SCIENCE CHINA
Information Sciences

January 2022, Vol. 65 110202:1–110202:17
https://doi.org/10.1007/s11432-020-3289-1

• RESEARCH PAPER •
Special Focus on Cyber-Physical Systems

Event-triggered robust MPC of nonlinear cyber-physical systems against DoS attacks

Qi SUN, Jicheng CHEN & Yang SHI*

Department of Mechanical Engineering, University of Victoria, Victoria V8W 3P6, *Canada*

Received 15 September 2020/Revised 25 March 2021/Accepted 17 June 2021/Published online 27 December 2021

Abstract This paper proposes an event-triggered robust nonlinear model predictive control (NMPC) framework for cyber-physical systems (CPS) in the presence of denial-of-service (DoS) attacks and additive disturbances. In the framework, a new robustness constraint is introduced to the NMPC optimization problem in order to deal with additive disturbances, and a packet transmission strategy is designed for NMPC such that DoS attacks can be tackled. Then, an event-triggered mechanism, which accommodates DoS attacks occurring in the communication network, is proposed to reduce the communication cost for resource-constrained CPSs. Besides, we prove that the NMPC algorithm is recursively feasible and the closed-loop system is input-to-state practical stable under some sufficient conditions. Simulation examples and comparisons are conducted to show the effectiveness of the proposed NMPC algorithm.

Keywords cyber-physical systems, nonlinear model predictive control, event-triggered mechanism, robust control, denial-of-service attacks

Citation Sun Q, Chen J C, Shi Y. Event-triggered robust MPC of nonlinear cyber-physical systems against DoS attacks. Sci China Inf Sci, 2022, 65(1): 110202, https://doi.org/10.1007/s11432-020-3289-1

1 Introduction

Cyber-physical systems (CPSs), which integrate advanced computation, communication and control technologies with physical process, are widely applied in research areas such as smart manufacturing, embedded systems and smart grid [1, 2]. Due to possible exposure to unreliable network and complex physical environment, CPSs may simultaneously face multiple cyber and physical issues, e.g., malicious cyber attacks [3], uncertainties and/or disturbances [4], limited resources [5]. Therefore, it is of great importance to develop resilient and resource-aware control strategies, especially for safe-critical CPS applications [5].

The major objectives of resilient control include security and robustness [4]. Security refers to the operational normalcy under malicious attacks [6]. In particular, two of the main concerns with respect to security are deception attacks and denial-of-service (DoS) attacks. Deception attackers intend to manipulate the data transmission by injecting false and interpolated data packets into the communication channel (e.g., [7] and references therein), whereas DoS attackers typically aim at jamming communication channel such that the data transmission can be disabled for some time periods (for instance, [6]). In this paper, we focus on designing resilient control strategies to guarantee security against DoS attacks and robustness to disturbances. Recent research advances towards resilient control can be seen in [8–11] and reference therein.

In addition to resilience, the control strategy for CPSs also need to consider resource-awareness including inherent physical constraints and networking limitations. Firstly, physical constraints are usually imposed on physical process such that states and control actions of that process fulfill operational safety and actuator saturation. Model predictive control (MPC) is widely regarded as one of the most successful control paradigms capable of handling these constraints in real applications such as oil refineries and chemical plant. MPC can generate control law based on the optimal control and state sequences

* Corresponding author (email: yshi@uvic.ca)

obtained by repeatedly solving constrained optimization problems with future system performance as objective functions [12]. Secondly, networking limitations reveal insufficient communication resources due to imperfect communication channel or limited communication bandwidth [13]. Since communication in CPSs is generally realized by data packets transmitted at discrete-time instants, the communication resource can become restricted especially when multiple devices share one communication channel. Hence, it is necessary to develop resilient and resource-aware control strategies that can reduce the data transmission without deteriorating stability and desired control performance, even in the presence of DoS attacks.

To fulfill the aforementioned control objectives, we propose an event-triggered robust nonlinear model predictive control (NMPC) strategy, where the packet transmission time instants are determined using an event-triggered mechanism (ETM). The main contributions of this paper are as follows.

(1) A new robustness constraint is designed for the MPC optimization problem in order to tackle additive disturbance. Different from the existing techniques [14, 15], the proposed robustness constraint is constructed based on the state constraint set rather than the terminal state constraint, which can bring the additional benefit of being able to act as state constraints.

(2) An improved packet transmission strategy is designed for the event-triggered robust NMPC framework, where two dynamic buffers are respectively designed such that the actuator and the ETM can receive real-time control signals and reference states despite the existence of DoS attacks. Based on this transmission strategy, the proposed ETM can save more communication resources than the conventional ETMs since it can accommodate the case when the intervals between any two consecutive triggering instants can be larger than the prediction horizon.

(3) Sufficient conditions for the recursive feasibility of event-triggered robust NMPC and the input-to-state practical stability (ISpS) of the closed-loop system are respectively given. Despite the existence of DoS attacks and additive disturbances, the optimal value function of the NMPC optimization problem can be proved as an ISpS-Lyapunov function.

Related work. In the vast majority of literature on resilient control, two types of DoS attacks have been respectively formulated using deterministic and stochastic settings. The former characterizes attacks by considering attack launching times and durations (e.g., periodic attacks [16–18] and time-sequence based attacks [19–21]), whereas the latter focuses on stochastic nature of some malicious attackers (e.g., Bernoulli attacks [22] and Markov-modulated attacks [23]). Deterministic DoS attacks are often believed to be more realistic since attackers do have clear incentives to sabotage control objectives [19]. In addition, since time-sequence based attacks only impose explicit constraints on the attack duration and/or frequency, periodic DoS attacks can be conveniently modeled using the time-sequence setup [19]. Throughout this paper, we formulate DoS attacks in the duration-constrained fashion; e.g., [21]. In [16], an event-triggered control of continuous linear time-invariant (LTI) systems under periodic jamming attacks was proposed, where the attack was formulated as a pulse-width modulated (PWM) signal that has a uniform upper bound. In [17], the authors presented a relative-threshold triggering condition for event-triggered control of continuous LTI system under periodic DoS attacks in forward and backward channels. In this method, a zero-input strategy was applied due to DoS attacks, whereas the closed-loop stability was derived using the time delay and switched system approach. In [18], the periodic DoS attacks are characterized by a cyclic dwell-time switching strategy, by which the resulting augmented system can be transformed to a stable and an unstable subsystems.

The ETM triggering rules rely on the state or output measurements, leading to the so-called Lebesgue sampling based control, i.e., event-triggered control (ETC) [24, 25]. Compared with the conventional periodic control scheme, ETC is effective to avoid unnecessary controller updates without jeopardizing control performance. In particular, the integration of ETM into MPC is more beneficial in terms of communication and computation reduction since MPC usually features heavier computational complexity. Hence, many research efforts on event-triggered MPC (ET-MPC) have been undertaken by [14,15,26–28]. It is also of great importance to study ET-MPC for safe-critical CPSs since ET-MPC is a promising tool that can exhibit remarkable performance of resource-awareness under imperfect communication networks. However, the related research topics have largely remained unexplored with a few notable exceptions including [29–31]. Specifically, DoS attacks and deception attacks have been respectively studied by [29, 30] in periodic sampling-based MPC settings. In order to save the communication resource, the authors in [31] have introduced a robust ET-MPC framework for linear time-invariant systems under DoS attacks and additive disturbances, where the closed-loop system was proved to be input-to-state practical stable. Due to fixed-length control packets induced by MPC controllers, the packet transmission strategy in [31]

may not fit well with resilient and resource-aware control objectives. In this paper, we aim to achieve resilient and resource-aware control objectives for nonlinear CPSs with additive disturbances via an event-triggered robust NMPC framework.

