Robust Self-Triggered Control for Nonlinear Cyber-Physical Systems with State Constraints under DoS Attacks

Zhaoyang Cuan
University of Science and Technology Beijing
Dawei Ding (ddaweiauto@163.com)
University of Science and Technology Beijing https://orcid.org/0000-0003-1201-7785
Heng Wang
University of Science and Technology Beijing

Research Article

Keywords: Cyber-physical systems, state constraints, DoS attacks, Zeno behavior, nonlinear systems.

Posted Date: December 22nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1098276/v1

Robust Self-Triggered Control for Nonlinear Cyber-Physical Systems with State Constraints under DoS Attacks

Zhaoyang Cuan[1], Da-Wei Ding[1*] and Heng Wang[1]

[1]School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing, 100083, China.

*Corresponding author(s). E-mail(s): ddaweiauto@163.com;
Contributing authors: b20200303@xs.ustb.edu.cn; hengwang@ustb.edu.cn;

Abstract

This paper is concerned with the event-based control problem for nonlinear cyber-physical systems (CPSs) with state constraints. A novel security control strategy consisting of a self-triggered mechanism is developed to decrease the network communication loads to the most extent on the basis of ensuring system safety and stability. The maximum capability of the designed self-triggered mechanism to resist denial-of-service (DoS) attacks occurring in controller-actuator (C-A) and sensor-controller (S-C) channels synchronously is also analyzed. In particular, we prove that the security control strategy guarantees the system safety and stability without resulting in Zeno behavior. Finally, a numerical example is provided to demonstrate the prominent effectiveness and the advantages over the existing results.

Keywords: Cyber-physical systems, state constraints, DoS attacks, Zeno behavior, nonlinear systems.

1 Introduction

With the rapid development of sensing and information technologies, cyber-physical systems (CPSs) have become a research hotspot, which have emerging and wide applications in areas such as transportation, remote medical services, smart grids, power plant, military communities, and so on [1]-[7]. CPSs share data through wireless communication networks [6]. However, especially, conventional control strategies regularly transmit control inputs [5], which may consume unnecessary communication resources and overload the network in CPSs. And what's worse, no one can guarantee that safety constraints will still hold for CPSs. Since the sampling frequency of plant is fixed, it could make the system violate safety constraints between two consecutive sampled time instants. The event-based mechanism (EBM) provides a promising solution to this problem [8]. The essential characteristic of EBM lies in deciding time instant to update the controller, which is specified by satisfying a certain prescribed triggering condition. Furthermore, EBM can effectually decrease communication consumption loads and reduce the frequency to calculate control inputs. Therefore, on the basis of saving conmmunication resources, it is necessary to design an efficient approach to guarantee the stability and safety of nonlinear CPSs.

Generally speaking, the works about EBM primarily consist of three portions: 1) the event-triggered control (ETC) [9]-[10]; 2) the self-triggered control (STC) [11]-[13]; and 3) the periodic triggering control (PTC) [14]-[15]. The ETC strategy continously monitors the real and its nominal states of system to determine the next triggering time instant until prescribed triggering condition is satisfied. In order to reduce the monitoring consumption of ETC, STC is proposed, where the next triggering time instant is decided by examing a prescribed triggering condition at the current time instant. The PTC is at the intermediate level, but the system states still need to be monitored periodically.

Although EBM has a great advantage in decreasing communication loads, real-time control is central to many nonlinear CPSs with state constraints. The design of a real-time controller must take into account several factors, including computional resources, safety and stability. In particular, a critical way to achieve the last two purposes is to utilize Control Lyapunov Functions (CLFs) [16]-[17] for stability and Control Barrier Functions (CBFs) [18]-[21] for safety that can be combined through quadratic programs (QPs), which are adopted in many safety-critical nonlinear CPSs. Notwithstanding, most of real-time controllers are based on a continuous-time formulation, which is in contradiction with the reality that these controllers are implemented on digital platform, where the updates to the control law can be conducted only at discrete time instants.

Based on the above discussions, the fundamental difficulty lies in how to achieve the real-time control for nonlinear CPSs with state constraints on the basis of minimizing the consumption of network communication resources. To the best of our knowledge, there has been few researches concerning this problem. Motivated by CLFs and CBFs, in this paper, we aim at designing a robust self-triggered security control strategy for nonlinear CPSs with state constraints, and analyzing the maximum ability to resist denial-of-service (DoS) attacks occurring in controller-actuator (C-A) and sensor-controller (S-C) channels synchronously. Compared with most existing results, the distinguished contributions of this paper can be summarized as follows:

1) A novel self-triggered mechanism is designed to minimize the consumption of network communication resources.

2) The maximum capability to resist DoS attacks of the designed self-triggered mechanism is analyzed. Particularly, the maximum duration of DoS attacks is calculated on the premise of guaranteeing safety and stability of nonlinear CPSs, where the DoS attacks occur in C-A and S-C channels synchronously.

3) A security control strategy is developed to guarantee that state constraints are always satisfied under the condition that the aperiodic update of control signals and transmission of control inputs is achieved to reduce the consumption of network communication resources under DoS attacks, i.e., the safety and stability of nonlinear CPSs are both guaranteed.

The rest of this paper is organized as follows. Section II is the preliminaries and problem formulation. Section III presents the detailed analysis of maximum capability to resist DoS attacks of the designed self-triggered mechanism and the novel security control strategy based on designed self-triggered mechanism. Then, simulation and comparisons are provided in Section IV. Finally, Section V concludes this paper.

