Heliyon 7 (2021) e07294

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Trust-based fault detection and robust fault-tolerant control of uncertain cyber-physical systems against time-delay injection attacks ☆

Salman Baromand [a], Amirreza Zaman [b,*], Lyudmila Mihaylova [c]

[a] Department of Electrical Engineering, Fasa University, Fasa, Iran
[b] Control Engineering Group, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden
[c] Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, UK

ARTICLE INFO

Keywords:
Correlation analysis
Cyberattacks
Kullback-Leibler divergence
Linear matrix inequalities (LMIs)
Robust control
Uncertain systems
Unknown time-delay attacks

ABSTRACT

Control systems need to be able to operate under uncertainty and especially under attacks. To address such challenges, this paper formulates the solution of robust control for uncertain systems under time-varying and unknown time-delay attacks in cyber-physical systems (CPSs). A novel control method able to deal with thwart time-delay attacks on closed-loop control systems is proposed. Using a descriptor model and an appropriate Lyapunov functional, sufficient conditions for closed-loop stability are derived based on linear matrix inequalities (LMIs). A design procedure is proposed to obtain an optimal state feedback control gain such that the uncertain system can be resistant under an injection time-delay attack with variable delay. Furthermore, various fault detection frameworks are proposed by following the dynamics of the measured data at the system's input and output using statistical analysis such as correlation analysis and K-L (Kullback-Leibler) divergence criteria to detect attack's existence and to prevent possible instability. Finally, an example is provided to evaluate the proposed design method's effectiveness.

1. Introduction

During the last few years, uncertain systems have been widely encountered because of the environmental changes, systems' failures, and disturbances [1, 2]. These systems have been widely used in the application of electronic circuits, power systems, spring damping systems, and mechanical systems [3, 4, 5]. Since the industrial application of cyber-physical uncertain systems increases, stealthy cyber-attacks may occur to prevent systems' productivity and degrade systems' performances.

One important factor that can cause instability in most practical systems is time-delay effects. These effects in nonlinear systems can be the main reason for weaknesses of control approaches in most cases [6], [7]. Therefore, several robust and adaptive strategies have been done to control uncertain and nonlinear systems under time-delay effects with the assumption of parametric uncertainties. Therefore, several robust and adaptive strategies have been done to control uncertain and nonlinear systems under time-delay effects with the assumption of parametric uncertainties [8, 9, 10, 11, 12, 13], such as approaches with backstepping and dynamic surface designs [14, 15]. In [16], a set of network-based uncertain systems is introduced by modeling these problems with event-triggered robust filtering. A recent event-triggered control proposition is stated in [17] to synchronize a switched delayed neural network. When it comes to decentralized nets, in [18], the event-triggered filtering for a decentralized network interconnecting nonlinear system is developed. Also, some event-triggered methods using a periodic sampled-data control and with fuzzy systems are introduced in [19, 20, 21, 22, 23]. In [24], the networked control of uncertain nonlinear systems is investigated with an adaptive event-triggered strategy under unknown time-delay conditions.

Even though various studies have been done regarding robust and adaptive control of uncertain systems, a few approaches are related to designing the robust and adaptive control strategies of uncertain CPSs with time delays and considering cyber components. Besides, because of the unavailability of error surfaces of the measured and sent state information by sensors in CPSs, which various attackers could alter these surfaces, previous approaches [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24] cannot be applied to prevent cyberattacks in uncertain CPSs. Thus, the problem of designing control methods to resist

☆ Funding received from the Horizon 2020 Research Programme of the European Commission under the grant number 956059 (ECO-Qube) is hereby gratefully acknowledged.

* Corresponding author.
E-mail address: amirreza.zaman@ltu.se (A. Zaman).

https://doi.org/10.1016/j.heliyon.2021.e07294
Received 30 April 2021; Received in revised form 26 May 2021; Accepted 9 June 2021

uncertain time-delayed CPSs against different attack strategies is still an interesting subject to follow and consider.

Some approaches have been devoted to state the importance of the security issue of CPSs [25, 26, 27, 28, 29]. Control problems in these systems are categorized into three groups based on different cyber-attack scenarios; denial-of-service (DoS) attacks [30, 31, 32, 33], deception attacks [34, 35, 36, 37, 38], and replay attacks [39, 40, 41]. The latest studies regarding security control of CPSs against cyberattacks are as follows. In [42], the issue of designing event-based security control for uncertain state-dependent systems with the existence of hybrid attacks is proposed. Besides, the finite-time H_∞ filtering method for networked state-dependent uncertain systems under multiple attacks (DoS, deception, and replay attacks) by considering the event-triggered approach is investigated in [43]. Another control strategy of nonlinear time-delayed CPSs under unspecific deception attacks is developed in [44], in which an adaptive, resilient, dynamic surface control using the neural-network scheme is proposed for deception attacks on both sensor and actuator sides.

One kind of malicious attack that can cause trouble in operating uncertain systems is a time-delay attack. A time-delay attack on a control system is the reason for adversaries that fundamentally add time delays into such systems and potentially forcing them to instability and crash. A recent approach has been made regarding time-delay attacks [45]. First, it is shown that cryptographic methods against these attacks would be useless in detecting cyber components. A cryptography-free time-delay attack recovery (CF-TDR) communication protocol is developed to identify failures and recover from these attacks' destructive effects.

Previous designed robust control approaches against time delays considered the existence of time-independent delays with known values. There is still no approach to investigating time-delay attacks with unknown and time-varying values on uncertain systems with a robust approach to detect these attacks and recover the system's performance. Various protection-based methods against data injection attacks have been developed lately. Most of them involve using protected measurement data or using estimated system data. However, if the attackers can infiltrate security systems and manipulate metering data, the control system will be compromised. On the other hand, these methods may not detect contaminated data with a statistical distribution similar to the previously measured safe data.

It is well known that a robust controller can often maintain states of a system bounded against various types of uncertainties, which can be the modeling uncertainties or environmental uncertainties. On the other hand, if unknown and time-varying delays are injected into the system's performance by an intruder, formerly applied robust control approaches cannot be further beneficial. Consequently, the uncertain system's stability under unknown and time-varying delays will be enhanced, and hence, the states of the system will remain bounded under various time delays. Besides, it is necessary to detect the delay's occurrence to implement other safety protocols. The main contributions are itemized as follows:

1. We allocate a robust controller that attenuates and partially eliminates the harmful effects of delayed contaminated data injection on system stability. Besides, to show the proposed approach's efficiency, the amount of delay is assumed to be randomly selected. Therefore, the designed feedback controller will prevent system instability based on random time delays.
2. We define uncertainties in the system as unknown values with the norm-bounded feature. Using a descriptor model representation and an appropriate Lyapunov functional, we formulate sufficient conditions for closed-loop stability based on the linear matrix inequalities (LMIs).
3. We present the online fault detection framework by following the dynamics of the measured data at the system's input and output to prevent the operating system from going into the faulty phase as quickly as possible. Attack detection methods are proposed and compared using statistical analysis such as correlation analysis and K-L divergence attack detection criteria.
4. Simulation results verify that the considered uncertain system will be resilient against malicious time-delay attacks. Therefore, the trustworthiness of the system's performance will be enhanced over time by applying the developed robust control protocol. Additionally, using the provided fault detection strategies, stealthy time-delay attacks can be detected at the time of their occurrence.