The remainder of this paper is organized as follows. Necessary notations and preliminaries are given in Section 2. In Section 3, we describe the problem formulation. The event-triggered NMPC scheme is introduced in Section 4. Section 5 presents some sufficient conditions under which the MPC optimization problem is recursively feasible and the closed-loop system is input-to-state practical stable. In Section 6, simulation and comparison examples are presented to verify the effectiveness of the proposed strategy. Finally, we conclude this work in Section 7.

2 Notations and preliminaries

2.1 Notations

All real numbers and all the nonnegative real numbers are respectively denoted by $\mathbb{R}$ and $\mathbb{R}_{\geqslant 0}$. The symbols $\mathbb{N}_{\geqslant 0}$ and $\mathbb{N}_{>0}$ represent the set of all nonnegative integers and the set of all positive integers. Let $\mathbb{N}_{[a,b)}$ denote all the integers larger than or equal to a and smaller than b. For a real number $r \in \mathbb{R}$, $\lceil r \rceil$ and $\lfloor r \rfloor$ are the greatest and smallest integers around r. For a given matrix X, we use X^{T} and X^{-1} to denote its transpose and inverse. We write $X \succ 0$ or $X \succeq 0$ if X is positive definite (PD) or positive semidefinite (PSD). The largest and smallest eigenvalues of X are denoted by $\overline{\lambda}(X)$ and $\underline{\lambda}(X)$, respectively. Given a column vector $x \in \mathbb{R}^n$, $\|x\|$ represents its Euclidean norm and $\|x\|_P := \sqrt{x^{\mathrm{T}} P x}$ is the P-weighted norm. For any set $\mathbb{X} \subseteq \mathbb{R}^n$, we define a metric on $\mathbb{R}^n$ as $\|\mathbb{X}\| \triangleq \sup_{x \in \mathbb{X}} \|x\|$. Note that $\alpha \mathbb{X} \triangleq \{\alpha x : x \in \mathbb{X}\}$ is elementary-wise multiplication of $\mathbb{X}$, where $\alpha \in (0, 1)$. Given two functions α_1 and α_2, $\alpha_1 \circ \alpha_2$ denotes the function composition of these two functions.

2.2 Input-to-state practical stability

Consider the following discrete-time nonlinear perturbed system:

$$x_{k+1} = g(x_k, w_k), \tag{1}$$

where $x_k \in \mathbb{R}^n$ and $w_k \in \mathbb{W} \subset \mathbb{R}^n$ are, respectively, the system state and the unknown but bounded uncertainty with appropriate dimensions; $\mathbb{W}$ is a compact set containing the origin in its interior; $g : \mathbb{R}^n \times \mathbb{W} \mapsto \mathbb{R}^n$ is a continuous mapping with $g(0, 0) = 0$. Note that the disturbance bound can be represented by $\|\mathbb{W}\| \triangleq \sup_{w \in \mathbb{W}} \|w\|$.

Definition 1. Let $\mathcal{K}$ denote a class of continuous, positive-definite, and strictly increasing functions, e.g., $\alpha \in \mathcal{K}$ means that $\alpha : \mathbb{R}_{\geqslant 0} \mapsto \mathbb{R}_{\geqslant 0}$ is strictly increasing with $\alpha(0) = 0$. A function $\alpha \in \mathcal{K}$ belongs to class $\mathcal{K}_\infty$ if $\alpha(r) \to \infty$ as $r \to \infty$. A continuous function $\beta : \mathbb{R}_{\geqslant 0} \times \mathbb{N}_{\geqslant 0} \mapsto \mathbb{R}_{\geqslant 0}$ belongs to class $\mathcal{KL}$ if: (1) $\beta(\cdot, s) \in \mathcal{K}$ for each fixed $s \geqslant 0$; (2) $\beta(r, \cdot)$ is strictly decreasing with $\beta(r, s) \to 0$ as $s \to \infty$ for each fixed $r \geqslant 0$.

By virtue of the comparison functions, we recall a very well-known stability definition.

Definition 2 (ISpS [32])**.** The system in (1) is said to be input-to-state practical stable if there exist $\beta \in \mathcal{KL}$, $\gamma \in \mathcal{K}$ and a constant $c \geqslant 0$ such that, for all $w \in \mathbb{W}$, the state trajectory x_k satisfies

$$\|x_k\| \leqslant \beta(\|x_0\|, k) + \gamma(\|\mathbb{W}\|) + c \tag{2}$$

for all $k \in \mathbb{N}$.

Based on these definitions, we are ready to present the following important ISpS result, which will be used for analyzing the closed-loop stability.

Lemma 1 ([32])**.** If the system in (1) admits a continuous function $V : \mathbb{R}^n \mapsto \mathbb{R}_{\geqslant 0}$ such that

$$\underline{\alpha}_V(\|x\|) \leqslant V(x) \leqslant \bar{\alpha}_V(\|x\|) + c_1,$$
$$V(g(x, w)) - V(x) \leqslant -\alpha_V(\|x\|) + \gamma_V(\|\mathbb{W}\|) + c_2,$$

where $\underline{\alpha}_V, \bar{\alpha}_V, \alpha_V \in \mathcal{K}_\infty$, $\gamma_V \in \mathcal{K}$ and $c_1, c_2 > 0$, then it is input-to-state practical stable. Besides, V is called an ISpS-Lyapunov function for the system in (1).

2.3 DoS attacks

As a common threat to CPSs, DoS attacks are launched by malicious adversaries to compromise communication channel, rendering the CPS information (i.e., control signals) inaccessible from the key CPS components such as the controller. Inspired by [19], we model the DoS attack by its launching time instants and durations.

Let $\mathcal{T}^a \triangleq \{k_\ell^a \in \mathbb{N}_{\geqslant 0} | \ell \in \mathbb{N}\}$ and $\mathcal{D}^a \triangleq \{d_\ell^a \in \mathbb{N}_{>0} | \ell \in \mathbb{N}\}$ denote, respectively, all the launching time instants and corresponding durations of the DoS attack, where ℓ denotes the ℓth launching. Using the above configuration, the DoS attack can be properly formulated by a piecewise discrete-time sequence. It is also worth noting that $d_\ell^a < k_{\ell+1}^a - k_\ell^a$, i.e., the time steps between the two consecutive launching time instants must be larger than the ℓth DoS attack duration. Using the above notations, we can define the total activation time of the DoS attack as

$$\Xi(0,\infty) \triangleq \bigcup_{\ell \in \mathbb{N}} \mathbb{N}_{[k_\ell^a, k_\ell^a + d_\ell^a)} \tag{3}$$

and consequently define the overall successful transmission time as

$$\Theta(0,\infty) \triangleq \mathbb{N}_{[0,\infty)} \backslash \Xi(0,\infty). \tag{4}$$

Note that Eqs. (3) and (4) provide a general way to describe any DoS attack on an infinite horizon. Based on the above formulation, the DoS attack effect on the communication network can be described as an indicator function, i.e.,

$$\mathbf{1}_\Xi(k) = \begin{cases} 1, \ k \in \Xi(0,\infty), \\ 0, \ k \in \Theta(0,\infty), \end{cases} \tag{5}$$

where $\mathbf{1}_\Xi = 1$ represents the communication channel is blocked and $\mathbf{1}_\Xi = 0$ indicates a successful transmission can be made through this channel.

