IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 16, 2020, accepted December 4, 2020, date of publication December 8, 2020, date of current version January 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3043238

Security Control for Adaptive Event-Triggered Networked Control Systems Under Deception Attacks

TINGTING YIN[1] AND ZHOU GU[1,2], (Member, IEEE)
[1]College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China
[2]College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao 266061, China

Corresponding author: Zhou Gu (gzh1808@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62022044 and Grant 61473156, and in part by the Jiangsu Natural Science Foundation for Distinguished Young Scholars under Grant BK20190039.

ABSTRACT This paper addresses the problem of the security control for adaptive event-triggered networked control systems under deception attacks. For the considered systems, data transmission is based on the network. To alleviate the network bandwidth pressure, an adaptive event-triggered mechanism, the triggered condition of which can be regulated adaptively according to the system states, is employed. By considering the effects of deception attacks, a novel mathematical model is established for networked control systems under discussion. Then by implementing Lyapunov stability theory, the co-design of controller gain and the parameter of adaptive event-triggered mechanism is achieved. Finally, a simulated example is offered to illustrate the feasibility of the proposed method.

INDEX TERMS Networked control systems, adaptive event-triggered control, deception attacks.

I. INTRODUCTION

Networked control systems (NCSs) integrate the communication networks, control systems and computation techniques, which have extensive applications including space and land exploration, factory automation, home robots, vehicles and healthcare [1]–[3]. For instance, NCSs are applied in [4] where the authors focus on the path planning and tracking problem for the vehicle collision avoidance. The authors in [5] study the real-time continuous zero-moment point pattern generation for a humanoid robot on basis of capture point. From the point of view of control theory, different problems of NCSs have been considered and discussed, such as robust stability [6]–[10], state estimator design [11], [15] and filter design [12]. Multitudinous scholars devote themselves into the researches of NCSs and lot of achievements are available [13], [14], [17]. For example, the quantized stabilization for NCSs with quantization is studied in [9]. The H_∞ control issue for a class of NCSs is addressed in [13]. The authors in [16] concentrate on the problem of the security-based control for the resilient event-triggered NCSs.

In the NCSs, some issues brought by the limited network resources have great influences on the system performance. Quantities of efforts are made to overcome these problems and great achievements are procurable [18]. The time-triggered scheme is applied widely in the NCSs because of its simple task model, but it may produce many redundant data while the system reaches stable, which leads to the resource waste and network congestion. Then more effective data transmission schemes are developed to solve the problem. In [19], the authors propose an event-triggered scheme (ETS) based on the discrete supervision of system states. Under this ETS, the sampling data should be delivered only when satisfying the presupposed triggering condition. Motivated by the ETS in [19], hybrid-triggered mechanism [20] and adaptive ETS [10] are developed. It is worth of being noted that the adaptive ETS receives widespread application due to the varying event-triggered condition. More concretely, the threshold variable of the triggering condition can adjust the sampling interval adaptively under the situation of maintaining the desired system performance [10]. On the basis of such a scheme, the problem of the H_∞ load frequency control is discussed for network-based power systems in [21]. The security control strategy is proposed in [22] for T-S fuzzy systems subject to multiple cyber-attacks through using this scheme.

The existence of the network brings many conveniences because of its openness and sharing, at the same time,

The associate editor coordinating the review of this manuscript and approving it for publication was Fan Zhang.

the data transmitted via the network are vulnerable to spiteful signal, such as cyber attacks [21], [23]. Cyber attacks pose a great threat to system performance [24]–[26]. Generally, cyber attacks widely investigated in the literatures include replay attacks [27], denial of service (DoS) attacks [9], [16], [28] and deception attacks [12], [20], [29]. Replay attackers launch an attack by registering the transmitted signals then randomly releasing these recorded signals again. Under the circumstances of replay attacks, a kind of the coding detection scheme is developed for cyber-physical systems in [27]. The cooperative control for a class of cyber-physical multi-agent NCSs is studied with replay attacks in [30]. DoS attacks reduce the system performance with the methods of taking up the network bandwidth resources and blocking data transmission. The authors in [9] develop the event-triggered control strategy for observer-based networked linear systems under DoS attacks. The consensus of multi-agent systems subject to DoS attack is studied in [28]. Deception attack signals may substitute for normal transmitted signals, thus leading to the system performance deterioration. The problem of the H_∞ control for hybrid-driven-based networked cascade control systems in the situation of deception attacks in [20]. Considering deception attacks, the state estimator design issue for sensor networked systems is discussed in [11]. The authors in [12] propose the local design of distributed H_∞-consensus filtering for sensor networks with deception attacks. To the best of our knowledge, the security control for the adaptive event-triggered NCSs with deception attacks has not been fully studied, which partly promotes this study.

Based on the aforesaid consideration, this paper is mainly concerned with the problem of the adaptive event-triggered control for NCSs subject to deception attacks. The contribution of this paper can be included as:

i) A new deception attack model is proposed by assuming the attack satisfies the feature of a sector nonlinearity, which is more close to the real scenarios.
ii) An adaptive event-triggered mechanism is utilized to save the limited communication resources of the NCSs under deception attacks and stochastic nonlinearity. Compared with the literatures [7], [19] with a given threshold, its triggering condition can be adaptively adjusted on the basis of the current system states such as to acquire a better system performance when NCSs suffer from deception attacks.
iii) A control strategy is proposed to achieve the security control of the NCSs under the consideration of deception attacks and stochastic nonlinearity. In comparison with the published results on NCSs [6], [10], this paper considers the influences of deception attacks and random nonlinearity, which is more reasonable to describe the actual situation.

The reminder of this paper is summarized below. Section II presents the problem formulation and modeling for the considered NCSs. The main results of the co-design for controller and adaptive event generator in the NCSs is given in Section III. In Section IV, the feasibility of designed method is demonstrated by the simulated example. The conclusion of this paper is drew in Section V.

II. PROBLEM FORMULATION AND MODELING

The structure of adaptive event-triggered control for NCSs with deception attacks is exhibited in Fig. 1. It contains the sensor, the adaptive ETS and the controller. The sampling data are delivered and transmitted through the network, and the deception attacks are also under consideration.

