Nonlinear Dyn (2021) 106:2245–2257
https://doi.org/10.1007/s11071-021-06825-1

ORIGINAL PAPER

Switched event-based control for nonlinear cyber-physical systems under deception attacks

Fan Yang · Zhou Gu · Shen Yan

Received: 25 January 2021 / Accepted: 12 August 2021 / Published online: 8 October 2021

Abstract We address the event-based control of nonlinear cyber-physical systems subject to deception attacks. In particular, an improved Takagi–Sugeno (T–S) fuzzy model is employed to solve the mismatch problem between the fuzzy system and fuzzy controllers. From the perspective of attack detection, we construct a novel queuing model to depict deception attacks. Then, a switched event-based communication scheme is proposed, which dynamically converts with different attack modes. The idea is to appropriately reduce the number of triggers according to the severity level of attacks, which can further save network resources. By using piecewise Lyapunov functional methods, we find a solution to the co-design of fuzzy controllers and event-triggering parameters while the concerned system is guaranteed to be exponentially stable. Finally, we apply the proposed approach to a mass–spring–damper system, where the effectiveness is well verified.

Keywords Cyber-physical systems · Event-triggered mechanism · Takagi–Sugeno fuzzy model · Deception attacks · Piecewise Lyapunov functional

Z. Gu (✉) · F. Yang · S. Yan
College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing 210037, People's Republic of China
e-mail: gzh1808@163.com

F. Yang
e-mail: yfan0510@sina.cn

S. Yan
e-mail: yanshenzdh@gmail.com

1 Introduction

Recent years have witnessed remarkable processes of cyber-physical systems (CPSs), which can be defined as a tight coupling of computation, communication, and physical plants [1,2]. Some potential applications include, but are not limited to, next-generation smart grids, autonomous vehicles, healthcare devices, and home automations [3]. From the perspective of control modeling, the dynamic physical process of CPSs is more likely assumed to be a linear model [4], while the nonlinear characteristic is consistent with the actual situation. Then, linear approximation approaches have been developed to resolve the difficulty in analyzing nonlinear systems, for instance, Takagi–Sugeno (T–S) fuzzy models have been verified as an effective alternative [5]. Compared with conventional T-S fuzzy approaches, where the same membership and premise variables are employed, an imperfect premise matching design strategy is proposed to increase the design flexibility [6], especially in network circumstances. [7] constructed independent membership and premise variables for the concerned system and feedback controllers in the presence of cyber-attacks. In [8], a novel type-2 fuzzy filter was established to investigate nonlinear networked control systems subject to parameter uncertainties, where the premise variables were different from those of the fuzzy system.

During the operation of a CPS, there is no doubt that shared or own networks are regarded as a core ingredient. Every component and their interconnec-

tions can be a risk factor to cyber-attacks because CPSs are large-scale and geographically dispersed [9]. Moreover, cyber-security techniques alone are not enough to guarantee CPSs' security, while control approaches can be adopted as a kind of compensation practices [10]. Then, new challenges are posed to control issues, in which denial of service (DoS) attacks and deception attacks have attracted plenty of research interests [11–15]. It is definitely a critical task to model cyber-attacks appropriately before control design. For DoS attacks, a few typical models or handling methods have been proposed. Stochastic models were employed to depict DoS attacks, for instances, Bernoulli models [16] and Markov models [17]. However, [18] mentioned that it was not entirely realistic to reflect the real intentions of attackers by stochastic models. Then, the so-called queuing model was established and the effect of DoS attacks was treated as a special kind of network-induced delay. The concepts of DoS frequency and duration are used to constrain the attacker's behaviors. In such a way, it is possible to capture more types of DoS attacks. On this basis, [19] set constraints on sleeping and active time intervals of nonperiodic DoS attacks, which could be considered as an extension of DoS frequency and duration. When it comes to deception attacks, almost all related mathematical models in the literature belong to stochastic approaches [20], which do not give full attention to the deception attack itself, especially from the attacker's point of view. Deception attacks are a type of stealth attack, and time-varying attack behaviors contribute to evading security detection mechanisms. In this sense, it is of theoretical and practical significance to model deception attacks in terms of queuing approaches, which motivates us in the present work.

On the other hand, network resources are not scarce for current technologies, but idle resources take an outstanding role in the scene of emergency processing. To improve the utilization of network resources, event-based control strategies have been developed, for instance, [21] constructed an event-based sampling strategy, in which the control input was updated only at a bunch of discrete time instants; [22] considered the nature of digital information and proposed a novel event-triggered mechanism (ETM) with periodic sampling behaviors. This kind of ETM skillfully excludes the Zeno behavior as data can only be released at the sampling instants. These approaches have inspired a massive amount of outcomes [23–27] and the reference therein. In recent years, great efforts have been made to improve the ETMs. In [28], a new event-triggered data transmission scheme was proposed, in which the related triggering parameter was adaptive according to the variation of state error. [29] proposed a memory event-triggered scheme to reduce the redundant packet transmission, in which some recent released data were stored at the event generator. [30] investigated dynamic event-triggered control strategies, which gave rise to a larger inter-execution time compared to static strategies. In [31], a novel resilient triggering strategy was established by taking into account the uncertainty caused by DoS attacks. In [32], the event-triggered strategy and periodic control strategy were integrated to reduce the transmission delay caused by DoS attacks. It is worth noting that related work is still an ongoing research issue, especially for CPSs subject to cyber-attacks, e.g., it is a promising work to adjust event-triggered strategies in the presence of deception attacks, which inspires another motivation of this work.

The objective of this paper is to put forward the joint investigation of security requirements and resource constraints for nonlinear CPSs. Considering the network between system plant and remote controllers, T-S fuzzy models of the monitored system and controllers are designed separately to characterize the nonlinear factors. By combining with the attack detection technology, deception attacks are depicted as a kind of queuing model, which is composed of sleeping and active time intervals. Thus, diverse event-triggered strategies are designed for different attack modes to further save network resources. To sum up, the main contributions of this paper are summarized as follows:

(1) An improved T-S fuzzy model is employed to characterize the nonlinear factors of the monitored system and increase the design flexibility;

(2) Different from the stochastic approaches of deception attacks in the literature, a novel queuing model is developed based on real-time attack detection. To the best of the authors' knowledge, it is the first attempt to exploit such a queuing model;

(3) A new switched event-triggered communication scheme is proposed in this work. Compared to the improved schemes in [29,30], the new approach is adaptive for time-varying aggressive behaviors of deception attacks and can further alleviate the burden of network resources;

(4) By using piecewise Lyapunov functional methods, we find a solution to jointly design fuzzy controllers and event-triggering parameters, which can

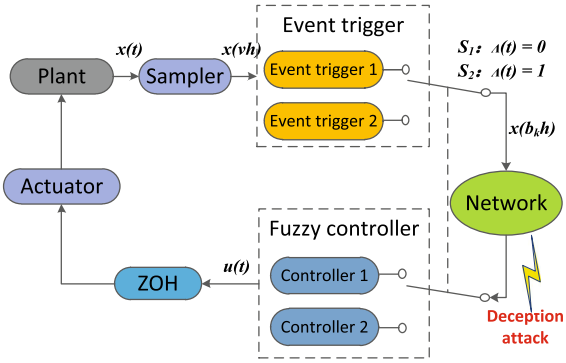

Fig. 1 System plant

guarantee the monitored system exponentially stable under cyber-attacks. Finally, a mass–spring–damper system is introduced to verify the effectiveness of the proposed approaches.

Notation: In this paper, $\mathbb{R}^{n_x}$ represents the n_x-dimensional Euclidean space, I is an identity matrix, and $\mathbb{R}^{n\times m}$ represents a $n \times m$ real matrix. For a matrix P, P^{-1} denotes its inverse while P^T is the transpose. For a symmetric matrix P, we define $\lambda_{min}(P)$ and $\lambda_{max}(P)$ as the minimum and maximal eigenvalue of P. For a real number h, $\lfloor h \rfloor$ means the largest integer no more than h. Without special declarations, matrices are assumed to have compatible dimensions.

2 Preliminaries

Figure 1 illustrates the designed event-based communication scheme for CPSs under deception attacks. The system state is periodically sampled, and the sampled data is transmitted over the network only when some preset conditions are satisfied, which is decided by the ETM. A zero-order holder (ZOH) is employed to keep the control information until next event occurs. It is noticeable that switched event triggers and controllers are adopted, which is relevant to the dynamic event-triggered strategies to be designed. In the following, the detailed models of fuzzy system, deception attacks, ETM, and fuzzy controllers will be demonstrated successively.

