Received: 31 August 2018 | Revised: 27 February 2019 | Accepted: 9 June 2019

DOI: 10.1002/rnc.4654

RESEARCH ARTICLE

Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks

Yuan-Cheng Sun[1] | **Guang-Hong Yang**[1,2]

[1]College of Information Science and Engineering, Northeastern University, Shenyang, China

[2]State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, China

Correspondence
Guang-Hong Yang, College of Information Science and Engineering, Northeastern University, Shenyang 110819, China; or State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang 110819, China.
Email: yangguanghong@ise.neu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Number: 61621004 and 61420106016; Research Fund of State Key Laboratory of Synthetical Automation for Process Industries, Grant/Award Number: 2018ZCX03

Summary

This paper investigates the resilient control problem for constrained continuous-time cyber-physical systems subject to bounded disturbances and denial-of-service (DoS) attacks. A sampled-data robust model predictive control law with a packet-based transmission scheduling is taken advantage to compensate for the loss of the control data during the intermittent DoS intervals, and an event-triggered control strategy is designed to save communication and computation resources. The robust constraint satisfaction and the stability of the closed-loop system under DoS attacks are proved. In contrast to the existing studies that guarantee the system under DoS attacks is input-to-state stable, the predicted input error caused by the system constraints can be dealt with by the input-to-state practical stability framework. Finally, a simulation example is performed to verify the feasibility and efficiency of the proposed strategy.

KEYWORDS

cyber-physical systems, denial-of-service attacks, event-triggered control, model predictive control

1 | INTRODUCTION

Cyber-physical systems (CPSs) where sampled signals and control inputs are generally transmitted via shared communication networks connect the cyber layer to the physical plant flexibly. Since the networks are vulnerable to cyber attacks,[1] the analysis and control of critical infrastructures have witnessed increasing research interests, such as power-grid, autonomous vehicles, and water distribution systems.[2-4] The research areas on security of CPSs in the literature involve attack detection and identification,[5] optimal attack scheduling,[6] remote state estimation,[7,8] resilient control under attacks,[9] and so on.

There are kinds of cyber attacks, including false injection attacks, replay attacks, and denial-of-service (DoS) attacks. Among them, the goal of DoS attacks is to jam the network communication channels between system devices and components. Extensive attention to the security research of the CPSs under DoS attacks has been attracted, including optimal DoS attack scheduling[10] and resilient control under DoS attacks.[11,12] In the work of De Persis and Tesi,[13] the DoS model, which is characterized by frequency and duration, is proposed, and the closed-loop system is proved to be input-to-state stable. Based on the general DoS model, several studies have been presented for linear systems,[14,15] nonlinear systems,[16] CPSs with multiple transmission channels,[17] and CPSs with event-triggered control strategy.[18,19] However, the resilient control methods of the aforementioned works mainly focus on the transmission times scheduling and input-to-state stability (ISS) framework. There have been few theoretical studies appeared on control methodology to guarantee the control performance under DoS attacks, especially when the state and input of the physical plant are subject to hard constraints.

Model predictive control (MPC) is a control method that the control input at each sampling instant is defined as the first part of the solution of a finite-horizon optimal control problem.[20] The MPC is widely utilized in industrial control systems and extensive literature exists. For instance, Mayne et al[21] concerned the problem of robust MPC for constrained linear discrete-time systems with bounded disturbances. The "tube-based" approach for discrete-time MPC algorithms is extended in the work of Farina and Scattolini[22] for the continuous-time case. In the work of He et al,[23] a self-triggered MPC algorithm is developed based on first-order hold for continuous-time systems. In the work of Liu et al,[24] a robust self-triggered min-max MPC algorithm is developed for nonlinear systems. To achieve a more appropriate trade-off between control performance and communication utilization, event-triggered control[25] for networked control systems has been widely investigated. The design of event-triggered MPC strategies is of great importance since it enables the reduction in frequencies of solving optimization problems and saves computation resources.[26] In the work of Brunner et al,[27] a robust event-triggered MPC method is proposed for constrained discrete-time systems subject to bounded stochastic disturbances.

When the DoS attacks are present, if the optimal control values are still available, the control performance is still guaranteed. Inspired by the predictor-based control framework,[15,18,19] a robust MPC strategy for linear CPSs with disturbances under DoS attacks is investigated in this paper. The physical plant considered in this paper is a constrained continuous-time system, and the robust sampled-data MPC strategy is designed to calculate the optimal control sequences. In order to save the communication and computation resources of the system, an event-triggered strategy is designed to determine the time instants at which to solve the optimal problem and transmit the control data packets to the buffered actuator. It is worth noting that the existing results of event-triggered MPC cannot handle the system under DoS attacks since the constraints and the robustly asymptotically stability to a set may not be satisfied. Motivated by these facts, new conditions are presented to prove the feasibility under DoS attacks. To establish the time characteristics of the tolerable attack intensity, the input-to-state practical stability (ISpS) framework is used to prove the stability under DoS attacks.

The main results and contributions are summarized as follows. First, a robust MPC algorithm is designed to achieve resilient control for generic constrained continuous-time CPSs with bounded disturbances under DoS attacks, and the MPC algorithm is proved to be recursively feasible with some conditions by taking advantage of the worst case of all possible uncertainty realizations caused by the DoS attacks. Second, compared to the existing results, which ensure ISS under DoS attacks, the stability of the closed-loop system with the predicted input error caused by the system constraints is guaranteed by the ISpS framework, and an even better control performance is achieved. Furthermore, a link between the prediction horizon and the tolerable attack intensity that can guarantee the stability is obtained. Third, the sampled-data MPC is used to continuous-time CPSs based on the event-triggered strategy, inspired by lemma 1 in the work of De Persis and Tesi,[13] the relationship between the sampling period and the event-triggering condition (ETC) is obtained.

The remainder of this paper is organized as follows. Section 2 presents the preliminaries and problem formulation. The event-triggered MPC algorithm under DoS attacks is designed in Section 3. In Section 4, the main results are proposed, including robust constraint satisfaction and the stability proof. Then, Section 5 gives the simulation, and Section 6 concludes this paper.

Notation. Denote the set of reals by $\mathbb{R}$, $\mathbb{R}^n$ is the n-dimensional Euclidean space. Given $\alpha, \beta \in \mathbb{R}$, $\mathbb{R}_{\geq\alpha}$ is the set of reals greater than or equal to α and $\mathbb{R}_{[\alpha,\beta]}$ is the set $\{a \in \mathbb{R} | \alpha \leq a \leq \beta\}$. Let $\mathbb{N}$ be the nonnegative integers set. For a vector $x \in \mathbb{R}^n$, $\|x\|$ is the Euclidean norm. For a matrix A, A^T, $\|A\|$, and μ_A denote the transpose, spectral norm, and logarithmic norm,[28] respectively, where $\mu_A = \max\{\lambda | \lambda \in \text{spectrum}\{\frac{A+A^T}{2}\}\}$. Given two sets S_1 and S_2, a scalar α and matrices $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{n\times m}$, let $S_2 \setminus S_1$ be the relative complement of S_1 in S_2, $\alpha S_1 = \{\alpha x | x \in S_1\}$, $AS_1 = \{Ax | x \in S_1\}$, and $B^{-1}S_1 = \{x \in \mathbb{R}^n | Bx \in S_1\}$. Define that the Minkowski set addition is $S_1 \oplus S_2 = \{x + y | x \in S_1, y \in S_2\}$ and the Pontryagin set difference is $S_1 \ominus S_2 = \{z \in \mathbb{R}^n | z \oplus S_2 \subseteq S_1\}$. For a sequence of sets S_i, $i \in \mathbb{N}_{[a,b]}$ with $a, b \in \mathbb{N}$, define $\oplus_{i=a}^{b} S_i = S_a \oplus S_{a+1} \oplus \cdots \oplus S_b$. For an interval $T = [t_1, t_2)$, the length is denoted by $|T(t_1, t_2)| = t_2 - t_1$. For a measurable function $f(t)$ with interval $[0, t)$, the $\mathcal{L}_\infty$ norm of $f(\cdot)$ on $[0, t)$ is given as $\|f_t\|_\infty = \text{ess}\ \sup_{s\in[0,t)} \|\mathrm{f(s)}\|$. $\lfloor\cdot\rfloor$ is defined as the floor integral function.