However, it is practically impossible to evaluate the DoS attack effect on an infinite horizon. Thus, a straightforward concept called the DoS attack duration is adopted, where the DoS attack effect on the communication network can be measured on specific finite horizons (e.g., [8]). For any time interval $[k_0, k) \subset [0,\infty)$, we introduce the following similar notations:

$$\Xi(k_0, k) \triangleq \Xi(0,\infty) \bigcap \mathbb{N}_{[k_0,k)} \tag{6}$$

and

$$\Theta(k_0, k) \triangleq \mathbb{N}_{[k_0,k)} \backslash \Xi(k_0, k), \tag{7}$$

where $k_0 \in \mathbb{N}_{\geqslant 0}, k \in \mathbb{N}_{>0}$ and $k > k_0$.

3 Problem statement

Consider a nonlinear CPS whose dynamics is governed by the following nonlinear discrete-time system:

$$x_{k+1} = f(x_k, u_k) + w_k, \tag{8}$$

where $x_k \in \mathbb{X} \subset \mathbb{R}^n$, $u_k \in \mathbb{U} \subset \mathbb{R}^m$, and $w_k \in \mathbb{W} \subset \mathbb{R}^n$ are the constrained system state, the constrained control input, and the unknown but bounded additive disturbance, respectively. The nonlinear function $f : \mathbb{X} \times \mathbb{U} \mapsto \mathbb{R}^n$ is a continuous mapping with $f(0,0) = 0$, where $\mathbb{X}$ and $\mathbb{U}$ are all compact sets containing the origin.

Assumption 1. For the system in (8), the following condition holds for all $x, z \in \mathbb{X}$ and $u \in \mathbb{U}$:

$$\|f(x,u) - f(z,u)\| \leqslant L_f(\|x - z\|), \tag{9}$$

where L_f is the Lipschitz constant.

The CPS is deployed over a wireless Ethernet-like communication network subject to DoS attacks. The DoS attack can block the information transmission among the CPS components including the remote controller, the actuator and the physical plant. Specifically, we consider DoS attacks occurring at the controller-to-actuator (C-A) communication channel, where the control packets from the remote controller to the actuator can be lost at some time instants. The following assumption from [21] is introduced to characterize DoS attacks in terms of the total attack duration.

Assumption 2. Given the DoS attack induced activation time sequence in (6), there exist two constants $\pi \geqslant 0$ and $\rho \in (0,1)$ such that

$$\operatorname{card}\left(\Xi(k_0,k)\right) = \sum_{i=k_0}^{k} \mathbf{1}_{\Xi}(i) \leqslant \pi + \rho(k-k_0), \tag{10}$$

where $\operatorname{card}\left(\Xi(k_0,k)\right)$ denotes the total duration of DoS attacks between time instants k_0 and k.

Remark 1. Under the configuration of Assumption 2, DoS attacks considered in this paper are allowed to launch at arbitrary time instants. Note that ρ depicts the ratio of the total attack duration in long time intervals, i.e., $\lim\limits_{k\to\infty} \frac{\operatorname{card}(\Xi(k_0,k))}{k-k_0} = \rho$. The other constant π provides an upper bound of duration for consecutive DoS attacks. In addition, by assuming that all the time instants from k_0 to k are affected by DoS attacks, we can obtain the maximum duration of attack as $N_a \triangleq \lceil \pi/(1-\rho) \rceil$.

The control strategy aims at regulating the system state into a small region around the origin in the presence of additive disturbance and DoS attacks that can tamper the C-A communication channel. To fulfill the control objective, an ET-MPC strategy is implemented using an optimization-based controller that computes optimal control and state sequences and an aperiodic scheduling scheme that determines when the system state is sampled and the optimization control problem (OCP) is solved. At each sampling time instant k_j, the cost function of the OCP is defined as

$$J\left(x_{k_j}, \boldsymbol{u}_{k_j}\right) \triangleq \sum_{i=0}^{N_p-1} L(x_{i+k_j|k_j}, u_{i+k_j|k_j}) + V_f(x_{N_p+k_j|k_j}), \tag{11}$$

where N_p is the prediction horizon, x_{k_j} is the state sampled at k_j, $\boldsymbol{u}_{k_j} \triangleq \{u_{k_j|k_j}, u_{1+k_j|k_j}, \ldots, u_{N_p-1+k_j|k_j}\}$ is the control sequence to be determined, $x_{i+k_j|k_j}$ is the ith predicted state, $L : \mathbb{X} \times \mathbb{U} \mapsto \mathbb{R}_{\geqslant 0}$ is the stage cost function, and $V_f : \mathbb{X}_f \mapsto \mathbb{R}_{\geqslant 0}$ is the terminal cost function. Note that L and V_f are continuous with $L(0,0) = 0$ and $V_f(0) = 0$.

Problem 1. The objective of this paper is to design an event-triggered robust NMPC law $u_k^{\mathrm{ET}} = \mu_{k-k_j}(x_{k_j})$, which is obtained by minimizing the finite-horizon cost J in (11) and determining the sampling instants k_j with an ETM, such that the following two objectives are met: (1) the designed control law can stabilize the system in (8) subject to DoS attacks and additive disturbances; (2) the proposed ETM should ensure that not only the communication consumption is reduced but also the operational normalcy is maintained at all time instants despite DoS attacks.

Remark 2. Due to vulnerability of wireless Ethernet-like communication networks, the CPS information flowing among components of the CPS (e.g., the sensor, the actuator, and the remote controller) can be tampered with by malicious DoS attacks. In such case, the control signal updates will be transmitted over erasure communication channels such that the controlled system cannot get the control signals from the remote controller at some time instants. Therefore, when the system in (8) is under DoS attacks, the actual applied control law will be inevitably affected by DoS attacks (e.g., some control signals have to be zero or kept with zero-order-hold), which will often cause severe adverse effects such as significant control performance degradation or even system destabilization.

4 Event-triggered NMPC under DoS attacks

In this section, we propose an ET-MPC framework under DoS attacks (see Figure 1). Firstly, the MPC optimization problem is designed using a new robustness constraint, where the optimal solutions (i.e., the optimal control sequence and optimal state sequence) can be computed in the cyber layer and sent to the actuator via a communication network. Secondly, the packet transmission strategy is presented, where the dynamic buffer mechanism is introduced to compensate the adverse effect induced by DoS attacks.

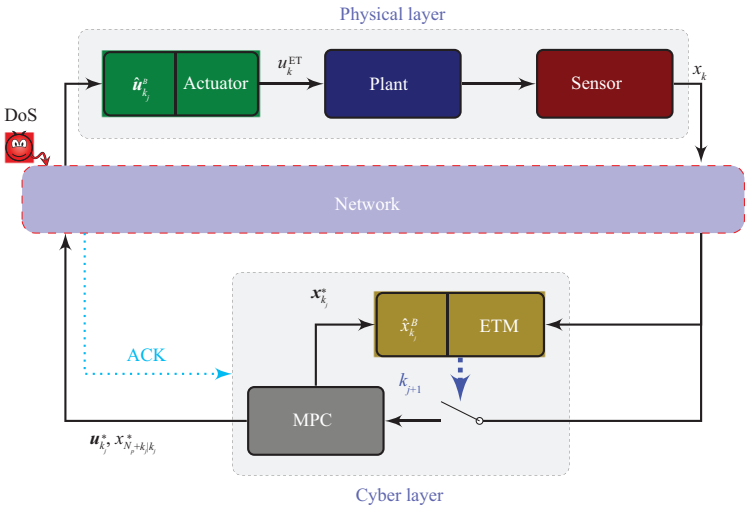

Figure 1 (Color online) The ET-MPC scheme under DoS attacks. The physical layer consists of the plant, the actuator and the sensor. The cyber layer includes the MPC controller and the ETM. Two dynamic buffers are located respectively in the actuator and the ETM in order to provide real-time control signals and the reference states.