2.1 Physical plant

Consider a nonlinear cyber-physical system, which can be approximated by a T-S fuzzy model:

Plant rule i:
IF $\phi_1(x(t))$ is W_{i1} and $\cdots$ and $\phi_r(x(t))$ is W_{ir}
THEN

$$\dot{x}(t) = A_i x(t) + B_i u(t), \qquad i = 1, 2, \ldots, q \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$ and $u(t) \in \mathbb{R}^{n_u}$ are the state vector and control input, respectively; A_i, B_i are constant matrices with appropriate dimensions corresponding to rule i; q is the number of fuzzy rules, $\phi(x(t)) = [\phi_1(x(t)), \phi_2(x(t)), \ldots, \phi_r(x(t))]$ denotes the premise variable, W_{iv} $(v = 1, 2, \ldots, r)$ represents the fuzzy set.

Through the singleton fuzzifier, product interference, and center-average defuzzifier, the concerned system (1) can be expressed as

$$\dot{x}(t) = \sum_{i=1}^{q} \vartheta_i(\phi(t))[A_i x(t) + B_i u(t)] \tag{2}$$

where

$$\vartheta_i(\phi(x(t))) = \frac{\varpi_i(\phi(x(t)))}{\sum_{i=1}^{q} \varpi_i(\phi(x(t)))},$$
$$\varpi_i(\phi(x(t))) = \prod_{v=1}^{r} W_{iv}(\phi_v(x(t))).$$

Here, it is assumed that $\varpi_i(\phi(x(t))) > 0$ for all $t > 0$, which yields $\vartheta_i(\phi(x(t))) > 0$ and $\sum_{i=1}^{q} \vartheta_i(\phi(x(t))) = 1$. For simplicity, we use ϑ_i to represent $\vartheta_i(\phi(x(t)))$ in the following presentation.

Due to the network, fuzzy controllers and the system do not need to share the same premise variables [8], which can increase the design flexibility. The rule of the jth controller can be given by:
IF $\hat{\phi}_1(\hat{x}(t))$ is $\hat{W}_{j1}$ and $\cdots$ and $\hat{\phi}_p(\hat{x}(t))$ is $\hat{W}_{jp}$
THEN

$$u(t) = K_j \hat{x}(t), \qquad j = 1, 2, \ldots, q \tag{3}$$

where $\hat{x}(t)$ denotes the real state information arriving at the controller side through network, $K_j (j = 1, 2, \ldots, q)$ is the controller gain, $\hat{\phi}(\hat{x}(t)) = [\hat{\phi}_1(\hat{x}(t)), \hat{\phi}_2(\hat{x}(t)), \ldots, \hat{\phi}_p(\hat{x}(t))]$ and $\hat{W}_{jv}$ $(v = 1, 2, \ldots, p)$ are the premise variables and fuzzy sets, respectively.

The defuzzified form of (3) can be expressed as

$$u(t) = \sum_{j=1}^{q} \omega_j(\hat{\phi}(\hat{x}(t)))K_j \hat{x}(t) \tag{4}$$

where

$$\omega_j(\hat{\phi}(\hat{x}(t))) = \frac{\gamma_j(\hat{\phi}(\hat{x}(t)))}{\sum_{j=1}^{q}\gamma_j(\hat{\phi}(\hat{x}(t)))},$$
$$\gamma_j(\hat{\phi}(\hat{x}(t))) = \prod_{v=1}^{p}\hat{W}_{jv}(\hat{\phi}(\hat{x}(t))).$$

where the properties of $\gamma_j(\hat{\phi}(\hat{x}(t)))$ and $\omega_j(\hat{\phi}(\hat{x}(t)))$ can refer to the ones in the system model; similarly, we use ω_j to represent $\omega_j(\hat{\phi}(\hat{x}(t)))$.

Here, we make the following assumption, which is of great significance for detailed design work.

Assumption 1 During network transmission, the transmission delays and package losses are out of scope of this paper. Moreover, we assume the system states can be measured integrally.

2.2 Modelling of deception attacks

We consider a type of deception attacks, known as the false data injection attack, and the state information arriving at the controller side can be expressed as:

$$\hat{x}(t) = x(t) + \varsigma(t) \tag{5}$$

where $\varsigma(t)$ denotes the injected false data, which is a bounded energy signal.

Network security is a process of game between the attackers and defenders. From the perspective of attack detection, we define the following signal function:

$$\Lambda(t) = \begin{cases} 1, & t \in [f^n, f^n + f^n_{off}) \\ 2, & t \in [f^n + f^n_{off}, f^{n+1}) \end{cases} \tag{6}$$

where $0 \le f^n < f^n + f^n_{off} < f^{n+1}$ holds for $n \in \mathbb{N}$ and $\Lambda(t)$ is used to demonstrate whether the attack can be detected. We define $\Upsilon^1_n \triangleq [f^n, f^n + f^n_{off})$ as the sleeping time interval of deception attacks, which means the attack is weak enough to escape from network security mechanisms. In this situation, the energy signal $\varsigma(t)$ satisfies:

$$\| \varsigma(t) \|_2 \leqslant \varepsilon_1 \| x(t) \|_2, \qquad t \in [f^n, f^n + f^n_{off}) \tag{7}$$

Meanwhile, $\Upsilon^2_n \triangleq [f^n + f^n_{off}, f^{n+1})$ is regarded as the active time interval, which means the system suffers from a high level of malicious attack, and the energy signal $\varsigma(t)$ satisfies:

$$\varepsilon_1 \| x(t) \|_2 < \| \varsigma(t) \|_2 \leqslant \varepsilon_2 \| x(t) \|_2, \quad t \in [f^n + f^n_{off}, f^{n+1}) \tag{8}$$

Remark 1 Note that previous works dealing with deception attacks, such as [24,33], are inclined to model the attack as a stochastic process. Such approaches rely heavily on the intention of attackers, which is sometimes hard to determine in advance. Relatively, through real-time attack detection, the control approach can be designed much more precisely.

Inspired by the queueing model of DoS attacks in [19], it is reasonable to make the following assumption.

Assumption 2 For Υ^1_n, we can always find a scalar $f_{min} > 0$ satisfying

$$\inf_{n\in\mathbb{N}}\{f^n_{off}\} \ge f_{min} \tag{9}$$

For Υ^2_n, we can always find a scalar $f_{max} > 0$ satisfying

$$\sup_{n\in\mathbb{N}}\{f^n_{on}\} \le f_{max} \tag{10}$$

where $f^n_{on} = f^{n+1} - f^n - f^n_{off}$ is defined as the duration of the nth malicious attack.

Remark 2 Different from the simplicity of creating DoS attacks, attackers usually need to detect and gain some critical information of the target system, which yields $\varsigma(t) = \varsigma(x(t))$. Such a process will bring a noticeable rise in energy consumption. So, it is reasonable to set some power constraints for deception attacks. Through the lower bound f_{min} and the upper bound f_{max}, Assumption 2 depicts the constraints in terms of time duration.

Before proceeding further, we first make a modification on the model of deception attacks. As an event-triggered communication scheme is employed in Fig. 1, the analyzing emphasis is based on the sampling instants. Then, the attack sequences in Eq. (6) can be rewritten as

$$\Lambda(t) = \begin{cases} 1, & t \in [F^n, F^n + F^n_{off}) \\ 2, & t \in [F^n + F^n_{off}, F^{n+1}) \end{cases} \tag{11}$$

where $F^n = (\lfloor f^n/h \rfloor + 1)h$, $F^n_{off} = \{\lfloor (f^n + f^n_{off})/h \rfloor + 1\}h - F^n$, for more detailed definitions of F^n and F^n_{off}, we can refer to the ones in Eq. (6).

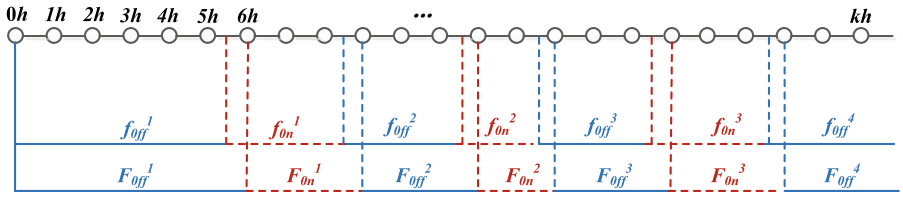

Fig. 2 Time sequence for intermittent deception attacks

Without loss of generality, we redefine $\Upsilon_n^1 \triangleq [F^n, F^n + F_{off}^n)$ as the sleeping time interval and $\Upsilon_n^2 \triangleq [F^n + F_{off}^n, F^{n+1})$ as the active time interval. Assumption 2 should also be updated as follows:

Assumption 3 For Υ_n^1, we can always find a scalar $F_{min} > 0$ satisfying

$$\inf_{n\in\mathbb{N}}\{F_{off}^n\} \geq F_{min} = \lfloor f_{min}/h \rfloor h \tag{12}$$

For Υ_n^2, we can always find a scalar $F_{max} > 0$ satisfying

$$\sup_{n\in\mathbb{N}}\{F_{on}^n\} \leq F_{max} = (\lfloor f_{max}/h \rfloor + 1)h \tag{13}$$

where $F_{on}^n = F^{n+1} - F^n - F_{off}^n$.