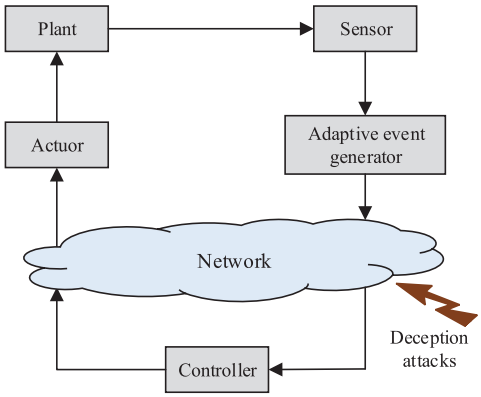

FIGURE 1. Structure of the considered NCSs under deception attacks.

Remark 1: Fig. 1 shows a structure of NCSs, where the adaptive ETS is introduced to address the problem of limited bandwidth. This framework can be applied to describe various systems in the real world, such as networked unmanned aerial vehicle (UAV). Wireless network is introduced to convenient communication of the control system, wherein the plant is UAV system; the actuator is steering gear; the event-generator and the controller are implemented by embeded system to decide which communication-data are necessary and to guarantee the performance of ETM-based UAV systems, respectively.

The NCSs are modeled as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + Hh(x(t), t) \tag{1}$$

where $x(t) \in \mathrm{R}^a$ an $u(t) \in \mathrm{R}^b$ are the state vector and the control output vector, respectively; A, B and H are constant matrices of appropriate dimensions. The function $h(x(t), t) = \begin{cases} r(x(t), t), \theta(t) = 1, \\ l(x(t), t), \theta(t) = 0 \end{cases}$, where $r(x(t), t)$ and $l(x(t), t)$ are nonlinear functions which satisfy the following conditions [32]:

$$\|r(x(t), t)\| \leq \|\mathcal{M}_1 x(t)\| \tag{2}$$

$$\|l(x(t), t)\| \leq \|\mathcal{M}_2 x(t)\| \tag{3}$$

where $\mathcal{M}_1$ and $\mathcal{M}_2$ are known constant matrices.

Remark 2: In (1), the nonlinearity is considered which results from the model errors and uncertain disturbances of the NCSs under discussion in this study. To describe it more reasonably, a Bernoulli random variable $\theta(t) \in \{0, 1\}$ is

implemented, then one can obtain a switching nonlinear function $h(x(t), t)$. It needs to be mentioned that the mathematical variance and expectation of $\theta(t)$ are denoted as ρ_1^2 and $\bar{\theta}$, respectively.

Remark 3: During the recent years, NCSs have attracted the interests from plenty of scholars due to the widespread applications in biology, medicine, metallurgy, power, smart home and traffic management [1], [2]. Quantities of achievements on NCSs are available [11]–[17]. In view of the existing work, this study focuses on the problem of the security control for adaptive event-triggered NCSs under deception attacks.

To save the network bandwidth resources, the adaptive event-triggered mechanism shown in Fig. 1 is utilized in this study. Under this adaptive ETS, the next triggering instant $t_{k+1}h$ is presented as follows:

$$t_{k+1}h = t_k h + \min_{c\in\mathcal{N}}\{ch|\xi^T(t)\Omega\xi(t) - \psi(t)x^T(t_k h + ch)\Omega x(t_k h + ch) \le 0\} \quad (4)$$

where h is the sampling period, $t_k h$ denotes the latest transmitting instant; $\xi(t) = x(t_k h) - x(t_k h + ch)$, $x(t_k h)$ represents the latest transmitted data, $x(t_k h + ch)$ denotes the current sampling data. The weighting matrix $\Omega > 0$; the variable threshold $\psi(t)$ satisfies the equation as below.

$$\dot{\psi}(t) = \left(\frac{1}{\psi^2(t)} - \frac{\varpi}{\psi(t)}\right)\xi^T(t)\Omega\xi(t) \quad (5)$$

where $\varpi \ge 1$ can adjust the convergence rate of $\psi(t)$.

Considering the impacts of the network, it is supposed that λ_{t_k} stands for the network time-delay at the instant t_{kh}. Then the time interval $[t_k h + \lambda_{t_k}, t_{k+1}h + \lambda_{k+1})$ can be divided into $c_m + 1$ subintervals, namely, $[t_k h + \lambda_{t_k}, t_{k+1}h + \lambda_{k+1}) = \cup_{c=0}^{c_m}[t_k h + ch + \lambda_{t_k}, t_k h + ch + h + \lambda_{k+1})$, where c_m is a positive constant similar to the definition in [10]. Define $\lambda(t) = t - t_k h - ch, c = 0, 1, 2, \cdots$, then one can acquire that $0 < \lambda_{t_k} \le \lambda(t) \le h + \max\{\lambda_{t_k}, \lambda_{k+1}\} = h + \bar{\lambda} \triangleq \lambda_m$.

Moreover, the sampled data through adaptive ETS can be expressed as

$$\tilde{x}(t) = x(t - \lambda(t)) + \xi(t) \quad (6)$$

where the networked-introduced time delay $\lambda(t) \in [\lambda_n, \lambda_m]$, λ_n and λ_m are respectively the lower and upper bounds of $\lambda(t)$.

Remark 4: The threshold $\psi(t)$ in (5) can be dynamically adjusted according to the latest state of the system, which differs from the constant threshold in [19]. The use of the adaptive ETS can reduce the network bandwidth load in a great degree. Therefore, in this study, the adaptive ETS (4) is implemented to investigate the security control for adaptive event-triggered NCSs subject to deception attacks.

Due to the existence of the network in the NCSs, there is a strong possibility that the network suffers from malicious signals, for instance, deception attacks and replay attacks. In this study, the influences of deception attacks are considered, which is presented in Fig. 1.

When deception attackers launch attacks, the normal transmission data may be supplanted by the deception attack signal $d(t)$. To depict the deception attacks, the variable $\delta(t)$ whose expectation and mathematical variance are respectively denoted as $\bar{\delta}$ and ρ_2^2, is employed in this study. Then the ideal controller input $\bar{x}(t)$ subject to the deception attacks is given as follows:

$$\bar{x}(t) = (1 - \delta(t))\tilde{x}(t) + \delta(t)d(t) \quad (7)$$

where $\delta(t) \in \{0, 1\}$. $\delta(t) = 1$ denotes that the network suffers from the deception attacks; $\delta(t) = 0$ stands for the absence of the deception attacks.

