrm{T}}(t-d(t)) & \xi^{\mathrm{T}}(t-d_M) & \xi^{\mathrm{T}}(t-\tau(t))\end{bmatrix}$, $\rho_2(t)=\begin{bmatrix}\xi^{\mathrm{T}}(t-\tau_M) & \xi^{\mathrm{T}}(t-r(t)) & \xi^{\mathrm{T}}(t-r_M) & e^{\mathrm{T}}(t_r) & e^{\mathrm{T}}(t)\end{bmatrix}$, $\rho_3(t)=\begin{bmatrix}f(y(t-\tau(t))) & \omega(t) & \varrho(y(t-d(t)))\end{bmatrix}$.

Note that

$$\begin{aligned}\mathbb{E}\{\dot{\xi}^{\mathrm{T}}(t)R_1\dot{\xi}(t)\}=&\,\mathcal{A}^{\mathrm{T}}R_1\mathcal{A}+\theta_1^2\mathcal{B}^{\mathrm{T}}R_1\mathcal{B}\\&+\theta_2^2\mathcal{C}^{\mathrm{T}}R_1\mathcal{C}+\theta_1^2\theta_2^2\mathcal{D}^{\mathrm{T}}R_1\mathcal{D}\end{aligned}\tag{34}$$

where $\mathcal{A}=\bar{A}\xi(t)+\bar{B}\omega(t)+(1-\bar{\beta})\bar{E}\bar{C}\xi(t-r(t))+(1-\bar{\beta})\bar{E}e(t-r(t))+(1-\bar{\alpha})\bar{\beta}\bar{E}f(y(t-\tau(t)))+\bar{\alpha}\bar{\beta}\bar{C}H\xi(t-d(t))+{}+\bar{\alpha}\bar{\beta}\bar{C}e(t)-\bar{\alpha}\bar{\beta}\bar{E}\varrho(y(t-d(t)))$, $\mathcal{B}=-\bar{\beta}\bar{E}f(y(t-\tau(t)))+\bar{\beta}\bar{C}H\xi(t-d(t))+\bar{\beta}\bar{C}e(t)-\bar{\beta}\bar{E}\varrho(y(t-d(t)))$, $\mathcal{C}=-\bar{E}\bar{C}\xi(t-r(t))-\bar{E}e(t-r(t))+(1-\bar{\alpha})\bar{E}f(y(t-\tau(t)))+\bar{\alpha}\bar{C}H\xi(t-d(t))+\bar{\alpha}\bar{C}e(t)-\bar{\alpha}\bar{E}\varrho(y(t-d(t)))$, $\mathcal{D}=-\bar{E}f(y(t-\tau(t)))+\bar{C}H\xi(t-d(t))+\bar{C}e(t)-\bar{E}\varrho(y(t-d(t)))$.

The input constraint can be acquired from (5)

$$\mu\xi^{\mathrm{T}}(t-d(t))C_1^{\mathrm{T}}C_1\xi(t-d(t))-\varrho^{\mathrm{T}}(y(t))\varrho(y(t))>0.\tag{35}$$

According to (6) and (7), one can obtain the constraint of the adaptive event-triggered scheme

$$\xi^{\mathrm{T}}(t-d(t))H^{\mathrm{T}}\Omega H\xi(t-d(t))-\pi e^{\mathrm{T}}(t)\Omega e(t)>0.\tag{36}$$

Moreover, the following inequality can be derived from Assumption 1:

$$\xi^{\mathrm{T}}(t)C_1^{\mathrm{T}}F^{\mathrm{T}}FC_1\xi(t)-f^{\mathrm{T}}(y(t))f(y(t)\ge 0.\tag{37}$$

Combining (32)–(37) and using the Schur complement and Lemma 1, it yields

$$\begin{aligned}&\mathbb{E}\{\dot{V}_1(t)\}+\bar{z}^{\mathrm{T}}(t)\bar{z}(t)-\gamma^2\omega^{\mathrm{T}}(t)\omega(t)\\&\quad\le-2\varsigma_1V_1(t)+\rho^{\mathrm{T}}(t)\end{aligned}$$

$$\times \Big[\Phi_1 + \mathbb{E}\big\{\dot{\xi}^{\mathrm{T}}(t)R_1\dot{\xi}(t)\big\} + J_1e^{2\varsigma_1 h}R_{12}^{-1}J_1^{\mathrm{T}} + M_1e^{2\varsigma_1 h}R_{12}^{-1}M_1^{\mathrm{T}} + N_1e^{2\varsigma_1 h}R_{11}^{-1}N_1^{\mathrm{T}} + Z_1e^{2\varsigma_1 h}R_{11}^{-1}Z_1^{\mathrm{T}} + U_1e^{2\varsigma_1 h}R_{13}^{-1}U_1^{\mathrm{T}} + V_1e^{2\varsigma_1 h}R_{13}^{-1}V_1^{\mathrm{T}}\Big]\rho(t). \quad (38)$$

Using (20), it can be obtained that $\mathbb{E}\{\dot{V}_1(t)\} + \bar{z}^{\mathrm{T}}(t)\bar{z}(t) - \gamma^2\omega^{\mathrm{T}}(t)\omega(t) \le -2\varsigma_1 V_1(t)$.