2 | PRELIMINARIES AND PROBLEM FORMULATION

2.1 | Process dynamics and network

The concerned CPS process is shown in Figure 1, the plant and the sensor are integrated with the actuator and they are distributed with the controller. The controller is remotely connected to the actuator via a resource-limited wireless

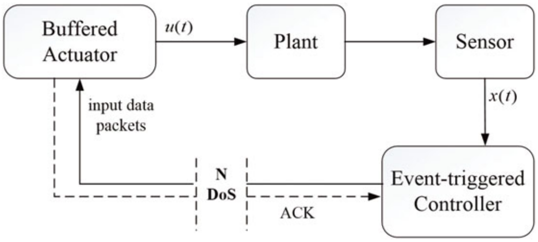

FIGURE 1 Control structure of the cyber-physical system under denial-of-service (DoS) attacks. ACK, acknowledge [Colour figure can be viewed at wileyonlinelibrary.com]

network, and the network is vulnerable to DoS attacks by malicious adversaries leading to the open-loop of the system. Consider the CPS described in the following continuous-time linear form

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

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^m$ are system state and input, respectively. The disturbance $w(t)$ is time-varying, unknown bounded, and satisfies $w(t) \in \mathcal{W} \subseteq \mathbb{R}^n$, $t \in \mathbb{R}_{\geq 0}$. Furthermore, hard constraints on the state and input are given as $x(t) \in \mathcal{X}$, $u(t) \in \mathcal{U}$, where $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{U} \subseteq \mathbb{R}^m$, and $\mathcal{W}$ are compact convex sets containing the origin. Assume that the controller can obtain the state $x(t)$ as a measurement at any time instant $t \in \mathbb{R}_{\geq 0}$.[27] The matrix pair (A, B) is assumed to be stabilizable.

To increase the reliability of the communication, a packet-based control strategy is designed. Each data packet contains a sequence of control values that comes from a sampled-data controller. Denote by $\{t_k\}_{k\in\mathbb{N}}$ the sequence of the transmission attempts of the networked communication, and define Δ_k as the interval between any two consecutive data packets transmission attempts, which satisfies

$$\delta \leq t_{k+1} - t_k = \Delta_k \leq \bar{\Delta}, \tag{2}$$

where δ is the sampling period of the controller computation platform, and $\bar{\Delta} \in \mathbb{R}$ is the upper bound of the intervals. When the discrete control values are transmitted to the buffered actuator, the actuator implements a sample-and-hold policy to obtain the continuous control input $u(t)$.

2.2 | DoS attacks

Due to the energy constraint, or several provisions such as spreading and high-pass filtering techniques to restrict DoS attacks, the attack signals generally occur in a random and intermittent mode. Here, a general DoS model is considered, which the attack behavior is characterized as time by posing restrictions on the frequency and duration merely. Denote by $\{h_n\}_{n\in\mathbb{N}}$ with $h_0 \geq 0$ the sequence of DoS off/on transitions, which are the time instants when DoS attacks transform from null (transmission attempts are all successful) to one (transmission attempts fail).[14] The nth DoS interval is defined as $H_n = \{h_n\} \cup [h_n, h_n + \tau_n)$, where $\tau_n \in \mathbb{R}_{\geq 0}$ is its length. If $\tau_n = 0$, H_n degenerates into a pulse. Assume that there is no overlap in $\{H_n\}_{n\in\mathbb{N}}$. Given any interval $[t_1, t_2)$, $0 \leq t_1 < t_2$, let

$$\mathcal{D}(t_1, t_2) = \bigcup_{n\in\mathbb{N}} H_n \cap [t_1, t_2) \tag{3a}$$

$$\mathcal{H}(t_1, t_2) = [t_1, t_2) \setminus \mathcal{D}(t_1, t_2) \tag{3b}$$

be the subsets of $[t_1, t_2)$, where the network channel is in DoS and healthy status, respectively. Denote by $n(t_1, t_2)$ the number of DoS off/on transitions over $[t_1, t_2)$. Referring to the work of De Persis and Tesi,[13] the following assumptions are proposed to model the frequency and duration of DoS attacks.

Assumption 1 (See the work of De Persis and Tesi[13]). For any $0 \leq t_1 < t_2$, there exist $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{\geq 0}$ such that

$$n(t_1, t_2) \leq \eta + \frac{t_2 - t_1}{\tau_D}. \tag{4}$$

Assumption 2 (See the work of De Persis and Tesi[13]). For any $0 \leq t_1 < t_2$, there exist $\varsigma \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ such that

$$|\mathcal{D}(t_1, t_2)| \leq \varsigma + \frac{t_2 - t_1}{T}. \tag{5}$$

Remark 1. It is necessary for guaranteeing the controllability of the system (1) to propose Assumptions 1 and 2 as in the work of De Persis and Tesi.[13] Suppose that $\tau_D \to 0$ or $T = 1$, each transmission attempt can be jammed by the adversary, which is equivalent to the case where the system is in open-loop status all the time. Furthermore, this general DoS model can also constrain random losses of the networks. For the continuous-time, the length of a random loss is zero, but the sum of the number of malicious attacks and random losses is constrained by (4). Besides, it is impossible to know whether the data losses are due to malicious attacks or random packet losses for the defender. It means that, no matter whether the data losses are due to malicious attacks or random losses, the total data loss actions satisfy Assumptions 1 and 2.

2.3 | Event-triggered strategy

The event-triggered control strategy is defined as follows:

$$u(t) = \mu(x(t_k), t - t_k),\ t \in \mathbb{R}_{[t_k, t_{k+1})}, \tag{6}$$

where $k \in \mathbb{N}$ represents the sequence of the input data transmission attempts when the event triggered, and $t_0 = 0$. Furthermore, it is assumed that there is no network-induced delay.

The event-triggered transmission logic is designed based on the discrete time sequence of the controller computation platform. Consider the following transmission logic.

i. Transmission mode under normal status. If t_k does not belong to a DoS interval, then

$$t_{k+1} = \inf\{t \in \mathbb{R}_{\geq t_k+\delta} | x(t) \notin \mathcal{E}(x(t_k), t - t_k) \vee t - t_k \geq \bar{\Delta}\}, \tag{7}$$

where $x(t) \notin \mathcal{E}(x(t_k), t - t_k)$ is the ETC, $t \in \mathbb{R}_{[t_k, t_{k+1})}$, $k \in \mathbb{N}$.

ii. Transmission mode under DoS status. If t_k belongs to some DoS interval, then $t_{k+1} = t_k + \delta$, where δ is the sampling interval of the sampled-data control unit.

That is, when the DoS attacks are absent, the control data is updated only at the event instants t_k based on the current state $x(t_k)$ as in (7). The data packet, which contains the whole sequence $\{u(t_k), \dots, u(t_k + (N-1)\delta)\}$ transmitted to the actuator at t_k, is able to improve the system performance of the open loop intervals, $N \in \mathbb{N}_{\geq 1}$ is the prediction horizon (buffer size). The control values still stored in the buffered actuator will be discarded when the next data packet arrives at t_{k+1}. On the other side, when the DoS attacks are present, the transmission attempt at t_k fails, the controller cannot receive an acknowledge (ACK) signal from the actuator to confirm that the transmission at t_k was successful or not. Then, the next transmission attempt occurs at $t_{k+1} = t_k + \delta$ until the controller receives the ACK signal. In this mode, the actuator will use the data stored in the buffer until it is empty, and the actuator holds the last control value.

2.4 | Control objective

In this paper, the control objectives to be achieved will be centered around the following definition.

Definition 1 (See the work of Lazar et al[29]). System (1) is said to be input-to-state practical stable if there exist a $\mathcal{KL}$-function f_1, a $\mathcal{K}$-function f_2, and a number d such that

$$\|x(t)\| \leq f_1(\|x(0)\|, t) + f_2(\|v\|) + d \tag{8}$$

holds for all $t \in \mathbb{R}_{\geq 0}$, $x(0) \in \mathcal{X}$. If (8) holds for $d \equiv 0$, then system (1) is said to be input-to-state stable (ISS) in $\mathcal{X}$. Furthermore, if (8) holds for $v \equiv 0$ and $d \equiv 0$, then system (1) is globally asymptotically stable (GAS) in $\mathcal{X}$.

The objective is to design the control strategy $\mu : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^m$ and the set-valued function $\mathcal{E} : \mathbb{R}^n \times \mathbb{N} \to 2^{\mathbb{R}^n}$ for the closed-loop system (1) and (6) under the DoS attacks modeled as Assumptions 1 and 2 such that:

i. the constraints $x(t) \in \mathcal{X}$ and $u(t) \in \mathcal{U}$ are robustly satisfied;
ii. the closed-loop system is ISpS;
iii. the tolerable DoS attacks are as long as possible with a suitable chosen buffer size N.

Several properties of the Minkowski set addition and the Pontryagin set difference are summarized as the following lemma to be used in this paper.