Based on the optimal solutions, there are two dynamic buffers respectively generated at the actuator side and the ETM side. Thirdly, the ETM is designed by continuously checking the discrepancy between the real state and the reference state from the ETM buffer, which aims at reducing the communication power consumption. Finally, we formulate the explicit control law by using the control signals from the actuator buffer.

4.1 Constrained optimization problem

For the nonlinear system in (8), the corresponding OCP can be formulated as

$$\boldsymbol{u}_{k_j}^* = \arg\min_{\boldsymbol{u}\in\mathbb{U}^{N_p}} J\left(x_{k_j}, \boldsymbol{u}_{k_j}\right) \tag{12a}$$

$$\text{s.t.} \quad x_{k_j|k_j} = x_{k_j}, \tag{12b}$$

$$x_{i+1+k_j|k_j} = f(x_{i+k_j|k_j}, u_{i+k_j|k_j}), \tag{12c}$$

$$x_{i+k_j|k_j} \in \left(1 - \frac{i}{N_p}\zeta\right)\mathbb{X}, \tag{12d}$$

$$u_{i+k_j|k_j} \in \mathbb{U},\ i \in \mathbb{N}_{[0,N_p)}, \tag{12e}$$

$$x_{N_p+k_j|k_j} \in \xi\mathbb{X}_f, \tag{12f}$$

where $\mathbb{U}$ is the control constraint, $\mathbb{X}$ is the state constraint, $\xi\mathbb{X}_f$ is the terminal constraint, and $\zeta, \xi \in (0,1)$ are scaling parameters for the robustness constraint in (12d) and terminal constraint. It is worth noting that we require the proper design for ζ such that $\mathbb{X}_f \subset (1-\zeta)\mathbb{X}$, since the robustness constraint needs to obey the terminal constraint. In addition, we also have $\|\xi\mathbb{X}_f\| = \xi\|\mathbb{X}_f\|$. By solving the OCP at k_j, we obtain the optimal control sequence and the optimal state sequence as $\boldsymbol{u}_{k_j}^* \triangleq \{u_{k_j|k_j}^*, u_{1+k_j|k_j}^*, \ldots, u_{N_p-1+k_j|k_j}^*\}$ and $\boldsymbol{x}_{k_j}^* \triangleq \{x_{k_j|k_j}^*, x_{1+k_j|k_j}^*, \ldots, x_{N_p+k_j|k_j}^*\}$, respectively. Note that the OCP can be efficiently solved by using a direct multiple shooting method, where all the elements in the above two sequences are treated as decision variables.

4.2 Packet transmission strategy

At each sampling instant k_j, the MPC controller generates an optimal control sequence $\boldsymbol{u}_{k_j}^*$ with appropriately chosen prediction horizon N_p. Then, this control sequence will be sent to the actuator through the C-A channel. The sequence transmission is implemented by using a TCP-like protocol, which can send back an acknowledgement (ACK) signal to the MPC controller if a successful transmission is verified [33]. In other words, the controller can always know, in real-time, whether its current transmission to the actuator is successful or not via the TCP-like protocol.

In order to deal with packet dropouts induced by DoS attacks, we propose to use a dynamic buffer mechanism aiming to not only generate the real-time control signal for the actuator but also generate the reference state for the ETM. How the mechanism works with the actuator and the ETM will be introduced later in Subsections 4.3 and 4.4. Before that, we give the detailed explanation of the proposed buffer mechanism. In the mechanism, there are two dynamic buffers (i.e., $\hat{\boldsymbol{u}}^B_{k_j}$ and $\hat{\boldsymbol{x}}^B_{k_j}$) designed using the optimal control and state sequences obtained by solving OCP at k_j. Specifically, $\hat{\boldsymbol{u}}^B_{k_j}$ is designed for generating real-time control signals, where each of its component is

$$\hat{u}^B_{k|k_j} = \begin{cases} u^*_{k|k_j}, & \text{if } k \in \mathbb{N}_{[k_j, N_p+k_j)}, \\ \kappa_f(\hat{x}_{k|k_j}), & \text{if } k \in \mathbb{N}_{[N_p+k_j, \infty)}. \end{cases} \tag{13}$$

$\hat{\boldsymbol{x}}^B_{k_j}$ is designed for generating reference states to ETM, where each of its component is

$$\hat{x}^B_{k|k_j} = \begin{cases} x^*_{k|k_j}, & \text{if } k \in \mathbb{N}_{[k_j+1, N_p+1+k_j)}, \\ \hat{x}_{k|k_j}, & \text{if } k \in \mathbb{N}_{[N_p+1+k_j, \infty)}. \end{cases} \tag{14}$$

Note that the dynamic model $\hat{x}_{k+1|k_j} = f(\hat{x}_{k|k_j}, \kappa_f(\hat{x}_{k|k_j}))$, $\forall k \in \mathbb{N}_{[N_p+k_j,\infty)}$ with $\hat{x}_{N_p+k_j|k_j} \triangleq x^*_{N_p+k_j|k_j}$ has been used, where κ_f is the terminal control law defined in Assumption 3. At any time instant $k \in \mathbb{N}_{[k_j,\infty)}$, the dynamic buffers are able to generate corresponding signals (i.e., $\hat{u}^B_{k|k_j}$ and $\hat{x}^B_{k|k_j}$), thanks to the dynamic model used in constructing these two buffers.

Remark 3. Different from the conventional buffer mechanisms in [29,33,34], we apply a dynamic one, where the real-time control signal is generated based on the latest received optimal control sequence and the terminal control law. Specifically, the conventional buffers have fixed sizes subject to the prediction horizon N_p because they only use the optimal control sequence, while our proposed buffers have varying sizes since they supplement the optimal control sequence with dynamically generated control signals. Therefore, there could be still control signals generated at the actuator side even if the time interval between the current time instant and the last sampling instant is larger than the prediction horizon. This feature of the dynamic buffer is important to deal with DoS attacks since DoS attacks may tamper the communication channel such that the sampling interval can exceed the prediction horizon.

4.3 Resilient event-triggering condition

In order to alleviate the communication load and reduce the network transmission, an event-triggered scheduler is introduced to determine the sampling instants $\{k_0, k_1, \ldots, k_j, \ldots\}, j \in \mathbb{N}$ at which the optimization problem will be solved and consequently the control packets will be transmitted. The ETM receives the ACK signal, the measured system state and the reference state from the dynamic buffer. Based on the above formulation, the triggering condition can be designed as

$$k_{j+1} = \inf\left\{k \in \Theta(k_j+1, \infty) : \|x_k - \hat{x}^B_{k|k_j}\| \geqslant \sigma\right\}, \tag{15}$$

where σ is the triggering level to be designed. Due to the presence of DoS attacks, an additional condition, i.e., $k_{j+1} \in \Theta(k_j+1, \infty)$, is applied for guaranteeing that the control input sequence can be successfully transmitted. This condition ensures that the sampling instants are not being attacked by DoS and the minimum sampling interval is larger than one.