Remark 3 The modification on the model of deception attacks is precisely illustrated in Fig. 2. For example, the deception attack is detected between the fifth and sixth sampling instant. In the framework of the designed communication scheme, we can consider the sixth sampling instant as the initial point of an active time interval.

2.3 Design of switched event-triggered mechanism

Considering the signal function $\Lambda(t)$, a novel switched event-triggered mechanism is proposed:

$$b_{n,k+1}^{\Lambda(t)}h = b_{n,k}^{\Lambda(t)}h + \min_{s\geq 1, s\in\mathbb{N}}\Big\{sh \mid e^T(t)\Omega_{\Lambda(t)}e(t) - \delta x^T(b_{n,k}^{\Lambda(t)}h)\Omega_{\Lambda(t)}x(b_{n,k}^{\Lambda(t)}h) \geq \varrho(sh)\Big\} \tag{14}$$

in which

$$\varrho(sh) = \alpha\varepsilon_2(\Lambda(t) - 1)x^T(b_{n,k}^{\Lambda(t)}h + sh)\ \Omega_{\Lambda(t)}x(b_{n,k}^{\Lambda(t)}h + sh) \tag{15}$$

$$e(t) = x(b_{n,k}^{\Lambda(t)}h) - x(b_{n,k}^{\Lambda(t)}h + sh) \tag{16}$$

$$b_{n,0}^{\Lambda(t)}h \triangleq \begin{cases} F^n, & \Lambda(t) = 1 \\ F^n + F_{off}^n, & \Lambda(t) = 2 \end{cases} \tag{17}$$

where α and δ are predefined positive scalars, h is the sampling period. For $k \in \mathbb{N}$, $\{b_{n,k}^1\}$ are the releasing instants in the nth sleeping interval Υ_n^1 while $\{b_{n,k}^2\}$ are the releasing instants in the nth active interval Υ_n^2. $x(b_{n,k}^{\Lambda(t)}h + sh)$ denotes the current system state to be determine whether it should be transmitted. $\Omega_{\Lambda(t)} > 0$ is a weighting matrix to be designed.

Remark 4 In fact, the switched ETM (14) provides diverse triggering strategies corresponding to the malicious extent of deception attacks. When $\Lambda(t) = 1$, the triggering condition degenerates into the typical form as in [22]. When $\Lambda(t) = 2$, it is not needed that $e^T(t)\Omega_{\Lambda(t)}\, e(t) - \delta x^T(b_{n,k}^2 h)\Omega_{\Lambda(t)}x(b_{n,k}^2 h)$ keeps always negative as $\varrho(sh)$ remains positive. And a larger inter-execution time can be obtained. In fact, when the data is corrupted by malicious attacks, less data are expected to be released in the active interval. Note that the tendency of inter-execution time is related to the value of ε_2 in Eq. (8), and a larger ε_2 yields a larger inter-execution time. Moreover, it can be inferred from Eq. (17) that event triggerings are compulsorily executed at the sampling instants when off/on or on/off transitions occur. So, the following constraint relationships hold:

$$\begin{cases} \sup_{k\in\mathbb{N}}\{b_{n,k}^1 h\} < F^n + F_{off}^n \\ \sup_{k\in\mathbb{N}}\{b_{n,k}^2 h\} < F^{n+1} \end{cases} \tag{18}$$

Meanwhile, let $\lambda_n^1 \triangleq \sup\left\{k \mid b_{n,k}^1 h < F^n + F_{off}^n\right\}$ and $\lambda_n^2 \triangleq \sup\left\{k \mid b_{n,k}^2 h < F^{n+1}\right\}$. Without loss of generality, we assume $b_{n,\lambda_n^1+1}^1 h \triangleq F^n + F_{off}^n$ and $b_{n,\lambda_n^2+1}^2 h \triangleq F^{n+1}$, which will contribute to the analysis below.

2.4 The overall model

Referring to the work in [22], we divide $[b_{n,k}^{\Lambda(t)}h\ ,\ b_{n,k+1}^{\Lambda(t)}h)$ for $k \in \{0, 1, \ldots, \lambda_n^{\Lambda(t)}\}$ into $s_M + 1$ subin-

tervals with $s_M \in \mathbb{N}$. Each subinterval is expressed as $\chi_{n,k,s}^{\Lambda(t)} \triangleq [S_{n,k,s}^{\Lambda(t)}, S_{n,k,s+1}^{\Lambda(t)})$, where $S_{n,k,s}^{\Lambda(t)} \triangleq b_{n,k}^{\Lambda(t)} h + sh$, $\chi_{n,k,s}^{\Lambda(t)} \in \bigcup_{n\in\mathbb{N}} \Upsilon_n^{\Lambda(t)}$. Obviously, $[b_{n,k}^{\Lambda(t)} h, b_{n,k+1}^{\Lambda(t)} h) = \bigcup_{s=0}^{s_M} \chi_{n,k,s}^{\Lambda(t)}$.

For $t \in \chi_{n,k,s}^{\Lambda(t)}$, defining $\eta(t) = t - b_{n,k}^{\Lambda(t)} h - sh$ yields

$$0 \le \eta(t) < h \tag{19}$$

As a zero-order holder is employed in the physical plant, the control input can be expressed as

$$u(t) = \sum_{j=1}^{q} \omega_j K_{j,\Lambda(t)} \big(x(b_{n,k}^{\Lambda(t)} h) + \varsigma(t)\big), \quad t \in \chi_{n,k,s}^{\Lambda(t)} \tag{20}$$

where $\{K_{j,\Lambda(t)}\}$ are the cotroller gains.

According to the Eqs. (2), (19), (20), we obtain an overall closed-loop system model expressed as:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{q}\sum_{j=1}^{q} \vartheta_i \omega_j [A_i x(t) + B_i K_{j,\Lambda(t)} (e(t) \\ \qquad + x(t - \eta(t)) + \varsigma(t))], t \in \chi_{n,k,s}^{\Lambda(t)} \\ x(t) = \psi(t), \qquad t \in [-h, 0] \end{cases} \tag{21}$$

Definition 1 (Attack Frequency): Define $N(0,t) = \text{card}\left\{n \in \mathbb{N} \mid 0 < F^n + F_{off}^n < t\right\}$ as the number of off/on transitions of deception attacks over $(0,t)$, where card denotes the number of elements in the set. If there are constants $\tau_a > 0$ and $\nu > 0$ satisfying $N(0,t) \le \nu + t/\tau_a$, we say that the deception attack signal merged by Υ_n^1 and Υ_n^2 satisfies the attack frequency constraint described by τ_a and ν.

Definition 2 (Exponentially Stable): The concerned system (21) is guaranteed to be exponentially stable (ES), if there exist positive constants ϱ and ϵ such that $\| x(t) \| \le \epsilon e^{-\varrho t} \| \psi_0 \|_h$ holds for all $t > 0$, where $\| \psi_0 \|_h \triangleq sup_{-h\le\theta\le 0} \{\| x(\theta) \|, \| \dot{x}(\theta) \|\}$, ϱ is called the decay rate.

We are now in a position to begin the control issue as: based on the proposed switched ETM (14), the control objective is to design appropriate switched fuzzy controllers, which can guarantee the concerned system (21) ES under the deception attack signal (11).

3 Main results

Theorem 1 *For prescribed positive scalars $\delta \in (0,1)$, α, ε_m, β_m, $\mu_m \in (1,\infty)$, $m \in \{1,2\}$, F_{min}, F_{max}, τ_a and h satisfying*

$$\begin{aligned} \varrho = {} & (2\beta_1 F_{min} - 2(\beta_1 + \beta_2)h \\ & -2\beta_2 F_{max} - \ln(\mu_1\mu_2))/\tau_a > 0 \end{aligned} \tag{22}$$