Notations : Let $\mathbb{N}$ and $\mathbb{R}$ denote the set of integers and the set of real numbers, respectively. $\mathbb{R}^n$ is the set of all n-dimensional column vectors. The Lie derivative of a smooth function $h(x)$ along dynamics $\dot{x} = f(x)$ is denoted as $L_f h(x) := \frac{\partial h(x)}{\partial x} f(x)$. A function $f : \mathbb{R}^n \mapsto \mathbb{R}^m$ is Lipschitz continuous on $\mathbb{R}^n$ if the equality $\|f(y) - f(x)\| \leq L\|y - x\|$, $\forall x, y \in \mathbb{R}^n$. A continuous function $\alpha : [-b, a) \mapsto [-\infty, \infty)$, for some a, b > 0, belongs to the extended class $\mathcal{K}$ if it is strictly increasing and $\alpha(0) = 0$.

2 Preliminaries and Problem Formulation

2.1 System Dynamics

We consider the structure of CPSs presented in Fig. 1, in which the controller is in the cloud platform which belongs to the cyber portion, and the actuator, plant, and sensor are in the physical portion. As shown in Fig. 1, the physical

process is controlled through wireless communication networks, where both the C-A and S-C channels might be attacked by the DoS attacks synchronously. Here, the physical plant to be controlled is described by the following nonlinear continuous-time system dynamics:

$$\dot{x} = f(x) + g(x)u, \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the system state, $u \in \mathbb{R}^m$ denotes the control input. Let $x_0 := x(t_0) \in \mathbb{R}^n$.

The system states are constrained by a set of safety constraints depicted as follows

$$\mathcal{C} = \{x \in \mathbb{R}^n \mid h(x) \geq 0\}, \tag{2}$$

where $h(\cdot) : \mathbb{R}^n \to \mathbb{R}$ is continuously differentiable.

The set $\mathcal{C}$ is denoted as forward invariant for system (1) if $x_0 \in \mathcal{C}$ implies $x(t) \in \mathcal{C}, \forall\, t \in I(x_0)$. Hence, in this paper, the set $\mathcal{C}$ must be always guaranteed as forward invariant.

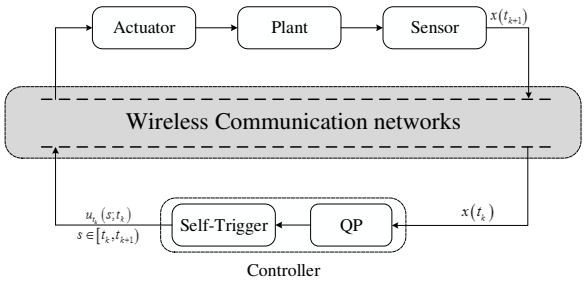

Fig. 1 The schematic diagram of the CPSs

Consequently, for nonlinear CPSs shown in Fig. 1, the objectives to be achieved in this paper are depicted as follows:

1) The first objective is to design a self-triggered mechanism for (1) to decrease networked communication loads to the most extent;

2) The second objective is to analyze the maximum capability to resist DoS attacks of the designed self-triggered mechanism, especially to calculate the maximum duration of DoS attacks on the premise of guaranteeing the safety and stability of nonlinear CPSs;

3) The third objective is to develop a novel security control strategy based on the designed self-triggered mechanism to guarantee that the system (1) is at least asymptotically stable while state constraints (2) are satisfied under the condition that the aperiodic update of control signals and transmission of control inputs are achieved to reduce the consumption of network communication resources to the most extent under DoS attacks.

To facilitate the control strategy development, the following assumption and definition are made for system (1).

Assumption 1 : The function $f(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ and $g(\cdot) : \mathbb{R}^n \to \mathbb{R}^{n*m}$ are locally Lipschitz continuous over the region of interest about system state x with Lipschitz constant L_f and over the control input u with Lipschitz constant L_g, respectively.

Definition 1: For the dynamical system (1) and the set $\mathcal{C}$ defined by (2) for some continuous differentiable function $h : \mathbb{R}^n \to \mathbb{R}$, if there exist an extended class $\mathcal{K}$ function α and a set $\mathcal{C}$ such that

$$\sup_{u \in U} \left[L_f h(x) + L_g h(x) u + \alpha(h(x))\right] \geq 0, \forall x \in \mathcal{C} \tag{3}$$

then the function h is called zeroing control barrier function (ZCBF).

2.2 Optimal Control Problem

For the continuous dynamical system (1), an initial state $x_0 \in \mathcal{C}$. In order to stabilize the system state to a desired state $x_d \in \mathbb{R}^n$ on the premise of ensuring that the safety constraints are met, we design a self-triggered mechanism to actively compute the next update instance at which controller update the control inputs given the safety constraints and stability constraints, where control input is calculated through resolving the following optimal control problem denoted as QPs.

Given system (1), the QPs are defined as follows:

$$\begin{aligned} u^*(x) &= \operatorname{argmin}\left[\frac{1}{2}u^T H(x)u + F^T(x)u\right], \\ \text{s.t.} \quad &\begin{cases} L_f h(x) + L_g h(x) u + \alpha(h(x)) \geq 0 \\ L_f V(x) + L_g V(x) u + \epsilon(V(x)) \leq 0 \end{cases} \end{aligned} \tag{4}$$

where $V(x)$ is CLFs, $H(x) \in R^{(m)*(m)}$ and $F(x) \in R^m$ are arbitary cost functions, which can be selected on the basis of the desired (state based) weighting of control inputs.

Particularly, the self-triggered mechanism to be designed introduces the notions of CBFs safe

period for the safety constraints (ι_{CBF}) and CLFs update period for stability constraints (ι_{CLF}). The safe period and update period are obtained by computing a lower bound on the CBFs constraints and a upper bound on the CLFs constraints, and bounds of trajectories of system states. Let the sequence $\{t_k\}_{k\in\mathbb{N}_{\geq 0}}$ represent the time instants at which the control signal is updated and controller update the control input, then the next update instant can be obtained as $t_{k+1} := t_k + min(\iota_{CBF}, \iota_{CLF})$.

