Resilient Event-based Control for Nonlinear Cyber-Physical Systems under Intermittent Deception Attacks

Fan Yang · Zhou Gu · Shen Yan

Received: date / Accepted: date

Abstract We address the resilient 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 attacker’s point of view, we construct a novel queuing model to depict the intermittent behaviors of deception attacks. Then, a resilient event-based communication scheme is proposed, which is dynamically switched 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 approaches to a mass–spring–damping system, where the effectiveness is well verified.

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

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, health-care 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 in the design of fuzzy systems and fuzzy controllers, an imperfect premise matching 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 interconnections 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 CPS’s 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 the 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 action. In such a way, it is possible to capture more types of DoS attacks. On this basis, [19] set the constraints on sleeping and active intervals of nonperiodic DoS attacks, which can 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 don’t give full attention to the deception attack itself, especially from the attacker’s point of view. Deception attacks are a type of stealth attacks, and intermittent 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, frequency and duration, which motivates us in present work.

On another hand, network resources are not scarce for current technologies, but idle resources takes an outstanding role in the scene of an emergency. To improve the utilization of network resources, event-triggered control strategies have been developed, for instances, [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. 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 the CPSs subject to cyber attacks, e.g., it is a promising work to adjust the event-triggered strategy 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, the T-S fuzzy models of the monitored system and controllers are designed separately to characterize the nonlinear factors. Unlike previous stochastic approaches, deception attacks in present work are depicted as a kind of queuing model, which is closer to the real intention of attackers. To the best of the authors’ knowledge, it is the first attempt to exploit such a queuing model. Moreover, this work devotes to the perfection of ETMs. Compared to the improved schemes [29–32], the properties of deception attacks are tightly integrated in the design of event-triggered strategies. To sum up, the main contributions of this paper are summarized as follows: 1) Improved T-S fuzzy models are employed to increase the design flexibility; and a novel queuing model is constructed to depict deception attacks; 2) A new dynamic event-triggered communication scheme is developed to alleviate the burden of network resources, which is adaptive for the intermittent aggressive behaviors of deception attacks; and 3) By using piecewise Lyapunov functional methods, we propose a solution to jointly design fuzzy controllers and event-triggering parameters, which can guarantee the monitored system exponentially stable under deception attacks. Finally, a mass–spring–damping system is introduced to verify the effectiveness of the proposed approaches.

**Notation:** In this paper, $\mathbb{R}^n$ represents the $n$-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

Fig. 1 illustrates a typical event-based communication scheme for CPSs under deception attacks. The sys-
tem state is periodically sampled, and the sampled data is transmitted over the network only when some pre-set conditions are satisfied, for instance, the system error exceeds a prescribed threshold, which is decided by the event trigger. A zero-order-holder (ZOH) is employed to keep the control information until next event occurs. It is noticeable that switching 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 $i$:

\[
\text{IF } \phi_i(x(t)) \text{ is } W_{i1} \text{ and } \ldots \text{ and } \phi_r(x(t)) \text{ is } W_{ir} \text{ THEN } x(t) = A_i x(t) + B_i u(t), \quad i = 1, 2, \ldots, q
\]

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, $\phi(x(t)) = [\phi_1(x(t)), \phi_2(x(t)), \ldots, \phi_r(x(t))]$ denote the premise variables, $W_{iv}$ $(v = 1, 2, \ldots, r)$ represent the fuzzy sets.

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

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

where

\[
\vartheta_i(\phi(x(t))) = \frac{\omega_i(\phi(x(t)))}{\sum_{i=1}^{q} \omega_i(\phi(x(t)))},
\]

\[
\omega_i(\phi(x(t))) = \prod_{v=1}^{p} W_{iv}(\phi(x(t))).
\]

Here, it is assumed that $\omega_i(\phi(x(t))) > 0$ 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 $\vartheta_i$ to represent $\vartheta_i(\phi(x(t)))$ in the following presentation.

Due to the presence of the network, fuzzy controllers and the system model do not need to share the same premise variables [8], which can increase the design flexibility. The rule of the $j$th controller can be given by

\[
\text{IF } \hat{\phi}_j(\hat{x}(t)) \text{ is } W_{j1} \text{ and } \ldots \text{ and } \hat{\phi}_p(\hat{x}(t)) \text{ is } W_{jp} \text{ THEN } u(t) = K_j \hat{x}(t), \quad j = 1, 2, \ldots, q
\]

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 $W_{jv}$ $(v = 1, 2, \ldots, p)$ are the premise variables and fuzzy sets, respectively.

The defuzzified form of (3) can be expressed as

\[
u(t) = \sum_{j=1}^{q} \omega_j(\hat{\phi}(\hat{x}(t)))K_j \hat{x}(t)
\]

where

\[
\omega_j(\hat{\phi}(\hat{x}(t))) = \frac{\gamma_j(\hat{\phi}(\hat{x}(t)))}{\sum_{j=1}^{q} \gamma_j(\hat{\phi}(\hat{x}(t)))},
\]

\[
\gamma_j(\hat{\phi}(\hat{x}(t))) = \prod_{v=1}^{p} W_{jv}(\hat{\phi}(\hat{x}(t))).
\]

Here, we consider the following assumption, which are 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.