The system (21) with given gain matrices K_{jm} is exponentially stable under the intermittent deception attack (11) if the membership functions satisfy $\omega_j - \iota_j \vartheta_j \ge 0$, and there exist $P_m > 0$, $Q_m > 0$, $R_m > 0$, $\Omega_m > 0$, and N_{ml}, M_{ml}, $l \in \{1,2\}$, $\Delta_i^m = \Delta_i^{m^T}$ with appropriate dimensions satisfying:

$$\begin{cases} P_1 \le \mu_2 P_2,\ P_2 \le \beta_0 \mu_1 P_1 \\ Q_1 \le \mu_2 Q_2,\ Q_2 \le \mu_1 Q_1 \\ R_1 \le \mu_2 R_2,\ R_2 \le \mu_1 R_1 \end{cases} \tag{23}$$

$$\Psi_{ij}^m - \Delta_i^m < 0, (i, j = 1, 2, \ldots, q) \tag{24}$$

$$\iota_i \Psi_{ii}^m - \iota_i \Delta_i^m + \Delta_i^m < 0 \tag{25}$$

$$\begin{aligned} & \iota_j \Psi_{ij}^m + \iota_i \Psi_{ji}^m - \iota_i \Delta_j^m - \iota_j \Delta_i^m + \Delta_i^m + \Delta_j^m \\ & < 0, i < j \end{aligned} \tag{26}$$

where

$$\Psi_{ij}^m = \begin{bmatrix} \Pi_{11}^m & * & * \\ \Pi_{21}^m & \Pi_{22}^m & * \\ \Pi_{31}^m & 0 & \Pi_{33}^m \end{bmatrix},$$

$$\Pi_{11}^m = \begin{bmatrix} \Xi_1^m & * & * & * & * \\ 0 & \Xi_2^m & * & * & * \\ K_{jm}^T B_i^T P_m & 0 & -\Omega_m & * & * \\ \Xi_3^m & N_{m1}^T - N_{m2} & 0 & \Xi_4^m & * \\ K_{j1}^T B_i^T P_1 & 0 & 0 & 0 & -I \end{bmatrix},$$

$$\Pi_{21}^m = \begin{bmatrix} \sqrt{h} A_i & 0 & \sqrt{h} B_i K_{jm} & \sqrt{h} B_i K_{jm} & \sqrt{h} B_i K_{jm} \\ 0 & 0 & \sqrt{\delta} & \sqrt{\delta} & 0 \\ 0 & 0 & \sqrt{\varepsilon_m} & \sqrt{\varepsilon_m} & 0 \end{bmatrix},$$

$$\Pi_{22}^m = diag\{-R_m^{-1}, -\Omega_m^{-1}, -I\},$$

$$\Pi_{31}^m = \begin{bmatrix} \sqrt{h} M_{m1}^T & 0 & 0 & \sqrt{h} M_{m2}^T & 0 \\ 0 & \sqrt{h} N_{m1}^T & 0 & \sqrt{h} N_{m2}^T & 0 \end{bmatrix},$$

$$\Pi_{33}^m = diag\{-e^{-2(2-m)\beta_m h} R_m, -e^{-2(2-m)\beta_m h} R_m\},$$

$$\begin{aligned} \Xi_1^m = {} & (-1)^{m-1} 2\beta_m P_m + A_i^T P_m + P_m A_i + Q_m \\ & + M_{m1} + M_{m1}^T, \end{aligned}$$

$$\Xi_2^m = -e^{(-1)^m 2\beta_m h} Q_m - N_{m1} - N_{m1}^T,$$

$$\Xi_3^m = K_{jm}^T B_i^T P_m - M_{m1}^T + M_{m2},$$

$$\begin{aligned} \Xi_4^m = {} & -M_{m2} - M_{m2}^T + N_{m2} \\ & + N_{m2}^T - (m-1)\alpha\varepsilon_2\Omega_2, \end{aligned}$$

$$\beta_0 = e^{2(\beta_1+\beta_2)h}.$$

Proof Without loss of generality, it is assumed that $m = 1$ and $m = 2$ are corresponding to the sleeping mode ($\Lambda(t) = 1$) and the active mode ($\Lambda(t) = 2$), respectively. The following Lyapunov–Krasovskii functional is adopted:

$$
\begin{aligned}
V_m(t) &= V_{m1}(t) + V_{m2}(t) + V_{m3}(t)\\
V_{m1}(t) &= x^T(t)P_m x(t)\\
V_{m2}(t) &= \int_{t-h}^{t} \kappa_m x^T(s)Q_m x(s)\mathrm{d}s\\
V_{m3}(t) &= \int_{-h}^{0}\int_{t+v}^{t} \kappa_m \dot{x}^T(s)R_m\dot{x}(s)\mathrm{d}s\mathrm{d}v
\end{aligned}
$$

□

where P_m, Q_m, and R_m are positive definite matrices, $\kappa_m \triangleq e^{2(-1)^m\beta_m(t-s)}$ and β_m is a positive scalar.

Case 1 Consider the situation that $t \in [S^m_{n,k,s}, S^m_{n,k,s+1})$ with $m = 1$. The time derivative of $V_{13}(t)$ is expressed as:

$$
\begin{aligned}
\dot{V}_{13}(t) =& -2\beta_1 V_{13}(t) + h\dot{x}^T(t)R_1\dot{x}(t)\\
&- \int_{t-h}^{t-\eta(t)} e^{-2\beta_1(t-s)}\dot{x}(s)^T R_1\dot{x}(s)\mathrm{d}s\\
&- \int_{t-\eta(t)}^{t} e^{-2\beta_1(t-s)}\dot{x}(s)^T R_1\dot{x}(s)\mathrm{d}s\\
&+ 2\xi_1^T(t)M_1G_1(t) + 2\xi_1^T(t)N_1G_2(t)
\end{aligned}
\tag{27}
$$

where

$$
\begin{aligned}
G_1(t) &= x(t) - x(t-\eta(t)) - \int_{t-\eta(t)}^{t}\dot{x}(s)\mathrm{d}s,\\
G_2(t) &= x(t-\eta(t)) - x(t-h) - \int_{t-h}^{t-\eta(t)}\dot{x}(s)\mathrm{d}s,\\
\xi_1(t) &= \left[x^T(t)\ x^T(t-h)\ e^T(t)\ x^T(t-\eta(t)\ \varsigma^T(t))\right]^T
\end{aligned}
$$

It is not difficult to derive that

$$
\begin{aligned}
-2\xi_1^T(t)M_1\int_{t-\eta(t)}^{t}\dot{x}(s)\mathrm{d}s \le\ & h\xi_1^T(t)M_1e^{2\beta_1 h}R_1^{-1}\\
& M_1^T\xi_1(t) + \int_{t-\eta(t)}^{t} e^{-2\beta_1 h}\dot{x}(s)R_1\dot{x}(s)\mathrm{d}s
\end{aligned}
\tag{28}
$$

$$
\begin{aligned}
-2\xi_1^T(t)N_1\int_{t-h}^{t-\eta(t)}\dot{x}(s)\mathrm{d}s \le\ & h\xi_1^T(t)N_1e^{2\beta_1 h}R_1^{-1}\\
& N_1^T\xi_1(t) + \int_{t-h}^{t-\eta(t)} e^{-2\beta_1 h}\dot{x}(s)R_1\dot{x}(s)\mathrm{d}s
\end{aligned}
\tag{29}
$$

Then, we define

$$
M_1 = \left[M_{11}^T\ 0\ 0\ M_{12}^T\ 0\right]^T,\ N_1 = \left[0\ N_{11}^T\ 0\ N_{12}^T\ 0\right]^T,
$$

where M_{11}, M_{12}, N_{11}, N_{12} are arbitrary matrices with suitable dimensions.

Combining the time derivative of $V_{11}(t)$, $V_{12}(t)$ and the Eqs. (21), (27), (28) and (29), one has

$$
\begin{aligned}
&\dot{V}_1(t) + 2\beta_1 V_1(t)\\
&\le \sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\big\{x^T(2\beta_1 P_1 + A_i^T P_1\\
&\quad + P_1A_i + Q_1 + M_{11} + M_{11}^T)x(t)\\
&\quad + 2x(t-\eta(t))^T(K_{j1}^T B_i^T P_1 - M_{11}^T\\
&\quad + M_{12})x(t)\\
&\quad + 2e(t)^T K_{j1}^T B_i^T P_1 x(t)\\
&\quad + 2\varsigma(t)^T K_{j1}^T B_i^T P_1 x(t)\\
&\quad + x^T(t-h)(-N_{11} - N_{11}^T)x(t-h)\\
&\quad + x^T(t-\eta(t))(-M_{12} - M_{12}^T + N_{12}\\
&\quad + N_{12}^T)x(t-\eta(t))\\
&\quad + x^T(t-\eta(t))(N_{11}^T - N_{12})x(t-h)\\
&\quad + h\xi_1^T(t)M_1e^{2\beta_1 h}R_1^{-1}M_1^T\xi_1(t)\\
&\quad + h\xi_1^T(t)N_1e^{2\beta_1 h}R_1^{-1}N_1^T\xi_1(t)\\
&\quad + e^T(t)\Omega_1 e(t) - e^T(t)\Omega_1 e(t)\\
&\quad + \varsigma(t)^T\varsigma(t) - \varsigma(t)^T\varsigma(t)\\
&\quad + h\dot{x}^T(t)R_1\dot{x}(t)\big\}
\end{aligned}
\tag{30}
$$

Taking consideration of the ETM (14), we gain

$$
\begin{aligned}
&\dot{V}_1(t) + 2\beta_1 V_1(t)\\
&\le \sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\xi_1^T(\Pi_{11}^1 - \Pi_{21}^{1^T}\Pi_{22}^{1^{-1}}\Pi_{21}^1\\
&\quad - \Pi_{31}^{1^T}\Pi_{33}^{1^{-1}}\Pi_{31}^1)\xi_1
\end{aligned}
\tag{31}
$$

Applying the Schur's complement to Eq. (31), it is indicated that $\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\Psi_{ij}^1 < 0$ is the sufficient condition to guarantee $\dot{V}_1(t) + 2\beta_1 V_1(t) < 0$.