At every update instant t_k, resolve (4) to compute the optimal control input u_k and apply it in a Zeroth-Order-Hold (ZOH) pattern [22] until the next update instant t_{k+1}. In particular, the strategy utilized by our designed self-triggered mechanism aims at guaranteeing that u_k applied in a ZOH manner could make the safety constraint and stability constraint in (4) will still hold at the interval $t_k \leq t \leq t_{k+1}$.

Remark 1 It should be pointed out that $h(x)$ acts as safety constraint of system (1), and $V(x)$ plays the part of stability constraint, which must hold at any time. Therefore, it is significant to guarantee two constraints hold when $t \in [t_k, t_{k+1})$ under the designed self-triggered mechanism. On the one hand, the self-triggered mechanism can reduce the consumption of network communication resources to the most extent, and on the other hand, it does not violate safety constraint and stability constraint.

3 Main Results

In this section, firstly, we will illustrate the designed self-triggered mechanism including the detailed issues about the calculation process of CBFs safe period (ι_{CBF}) and CLFs update period (ι_{CLF}). Then, we analyze the maximum capability to resist DoS attacks of the designed self-triggered mechanism. Particularly, the maximum duration of DoS attacks is calculated on the premise of guaranteeing safety and stability of nonlinear CPSs, which is summarized in Theorem 1. Finally, based on the designed self-triggered mechanism, we further develop a novel security control strategy, which is summarized in Algorithm 1 and Theorem 2.

3.1 CBFs Safe Period

For the computation of the CBFs safe period, we count on calculating bounds of the inequalities in (4). Concretely speaking, we try to find a bound on the system trajectory which exclusively relies on prevailing features of system dynamics. Then, at every t_k, we evaluate the trajectory bound, denote $w_{t_k}(t) = w(t + t_k)$, $\forall t \geq t_k$, and denote the upper bound of w_{t_k} as $\overline{w}_{t_k}$.

Before introducing the main result of this subsection, we first show that the upper bound of w_{t_k} can be obtained, the result is summarized in lemma 1.

Lemma 1 Given the continuous dynamical system (1), starting from $x(t_k)$, the distance between the trajectory $x(t + t_k)$ and $x(t_k)$ is bounded by $\overline{w}_{t_k}(t) = e^{L(t-t_k)}r_0 \text{-} \frac{1}{L}(1 - e^{L(t-t_k)})\|f(x(t_k)) + g(x(t_k))u(t_k)\|$, $\forall t \geq t_k$.

Proof Let $w_{t_k}(t) = \|x(t_k + t) - x(t_k)\|$. Calculate its derivative $\dot{w}(t)$ as $\dot{w}(x(t + t_k)) = \frac{(x(t+t_k)-x(t_k))^T}{\|x(t+t_k)-x(t_k)\|} f(x(t + t_k), u)$. Since $\frac{(x(t+t_k)-x(t_k))^T}{\|x(t+t_k)-x(t_k)\|}$ is a unit vector, then we can get

$$\begin{aligned}\dot{w}(t_k) &\leq \|f(x(t + t_k), u)\| \\ &\leq \|f(x(t + t_k), u) - f(x(t_k), u)\| + \|f(x_{t_k}, u)\|.\end{aligned} \tag{5}$$

Due to the assumption that the system dynamics is Lipschitz continuous, then the following equality holds

$$\|f(x(t + t_k), u) - f(x(t_k), u)\| \leq L\|x(t + t_k) - x(t_k)\|, \tag{6}$$

where L is the Lipschitz constant for f. Substituting (6) into (5), we have

$$\dot{\overline{w}}_{t_k(t)} \leq L\overline{w}(t + t_k) + \|f(x(t_k), u)\|, \tag{7}$$

then, we have

$$\|f(x(t_k), u)\| = \|f(x(t_k)) + g(x(t_k))u_k\|. \tag{8}$$

Then, the solution of (7) is

$$\begin{aligned}\overline{w}_{t_k}(t) \leq & e^{L(t-t_k)}w_0 + \\ & \frac{1}{L}(e^{L(t-t_k)} - 1)\|f(x(t_k)) + g(x(t_k))u(t_k)\|,\end{aligned} \tag{9}$$

where $w_0 = \overline{w}_{t_k}(t_k)$, $\overline{w}_{t_k}(0) = w_{t_k}(0)$.

Finally, once we get $\overline{w}_{t_k}(t)$,then a ball bounding the trajectory under system dynamics (1) can be defined as follows

$$B_{w_{t_k}} = \{x \in \mathbb{R}_n : \|x(t) - x(t_k)\| \leq \overline{w}_{t_k}\}. \tag{10}$$

□

Lemma 1 verifies that the upper bound of the distance between trajectory $x(t+t_k)$ and $x(t_k)$ can be obtained. Next, we will make it clear that the CBFs safe period can be calculated based on the above result.

Definition 1 For dynamical system (1) starting at $x(t_k) \in \mathcal{C}$, if there exists a ι_{CBF} such that $x(t_k+\iota_{CBF}) \in \mathcal{C}$ for all $t \in [t_k, t_k+\iota_{CBF})$ under a constant control input u_k, then ι_{CBF} is seen as a safe period for system (1) at time t_k.