Lemma 1 (See the work of Brunner et al[27]). *Let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ be compact convex sets, and $A \in \mathbb{R}^{m\times n}$. Then, $\mathcal{X} \oplus \mathcal{Y} = \mathcal{Y} \oplus \mathcal{X}$, $\mathcal{X} \ominus (\mathcal{Y} \oplus \mathcal{Z}) = (\mathcal{X} \ominus \mathcal{Y}) \ominus \mathcal{Z}$, $(\mathcal{X} \oplus \mathcal{Y}) \ominus \mathcal{Y} = \mathcal{X}$, $(\mathcal{X} \ominus \mathcal{Y}) \oplus \mathcal{Y} \subseteq \mathcal{X}$, $A(\mathcal{X} \oplus \mathcal{Y}) = A\mathcal{X} \oplus A\mathcal{Y}$, and $(\mathcal{X} \cap \mathcal{Y}) \oplus \mathcal{Z} \subseteq (\mathcal{X} \oplus \mathcal{Z}) \cap (\mathcal{Y} \oplus \mathcal{Z})$.*

3 | EVENT-TRIGGERED MPC UNDER DOS ATTACKS

In this section, an event-triggered robust MPC algorithm is presented to solve the problem proposed in Section 2. That is, function μ and $\mathcal{E}$ are obtained by the solution of an optimal control problem in finite horizon, which is achieved online at the event instants t_k, $k \in \mathbb{N}$

The decision variable of the optimization problem at t_k is

$$\mathrm{d} = ((x_{0|t_k}, \ \dots \ , x_{N|t_k}), (u_{0|t_k}, \ \dots \ , u_{N-1|t_k})) \in \mathbb{D}_N, \tag{9}$$

where $\mathbb{D}_N = \mathbb{R}^n \times \cdots \times \mathbb{R}^n \times \mathbb{R}^m \times \cdots \times \mathbb{R}^m$ and $N \in \mathbb{N}_{\geq 1}$ is the prediction horizon. Let $A_\delta = e^{A\delta}$ and $B_\delta = \int_0^\delta e^{A\tau} B d\tau$, the following constraints are imposed on d:

$$x_{0|t_k} = x(t_k) \tag{10a}$$

$$\forall i \in \mathbb{N}_{[0,N-1]}, \ x_{i+1|t_k} = A_\delta x_{i|t_k} + B_\delta u_{i|t_k} \tag{10b}$$

$$\forall i \in \mathbb{N}_{[0,N-1]}, \ x_{i|t_k} \in \mathcal{X}_i \tag{10c}$$

$$\forall i \in \mathbb{N}_{[0,N-1]}, \ u_{i|t_k} \in \mathcal{U}_i \tag{10d}$$

$$x_{N|t_k} \in \mathcal{X}_f, \tag{10e}$$

where variables $x_{i|t_k}$ are defined as a predicted state trajectory for the nominal system generated by the predicted inputs $u_{i|t_k}$ according to (10b). The sets $\mathcal{X}_i$ and $\mathcal{U}_i$ depending on the step i in the prediction horizon are tightened constraint sets with $i \in \mathbb{N}_{[0,N-1]}$, which can be defined as

$$\mathcal{X}_i = \mathcal{X} \ominus \mathcal{F}_i, \ i \in \mathbb{N}_{[0,N-1]} \tag{11a}$$

$$\mathcal{U}_i = \mathcal{U} \ominus K\mathcal{F}_i, \ i \in \mathbb{N}_{[0,N-1]}, \tag{11b}$$

where the sets $\mathcal{F}_i \subseteq \mathbb{R}^n$ are the uncertainty sets to describe a tube containing all possible error around the nominal state given by $x_{i|t_k}$. The set $\mathcal{X}_f$ is a compact and convex set representing the terminal set. $\mathcal{F}_i$ and $\mathcal{X}_f$ will be given later. Given $x(t_k) \in \mathbb{R}^n$, the set contains all the feasible decision variables that is defined as

$$\mathcal{D}_N(x(t_k)) = \{\mathrm{d} \in \mathbb{D}_N | (10\mathrm{a}) \ \mathit{to} \ (10\mathrm{e})\}. \tag{12}$$

An auxiliary feedback law is used to design the control strategy, which is assumed to be the desired feedback with the gain matrix $K \in \mathbb{R}^{m\times n}$ for the plant if the system constraints are ignored. K is selected to make the matrix $A_\delta + B_\delta K$ Schur stable. Based on the difference between the predicted input $u_{i|t_k}$ and the expected feedback using the predicted state, the cost function of the optimal control problem is given as follows:

$$J_N(\mathrm{d}) = \sum_{i=0}^{N-1} l(u_{i|t_k} - Kx_{i|t_k}), \tag{13}$$

where $l : \mathbb{R}^m \to \mathbb{R}_{\geq 0}$ is a stage cost function to be defined as $l(v) = v^T L v$, where v is the error between the predicted input and the desired feedback input of the predicted state, that is, $v_i = u_{i|t} - Kx_{i|t}$ for $i \in \mathbb{N}_{[0,N]}$ with $v_0 = 0$, L is a positive definite symmetric matrix. The finite horizon optimal control problem can be defined as

$$J_N^0(x(t_k)) = \min_{\mathrm{d} \in \mathcal{D}_N(x(t_k))} J_N(\mathrm{d}) \tag{14}$$

$$\mathrm{d}^*(x(t_k)) = \arg \min_{\mathrm{d} \in \mathcal{D}_N(x(t_k))} J_N(\mathrm{d}), \tag{15}$$

where $\mathrm{d}^*(x(t_k))$ is the optimization decision variable at time t_k. The set containing all the feasible state for the optimization problem is defined by $\hat{\mathcal{X}}_N = \{x \in \mathbb{R}^n | \mathcal{D}_N(x) \neq \emptyset\}$. Given any optimization decision variable $\mathrm{d}^*(x_{t_k}) = ((x^*_{0|t_k}, \dots, x^*_{N|t_k}), (u^*_{0|t_k}, \dots, u^*_{N-1|t_k}))$, the ETC is given as

$$\mathcal{E}(x(t_k), t - t_k) = x^*_{t-t_k|t_k} \oplus \mathcal{T}_{t-t_j}, \tag{16}$$

where $\mathcal{T}_i \subseteq \mathbb{R}^n,\ i \in \mathbb{N}_{[1,N]}$ are given closed sets that describe the difference between the actual system trajectory and the predicted one of the normal system. Define $\mathcal{T}_N = \emptyset$ such that an event is triggered within the transmission interval bound and $\mathcal{T}_0 = \{0\}$.

Consider the mode where the DoS attacks are present. Denote by $\{z_r\}_{r\in\mathbb{N}}$ the sequence of time instants at which the control unit successfully transmits a packet containing N predicted control values. That is, if $t_k \in \mathcal{H}(t_1, t_2)$, $z_r = t_k$; if $t_k \in \mathcal{D}(t_1, t_2)$, $z_r = \inf\{t \in \mathbb{R}_{\geq t_k+\delta} | t \in \mathcal{H}(t_1, t_2)\}$. The length of the interval $[z_r, z_{r+1})$ is an integer multiple of δ since the event condition is verified with the period δ. Then, the control input of the system under DoS attacks is given by

$$\mu(x(z_r), t - z_r) = \begin{cases} 0, & t \in \mathbb{R}_{[0,z_0]} \\ u^*_{\lfloor (t-z_r)/\delta \rfloor | z_r}, & t \in \mathbb{R}_{[z_r, z_r+(N-1)\delta)} \\ u^*_{N-1|z_r}, & t \in \mathbb{R}_{[z_r+(N-1)\delta, z_{r+1})}. \end{cases} \tag{17}$$

Lemma 2. *If the DoS attacks considered satisfy Assumptions 1 and 2, and $1/T + \delta/\tau_D < 1$ holds, then the sequence $\{z_r\}_{r\in\mathbb{N}}$ satisfies $z_0 \leq Q$ and $z_{r+1} - z_r \leq Q + \bar{\Delta}$, where*

$$Q = (\varsigma + \eta\delta)\left(1 - \frac{1}{T} - \frac{\delta}{\tau_D}\right)^{-1}. \tag{18}$$

Remark 2. Similar lemmas have been proved in the works of Feng and Tesi.[14,15] The difference of the lemma in this paper is the consideration of the event triggering intervals. The upper bound of the event intervals is $\bar{\Delta}$ with $\bar{\Delta} \leq N\delta$. Take account of the worst case, where a DoS attack occurs at the instant when the event triggered after an interval with length $\bar{\Delta}$, then $z_{r+1} - z_r \leq Q + \bar{\Delta}$ is obtained. The uniform boundedness of the time elapsing between two successful transmissions is guaranteed by the lemma.

Then, the sets $\mathcal{F}_i, i \in \mathbb{N}$ that contain the uncertainty of the prediction are given as

$$\mathcal{F}_i = \begin{cases} \bigoplus\limits_{j=0}^{i-1} (A_\delta + B_\delta K)^j \mathcal{W}, & i \in \mathbb{N}_{[0,N]} \\ A_\delta^{i-N}\left(\bigoplus\limits_{j=0}^{N-1} (A_\delta + B_\delta K)^j \mathcal{W}\right) & \\ \oplus \bigoplus\limits_{j=0}^{i-N-1} A_\delta^j \mathcal{W}, & i \in \mathbb{N}_{[N+1,M]}, \end{cases} \tag{19}$$

where $M = \lfloor (Q + \bar{\Delta})/\delta \rfloor$.

The following assumption should be satisfied for the event threshold sets $\mathcal{T}_i$ and the uncertainty sets $\mathcal{F}_i$ for $i \in \mathbb{N}_{[0,N]}$.

Assumption 3 (See the work of Brunner et al[27]). There exist sets $\mathcal{R}_i$ defied as $\mathcal{R}_{i+1} = A_\delta(\mathcal{R}_i \cap \mathcal{T}_i) \oplus \mathcal{W}$ with $\mathcal{R}_0 = \{0\}$ for $i \in \mathbb{N}_{[0,N]}$ such that $\mathcal{R}_i \subseteq \mathcal{F}_i$ holds.