Next, consider $\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\vartheta_j - \omega_j)\Delta_i^1 = \sum_{i=1}^{q}\vartheta_i\ (\sum_{j=1}^{q}\vartheta_j - \sum_{j=1}^{q}\omega_j)\Delta_i^1 = 0$, where $\Delta_i^1 = \Delta_i^{1^T}$, we have

$$
\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\Psi_{ij}^1 = \sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\Psi_{ij}^1
$$

$$
\begin{aligned}
&+\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\vartheta_j-\omega_j+\iota_j\vartheta_j-\iota_j\vartheta_j)\Delta_i^1\\
&=\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\omega_j+\iota_j\vartheta_j-\iota_j\vartheta_j)\Psi_{ij}^1\\
&+\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\vartheta_j\\
&-\iota_j\vartheta_j)\Delta_i^1-\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\omega_j-\iota_j\vartheta_j)\Delta_i^1\\
&=\sum_{i=1}^{q}\vartheta_i^2(\iota_i\Psi_{ii}^1-\iota_i\Delta_i^1+\Delta_i^1)\\
&+\sum_{i=1}^{q-1}\sum_{j=i+1}^{q}\vartheta_i\omega_j(\iota_j\Psi_{ij}^1\\
&-\iota_j\Delta_i^1+\Delta_i^1+\iota_i\Psi_{ji}^1-\iota_i\Delta_j^1+\Delta_j^1)\\
&+\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i(\omega_j-\iota_j\vartheta_j)(\Psi_{ij}^1-\Delta_i^1)
\end{aligned}
\tag{32}
$$

With $\omega_j-\iota_j\vartheta_j\geq 0$, it is clear that (24)–(26) are sufficient conditions to guarantee $\sum_{i=1}^{q}\sum_{j=1}^{q}\vartheta_i\omega_j\Psi_{ij}^1<0$, which yields

$$\dot{V}_1(t)+2\beta_1V_1(t)<0 \tag{33}$$

Integrating both sides of (33) for $t\in[S_{n,k,s}^1, S_{n,k,s+1}^1)$, one has

$$V_1(t)<e^{-2\beta_1(t-S_{n,k,s}^1)}V_1(S_{n,k,s}^1) \tag{34}$$

Case 2 Consider the situation that $t\in[S_{n,k,s}^m, S_{n,k,s+1}^m)$ with $m=2$. By conducting a similar analytical procedure as in Case 1, we conclude that the conditions (24)–(26) with $m=2$ can guarantee $\dot{V}_2(t)-2\beta_2V_2(t)<0$.

Integrating both sides of it for $t\in[S_{n,k,s}^2, S_{n,k,s+1}^2)$, we obtain

$$V_2(t)\leq e^{2\beta_2(t-S_{n,k,s}^2)}V_2(S_{n,k,s}^2) \tag{35}$$

According to the sufficient condition (23), it is not difficult to see that

$$\begin{cases} V_1(S_{n,k,s}^1))\leq\mu_2V_2(S_{n,k,s}^{1^-}))\\ V_2(S_{n,k,s}^2))\leq\beta_0\mu_1V_1(S_{n,k,s}^{2^-})) \end{cases} \tag{36}$$

where $\beta_0=e^{2(\beta_1+\beta_2)h}$.

Next, by combining cases 1 and 2, we try to gain the general relationship between $V(t)$ and $V(0)$ for all $t>0$. We assume that n off/on transitions of intermittent deception attacks occur within $(0,t)$, which yields $t\in[F^n+F_{off}^n, F^{n+1})$ or $t\in[F^{n+1}, F^{n+1}+F_{off}^{n+1})$.

For $t\in[F^n+F_{off}^n, F^{n+1})$ as shown in Fig. 3, combining Eqs. (34)–(36) and Assumption 3, we have

$$
\begin{aligned}
V(t)&\leq e^{2\beta_2(t-b_{n,0}^2)h}V_2(b_{n,0}^2h)\\
&\leq\beta_0\mu_1e^{2\beta_2(t-b_{n,0}^2h)}V_1(b_{n,0}^{2^-}h)\\
&\leq\beta_0\mu_1e^{2\beta_2(t-b_{n,0}^2h)}e^{-2\beta_1(b_{n,0}^2h-b_{n,0}^1h)}V_1(b_{n,0}^1h)\\
&\leq\beta_0\mu_1\mu_2e^{2\beta_2(t-b_{n,0}^2h)}e^{-2\beta_1(b_{n,0}^2h-b_{n,0}^1h)}V_1(b_{n,0}^{1^-}h)\\
&\vdots\\
&\leq\beta_0^n\mu_1^n\mu_2^{n-1}e^{2n\beta_2F_{max}}e^{-2n\beta_1F_{min}}V_1(0)\\
&\leq\beta_0^n\mu_1^n\mu_2^ne^{2n\beta_2F_{max}}e^{-2n\beta_1F_{min}}V_1(0)\\
&\leq e^{-\varrho t}V_1(0)
\end{aligned}
\tag{37}
$$

where $\varrho=(2\beta_1F_{min}-2(\beta_1+\beta_2)h-2\beta_2F_{max}-\ln(\mu_1\mu_2))/\tau_a$.

For $t\in[F^{n+1}, F^{n+1}+F_{off}^{n+1})$, similarly, we have

$$
\begin{aligned}
V(t)&\leq\beta_0^n\mu_1^n\mu_2^ne^{2n\beta_2F_{max}}e^{-2(n+1)\beta_1F_{min}}V_1(0)\\
&\leq e^{-2\beta_1F_{min}}e^{-\varrho t}V_1(0)\\
&\leq e^{-\varrho t}V_1(0)
\end{aligned}
\tag{38}
$$

From the constructed Lyapunov–Krasovskii functional, it is easy to see that

$$\lambda_1\parallel x(t)\parallel^2\leq V(0)\leq\epsilon\parallel\psi_0\parallel_h^2 \tag{39}$$

where $\epsilon=\lambda_2+h\lambda_3+(h^2/2)(\lambda_4+\lambda_5)>0$, $\lambda_1=min\{\lambda_{min}(P_m)\}$, $\lambda_2=max\{\lambda_{max}(P_m)\}$, $\lambda_3=max\{\lambda_{max}(Q_m)\}$, $\lambda_4=max\{\lambda_{max}(R_m)\}$, $m\in\{1,2\}$.

Taking (38) and (39) into account, it yields that

$$\parallel x(t)\parallel\leq\sqrt{\epsilon}e^{-\varrho/2t}\parallel\psi_0\parallel_h \tag{40}$$

So far, we can conclude that the concerned system (21) is exponentially stable with a decay rate $\varrho/2$. This completes the proof.

On this basis, we devote our attention to developing a co-design method for fuzzy controllers and event-triggering parameters.

Theorem 2 *For prescribed positive scalars $\delta\in(0,1)$, α, ε_m, β_m, $\mu_m\in(1,\infty)$, $m\in\{1,2\}$, F_{min}, F_{max}, τ_a, h, ρ_{ml}, $l\in\{1,2,3\}$ satisfying (22). The system (21) with controller gains $K_{jm}=Y_{jm}X_m^{-1}$ is exponentially stable under the intermittent deception attack (11) if the membership functions satisfy $\omega_j-\iota_j\vartheta_j\geq 0$, and*

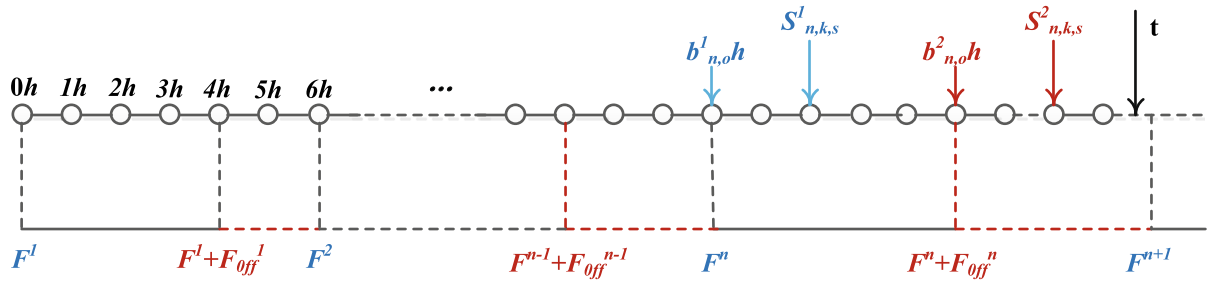

Fig. 3 Time sequence for intermittent deception attacks

there exist $X_m > 0$, $\widetilde{Q}_m > 0$, $\widetilde{R}_m > 0$, $\widetilde{\Omega}_m > 0$, *and* $\widetilde{N}_{ml}$, $\widetilde{M}_{ml}$, $\widetilde{\Delta}_i^m = \widetilde{\Delta}_i^{m^T}$ *with appropriate dimensions satisfying:*