Compared with the conventional periodic sampling scheme, the aperiodic setting provides more flexibility on avoiding unnecessary control updates, especially for the case when the computationally demanded OCP (12) has to be frequently solved. Similar event-triggering conditions can be found in [14,15]. However, unlike the existing mechanisms, our ETM does not enforce an explicit upper bound between two consecutive sampling instants k_{j+1} and k_j, which can potentially produce larger triggering intervals such that more communicational resources can be saved.

Remark 4. The main difference between self-triggered mechanism (STM) and ETM is that ETM needs to continuously check the system state in order to generate the next triggered time instant, whereas STM determines the next triggered time instant based on the current state. That is to say, the triggered time instant k_j generated by ETM is a function of real system state (i.e., x_k), while the one generated by STM is a function of last sampled system state (i.e., $x_{k_{j-1}}$). Therefore, STM can potentially reduce more

communication power consumption compared with ETM. However, it may not be a very good choice to use STM when the DoS attack is present. This is because the DoS attack may occur between the triggered time instants. STM cannot handle this behavior since it lacks the proactive state measuring capability like ETM. Although STM may provide better network performance, we use ETM in order to deal with DoS attacks.

4.4 Explicit control law

Based on the MPC optimization problem, the buffer mechanism and the resilient event-triggering condition, the resultant control law can be written as

$$u_k^{\mathrm{ET}} \triangleq \hat{u}_{k|k_j}^B, \quad k \in \mathbb{N}_{[k_j,k_{j+1})}, \tag{16}$$

where $\{k_0, k_1, \ldots, k_j, \ldots\}$ denotes all the triggered time instants generated by (15). Then the closed-loop system can be formally given by

$$x_{k+1} = f(x_k, u_k^{\mathrm{ET}}) + w_k, \quad k \in \mathbb{N}_{[k_j,k_{j+1})}. \tag{17}$$

For a clear view of the event-triggered robust NMPC framework, we provide the detailed procedures as shown in Algorithm 1.

Algorithm 1 Event-triggered robust NMPC under DoS attacks

Input: Initial state x_0; the DoS attack satisfying (10); the time instant $k = k_0 = 0$; $j = 0$; the terminal control law κ_f.

repeat
  Sample the system state at k_j and solve OCP at k_j;
  Construct the dynamic buffers $\hat{\boldsymbol{u}}_{k_j}^B$ and $\hat{\boldsymbol{x}}_{k_j}^B$ according to (13) and (14);
  while The condition in (15) is not triggered **do**
    Apply $\hat{u}_{k|k_j}^B$ to the system in (8);
    $k = k + 1$;
  end while
  Obtain the next triggered time instant k_{j+1} using (15);
  $j = j + 1$;
until The control objective is achieved.

Remark 5. Through the proposed elaborate design of the ET-MPC scheme, the negative effect arising from the DoS attack can be significantly and proactively alleviated. In this scheme, we develop two strategies for dealing with DoS attacks. (1) The first one is the packet transmission strategy based on optimal control and predicted state sequences obtained by solving MPC optimization problem. Using this strategy, we can design two dynamic buffers that can not only generate the real-time control signals to the actuator but also generate the reference states to ETM. In particular, these two buffers can be generated via the dynamic model in order to tackle DoS attacks. (2) The second one is the resilient event-triggering condition based on checking the discrepancy between the real state and the reference state. In this condition, we apply the dynamic buffer to the ETM in order to deal with DoS attacks. Besides, by using the dynamic buffer, we can also remove the explicit upper bound of the triggered sampling interval, which is able to save more communication resources compared with existing ETMs. Thanks to these two proposed strategies, the proposed robust NMPC can achieve better performance, compared with the case of applying conventional ET-MPC.

5 Theoretical analysis

In this section, we first derive sufficient conditions for ensuring the recursive feasibility of OCP (12). Then, the closed-loop stability in the sense of ISpS is investigated for the closed-loop system in the presence of DoS attacks and additive disturbance. Before proceeding, we show some important properties of the ETM in the following lemma.

Lemma 2. Suppose that Assumptions 1 and 2 hold. Given the ETM (15) and the DoS attack duration constraint (10), the following two statements hold true.

(a) The time interval between any two consecutive triggered time instants k_{j+1} and k_j satisfies

$$\inf_{j\in\mathbb{N}}\{k_{j+1}-k_j\}\geqslant\begin{cases}\frac{\ln(\sigma(L_f-1)/\|\mathbb{W}\|+1)}{\ln(L_f)}, & \text{if } L_f\neq 1,\\ \frac{\sigma}{\|\mathbb{W}\|}, & \text{if } L_f=1.\end{cases}\tag{18}$$

(b) The difference between the actual state $x_{k_{j+1}}$ and the reference state $\hat{x}^B_{k_{j+1}|k_j}$ is upper bounded as follows:

$$\sup_{j\in\mathbb{N}}\{\|x_{k_{j+1}}-\hat{x}^B_{k_{j+1}|k_j}\|\}\leqslant L_f^{N_a+1}\sigma+\sum_{i=0}^{N_a}L_f^i\|\mathbb{W}\|,\tag{19}$$

where $N_a\triangleq\lceil\pi/(1-\rho)\rceil$.

Proof. Without loss of generality, we consider the two state trajectories (i.e., the real state trajectory x_k and the reference state trajectory $\hat{x}^B_{k|k_j}$) on the time interval between any two consecutive triggered time instants k_j and k_{j+1}. By solving OCP at k_j, one can get an optimal control sequence $\boldsymbol{u}^*_{k_j}$ and its corresponding optimal state trajectory $\boldsymbol{x}^*_{k_j}$. From the buffer mechanisms, we can have $\hat{x}^B_{k+1|k_j}=f(\hat{x}^B_{k|k_j},\hat{u}^B_{k|k_j})$. Because we apply the control input signals stored in $\hat{\boldsymbol{u}}^B_{k_j}$ to the plant, the real state trajectory evolves as $x_{k+1}=f(x_k,\hat{u}^B_{k|k_j})+w_k$, where $w_k\in\mathbb{W}$.

Then we show the first result by investigating the error between the real state trajectory x_k and the reference state trajectory $\hat{x}^B_{k|k_j}$ on $k\in\mathbb{N}_{[k_j+1,k_{j+1})}$. With the help of Lipschitz continuity, one can have

$$\begin{aligned}&\|x_k-\hat{x}^B_{k|k_j}\|\\&\quad\leqslant\|f(x_{k-1},\hat{u}^B_{k-1|k_j})-f(\hat{x}^B_{k-1|k_j},\hat{u}^B_{k-1|k_j})\|+\|w_{k-1}\|\\&\quad\leqslant L_f\|x_{k-1}-\hat{x}^B_{k-1|k_j}\|+\|\mathbb{W}\|\\&\quad\leqslant L_f^{k-k_j-1}\|x_{k_j}-\hat{x}^B_{k_j|k_j}\|+\cdots+L_f\|\mathbb{W}\|+\|\mathbb{W}\|\\&\quad\leqslant\sum_{i=0}^{k-k_j-1}L_f^i\|\mathbb{W}\|.\end{aligned}$$

Combining the triggering condition (15) with the above inequality yields

$$\frac{L_f^{k_{j+1}-k_j}-1}{L_f-1}\|\mathbb{W}\|\geqslant\sigma$$

for $L_f\neq 1$, and

$$(k_{j+1}-k_j)\|\mathbb{W}\|\geqslant\sigma$$

for $L_f=1$. From the above inequalities, we can obtain (18).