Remark 3. This assumption is proposed and discussed in the work of Brunner et al,[27] which requires that the tolerable error sets are included in the uncertainty sets $\mathcal{F}_i$ at the event intervals. The suitable event threshold sets $\mathcal{T}_i$ should be designed to satisfy this assumption, and the detailed design will be given in Section 4.2.

The terminal constraint (10e) is formulated to guarantee the recursive feasibility of the system constraints as in (10c)-(10d) as the following scenario. If an input sequence at z_r satisfying the constraints in (10c)-(10d) is applied to system (1) for an interval $\bar{\Delta}$, then the worst DoS attack begins. At the end of the DoS interval, the existence of a control sequence that satisfies the constraints as (10c)-(10d) is still guaranteed. To ensure this feature, the terminal set $\mathcal{X}_f$ is required to ensure the following assumption hold referring to the relevant assumptions in the works of Brunner et al.[20,27]

Assumption 4. For all $i \in \mathbb{N}_{[0,M-N]}$, the terminal set $\mathcal{X}_f$ satisfies

$$A_\delta^i \mathcal{X}_f \oplus \mathcal{F}_{N+i} \subseteq \mathcal{X} \tag{20a}$$

$$KA_\delta^i \mathcal{X}_f \oplus K\mathcal{F}_{N+i} \subseteq \mathcal{U} \tag{20b}$$

$$(A_\delta + B_\delta K)\mathcal{X}_f \oplus (A_\delta + B_\delta K)^N \mathcal{W} \subseteq \mathcal{X}_f \tag{20c}$$

$$A_\delta \mathcal{X}_f \oplus A_\delta^N \mathcal{W} \subseteq \mathcal{X}_f. \tag{20d}$$

Remark 4. Similar assumptions are proposed in the works of Brunner et al.[20,27] Notice that, if there is no DoS attack, a properly selected upper bound of the event intervals $\bar{\Delta}$ has no effect to the system. However, $\bar{\Delta}$ should be defined as $\bar{\Delta} \le N\delta$ when the DoS attacks occurred to make the system aware of the attacks as early as possible. If $z_{r+1} - z_r \le N\delta$, the prediction horizon involves the open-loop interval, then the assumption is satisfied from (11) and (19). On the other hand, if $z_{r+1} - z_r > N\delta$, the assumption is more conservative than those in the aforementioned work.[20,27] It is a trade-off that this assumption increases the conservatism of the set constraints in exchange for the robustness against DoS attacks.

4 | MAIN RESULTS

In this section, the main results of this paper are proposed, that is, recursive feasibility of the optimal problem (14) with robust constraint satisfaction and the ISpS of the closed-loop system.

4.1 | Feasibility result

Theorem 1. *Let any* $z_r \in \mathbb{R}_{\ge 0}$ *with* $r \in \mathbb{N}$, $x(z_r) \in \mathbb{R}^n$ *and any decision variable* $\mathrm{d} = ((x_{0|z_r}, \dots, x_{N|z_r}), (u_{0|z_r}, \dots, u_{N-1|z_r})) \in \mathbb{D}_N$ *be given. For the system (1) with the input (17), there exists a* $\mathrm{d}_N \in \mathcal{D}_N(x(z_{r+1}))$. *Furthermore, for all* $x(0) \in \hat{\mathcal{X}}_N$ *and any disturbances* $w(t) \in \mathcal{W}$, $x(t) \in \mathcal{X}$ *and* $u(t) \in \mathcal{U}$ *for all* $t \in \mathbb{N}_{[z_r, z_{r+1})}$ *hold when Assumptions 3 and 4 are satisfied.*

Proof. Denote by

$$z_r + s\delta = \min\{z_r + j\delta \in \mathbb{R}_{\ge z_r+\delta} | x(z_r + j\delta) \notin x_{j|z_r} \oplus \mathcal{T}_j\} \tag{21}$$

the first transmission attempt instant during a DoS interval, where $s, j \in \mathbb{N}_{[1,N]}$, it holds that $x(z_r + s\delta) - x_{s|z_r} \in \mathcal{T}_s$. According to Assumption 3, it can be obtained that

$$x(z_r + s\delta) - x_{s|z_r} \in \mathcal{R}_s \subseteq \mathcal{F}_s, \tag{22}$$

for $s \in \mathbb{N}_{[1,N]}$. For the time step $z_r + s\delta$, the transmission attempt fails because of the DoS attack occurred during $(z_r, z_r + s\delta]$. Then, the transmission mode is under DoS status, the optimal problem is calculated at each sampling step. For $\tilde{s} \in \mathbb{N}_{[s,N]}$, consider the decision variable $\tilde{\mathrm{d}} = ((x_{0|z_r+\tilde{s}}, \dots, x_{N|z_r+\tilde{s}}), (u_{0|z_r+\tilde{s}}, \dots, u_{N-1|z_r+\tilde{s}}))$, where

$$\begin{aligned} x_{i|z_r+\tilde{s}} &= (A_\delta + B_\delta K)^i (x(z_r + \tilde{s}\delta) - x_{\tilde{s}|z_r}) + x_{\tilde{s}+i|z_r}, && i \in \mathbb{N}_{[0,N]} \\ x_{\tilde{s}+i|z_r} &= (A_\delta + B_\delta K)^{\tilde{s}+i-N} x_{N|z_r}, && i \in \mathbb{N}_{[N-\tilde{s}+1,N]} \end{aligned} \tag{23}$$

$$\begin{aligned} u_{i|z_r+\tilde{s}} &= K(A_\delta + B_\delta K)^i (x(z_r + \tilde{s}\delta) - x_{\tilde{s}|z_r}) + u_{\tilde{s}+i|z_r}, && i \in \mathbb{N}_{[0,N-1]} \\ u_{\tilde{s}+i|z_r} &= K(A_\delta + B_\delta K)^{\tilde{s}+i-N} x_{N|z_r}, && i \in \mathbb{N}_{[N-\tilde{s},N-1]}. \end{aligned} \tag{24}$$

For $\tilde{s} \in \mathbb{N}_{[s,N]}$, the buffered control values obtained at z_r are still available for the system. By induction, it can be obtained from (23) and (24) that

$$\begin{aligned} x(z_r + (\tilde{s} + i)\delta) - x_{i|z_r+\tilde{s}} &= (A_\delta + B_\delta K)^i (x(z_r + \tilde{s}\delta) - x_{\tilde{s}|z_r}) \\ &\quad + \sum_{j=0}^{i-1} (A_\delta + B_\delta K)^j E_\delta w(z_r + (\tilde{s} + i - j - 1)\delta) \\ &\in (A_\delta + B_\delta K)^i \mathcal{F}_{\tilde{s}} \oplus \sum_{j=0}^{i-1} (A_\delta + B_\delta K)^j \mathcal{W} \\ &= \mathcal{F}_{\tilde{s}+i}, \end{aligned} \tag{25}$$

where $E_\delta = \int_0^\delta e^{A\tau} d\tau I$ with $E_\delta w(z_r + j\delta) \in \mathcal{W}$. From (10c) and (11a), it holds that $x(z_r + (\tilde{s} + i)\delta) \in \mathcal{X}$ for $i \in \mathbb{N}_{[0,N]}$. Similarly, it holds that $u(z_r + (\tilde{s} + i)\delta) \in \mathcal{U}$ for $i \in \mathbb{N}_{[0,N-1]}$. Furthermore, using (20c) with iteration, we have $(A_\delta + B_\delta K)^k \mathcal{X}_f \oplus (A_\delta + B_\delta K)^N \mathcal{F}_k \subseteq \mathcal{X}_f$. Then,

$$\begin{aligned} x_{N|z_r+\tilde{s}} &\in x_{\tilde{s}+N|z_r} \oplus (A_\delta + B_\delta K)^N \mathcal{F}_{\tilde{s}} \\ &= (A_\delta + B_\delta K)^{\tilde{s}} x_{N|z_r} \oplus (A_\delta + B_\delta K)^N \mathcal{F}_{\tilde{s}} \\ &\in \mathcal{X}_f, \end{aligned} \tag{26}$$

leading to $\tilde{\mathrm{d}} \in \mathcal{D}_N(x(z_r + \tilde{s}\delta))$. Notice that, if $z_{r+1} - z_r < N\delta$, the proof is completed here.

When $z_{r+1} - z_r \geq N\delta$, for $\hat{s} \in \mathbb{N}_{[N, z_{r+1}-z_r]}$, the buffered control values are used up, then $u(z_r + \hat{s}\delta) = u_{N|z_r}$, we have

$$\begin{aligned} x(z_r + (\hat{s} + i)\delta) - x_{\hat{s}+i|z_r} &= A_\delta^{\hat{s}+i-N}(x(z_r + N\delta) - x_{N|z_r}) + \sum_{j=0}^{\hat{s}+i-N-1} A_\delta^j E_\delta w(z_r{}^*) \\ &\in A_\delta^{\hat{s}+i-N} \left(\bigoplus_{j=0}^{N-1} (A_\delta + B_\delta K)^j \mathcal{W} \right) \oplus \bigoplus_{i=0}^{\hat{s}+i-N-1} A_\delta^j \mathcal{W} \\ &= \mathcal{F}_{\hat{s}+i}, \end{aligned} \tag{27}$$

where $z_r{}^* = z_r + (\hat{s} + i - j - 1)\delta$ for $i \in \mathbb{N}_{[0,N]}$. It can be obtained from (20a) and (20b) that $x(z_r + (\hat{s} + i)\delta) \in A_\delta^{\hat{s}+i-N} \mathcal{X}_f \oplus \mathcal{F}_{\hat{s}+i} \subseteq \mathcal{X}$ for $i \in \mathbb{N}_{[0,N]}$ and $u(z_r + (\hat{s} + i)\delta) \in K A_\delta^{\hat{s}+i-N} \mathcal{X}_f \oplus K\mathcal{F}_{\hat{s}+i} \subseteq \mathcal{U}$ for $i \in \mathbb{N}_{[0,N-1]}$ hold.