$$\begin{cases} X_1 \le \beta_0\mu_1 X_2, X_2 \le \mu_2 X_1 \\ \widetilde{Q}_1 \le \mu_2\widetilde{Q}_2, \widetilde{Q}_2 \le \mu_1\widetilde{Q}_1 \\ \widetilde{R}_1 \le \mu_2\widetilde{R}_2, \widetilde{R}_2 \le \mu_1\widetilde{R}_1 \end{cases} \tag{41}$$

$$\widetilde{\Psi}_{ij}^m - \widetilde{\Delta}_i^m < 0, (i, j = 1, 2, \ldots, q) \tag{42}$$

$$\iota_i\widetilde{\Psi}_{ii}^m - \iota_i\widetilde{\Delta}_i^m + \widetilde{\Delta}_i^m < 0 \tag{43}$$

$$\iota_j\widetilde{\Psi}_{ij}^m + \iota_i\widetilde{\Psi}_{ji}^m - \iota_i\widetilde{\Delta}_j^m - \iota_j\widetilde{\Delta}_i^m + \widetilde{\Delta}_i^m + \widetilde{\Delta}_j^m < 0, i < j \tag{44}$$

where

$$\widetilde{\Psi}_{ij}^m = \begin{bmatrix} \widetilde{\Pi}_{11}^m & * & * \\ \widetilde{\Pi}_{21}^m & \widetilde{\Pi}_{22}^m & * \\ \widetilde{\Pi}_{31}^m & 0 & \widetilde{\Pi}_{33}^m \end{bmatrix},$$

$$\Pi_{11}^m = \begin{bmatrix} \widetilde{\Xi}_1^m & * & * & * & * \\ 0 & \widetilde{\Xi}_2^m & * & * & * \\ Y_{jm}^T B_i^T & 0 & -\widetilde{\Omega}_m & * & * \\ \widetilde{\Xi}_3^m & \widetilde{N}_{m1}^T - \widetilde{N}_{m2} & 0 & \widetilde{\Xi}_4^m & * \\ Y_{jm}^T B_i^T & 0 & 0 & 0 & -2\rho_{m3}X_m + \rho_{m3}^2 \end{bmatrix},$$

$$\widetilde{\Pi}_{21}^m = \begin{bmatrix} \sqrt{h}A_i X_m & 0 & \sqrt{h}B_i Y_{jm} & \sqrt{h}B_i Y_{jm} & \sqrt{h}B_i Y_{jm} \\ 0 & 0 & \sqrt{\delta}X_m & \sqrt{\delta}X_m & 0 \\ 0 & 0 & \sqrt{\varepsilon_m}X_m & \sqrt{\varepsilon_m}X_m & 0 \end{bmatrix},$$

$$\Pi_{22}^m = diag\{-2\rho_{m1}X_m + \rho_{m1}^2\widetilde{R}_m, -2\rho_{m2}X_m + \rho_{m2}^2\widetilde{\Omega}_m, -I\},$$

$$\Pi_{31}^m = \begin{bmatrix} \sqrt{h}\widetilde{M}_{m1}^T & 0 & 0 & \sqrt{h}\widetilde{M}_{m2}^T & 0 \\ 0 & \sqrt{h}\widetilde{N}_{m1}^T & 0 & \sqrt{h}\widetilde{N}_{m2}^T & 0 \end{bmatrix},$$

$$\Pi_{33}^m = diag\{-e^{-2(2-m)\beta_m h}\widetilde{R}_m, -e^{-2(2-m)\beta_m h}\widetilde{R}_m\},$$

$$\Xi_1^m = (-1)^{m-1}2\beta_m X_m + X_m A_i^T + A_i X_m + \widetilde{Q}_m + \widetilde{M}_{m1} + \widetilde{M}_{m1}^T,$$

$$\Xi_2^m = -e^{(-1)^m 2\beta_m h}\widetilde{Q}_m - \widetilde{N}_{m1} - \widetilde{N}_{m1}^T,$$

$$\Xi_3^m = Y_{jm}^T B_i^T - \widetilde{M}_{m1}^T + \widetilde{M}_{m2},$$

$$\Xi_4^m = -\widetilde{M}_{m2} - \widetilde{M}_{m2}^T + \widetilde{N}_{m2} + \widetilde{N}_{m2}^T - (m-1)\alpha\varepsilon_2\widetilde{\Omega}_2,$$

$$\beta_0 = e^{2(\beta_1+\beta_2)h}.$$

Proof According to Theorem 1, we assume that $X_m = P_m^{-1}$, $Y_{jm} = K_{jm}X_m$, $\widetilde{Q}_m = X_m Q_m X_m$, $\widetilde{R}_m = X_m R_m X_m$, $\widetilde{\Omega}_m = X_m\Omega_m X_m$, $\widetilde{M}_{ml} = X_m M_{ml} X_m$, $\widetilde{N}_{ml} = X_m N_{ml} X_m$, where $m \in \{1, 2\}$, $l \in \{1, 2\}$.

Meanwhile, we define

$$\begin{cases} \Phi_1 = diag\{I, I, I, I, I, P_1, P_1, I, I, I\}, \\ \Phi_2 = diag\{X, X, X, X, X, X, X, I, X, X\}. \end{cases}$$

For $P_m > 0$, $R_m > 0$ and $\rho_{m1} > 0$, we can find that $(\rho_{m1}R_m - P_m)R_m^{-1}(\rho_{m1}R_{im} - P_{im}) \ge 0$, which is equal to

$$-P_m R_m^{-1} P_m \le -2\rho_{m1}P_m + \rho_{m1}^2 R_m \tag{45}$$

Similarly, it is noticeable that

$$-P_m\Omega_m^{-1}P_m \le -2\rho_{m2}P_m + \rho_{m2}^2\Omega_m \tag{46}$$

$$-X_m I X_m \le -2\rho_{m3}X_m + \rho_{m3}^2 \tag{47}$$

Combining Eqs. (45)–(47), pre- and post- multiplying (24)–(26) with Φ_1 and Φ_2, and their transposes, successively, it is inferred that (42)–(44) are sufficient conditions of (24)–(26). And it yields that $\widetilde{\Delta}_i^m = \Phi_{m2}\Phi_{m1}\Delta_i^1\Phi_{m1}\Phi_{m2}$. Moreover, we can notice that Eq. (41) is equal to Eq. (23). Through the LMI Toolbox in MATLAB, we first obtain the matrices Y_{jm}, X_m and $\widetilde{\Omega}_m$. According to $Y_{jm} = K_{jm}X_m$, $\widetilde{\Omega}_m = X_m\Omega_m X_m$, we can get the fuzzy controller gains and the ETM parameters as $K_{jm} = Y_{jm}X_m^{-1}$, $\Omega_m = X_m^{-1}\widetilde{\Omega}_m X_m^{-1}$. The proof is completed. □

4 Simulation examples

A mass–spring–damper system is considered to verify the proposed approach [34], whose dynamic equation is defined as:

$$m\ddot{x} + F_f + F_s = u(t) \tag{48}$$

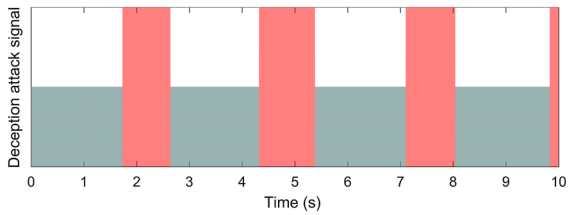

Fig. 4 Deception attack signal

where m is the mass, x denotes the displacement from a reference point, u(t) stands for the external control input. The fricion force F_f is defined as $F_f = c\dot{x}$ with $c > 0$; the restoring force of the spring F_s is given by $F_s = \hat{k}(1 + a^2x^2)x$ with constants $\hat{k}$ and a. Then, the dynamic equation can be rewritten as:

$$m\ddot{x} + c\dot{x} + \hat{k}x + \hat{k}a^2x^3 = u(t) \tag{49}$$

Define $x(t) = [x_1(t) \quad x_2(t)]^T$, where $x_1(t) = x$ and $x_2(t) = \dot{x}$. Let $x_1(t) \in [-2, 2]$, $m = 1kg$, $c = 2N \cdot m/s$, $\hat{k} = 8$, and $a = 0.3m^{-1}$. We choose $x_1(t)$ as the premise variable and construct a T-S fuzzy model for (49):

Plant rule 1: **IF** $x_1(t)$ is ± 2, **THEN**

$$\dot{x}(t) = A_1x(t) + B_1u(t) \tag{50}$$

Plant rule 2: **IF** $x_1(t)$ is 0, **THEN**

$$\dot{x}(t) = A_2x(t) + B_2u(t) \tag{51}$$

where the corresponding matrices can be given as:

$$A_1 = \begin{bmatrix} 0 & 1 \\ \frac{-\hat{k}-4\hat{k}a^2}{m} & -\frac{c}{m} \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 \\ \frac{-\hat{k}}{m} & -\frac{c}{m} \end{bmatrix},$$
$$B_1 = \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix}, B_2 = \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix}.$$

According to the modeling method in [34], the membership functions can be defined as $\vartheta_1 = x_1^2(t)/4$ and $\vartheta_2 = 1 - \vartheta_1$.