Processing $V_2(t)$ in the same way, one obtains

$$\mathbb{E}\big\{\dot{V}_2(t)\big\} + \bar{z}^{\mathrm{T}}(t)\bar{z}(t) - \gamma^2\omega^{\mathrm{T}}(t)\omega(t) \le -2\varsigma_2 V_2(t) + \rho^{\mathrm{T}}(t)\big[\Phi_2 + \mathbb{E}\big\{\dot{\xi}^{\mathrm{T}}(t)R_2\dot{\xi}(t)\big\} + J_2e^{2\varsigma_2 h}R_{22}^{-1}J_2^{\mathrm{T}} + M_2e^{2\varsigma_2 h}R_{22}^{-1}M_2^{\mathrm{T}} + N_2e^{2\varsigma_2 h}R_{21}^{-1}N_2^{\mathrm{T}} + Z_2e^{2\varsigma_2 h}R_{21}^{-1}Z_2^{\mathrm{T}} + U_2e^{2\varsigma_2 h}R_{23}^{-1}U_2^{\mathrm{T}} + V_2e^{2\varsigma_2 h}R_{23}^{-1}V_2^{\mathrm{T}}\Big]\rho(t) \quad (39)$$

and $\mathbb{E}\{\dot{V}_2(t)\} + \bar{z}^{\mathrm{T}}(t)\bar{z}(t) - \gamma^2\omega^{\mathrm{T}}(t)\omega(t) \le -2\varsigma_2 V_2(t)$.

Then, it follows that:

$$\begin{cases} \mathbb{E}\{V_1(t)\} \le e^{-2\varsigma_1(t-a_n)}\mathbb{E}\{a_n\}, & t \in [a_n, l_n) \\ \mathbb{E}\{V_2(t)\} \le e^{2\varsigma_2(t-l_n)}\mathbb{E}\{l_n\}, & t \in [l_n, a_{n+1}). \end{cases} \quad (40)$$

Using the inequalities (22)–(25) yields

$$\begin{cases} \mathbb{E}\{V_1(a_n)\} \le \lambda_2\mathbb{E}\big\{V_2\big(a_n^-\big)\big\} \\ \mathbb{E}\{V_2(l_n)\} \le \lambda_1 e^{2(\varsigma_1+\varsigma_2)h}\mathbb{E}\big\{V_2\big(l_n^-\big)\big\}. \end{cases} \quad (41)$$

For $t \in [a_n, l_n)$, from (40) and (41), it can be obtained that

$$\begin{aligned} \mathbb{E}\{V_1(t)\} &\le \lambda_2 e^{-2\varsigma_1(t-a_n)}\mathbb{E}\big\{V_2\big(a_n^-\big)\big\} \\ &\le \lambda_2 e^{-2\varsigma_1(t-a_n)}e^{2\varsigma_2(a_n-l_{n-1})}\mathbb{E}\{V_2(l_{n-1})\} \\ &\vdots \\ &\le e^{m_1(t)}\mathbb{E}\{V_1(0)\} \end{aligned} \quad (42)$$

where $m_1(t) = (\nu_1 + [t/\varpi])[2(\varsigma_1+\varsigma_2)h + 2\varsigma_2 b_{\max} - 2\varsigma_1 s_{\min} + \ln(\lambda_1\lambda_2)]$.

According to (21)

$$\mathbb{E}\{V_1(t)\} \le e^{n_1}e^{-gt}\mathbb{E}\{V_1(0)\} \quad (43)$$

where $n_1 = \nu_1[2(\varsigma_1+\varsigma_2)h + 2\varsigma_2 b_{\max} - 2\varsigma_1 s_{\min} + \ln(\lambda_1\lambda_2)]$,

$$g = \frac{\varsigma_1 s_{\min} - (\varsigma_1+\varsigma_2)h - \varsigma_2 b_{\max} - 1/2\ln\lambda_1\lambda_2}{\varpi}.$$

Similarly

$$\mathbb{E}\{V_2(t)\} \le \frac{1}{\lambda_2}e^{n_2}e^{-gt}\mathbb{E}\{V_1(0)\} \quad (44)$$

where $n_2 = (\nu_1+1)[2(\varsigma_1+\varsigma_2)h + 2\varsigma_2 b_{\max} - 2\varsigma_1 s_{\min} + \ln(\lambda_1\lambda_2)]$.