In this case, the decision variable of the controller changes since the predicted input data at the last successful transmission instant has been used up. Consider the decision variable $\hat{\mathrm{d}} = ((x_{0|z_r+\hat{s}}, \dots, x_{N|z_r+\hat{s}}), (u_{0|z_r+\hat{s}}, \dots, u_{N-1|z_r+\hat{s}}))$, where

$$x_{i|z_r+\hat{s}} = A_\delta^{\hat{s}+i-N}(x(z_r + \hat{s}\delta) - x_{N|z_r}) + x_{\hat{s}+i|z_r},\ i \in \mathbb{N}_{[0,N]} \tag{28}$$

$$u_{i|z_r+\hat{s}} = K A_\delta^{\hat{s}+i-N}(x(z_r + \hat{s}\delta) - x_{N|z_r}) + u_{\hat{s}+i|z_r},\ i \in \mathbb{N}_{[0,N-1]}. \tag{29}$$

Based on $A_\delta \mathcal{X}_f \oplus A_\delta^N \mathcal{W} \subseteq \mathcal{X}_f$ from (20d), assume that $A_\delta^k \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_{k+N} \subseteq \mathcal{X}_f$ holds for $k \in \mathbb{N}_{[0,M-N]}$, and yields

$$\begin{aligned} A_\delta^{k+1} \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_{k+N+1} &= A_\delta^{k+1} \mathcal{X}_f \oplus A_\delta^N (A_\delta \mathcal{F}_{k+N} \oplus \mathcal{W}) \\ &= A_\delta \left(A_\delta^k \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_{k+N} \right) \oplus A_\delta^N \mathcal{W} \\ &\subseteq \mathcal{X}_f. \end{aligned} \tag{30}$$

Then, $A_\delta^k \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_{k+N} \subseteq \mathcal{X}_f$ holds. Combined with (28), it yields

$$\begin{aligned} x_{N|z_r+\hat{s}} &\in A_\delta^{\hat{s}} \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_{\hat{s}} \\ &\subseteq A_\delta^M \mathcal{X}_f \oplus A_\delta^N \mathcal{F}_M \subseteq \mathcal{X}_f, \end{aligned} \tag{31}$$

for $\hat{s} \leq M$. Consider that $\hat{s}\delta = z_{r+1} - z_r$, it readily follows that $\mathrm{d}_N \in \mathcal{D}_N(x(z_{r+1}))$ with $\mathrm{d}_N = ((x_{0|z_{r+1}}, \dots, x_{N|z_{r+1}}), (u_{0|z_{r+1}}, \dots, u_{N-1|z_{r+1}}))$, and the system constraints are satisfied for all $t \in \mathbb{R}_{[z_r, z_{r+1})}$ for the closed-loop system. Then, the proof is completed. □

Remark 5. The main difficulty compared with the work of Brunner et al[27] is the proof of the recursive feasibility at DoS intervals, especially when the N prediction input values stored in the buffer are used up. In this case, the predicted state and input are different from the normal case. The idea is to predict the current state of the open-loop interval to provide the optimal input information for the first successful transmission after an attack, as shown in (28) and (29). This design has increased the robustness against the DoS attacks, but a larger terminal set is required as a trade-off, as shown in Assumption 4.

4.2 Stability analysis

Notice that the optimal solution of the MPC optimization problem (14) is $u_{i|t} = Kx_{i|t}$, which means that the additional input $v_i = 0$. If the constraints are tight, $v_i \neq 0$. For $t \in \mathbb{R}_{[z_r+i\delta, z_r+(i+1)\delta)}$, $v(t) = v_i$. In this sense, $v(t)$ can be regarded as an exogenous signal to the closed-loop system when the MPC optimization problem (14) is feasible.

Denote by $e(t+i\delta) = x_{i|t} - x(t+i\delta)$, $i \in \mathbb{N}_{[0,N]}$ is the prediction error. Then, using sample-and-hold unit, it can be obtained that

$$e(t) = x_{i|t} - x(t), \tag{32}$$

where $e(t) \in \mathcal{F}_i$ for $t \in \mathbb{R}_{[z_r+i\delta, z_r+(i+1)\delta)}$. Then, for $t \in \mathbb{R}_{\geq 0}$, the process dynamics can be transformed as

$$\dot{x}(t) = (A+BK)x(t) + BKe(t) + Bv(t) + w(t). \tag{33}$$

The event-triggering threshold sets are given as

$$\mathcal{T}_i = \{e(t+i\delta) \in \mathbb{R}^n, i \in \mathbb{N}_{[0,N-1]} | \ \|e(t+i\delta)\| \leq \sigma \|x(t+i\delta)\| \}. \tag{34}$$

Lemma 3. *For $\mathcal{T}_i, i \in \mathbb{N}_{[0,N]}$ given in (34), if $0 < \sigma \leq \|A_\delta\|^{-1}$ is satisfied for the constant σ, Assumption 3 is satisfied.*

Proof. For $i = 0$, $\mathcal{R}_0 \subseteq \mathcal{F}_0$ is trivially satisfied from $\mathcal{R}_0 = \{0\}$ and $\mathcal{F}_0 = \mathcal{W}$. For $\bar{e} = \sup\{i \in \mathbb{N}_{[0,N]} | e(t+i\delta) \in \mathcal{T}_i\}$, it can be obtained that it is bounded as $e(t+i\delta) \in \mathcal{F}_i = \{e(t+i\delta) : \|e(t+i\delta)\| \leq e_{\max}\}$, where $e_{\max} = \|A_\delta\| \bar{e} + \max_{w\in\mathcal{W}} \|w\|$. Then, if $0 < \sigma \leq \|A_\delta\|^{-1}$ holds, one has $A_\delta \mathcal{T}_i \oplus \mathcal{W} \subseteq \mathcal{F}_{i+1}$. It follows that, for $i \in \mathbb{N}_{[1,N]}$,

$$\begin{aligned} \mathcal{R}_i &= A_\delta(\mathcal{R}_{i-1} \cap \mathcal{T}_{i-1}) \oplus \mathcal{W} \\ &\subseteq A_\delta \mathcal{T}_{i-1} \oplus \mathcal{W} \\ &\subseteq (\mathcal{F}_i \ominus \mathcal{W}) \oplus \mathcal{W} \subseteq \mathcal{F}_i \end{aligned} \tag{35}$$

holds. Then, Assumption 3 is satisfied. □

The stability proof is based on the Lyapunov function chosen as $V(t) = x^T(t)Px(t)$, where P can be solved from the following equation:

$$P\Phi + \Phi^T P = -Q, \tag{36}$$

with $\Phi = A + BK$, and Q is defined as an any given positive definite symmetric matrix. Then,

$$\alpha_2 \|x(t)\| \leq V(t) \leq \alpha_1 \|x(t)\| \tag{37}$$

$$\dot{V}(t) \leq -\gamma_1 \|x(t)\|^2 + \gamma_2 \|x(t)\| \|e(t)\| + \gamma_3 \|x(t)\| \|v(t)\| + \gamma_4 \|x(t)\| \|w(t)\|, \tag{38}$$

where α_1 and α_2 denote the largest and smallest eigenvalues of P, respectively. Denote by γ_1 the smallest eigenvalue of Q, $\gamma_2 = \|2PBK\|$, $\gamma_3 = \|2PB\|$, and $\gamma_4 = \|2P\|$.