As shown in Fig. 4, a deception attack signal is considered with power-constrained parameters $f_{min} = 200h$, $f_{max} = 80h$. According to Assumption 3, we have $F_{min} = 200h$, $F_{max} = 81h$, where the sampling period is set as $h = 0.01$. In the sleeping time intervals, the gray area in Fig. 4, the function of deception attacks is assumed to be $\varsigma(t) = \begin{bmatrix} -tanh(0.1x_1(t)) \\ -tanh(0.1x_2(t)) \end{bmatrix}$. In the active time intervals, the red area in Fig. 4, we set $\varsigma(t) = \begin{bmatrix} -tanh(0.8x_1(t)) \\ -tanh(0.8x_2(t)) \end{bmatrix}$. It is clear that $\varepsilon_1 = 0.1$ and $\varepsilon_2 = 0.8$ can be gained. Moreover,

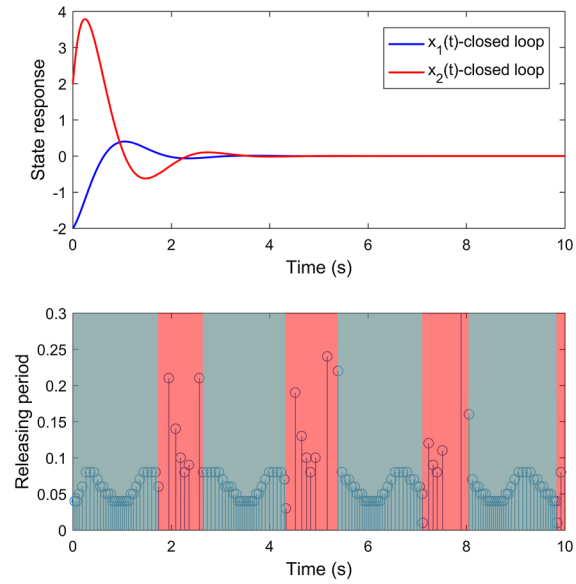

Fig. 5 State responses and releasing period

the other parameters involved in Theorem 2 are chosen as: $\beta_1 = 0.25$, $\beta_2 = 0.15$, $\mu_1 = 1.05$, $\mu_2 = 1.05$, $\rho_{11} = \rho_{12} = \rho_{21} = \rho_{22} = 1.5$, $\rho_{23} = \rho_{33} = 1.2$, $\alpha = 1.1$, $\iota_1 = 0.1$, $\iota_2 = 0.08$ and $\delta = 0.2$, which satisfies the sufficient condition (22). By using the LMI toolbox, feasible solutions of the inequations in Theorem 2 can be found. The weighting matrices of the ETM and the controller gains are given as

$$\Omega_1 = \begin{bmatrix} 0.9954 & 0.1463 \\ 0.1463 & 0.2626 \end{bmatrix},$$
$$\Omega_2 = \begin{bmatrix} 0.2876 & -0.0284 \\ -0.0284 & 0.2296 \end{bmatrix} \tag{52}$$

$$\begin{cases} K_{11} = \begin{bmatrix} 0.246 & -0.640 \end{bmatrix}, & K_{12} = \begin{bmatrix} 0.367 & -1.087 \end{bmatrix} \\ K_{21} = \begin{bmatrix} 0.217 & -0.601 \end{bmatrix}, & K_{22} = \begin{bmatrix} 0.396 & -1.292 \end{bmatrix} \end{cases} \tag{53}$$

For simulation purposes, we choose the initial state as $x_0 = \begin{bmatrix} -2 & 2 \end{bmatrix}^T$. The state responses and corresponding releasing period are depicted in Fig. 5. Some preliminary conclusions can be drawn as follows: the concerned system is asymptotic stable in the presence of deception attacks; comparatively well control performance can be gained owing to the adopted fuzzy control approach; and with the proposed ETM, network resources are saved observably. Only 143 sampled data are transmitted to the controller side while 1000 data

Table 1 Releasing number N_r for different values of δ

δ	0.05	0.1	0.2	0.3	0.4
N_r	247	192	143	122	99

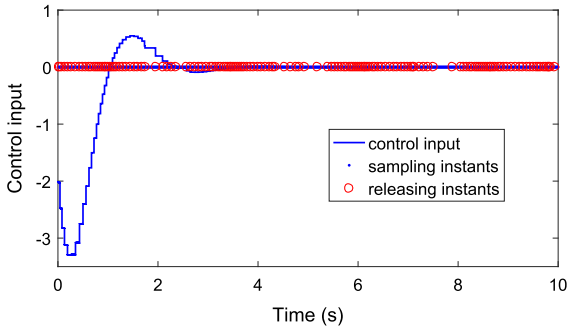

Fig. 6 Response of the control input

Table 2 Parameter settings and simulation results

Method	α	f_{max}	Releasing number
Switched ETM	0.5	80h	143
Switched ETM	0.3	80h	151
Switched ETM	0.1	80h	162
Switched ETM	0.05	80h	171
Switched ETM	0.01	80h	183

are sampled in total over [0,10s]. Comparative experiments are conducted with various values of δ. As shown in Table 1, the larger the triggering parameter δ, the fewer sampled data are transmitted. Figure 6 illustrates the responses of the control input, which is a piecewise continuous signal.

In Fig. 5, compared to the sleeping interval of deception attacks, it is clear that fewer data are triggered in the active interval. The switched ETM gives rise to a larger inter-execution time while the control performance remains a good level. Table 2 demonstrates that larger α yields a smaller releasing number. That is, the network resource utilization can be further enhanced. It is worth pointing out that there is always a certain upper bound for α when ε_2 is prescribed.

To further verify the effectiveness of the proposed communication scheme, the simulation result of the original ETM as in [22] is illustrated in Figs. 7 and 8. The triggering trend in the active interval is the same as that in the sleeping interval. 263 (143, in Fig. 5) sam-

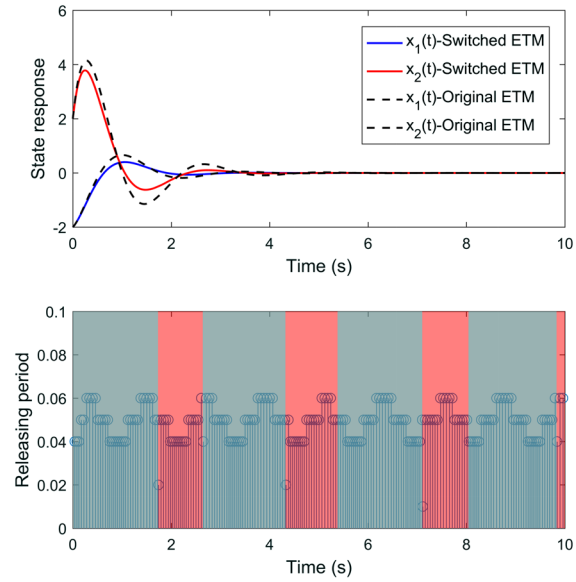

Fig. 7 State responses and releasing period

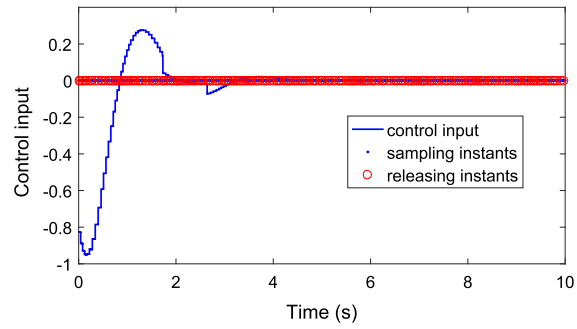

Fig. 8 Response of the control input

pled data are transmitted through the network while the control performance has no advantage over the one in Fig. 5. In fact, when the system is under a high level of malicious attack, on the contrary, more control information will degrade the system performance. So, it is inferred that the switched ETM is superior to the original ETM under this circumstances.

On another hand, an inter restricted relationship between F_{min} and F_{max} are involved in the sufficient condition (22). For prescribed parameters $\beta_1 = 0.09$, $\beta_2 = 0.15$, $\mu_1 = 1.05$, $\mu_2 = 1.05$, and $\tau_a = 0.4$, Tables 3, 4 and 5 shows the comparative results. Table 3 lists the maximum F_{max} allowed for every value of F_{min}. From Tables 4 and 5, we can notice that a larger sleeping interval of deception attacks generates a larger decay rate, while the larger the active interval,

Table 3 Restricted relationship between F_{min} and F_{max}

F_{min}	1	2	3	4	5
F_{max}	0.25	0.81	1.46	2.06	2.66

Table 4 Decay rate for different values of F_{max}

F_{max}	0.1	0.2	0.4	0.6	0.8
$\varrho/2$	0.2276	0.1976	0.1376	0.0776	0.0176

Table 5 Decay rate for different values of F_{min}

F_{min}	2	3	4	5	6
$\varrho/2$	0.0176	0.1976	0.3776	0.5576	0.7376

the smaller the decay rate. This result is consistent with the negative impact of deception attacks in the active interval.