Defining $M = \max\{e^{n_1}, (1/\lambda_2)e^{n_2}\}$

$$\mathbb{E}\{V(t)\} \le Me^{-gt}\mathbb{E}\{V_1(0)\}. \quad (45)$$

The following formulas result from the definition of $V(t)$:

$$\mathbb{E}\{V(t)\} \ge d_1\|\xi(t)\|^2, \quad \mathbb{E}\{V_1(0)\} \le d_2\|\varphi\|_h^2 \quad (46)$$

where $d_1 = \min\{\lambda_{\min}(P_i)\}$, $d_2 = \max\{\lambda_{\max}(P_i) + h\lambda_{\max}(Q_{i1} + Q_{i2} + Q_{i3}) + (h^2/2)\lambda_{\max}(R_{i1} + R_{i2} + R_{i3})\}$.

Then, combining (45) with (46), one obtains

$$\|\xi(t)\| \le \sqrt{\frac{Md_2}{d_1}}e^{-\frac{g}{2}t}\|\varphi\|_h. \quad (47)$$

This means system (17) is exponentially mean-square stable under the conditions (20)–(25), which completes the proof. ■

APPENDIX C
ELEMENTS OF MATRIX $\hat{\Phi}_i$ IN THEOREM 2

$$\hat{\Upsilon}_{11} = \hat{\Psi}_1 + \hat{\Gamma}_1 + \hat{\Gamma}_1^{\mathrm{T}}, \quad \hat{\Upsilon}_{21} = \hat{\Psi}_2 + \hat{\Gamma}_2 + \hat{\Gamma}_2^{\mathrm{T}}$$

$$\hat{\Gamma}_1 = \begin{bmatrix} \hat{J}_1 + \hat{N}_1 + \hat{U}_1 & -\hat{J}_1 + \hat{M}_1 & -\hat{M}_1 \\ & -\hat{N}_1 + \hat{Z}_1 - \hat{Z}_1 & -\hat{U}_1 + \hat{V}_1 \quad -\hat{V}_1 \end{bmatrix}$$

$$\hat{\Psi}_1 = \begin{bmatrix} \hat{\Lambda}_1 & (*) & (*) & (*) & (*) \\ \hat{\Lambda}_2 & \hat{\Lambda}_3 & (*) & (*) & (*) \\ 0 & 0 & \hat{\Lambda}_4 & (*) & (*) \\ \hat{\Lambda}_5 & 0 & 0 & \hat{\Lambda}_6 & (*) \\ \hat{\Lambda}_7 & 0 & 0 & 0 & \Lambda_8 \end{bmatrix}$$

$$\hat{\Lambda}_1 = 2\lambda_1\hat{P}_1 + \Pi_1 + \Pi_1^{\mathrm{T}} + \hat{Q}_{11} + \hat{Q}_{12} + \hat{Q}_{13}$$

$$\hat{P}_1 = \begin{bmatrix} P_{11} & \bar{P}_{13} \\ \bar{P}_{13} & \bar{P}_{13} \end{bmatrix}, \quad \Pi_1 = \begin{bmatrix} P_{11}A & \hat{A}_f \\ \bar{P}_{13}A & \hat{A}_f \end{bmatrix}$$

$$\hat{\Lambda}_2 = \begin{bmatrix} \bar{\alpha}\bar{\beta}C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}} & \bar{\alpha}\bar{\beta}C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}} \\ 0 & 0 \end{bmatrix}, \quad \hat{\Lambda}_3 = \begin{bmatrix} C^{\mathrm{T}}\Omega C & 0 \\ 0 & 0 \end{bmatrix}$$

$$\hat{\Lambda}_4 = \mathrm{diag}\Big\{-e^{-2\varsigma_1 d_M}\hat{Q}_{12}, 0, -e^{-2\varsigma_1\tau_M}\hat{Q}_{11}\Big\}$$

$$\hat{\Lambda}_5 = \big[\Pi_2^{\mathrm{T}} \quad 0 \quad \Pi_3^{\mathrm{T}} \quad \Pi_4^{\mathrm{T}}\big]^{\mathrm{T}}, \hat{\Lambda}_7 = \big[\Pi_5^{\mathrm{T}} \quad \Pi_6^{\mathrm{T}} \quad \Pi_7^{\mathrm{T}}\big]^{\mathrm{T}}$$

$$\Pi_2 = \begin{bmatrix} \bar{\beta}_1 C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}} & \bar{\beta}_1 C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}} \\ 0 & 0 \end{bmatrix}, \quad \Pi_{11} = \begin{bmatrix} \hat{B}_f \\ \hat{B}_f \end{bmatrix}$$