Theorem 2. *Consider the dynamical system (1) with the control input (6) and (17), the event condition is chosen as (16) and (34). Then, the closed-loop system (33) is ISpS in the absence of DoS attacks when $\gamma_1 > \sigma\gamma_2$ is satisfied, and the sampling interval of the controller unit satisfies*

$$\delta \leq \begin{cases} \frac{1}{\mu_A} \log\left(\frac{\mu_A \sigma}{\lambda(1+\sigma)} + 1\right), & \mu_A > 0 \\ \frac{\sigma}{\lambda(1+\sigma)}, & \mu_A \leq 0. \end{cases} \tag{39}$$

Proof. First, the predicted state $x_{i|t}$ is

$$x_{i|z_r} = A_\delta^i x_{0|z_r} + \sum_{j=0}^{i-1} A_\delta^{i-j-1} B_\delta (K x_{j|z_r} + v_j), \tag{40}$$

with $i \in \mathbb{N}_{[1,N-1]}$. The process dynamics with $t \in \mathbb{R}_{[z_r, z_{r+1})}$ satisfy

$$x(t) = e^{A(t-z_r)} x(z_r) + \int_{z_r}^{t} e^{A(t-\tau)} B(Kx(\tau) + v(\tau)) d\tau + \int_{z_r}^{t} e^{A(t-\tau)} w(\tau) d\tau. \tag{41}$$

It can be obtained that

$$\begin{aligned} e(z_r+i\delta) &= x_{i|t} - x(z_r+i\delta) \\ &= e^{Ai\delta}(x_{0|z_r} - x(z_r)) - \int_{z_r}^{z_r+i\delta} e^{A(z_r+i\delta-\tau)} w(\tau)d\tau, \end{aligned} \tag{42}$$

where $x_{0|z_r} = x(z_r)$ and following the same argument from lemma 2 in the work of Feng and Tesi[15] that

$$\int_{z_r}^{z_r+i\delta} e^{A(z_r+i\delta-\tau)} B(Kx(\tau)+v(\tau))d\tau = \sum_{j=0}^{i-1} A_\delta^{i-j-1} B_\delta(Kx_{j|z_r}+v_j),$$

with $s = z_r+(j+1)\delta-\tau$. Then, (42) yields $\|e(z_r+i\delta)\| \leq \varepsilon_1 \|w(z_r+i\delta)\|_\infty$, where $\varepsilon_1 = \begin{cases} \frac{1}{\mu_A}(e^{\mu_A(N-1)\delta}-1), & \mu_A > 0 \\ (N-1)\delta, & \mu_A \leq 0. \end{cases}$

Notice that the upper bound of the error dynamics $e(t)$ at the sampling times $z_r+i\delta$ is provided in (34), where $\varepsilon_1\|w(z_r+i\delta)\|_\infty \leq \sigma\,\|x(t+i\delta)\|$ for the worst case $i \in \mathbb{N}_{[1,N-1]}$. However, it is necessary to give the upper bound between intersamplings since if $\|e(t)\| = \sigma\,\|x(t)\|$ is satisfied between the sampling intervals, the upper bound at the sampling times may be invalid. The error dynamic is given as

$$\dot{e}(t) = Ae(t) - \Phi x_{i|t} - Bv(t) - w(t), \tag{43}$$

for $t \in \mathbb{R}_{[z_r+i\delta, z_r+(i+1)\delta)}$, $i \in \mathbb{N}_{[0,N-1]}$ with $e(z_r) = 0$. Denote by $g(t-z_r-i\delta) = \int_{z_r+i\delta}^{t} e^{\mu_A(t-\tau)}d\tau$ for $t \in \mathbb{R}_{\geq z_r+i\delta}$. Then, it can be obtained that

$$\begin{aligned} \|e(t)\| &\leq e^{\mu_A(t-z_r-i\delta)}\,\|e(t+i\delta)\| + \lambda g(t-z_r-i\delta)(\|w_t\|_\infty + \|v(t)\| + \|x_{i|t}\|) \\ &\leq \varepsilon_1\varepsilon_2\|w_t\|_\infty + \lambda g(\delta)(\|w_t\|_\infty + \|v(t)\| + \|e(t)\| + \|x(t)\|), \end{aligned} \tag{44}$$

where $\varepsilon_2 = \max\{e^{\mu_A\delta}, 1\}$ and $\lambda = \max\{\|\Phi\|, \|B\|, 1\}$. Notice that $g(0) = 0$ and $g(\cdot)$ is monotonically increasing with t, following the same argument as in theorem 1 in the work of De Persis and Tesi[13] and lemma 2 in the work of Feng and Tesi[15] in which the parameter σ is selected such that $\lambda g(\delta) \leq \frac{\sigma}{1+\sigma}$, it can be obtained that, for $t \in \mathbb{R}_{[z_r, z_r+i\delta)}$, $i \in \mathbb{N}_{[0,N]}$,

$$\|e(t)\| \leq \sigma\,\|x(t)\| + \sigma\,\|v(t)\| + \varepsilon\|w_t\|_\infty, \tag{45}$$

where $\varepsilon = \sigma + (1+\sigma)\varepsilon_1\varepsilon_2$. Besides, $\lambda g(\delta) \leq \frac{\sigma}{1+\sigma}$ leads to the condition (39) for the sampling interval of the controller unit.

Substituting (45) into (38), by using Young's inequality, yields

$$V(t) \leq e^{-\theta_1(t-z_r)}V(z_r) + \eta_1\|v(t)\|^2 + \eta_2\,\|w_t\|_\infty^2, \tag{46}$$

for $t \in \mathbb{R}_{[z_r, z_r+i\delta)}$, $i \in \mathbb{N}_{[0,N]}$, where $\theta_1 = \frac{\gamma_1-\sigma\gamma_2}{2\alpha_1}$, $\eta_1 = \frac{(\sigma\gamma_2+\gamma_3)^2}{\theta_1(\gamma_1-\sigma\gamma_2)}$ and $\eta_2 = \frac{(\varepsilon\gamma_2+\gamma_4)^2}{\theta_1(\gamma_1-\sigma\gamma_2)}$. Then, for $t \in \mathbb{R}_{\geq 0}$,

$$\|x(t)\| \leq \sqrt{\frac{\alpha_1}{\alpha_2}}e^{-\frac{\theta_1 t}{2}}\,\|x(0)\| + f(v) + \sqrt{\frac{\eta_2}{\alpha_2}}\|w_t\|_\infty, \tag{47}$$

where $f(v) = \sqrt{\frac{\eta_1}{\alpha_2}}\,\|v(t)\|$ is a $\mathcal{K}$-function and $\sqrt{\frac{\eta_2}{\alpha_2}}\|w_t\|_\infty$ is a constant for $w(t) \in \mathcal{W}$. Then, it can be concluded from Definition 1 that the closed-loop system is ISpS. Then, the proof is completed. □

Now, the main stability theorem is given as follows.

Theorem 3. *Consider the dynamical system (1) with the control input (6) and (17), the event condition is chosen as (16) and (34). For the DoS attacks with arbitrary ς, η, τ_D, and T satisfying Assumptions 1 and 2 and $\frac{1}{T} + \frac{\delta}{\tau_D} < 1$, the prediction horizon N satisfies $N \geq \frac{\theta_2(Q+\bar{\Delta})}{\delta(\theta_1+\theta_2)}$ with $\theta_1 = \frac{\gamma_1-\sigma\gamma_2}{2\alpha_1}$ and $\theta_2 = \frac{3\gamma_2}{2\alpha_2}$. Then, the closed-loop system (33) is ISpS.*

Proof. Denote by $z_r + i\delta$, $i \in \mathbb{N}_{[0,N]}$ the time instant that the next data packet is transmitted. When the DoS attacks are present in the interval $(z_r + (i-1)\delta, z_r + i\delta]$, consider the worst case that $i = \bar{\Delta}/\delta$ with $\bar{\Delta} \le N\delta$, $e(t) = x_{i|t} - x(t)$ for $t \in \mathbb{R}_{[z_r+N\delta, z_{r+1})}$, then

$$\|e(t)\| \le \|x(t)\| + \|x(z_r + N\delta)\| + \|e(z_r + N\delta)\| \,. \tag{48}$$

From (45), it can be obtained that $\|e(z_r + N\delta)\| \le \sigma \, \|x(z_r + N\delta)\| + \sigma \, \|v_N\| + \varepsilon \|w_t\|_\infty$. Then,

$$\begin{aligned}\dot{V}(t) &\le (-\gamma_1 + 2\gamma_2 + \sigma\gamma_2)\|x(t)\|^2 + (\sigma\gamma_2 + \gamma_3)\,\|x(t)\|\,\|v(t)\| + (\varepsilon\gamma_2 + \gamma_4)\,\|x(t)\|\,\|w_t\|_\infty \\ &\le 2\gamma_2\|x(t)\|^2 + \gamma_5\|v(t)\|^2 + \gamma_6\,\|d(t)\|_\infty^2 \,,\end{aligned} \tag{49}$$

where the first inequality is derived from $\|v_N\| \le \|v(t)\|$ and $\|x(z_r + N\delta)\| \le \|x(t)\|$ for $t \in \mathbb{R}_{[z_r+N\delta, z_{r+1})}$, the second inequality is derived from Young's inequality with $\gamma_5 = \frac{(\sigma\gamma_2+\gamma_3)^2}{2(\gamma_1-\sigma\gamma_2)}$ and $\gamma_6 = \frac{(\varepsilon\gamma_2+\gamma_4)^2}{2(\gamma_1-\sigma\gamma_2)}$. Then, we have

$$V(t) \le e^{\theta_2(t-z_r-N\delta)}V(z_r + N\delta) + e^{\theta_2(t-z_r-N\delta)}\left(\eta_3\|v(t)\|^2 + \eta_4\,\|w_t\|_\infty^2\right), \tag{50}$$

where $\theta_2 = \frac{2\gamma_2}{\alpha_2}$, $\eta_3 = \frac{\gamma_5}{\theta_2}$, and $\eta_4 = \frac{\gamma_6}{\theta_2}$. Combine (46) with (50), it can be obtained that, for all $t \in \mathbb{R}_{[z_r+N\delta, z_{r+1})}$ with $z_r + N\delta < z_{r+1}$,