To prove the second result in (19), we use contradiction. Suppose that k_j and k_{j+1} are a pair of two consecutive triggered time instants such that Eq. (19) does not hold. Due to Lipschitz continuity, one can obtain

$$\|x_{k_{j+1}}-\hat{x}^B_{k_{j+1}|k_j}\|\leqslant L_f^{N_a+1}\|x_{k_{j+1}-N_a-1}-\hat{x}^B_{k_{j+1}-N_a-1|k_j}\|+\sum_{i=0}^{N_a}L_f^i\|\mathbb{W}\|.$$

Since we assume that Eq. (19) does not hold, it follows

$$\left\|x_{k_{j+1}-N_a-1}-\hat{x}^B_{k_{j+1}-N_a-1|k_j}\right\|>\sigma.$$

Then there must exist another triggered time instant between k_j and k_{j+1}. However, this contradicts the fact that k_j and k_{j+1} are consecutive triggered time instants. Therefore, we have proven that the condition in (19) holds.

Remark 6. It is worth pointing out that $k_{j+1}-k_j$ can be larger than N_p due to the specific design of our ETM. This leads to the major difference of our ETM in (15) compared with the other existing ETM designs for MPC [14, 15]. The existing ETMs explicitly add an upper bound for the sampling interval between k_{j+1} and k_j, which leads to sampling intervals smaller than that of our ETM. In general, smaller sampling intervals reveal worse network performance since more frequent communication will be required. Although this unique feature of the proposed ETM is initially developed for tackling DoS attacks, it can be more effective than the existing ETMs in terms of communication reduction.

5.1 Recursive feasibility analysis

In order to analyze the recursive feasibility of the proposed MPC algorithm, we firstly formulate a candidate control sequence:

$$\tilde{\boldsymbol{u}}_{k_{j+1}} \triangleq \{\tilde{u}_{k_{j+1}|k_{j+1}}, \tilde{u}_{1+k_{j+1}|k_{j+1}}, \ldots, \tilde{u}_{N_p-1+k_{j+1}|k_{j+1}}\}$$

and its corresponding candidate state sequence:

$$\tilde{\boldsymbol{x}}_{k_{j+1}} \triangleq \{\tilde{x}_{k_{j+1}|k_{j+1}}, \tilde{x}_{1+k_{j+1}|k_{j+1}}, \ldots, \tilde{x}_{N_p+k_{j+1}|k_{j+1}}\}.$$

Specifically, we have

$$\tilde{u}_{k|k_{j+1}} \triangleq \begin{cases} \hat{u}^B_{k|k_j}, & \text{if } k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}, \\ \kappa_f(\tilde{x}_{k|k_j}), & \text{if } k \in \mathbb{N}_{[N_p+k_j,N_p+k_{j+1})}, \end{cases} \tag{20}$$

where $\tilde{\boldsymbol{x}}_{k_{j+1}}$ can be obtained by injecting $\tilde{\boldsymbol{u}}_{k_{j+1}}$ into the nominal system dynamics, i.e.,

$$\tilde{x}_{k+1|k_{j+1}} = f(\tilde{x}_{k|k_{j+1}}, \tilde{u}_{k|k_{j+1}}) \tag{21}$$

and $\tilde{x}_{k_{j+1}|k_{j+1}} = x_{k_{j+1}}$. Note that the similar formulations have been widely used to prove the recursive feasibility and stability, e.g., [14, 15].

The following conventional important notations and hypotheses for NMPC are introduced.

Assumption 3. There exist a function $\kappa_f : \mathbb{R}^n \mapsto \mathbb{R}^m$ with $\kappa_f(0) = 0$, $\alpha_L, \bar{\alpha}_{V_f}, \underline{\alpha}_{V_f}, \alpha_{N_p} \in \mathcal{K}_\infty$, and a set $\mathbb{X}_f \subseteq \mathbb{X}$ containing origin such that

$$L(x,u) \geqslant \alpha_L(\|x\|), \ \ \forall x \in \mathbb{X}, u \in \mathbb{U}, \tag{22}$$

$$\underline{\alpha}_{V_f}(\|x\|) \leqslant V_f(x) \leqslant \bar{\alpha}_{V_f}(\|x\|), \ \ \forall x \in \mathbb{X}_f, \tag{23}$$

$$\kappa_f(x) \in \mathbb{U}, \ \ f(x,\kappa_f(x)) \in \mathbb{X}_f, \ \ \forall x \in \mathbb{X}_f, \tag{24}$$

$$V_f(f(x,\kappa_f(x))) - V_f(x) \leqslant -L(x,\kappa_f(x)), \ \ \forall x \in \mathbb{X}_f, \tag{25}$$

$$\left|V_{N_p}(x) - V_{N_p}(z)\right| \leqslant \alpha_{N_p}(\|x-z\|), \ \ \forall x,z \in \mathbb{X}, \tag{26}$$

where L is the stage cost function, V_f is the terminal cost function, and $V_{N_p}(x) \triangleq J(x,\boldsymbol{u}^*(x))$ is the optimal value function used throughout this paper defined using the OCP in (12).

The conditions (22)–(25) in Assumption 3 are necessary for proving stability for general nonlinear MPC formulations [35]. It is also worth noting that continuity of the optimal value function in (26) is often used to show robust stability of nonlinear CPSs with constraints, e.g., [34].

Before presenting the main theoretical results, the following assumption for the initial feasibility is introduced.

Assumption 4 (Initially feasible region)**.** There exists an initially feasible region $\mathbb{X}_N \subseteq \mathbb{X}$ such that for all $x_0 \in \mathbb{X}_N$ the OCP in (12) admits a feasible solution with its initial value being x_0.

Due to the formulation of the candidate control sequence in (20), the control input constraint in the OCP is trivially satisfied. Then, to establish the recursive feasibility, it is equivalent to showing that $\tilde{\boldsymbol{x}}_{k_{j+1}}$ obeys the state constraint and enters the terminal set under Assumption 4.

Lemma 3. For the system in (8) under DoS attacks satisfying duration constraints in (10), suppose that Assumptions 1–4 hold. The OCP (12) is recursively feasible at the triggered time instant k_j generated by the proposed ETM (15) if the following conditions are satisfied:

$$L_f^{(1-\beta)N_p}\left(\sum_{i=0}^{N_a} L_f^i\|\mathbb{W}\| + L_f^{N_a+1}\sigma\right) \leqslant \max\left\{\zeta\|\mathbb{X}\|, (1-\xi)\|\mathbb{X}_f\|\right\}, \tag{27}$$

$$N_p \geqslant \frac{\overline{\alpha}_{V_f}(\|\mathbb{X}_f\|) - \underline{\alpha}_{V_f}(\xi\|\mathbb{X}_f\|)}{\beta\alpha_L(\xi\|\mathbb{X}_f\|)}, \tag{28}$$

where

$$\beta \triangleq \left\lfloor \frac{\ln\left(\sigma(L_f-1)/\|\mathbb{W}\|+1\right)}{\ln(L_f)} + 1 \right\rfloor / N_p. \tag{29}$$

Proof. Without loss of generality, we start the analysis by assuming that there exists an optimal solution $\boldsymbol{u}^*_{k_j}$ at the last triggered time instant k_j. According to (13), the control signal from the actuator-side buffer can be constructed as $\hat{u}^B_{k|k_j}$. Then we will inspect $\tilde{\boldsymbol{x}}_{k_{j+1}}$ on the time interval between k_{j+1} and $N_p + k_{j+1}$. To show recursive feasibility, it is equivalent to proving that $\tilde{\boldsymbol{x}}_{k_{j+1}}$ fulfills:

(C1) the tightened state constraint, i.e., $\tilde{x}_{k|k_{j+1}} \in \zeta(1-(k-k_{j+1})/N_p)\mathbb{X}$, $\forall k \in \mathbb{N}_{[k_{j+1},N_p+k_{j+1})}$;

(C2) the terminal constraint, i.e., $\tilde{x}_{N_p+k_{j+1}|k_{j+1}} \in \xi\mathbb{X}_f$.