Assumption 1: Suppose that the deception signal $d(t)$ can be expressed as

$$d(t) = \varrho(t) - x(t) \quad (8)$$

with the limited magnitude signal $\varrho(t)$ satisfying the sector-like bounded condition as follows:

$$(\varrho(t) - \gamma x(t))^T(\varrho(t) - \gamma x(t)) \le \phi^2 x^T(t)x(t) \quad (9)$$

where γ denotes a known real matrix, ϕ represents a known real constant which satisfies $\phi \ge 0$.

The aim of this paper is to realize the co-design of adaptive ETS and the controller for the studied NCSs under deception attacks. In the following, the controller design is formulated as

$$u(t) = K\bar{x}(t) \quad (10)$$

where the actual input of the controller is denoted as $\bar{x}(t) \in \mathrm{R}^a$, the controller gain K needs to be determined.

Remark 5: In the following derivation, a linear matrix inequality (LMI) technique will be used to achieve the gain of the controller in (10), therefore, a linear state feedback control strategy is considered in this study. Nonlinear control design methods are generally applied in dealing with nonlinear systems, such as in [2], [33]–[35], and references therein.

Then combining (1), (6)-(8) and (10), it is easy to obtain the overall system

$$\begin{aligned}\dot{x}(t) = {} & Ax(t) + \theta(t)r(x(t), t) + (1 - \theta(t))l(x(t), t) \\ & + \delta(t)BK\varrho(t) - \delta(t)BKx(t) \\ & + (1 - \delta(t))BK[x(t - \lambda(t)) + \xi(t)]\end{aligned} \quad (11)$$

Remark 6: In (11), the mathematical model of the discussed NCSs has been constructed with adaptive ETS and deception attacks. To our best knowledge, the researches on NCSs have not fully investigated in the past years. In this study, the security control problem for adaptive event-triggered NCSs under deception attacks is studied.

III. MAIN RESULTS

In this section, we will offer two theorems to exhibit the main results of the adaptive event-triggered control NCSs subject to deception attacks.

Theorem 1: For known λ_n, λ_m, matrix K, γ and scalars $\bar{\delta} \in (0, 1]$, $\phi \ge 0$, $\varpi \ge 1$, $h > 0$, the system (11) attains

stable in mean square if there are symmetric matrices $\Omega > 0$, $P > 0, Q_1 > 0, Q_2 > 0, R_1 > 0, R_2 > 0$ and matrices M with appropriate dimensions so as to the following inequalities holding.

$$\Gamma = \begin{bmatrix} \zeta_{11} & * & * & * \\ \zeta_{21} & \zeta_{22} & * & * \\ \zeta_{31} & \zeta_{32} & \zeta_{33} & * \\ \zeta_{41} & \zeta_{42} & 0 & \zeta_{44} \end{bmatrix} < 0 \tag{12}$$

$$\begin{bmatrix} R_2 & * \\ M & R_2 \end{bmatrix} \geq 0 \tag{13}$$

where

$$\zeta_{11} = \begin{bmatrix} \upsilon_1 & * & * \\ R_1 & -Q_1 - R_1 - R_2 & * \\ \upsilon_2 & R_2 + M & \upsilon_3 \end{bmatrix},$$

$$\upsilon_1 = PA + A^T P - \bar{\delta} PBK - \bar{\delta} K^T B^T P + Q_1 + Q_2 - R_1 - \phi^2 P, \quad \upsilon_2 = (1-\bar{\delta}) K^T B^T P,$$

$$\upsilon_3 = -2R_2 - M - M^T + \Omega,$$

$$\zeta_{21} = \begin{bmatrix} 0 & -M & R_2 + M \\ (1-\bar{\delta}) K^T B^T P & 0 & 0 \\ \bar{\delta} K^T B^T P - \gamma P & 0 & 0 \\ \bar{\theta} H^T P & 0 & 0 \\ (1-\bar{\theta}) H^T P & 0 & 0 \end{bmatrix},$$

$$\zeta_{22} = diag\{-Q_2 - R_2, -\varpi\Omega, -P, -P, -P\},$$

$$\zeta_{31} = \begin{bmatrix} 0 & 0 & 0 \\ P\gamma & 0 & 0 \\ P\mathcal{M}_1 & 0 & 0 \\ P\mathcal{M}_2 & 0 & 0 \end{bmatrix}, \quad \zeta_{32} = \begin{bmatrix} 0 & 0 & P & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\zeta_{33} = diag\{-2P, -P, -P, -P\},$$

$$\zeta_{41} = \begin{bmatrix} \lambda_n PA - \lambda_n \bar{\delta} PBK & 0 & \lambda_n (1-\bar{\delta}) PBK \\ \lambda_1 PA - \lambda_1 \bar{\delta} PBK & 0 & \lambda_1 (1-\bar{\delta}) PBK \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \lambda_n \rho_2\, PBK & 0 & -\lambda_n \rho_2\, PBK \\ \lambda_1 \rho_2\, PBK & 0 & -\lambda_1 \rho_2\, PBK \end{bmatrix},$$

$$\zeta_{42} = \begin{bmatrix} \zeta_{42}^1 & \zeta_{42}^2 \end{bmatrix}, \quad \lambda_1 = \lambda_m - \lambda_n,$$

$$\zeta_{42}^1 = \begin{bmatrix} 0 & \lambda_n (1-\bar{\delta}) PBK & \lambda_n \bar{\delta} PBK \\ 0 & \lambda_1 (1-\bar{\delta}) PBK & \lambda_1 \bar{\delta} \rho PBK \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -\lambda_n \rho_2\, PBK & \lambda_n \rho_2\, PBK \\ 0 & -\lambda_1 \rho_2\, PBK & \lambda_1 \rho_2\, PBK \end{bmatrix},$$

$$\zeta_{42}^2 = \begin{bmatrix} \lambda_n \bar{\theta} PH & \lambda_n (1-\bar{\theta}) PH \\ \lambda_1 \bar{\theta} PH & \lambda_1 (1-\bar{\theta}) PH \\ \lambda_n \rho_1\, PH & -\lambda_1 \rho_1\, PH \\ \lambda_1 \rho_1\, PH & -\lambda_1 \rho_1\, PH \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

$$\zeta_{44} = diag\{-PR_1^{-1}P, -PR_2^{-1}P, PR_1^{-1}P, -PR_2^{-1}P, -PR_1^{-1}P, -PR_2^{-1}P\}.$$