$$\begin{aligned}V(t) &\le e^{\theta_2(t-z_r-N\delta)-\theta_1 N\delta}V(z_r) + e^{\theta_2(t-z_r-N\delta)}\left((\eta_1 + \eta_3)\|v(t)\|^2 + (\eta_2 + \eta_4)\,\|w_t\|_\infty^2\right) \\ &\le e^{-\theta_3(t-z_r)}V(z_r) + \eta_5\|v(t)\|^2 + \eta_6\,\|w_t\|_\infty^2 \,,\end{aligned} \tag{51}$$

where $\eta_5 = e^{\theta_2(Q+\bar{\Delta}-N\delta)}(\eta_1+\eta_3)$, $\eta_6 = e^{\theta_2(Q+\bar{\Delta}-N\delta)}(\eta_2+\eta_4)$, $\theta_3 = \frac{\theta_1 N\delta-\theta_2(Q+\bar{\Delta}-N\delta)}{Q+N\delta}$ such that the time horizon is transformed from $z_{r+1} - z_r$ to $t - z_r$ with $t \in \mathbb{R}_{[z_r+N\delta, z_{r+1})}$ and $z_{r+1} - z_r \le Q + \bar{\Delta}$. In order to get a dissipation inequality from (51), the prediction horizon N should be chosen as $N \ge \frac{\theta_2(Q+\bar{\Delta})}{\delta(\theta_1+\theta_2)}$. Then, for any $t \in \mathbb{R}_{[z_r, z_{r+1})}$, by iterating the work of De Persis and Tesi[13] and let $\theta = \min\{\theta_1, \theta_3\}$ yield

$$\begin{aligned}V(t) &\le e^{-\theta(t-z_0)}V(z_0) + \left(1 + \sum_{k=0}^{r(t)-1} e^{-\theta(z_{r(t)}-z_k)}\right)\left(\eta_5\|v(t)\|^2 + \eta_6\,\|w_t\|_\infty^2\right) \\ &\le e^{-\theta(t-z_0)}V(z_0) + \left(1 + \frac{1}{1-e^{-\theta\delta}}\right)(\eta_5\|v(t)\|^2 + \eta_6\,\|w_t\|_\infty^2),\end{aligned} \tag{52}$$

where $r(t) = \sup\{m \in \mathbb{N} | z_r \le t\}$ is the number of successful transmission packets up to now and $t \ge z_0$. Then,

$$\|x(t)\| \le \sqrt{\frac{\alpha_1}{\alpha_2}e^{-\frac{\theta(t-z_0)}{2}}}\,\|x(z_0)\| + \sqrt{1 + \frac{1}{1-e^{-\theta\delta}}}\left(\sqrt{\frac{\eta_5}{\alpha_2}}\,\|v(t)\| + \sqrt{\frac{\eta_6}{\alpha_2}}\|w_t\|_\infty\right) \tag{53}$$

holds. From Definition 1, the ISpS of the closed-loop system (33) is achieved. Then, the proof is completed. □

Remark 6. Compared with the strategies proposed in the works of De Persis and Tesi[13] and Feng and Tesi,[15] where the system constraints are not concerned, the difficulties are the analysis of the event-triggered control and how to deal with the predicted input error $v(t)$. Based on the ISpS framework, not only the relationship between the stabilization criteria and the time characteristics of the tolerable DoS attacks is obtained but also $v(t)$ can be regarded as an additional input to prove the stability of the closed-loop system. When the DoS attacks are absent, Theorem 2 details the sufficient conditions of the ETC and the sampling interval to guarantee the ISpS of the closed-loop system. Notice that the prediction horizon N only influences the parameter ε_1. When $\varepsilon_1\|w(z_r + i\delta)\|_\infty \le \sigma\,\|x(t + i\delta)\|$ holds, the increasing of N increases the average triggering time. However, when N is large enough such that the aforementioned inequality is untenable, the average triggering time will not increase but may worsen the system performance on account of the increasing of η_2. When the DoS attacks are present, Theorem 3 shows that the robustness against the worst attacks depends on the selection of N. In this case, N may be a pretty large value when the worst case that an attack occurred at the instant when the N control values are used up. To reduce the conservatism of the selection of N, the upper bound of the event-triggering intervals $\bar{\Delta}$ is given.

5 | SIMULATION EXAMPLE

In this section, we consider a batch reactor model taken from the work of Walsh and Ye.[30] The system is an open-loop unstable process with coupled two-input and two-output. Besides, the control data is transmitted by network. The system matrices are given as $A = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix}$. The disturbance $w(t)$ is a random signal that satisfies uniform distribution in $[-0.3, 0.3]$. The system constraints are set as $-1 \le x(t) \le 1$ and $-2 \le u(t) \le 2$. The initial condition is $x(0) = [0.8, -1, 0, 0.3]^T$. The auxiliary feedback gain matrix is chosen by LQR as $K = \begin{bmatrix} -0.7299 & -0.5116 & -1.2459 & 0.1511 \\ 2.3638 & 0.1773 & 1.6615 & -2.7389 \end{bmatrix}$. Therelative parameters can be obtained that $\alpha_1 = 2.1581$, $\alpha_2 = 0.0466$, $\gamma_1 = 1$, $\gamma_2 = 15.9451$, $\gamma_3 = 3.9377$, $\gamma_4 = 1.5352$, and $\mu_A = 3.4425$. We select the ETC $\sigma = 0.0625$ and the sampling interval $\delta = 0.01$ s. The simulation time is selected as $T = 15$ s with $T_s = 1500$ steps for the controller unit.

When the DoS attacks are absent, the buffer size is chosen as $N = 20$, then the system state responds and the input signals are given in Figure 2. Consider the performance index $J_p = \frac{1}{T_s}\sum_{t=0}^{T_s-1} x_t^T Q x_t + u_t^T R u_t$ with $Q = I^{4\times4}$ and $R = I^{2\times2}$, the average triggering time and the performance indices for different prediction horizons are presented in Table 1.

It can be seen from Table 1 and Figure 2 that the event-triggered MPC strategy in this paper reduces the communication utilization and computation load while achieving comparable control performance.

When the DoS attacks are present, the system state responds and the input signals under DoS attacks are given in Figure 3. The total duration and the frequency of the DoS attacks are $|\mathcal{D}(0, 15)| = 10.93$ s and $n(0, 15) = 12$, respectively. This corresponds to values of $\varsigma = 0.146$, $T = 1.3724$, $\eta = 1.35$, and $\tau_D = 1.25$. Moreover, 73% of communication attempts fail, and $\frac{\delta}{\tau_D} + \frac{1}{T} \approx 0.737$. The upper bound of the event intervals is defined as $\bar{\Delta} = 0.7$ s. The buffer size can be obtained from Theorem 3 that $N \ge 129.3$ and $N = 135$ is selected. The performance index is $J_p = 0.1107$. Furthermore, the event intervals and the evolution of the event condition are given in Figure 4. In order to highlight the advantages of the methods in this paper, the comparison simulation results are given in Figure 5. The top of Figure 5 shows the result without the

TABLE 1 Performance comparison

	Average triggering time	J_p
Periodic	1	0.0869
$N = 5$	2.4712	0.0884
$N = 20$	2.5641	0.0889
$N = 100$	2.5510	0.0893

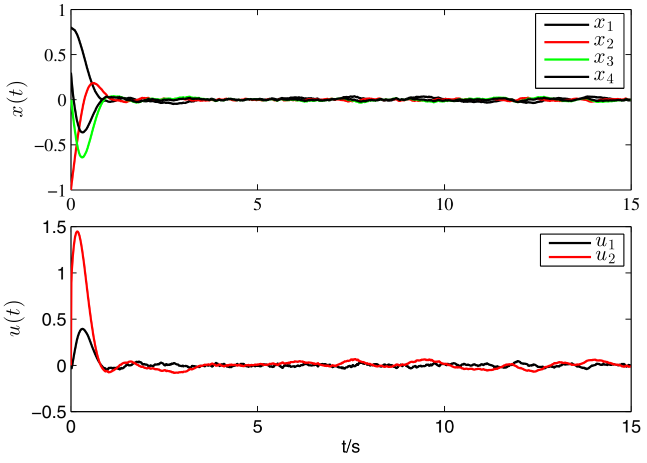

FIGURE 2 The state responds and the input signals [Colour figure can be viewed at wileyonlinelibrary.com]

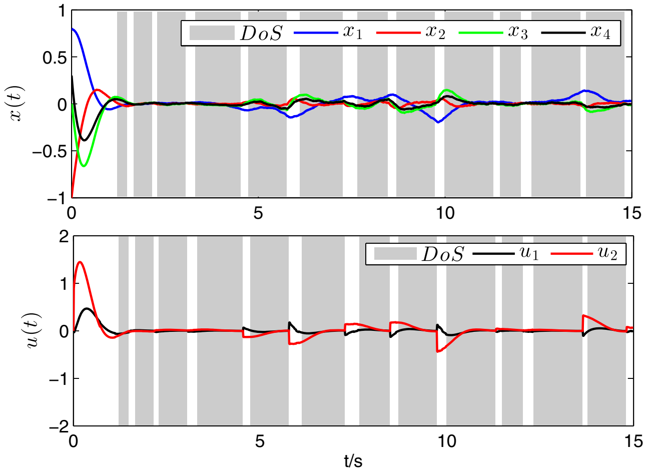

FIGURE 3 The state responds and the input signals under denial-of-service (DoS) attacks [Colour figure can be viewed at wileyonlinelibrary.com]