This paper's remainder is as follows: In Section 2, the uncertain control system is analyzed under the time-delay attack, and then, the robust H_∞ delay-independent controller is proposed to overcome instability conditions in the system. In Section 3, various statistical attack detection methods are reviewed to detect faults in the system under the time-delay attacker's existence. Eventually, numerical simulations and concluding sections are presented in Sections 4 and 5, respectively.

2. Time-delay attack analysis for uncertain systems

2.1. Problem statement

Real-life processes in a smart fashion such as smart industrial systems can be modeled as nonlinear systems. Assume the nonlinear system given by the below state-space equations

$$\begin{aligned} \dot{x}(t) &= \tilde{f}(x) + \tilde{B}u(t), \\ y(t) &= Cx(t), \end{aligned} \tag{1}$$

where $x \in R^n$ and $u \in R^m$ are the state and the control input vectors, respectively. Furthermore, $\tilde{B}$ is the input matrix, $\tilde{f}(x)$ is the nonlinear function of system states, and C is the output matrix of the system. Suppose the obtained linearized model around its equilibrium point is controllable and also has the state-space matrices $(A,\ B)$. So, $\tilde{f}(x)$ and $\tilde{B}$ can be decomposed as

$$\begin{cases} \tilde{f}(x) = (A + \Delta A)x(t), \\ \tilde{B} = B + \Delta B, \end{cases} \tag{2}$$

where ΔA, ΔB are model uncertainties and A, B, ΔA, and ΔB have applicable dimensions. Thus, the model of continuous-time uncertain system (1) (or approximation of system in a region of interest by an LTI system), can be expressed as following uncertain state space equations

$$\begin{aligned} \dot{x}(t) &= (A + \Delta A)x(t) + (B + \Delta B)u(t), \\ y(t) &= Cx(t). \end{aligned} \tag{3}$$

It is assumed that the attacker tries to inject a time-delay attack to force the system to be unstable or have abnormal operations. We can consider the given uncertain system (4) with an augmented time-delay attack as:

$$\begin{aligned} \dot{x}(t) = (A + \Delta A)x(t) + (B + \Delta B)u(t) + \sum_{i=1}^{k} \tilde{D}_i \dot{x}\left(t - g_i(t)\right) \\ + \sum_{i=1}^{k} H_i x\left(t - g_i(t)\right), \end{aligned} \tag{4}$$

where $\tilde{D}_i$ and H_i are the system matrices with appropriate dimensions and also $\sum_{i=1}^{k} \tilde{D}_i \dot{x}\left(t - g_i(t)\right) + \sum_{i=0}^{k} H_i x\left(t - g_i(t)\right)$ is assumed as a delay attack strategy, with $g_i(t) \geq 0$. It should be noted that the delay term $g_i(t)$ is assumed to be time-varying to obtain more general results in the paper for a worst-case scenario and to show the effectiveness of the proposed robust control solution with any random values of $g_i(t)$ in further analysis.

The purpose of the control solution protocol is to frame a delay-independent robust H_∞ controller $u(t) = Kx(t)$, which assures the robust stability of the system under delay attacks for maximum and unknown delay $g_i(t) \geq 0$. The structure of robust security control for the networked control system with time-delay attacks is illustrated in Fig. 1.

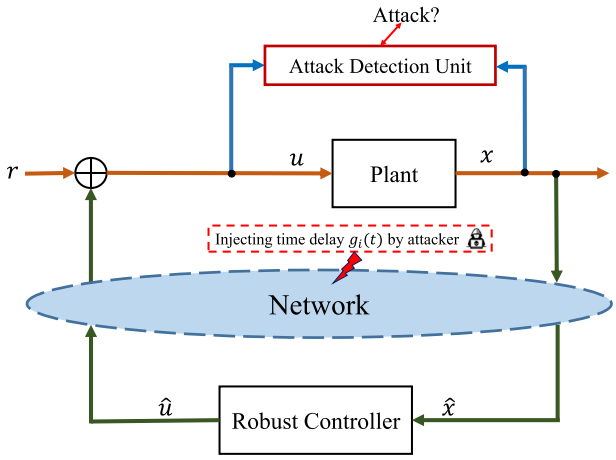

Fig. 1. The structure of the CPS with the proposed robust controller and attack detection unit under unknown time-delay attacks.

2.2. Robust H_∞ controller design for closed-loop uncertain CPSs

With the proposed robust H_∞ control law $u(t) = Kx(t)$, we have a closed-loop system as

$$\dot{x}(t) = \tilde{A}_0 x(t) + \sum_{i=1}^{k} \tilde{D}_i \dot{x}\left(t - g_i(t)\right) + \sum_{i=1}^{k} H_i x\left(t - g_i(t)\right), \tag{5}$$

where K is the robust controller feedback gain and

$$\tilde{A}_0 = A_0 + \Delta A_0, \tag{6}$$

$$\left(A_0 = A + BK, \quad \Delta A_0 = \Delta A + \Delta BK\right)$$

and

$$\tilde{D}_i = \overline{D}_i + \Delta\overline{D}_i, \tag{7}$$

where $\overline{D}_i$ and $\Delta\overline{D}_i$ are specific fixed-valued real matrices of applicable dimensions. Moreover, the possible system's uncertainties are described by the given equations

$$\left[\Delta A \quad \Delta B\right] = D_0 F_0(x,t) \left[E_a \quad E_b\right], \tag{8}$$

$$\Delta\overline{D}_i = D_i F_i(x,t) \overline{E}_i, \tag{9}$$

where D_0, E_a, E_b, D_i, and $\overline{E}_i$ are fixed-valued real matrices of applicable dimensions. Besides, $F_i(x,t)$ and $F_0(x,t)$ are anonymous real-valued time-varying matrices with Lebesgue measurable items complying the given bounds

$$F_i^T(x,t) F_i(x,t) \le I, \tag{10}$$

$$F_0^T(x,t) F_0(x,t) \le I, \quad \forall t. \tag{11}$$

Assumption A1. In deriving formulas, it is assumed that:

$$\sum_{i=1}^{k} |\tilde{D}_i| < 1, \tag{12}$$

where $|.|$ is any matrix norm. With the above assumption, both stability conditions associated with continuous and continuously differentiable initial functions are equivalent. To derive stability conditions, the following lemmas are essential to mention.