Proof: The following time-varying Lyapunov functional is selected for system (11):

$$\begin{aligned} V(t) = {} & x^T(t)Px(t) + \int_{t-\lambda_n}^{t} x^T(w)Q_1 x(w)dw \\ & + \int_{t-\lambda_m}^{t} x^T(w)Q_2 x(w)dw + \frac{1}{2}\psi^2(t) \\ & + \lambda_n \int_{t-\lambda_n}^{t} \int_{z}^{t} \dot{x}^T(w)R_1 \dot{x}(w)dwdz \\ & + (\lambda_m - \lambda_n) \int_{t-\lambda_m}^{t-\lambda_n} \int_{z}^{t} \dot{x}^T(w)R_2 \dot{x}(w)dwdz \end{aligned} \tag{14}$$

where $P > 0, Q_\varsigma > 0, R_\varsigma > 0\ (\varsigma = 1, 2)$.

In what follows, for the function $V(t)$, take its derivation and expectation, then it follows that

$$\begin{aligned} \mathbf{E}\{\dot{V}(t)\} = {} & \mathbf{E}\left\{x^T(t)\Psi_R x(t)\right\} + \dot{x}^T(t)(Q_1 + Q_2)\dot{x}(t) \\ & - x^T(t-\lambda_n)Q_1 x(t-\lambda_n) + 2x^T(t)P\dot{x}(t) \\ & - x^T(t-\lambda_m)Q_2 x(t-\lambda_m) + \psi(t)\dot{\psi}(t) \\ & - \lambda_n \int_{t-\lambda_n}^{t} x^T(z)R_1 x(z)dz \\ & - (\lambda_m - \lambda_n) \int_{t-\lambda_m}^{t-\lambda_n} \dot{x}^T(z)R_2 \dot{x}(z)dz \end{aligned} \tag{15}$$

Note that $\mathbf{E}\{x^T(t)\Psi_R x(t)\} = \mathcal{A}_1^T \Psi_R \mathcal{A}_1 + \rho_1^2 \mathcal{A}_2^T \Psi_R \mathcal{A}_2 + \rho_2^2 \mathcal{A}_3^T \Psi_R \mathcal{A}_3$, $\Psi_R = \lambda_n^2 R_1 + (\lambda_m - \lambda_n)^2 R_2$, $\mathcal{A}_1 = Ax(t) + \bar{\delta} Hr(x(t), t) + (1-\bar{\delta}) Hl(x(t), t) + \bar{\delta} BK[\varrho(t) - \xi(t)] + (1-\bar{\delta}) BK[x(t-\lambda(t)) + \xi(t)] + (1-\bar{\delta}) BK[x(t-\lambda(t)) + \xi(t)]$, $\mathcal{A}_2 = H[r(x(t), t) - l(x(t), t)]$, $\mathcal{A}_3 = BK[\varrho(t) - x(t) - x(t-\lambda(t)) - \xi(t)]$.

Due to the inequalities (2) and (3) holding, one can get

$$x^T(t)\mathcal{M}_1^T P \mathcal{M}_1 x(t) - r^T(x(t), t)Pr(x(t), t) \geq 0 \tag{16}$$

$$x^T(t)\mathcal{M}_2^T P \mathcal{M}_2 x(t) - l^T(x(t), t)Pl(x(t), t) \geq 0 \tag{17}$$

According to (4) and (5), it follows that

$$\psi(t)\dot{\psi}(t) \leq x^T(t-\lambda(t))\Omega x(t-\lambda(t)) - \varpi \xi^T(t)\Omega \xi(t) \tag{18}$$

By utilizing Jensen's inequality [11], it can be achieved that

$$\begin{aligned} -\lambda_n \int_{t-\lambda_n}^{t} x^T(z)R_1 x(z)dz \leq {} & \begin{bmatrix} x(t) \\ x(t-\lambda_n) \end{bmatrix}^T \\ & \times \begin{bmatrix} -R_1 & * \\ R_1 & -R_1 \end{bmatrix} \begin{bmatrix} x(t) \\ x(t-\lambda_n) \end{bmatrix}, \\ -(\lambda_m - \lambda_n) \int_{t-\lambda_m}^{t-\lambda_n} \dot{x}^T(z)R_2 \dot{x}(z)dz \leq {} & F_1^T F_2 F_1, \end{aligned} \tag{19}$$

$$F_1 = \begin{bmatrix} x(t-\lambda_n) \\ x(t-\lambda(t)) \\ x(t-\lambda_m) \end{bmatrix},$$

$$F_2 = \begin{bmatrix} -R_2 & * & * \\ R_2 + M & -2R_2 - M - M^T & * \\ -M & R_2 + M & -R_2 \end{bmatrix}. \tag{20}$$

Combining (9) and (15)-(20), then using Schur complement, one can get that

$$\mathbf{E}\{\dot{V}(t)\} \leq \Phi^T(t)\Gamma\Phi(t)$$

where $\Phi(t) = [x^T(t) \;\; x^T(t-\lambda_n) \;\; x^T(t-\lambda(t)) \;\; x^T(t-\lambda_m) \;\; \xi^T(t) \;\; \varrho^T(t) \;\; r^T(x(t),t) \;\; l^T(x(t),t)]^T$. Due to $\Gamma < 0$, one has that $\mathbf{E}\{\dot{V}(t)\} < 0$. Moreover, it is concluded that when inequalities (12) and (13) hold, the system (11) is mean square stable. That proof is completed.

In Theorem 1, the sufficient conditions to guarantee the mean square stability of system (11) are acquired. Then the controller gain and the parameter of adaptive ETS are derived in Theorem 2 when the discussed system under deception attacks is mean square stable.