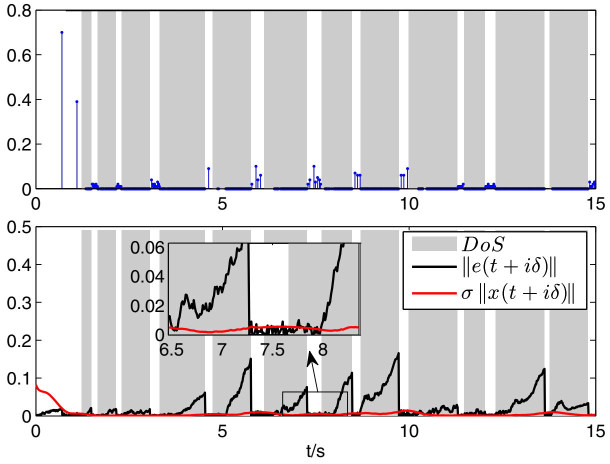

FIGURE 4 The event intervals and event condition. DoS, denial-of-service [Colour figure can be viewed at wileyonlinelibrary.com]

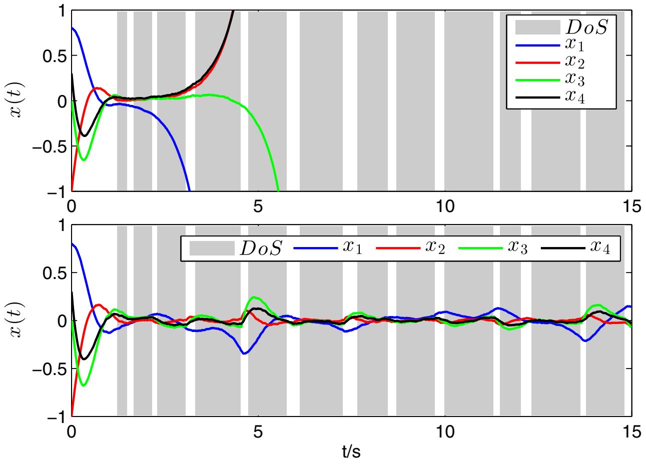

FIGURE 5 Top: The state responds without MPC strategy. Bottom: The simulation results of the algorithm in[15] [Colour figure can be viewed at wileyonlinelibrary.com]

MPC algorithm. It can be observed that the system cannot be stabilized without the packet-based method and predicted input signals. The bottom shows the result of the algorithm in the work of Feng and Tesi,[15] where a packed-based predictor method is used. It can be seen that the method in the aforementioned work[15] can tolerate the same DoS attacks. However, the performance index $J_p^* = 0.1359$ is larger than that in this paper. Besides, the event-triggered strategy in this paper can achieve a better control performance with much less communication and computation resources than the periodic transmission policy in the work of Feng and Tesi.[15]

6 | CONCLUSIONS

This paper concerns the resilient control problem based on the robust event-triggered MPC strategy for constrained continuous-time linear CPSs with bounded disturbances under DoS attacks. The ETC is designed to save the communication utilization and computation resources. The sampling-data MPC algorithm is designed to compensate the loss of the control data during the open-loop intervals. The recursive feasibility of the MPC algorithm and the ISpS of the closed-loop system is proved whether or not the DoS attacks are present. Moreover, the relationship between the sampling interval of the MPC control and the ETC is obtained. Simulation results have verified the effectiveness of the proposed method. In the future, one possible extension is to extend the algorithm to nonlinear systems[26,31] under DoS attacks.

ACKNOWLEDGEMENTS

This work was supported in part by the Funds of the National Natural Science Foundation of China (Grants 61621004 and 61420106016) and the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries (Grant 2018ZCX03).

ORCID

Guang-Hong Yang https://orcid.org/0000-0002-8911-0112

REFERENCES

1. Teixeira A, Shames I, Sandberg H, Johansson KH. A secure control framework for resource-limited adversaries. *Automatica*. 2015;51:135-148.
2. Hu F, Lu Y, Vasilakos AV, et al. Robust cyber-physical system: concept, model, and implementation. *Future Gener Comput Syst*. 2016;56:449-475.
3. Wang Y-L, Han Q-L, Fei M-R, Peng C. Network-based T–S fuzzy dynamic positioning controller design for unmanned marine vehicles. *IEEE Trans Cybern*. 2018;48(9):2750-2763.
4. Wang Y-L, Han Q-L. Network-based modelling and dynamic output feedback control for unmanned marine vehicles. *Automatica*. 2018;91:43-53.
5. Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems. *IEEE Trans Autom Control*. 2013;58(11):2715-2729.
6. An L, Yang G-H. Data-driven coordinated attack policy design based on adaptive L_2-gain optimal theory. *IEEE Trans Autom Control*. 2018;63(6):1850-1857.
7. Lu A-Y, Yang G-H. Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer. *Information Sciences*. 2017;417:454-464.
8. Xie C-H, Yang G-H. Secure estimation for cyber-physical systems with adversarial attacks and unknown input: an L_2-gain method. *Int J Robust Nonlinear Control*. 2018;28(6):2131-2143.
9. Cetinkaya A, Ishii H, Hayakawa T. Networked control under random and malicious packet losses. *IEEE Trans Autom Control*. 2017;62(5):2434-2449.
10. Zhang H, Cheng P, Shi L, Chen J. Optimal denial-of-service attacks scheduling with energy constraint. *IEEE Trans Autom Control*. 2015;60(11):3023-3028.
11. Yuan H, Xia Y, Yang H, Yuan Y. Resilient control for wireless networked control systems under DoS attack via a hierarchical game. *Int J Robust Nonlinear Control*. 2018;28(15):4604-4623.
12. Yuan H, Xia Y. Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework. *Information Sciences*. 2018;454-455:312-327.
13. De Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans Autom Control*. 2015;60(11):2930-2944.
14. Feng S, Tesi P. Resilient control under denial-of-service: robust design. *Automatica*. 2017;79:42-51.
15. Feng S, Tesi P. Networked control systems under denial-of-service: con-located vs. remote architectures. *Syst Control Lett*. 2017;108:40-47.
16. De Persis C, Tesi P. Networked control of nonlinear systems under denial-of-service. *Syst Control Lett*. 2016;96:124-131.
17. Lu A-Y, Yang G-H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial-of-service. *IEEE Trans Autom Control*. 2018;63(6):1813-1820.
18. Sun Y-C, Yang G-H. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. *J Franklin Inst*. 2018;355:5613-5631.
19. Sun Y-C, Yang G-H. Event-triggered resilient control for cyber-physical systems under asynchronous DoS attacks. *Information Sciences*. 2018;465:340-352.
20. Brunner FD, Heemels M, Allgöwer F. Robust self-triggered MPC for constrained linear systems: a tube-based approach. *Automatica*. 2016;72:73-83.

21. Mayne DQ, Seron MM, Raković SV. Robust model predictive control of constrained linear systems with bounded disturbances. *Automatica*. 2005;41:219-224.
22. Farina M, Scattolini R. Tube-based robust sampled-data MPC for linear continuous-time systems. *Automatica*. 2012;48:1473-1476.
23. He N, Shi D, Chen T. Self-triggered model predictive control for networked control systems based on first-order hold. *Int J Robust Nonlinear Control*. 2018;28(4):1303-1318.
24. Liu C, Li H, Gao J, Xu D. Robust self-triggered min-max model predictive control for discrete-time nonlinear systems. *Automatica*. 2018;89:333-339.
25. Peng C, Li F. A survey on recent advances in event-triggered communication and control. *Information Sciences*. 2018;457-458:113-125.
26. Li H, Shi Y. Event-triggered robust model predictive control of continuous-time nonlinear systems. *Automatica*. 2014;50:1507-1513.
27. Brunner FD, Heemels WPMH, Allgöwer F. Robust event-triggered MPC with guaranteed asymptotic bound and average sampling rate. *IEEE Trans Autom Control*. 2017;62(11):5694-5709.
28. Ström T. On logarithmic norm. *SIAM J Numer Anal*. 1975;12(5):741-753.
29. Lazar M, Muñoz de la Peña D, Heemels WPMH, Alamo T. On input-to-state stability of min–max nonlinear model predictive control. *Syst Control Lett*. 2008;57:39-48.
30. Walsh GC, Ye H. Scheduling of networked control systems. *IEEE Control Syst Mag*. 2001;21(1):57-65.
31. Peng C, Wu M, Xie X, Wang Y-L. Event-triggered predictive control for networked nonlinear systems with imperfect premise matching. *IEEE Trans Fuzzy Syst*. 2018;26(5):2797-2806.

How to cite this article: Sun Y-C, Yang G-H. Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. *Int J Robust Nonlinear Control*. 2019;1–15. https://doi.org/10.1002/rnc.4654