**Assumption 2** Network security is a process of game. The attackers devote themselves to escaping from network security mechanisms while the defenders try to detect and resist attacks effectively. For CPSs, it is a tough work to segregate the attack completely at the network layer while network control approaches can be considered as a kind of security arrangements. The cyber attacks in this work are assumed to be detectable, which contributes to controller design for better system performance.
2.2 Modelling of Deception Attacks

We consider a kind of intermittent attack signal expressed as:

\[
A(t) = \begin{cases} 
1, & t \in [f^n, f^n + f_{\text{off}}^n) \\
2, & t \in [f^n + f_{\text{off}}^n, f^{n+1})
\end{cases}
\]  

(5)

where \(\{f^n + f_{\text{off}}^n\}\) stand for the time instants when the deception attack begins to act on the system with \(0 \leq f^n < f^n + f_{\text{off}}^n < f^{n+1}\) for \(n \in \mathbb{N}\). From the definition, we define \(\Upsilon_1^n \triangleq [f^n, f^n + f_{\text{off}}^n)\) as the sleeping time interval of the malicious attack while \(\Upsilon_2^n \triangleq [f^n + f_{\text{off}}^n, f^{n+1})\) is regarded as the active time interval. Inspired by [19], it is reasonable to make the following assumption.

**Assumption 3** For \(\Upsilon_1^n\), we can always find a scalar \(f_{\text{min}} > 0\) satisfying

\[
\inf_{n \in \mathbb{N}} \{f_{\text{off}}^n\} \geq f_{\text{min}}
\]  

(6)

For \(\Upsilon_2^n\), we can always find a scalar \(f_{\text{max}} > 0\) satisfying

\[
\sup_{n \in \mathbb{N}} \{f_{\text{on}}^n\} \leq f_{\text{max}}
\]  

(7)

where \(f_{\text{on}}^n = f^{n+1} - f^n - f_{\text{off}}^n\) is defined as the duration of the \(n\)th attack.

**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 intentions of attackers, which are sometimes hard to determine in advance. Relatively, inspired by the queuing model of DoS attacks in [19], the intermittent deception attack signal is considered as a combination of sleeping time intervals and active time intervals. From the attacker’s point of view, such intermittent aggressive behaviours can create more confusion for security detection and a high level of malicious attack may be produced in a finite-time active interval.

**Remark 2** Different from the simplicity of creating DoS attacks, the deception attackers usually need to detect and gain some critical information of the target system. Such a process will bring a noticeable rise in energy consumption. So, it is reasonable to set some power constraints for intermittent deception attacks. Through the lower bound \(f_{\text{min}}\) and the upper bound \(f_{\text{max}}\). Assumption 3 depicts the constraints in terms of time duration.

Under the above deception attack, the real state information in (4) can be rewritten as

\[
\dot{x}(t) = x(t) + (A(t) - 1)\zeta(t)
\]  

(8)

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

**Assumption 4** It is assumed that the energy signal \(\zeta(t)\) satisfies:

\[
\|\zeta(t)\|_2 \leq \varepsilon \|x(t)\|_2
\]  

(9)

where the constant \(\varepsilon\) is determined by the characteristics of malicious attacks.

**Remark 3** Note that deception attacks aim to make the system deviate from the expected performance while they make efforts to avoid security monitoring. A customary approach is to produce the attack signal on the basis of the current system state with \(\zeta(t) = \zeta(x(t))\). So, Assumption 4 is reasonable from the attackers perspective.

Before proceeding further, we first make a modification on the model of deception attacks. As an event-triggered communication scheme with periodic sampling is employed in Fig. 1, the analyzing emphasis is laid on the sampling instants. From this point of view, the attack sequences in Eq. (5) can be rewritten as

\[
A(t) = \begin{cases} 
1, & t \in [F^n, F^n + F_{\text{off}}^n) \\
2, & t \in [F^n + F_{\text{off}}^n, F^{n+1})
\end{cases}
\]  

(10)

where \(F^n = (\lfloor f^n/h \rfloor + 1)h\), \(F_{\text{off}}^n = \lfloor (f^n + f_{\text{off}}^n)/h \rfloor + 1\) \(h - F^n\), for more detailed definitions of \(F^n\) and \(F_{\text{off}}\), we can refer to the ones in Eq. (5).

Without loss of generality, we redefine \(\Upsilon_1^n \triangleq [F^n, F^n + F_{\text{off}}^n)\) as the sleeping time interval and \(\Upsilon_2^n \triangleq [F^n + F_{\text{off}}^n, F^{n+1})\) the active time interval. Assumption 3 should also be updated as follows.
Assumption 5 For $T_n^1$, we can always find a scalar $F_{\min} > 0$ satisfying
\[
\inf_{n \in \mathbb{N}} \{ F_{\text{on}}^n \} \geq F_{\min} = \lfloor f_{\min}/h \rfloor h
\]  
(11)
For $T_n^2$, we can always find a scalar $F_{\max} > 0$ satisfying
\[
\sup_{n \in \mathbb{N}} \{ F_{\text{on}}^n \} \leq F_{\max} = (\lfloor f_{\max}/h \rfloor + 1)h
\]  
(12)
where $F_{\text{on}}^n = F_{\max} + F_{\text{off}}^n$.

Remark 4 The modification on the model of deception attacks is precisely illustrated in Fig. 2. For example, the deception attack arrives between the 5th and 6th sampling instant. In the framework of the designed communication scheme, we can consider the 6th sampling instant as the initial point of an effective attack. Such treatments make the behaviors of deception attacks synchronized with the event-triggered mechanism to be designed.