Case 1: $k_{j+1} < k_j + N_p$. In this case, we need to establish the conditions such that: (1) the candidate state $\tilde{x}_{k|k_{j+1}}$ enters $\mathbb{X}_f$ at $k = k_j + N_p$ and satisfies (C1) for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$; (2) the candidate state satisfies (C1) for $k \in \mathbb{N}_{[N_p+k_j,N_p+k_{j+1})}$ and finally enters $\xi\mathbb{X}_f$ (C2).

For $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$, we take an error term $\|\tilde{x}_{k|k_{j+1}} - \hat{x}^B_{k|k_j}\|$ to illustrate that the candidate state satisfies both (C1) and $\tilde{x}_{N_p+k_j|k_{j+1}} \in \mathbb{X}_f$. At the current triggered time instant k_{j+1} that is generated by the ETM in (14), we have $\tilde{x}_{k_{j+1}|k_{j+1}} = x_{k_{j+1}}$. Then using (19) in Lemma 2 and the Lipschitz continuity by Assumption 1, one can obtain

$$\left\|\tilde{x}_{k|k_{j+1}} - \hat{x}^B_{k|k_j}\right\| \leqslant L_f^{k-k_{j+1}}\bar{\sigma}$$

for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$. Note that we use a notation $\bar{\sigma} = L_f^{N_a+1}\sigma + \sum_{i=0}^{N_a} L_f^i\|\mathbb{W}\|$ for ease of exposition. Applying the triangle inequality to the above inequality yields

$$\|\tilde{x}_{k|k_{j+1}}\| \leqslant \|\hat{x}^B_{k|k_j}\| + L_f^{k-k_{j+1}}\bar{\sigma}. \tag{30}$$

In order to satisfy the tightened state constraint, we require

$$\|\tilde{x}_{k|k_{j+1}}\| \leqslant \left(1 - \frac{k-k_{j+1}}{N_p}\zeta\right)\|\mathbb{X}\|$$

for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$. Since $\|\hat{x}^B_{k|k_j}\| \leqslant (1-\frac{k-k_j}{N_p}\zeta)\|\mathbb{X}\|$, by combining the above two equations with (30), one can obtain

$$\left(1 - \frac{k-k_j}{N_p}\zeta\right)\|\mathbb{X}\| + L_f^{k-k_{j+1}}\bar{\sigma} \leqslant \left(1 - \frac{k-k_{j+1}}{N_p}\zeta\right)\|\mathbb{X}\|,$$

which consequently reveals

$$L_f^{k-k_{j+1}}\bar{\sigma} \leqslant \frac{\zeta(k_{j+1}-k_j)}{N_p}\|\mathbb{X}\| \leqslant \zeta\|\mathbb{X}\|.$$

Note from Lemma 2 that $k_{j+1} - k_j \geqslant \beta N_p$. Applying this fact into the above inequality, one can obtain

$$L_f^{(1-\beta)N_p}\bar{\sigma} \leqslant \zeta\|\mathbb{X}\|. \tag{31}$$

To show $\tilde{x}_{N_p+k_j|k_{j+1}} \in \mathbb{X}_f$, by following a similar reasoning, we have

$$\left\|\hat{x}^B_{N_p+k_j|k_j}\right\| + L_f^{(1-\beta)N_p}\bar{\sigma} \leqslant \|\mathbb{X}_f\|.$$

From the OCP in (12) and the buffer design, we can know $\hat{x}^B_{N_p+k_j|k_j} \in \xi\mathbb{X}_f$. To ensure that $\tilde{x}_{N_p+k_j|k_{j+1}}$ is driven into $\mathbb{X}_f$, the following condition needs to be satisfied:

$$L_f^{(1-\beta)N_p}\bar{\sigma} \leqslant (1-\xi)\|\mathbb{X}_f\|. \tag{32}$$

Combining the two conditions (31) and (32), we can obtain (27) such that the tightened state constraint satisfaction is guaranteed for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$ and $\tilde{x}_{N_p+k_j|k_{j+1}} \in \mathbb{X}_f$.

For $k \in \mathbb{N}_{[N_p+k_j, N_p+k_{j+1})}$, it can be seen from Assumption 3 that

$$V_f(\tilde{x}_{k+1|k_{j+1}}) - V_f(\tilde{x}_{k|k_{j+1}}) \leqslant -L(\tilde{x}_{k|k_{j+1}}, \kappa_f(\tilde{x}_{k|k_{j+1}})) \leqslant -\alpha_L(\|\tilde{x}_{k|k_{j+1}}\|).$$

Note that the tightened state constraint (C1) is satisfied because $\mathbb{X}_f$ is an invariant set for (21) and $\mathbb{X}_f \subset (1-\zeta)\mathbb{X}$. In addition, we need to show the terminal constraint satisfaction, i.e., $\tilde{x}_{N_p+k_{j+1}|k_{j+1}} \in \xi\mathbb{X}_f$. In order to achieve this, it needs to satisfy the following inequality:

$$V_f(\tilde{x}_{N_p+k_{j+1}|k_{j+1}}) \leqslant V_f(\tilde{x}_{N_p+k_j|k_{j+1}}) - \sum_{k=N_p+k_j}^{N_p-1+k_{j+1}} \alpha_L(\|\tilde{x}_{k|k_{j+1}}\|) \leqslant V_f(\xi\|\mathbb{X}_f\|).$$

Then using (22) and (23) in Assumption 3, the following inequality can be obtained:

$$\overline{\alpha}_{V_f}(\|\mathbb{X}_f\|) - \beta N_p \alpha_L(\xi\|\mathbb{X}_f\|) \leqslant \underline{\alpha}_{V_f}(\xi\|\mathbb{X}_f\|), \tag{33}$$

which can guarantee that the candidate state enters the terminal constraint set. As a result, we can readily establish the condition in (28), from (33), such that the candidate state enters $\xi\mathbb{X}_f$ at $k = k_{j+1} + N_p$.