Theorem 2: For known $\lambda_n, \lambda_m, \gamma$ and the scalars, including $\phi \geq 0$, $\bar{\delta} \in (0,1]$, $\varpi \geq 1$, $h > 0$, the system (11) attains stable in mean square if there are symmetric matrices matrices $Y, X > 0$, $\tilde{\Omega} > 0$, $\tilde{Q}_1 > 0$, $\tilde{Q}_2 > 0$, $\tilde{R}_1 > 0$, $\tilde{R}_2 > 0$ and matrices $\tilde{M}$ with appropriate dimensions so as to the following linear matrix inequalities holding.

$$\tilde{\Gamma} = \begin{bmatrix} \tilde{\zeta}_{11} & * & * & * \\ \tilde{\zeta}_{21} & \tilde{\zeta}_{22} & * & * \\ \tilde{\zeta}_{31} & \tilde{\zeta}_{32} & \tilde{\zeta}_{33} & * \\ \tilde{\zeta}_{41} & \tilde{\zeta}_{42} & 0 & \tilde{\zeta}_{43} \end{bmatrix} < 0 \tag{21}$$

$$\begin{bmatrix} \tilde{R}_2 & * \\ \tilde{M} & \tilde{R}_2 \end{bmatrix} \geq 0 \tag{22}$$

where

$$\begin{aligned}
\tilde{\zeta}_{11} &= \begin{bmatrix} \upsilon_1 & * & * \\ \tilde{R}_1 & -\tilde{Q}_1 - \tilde{R}_1 - \tilde{R}_2 & * \\ \upsilon_2 & \tilde{R}_2 + \tilde{M} & \upsilon_3 \end{bmatrix}, \\
\upsilon_1 &= AX + XA^T - \bar{\delta}BY - \bar{\delta}Y^TB^T + \tilde{Q}_1 \\
&\quad + \tilde{Q}_2 - \tilde{R}_1 - \phi^2 X, \upsilon_2 = (1-\bar{\delta})Y^TB^T, \\
\upsilon_3 &= -2\tilde{R}_2 - \tilde{M} - \tilde{M}^T + \tilde{\Omega}, \\
\tilde{\zeta}_{21} &= \begin{bmatrix} 0 & -\tilde{M} & \tilde{R}_2 + \tilde{M} \\ (1-\bar{\delta})Y^TB^T & 0 & 0 \\ \bar{\delta}Y^TB^T - X\gamma & 0 & 0 \\ \bar{\theta}XH^T & 0 & 0 \\ (1-\bar{\theta})XH^T & 0 & 0 \end{bmatrix}, \\
\tilde{\zeta}_{22} &= diag\{-\tilde{Q}_2 - \tilde{R}_2, -\varpi\tilde{\Omega}, -X, -X, -X\}, \\
\tilde{\zeta}_{31} &= \begin{bmatrix} 0 & 0 & 0 \\ \gamma X & 0 & 0 \\ \tilde{\mathcal{M}}_1 X & 0 & 0 \\ \tilde{\mathcal{M}}_2 X & 0 & 0 \end{bmatrix}, \quad \tilde{\zeta}_{32} = \begin{bmatrix} 0 & 0 & X & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\
\tilde{\zeta}_{33} &= diag\{-2X, -X, -X, -X\}, \\
\tilde{\zeta}_{41} &= \begin{bmatrix} \lambda_n AX - \lambda_n\bar{\delta}BY & 0 & \lambda_n(1-\bar{\delta})BY \\ \lambda_1 AX - \lambda_1\bar{\delta}BY & 0 & \lambda_1(1-\bar{\delta})BY \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \lambda_n\rho_2\, BY & 0 & -\lambda_n\rho_2\, BY \\ \lambda_1\rho_2\, BY & 0 & -\lambda_1\rho_2\, BY \end{bmatrix}, \\
\tilde{\zeta}_{42} &= \begin{bmatrix} \tilde{\zeta}_{42}^1 & \tilde{\zeta}_{42}^2 \end{bmatrix}, \quad \lambda_1 = \lambda_m - \lambda_n,
\end{aligned}$$

$$\begin{aligned}
\tilde{\zeta}_{42}^1 &= \begin{bmatrix} 0 & \lambda_n(1-\bar{\delta})BY & \lambda_n\bar{\delta}BY \\ 0 & \lambda_1(1-\bar{\delta})BY & \lambda_1\bar{\delta}\rho BY \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -\lambda_n\rho_2\, BY & \lambda_n\rho_2\, BY \\ 0 & -\lambda_1\rho_2\, BY & \lambda_1\rho_2\, BY \end{bmatrix}, \\
\tilde{\zeta}_{42}^2 &= \begin{bmatrix} \lambda_n\bar{\theta}HX & \lambda_n(1-\bar{\theta})HX \\ \lambda_1\bar{\theta}HX & \lambda_1(1-\bar{\theta})HX \\ \lambda_n\rho_1\, HX & -\lambda_1\rho_1\, HX \\ \lambda_1\rho_1\, HX & -\lambda_1\rho_1\, HX \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \\
\tilde{\zeta}_{44} &= diag\{-2e_1X + e_1^2\tilde{R}_1, -2e_2X + e_2^2\tilde{R}_2, \\
&\quad -2e_1X + e_1^2\tilde{R}_1, -2e_2X + e_2^2\tilde{R}_2, \\
&\quad -2e_1X + e_1^2\tilde{R}_1, -2e_2X + e_2^2\tilde{R}_2\}.
\end{aligned}$$

Moreover, the controller gain is achieved as follows:

$$K = YX^{-1} \tag{23}$$

Proof: According to $(R_\nu - e_\nu^{-1}P)R_\nu^{-1}(R_\nu - e_\nu^{-1}P) \geq 0$ $(\nu = 1, 2)$, it is easy to derive that

$$-PR_\nu^{-1}P \leq -2e_\nu P + e_\nu^2 R_1, \quad \nu = 1, 2 \tag{24}$$

Replacing the terms in ζ_{44} with $-2e_1P + e_1^2R_1$ and $-2e_2P + e_2^2R_2$, it follows that $\zeta_{33} = diag\{-2e_1P + e_1^2R_1, -2e_2P + e_2^2R_2, -2e_1P + e_1^2R_1, -2e_2P + e_2^2R_2, -2e_1P + e_1^2R_1, -2e_2P + e_2^2R_2\}$.