2.3 Design of Resilient Event-Triggered Mechanism

Inspired by [22], an improved event-triggered mechanism is proposed with consideration of the malicious attacks:
\[
b_{\text{on}}^{(t)}(n, k+1) h = b_{\text{on}}^{(t)}(n, k) h + \min_{s \geq 1, s \in \mathbb{N}} \{ sh | e_{\text{sup}}(t) \Omega e_{\text{sup}}(t) \}
\]
\[
- \delta e_{\text{sup}}(b_{\text{on}}^{(t)}(n, k) h) \Omega x(b_{\text{on}}^{(t)}(n, k) h) \geq \rho(sh)
\]  
(13)
in which
\[
\rho(sh) = \alpha \varepsilon(A(t) - 1)x_{\text{sup}}(b_{\text{on}}^{(t)}(n, k) h + sh) \Omega x(b_{\text{on}}^{(t)}(n, k) h + sh)
\]  
(14)
\[
e(t) = x(b_{\text{on}}^{(t)}(n, k) h) - x(b_{\text{on}}^{(t)}(n, k) h + sh)
\]  
(15)
\[
b_{\text{on}}^{(t)}(n, 0) h \triangleq \begin{cases} F_{\text{off}}^n, & A(t) = 1 \\ F_{\text{on}}^n, & A(t) = 2 \end{cases}
\]  
(16)
where $\alpha$ and $\delta$ are predefined positive scalars, $h$ is the sampling period. For $k \in \mathbb{N}$, $\{b_{1, n, k}\}$ are the releasing instants in the $n$th sleeping interval $T_n^1$ while $\{b_{2, n, k}\}$ are the releasing instants in the $n$th active interval $T_n^2$. $x(b_{\text{on}}^{(t)}(n, k) h + sh)$ denotes the current system state to be determined whether it should be transmitted. $\Omega > 0$ is a weighting matrix to be designed.

Remark 5 Note that Eqs. (13)-(16) give a full description of the proposed ETM, which is closely associated with the deception attack signal. It can be inferred from Eq. (16) that event triggerings are compulsorily executed at the sampling instants when off/on or on/off transitions of deception attacks occur. Moreover, it is not difficult to derive the following constraint relationships:
\[
\begin{aligned}
\sup_{k \in \mathbb{N}} \{ b_{1, n, k}^1 h \} &< F_{\text{on}}^n + F_{\text{off}}^n \\
\sup_{k \in \mathbb{N}} \{ b_{1, n, k}^2 h \} &< F_{\max} + F_{\text{off}}^n
\end{aligned}
\]  
(17)
Meanwhile, let $\lambda_n^1 \triangleq \sup \{ k | b_{1, n, k}^1 h < F_{\text{on}}^n + F_{\text{off}}^n \}$ and $\lambda_n^2 \triangleq \sup \{ k | b_{2, n, k}^1 h < F_{\max} + F_{\text{off}}^n \}$. Without loss of generality, we assume $b_{1, n, \lambda_n^1 + 2}^1 h \triangleq F_{\text{on}}^n + F_{\text{off}}^n$ and $b_{2, n, \lambda_n^2 + 1}^1 h \triangleq F_{\max} + F_{\text{off}}^n$, which will contribute to the analysis below.

Remark 6 In fact, the dynamic ETM (13) provides diverse triggering strategies corresponding to different attack modes. When the concerned system is healthy with $A(t) = 1$, the triggering condition degenerates into the typical form as in [22]. When the system is suffering from the malicious attacks with $A(t) = 2$, it is not needed that $e_{\text{sup}}(t) \Omega e_{\text{sup}}(t) - \delta e_{\text{sup}}(b_{\text{on}}^{(t)}(n, k) h) \Omega x(b_{\text{on}}^{(t)}(n, k) h)$ always negative when $\rho(sh)$ remains positive. It can be inferred that the ETM (13) with $A(t) = 2$ obtains a larger inter-execution time. In realistic circumstances, the data is corrupted by the attack and less data is expected to release in the active interval of deception attacks. Of course, the control performance should be ensured in the meantime. Note that the tendency of inter-execution time is related to the value of $\varepsilon$ in Assumption 4, and a larger $\varepsilon$ yields a larger inter-execution time.

2.4 The Overall Model

Referring to the work in [22], we divide $[b_{\text{on}}^{(t)}(n, k), b_{\text{on}}^{(t)}(n, k+1) h)$ for $k \in \{0, 1, \ldots, \lambda_n^{(t)}\}$ into $s_M + 1$ subintervals with $s_M \in \mathbb{N}$. Each subinterval is expressed as $\chi_{n, k, s}^{(t)} = [s_{n, k, s}^{(t)}, s_{n, k, s+1}^{(t)}]$, where $s_{n, k, s}^{(t)} \triangleq b_{\text{on}}^{(t)}(n, k) h + sh$, $\chi_{n, k, s}^{(t)} \in \bigcup_{n \in \mathbb{N}} T_n^{(t)}$. Obviously, $[b_{\text{on}}^{(t)}(n, k) h, b_{\text{on}}^{(t)}(n, k+1) h) = \bigcup_{s=0}^{s_M} \chi_{n, k, s}^{(t)}$.

For $t \in \chi_{n, k, s}^{(t)}$, defining $\eta(t) = t - b_{\text{on}}^{(t)}(n, k) h - sh$ yields
\[
0 \leq \eta(t) < h
\]  
(18)
As a zero-order-holder is employed in the physical plant, the control input with a switching control strategy under deception attacks is expressed as
\[
u(t) = \sum_{j=1}^{q} \omega_j K_j A(t) (x_{\text{on}}^{(t)}(n, k) h) + (A(t) - 1)c_0(t), t \in \chi_{n, k, s}^{(t)}
\]  
(19)
where $K_j A(t)$ are the controller gains of switching fuzzy controllers.
According to the Eqs. (2), (18), (19), we obtain an overall closed-loop system model expressed as:

\[
\begin{align*}
\dot{x}(t) &= \sum_{i=1}^{q} \sum_{j=1}^{q} \partial \omega_{ij} [A_i x(t) + B_i K_{j,A}(t) (e(t) + x(t - \eta(t))) + (A(t) - 1) \zeta(t)], \\
x(t) &= \psi(t), \quad t \in [-h, 0]
\end{align*}
\]

According to the definition of DoS Frequency in [34], the following definition is made.