$$\Pi_4 = \big[\bar{\beta}_1 C^{\mathrm{T}}\hat{E}^{\mathrm{T}} \quad \bar{\beta}_1 C^{\mathrm{T}}\hat{E}^{\mathrm{T}}\big], \quad \Pi_7 = \Big[-\bar{\alpha}\bar{\beta}\hat{B}_f^{\mathrm{T}} \quad -\bar{\alpha}\bar{\beta}\hat{B}_f^{\mathrm{T}}\Big]$$

$$\hat{\Lambda}_6 = \mathrm{diag}\Big\{\hat{\Lambda}_3, -e^{-2\varsigma_1 r_M}\hat{Q}_{13} - \nu\Omega, -\nu\Omega\Big\}$$

$$\Pi_3 = \Big[\bar{\alpha}\bar{\beta}C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}} \quad \bar{\alpha}\bar{\beta}C^{\mathrm{T}}\hat{B}_f^{\mathrm{T}}\Big]$$

$$\Pi_5 = \Big[\bar{\alpha}_1\bar{\beta}\hat{B}_f^{\mathrm{T}} \quad \bar{\alpha}_1\bar{\beta}\hat{B}_f^{\mathrm{T}}\Big], \quad \Pi_6 = \big[B^{\mathrm{T}}P_{11} \quad B^{\mathrm{T}}\bar{P}_{13}\big]$$

$$\Pi_8 = \begin{bmatrix} \hat{B}_f C & 0 \\ \hat{B}_f C & 0 \end{bmatrix}, \quad \Pi_9 = \begin{bmatrix} \hat{B}_f & 0 \\ \hat{B}_f & 0 \end{bmatrix}, \quad \Pi_{10} = \begin{bmatrix} \hat{B}_f C \\ \hat{B}_f C \end{bmatrix}$$

$$\hat{\Upsilon}_{14} = \big[\hat{\Lambda}_9 \quad \hat{\Lambda}_{10} \quad 0 \quad \hat{\Lambda}_{11} \quad \hat{\Lambda}_{12}\big]$$

$$\hat{\Lambda}_9 = \big[\Pi_1 \quad 0 \quad 0 \quad 0\big]^{\mathrm{T}}, \quad \theta_1 = \sqrt{\bar{\alpha}\bar{\alpha}_1}, \theta_2 = \bar{\beta}\bar{\beta}_1$$

$$\hat{\Lambda}_{10} = \big[\bar{\alpha}\bar{\beta}\Pi_8^{\mathrm{T}} \quad \bar{\alpha}\theta_2\Pi_8^{\mathrm{T}} \quad \bar{\beta}\theta_1\Pi_8^{\mathrm{T}} \quad \theta_1\theta_2\Pi_8^{\mathrm{T}}\big]^{\mathrm{T}}$$

$$\hat{\Lambda}_{11} = \begin{bmatrix} \bar{\beta}_1\Pi_9 & 0 & \bar{\alpha}\bar{\beta}\Pi_{10} & \bar{\beta}_1\Pi_{10} \\ -\theta_2\Pi_9 & 0 & \bar{\alpha}\theta_2\Pi_{10} & -\theta_2\Pi_{10} \\ 0 & 0 & \theta_1\bar{\beta}\Pi_{10} & 0 \\ 0 & 0 & \theta_1\theta_2\Pi_{10} & 0 \end{bmatrix}$$

$$\hat{\Lambda}_{12} = \begin{bmatrix} \bar{\alpha}_1\bar{\beta}\Pi_{11} & \Pi_6^{\mathrm{T}} & -\bar{\alpha}\bar{\beta}\Pi_{11} \\ \bar{\alpha}_1\theta_2\Pi_{11} & 0 & -\bar{\alpha}\theta_2\Pi_{11} \\ -\theta_1\bar{\beta}\Pi_{11} & 0 & -\theta_1\bar{\beta}\Pi_{11} \\ -\theta_1\theta_2\Pi_{11} & 0 & -\theta_1\theta_2\Pi_{11} \end{bmatrix}$$

$$\hat{\Upsilon}_{15} = \mathrm{diag}\Big\{-2e_1\hat{P}_1 + e_1^2\hat{R}_1, -2e_1\hat{P}_1 + e_1^2\hat{R}_1$$