Based on (3), we define the CBFs constraint as follows:

$$\Theta_{CBF}(t) = L_f h(x(t)) + L_g h(x(t))u + \alpha(h(x(t))), \tag{11}$$

for all $x \in \mathcal{C}$. If $\Theta_{CBF}(t) \geq 0$, then the system (1) is forward invariant. By Lemma 1, we can determine ι_{CBF} to obtain lower bound $\underline{\Theta}_{CBF}(t)$ by means of $\overline{w}_{t_k}(t)$ rather than only rely on the closed-form solution of $x(t)$. In other words, we will count on the implication as follows:

$$\underline{\Theta}_{CBF}(t) \geq 0 \Longrightarrow \Theta_{CBF}(t) \geq 0, \forall t_k \leq t \leq t_{k+1}. \tag{12}$$

At every update instant t_k, define the initial condition $\underline{\Theta}_{CBF}(t_k) = \Theta(t_k)$. In order to simplify the notation for the rest of this subsection, we define $\Theta(t) := \Theta_{ECBF}(t)$ which has a similar definition to $\underline{\Theta}$. Then $\underline{\Theta}$ can be obtained by means of another application of the comparison theorem:

$$\underline{\Theta}(t) = \dot{\underline{\Theta}}(t)t + \Theta(t_k), \tag{13}$$

where $\dot{\underline{\Theta}}(t) \leq \dot{\Theta}(t)$, for all $t \in [t_k, t_{k+1}]$. In order to get $\dot{\underline{\Theta}}(t)$, we denote the derivative of $\Theta(t)$ as

$$\dot{\Theta}(t) = \frac{\partial \Theta(t)}{\partial x}(f(x(t)) + g(x(t))u). \tag{14}$$

As we can see from (14), after factoring out each term, i.e., $\frac{\partial \Theta(t)}{\partial x} f(t)$ and $\frac{\partial \Theta(t)}{\partial x} g(t)u$, we can obtain explicit expression including state $x(t)$ and control input u. On the other hand, because u retains constant for all $t \in [t_k, t_{k+1}]$ under ZOH, then we only need to take state bound into consideration. By Lemma 1, we use $\overline{w}_{t_k}(t)$ to determine the boundary of the state and utilize Lipschitz condition Θ, f and g to obtain $\underline{\Theta}(t)$.

Remark 2 As we can see from the calculation process of $\underline{\Theta}(t)$, it is time dependent, since we substitute $x(t)$ with $w(t)$ in the original safety constraint $\Theta(t_k)$. Therefore, there is no necessity to calculate the closed-loop solution of (1) to appraise the safety constraint.

Obtaining the lower bound $\underline{\Theta}(t)$, the CBFs safe period ι_{CBF} can be determined to guarantee $\underline{\Theta}(t_k + \iota_{CBF}) = 0$. As a result, the considered problem is equal to calculate a root for $\underline{\Theta}$. Suppose that it is hard to get the closed-loop solution of (13) about t, we can calculate its roots by means of algorithms such as the secant method [23]. On the other hand, if there exist multiple CBFs constraints, every of which is denonted as Θ_i respectively, then the safe period that satisfies all CBFs constraints is denoted as follows:

$$\iota_{CBF} = min(\iota_{CBF}, i), \forall i. \tag{15}$$

3.2 CLFs Update Period

Except for the safety constraint (11), the CLFs constraint in (4) is also utilized to compute the next update instant t_{k+1}. Instinctively, if we naively apply this update rule $t_{k+1} := t_k + \iota_{CBF}$, the resulting state trajectory may be out of the equilibrium.

Since the QPs formula is resolved point by point in time, it is impossible to ensure the exponential convergence to the desired state on the ZOH implementation. Aiming at guaranteeing at least asymptotic stability, we define a CLFs update period, which guarantees that the Lyapunov function monotonously decreases at each step. A useful lemma is firstly recalled here.

Lemma 2 Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be continuously differentiable, and let x and y be two vectors in $\mathbb{R}^n$. Supposing that

$$\| \bigtriangledown f(x+ty) - \bigtriangledown f(x) \| \leq Lt\|y\|, \forall t \in [0,1], \tag{16}$$

where L is some scalar, $\bigtriangledown f(x) = \left[\frac{\partial f(x)}{\partial x_1}, \frac{\partial f(x)}{\partial x_2}, \frac{\partial f(x)}{\partial x_3}, \cdots, \frac{\partial f(x)}{\partial x_n}\right]^T$. Then, the following equality holds

$$f(x+y) \leq f(x) + \dot{y} \bigtriangledown f(x) + \frac{L}{2}\|y\|^2. \tag{17}$$

Proof For the ease of presentation, let t be a scalar parameter and let $g(t) = f(x+ty)$. The chain rule fields $(dg/dt)(t) = \dot{y} \bigtriangledown f(x+ty)$. Now

$$
\begin{aligned}
& f(x+y)-f(x) \\
&= g(1)-g(0) \\
&= \int_0^1 \frac{dg}{dt}(t)dt \\
&= \int_0^1 \dot{y} \bigtriangledown f(x+ty)dt \\
&\leq \int_0^1 \bigtriangledown f(x)dt + |\int_0^1 \dot{y}(\bigtriangledown f(x+ty) - \bigtriangledown f(x))dt| \\
&\leq \int_0^1 \bigtriangledown f(x)dt + \int_0^1 \|y\| \cdot \| \bigtriangledown f(x+ty) - \bigtriangledown f(x)\|dt \\
&= \dot{y} \bigtriangledown f(x) + \|y\| \int_0^1 Lt\|y\|dt \\
&= \dot{y} \bigtriangledown f(x) + \frac{L}{2}\|y\|^2,
\end{aligned}
\tag{18}
$$

furthermore, it yields that

$$
f(x+y) \leq f(x) + \dot{y} \bigtriangledown f(x) + \frac{L}{2}\|y\|^2. \tag{19}
$$

□

Definition 2 For the continuous dynamical system (1), if $V(x(t_k + \iota_{CLF})) - V(x(t_k)) \leq 0$, then the ι_{CLF} is a CLFs update period.