Lemma 1 *([46, 47]). For any $z,\ y \in R^n$ and any positive definite matrix $X \in R^{n\times n}$,*

$$-2z^T\ y \le z^T X^{-1} z + y^T X y. \tag{13}$$

Lemma 2 *([46, 47]). Let A, D, E, and F be real matrices of appropriate dimensions with $\|F\| \le I$. Accordingly, it can be concluded that:*

For any scalar $\epsilon > 0$,

$$DFE + E^T F^T D^T \le \varepsilon^{-1} DD^T + \varepsilon E^T E, \tag{14}$$

for any matrix $H > 0$ and scalar $\epsilon > 0$, which applies to the inequality $\varepsilon I - EHE^T > 0$,

$$\begin{aligned}&(A + DFE)\, H (A + DFE)^T \\ &\le AHA^T + AHE^T(\varepsilon I - EHE^T)^{-1} EHA^T + \varepsilon DD^T,\end{aligned} \tag{15}$$

for any matrix $H > 0$ and scalar > 0, which applies to the inequality $H - \varepsilon DD^T > 0$,

$$(A + DFE)^T H^{-1} (A + DFE) \le A^T (H - \varepsilon DD^T)^{-1} A + \varepsilon^{-1} E^T E. \tag{16}$$

2.3. Delay-independent stability for an uncertain system with time–delay attack

To find delay-independent stability condition, the descriptor representation of the system is given as follows

$$\dot{x}(t) = y(t), \tag{17}$$

$$y(t) = \tilde{A}_0 x(t) + \sum_{i=1}^{k} \tilde{D}_i y\left(t - g_i(t)\right) + \sum_{i=1}^{k} H_i x\left(t - g_i(t)\right). \tag{18}$$

By defining the Lyapunov-Krasovskii functional candidate as:

$$V(t) = \left[x^T(t) \quad y^T(t)\right] EP \begin{bmatrix} x(t) \\ y(t) \end{bmatrix} + \mathrm{V}_1 + \mathrm{V}_2, \tag{19}$$

where

$$\mathrm{E} = \begin{bmatrix} \mathrm{I} & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathrm{P} = \begin{bmatrix} P_1 & 0 \\ P_2 & P_3 \end{bmatrix}, \quad P_1 = P_1^T > 0,$$

and

$$\mathrm{V}_1 = \sum_{i=1}^{k} \int_{t-\mathrm{g_i}}^{t} y^T(s)\, \mathrm{Q_i} y^T(s)\, ds, \quad \mathrm{Q_i} > 0, \tag{20}$$

$$\mathrm{V}_2 = \sum_{i=1}^{k} \int_{t-\mathrm{g_i}}^{t} x^T(s)\, U_i x^T(s)\, ds, \quad \mathrm{U_i} > 0, \tag{21}$$

further results from the Theorem 1 can be concluded.

Theorem 1. *Under assumption A1, the uncertain system (3) under the injection time-delay attack introduced in (4) is stable for all delay values $g_i(t) > 0,\ i = 1, \ldots, k$ if there is a matrix $X = \begin{bmatrix} X_1 & 0 \\ X_2 & X_3 \end{bmatrix}$, $X_1 = X_1^T > 0$, X_2, $X_3, \overline{Q}_i = \overline{Q}_i^T$, $\overline{U}_i = \overline{U}_i^T$, $i = 1, \ldots, k$ that satisfies the following LMI*

$$W = \begin{bmatrix} \overline{\overline{\psi}}_1 & \overline{\theta}_1 & 0 & \overline{\theta}_2 & X^T vec\{I\} & X^T vec\{I\} \\ * & \overline{\theta}_3 & \overline{\theta}_4 & 0 & 0 & 0 \\ * & * & \overline{\theta}_5 & 0 & 0 & 0 \\ * & * & * & \overline{\theta}_6 & 0 & 0 \\ * & * & * & * & \overline{\theta}_7 & 0 \\ * & * & * & * & * & \overline{\theta}_8 \end{bmatrix} < 0, \tag{22}$$

where

$$\begin{aligned}\overline{\overline{\psi}}_1 = &\begin{bmatrix} 0 & 0 \\ AX_1 + BY & 0 \end{bmatrix} + \begin{bmatrix} 0 & (AX_1)^T + (BY)^T \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & I \\ 0 & -I \end{bmatrix} X \\ &+ X^T \begin{bmatrix} 0 & 0 \\ I & -I \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 2\sum_{i=1}^{m} \xi_i^{-1} D_i D_i^T \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & \xi_0^{-1} D_0 D_0^T \end{bmatrix} \\ &+ X^T \begin{bmatrix} \sum_{i=0}^{m} \xi_i E_i^T E_i & 0 \\ 0 & 0 \end{bmatrix} X.\end{aligned} \tag{23}$$

Additionally, other variables are defined as

$$\overline{\theta}_1 = vec\left\{\begin{bmatrix} 0 \\ D_i \end{bmatrix}\left(\overline{Q}_i\right)\right\},\ \overline{\theta}_2 = vec\left\{\begin{bmatrix} 0 \\ H_i \end{bmatrix}\left(\overline{U}_i\right)\right\},$$
$$\overline{\theta}_3 = -diag\left(\overline{Q}_i\right), \overline{\theta}_4 = vec\left\{\overline{E}_i^T\right\},$$
$$\overline{\theta}_5 = -diag\left(\xi_i^{-1}\ I\right),\ \overline{\theta}_6 = -diag\left(\overline{U}_i\right),\ \overline{\theta}_7 = -diag(\overline{Q}_i),$$
$$\overline{\theta}_8 = -diag(\overline{U}_i),\ \xi_i > 0,\ i = 1, \ldots,\ k.$$

Then, the optimal state-feedback gain is then calculated by $K = Y X_1^{-1}$ *where the augmented closed-loop matrix is denoted as* $A_0 = A + BK$.

Proof. See the appendix in the article's supplementary files. □

The primary importance of the presented robust approach is to provide a method to formulate the uncertainties caused by the cyber attacks instead of modeling with stochastic processes (system uncertainties and insufficient information from attackers are mostly modeled by considering noise and stochastic processes). Thus, we proposed a delay-independent H_∞ approach to reduce the disturbances' effects caused by the attacker and increase the system's robustness. Consequently, finding a solution to the discussed optimization problem yields to providing a method to counteract the disturbing effects of the attacker. However, it is not straightforward to propose an analytical solution in general, and hence, the robust protocol is formulated using LMI methods. The developed robust strategy performs conservatively, and we tried to reach the optimal solution using the descriptor representation stated in (17) and (18).

In cases that it is hard to satisfy proposed LMI conditions, the main LMI problem can be reformulated to a convex optimization problem with LMI conditions to provide a trade-off between the controller's performance and the system's sensitivity to the disturbances by setting the LMI conditions less than a constant error value. On the other hand, the considered attack form in (4) is formulated in a relatively complex formation, and therefore, further equations are derived in general conditions. For exceptional cases, feasible solutions can be achieved.

Remark 1. If we assume that the attacker has complete access to the control network and can inject time delays into the communication channels (worst-case attack scenario), consequently, the immediate measurement of the process state $x(t)$ and the actuator signal $u(t) = Kx(t)$, will be replaced by $\tilde{u}(t) = u\left(t - g_0\right) = Kx\left(t - g_0\right)$. Hence, the dynamic of the system (4) is reduced to

$$\dot{x}(t) = (A + \Delta A)x(t) + B_d u(t - g_0) + \sum_{i=1}^{k} \tilde{D}_i \dot{x}\left(t - g_i(t)\right) + \sum_{i=2}^{k} H_i x\left(t - g_i(t)\right). \tag{24}$$

According to (24), by substituting H_1 by $B_d(YX_1^{-1})$ and then setting $B=0$ in LMI condition (22), a time-independent criterion for analyzing the stability condition of the system (24) using the results in Theorem 1 will be obtained.