**Definition 1** (Attack Frequency): Define \( N(0, t) = \text{card} \{ n \in \mathbb{N} \mid 0 < F^n + F^m_{off} < t \} \) as the number of off/on transitions of intermittent 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 \( N(0, t) \leq \nu + t/\tau_a \), we say that the deception attack signal merged by \( T_a^m \) and \( T_a^n \) satisfies the attack frequency constraint described by \( \tau_a \) and \( \nu \).

We are now in a position to begin the control issue as: based on the proposed resilient ETM (13), the control objective of this work is to design appropriate switching fuzzy controllers, which can guarantee the concerned system (20) exponentially stable (ES) [19] under the intermittent deception attack signal (10).

### 3 Main results

**Theorem 1** For prescribed positive scalars \( \delta \in (0,1), \alpha, \varepsilon, \beta_m, \mu_m \in (1, \infty), m \in \{1, 2\}, \mu_{\min}, \mu_{\max}, T, \tau_a \) satisfying

\[
\vartheta = (2\beta_1 \mu_{\min} - 2(\beta_1 + \beta_2)h - 2\beta_2 \mu_{\max} - \ln(\mu_1 \mu_2)) / \tau_a > 0
\]

The system (20) with given gain matrices \( K_{j,m} \) is exponentially stable under the intermittent deception attack (10) if the membership functions satisfy \( \omega_j - \varepsilon_j \delta_j \geq 0 \), and there exist \( P_m > 0, Q_m > 0, R_m > 0, \Omega_m > 0 \), and \( N_{ml}, M_{ml}, l \in \{1, 2\} \), \( \Delta^m = \Delta^m_{\max} \) with appropriate dimensions satisfying:

\[
\begin{align*}
P_1 &\leq \mu Q_1, \quad P_2 \leq \beta_0 \mu_1 P_1 \\
Q_1 &\leq \mu Q_2, \quad Q_2 \leq \mu_1 Q_1 \\
R_1 &\leq \mu R_2, \quad R_2 \leq \mu_1 R_1
\end{align*}
\]

\[
\psi_{ij}^m - \Delta^m_{ij} < 0, \quad i, j = 1, 2, \ldots, q
\]

\[
i \psi_{ij}^m - \dot{\Delta}^m_{ij} + \Delta^m_{ij} < 0
\]

\[
i \psi_{ij}^m + i \psi_{ji}^m - i \Delta^m_{ij} < 0, \quad i < j
\]

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

\[ V_m(t) = V_{m1}(t) + V_{m2}(t) + V_{m3}(t) \]

\[ V_{m1}(t) = x^T(t)P_m x(t) \]

\[ V_{m2}(t) = \int_{t-h}^{t} \kappa_m x^T(s)Q_m x(s)ds \]

\[ V_{m3}(t) = \int_{t-h}^{t} \kappa_m x^T(s)R_m \dot{x}(s)dsdv \]

where \( P_m, Q_m, R_m \) are positive definite matrices, \( \kappa_m = e^{\Delta (t-\tau)} \), and \( \beta_m \) is a positive scalar.

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

\[ \dot{V}_{13}(t) = -2\beta_1 V_{13}(t) + h\dot{x}^T(t)R_1 \dot{x}(t) \]

\[ -\int_{t-h}^{t-\eta(t)} e^{-2\beta_1(t-s)} \dot{x}(s)^T R_1 \dot{x}(s)ds \]

\[ -\int_{t-h}^{t-\eta(t)} e^{-2\beta_1(t-s)} \dot{x}(s)^T R_1 \dot{x}(s)ds \]

\[ + 2\xi_1^T(t)(M_1G_1(t) + 2\xi_1^T(t)N_1G_2(t)) \]

Where

\[ G_1(t) = x(t) - x(t - \eta(t)) - \int_{t-\eta(t)}^{t} \dot{x}(s)ds, \]

\[ G_2(t) = x(t - \eta(t)) - x(t) - \int_{t-h}^{t-\eta(t)} \dot{x}(s)ds, \]

\[ \xi_1(t) = \left[ x^T(t) x^T(t - h) e^T(t) x^T(t - \eta(t)) \right]^T. \]

It is not difficult to derive that

\[ -2\xi_1^T(t)M_1 \int_{t-h}^{t} \dot{x}(s)ds \leq h\xi_1^T(t)M_1 e^{2\beta_1 h} R_1^{-1} \]

\[ M_1^T \xi_1(t) + \int_{t-h}^{t} e^{-2\beta_1 h} \dot{x}(s)R_1 \dot{x}(s)ds \]

\[ -2\xi_1^T(t)N_1 \int_{t-h}^{t} \dot{x}(s)ds \leq h\xi_1^T(t)N_1 e^{2\beta_1 h} R_1^{-1} \]

\[ N_1^T \xi_1(t) + \int_{t-h}^{t} e^{-2\beta_1 h} \dot{x}(s)R_1 \dot{x}(s)ds \]

Then, we define

\[ M_1 = [M_1^T 0 0 M_1^{1,2}]^T, N_1 = [0 N_1^T 0 N_1^{1,2}]^T, \]