$$-2e_1\hat{P}_1+e_1^2\hat{R}_1,-2e_1\hat{P}_1+e_1^2\hat{R}_1\Big\}$$

$$\hat{R}_1=\tau_M\hat{R}_{11}+d_M\hat{R}_{12}+r_M\hat{R}_{13}$$
$$\hat{R}_2=\tau_M\hat{R}_{21}+d_M\hat{R}_{22}+r_M\hat{R}_{23}$$
$$\hat{\Upsilon}_{i6}=\begin{bmatrix}\hat{J}_i & \hat{M}_i & \hat{N}_i & \hat{Z}_i & \hat{U}_i & \hat{V}_i\end{bmatrix}^{\mathrm{T}}$$
$$J_i^{\mathrm{T}}=\begin{bmatrix}\hat{J}_{i1}^{\mathrm{T}} & \hat{J}_{i2}^{\mathrm{T}} & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$
$$M_i^{\mathrm{T}}=\begin{bmatrix}0 & \hat{M}_{i2}^{\mathrm{T}} & \hat{M}_{i3}^{\mathrm{T}} & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$
$$N_i^{\mathrm{T}}=\begin{bmatrix}\hat{N}_{i1}^{\mathrm{T}} & 0 & 0 & \hat{N}_{i4}^{\mathrm{T}} & 0 & 0 & 0 & 0\end{bmatrix}$$
$$Z_i^{\mathrm{T}}=\begin{bmatrix}0 & 0 & 0 & \hat{Z}_{i4}^{\mathrm{T}} & \hat{Z}_{i5}^{\mathrm{T}} & 0 & 0 & 0\end{bmatrix}$$
$$U_i^{\mathrm{T}}=\begin{bmatrix}U_{i1}^{\mathrm{T}} & 0 & 0 & 0 & 0 & U_{i6}^{\mathrm{T}} & 0 & 0\end{bmatrix}$$
$$V_i^{\mathrm{T}}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & V_{i6}^{\mathrm{T}} & V_{i7}^{\mathrm{T}} & 0\end{bmatrix}$$
$$\hat{\hat{\Upsilon}}_{17}=\mathrm{diag}\Big\{-f_1\hat{R}_{12},-f_1\hat{R}_{12},-f_1\hat{R}_{11}$$
$$-f_1\hat{R}_{11},-f_1\hat{R}_{13},-f_1\hat{R}_{13}\Big\}$$
$$\hat{\Gamma}_2=\begin{bmatrix}\hat{J}_2+\hat{N}_2 & -\hat{J}_2+\hat{M}_2 & -\hat{M}_2 & -\hat{N}_2+\hat{Z}_2 & -\hat{Z}_2\end{bmatrix}$$
$$\hat{\Psi}_2=\begin{bmatrix}\hat{\Lambda}_{14} & (*) & (*) & (*) & (*) & (*) & (*) & (*)\\ 0 & 0 & (*) & (*) & (*) & (*) & (*) & (*)\\ 0 & 0 & \Pi_{14} & (*) & (*) & (*) & (*) & (*)\\ 0 & 0 & 0 & 0 & (*) & (*) & (*) & (*)\\ 0 & 0 & 0 & 0 & \Pi_{15} & (*) & (*) & (*)\\ 0 & 0 & 0 & 0 & 0 & 0 & (*) & (*)\\ 0 & 0 & 0 & 0 & 0 & 0 & \Pi_{16} & (*)\\ \Pi_{12} & 0 & 0 & 0 & 0 & 0 & 0 & -\gamma^2 I\end{bmatrix}$$
$$\Upsilon_{24}=\begin{bmatrix}\Pi_{13} & 0 & 0 & 0 & 0 & \Pi_{12}^{\mathrm{T}}\end{bmatrix},\quad \Pi_{14}=-f_2\hat{Q}_{22}$$
$$\Pi_{13}=\begin{bmatrix}P_{21}A & \hat{A}_f\\ \bar{P}_{23}A & \hat{A}_f\end{bmatrix},\quad \Pi_{12}=\begin{bmatrix}B^{\mathrm{T}}P_{21} & B^{\mathrm{T}}\bar{P}_{23}\end{bmatrix}$$
$$\hat{\Upsilon}_{25}=-2e_2\hat{P}_2+e_2^2\hat{R}_2,\quad \Pi_{15}=-f_3\hat{Q}_{21},\quad \Pi_{16}=-f_3\hat{Q}_{23}.$$