5 Conclusion

This paper has investigated the event-triggered control issue of CPSs subject to deception attacks. A queuing model is constructed to depict the cyber-attack. Then, a novel event-based communication scheme is proposed to further optimize network resources, which is dynamically switched corresponding with different attack modes. By piecewise Lyapunov functional approaches, the fuzzy controllers and event triggering parameters have been jointly designed. Finally, the effectiveness of the proposed approach is verified by a mass–spring–damper system, which is asymptotic stable with the proposed switched ETM under deception attacks. In our future work, we will extend the proposed method to the CPSs with exogenous disturbances in the presence of more general cyber-attacks. It is not a simple combination but another interesting research venue.

Acknowledgements This work was supported by a grant from the National Natural Science Foundation of China No. 52005266.

Author contributions The objective of this paper is to put forward the joint investigation of security requirements and resource constraints, which is one of the research hot spots in the field of cyber-physical systems (CPSs). In this work, an improved T-S fuzzy model is employed to characterize the nonlinear factors of the monitored system and increase the design flexibility. Different from the stochastic approaches of deception attacks in the literature, a novel queuing model is developed based on real-time attack detection. To the best of the authors' knowledge, it is the first attempt to exploit such a queuing model. A new switched event-triggered communication scheme is proposed in this work. Compared to the existing improved schemes, the new approach is adaptive for time-varying aggressive behaviors of deception attacks, and can further alleviate the burden of network resources. By using piecewise Lyapunov functional methods, we find a solution to jointly design fuzzy controllers and event-triggering parameters, which can guarantee the monitored system exponentially stable. Finally, a mass–spring–damper system is introduced to verify the effectiveness of the proposed approaches.

Funding This work was supported by a grant from the National Natural Science Foundation of China No. 52005266.

Availability of data and material All data generated or analyzed during this study are included in this manuscript and its supplementary information files.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Code availability The codes used during the current study are available from the corresponding author on reasonable request.

References

1. Yan, J., Yang, X., Luo, X., Guan, X.: Dynamic gain control of teleoperating cyber-physical system with time-varying delay. Nonlinear Dyn. **95**(4), 3049–3062 (2019)
2. Wang, X., Park, J.H., Liu, H., Zhang, X.: Cooperative output-feedback secure control of distributed linear cyber-physical systems resist intermittent dos attacks. IEEE Trans. Cybern. (2020). https://doi.org/10.1109/TCYB.2020.3034374
3. Chen, D., Sun, D., Liu, H., Zhao, M., Li, Y., Wan, P.: Robust control for cooperative driving system of heterogeneous vehicles with parameter uncertainties and communication constraints in the vicinity of traffic signals. Nonlinear Dyn. **99**(2), 1659–1674 (2020)
4. Zhang, D., Xu, Z., Karimi, H.R., Wang, Q.: Distributed filtering for switched linear systems with sensor networks in presence of packet dropouts and quantization. IEEE Trans. Circuits Syst. I Regul. Pap. **64**(10), 2783–2796 (2017)
5. Gu, Z., Ahn, C.K., Yue, D., Xie, X.: Event-triggered H_∞ filtering for t-s fuzzy-model-based nonlinear networked systems with multisensors against dos attacks. IEEE Trans. Cybern. (2020). https://doi.org/10.1109/TCYB.2020.3030028
6. Li, H., Wu, C., Wu, L., Lam, H.K., Gao, Y.: Filtering of interval type-2 fuzzy systems with intermittent measurements. IEEE Trans. Cybern. **46**(3), 668–678 (2017)
7. Liu, J., Wei, L., Xie, X., Tian, E., Fei, S.: Quantized stabilization for t-s fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. IEEE Trans. Fuzzy Syst. **26**(6), 3820–3834 (2018)

8. Pan, Y., Yang, G.H.: Novel event-triggered filter design for nonlinear networked control systems. J. Franklin Inst. **355**(3), 1259–1277 (2018)
9. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security: a survey. IEEE Internet Things J. **4**(6), 1802–1831 (2017)
10. Ding, D., Wang, Z., Ho, D.W.C., Wei, G.: Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. IEEE Trans. Cybern. **47**(8), 1936–1947 (2017)
11. Liu, S., Li, S., Xu, B.: Event-triggered resilient control for cyber-physical system under denial-of-service attacks. Int. J. Control **93**(8), 1907–1919 (2020)
12. Sun, Y.C., Yang, G.H.: Event-triggered resilient control for cyber-physical systems under asynchronous dos attacks. Inf. Sci. **465**, 340–352 (2018)
13. Zhang, Z.H., Liu, D., Deng, C., Fan, Q.Y.: A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous dos attacks. Inf. Sci. **519**, 260–272 (2020)
14. Rong, N., Wang, Z.: State-dependent asynchronous intermittent control for it2 ts fuzzy interconnected systems under deception attacks. Nonlinear Dyn. **100**(4), 3433–3448 (2020)
15. Fu, W., Qin, J., Shi, Y., Zheng, W.X., Kang, Y.: Resilient consensus of discrete-time complex cyber-physical networks under deception attacks. IEEE Trans. Industr. Inf. **16**(7), 4868–4877 (2020)
16. Amin, S., Schwartz, G.A., Shankar Sastry, S.: Security of interdependent and identical networked control systems. Automatica **49**(1), 186–192 (2013)
17. Befekadu, G.K., Gupta, V., Antsaklis, P.J.: Risk-sensitive control under Markov modulated denial-of-service (dos) attack strategies. IEEE Trans. Autom. Control **60**(12), 3299–3304 (2015)
18. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Trans. Autom. Control **60**(11), 2930–2944 (2015)
19. Chen, X., Hu, S., Yue, D., Xie, X., Dou, C.: Attack-tolerant switched fault detection filter for networked stochastic systems under resilient event-triggered scheme. IEEE Trans. Syst. Man Cybern. Syst. (2020). https://doi.org/10.1109/TSMC.2020.3035768
20. Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A.: Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges. Neurocomputing **338**, 101–115 (2019)
21. De Persis, C., Frasca, P.: Robust self-triggered coordination with ternary controllers. IEEE Trans. Autom. Control **58**(12), 3024–3038 (2013)
22. Yue, D., Tian, E., Han, Q.: A delay system method for designing event-triggered controllers of networked control systems. IEEE Trans. Autom. Control **58**(2), 475–481 (2013)
23. Xiao, X., Park, J.H., Zhou, L., Lu, G.: Event-triggered control of discrete-time switched linear systems with network transmission delays. Automatica **111**, 1–6 (2020)
24. Liu, J., Yang, M., Xie, X., Peng, C., Yan, H.: Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. IEEE Trans. Circuits Syst. I Regul. Pap. **67**(3), 1021–1034 (2020)
25. Peng, C., Zhang, J., Han, Q.L.: Consensus of multiagent systems with nonlinear dynamics using an integrated sampled-data-based event-triggered communication scheme. IEEE Trans. Syst. Man Cybern. Syst. **49**(3), 589–599 (2019)
26. Zhang, K., Zhao, T., Dian, S.: Dynamic output feedback control for nonlinear networked control systems with a two-terminal event-triggered mechanism. Nonlinear Dyn. **100**(3), 2537–2555 (2020)
27. Hu, S., Yuan, P., Yue, D., Dou, C., Cheng, Z., Zhang, Y.: Attack-resilient event-triggered controller design of dc microgrids under dos attacks. IEEE Trans. Circuits Syst. I Regul. Pap. **67**(2), 699–710 (2020)
28. Gu, Z., Yue, D., Tian, E.: On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems. Inf. Sci. **422**, 257–270 (2017)
29. Tian, E., Wang, K., Zhao, X., Shen, S., Liu, J.: An improved memory-event-triggered control for networked control systems. J. Franklin Inst. **356**(13), 7210–7223 (2019)
30. Luo, S., Deng, F., Chen, W.H.: Dynamic event-triggered control for linear stochastic systems with sporadic measurements and communication delays. Automatica **107**, 86–94 (2019)
31. Sun, H., Peng, C., Zhang, W., Yang, T., Wang, Z.: Security-based resilient event-triggered control of networked control systems under denial of service attacks. J. Franklin Inst. **356**(17), 10277–10295 (2019)
32. Sun, Y.C., Yang, G.H.: Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. J. Franklin Inst. **355**(13), 5613–5631 (2018)
33. Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A.: Secure control of cyber physical systems subject to stochastic distributed dos and deception attacks. Int. J. Syst. Sci. **51**(9), 1653–1668 (2020)
34. Li, H., Pan, Y., Shi, P., Shi, Y.: Switched fuzzy output feedback control and its application to mass-spring-damping system. IEEE Trans. Fuzzy Syst. **24**(99), 1259–1269 (2016)