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. (20), (26), (27) and (28), one has

\[ \dot{V}_1(t) + 2\beta_1 V_1(t) \leq \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \left\{ x^T(2\beta_1 P_1 + A_1^T P_1 + P_1 A_1 + Q_1 + M_{11} + M_{11}^T) x(t) \right\} \]

\[ + 2x(t - \eta(t))^T(K_{11}^T B_1 P_1 - M_1^T) \]

\[ + 2x^T(t - h)(-N_{11} - N_{11}^T) x(t - h) \]

\[ + x^T(t - \eta(t))(-M_{12} - M_{12}^T + N_{11} + N_{12}^T) x(t - \eta(t)) \]

\[ + x^T(t - \eta(t))(-N_{12} - N_{12}^T) x(t - \eta(t)) \]

\[ + M_{12} x(t) \]

\[ + 2x^T(t - h)(-N_{12} - N_{12}^T) x(t - h) \]

\[ + x^T(t - \eta(t))(-M_{12} - M_{12}^T + N_{11} + N_{12}^T) x(t - \eta(t)) \]

\[ + x^T(t - \eta(t))(-N_{12} - N_{12}^T) x(t - \eta(t)) \]

\[ + h\xi_1^T(t)M_1 e^{2\beta_1 h} R_1^{-1} M_1^T \xi_1(t) \]

\[ + h\xi_1^T(t)N_1 e^{2\beta_1 h} R_1^{-1} N_1^T \xi_1(t) \]

\[ + e^T(t) \Omega_1 e(t) - e^T(t) \Omega_1 e(t) \}

\[ + h \dot{x}^T(t)R_1 \dot{x}(t) \]

(29)

Taking consideration of the ETM (13), we gain

\[ \dot{V}_1(t) + 2\beta_1 V_1(t) \leq \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \xi_1^T(t)(H_{11}^T - H_{11}^T H_{11}^{-1} H_{11}^T) \]

\[ - H_{11}^T H_{11}^{-1} H_{11}^T \xi_1(t) \]

(30)

Applying the Schur’s complement to Eq. (30), it is indicated that \( \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} (\eta_j - \eta_i) B_i = \sum_{i=1}^{q} \vartheta_i \left( \sum_{j=1}^{q} \eta_j - \sum_{j=1}^{q} \eta_j \right) B_i = 0 \), where \( B_i = B_1 \), we have

\[ \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \psi_{ij} \]

\[ = \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \psi_{ij} \]

\[ + \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_i (\eta_j - \eta_i) \psi_{ij} \]

\[ + \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_i (\eta_j - \eta_i) \psi_{ij} \]

\[ = \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \psi_{ij} \]

\[ - \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_i (\eta_j - \eta_i) \psi_{ij} \]

\[ + \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_i (\eta_j - \eta_i) \psi_{ij} \]

(31)

With \( \eta_j - \eta_i \geq 0 \), it is clear that (23)-(25) are sufficient conditions to guarantee \( \sum_{i=1}^{q} \sum_{j=1}^{q} \vartheta_{ij} \psi_{ij} < 0 \), which yields

\[ \dot{V}_1(t) + 2\beta_1 V_1(t) < 0 \]

(32)
Integrating both sides of (32) for \( t \in [S_{n,k,s}^1, S_{n,k,s}^1] \), one has
\[
V_1(t) < e^{-2\beta_1(t - S_{n,k,s}^1)}V_1(S_{n,k,s}^1)
\] (33)

Case 2: Consider the situation that \( t \in [S_{n,k,s}^m, S_{n,k,s}^m] \) with \( m = 2 \). By conducting a similar analytical procedure as in Case 1, we conclude that the conditions (23) - (25) with \( m = 2 \) can guarantee \( V_2(t) - 2\beta_2 V_2(t) < 0 \). Integrating both sides of it for \( t \in [S_{n,k,s}^2, S_{n,k,s}^2] \), we obtain
\[
V_2(t) \leq e^{2\beta_2(t - S_{n,k,s}^2)}V_2(S_{n,k,s}^2)
\] (34)

According to the sufficient condition (22), it is not difficult to see that
\[
\begin{cases}
V_1(S_{n,k,s}^1) \leq \mu_2 V_2(S_{n,k,s}^1)
\leq \beta_0 \mu_1 V_1(S_{n,k,s}^1)
\end{cases}
\] (35)

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

Next, by combining Case 1 and Case 2, we try to gain the general relationship between \( V(t) \) and \( V(0) \) for all \( t > 0 \). Assume that at \( t = 0 \) the system (30) is exponentially stable with a decay rate \( \theta_0/2 \). Hence, it is not difficult to see that
\[
\begin{align*}
\| x(t) \| &\leq e^{-\theta_0 t} \| x(0) \|
\leq e^{-\theta_0 t} \| x(t) \| \leq e^{-\theta_0 t} \| \tilde{y}(t) \|
\end{align*}
\]

and
\[
\begin{align*}
\tilde{x}(t) &\leq e^{-\theta_0 t} \tilde{x}(0)
\leq e^{-\theta_0 t} \tilde{x}(t) \leq e^{-\theta_0 t} \tilde{x}(t)
\end{align*}
\]

where \( \theta_0 = \frac{\beta_0 \mu_1}{\beta_0 \mu_1} \leq \frac{\beta_0 \mu_1}{\beta_0 \mu_1} \leq \frac{\beta_0 \mu_1}{\beta_0 \mu_1} \leq \frac{\beta_0 \mu_1}{\beta_0 \mu_1} \).

From the constructed Lyapunov-Krasovskii functional, it is easy to see that
\[
\lambda_1 \| x(t) \|^2 \leq V(0) \leq \epsilon \| x_0 \|^2
\] (38)

where \( \epsilon = \lambda_2 + h\lambda_3 + (h^2/2)(\lambda_4 + \lambda_5) > 0 \).