Remark 2. It should be noted that there is always a small amount of delay in transmitting data packets in smart network control systems, even without any attacks in the system. When time-delay attacks occur, the attacker's delay is augmented to this intrinsic network communication's delay value. Besides, in analyzing delays in small-scale networks, only the delay from the time-delay attack is mostly considered to derive formulas. However, in large-scale networks such as large-scale load frequency control networks with time-delay attacks [45], the system's delay should also be considered to avoid the network's instability in a large-scale fashion. In this article's formulations, the augmented delay term is assumed to be a general delay term to cover the system's delay, too. By this assumption, this paper's methodology can be implemented to overcome the issue of the existence of the system's delay and the attacker's delay together.

3. Fault detection for a robust, resilient control protocol against time-delay attacks

Knowing the attack event and the maximum tolerable time delay, an attack detector will direct the system into an alarm state. Under the investigated control strategy, the proposed scheme is maintained in a stable condition in the alert state by the designed robust controller. It remains in this state until the system status is restored. This method can be used as an economical and straightforward method to ensure industrial control systems' stability and safety. In the presented control method, due to the system being stable at the time of the attack event and due to the system states' limited values, we expect to be able to implement the residual-based fault detection methods or distance selection criteria to detect a fault in the system. In this section, we compare and analyze the ability of different attack detection techniques.

3.1. Fault detection based on maximum correlation

The correlation coefficient is one of the criteria used to determine the association between two variables. The correlation coefficient indicates the severity of the relationship and the type of connection (direct or inverse). This coefficient is between 1 and -1 and is zero if there is no relationship between the two variables. The correlation coefficient between the two input variables $u(k)$ and the output of state $x(k)$ is defined as follows:

$$\rho(u(k), x(k)) = \frac{Cov(u(k), x(k))}{\sqrt{D(u(k))}\sqrt{D(x(k))}} = \frac{\sum_{k=1}^{N}\left(u(k) - \mu_u\right)\left(x(k) - \mu_x\right)}{\sqrt{\sum_{k=1}^{N}\left(u(k) - \mu_u\right)^2}\sqrt{\sum_{k=1}^{N}\left(x(k) - \mu_x\right)^2}}, \tag{25}$$

where μ_x and μ_u are the average of the input and output data. The most important thing to remember about the correlation coefficient is that the correlation coefficient only indicates the linear relationship between two variables.

In the non-attack mode, according to (4), the output change is statically related to the input change; that means any arbitrary inputs entirely generate different output values. So, if the data does not change, the output of the system will be retained. Thus, we expect that by injecting the attack's signal into the system, we will see a decrease in the correlation between the system's input and output variables. With a delay in the system, we expect the correlation coefficients to be decreased due to input and output sequences since the output does not correlate with the input. Therefore, in the delay-based attack detection algorithm and the general correlation-based delay estimation, the correlation coefficient between the input sequence and the output sequence can be calculated. Furthermore, the delay length corresponding to the maximum confidence coefficient can be considered as an estimation of the time delay value. Besides, the simulation results illustrate that the correlation coefficient is effective for accurately identifying the time-delay attack.

3.2. Fault detection based on K-L divergence analysis

One of the most common methods for detecting the malicious injected data is to monitor the dynamics of the measured data from the system and use the distance criterion. To quantify measurement changes, one can use both absolute distance indices and the K-L divergence criterion. For both distance indices, the two probability distributions P and Q must be considered, where the probability distribution Q is the statistical distribution of non-invasive measurements and P is also the statistical distribution of the measurement data exposed to injecting contaminated data. If there is no attack, the distance index will

be relatively small, while the mentioned index will increase when the attacker's malicious data is injected into the system. By comparing the current time interval index P with Q, one can determine whether inaccurate data has been injected into the system or not. In the following, the common distance-based statistical attack detection criteria are reviewed and in the numerical results, their effectiveness in detecting the current article's proposed attack is investigated.

3.2.1. Absolute distance criterion

A simple comparison criterion for the two probability distributions P and Q is the calculation of the absolute distance and can be defined as follows

$$D_A(P \parallel Q) = \sum_x |P(x) - Q(x)|. \tag{26}$$

3.2.2. K-L divergence measurement

For the two probability distributions P and Q, the K-L divergence criterion is defined as

$$D_{KL}(P \parallel Q) = \sum_x P(x) \log P(x)/Q(x)\ . \tag{27}$$

Two essential features of the K-L divergence criterion are that it: (1) is always non-negative, i.e., $D_{KL}(P \parallel Q) \geq 0$; and (2) equals to zero if, and only if $P = Q$.

When the inaccurate, malicious data is injected into the system, the probability distribution of the altered measurement data deviates from the probability distribution of the error-free data, resulting in a more considerable K-L divergence calculated value.

Corollary 1. *If the two distributions P and Q are Gaussian, the introduced K-L divergence criterion can be simplified as the following*

$$\begin{aligned} D_{KL}(P \parallel Q) = \frac{1}{2}\left(\log\frac{|\Sigma_Q|}{|\Sigma_P|} - n + tr\left(\Sigma_Q^{-1}\Sigma_P\right)\right) \\ + \frac{1}{2}\left(\mu_Q - \mu_P\right)^T \Sigma_Q^{-1}(\mu_{Q-}\mu_P), \end{aligned} \tag{28}$$

where μ_P and Σ_P are the mean and covariance of the sequence P, and also, μ_Q and Σ_Q are defined as the mean and covariance of the sequence Q. Also, n is the dimension of the sequences in general.

4. Numerical simulations

The effectiveness of the proposed robust H_∞ control strategy under a time-delay attack is illustrated in this section.

An uncertain CPS with a malicious time-delay attack is assumed as the following form:

$$\dot{x}(t) = (A + \Delta A)x(t) + Bu(t) + (\overline{D}_1 + \Delta\overline{D}_1)\dot{x}(t - g(t)) + H_1 x(t - g(t)), \tag{29}$$

$$g(t) = T_0 |\sin(3t)|, \tag{30}$$

where

$$A = \begin{bmatrix} -2 & -0.1 & 0 \\ 0 & -0.3 & 0.5 \\ 1 & 0 & -1 \end{bmatrix},\ B = \begin{bmatrix} -1 \\ 1.5 \\ 1 \end{bmatrix},\ \overline{D}_1 = \begin{bmatrix} -0.2 & -0.5 & 0 \\ 0 & 0.3 & 0 \\ 1 & 0 & -0.6 \end{bmatrix},$$

$$H_1 = \begin{bmatrix} -1 & 0.1 & 0 \\ 0 & 0.2 & 0 \\ 0 & -1 & 0.2 \end{bmatrix},$$

and

$$\Delta A = \begin{bmatrix} 0.01 & 0.1 & -0.1 \\ 0.04 & 0.4 & 0.4 \\ 0 & 0.01 & 0.02 \end{bmatrix}, \Delta\overline{D}_1 = \begin{bmatrix} -0.01 & 0.1 & 0.05 \\ 0 & 0.5 & 0.05 \\ 1 & 0 & -0.05 \end{bmatrix}.$$

Table 1. Calculated MSE of system states with the proposed robust control strategy against time-delay attacks under various system uncertainties.