APPENDIX D
PROOF OF THEOREM 2

By applying Lemma 2, for positive scalar e_1, one can obtain

$$-P_1R_1^{-1}P_1\le -2e_1P_1+e_1^2R_1. \tag{48}$$

Similarly, we have

$$-P_2R_2^{-1}P_2\le -2e_2P_2+e_2^2R_2. \tag{49}$$

Since $\bar{P}_{i3}>0$, there exist P_{i2} and $P_{i3}>0$ satisfying $\bar{P}_{i3}=P_{i2}^{\mathrm{T}}P_{i3}P_{i2}$. Define that $P_i=\begin{bmatrix}P_{i1} & P_{i2}^{\mathrm{T}}\\ P_{i2} & P_{i3}\end{bmatrix}$, $Y_i=\begin{bmatrix}I & 0\\ 0 & P_{i2}^{\mathrm{T}}P_{i3}^{-1}\end{bmatrix}$, $S_i=Y_{3-i}Y_i^{-1}$. Then premultiplying and postmultiplying (20) by $\{\underbrace{Y_i,\ldots,Y_i}_{6},\underbrace{I,\ldots,I}_{8},\underbrace{Y_i,\ldots,Y_i}_{8}\}$ and its transposition. Define $\hat{P}_i=Y_iP_iY_i^{\mathrm{T}}$, $\hat{Q}_{ij}=Y_iQ_{ij}Y_i^{\mathrm{T}}$, $\hat{R}_{ij}=Y_iR_{ij}Y_i^{\mathrm{T}}$, $\hat{J}_{ik}=Y_iJ_{ik}Y_i^{\mathrm{T}}$, $\hat{N}_{ik}=Y_iN_{ik}Y_i^{\mathrm{T}}$, $\hat{M}_{ik}=Y_iM_{ik}Y_i^{\mathrm{T}}$, $\hat{Z}_{ik}=Y_iZ_{ik}Y_i^{\mathrm{T}}$, $\hat{U}_{ik}=Y_iU_{ik}Y_i^{\mathrm{T}}$, $\hat{V}_{ik}=Y_iV_{ik}Y_i^{\mathrm{T}}$ for $j=1,2,3$; $k=1,2$. then we have (26) from (20). Since $P_i>0$, by using the Schur complement, one can obtain (27).

Define variables

$$\begin{cases}\hat{A}_f=\tilde{A}_f\bar{P}_{13},\tilde{A}_f=P_{12}^{\mathrm{T}}A_fP_{12}^{-T}\\ \hat{B}_f=P_{12}^{\mathrm{T}}B_f\\ \hat{C}_f=\tilde{C}_f\bar{P}_{13},\tilde{C}_f=C_fP_{12}^{-T}.\end{cases} \tag{50}$$

According to the above definitions, similar to the method of [44], the parameters of filter can be expressed as $A_f=P_{12}^{-T}\tilde{A}_fP_{12}^{\mathrm{T}}$, $B_f=P_{12}^{-T}\hat{B}_f$, and $C_f=\tilde{C}_fP_{12}$.

Define $\hat{x}_f(t)=P_{12}^{\mathrm{T}}x_f(t)$, (2) can be rewritten as

$$\begin{cases}\dot{\hat{x}}_f(t)=\tilde{A}_f\hat{x}_f(t)+\hat{B}_f\hat{y}(t)\\ z_f(t)=\tilde{C}_f\hat{x}(t).\end{cases} \tag{51}$$

Then, one can obtain (30) from (50) and (51). That completes the proof.

REFERENCES

[1] H. Zhang, F. Teng, Q. Sun, and Q. Shan, "Distributed optimization based on a multiagent system disturbed by general noise," *IEEE Trans. Cybern.*, vol. 49, no. 8, pp. 3209–3213, Aug. 2019.

[2] J. Liu, T. Yin, D. Yue, H. R. Karimi, and J. Cao, "Event-based secure leader-following consensus control for multi-agent systems with multiple cyber-attacks," *IEEE Trans. Cybern.*, early access, Feb. 19, 2020. [Online]. Available: https://doi.org/10.1109/TCYB.2020.2970556, doi: 10.1109/TCYB.2020.2970556

[3] G. Wen, C. L. P. Chen, Y. J. Liu, and Z. Liu, "Neural network-based adaptive leader-following consensus control for a class of nonlinear multiagent state-delay systems," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2151–2160, Aug. 2017.

[4] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[5] D. Sun, Q. Liao, X. Gu, C. Li, and H. Ren, "Multilateral teleoperation with new cooperative structure based on reconfigurable robots and type-2 fuzzy logic," *IEEE Trans. Cybern.*, vol. 49, no. 8, pp. 2845–2859, Aug. 2019.

[6] E. Tian and C. Peng, "Memory-based event-triggering H-infinity load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, early access, Mar. 12, 2020. [Online]. Available: https://doi.org/10.1109/TCYB.2020.2972384, doi: 10.1109/TCYB.2020.2972384.

[7] H.-T. Zhang, Q. Wang, Z. Chen, and F.-L. Wei, "Dynamics and feedback control of electrospinning processes," *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 2, pp. 611–618, Mar. 2017.

[8] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2049–2061, Sep. 2017.

[9] Y. L. Wang, P. Shi, C. C. Lim, and Y. Liu, "Event-triggered fault detection filter design for a continuous-time networked control system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3414–3426, Dec. 2016.