Therefore, we conclude that the system (20) is exponentially stable with a decay rate \( \theta_0/2 \). 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 \( \delta \in (0, 1), \alpha, \varepsilon, \beta_m, \mu_m \in (1, \infty), m \in \{1, 2\}, F_{\min}, F_{\max}, \tau_a, h, \rho_m, l \in \{1, 2\}, \rho_{2m} \) satisfying (21). The system (20) with controller gains \( K_{jm} = Y_{jm}X_{jm}^{-1} \) is exponentially stable under the intermittent defense attack (10) if the membership functions satisfy \( \omega_j - \delta \delta \geq 0 \), and there exist \( \hat{X}_m \geq 0, \hat{Q}_{2m} > 0, \hat{R}_m > 0, \hat{M}_m > 0, \) and \( \check{N}_m, \hat{M}_m, \hat{\Delta}^m = \Delta^m \) with appropriate dimensions satisfying:

\[
\begin{align*}
X_1 &\leq \beta_0 \mu_1 X_2, X_2 \leq \mu_2 X_1
\odot \leq \mu_2 \check{Q}_2, \check{Q}_2 \leq \mu_1 \check{Q}_1
\odot \leq \beta_2 \mu_1 \check{R}_2, \check{R}_2 \leq \mu_1 \check{R}_1
\end{align*}
\] (40)

where
\[
\begin{align*}
\tilde{y}_m &\leq \Delta^m < 0, (i, j = 1, 2, \cdots, q)
\odot \leq \beta_1 F_{\min} - 2(\beta_1 + \beta_2) h - 2\beta_2 F_{\max} - \ln(\mu_1 \mu_2) / \tau_a
\end{align*}
\] (41)

For \( t \in [F_{\min} + F_{\max} + \max F_{\min}] \), similarly, we have
\[
\begin{align*}
V(t) &\leq e^{-2\beta_1(h - 2\beta_2 F_{\max} - \ln(\mu_1 \mu_2))}V_1(t)
\odot \leq e^{-2\beta_1(\max F_{\min})}V_1(t)
\end{align*}
\] (39)

where \( \delta_0 = (2\beta_1 F_{\min} - 2(\beta_1 + \beta_2) h - 2\beta_2 F_{\max} - \ln(\mu_1 \mu_2)) / \tau_a
\)
Meanwhile, we define
\[ \tilde{X}_5 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \tilde{Z}_6 & 0 & 0 & 0 \\ \tilde{Z}_7 & \tilde{N}_{21} - \tilde{N}_{22} & 0 & \tilde{Z}_8 \end{bmatrix} , \]
\[ \hat{V}_{11} = \begin{bmatrix} \tilde{Z}_5 & * & * & * \\ 0 & \hat{Z}_6 & * & * \\ \tilde{N}_{21} & \tilde{N}_{22} & 0 & \tilde{Z}_8 \end{bmatrix} , \]
\[ \hat{V}_{21} = \begin{bmatrix} \sqrt{\bar{\Sigma}} A_2 X_2 & 0 & \sqrt{\bar{\Sigma}} B_2 Y_{12} & 0 & \sqrt{\bar{\Sigma}} B_2 Y_{12} \\ 0 & 0 & \sqrt{\bar{\Sigma}} X_2 & 0 & \sqrt{\bar{\Sigma}} X_2 \\ 0 & 0 & \varepsilon X_2 & 0 & \varepsilon X_2 \end{bmatrix} , \]
\[ \hat{V}_{22} = diag\{-2\rho_21X_2 + \rho_22\tilde{R}_{21} - 2\rho_22X_2 + \rho_22^2\tilde{Q}_{22} - I\} , \]
\[ \hat{V}_{31} = diag\{-e^{-2(\bar{m})\beta_1h}\tilde{R}_m - e^{-2(\bar{m})\beta_2h}\tilde{R}_m\} , \]
\[ \hat{V}_{32} = \begin{bmatrix} \sqrt{\bar{\Sigma}} \hat{M}_{21}^T & 0 & 0 \\ 0 & \sqrt{\bar{\Sigma}} \hat{X}_{22} & 0 \end{bmatrix} , \]
\[ \hat{V}_{33} = \begin{bmatrix} \tilde{Z}_3 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{34} = \begin{bmatrix} \tilde{Z}_4 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{35} = \begin{bmatrix} \tilde{Z}_5 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{36} = \begin{bmatrix} \tilde{Z}_6 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{37} = \begin{bmatrix} \tilde{Z}_7 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{38} = \begin{bmatrix} \tilde{Z}_8 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} , \]
\[ \hat{V}_{39} = \begin{bmatrix} \tilde{Z}_9 & -\tilde{M}_{22} + \tilde{N}_{12} \end{bmatrix} . \]

\[ \beta_0 = e^{(\beta_1 + \beta_2)h} . \]

**Proof** According to Theorem 1, we assume that
\[ X_m = P_m^{-1} Y_{jm} = K_{jm} X_m , \]
\[ Q_m = X_m Q_m X_m , \]
\[ \tilde{R}_m = X_m R_m X_m \]
\[ \tilde{Q}_m = X_m Q_m X_m \]
\[ \tilde{M}_m = X_m M_m X_m \]
\[ \tilde{N}_m = X_m N_m X_m . \]

Furthermore, we define
\[ \Phi_{11} = diag(I, I, I, I, P_1, P_1, I, I) , \]
\[ \Phi_{12} = diag(X, X, X, X, X, X, X, X) , \]
\[ \Phi_{21} = diag(I, I, I, I, P_1, P_1, I, I) , \]
\[ \Phi_{22} = diag(X, X, X, X, X, X, I, I, X, X) . \]