Define $X = P^{-1}$, $\Theta_X = diag\left\{\underbrace{X, \cdots, X}_{18}\right\}$, then multiply Γ by Θ_X from the left side and Θ_X^T from the right side. Denote $\tilde{Q}_\varsigma = XQ_\varsigma X$, $\tilde{R}_\varsigma = XR_\varsigma X$ $(\varsigma = 1, 2)$, $\tilde{M} = XMX$, $\tilde{\Omega} = X\Omega X$ and $Y = KX$, then one can get $\tilde{\Gamma}$, further, it can be easily acquired that $\mathbf{E}\{\dot{V}(t)\} < 0$. For the inequality (13), pre- and post-multiplying it with Υ and Υ^T $(\Upsilon = diag\{X, X\})$, respectively, it can be obtained that the inequalities (22) holds. According to inequalities (21) and (22), one can get that system (11) achieves mean square stability. Due to $Y = KX$, then the controller gain can be written as $K = YX^{-1}$. That completes this proof.

IV. SIMULATION EXAMPLES

In this section, we testify the proposed theory via a well-understood benchmark example containing the model of a batch reactor, where the linearised batch reactor is given by (1) with the following parameter matrices [31]

$$A = \begin{bmatrix} -0.55 & -0.4 \\ 0.3 & -0.7 \end{bmatrix}, \quad B = \begin{bmatrix} 0.5 \\ 0.3 \end{bmatrix}, \quad H = I_2.$$

The initial parameter of system (11) is given as $x_0 = \begin{bmatrix} -2 & 3 \end{bmatrix}^T$. The deception attacks function is chosen as $\varrho(t) = [-tanh^T(0.15x_1(t)) \;\; -tanh^T(0.25x_2(t)]^T$, which means that $\gamma = diag\{0.15, 0.25\}$ such that the inequality (9) holds for $\phi = 0$.

In the following, two cases are discussed according to whether deception attacks happen or not.

Case 1: No deception attacks take place in the NCSs. It implies that $\bar{\delta} = 0$. Let $\bar{\theta} = 0.25$, $h = 0.05$s, $\lambda_m = 0.3$, $\lambda_n = 0.01$, $\varpi = 1.4$, $\psi(0) = 0.7$, $e_1 = 1$, $e_2 = 1$, then the following controller gain and triggering parameter can be obtained with the method of solving the linear matrix inequalities of Theorem 2 in MATLAB.

$$K = \begin{bmatrix} -0.0027 & -0.0013 \end{bmatrix}, \quad \Omega = \begin{bmatrix} 0.6884 & 0.2777 \\ 0.2777 & 0.3994 \end{bmatrix}.$$

Fig. 2 exhibits the state response of the system, where the blue line and red line denote the response of the system state $x_1(t)$ and $x_2(t)$, respectively. The response of the control input is also given in Fig. 2. From Fig. 2, one can see that system attains mean square stable, which indicates that the considered NCSs perform well in the absence of deception attacks.

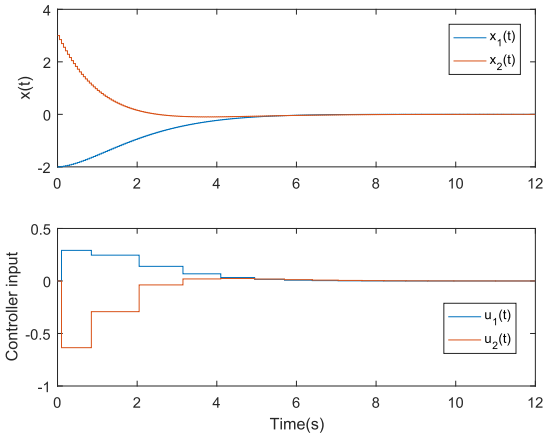

FIGURE 2. Response of $x(t)$ and control input in Case 1.

Case 2: The network suffers from deception attacks, in this situation, let $\bar{\delta} = 0.1$, $\bar{\theta} = 0.25$, $h = 0.05$s, $\lambda_m = 0.3$, $\lambda_n = 0.01$, $\varpi = 1.4$, $\psi(0) = 0.7$, $e_1 = 1$, $e_2 = 1$, then by solving the linear matrix inequalities of Theorem 2 in MATLAB, the following controller gain and triggering parameter are derived.

$$K = \begin{bmatrix} -0.1029 & -0.0446 \end{bmatrix}, \quad \Omega = \begin{bmatrix} 1.1453 & 0.4019 \\ 0.4019 & 1.0182 \end{bmatrix}.$$

Fig. 3–Fig. 6 present the simulated results. The state response and controller input of the system are presented in Fig. 3, which show that the considered NCSs perform well while the network is subjected to deception attacks. In the comparison with Case 1, the controller input in Case 2 has an obvious sudden change at about 1s, which results from the existing of deception attacks. In addition, one can see from the first figure in Fig. 3 that the state vector $x(t)$ has a relatively large change during the interval [0,1) when the system does not attain stable, which also is one of the reasons for the sudden change of the controller input in Case 2.

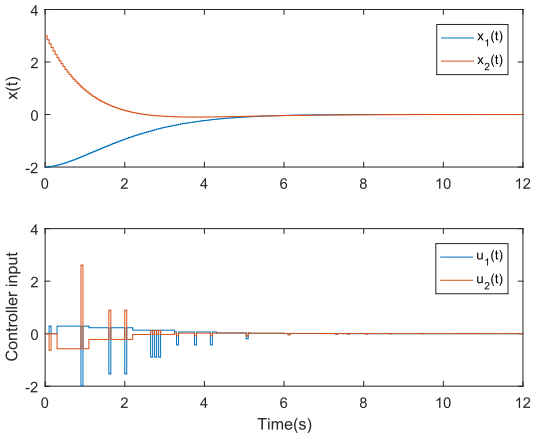

FIGURE 3. Response of $x(t)$ and control input in Case 2.

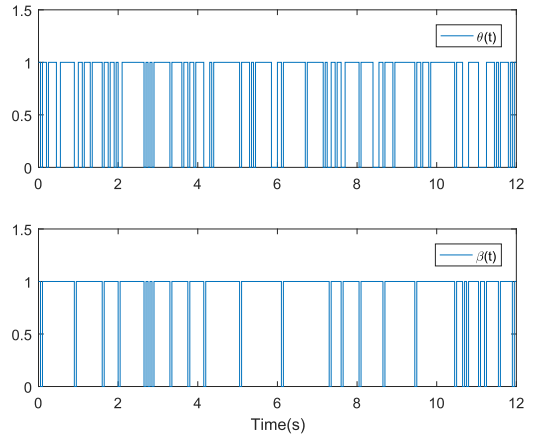

FIGURE 4. Bernoulli distribution of $\theta(t)$ and $\delta(t)$ in Case 2.