[10] H. Sun, C. Peng, W. Zhang, T. Yang, and Z. Wang, "Security-based resilient event-triggered control of networked control systems under denial of service attacks," *J. Franklin Inst.*, vol. 356, no. 17, pp. 10277–10295, 2019.

[11] Z. Chen, Z. Li, and C. L. P. Chen, "Adaptive neural control of uncertain MIMO nonlinear systems with state and input constraints," *IEEE Trans. Neural Netw. Learn. Syst.* , vol. 28, no. 6, pp. 1318–1330, Jun. 2017.

[12] Z. Peng, J. Wang, and Q.-L. Han, "Path-following control of autonomous underwater vehicles subject to velocity and input constraints via neurodynamic optimization," *IEEE Trans. Ind. Electron.*, vol. 66, no. 11, pp. 8724–8732, Nov. 2019.

[13] J. Qiu, K. Sun, I. J. Rudas, and H. Gao, "Command filter-based adaptive NN control for MIMO nonlinear systems with full state constraints and actuator hysteresis," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 2905–2915, Jul. 2020. [Online]. Available: https://doi.org/10.1109/TCYB.2019.2944761

[14] K. Sun, S. Mou, J. Qiu, T. Wang, and H. Gao, "Adaptive fuzzy control for non-triangular structural stochastic switched nonlinear systems with full state constraints," *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 8, pp. 1587–1601, Aug. 2019.

[15] S. Wen, T. Huang, X. Yu, M. Z. Q. Chen, and Z. Zeng, "Aperiodic sampled-data sliding-mode control of fuzzy systems with communication delays via the event-triggered method," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 5, pp. 1048–1057, Oct. 2016.

[16] H. Zhang, J. Han, Y. Wang, and H. Jiang, "H_∞ consensus for linear heterogeneous multiagent systems based on event-triggered output feedback control scheme," *IEEE Trans. Cybern.*, vol. 49, no. 6, pp. 2268–2279, Jun. 2019.

[17] D. Yue, E. Tian, and Q. L. Han, "A delay system method for designing event-triggered controllers of networked control systems," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 475–481, Feb. 2013.

[18] C. Peng and T. C. Yang, "Event-triggered communication and H_∞ control co-design for networked control systems," *Automatica*, vol. 49, no. 5, pp. 1326–1332, 2013.

[19] S. Wen, Z. Zeng, M. Z. Q. Chen, and T. Huang, "Synchronization of switched neural networks with communication delays via the event-triggered control," *IEEE Trans. Neural Netw. Learn. Syst.* , vol. 28, no. 10, pp. 2334–2343, Oct. 2017.

[20] Z. Gu, J. H. Park, D. Yue, Z. G. Wu, and X. Xie, "Event triggered security output feedback control for networked interconnected systems subject to cyber-attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Jan. 7, 2020. [Online]. Available: https://doi.org/10.1109/TSMC.2019.2960115, doi: 10.1109/TSMC.2019.2960115.

[21] J. Liu, L. Wei, X. Xie, E. Tian, and S. Fei, "Quantized stabilization for T–S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3820–3834, Dec. 2018.

[22] J. Liu, Z. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber-attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Jan. 4, 2019. [Online]. Available: https://doi.org/10.1109/TSMC.2018.2888633, doi: 10.1109/TSMC.2018.2888633.

[23] J. Liu, Y. Gu, X. Xie, D. Yue, and J. H. Park, "Hybrid-driven-based H_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 12, pp. 2452–2463, Dec. 2019.

[24] Z. Gu, D. Yue, and E. Tian, "On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems," *Inf. Sci.*, vol. 422, pp. 257–270, Jan. 2018.

[25] J. Qiu, K. Sun, T. Wang, and H. Gao, "Observer-based fuzzy adaptive event-triggered control for pure-feedback nonlinear systems with prescribed performance," *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 11, pp. 2152–2162, Nov. 2019.

[26] L. Zhang, H. Liang, Y. Sun, and C. K. Ahn, "Adaptive event-triggered fault detection scheme for Semi-Markovian jump systems with output quantization," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, May 7, 2019. [Online]. Available: https://doi.org/10.1109/TSMC.2019.2912846, doi: 10.1109/TSMC.2019.2912846.

[27] C. Peng, J. Zhang, and Q. L. Han, "Quantized stabilization for T–S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1685–1694, Dec. 2018.

[28] Z. Gu, P. Shi, D. Yue, and Z. Ding, "Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems," *IEEE Trans. Cybern.*, vol. 49, no. 5, pp. 1570–1579, May 2019.

[29] H. Li, Z. Zhang, H. Yan, and X. Xie, "Adaptive event-triggered fuzzy control for uncertain active suspension systems," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4388–4397, Dec. 2019.