For \( P_m > 0, R_m > 0 \) and \( \rho_m > 0 \), we can find that \( (\rho_m R_m - P_m) R_m^{-1} (\rho_m R_m - P_m) \geq 0 \), which is equal to
\[ -P_m R_m^{-1} P_m \leq -2\rho_m P_m + \rho_m^2 R_m \]

Similarly, it is noticeable that
\[ -P_m Q_m^{-1} P_m \leq -2\rho_m P_m + \rho_m^2 Q_m \]

Combining Eqs. (44) - (46), pre- and post-multiplying (23) - (25) with \( \Phi_{11} \) and \( \Phi_{12} (m = 1) \), \( \Phi_{21} \) and \( \Phi_{22} (m = 2) \), and their transposes, successively, it is inferred that (41) - (43) are sufficient conditions of (23) - (25). And it yields that \( \Delta^m = \phi_m^2 \delta_m^1 \phi_m \delta_m^2 \). Moreover, we can notice that Eq. (40) is equal to Eq. (22). Through the LMI Toolbox in MATLAB, we first obtain the matrices \( Y_{jm}, X_m \), and \( \tilde{\Omega}_m \). According to \( Y_{jm} = K_{jm} X_m, \tilde{\Omega}_m = X_m \Omega_m X_m \), we can get the fuzzy controller gains and the ETM parameters as \( K_{jm} = Y_{jm}^{-1}, \Omega_m = X_m \tilde{\Omega}_m X_m \). The proof is completed.

**4 Simulation Examples**

A mass-spring-damping system is considered to verify the proposed approach [35], whose dynamic equation is defined as:
\[ m\ddot{x} + F_{f} + F_{s} = u(t) \]

where \( m \) is the mass, \( x \) denotes the displacement from a reference point, \( u(t) \) stands for the external control input. The friction 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 \( F_s = k(1 + a^2 x^2) \) with constants \( k \) and \( a \). Then, the dynamic equation can be rewritten as:
\[ m\ddot{x} + c\dot{x} + kx + ka^2 x^3 = u(t) \]

Define \( x(t) = [x_1(t) \ x_2(t)]^T \), where \( x_1(t) = x \) and \( x_2(t) = \dot{x} \). Let \( x_1(t) \in \left[-2, 2\right], m = 1kg, c = 2N \cdot m/s, k = 8 \), and \( a = 0.3m^{-1} \). We choose \( x_1(t) \) as the premise variable and construct a T-S fuzzy model for (48):

**Plant rule 1:** IF \( x_1(t) \) is \( \pm 2 \), THEN
\[ \dot{x}(t) = A_1 x(t) + B_1 u(t) \]
Plant rule 2: IF $x_1(t)$ is 0, THEN

$$\dot{x}(t) = A_2 x(t) + B_2 u(t)$$

(50)

where the corresponding matrices can be given as:

$$A_1 = \begin{bmatrix} \frac{1}{m} - \frac{c}{m} \end{bmatrix}, A_2 = \begin{bmatrix} 0 \frac{1}{m} \end{bmatrix},$$

$$B_1 = \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix}, B_2 = \begin{bmatrix} \frac{1}{m} \end{bmatrix}.$$
fuzzy control approach; and with the proposed ETM, network resources are saved observably. Only 177 sampled data are transmitted to the controller side while 1000 data are sampled in total over [0,10s]. Meanwhile, as shown in Table 1, the larger the triggering parameter \(\delta\), the fewer sampled data are transmitted. Fig. 6 illustrates the responses of the control input, which is a piecewise continuous signal.

To further verify the effectiveness of the proposed switching event-triggered communication scheme, comparative experiments are conducted with various values of \(\alpha\) and in different network environments, that is, with and without deception attacks. Table 2 lists the related parameter settings and simulation results. For the proposed resilient ETM, larger \(\alpha\) yields smaller releasing number. That is, the network resource utilization can be further enhanced. In Fig. 5, compared to the sleeping interval of deception attacks, it is clear that fewer data are triggered in the active interval. It is worth pointing out that there is always a certain upper bound for \(\alpha\) when \(\varepsilon\) is prescribed. Here, the situation \(\alpha = 0\) denotes a special case, where the resilient ETM degenerates into

### Table 2: Parameter settings and simulation results

| Method         | \(\alpha\) | \(f_{max}\) | releasing number |
|----------------|------------|-------------|-----------------|
| resilient ETM  | 0.5        | 80h         | 158             |
| resilient ETM  | 0.3        | 80h         | 177             |
| resilient ETM  | 0.1        | 80h         | 210             |
| resilient ETM  | 0.05       | 80h         | 222             |
| original ETM   | 0          | 80h         | 258             |
| resilient ETM  | 0.3        | 0h          | 70              |

### 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 |
|--------------|-----|-----|-----|-----|-----|
| \(\varphi/2\) | 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 |
|-------------|---|---|---|---|---|
| \(\varphi/2\) | 0.0176 | 0.1976 | 0.3776 | 0.5576 | 0.7376 |

### Fig. 7: State responses and Releasing period

![Fig. 7: State responses and Releasing period](image)

### Fig. 8: State responses and Releasing period

![Fig. 8: State responses and Releasing period](image)
the original ETM as in [22]. The corresponding state responses and releasing period are demonstrated in Fig. 7. The triggering trend in the active interval is the same as that in the sleeping interval. 258 (177, in Fig. 5) sampled data are transmitted through network while the control performance has no advantage over the one in Fig. 5. It is inferred that the resilient ETM is superior to the original ETM in saving network resources. Moreover, Fig. 8 gives the comparative results, with and without deception attacks. Owing to the switching controllers, almost equally good control performance is obtained in the two circumstances. Of course, only 70 event triggerings are needed when no deception attacks are injected to the system.