For systems whose closed-loop solution can not be easily obtained for their trajectory, it is necessary to get an upper bound $\hat{V}(t)$ such that $\hat{V}(t) \geq V(x(t)), \forall\ t_k \leq t \leq t_{k+1}$,

$$
\hat{V}(t) \leq 0 \Longrightarrow V(x(t)) \leq 0, \forall t_k \leq t \leq t_{k+1}. \tag{20}
$$

By means of descent lemma [24], we can calculate the upper bound of $V(x(t))$. The following inequality holds

$$
V(t) \leq V(t_k) + (t-t_k)\dot{V}(t_k) + (t-t_k)^2\frac{M}{2} \doteq \hat{V}(t). \tag{21}
$$

where $M := \max_{x\in\mathcal{C}} \ddot{V}(t)$, and we use the notation $V(t) = V(x(t))$; The proof can be found in [24], [25].

Remark 3 In order to obtain sharper bound on M, we can maximize the second derivative on $\mathcal{C} \cap \{x : V(x) < V(x(t_k))\}$.

Remark 4 We utilize distinct bounds for computing ι_{CBF} and those used for ι_{CLF} because otherwise in many general situations we will begin with a bound very close to zero near the equilibrium, thus implying a vanishing ι_{CLF}.

Because $\hat{V}(t)$ is a square function of t, then there must exist closed-loop solution for the roots. Accordingly, in the process of determining ι_{CLF}, the condition that we aim at enforcing is $\hat{V}(t) - V(x(t_k)) \leq 0$, which leads to the non-zero root of $\dot{\hat{V}}(t) = 0$ as

$$
\iota_{CLF} = \frac{-2\dot{V}(x(t_k))}{M}. \tag{22}
$$

Before we proceed to the analysis, the following assumption should be made.

Assumption 1 For the inequality constraint $\dot{V}(x(t)) \leq -\epsilon V(x(t))$ in (4), we give a assumption that there exists a neighborhood of equilibrium such that the optimal solution through resolving the QPs will make the inequality above gradually develop into an equality $\dot{V}(x(t)) = -\epsilon V(x(t))$. Suppose that this assumption is valid, considering the nature of the cost and two constraints of the QPs, namely satisfying the CLFs constraints while minimizing control effort, then the Lyapunov function $V(x(t))$ decreases to zero in the process of the system approaching the desired equilibrium. At this moment, the CLFs constraint is the sole active constraint, while all the other constraints are not active.

Proposition 1 For the nonlinear continuous time dynamical system (1),

$$
\lim_{x\to x_d} \iota_{CLF} > 0, \tag{23}
$$

that is to say, in the total process that system converge to equilbrium, the sequence of ι_{CLF} keeps bounded far away from zero.

Proof In order to complete the proof, it is necessary to prove that the limit (22) will become a constant strictly greater than zero in the process that the system approaches the equilbrium, i.e., on condition that the Assumption 1 is true, the following equality holds

$$
\begin{aligned}
\iota_{CLF} &= \frac{2\epsilon V(x(t_k))}{M} \\
&= \frac{2\epsilon V(x(t_k))}{max_{x\in\mathcal{C}}\ddot{V}(x(t))}.
\end{aligned}
\tag{24}
$$

Furthermore, a closed-loop solution for control u of (4) exists. Based on the equality assumption of

Assumption 1, the control input can be analytically determined as

$$u^* = \frac{-\epsilon V(x(t)) - L_f V(x(t_k))}{L_g V(x(t_k))}. \tag{25}$$

Since $\ddot{V}(x(t))$ counts on both control input u and state $x(t)$, which is hard to get. By means of the closed form of (25), we can see that the numerator and denominator of (24) get the same order of magnitude about $V(x(t))$. As a result, the ι_{CLF} becomes a constant strictly greater than zero as the system approaches the ideal equilibrium. Then, the Zeno behavior is avoided. □

3.3 Maximum Capability to Resist Against DoS Attacks

In this subsection, we focus on analysing the maximum capability to resist DoS attacks of the designed self-triggered mechanism and further developing a novel security control strategy. The attacker is only capable of launching limited times attacks owing to its limited power energy. Thus, before proceeding to make analysis, let us make the following assumption.

Assumption 2 Given the CPSs shown in Fig. 1, it is assumed that the DoS attacks do not occur when $t = 0$.

Theorem 1 Given the CPSs shown in Fig. 1, the safety constraint and stability constraint of (1) can be both guaranteed if the following conditions hold

$$dur(A_t) \leq min(\iota_{CBF}, \iota_{CLF}), \tag{26}$$

where $dur(A_t)$ indicates duration of DoS attacks starting from time t, $\min(\iota_{CBF}, \iota_{CLF})$ indicates the minimal one of ι_{CBF} and ι_{CLF} calculated at time t.

Proof Based on the designed self-triggered mechanism, we can see that if the DoS attacks occur at time t_k which is the k-th trigger instant to resolve (4) to obtain u_k, then the safety and stability of (1) can be ensured if (26) holds. □

Remark 5 The DoS attacks duration denote the total time on which the C-A and S-C communication channels are jammed. In particular, the DoS attacks with larger duration make the communication channels unavailable for more time. Besides, there might exist some extreme cases where the C-A and S-C channels are totally disabled such that all the control inputs can not be transmitted. Therefore, it is reasonable to consider that the DoS attacks are contrained by (26).

Based on the designed self-triggered mechanism, the security control strategy is summarized in Algorithm 1 and Theorem 2.

Algorithm 1 Robust Self-Triggered Control

procedure: initialize $x_0, h(x)$ *and* $V(x)$

$x(t_k) := x_0$, $\forall x_0 \in \mathcal{C}$
while $x_{t_k} \notin Goal$ **do**
  while DoS attack does not occur **do**
    Solve (4) to calculate the optimal control input u_k
    Calculate the CBFs safe period ι_{CBF} from (15)
    Calculate the CLFs update period ι_{CLF} from (22)
    $t_{k+1} := t_k + min(\iota_{CBF}, \iota_{CLF})$
  end while
  while DoS attack occurs **do**
    Calculate the starting time t_s of the DoS attacks
    Calculate the solution of (4) at time t_s, and apply it to (1)
    Calculate the CBFs safe period ι_{CBF} from (15)
    Calculate the CLFs update period ι_{CLF} from (22)
    $t_k = t_s$, $t_{k+1} := t_k + min(\iota_{CBF} + \iota_{CLF})$
  end while
end while

end procedure

Theorem 2 For the nonlinear continuous-time system (1) with the control law given by Algorithm 1, supposing that Assumptions 1 and 2 are true, then the closed-loop system (1) under DoS attacks is asymptotically stable without violating state constraint.