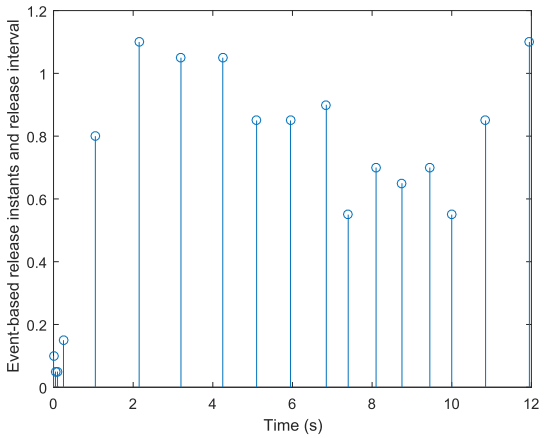

FIGURE 5. Release instants and release intervals in Case 2.

Bernoulli distribution of $\theta(t)$ is exhibited in Fig. 4, from which it can be observed that the nonlinear function $h(x(t), t)$ is switched among $r(x(t), t)$ and $l(x(t), t)$ in 12s. More specifically, when $\theta(t) = 1$, $h(x(t), t) = r(x(t), t)$; when $\theta(t) = 0$, the nonlinear function $h(x(t), t) = l(x(t), t)$. The dense line of

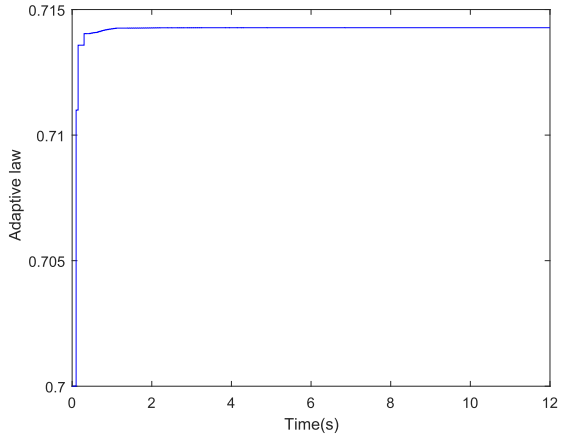

FIGURE 6. Adaptive law of $\psi(t)$ in Case 2.

the first figure in Fig. 4 represents higher switching frequency between $r(x(t), t)$ and $l(x(t), t)$ in 12s.

Fig. 4 also shows the Bernoulli distribution of $\delta(t)$ which can describe whether the deception attacks happen or not, where $\delta(t) = 1$ means that deception attacks occur at this instant while $\delta(t) = 0$ denotes the deception attacks do not take place. The dense line of the second figure in Fig. 4 represents the frequency of cyber-attacks is high.

The release instants and intervals of adaptive ETS are exhibited in Fig. 5, from which one can clearly observe that lots of sampled data are abandoned and fewer signals are delivered into the network, resulting in economizing the limited network resources. The adaptive law of $\psi(t)$ is shown in Fig. 6, where one can see that $\psi(t)$ converge to 0.7143 when the system is stable with the initial parameter $\psi(0) = 0.7$. When $\psi(t) = 0.7143$, it becomes a conventional time-triggered mechanism. Based on the simulation results, the conclusion is drawn that the designed method for the discussed NCSs is effective no matter whether deception attacks occur or not.

For the purpose of demonstrate the strong point of our adopted adaptive ETS, some comparisons of time-triggered scheme (TTS) and ETS in [19] are carried out. By setting different sampling period h, numbers of transmitted data packets for the considered NCSs are recorded in Table 1.

TABLE 1. Numbers of transmitted data packets within 12*s*.

	$h = 0.05s$	$h = 0.1s$	$h = 0.2s$
TTS	240	20	17
ETS in [19]	120	20	16
Adaptive ETS	60	17	13

In comparison with the numbers of transmitted data packets for three kinds of triggering schemes within $12s$, it can be summed up that the use of adaptive ETS this study results in fewer transmitted data packets than the other schemes under the condition of ensuring the desired performance of NCSs, which implies that adaptive ETS adopted in this study has the advantages of avoiding the network resources wasting to some degree.

V. CONCLUSION

In this paper, the security control for adaptive event-triggered NCSs under deception attacks has been investigated. To mitigate the communication pressure, the adaptive event-triggered mechanism is employed to decide whether the releasing data should be delivered. Different form the ETS with the constant threshold, the threshold of adaptive event-triggered condition can be dynamically adjusted under the circumstances of ensuring the system performance. Through considering the influences of deception attacks, the model of NCSs is built with adaptive event-triggered mechanism. Applying the Lyapunov stability theory, the co-design of controller gain and the adaptive event-triggered parameter is realized. Lastly, the feasibility of the proposed method is demonstrated through the simulated example based on a batch reactor. Future study will concentrate on the attack detection and defense for NCSs against deception attacks.

REFERENCES

[1] C. Hu, Y. Chen, and J. Wang, "Fuzzy observer-based transitional path-tracking control for autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 16, 2020, doi: 10.1109/TITS.2020.2979431.

[2] H. Huang, J. Zhou, Q. Di, J. Zhou, and J. Li, "Robust neural network–based tracking control and stabilization of a wheeled mobile robot with input saturation," *Int. J. Robust Nonlinear Control*, vol. 29, no. 2, pp. 375–392, Jan. 2019.

[3] M. Pazera, M. Witczak, N. Kukurowski, and M. Buciakowski, "Towards simultaneous actuator and sensor faults estimation for a class of Takagi-Sugeno fuzzy systems: A twin-rotor system application," *Sensors*, vol. 20, no. 12, p. 3486, Jun. 2020.

[4] J. Ji, A. Khajepour, W. W. Melek, and Y. Huang, "Path planning and tracking for vehicle collision avoidance based on model predictive control with multiconstraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 952–964, Feb. 2017.

[5] S. Park and J. Oh, "Real-time continuous ZMP pattern generation of a humanoid robot using an analytic method based on capture point," *Adv. Robot.*, vol. 33, no. 1, pp. 33–48, Jan. 2019.