On another hand, the inter restricted relationship between \( F_{\text{min}} \) and \( F_{\text{max}} \) are involved in the sufficient condition (21). For prescribed parameters \( \beta_1 = 0.09, \beta_2 = 0.15, \mu_1 = 1.05, \mu_2 = 1.05, \text{and} \; \tau_0 = 0.4, \) Tables 3 - 5 shows the comparative results. Table 3 lists the maximum \( F_{\text{max}} \) allowed for every value of \( F_{\text{min}} \). From Table 4 and Table 5, we can notice that a larger sleeping interval of deception attacks generates a larger decay rate, while the larger the active interval, 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 intermittent deception attacks. A queuing model is constructed to depict the deception attack. Then, a novel event-based communication scheme is proposed to further optimize network resources, which is dynamically switched corresponding with the intermittent attack behaviors. By piecewise Lyapunov functional approaches, the fuzzy controllers and event-triggering parameters have been jointly designed. Finally, the effectiveness of the proposed approaches is verified by a mass–spring–damping system. The triggering trend in the active interval is the same as that in the sleeping interval, 258 (177, in Fig. 5) sampled data are transmitted through network while the control performance has no advantage over the one in Fig. 5. It is inferred that the resilient ETM is superior to the original ETM in saving network resources. Moreover, Fig. 8 gives the comparative results, with and without deception attacks. Owing to the switching controllers, almost equally good control performance is obtained in the two circumstances. Of course, only 70 event triggerings are needed when no deception attacks are injected to the system.

Declarations

Funding This work was supported by a grant from the National Natural Science Foundation of China No. 52005266.
Conflict of interest The authors declare that they have no conflict of interest.
Availability of data and material All data generated or analysed during this study are included in this manuscript and its supplementary information files.
Code availability The codes used during the current study are available from the corresponding author on reasonable request.
Authors’ 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 hotspots in the field of Cyber-Physical Systems (CPSs). In this work, an improved T-S fuzzy model is employed to increase the design flexibility of nonlinear CPSs while a novel queuing model is constructed to depict deception attacks. A new dynamic event-triggered communication scheme is developed to alleviate the burden of network resources, which is adaptive for the severity level of deception attacks. Meanwhile, we propose a solution to jointly design fuzzy controllers and event-triggering parameters, which can guarantee the monitored system exponentially stable under deception attacks. The presented theories and algorithms have been successfully applied to a practical example of a mass-spring-damping system.

References

1. Yan, J., Yang, X., Luo, X., Guan, X.: Dynamic gain control of teleoperating cyber-physical system with time-varying delay. Nonlinear Dynamics 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 Transactions on Cybernetics (2020). http://dx.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 Dynamics 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 Transactions on Circuits and Systems I: Regular Papers 64(10), 2783-2796 (2017)
5. Gu, Z., Ahn, C.K., Yue, D., Xie, X.: Event-triggered \( H_{\infty} \) filtering for t-s fuzzy-model-based nonlinear networked systems with multisensors against dos attacks. IEEE Transactions on Cybernetics (2020). http://dx.doi.org/10.1109/TCYB.2020.3030028

Acknowledgements This work was supported by a grant from the National Natural Science Foundation of China No. 52005266.
6. Li, H., Wu, C., Wu, L., Lam, H.K., Gao, Y.: Filtering of interval type-2 fuzzy systems with intermittent measurements. IEEE Transactions on Cybernetics 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 Transactions on Fuzzy Systems 26(6), 3820 – 3834 (2018)
8. Pan, Y., Yang, G.H.: Novel event-triggered filter design for nonlinear networked control systems. Journal of the Franklin Institute 355(3), 1259–1277 (2018)
9. Humayed, A., Liu, J., Li, F., Luo, B.: Cyber-physical systems security – a survey. IEEE Internet of Things Journal 4(6), 1802–1813 (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 Transactions on Cybernetics 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. International Journal of 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. Information Sciences 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. Information Sciences 519, 260 – 272 (2020)
14. Rong, N., Wang, Z.: State-dependent asynchronous intermittent control for t2 ts fuzzy interconnected systems under deception attacks. Nonlinear Dynamics 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 Transactions on Industrial Informatics 16(7), 4868 – 4877 (2020)
16. Amin, S., Schwartz, G.A., Shanlar 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 Transactions on Automatic Control 60(12), 3299 – 3304 (2015)
18. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Transactions on Automatic 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 Transactions on Systems, Man, and Cybernetics: Systems (2020). http://dx.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(Apr.21), 101–115 (2019)
21. De Persis, C., Frasca, P.: Robust self-triggered coordination with ternary controllers. IEEE Transactions on Automatic 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 Transactions on Automatic 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 $H_\infty$ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. IEEE Transactions on Circuits and Systems I: Regular Papers 67(3), 1021 – 1034 (2020)
25. Peng, C., Zhang, J., Han, Q.L.: Consensus of multi-agent systems with nonlinear dynamics using an integrated sampled-data-based event-triggered communication scheme. IEEE Transactions on Systems, Man, and Cybernetics: Systems 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 Dynamics 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 Transactions on Circuits and Systems I: Regular Papers 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. Information Sciences 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. Journal of the Franklin Institute 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. Journal of the Franklin Institute 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. Journal of the Franklin Institute 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. International Journal of Systems Science 51(9), 1653 – 1668 (2020)
34. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Transactions on Automatic Control 60(11), 2930 – 2944 (2015)
35. Li, H., Pan, Y., Shi, P., Shi, Y.: Switched fuzzy output feedback control and its application to mass-spring-damping system. IEEE Transactions on Fuzzy Systems 24(99), 1259–1269 (2016)