Proof We first prove that the closed-loop system (1) with the control law given by Algorithm 1 is asymptotically stable, when there are no DoS attacks.

Based on Lemma 1, Lemma 2 and Proposition 1, it can be seen that the closed-loop system (1) is exponentially stable under the control input u^* with the

control law given by Algorithm 1 when there are no DoS attacks.

Then, we prove that the closed-loop system (1) with the control law given by Algorithm 1 is asymptotically stable when there are DoS attacks.

Assumption 2 indicates that duration of each DoS attack shall not exceed $min(\iota_{CBF}, \iota_{CLF})$ calculated at the moment of attack occurring. Then, using the control law given by Algorithm 1, the closed-loop system (1) is equivalent to the case without DoS attacks. The proof is completed. □

4 Simulation Results

In this section, we will demonstrate the efficiency of the proposed security control strategy by one numerical example.

We consider the concrete nonholonomic mobile robot in CPSs, which has the nonlinear continuous-time system dynamics as follows:

$$\begin{bmatrix} \dot{x}(t) \\ \dot{y}(t) \\ \dot{\theta}(t) \end{bmatrix} = \begin{bmatrix} \cos(\theta(t)) & 0 \\ \sin(\theta(t)) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v(t) \\ \omega(t) \end{bmatrix}. \tag{27}$$

Here, the position of robot is expressed by $[x(t), y(t)]^T$, and the orientation is expressed by $\theta(t)$, then the system state variable are denoted as $[x(t), y(t), \theta(t)]^T$. The control input of robot is u, which is comprised of linear velocity $v(t)$ and angular velocity $\omega(t)$. In addition, the calculated Lipschitz constants are $L_f = 1.5\sqrt{2}$, $L_g = 1$, respectively.

We consider a problem of trajectory tracking, where a mobile robot aims at tracking a target moving in curve line and needs to avoid two moving obstacles in straight-line movement and curve-line movement. Firstly, we transform the tracking-error model expressed in the inertial frame to the body-fixed frame, and denote the error coordinates as

$$\begin{bmatrix} e_x \\ e_y \\ e_\theta \end{bmatrix} = \begin{bmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_d - x \\ y_d - y \\ \theta_d - \theta \end{bmatrix}. \tag{28}$$

The state error is $e = [e_x,\ e_y,\ e_\theta]$ described from the body-fixed frame, $[x_d, y_d, \theta_d]$ means target state. Our goal is to find feasible control inputs v_c and ω_c to stabilize e_x, e_y and e_θ such that mobile robot can track target accurately in the procedure of avoiding obstacles.

The target moves with a cubic spline curve trajectory, with points euqal to [-12.5 -2.5; -10.75 -0.25; -8.75 2; -5.75 1; -3.5 -1; -0.5 -0.5], $t = [0\ 6\ 12\ 18\ 24\ 30]$. The obstacle in straight-line movement is described as follows: points equal to [-13.5 0.5; -10.15 0.5; -8.75 0.5; -6.8 0.5; -5.0 0.5; -4.0 0.5], when $t = 0$ *s*, $v_d \neq 0$ *m/s*, $v_o \neq 0$ *m/s*. The initial mobile robot state is (-15.15 -4.6 0), and t ranges from 0 to 30 *s*. Here, we design control Lyapunov function as

$$V = \sqrt{\overline{e}_\theta^2 + 1} + k\pi - (k+1), \tag{29}$$

where $\overline{e}_\theta = \beta e_\theta + \frac{e_y}{\pi}$, $\pi = \sqrt{e_x^2 + e_y^2 + 1}$, β is a positive constant and $k > \frac{1}{2}$.

Furthermore, we choose ZCBF h as follows:

$$\sqrt{(x - x_{ob})^2 + (y - y_{ob})^2} \geq 0.5, \tag{30}$$

where x_{ob}, y_{ob} mean the position of obstacle.

The safety constraint (30) indicates that the distance between the mobile robot and obstacles must be greater than 0.5 unit, where 0.5 unit can be chosen base on practical situations.

Then, we define the dynamics for the nonlinear CPSs as

$$\dot{x} = f(x) + g(x)u, \tag{31}$$

where $u = [u_0,\ u_1]^T = [v_c,\ \omega_c]^T$, $x = [\overline{e}_\theta,\ e_y,\ -e_x]^T$, and $q_d = [v_d,\ \omega_d]^T$ is the desired velocity in the body-fixed frame.

Thus, the system dynamics can be denoted as follows:

$$f(x) = \begin{bmatrix} \beta\omega_d + \frac{1}{\pi^3}\left\{(e_x^2 + 1)v_d \sin(e_\theta) - v_d e_y e_x \cos(e_\theta)\right\} \\ u_d \sin(e_\theta) \\ -u_d \cos(e_\theta) \end{bmatrix}, \tag{32}$$

$$g(x) = \begin{bmatrix} \frac{1}{\pi^3}(e_y e_x) & -\beta + \frac{1}{\pi^3}\left[-e_x^3 - e_x - e_y^2 e_x\right] \\ 0 & -e_x \\ 1 & -e_y \end{bmatrix}. \tag{33}$$

Our goal is to find control inputs $[u_0, u_1]^T$ based on the developed security control strategy to stabilize $[\overline{e}_\theta, e_y, -e_x]^T$ on the basis of guaranteeing safety constraint (30) hold under DoS attacks.