[30] Y. Wang, Y. Xia, C. K. Ahn, and Y. Zhu, "Exponential stabilization of Takagi–Sugeno fuzzy systems with aperiodic sampling: An aperiodic adaptive event-triggered method," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 2, pp. 444–454, Feb. 2019.

[31] L. An and G. H. Yang, "Distributed secure state estimation for cyber–physical systems under sensor attacks," *Automatica*, vol. 107, pp. 526–538, Sep. 2019.

[32] L. An and G. H. Yang, "Improved adaptive resilient control against sensor and actuator attacks," *Inf. Sci.*, vol. 423, pp. 145–156, Jan. 2018.

[33] K. Wang, E. Tian, J. Liu, L. Wei, and D. Yue, "Resilient control of networked control systems under deception attacks: A memory-event-triggered communication scheme," *Int. J. Robust Nonlin. Control*, vol. 30, no. 4, pp. 1534–1548, 2020.

[34] L. Ma, Z. Wang, Q. L. Han, and H. K. Lam, "Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks," *IEEE Sensors J.*, vol. 17, no. 7, pp. 2279–2288, Apr. 2017.

[35] D. Ding, Z. Wang, Q. L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[36] H. Yuan and Y. Xia, "Secure filtering for stochastic non-linear systems under multiple missing measurements and deception attacks," *IET Control Theory Appl.*, vol. 12, no. 4, pp. 515–523, Mar. 2018.

[37] 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.

[38] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun. Control Comput.*, 2009, pp. 911–918.

[39] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[40] S. Hu, D. Yue, X. Chen, Z. Cheng, and X. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Mar. 14, 2019. [Online]. Available: https://doi.org/10.1109/TSMC.2019.2896249, doi: 10.1109/TSMC.2019.2896249.

[41] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[42] X. Chen, Y. Wang, and S. Hu, "Event-triggered quantized H_∞ control for networked control systems in the presence of denial-of-service jamming attacks," *Nonlin. Anal. Hybrid Syst.*, vol. 33, pp. 265–281, Aug. 2019.

[43] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[44] C. Lin, Q. G. Wang, H. L. Tong, and B. Chen, "Filter design for nonlinear systems with time-delay through T–S fuzzy model approach," *IEEE Trans. Fuzzy Syst.*, vol. 16, no. 3, pp. 739–746, Jun. 2008.

Jinliang Liu (Member, IEEE) received the Ph.D. degree in networked control systems from Donghua University, Shanghai, China, in 2011.

From December 2013 to June 2016, he was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China. From October 2016 to October 2017, he was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong. From November 2017 to January 2018, he was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea. He is currently a Professor with the Nanjing University of Finance and Economics, Nanjing. His research interests include networked control systems, complex dynamical networks, T–S fuzzy systems, and time-delay systems.

Yuda Wang, photograph and biography not available at the time of publication.

Jinde Cao (Fellow, IEEE) received the B.S. degree in mathematics/applied mathematics from Anhui Normal University, Wuhu, China, in 1986, the M.S. degree in mathematics/applied mathematics from Yunnan University, Kunming, China, in 1989, and the Ph.D. degree from in mathematics/applied mathematics Sichuan University, Chengdu, China, in 1998.

He joined the School of Mathematics, Southeast University, Nanjing, China, in 2000, where he is an Endowed Chair Professor, the Dean of the School of Mathematics and the Director of the Research Center for Complex Systems and Network Sciences. From 1989 to 2000, he was with Yunnan University. From 2001 to 2002, he was a Postdoctoral Research Fellow with the Chinese University of Hong Kong, Hong Kong.

Prof. Cao was a recipient of the National Innovation Award of China in 2017 and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Thomson Reuters/Clarivate Analytics. He was an Associate Editor of the IEEE TRANSACTIONS ON NEURAL NETWORKS and *Neurocomputing*. He is an Associate Editor of the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE TRANSACTIONS ON COGNITIVE AND DEVELOPMENTAL SYSTEMS, the *Journal of the Franklin Institute*, *Mathematics and Computers in Simulation*, *Cognitive Neurodynamics*, and *Neural Networks*. He is a member of the Academy of Europe and the European Academy of Sciences and Arts, and a Fellow of the Pakistan Academy of Sciences.

Dong Yue (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from the South China University of Technology, Guangzhou, China, in 1995.

He is currently a Changjiang Professor and the Dean of the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and Internet of Things.

Prof. Yue is/was an Associate Editor for some international journals, including the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, the *Journal of the Franklin Institute*, and the *International Journal of Systems Science*.

Xiangpeng Xie (Member, IEEE) received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2012 to 2014, he was a Postdoctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently an Associate Professor with the Research Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.