$\|\Delta B\|_2$	$MSE(x_1)$	$MSE(x_2)$	$MSE(x_3)$	*sum*
0	0.0211	0.0148	0.0129	0.0489
0.4	0.0341	0.0156	0.0194	0.0692
0.8	0.0549	0.0165	0.0370	0.1085
1.2	0.0865	0.0177	0.0678	0.1720

The total simulation time was set to *20 sec*, and the sampling time to *0.02 sec*. Based on the considered attack scenario, a time-delay attack is injected at time $t = 8$ *sec* with the maximum delay $T_0 = 4$ *sec* to all system states.

Fig. 2 shows the system's instability under this attack with the formerly developed robust controller as the one stated in [4]. We can conclude from Fig. 2 that designing a new robust control strategy is a must. Therefore, according to the developed robust control strategy, the feedback gain matrix K is calculated as

$$K = \begin{bmatrix} -0.0101 & 0.164 & -0.175 \end{bmatrix}.$$

Moreover, Fig. 3 depicts the provided system's stability with the proposed robust controller against time-delay attacks. Additionally, Fig. 4 shows that system states and the proposed robust control signal under the time-delay attack remain bounded. As a result, the system could tolerate unknown time-delay attacks with the developed robust control strategy with the presented robust approach. Additionally, the system states' mean square error (MSE) values from the proposed robust control method based on various uncertainties under time-delay attacks are calculated in Table 1. According to Table 1, system states remain bounded under time-delay attacks with different uncertainty values.

Next step is to detect the attack's occurrence with various fault detection methods introduced in previous sections. Fig. 5 indicates the calculated correlation coefficient values before and after the time-delay attack. It can be observed that for data without attack, correlations are relatively close to 1 or -1, while the time-delay attack decreases the correlation coefficient value.

Another way to detect faults can be developed by using the absolute distance criterion. Absolute distances D_A and D_{KL} between P (system with attack) and Q (system without attack) are indicated in Fig. 6. So, it can be inferred that injecting false data attacks to the system enhances the Absolute distance values D_A and D_{KL}.

In false data injection attacks, compared with absolute distance (Fig. 6.a), the K-L distance (Fig. 6.b) is more significant. Therefore, in total, the absolute distance criterion is not an ideal candidate to test false data injection attacks' existence. To detect false data injection attacks with the K-L divergence criterion, we should analyze and set its detection threshold from the standard data. If the K-L divergence runtime is larger than the threshold, false data have likely been injected into the system.

It is worth noticing that the absolute distance and K-L divergence methods only require the system's output data in a non-attack mode or at least an accurate estimation of the system's output. Since the designed controller is relatively resistant to attack, the system's output data does not change much abruptly, and based on Fig. 6, there would be no significant changes in D_A and D_{KL} at the time of the onset of the attack. Although these attack detection parameters grow over time, injection of contaminated data into the system can be detected by decreasing the correlation level of the system's input and output data at the time of the attack event.

Remark 3. By the developed control method, the goal is to prevent the system from entering the destruction phase and, at the same time, to detect attacks. Therefore, previously introduced residual-based detection methods will be significantly ineffective in detecting attacks with low-amplitude or a small number of delays. So, considering a delay in the

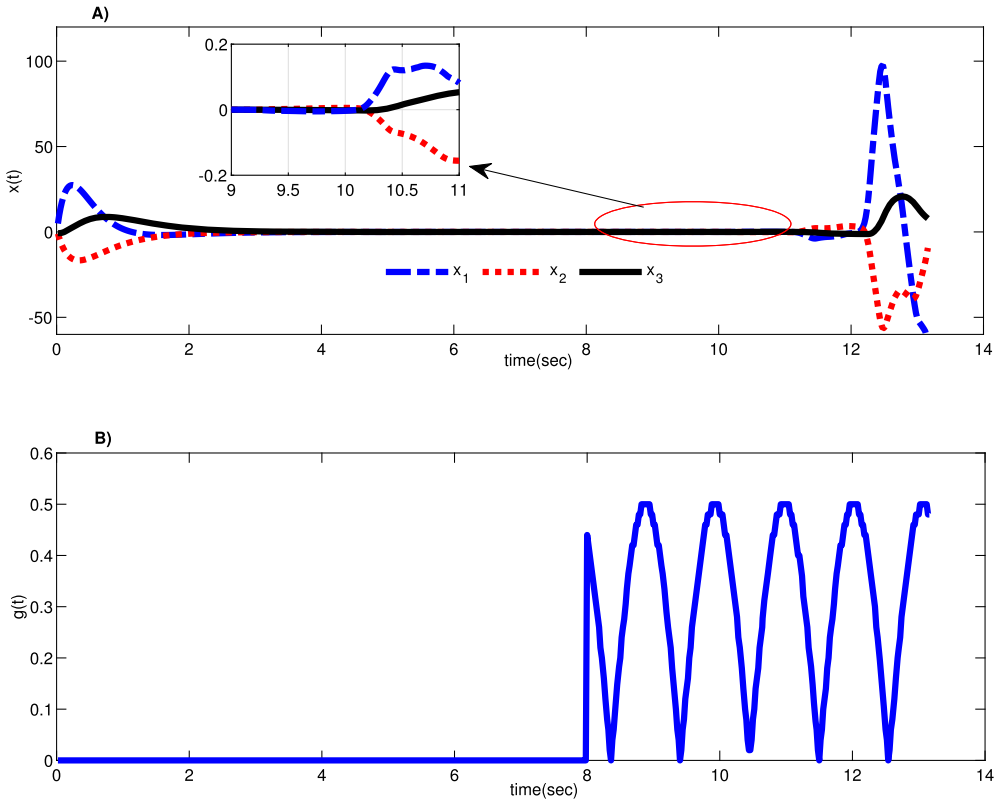

Fig. 2. A) Instability of the uncertain system states trajectory by implementing conventional robust controller [4] under the time-delay attack, and B) assumed time delay attack $g(t)$.