The simulation is conducted on a computer with Intel Core i7 CPU and dominant frequency

of 3.9GHz with 8GB RAM. And the optimization problem is solved by *quadprog* function in MATLAB. Figs 2-4 present the simulation results with the initial state (-15.15 -4.6 0). Fig. 2 illustrates that the mobile robot approaches the target fastly. The coordinates and direction angle errors gradually decrease over time, and the mobile robot avoids the moving obstacle precisely. Fig. 3 verifies that the state of mobile robot does not viloate the state constraint $h(x)$ in the process of tracking the desired trajectory and avoiding obstacles. Fig. 4 shows the comparison simulation. The DoS attacks are presented in Fig. 5, where $dur(A_t) \leq min(\iota_{CBF}, \iota_{CLF})$.

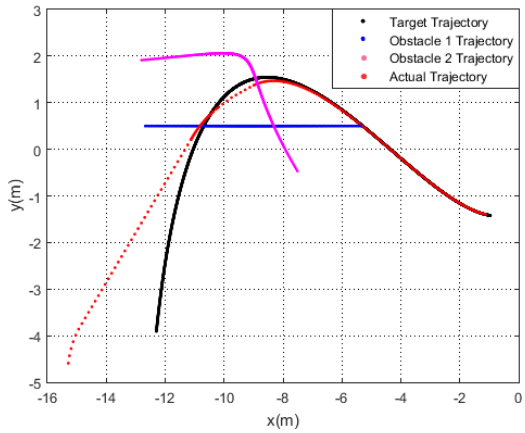

Fig. 2 The evolution of trajectory when avoiding obstacles in straight-line and curve-line movements

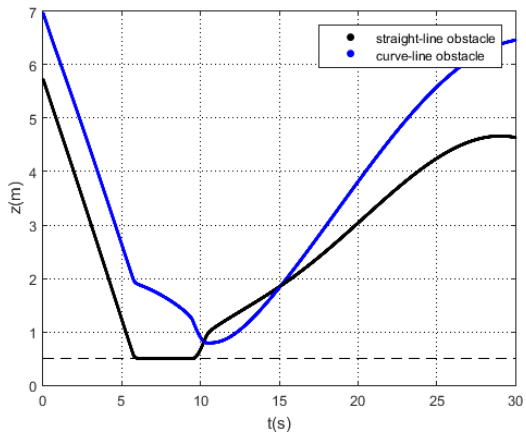

Fig. 3 The evolution of distance between the mobile robot and obstacles

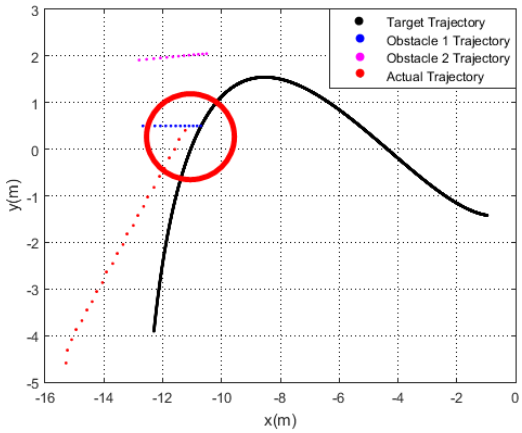

Fig. 4 The evolution of trajectory when avoiding obstacles in straight-line and curve-line movements

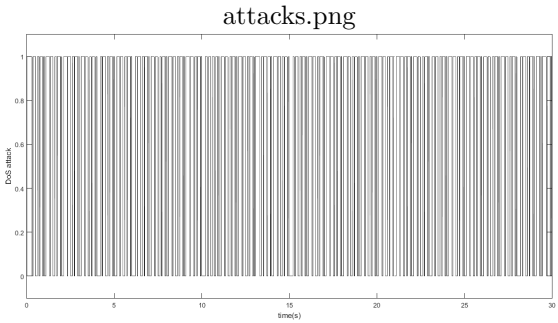

Fig. 5 DoS attacks. 1 represents that there exist no DoS attacks in the communication channel, and 0 represents that there exist DoS attacks in the communication channel.

As we can see from Fig. 2, the mobile robot approaches the target fastly. The coordinates and direction angle errors gradually decrease over time, and the mobile robot avoids the moving obstacles precisely and smoothly. In addition, the density of sampling points on the curve is different in different time periods. At the beginning, the calculated $\min(\iota_{CBF}, \iota_{CLF})$ is a little greater, because the distance between the mobile robot and obstacles is far greater than 0.5 unit at the moment. When the mobile robot approaches the obstacles, the calculated $\min(\iota_{CBF}, \iota_{CLF})$ becomes much shorter to update the control input timely to avoid the violation of state constraints. Finally, when the mobile robot is already tracked precisely, $\min(\iota_{CBF}, \iota_{CLF})$ becomes approximately a constant. Fig. 3 shows the changing distance between the mobile robot and the moving obstacles during the target tracking. It can be easily observed that the distance is

always greater than 0.5 unit, which verifies that obstacle is avoided accurately. On the contrary, as shown in the red circle in Fig. 4, utilizing the conventional approach in [18] fails to satisfy the state constraints, where the sample period is chosen as 5 ms, which leads to the end of iterations and failure of algorithm, and the mobile robot can not continue to move to track target or avoid obstacles. In conclusion, the comparison simulation implies the much better performance of our approach compared to the conventional method in [18].

5 Conclusions

In this paper, we have developed a robust self-triggered control algorithm for nonlinear cyber-physical systems with state constraints under DoS attacks. In this method, we have designed a self-triggered mechanism to decrease network communication loads to the most extent. The sufficient conditions are in place to ensure the algorithm feasibility and closed-loop stability. In the final, the numerical example has been provided to demonstrate the prominent feasibility and advantages of proposed approach.