[6] Z. Gu, P. Shi, D. Yue, S. Yan, and X. Xie, "Memory-based continuous event-triggered control for networked T-S fuzzy systems against cyber-attacks," *IEEE Trans. Fuzzy Syst.*, early access, Jul. 29, 2020, doi: 10.1109/TFUZZ.2020.3012771.

[7] 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, doi: 10.1109/TSMC.2019.2960115.

[8] S. Yan, M. Shen, S. Kiong Nguang, and G. Zhang, "Event-triggered H_∞ control of networked control systems with distributed transmission delay," *IEEE Trans. Autom. Control*, vol. 65, no. 10, pp. 4295–4301, Oct. 2020.

[9] Y. Xu and Z.-G. Wu, "Distributed adaptive event-triggered fault-tolerant synchronization for multiagent systems," *IEEE Trans. Ind. Electron.*, vol. 68, no. 2, pp. 1537–1547, Feb. 2021.

[10] 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.

[11] H. Wang, S. Xie, B. Zhou, and W. Wang, "Non-fragile robust H_∞ filtering of Takagi-Sugeno fuzzy networked control systems with sensor failures," *Sensors*, vol. 20, no. 1, p. 17, Jan. 2020.

[12] F. Han, H. Dong, Z. Wang, and G. Li, "Local design of distributed H_∞-consensus filtering over sensor networks under multiplicative noises and deception attacks," *Int. J. Robust Nonlinear Control*, vol. 29, no. 8, pp. 2296–2314, May 2019.

[13] C. Peng, M. J. Yang, J. Zhang, M. R. Fei, and S. L. Hu, "Network-based H_∞ control for T-S fuzzy systems with an adaptive event-triggered communication scheme," *Fuzzy Sets Syst.*, vol. 329, pp. 61–76, Dec. 2017.

[14] D. Shah, A. Mehta, K. Patel, and A. Bartoszewicz, "Event-triggered discrete higher-order SMC for networked control system having network irregularities," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 6837–6847, Nov. 2020.
[15] J.-W. Hu, X.-S. Zhan, J. Wu, and H.-C. Yan, "Analysis of optimal performance of MIMO networked control systems with encoding and packet dropout constraints," *IET Control Theory Appl.*, vol. 14, no. 13, pp. 1762–1768, Sep. 2020.
[16] 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, Nov. 2019.
[17] S. Yan, F. Yang, and Z. Gu, "Derivative-based event-triggered control for networked systems with quantization," *Appl. Math. Comput.*, vol. 383, Oct. 2020, Art. no. 125359.
[18] X. Sun, Z. Gu, F. Yang, and S. Yan, "Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks," *Inf. Sci.*, vol. 543, pp. 1–17, Jan. 2021.
[19] 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.
[20] 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.
[21] C. Peng, J. Li, and M. Fei, "Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2017.
[22] J. Liu, T. Yin, J. Cao, D. Yue, and H. R. Karimi, "Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Jan. 15, 2020, doi: 10.1109/TSMC.2019.2963143.
[23] J. Zhang, J. Sun, and C. Zhang, "Stochastic game in linear quadratic Gaussian control for wireless networked control systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Oct. 5, 2020, doi: 10.1109/TSMC.2020.3010515.
[24] Y. Xu, M. Fang, Y. Pan, K. Shi, and Z. Wu, "Event-triggered output synchronization for nonhomogeneous agent systems with periodic denial-of-service attacks," *Int. J. Robust Nonlinear Control*, Sep. 2020, doi: 10.1002/rnc.5223.
[25] 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.
[26] X. Zhou and Z. Gu, "Event-triggered H_∞ filter design of T-S fuzzy systems subject to hybrid attacks and sensor saturation," *IEEE Access*, vol. 8, pp. 126530–126539, 2020.
[27] 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.
[28] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.
[29] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, Apr. 2017.
[30] A. H. Tahoun and M. Arafa, "Cooperative control for cyber–physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks," *ISA Trans.*, Oct. 2020, doi: 10.1016/j.isatra.2020.10.002.
[31] H. Zhang, D. Yue, X. Yin, and J. Chen, "Adaptive model-based event-triggered control of networked control system with external disturbance," *IET Control Theory Appl.*, vol. 10, no. 15, pp. 1956–1962, Oct. 2016.
[32] E. Tian and D. Yue, "Decentralized control of network-based interconnected systems: A state-dependent triggering method," *Int. J. Robust Nonlinear Control*, vol. 47, no. 8, pp. 2279–2287, 2017.
[33] N. I. Chaudhary, Z. A. Khan, S. Zubair, M. A. Z. Raja, and N. Dedovic, "Normalized fractional adaptive methods for nonlinear control autoregressive systems," *Appl. Math. Model.*, vol. 66, pp. 457–471, Feb. 2019.
[34] H. Ouyang, X. Xu, and G. Zhang, "Tracking and load sway reduction for double-pendulum rotary cranes using adaptive nonlinear control approach," *Int. J. Robust Nonlinear Control*, vol. 30, no. 5, pp. 1872–1885, Mar. 2020.
[35] W. Li and M. Krstic, "Stochastic adaptive nonlinear control with filterless least-squares," *IEEE Trans. Autom. Control*, early access, Sep. 29, 2020, doi: 10.1109/TAC.2020.3027650.

TINGTING YIN was born in Jiangsu, China, in 1993. She received the B.S. degree in network engineering from the Nanjing University of Posts and Telecommunications, Yangzhou, China, in 2017, and the M.S. degree in software engineering from the Nanjing University of Finance and Economics, Nanjing, China, in 2020, respectively. She is currently pursuing the Ph.D. degree with the Nanjing Forestry University, Nanjing. Her research interests include T-S fuzzy systems, cyber-physical systems, and multi-agent systems.

ZHOU GU (Member, IEEE) received the B.S. degree from North China Electric Power University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in control science and engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007 and 2010, respectively. From September 1996 to January 2013, he was with the School of Power engineering, Nanjing Normal University, as an Associate Professor. He was a Visiting Scholar with Central Queensland University, Rockhampton, Queensland, Australia, and The University of Manchester, Manchester, U.K. He is currently a Professor with Nanjing Forestry University, Nanjing. His current research interests include networked control systems, time-delay systems, as well as reliable control and their applications.