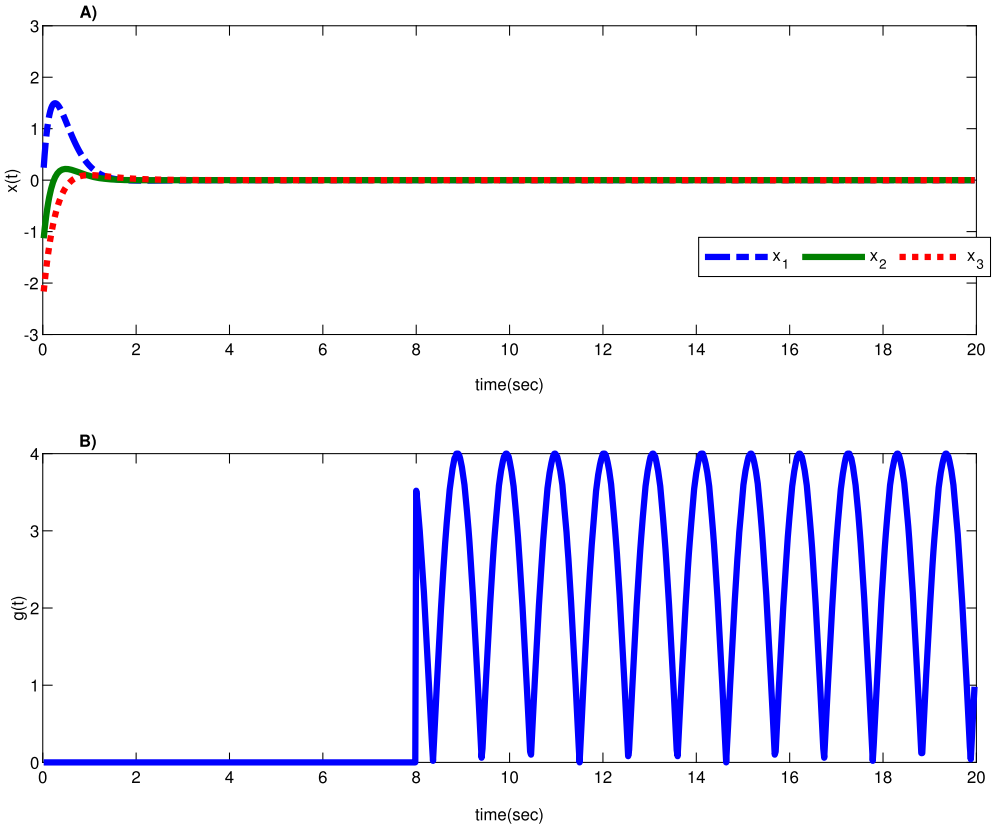

Fig. 3. A) System states convergence against time-delay attack with the proposed robust controller, and B) assumed time delay attack $g(t)$.

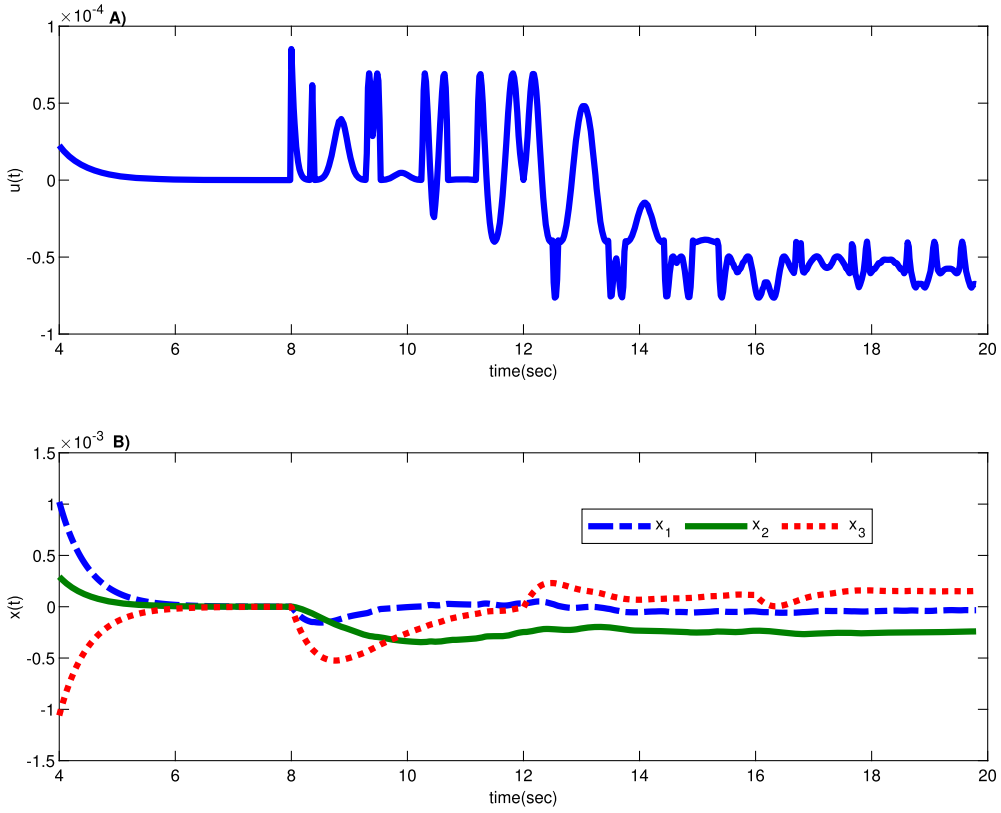

Fig. 4. A) The proposed bounded robust control trajectory and B) system states trajectory under the time-delay attack injected at time $t = 8\ sec$.

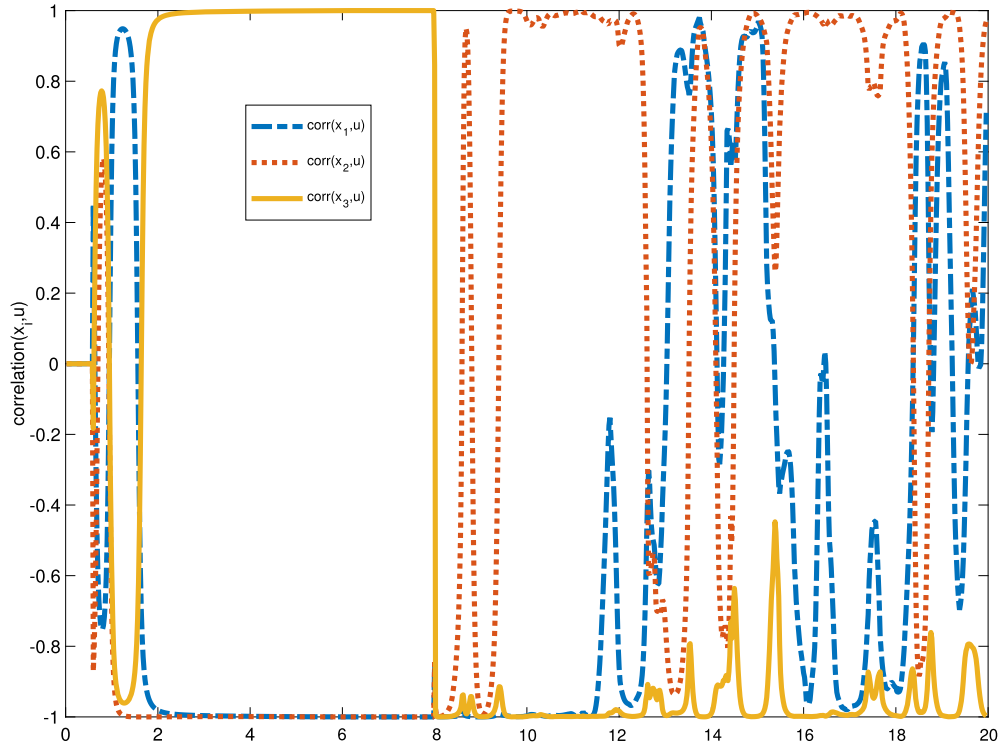

Fig. 5. Correlation trajectory between states and control signal before and after the time-delay attack's existence.