For our future studies directions, some possible enhancements of the proposed work need to be taken into account.

1) Develop a more resilient approach to handle control input constraint [26] under more complex cyber-physical environment, where cyber threats such as DoS attacks and deception attacks [27] might coexist.

2) Combine the proposed framework with model predictive control [28]-[30] and extend them to large-scale CPSs.

Statements & Declarations

- Funding
  This work was supported by National Natural Science Foundation of China (Nos. 61873028, 61673098), and National Key R&D Program of China (No. 2019YFC0605300).
- Conflict of interest
  The authors have no conflicts of interest to declare that are relevant to the content of this article.
- Author Contributions
  All authors contributed to the study conception and design. The first draft of the manuscript was written by Zhaoyang Cuan and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.
- Data Availability
  The author declares that the data supporting the results of this study are available in the article.

References

[1] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674-1683, Jan. 2018.

[2] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, pp. 210, Feb. 2019.

[3] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Informatics*, vol. 57, no. 7, pp. 2527-2535, Jul. 2010.

[4] M. S. Mahmoud, M. M. Hamdan and U. A. Baroudi, "Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101-115, Apr. 2019.

[5] H. Chen and F. Allgöwer, "A quasi-infinite horizon nonlinear model predictive control scheme with guaranteed stability," *Automatica*, vol. 34, no. 10, pp. 1205-1217, 1998.

[6] S. Asif and P. Webb, "Networked control system- An overview," *International Journal of Computer Applications*, vol. 115, no. 6, pp. 26-30, 2015.

[7] G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory and Technology*, vol. 14, no. 1, pp. 2-10, Feb. 2016.

[8] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proc. IEEE. Conf. Decis. Control, 2012*, pp. 3270-3285.

[9] X. Yang, H. He, and D. Liu, "Event-triggered optimal neuro-controller design with reinforcement learning for unknown nonlinear systems," *IEEE Transactions on Systems Man Cybernetics-Systems*, vol. 49, no. 9, pp. 1866-1878, Sep. 2019.

[10] A. Girard, "Dynamical triggering mechanisms for event-triggered control," *IEEE Transactions on Automatic Control*, vol. 60, no. 7, pp. 1992-1997, Jul. 2015.

[11] M. Mazo, Jr. A. Anta and P. Tabuada, "An ISS self-triggered implementation of linear controllers," *Automatica*, vol. 46, no. 8, pp. 1310-1314, 2010.

[12] X. Wang and M. D. Lemmon, "Self-triggered feedback control systems with finite-gain L_2 stability," *IEEE Transactions on Automatic Control*, vol. 54, no. 3, pp. 452-467, Mar. 2009.

[13] A. Anta and P. Tabuada, "To sample or not to sample: Self-triggered control for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2030-2042, sep. 2010.

[14] W. P. M. H. Heemels, M. C. F. Donkers, and A. R. Teel, "Periodic event-triggered control for linear systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 847-861, Apr. 2013.

[15] H. Li, W. Yan, Y. Shi, and Y. Wang, "Periodic event-triggering in distributed receding horizon control of nonlinear systems," *Systems & Control Letters*, vol. 86, pp. 16-23, Dec. 2015.

[16] E. D. Sontag, "Smooth stabilization implies coprime factorization," *IEEE Transactions on Automatic Control*, vol. 34 , no. 4, pp. 435-443, Apr. 1989.

[17] A. D. Ames, K. Galloway, J. W. Grizzle, and K. Sreenath, "Rapidly exponentially stabilizing control Lyapunov functions and hybrid zero dynamics," *IEEE Transactions on Automatic Control*, vol. 59, no. 4, pp. 876-891, Apr. 2014.

[18] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *Proc. of the 53rd IEEE Conference on Decision and Control*, Los Angeles, CA, USA, Dec. 2014, pp. 6271-6278.

[19] X. Xu, J. W. Grizzle, P. Tabuada, and A. D. Ames, "Correctness guarantees for the composition of lane keeping and adaptive cruise control," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 3, pp. 1216-1229, Jul. 2018.

[20] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada,"Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861-3876, Aug. 2017.

[21] F. Blanchini and S. Miani, Set-theoretic methods in control. Birkhauser, 2008.

[22] B. Wang, X. Yu and X. Li, "ZOH Discretization Effect on Higher-Order Sliding-Mode Control Systems," *IEEE Transactions on Industrial Electronic*, vol. 55, no. 11, pp. 194-220, Set. 2008.

[23] R. P. Brent, "Algorithms for minimization without derivatives". *Courier Corporation*, 2013.

[24] D. P. Bertsekas, "Nonlinear programming." *Athena scientific Belmont*, 1999.

[25] H. K. Khalil. *Nonlinear Systems*, third edition. Englewood Cliffs, NJ: Prentice Hall, 2002.

[26] C. Mu, K. Liao and K. Wang, "Event-triggered design for discrete-time nonlinear systems with control constraints," vol. 103, pp. 2645-2657, Feb. 2021.

[27] F. Yang, Z. Gu and S. Yan, "Swithched event_based control for nonlinear cyber-physical systems under deception attacks," *Nonlinear Dynamics*, vol. 106, pp. 2245-2257, Oct. 2021.

[28] Q. Sun, K. Zhang, and Y. Shi, "Resilient Model Predictive Control of Cyber-Physical Systems Under DoS Attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4920-4927, Jul. 2020.

[29] D. Cui and H. Li, "Dual Self-Triggered Model-Predictive Control for Nonlinear Cyber-Physical Systems," *IEEE Transactions on Systems Man Cybernetics-Systems*, to be published, doi: 10.1109/TSMC.2021.3070229.

[30] H. Li and Y. Shi, "Robust Distributed Model Predictive Control of Constrained

Continuous-Time Nonlinear Systems: A Robustness Constraint Approach," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1673-1678, Jun. 2014.