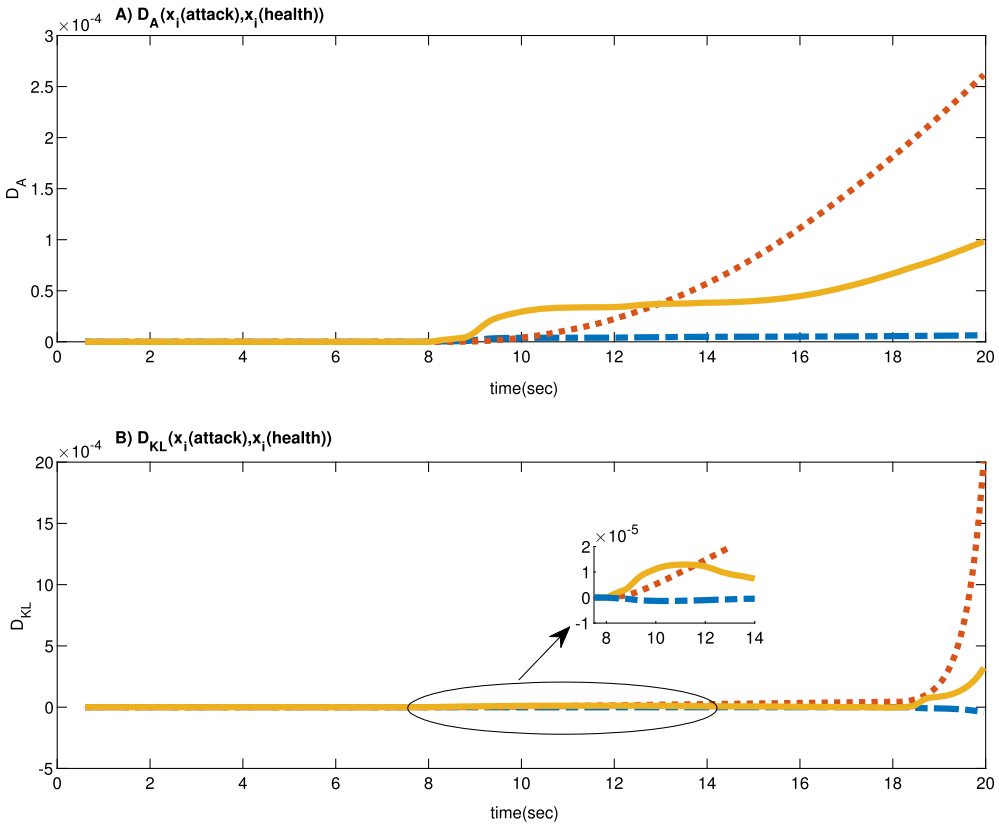

Fig. 6. Measurement variation with false data injection attacks in $t = 8$ *sec*: A) Absolute distance value D_A. B) K-L divergence value D_{KL}.

system with the variable sinusoidal behavior is practically the worst-case scenario. Based on this article's approach, the system can maintain its stability under this condition, as shown in simulation results. Thus, the system's response accuracy will be much higher than other control strategies, specifically in industrial systems.

Remark 4. Since the proposed robust control strategy can maintain the system states bounded under time-delay attacks with time-varying and unknown delays, the trustworthiness of the system's performance is increased. Moreover, by proposing the statistical methods to detect faults for the mentioned attacks, we illustrated in simulation results that attacks can be detected at the time of their occurrence and thus, we stated the term 'Trust-based' in the paper title to state that both provided fault detection and robust control strategies are trustworthy.

5. Conclusions

This article has proposed the secure, robust control design issue against unknown time-delay attacks of uncertain CPSs. The system's stability has been analyzed using a descriptor model representation and appropriate Lyapunov functional conditions for the closed-loop system. Furthermore, closed-loop security has been guaranteed by calculating the optimal feedback control gain in linear matrix inequalities (LMIs). Different time-delay attack detection frameworks have been proposed and compared according to the statistical analysis fault detection methods such as correlation analysis and Kullback-Leibler (K-L) divergence criteria from the mathematical view and in simulations. Finally, numerical results illustrated that the closed-loop uncertain system could remain stable with the proposed robust controller under time-delay attacks. The proposed approach can be applied to controlling systems with inaccurate models with variable environmental changes. Besides, suppose the system includes some delays or a threat of system instability due to delay effects caused by environmental changes. In that case, the presented conservative robust approach can be used to provide the system's stability, and it will enhance the system's resiliency. If the injected attack signals involve non-Gaussian distributions, new robust approaches should be developed since this paper's design cannot maintain the system's stability under non-Gaussian adversaries. Thus, subsequent studies include the security analysis of various types of CPSs in smart infrastructures under time-delay adversaries added to different types of Gaussian/non-Gaussian cyber threats and the design of associated fault detection and protection strategies.

Declarations

Author contribution statement

S. Baromand: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

A. Zaman: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

L. Mihaylova: Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This work was supported by ECO-Qube (956059).

Data availability statement

Data will be made available on request.

Declaration of interests statement

The authors declare no conflict of interest.

Additional information

Supplementary content related to this article has been published online at https://doi.org/10.1016/j.heliyon.2021.e07294.

References

[1] J. Ma, Z. Cheng, X. Zhang, M. Tomizuka, T.H. Lee, Optimal decentralized control for uncertain systems by symmetric Gauss-Seidel semi-proximal alm, IEEE Trans. Autom. Control (2021) 1.

[2] X. Zhao, L. Zhang, P. Shi, H.R. Karimi, Novel stability criteria for t–s fuzzy systems, IEEE Trans. Fuzzy Syst. 22 (2) (2014) 313–323.

[3] X. Li, G. Yang, Fls-based adaptive synchronization control of complex dynamical networks with nonlinear couplings and state-dependent uncertainties, IEEE Trans. Cybern. 46 (1) (2016) 171–180.

[4] Z. Li, X. Zhao, J. Yu, On robust control of continuous-time systems with state-dependent uncertainties and its application to mechanical systems, ISA Trans. 60 (2015).

[5] G. Wang, M. Chadli, H. Chen, Z. Zhou, Event-triggered control for active vehicle suspension systems with network-induced delays, J. Franklin Inst. 10 (2018).

[6] S.-I. Niculescu, K. Gu, Advances in Time-Delay Systems, vol. 38, 2004.

[7] X. Li, P. Li, Stability of time-delay systems with impulsive control involving stabilizing delays, Automatica 124 (2021) 109336.

[8] R. Yang, G. Zhang, L. Sun, Observer-based finite-time robust control of nonlinear time-delay systems via Hamiltonian function method, Int. J. Control (2020) 1–18, https://www.tandfonline.com/doi/full/10.1080/00207179.2020.1774657.

[9] H. Choi, J. Hammer, Optimal robust control of nonlinear time-delay systems: maintaining low operating errors during feedback outages, Int. J. Control 91 (2) (2018) 297–319.

[10] R. Sakthivel, K. Mathiyalagan, S.M. Anthoni, Robust stability and control for uncertain neutral time delay systems, Int. J. Control 85 (4) (2012) 373–383.

[11] Sing Kiong Nguang, Robust stabilization of a class of time-delay nonlinear systems, IEEE Trans. Autom. Control 45 (4) (2000) 756–762.

[12] C. Hua, G. Feng, Robust control design of a class of nonlinear time delay systems via backstepping method, Automatica 44 (2008) 567–573.

[13] S. Yoo, J. Park, Y.H. Choi, Adaptive dynamic surface control for stabilization of parametric strict-feedback nonlinear systems with unknown time delays, IEEE Trans. Autom. Control 52 (2008) 2360–2365.

[14] D. Swaroop, J.K. Hedrick, P.P. Yip, J.C. Gerdes, Dynamic surface control for a class of nonlinear systems, IEEE Trans. Autom. Control 45 (10) (2000) 1893–1899.

[15] T. Zhang, S. Ge, Adaptive dynamic surface control of nonlinear systems with unknown dead-zone in pure feedback form, Automatica 44 (2008) 1895–1903.

[16] Y. Sun, J. Yu, Z. Li, Event-triggered finite-time robust filtering for a class of state-dependent uncertain systems with network transmission delay, IEEE Trans. Circuits Syst. I, Regul. Pap. 66 (3) (2019) 1076–1089.

[17] S. Wen, Z. Zeng, M.Z.Q. Chen, T. Huang, Synchronization of switched neural networks with communication delays via the event-triggered control, IEEE Trans. Neural Netw. Learn. Syst. 28 (10) (2017) 2334–2343.

[18] Z. Gu, P. Shi, D. Yue, Z. Ding, Decentralized adaptive event-triggered h_∞ filtering for a class of networked nonlinear interconnected systems, IEEE Transactions on Cybernetics 49 (5) (2018) 1570–1579.

[19] S. Wen, T. Huang, X. Yu, M.Z.Q. Chen, Z. Zeng, Aperiodic sampled-data sliding-mode control of fuzzy systems with communication delays via the event-triggered method, IEEE Trans. Fuzzy Syst. 24 (5) (2016) 1048–1057.

[20] Z. Wu, Y. Xu, Y. Pan, H. Su, Y. Tang, Event-triggered control for consensus problem in multi-agent systems with quantized relative state measurements and external disturbance, IEEE Trans. Circuits Syst. I, Regul. Pap. 65 (7) (2018) 2232–2242.

[21] Q. Jia, W.K.S. Tang, Event-triggered protocol for the consensus of multi-agent systems with state-dependent nonlinear coupling, IEEE Trans. Circuits Syst. I, Regul. Pap. 65 (2) (2018) 723–732.

[22] E. Tian, Z. Wang, L. Zou, D. Yue, Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication, Int. J. Robust Nonlinear Control 29 (2018).

[23] S. Wen, X. Yu, Z. Zeng, J. Wang, Event-triggering load frequency control for multi-area power systems with communication delays, IEEE Trans. Ind. Electron. 63 (2) (2016) 1308–1317.

[24] Y. Choi, S. Yoo, Event-triggered output-feedback tracking of a class of nonlinear systems with unknown time delays, Nonlinear Dyn. 96 (2019).

[25] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X.-M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (2018) 1674–1683.

[26] J. Liu, E. Tian, X.-P. Xie, H. Lin, Distributed event-triggered control for networked control systems with stochastic cyber-attacks, J. Franklin Inst. 356 (2018).

[27] L. An, G. Yang, Secure state estimation against sparse sensor attacks with adaptive switching mechanism, IEEE Trans. Autom. Control 63 (8) (2018) 2596–2603.

[28] N. Jahanshahi, N. Meskin, F. Abdollahi, W.M. Haddad, An adaptive sliding mode observer for linear systems under malicious attack, in: 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 001437–001442.

[29] W. Ao, Y. Song, C. Wen, Adaptive cyber-physical system attack detection and reconstruction with application to power systems, IET Control Theory Appl. 10 (12) (2016) 1458–1468.

[30] S. Amin, A.A. Cárdenas, S.S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: R. Majumdar, P. Tabuada (Eds.), Hybrid Systems: Computation and Control, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 31–45.

[31] I. Corona, G. Giacinto, F. Roli, Adversarial attacks against intrusion detection systems: taxonomy, solutions and open issues, Inf. Sci. 239 (2013) 201–225.

[32] V.S. Dolk, P. Tesi, C. De Persis, W.P.M.H. Heemels, Event-triggered control systems under denial-of-service attacks, IEEE Trans. Control Netw. Syst. 4 (1) (2017) 93–105.

[33] L. An, G. Yang, Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent dos attacks, IEEE Trans. Cybern. 49 (3) (2019) 827–838.

[34] C. Kwon, I. Hwang, Cyber attack mitigation for cyber–physical systems: hybrid system approach to controller design, IET Control Theory Appl. 10 (7) (2016) 731–741.

[35] J. Wang, Z. Liu, S. Zhang, X. Zhang, Defending collaborative false data injection attacks in wireless sensor networks, Inf. Sci. 254 (2014) 39–53.

[36] W. He, X. Gao, W. Zhong, F. Qian, Secure impulsive synchronization control of multi-agent systems under deception attacks, Inf. Sci. 459 (2018).

[37] D. Ding, Z. Wang, Q. Han, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst. Man Cybern. Syst. 48 (5) (2018) 779–789.

[38] L. An, G. Yang, Lq secure control for cyber-physical systems against sparse sensor and actuator attacks, IEEE Trans. Control Netw. Syst. 6 (2) (2019) 833–841.

[39] A. Zaman, B. Safarinejadian, W. Birk, Security Analysis and Fault Detection Against Stealthy Replay Attacks, Taylor & Francis, 2020, pp. 1–22, https://www.tandfonline.com/doi/full/10.1080/00207179.2020.1862917.

[40] M. Zhu, S. Martínez, On the performance analysis of resilient networked control systems under replay attacks, IEEE Trans. Autom. Control 59 (3) (2014) 804–808.

[41] A.J. Gallo, M.S. Turan, F. Boem, G. Ferrari-Trecate, T. Parisini, Distributed watermarking for secure control of microgrids under replay attacks, in: 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems NECSYS 2018, 2018, https://www.sciencedirect.com/science/article/pii/S240589631833564X.

[42] J. Liu, M. Yang, E. Tian, J. Cao, S. Fei, Event-based security control for state-dependent uncertain systems under hybrid-attacks and its application to electronic circuits, IEEE Trans. Circuits Syst. I, Regul. Pap. 66 (12) (2019) 4817–4828.

[43] J. Liu, M. Yang, X. Xie, C. Peng, H. Yan, 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) (2020) 1021–1034.

[44] S.J. Yoo, Neural-network-based adaptive resilient dynamic surface control against unknown deception attacks of uncertain nonlinear time-delay cyberphysical systems, IEEE Trans. Neural Netw. Learn. Syst. 31 (10) (2020) 4341–4353.

[45] A. Sargolzaei, K.K. Yen, M.N. Abdelghani, S. Sargolzaei, B. Carbunar, Resilient design of networked control systems under time delay switch attacks, application in smart grid, IEEE Access 5 (2017) 15901–15912.

[46] S. Boyd, L. El Ghaoui, E. Feron, V. Balakrishnan, Linear Matrix Inequalities in System and Control Theory, Studies in Applied Mathematics, vol. 15, SIAM, Philadelphia, PA, 1994.

[47] C.E. de Souza, X. Li, Delay-dependent robust h_∞ control of uncertain linear state-delayed systems, Automatica 35 (7) (1999) 1313–1321.