Case 2: $k_{j+1} \geqslant k_j + N_p$. Recalling the dynamic buffer design, the reference state trajectory after N_p steps remains inside $\xi\mathbb{X}_f$ due to (25) in Assumption 3, i.e., $\hat{x}^B_{k_{j+1}|k_j} \in \xi\mathbb{X}_f$. In order to satisfy both (C1) and (C2), we need to construct a candidate state sequence $\tilde{\boldsymbol{x}}_{k_{j+1}}$ in which the first component $\tilde{x}_{k_{j+1}|k_{j+1}}$ is inside $\mathbb{X}_f$ and the last component $\tilde{x}_{k_{j+1}+N_p|k_{j+1}}$ enters $\xi\mathbb{X}_f$. To achieve this objective, we should have

$$\|\tilde{x}_{k_{j+1}|k_{j+1}}\| \leqslant \|\hat{x}^B_{k_{j+1}|k_j}\| + \bar{\sigma} \leqslant \|\mathbb{X}_f\|,$$

which shows

$$\bar{\sigma} \leqslant (1-\xi)\|\mathbb{X}_f\|. \tag{34}$$

Then following a similar procedure in Case 1, one can obtain

$$\overline{\alpha}_{V_f}(\|\mathbb{X}_f\|) - N_p \alpha_L(\xi\|\mathbb{X}_f\|) \leqslant \underline{\alpha}_{V_f}(\xi\|\mathbb{X}_f\|), \tag{35}$$

such that $\tilde{x}_{k_{j+1}+N_p|k_{j+1}} \in \xi\mathbb{X}_f$.

By combining (31)–(35), we can conclude that the OCP is recursively feasible if the conditions (27) and (28) are satisfied.

Remark 7. When choosing the terminal cost function V_f and the stage cost function L as quadratic functions such as $x^{\mathrm{T}}Px$ and $\|x\|^2_Q + \|u\|^2_R$, the $\mathcal{K}_\infty$ functions $\underline{\alpha}_{V_f}$ and α_L can be simply obtained as $\underline{\lambda}(P)(\|x\|)$ and $(\overline{\lambda}(Q)+\epsilon)(\|x\|)$. Due to the presence of additive disturbances, the prediction horizon N_p cannot be too large; otherwise the recursive feasibility may not be guaranteed. Besides, the maximum allowable DoS attack duration N_a also affects the recursive feasibility. As long as the actual DoS attack duration is less than N_a, we can always ensure that the proposed robust NMPC algorithm admits feasible solutions at each triggered time instant under the prerequisite of satisfying the established feasibility conditions.

5.2 Input-to-state stability analysis

For the proposed robust NMPC of the nonlinear system subject to disturbances and DoS attacks, we analyze the ISpS of the resulting closed-loop system. Specifically, we will show that the optimal value function $V_{N_p}(x)$ is the Lyapunov function for the closed-loop system. In doing so, the decreasing property of $V_{N_p}(x)$ will be investigated with the help of the candidate control and state sequences introduced in Subsection 5.1.

Theorem 1. Suppose that Assumptions 1–4 hold. If the conditions in Lemma 3 are satisfied, then given any $x_{k_0} \in \mathbb{X}_N$ where k_0 is the first triggered time instant, the closed-loop system in (17) is input-to-state practical stable in the presence of DoS attacks satisfying (10) and additive disturbance.

Proof. To prove the ISpS, we use the optimal value function on the two consecutive triggered time instants, i.e., the upper bound for $V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j})$. In order to achieve this, we introduce an

intermediate value function $V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))$, where $\bar{f}^{i+1}(x_{k_j}) = f(\bar{f}^i(x_{k_j}), \hat{u}^B_{i+k_j|k_j})$ and $\bar{f}^0(x_{k_j}) \triangleq x_{k_j}$. Then $V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j})$ can be rewritten as

$$V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j}) = \left(V_{N_p}(x_{k_{j+1}}) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))\right) + \left(V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j})\right),$$

where the two separated terms will be considered respectively in the following discussion.

Firstly, we consider the term $V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j})$. By using the candidate control and state sequences, one can obtain

$$\begin{aligned}
&V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\
&\leqslant J(\bar{f}^{k_{j+1}-k_j}(x_{k_j}), \tilde{\boldsymbol{u}}_{k_{j+1}}) - V_{N_p}(x_{k_j}) \\
&= \sum_{k=k_{j+1}}^{N_p-1+k_{j+1}} L(\bar{f}^{k-k_j}(x_{k_j}), \hat{u}^B_{k|k_j}) + V_f(\bar{f}^{N_p+k_{j+1}-k_j}(x_{k_j})) - \left(\sum_{k=k_j}^{N_p-1+k_j} L(x^*_{k|k_j}, u^*_{k|k_j}) + V_f(x^*_{N_p+k_j|k_j})\right) \\
&= -\sum_{k=k_j}^{\min\{k_{j+1}, N_p+k_j\}} L(x^*_{k|k_j}, u^*_{k|k_j}) + \sum_{k=\max\{k_{j+1}, N_p+k_j\}}^{N_p-1+k_{j+1}} L(\bar{f}^{k-k_j}(x_{k_j}), \kappa_f(\bar{f}^{k-k_j}(x_{k_j}))) \\
&\quad + V_f(\bar{f}^{N_p+k_{j+1}-k_j}(x_{k_j})) - V_f(x^*_{N_p+k_j|k_j}).
\end{aligned} \tag{36}$$

Now consider two different cases of the above inequality when $k_{j+1} < N_p + k_j$ and $k_{j+1} \geqslant N_p + k_j$. For $k_{j+1} < N_p + k_j$, applying (25) in Assumption 3 and the fact $x^*_{N_p+k_j|k_j} = \bar{f}^{N_p}(x_{k_j})$ to (36) yields

$$\begin{aligned}
&V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\
&\quad\leqslant -\sum_{k=k_j}^{k_{j+1}} L(x^*_{k|k_j}, u^*_{k|k_j}) \\
&\quad\leqslant -L(x^*_{k_j|k_j}, u^*_{k_j|k_j}) \\
&\quad\leqslant -\alpha_L(\|x_{k_j}\|).
\end{aligned} \tag{37}$$

For $k_{j+1} \geqslant N_p + k_j$, we can rewrite (36) as

$$\begin{aligned}
&V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\
&\quad\leqslant -\sum_{k=k_j}^{N_p-1+k_j} L(x^*_{k|k_j}, u^*_{k|k_j}) + \left|V_f(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_f(x^*_{N_p+k_j|k_j})\right| \\
&\quad\leqslant -L(x^*_{k_j|k_j}, u^*_{k_j|k_j}) + \max\{V_f(\bar{f}^{k_{j+1}-k_j}(x_{k_j})), V_f(x^*_{N_p+k_j|k_j})\} \\
&\quad\leqslant -\alpha_L(\|x_{k_j}\|) + \bar{\alpha}_{V_f}(\|\mathbb{X}_f\|).
\end{aligned} \tag{38}$$

Secondly, we investigate the upper bound for the other term $V_{N_p}(x_{k_{j+1}}) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))$. Note that we have $V_{N_p}(x_{k_{j+1}}) = V_{N_p}(f^{k_{j+1}-k_j}(x_{k_j}))$, where $f^{i+1}(x_{k_j}) = f(f^i(x_{k_j}), \hat{u}^B_{i+k_j|k_j}) + w_{i+k_j}$ and $f^0(x_{k_j}) \triangleq x_{k_j}$. In the above equation, $f^{k-k_j}(x_{k_j})$ denotes the real trajectory of the perturbed nonlinear dynamics (8) with the initial state x_{k_j} and the disturbance w_k. Then, we can have

$$\begin{aligned}
&\left|V_{N_p}(x_{k_{j+1}}) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))\right| \\
&\quad= \left|V_{N_p}(f^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))\right| \\
&\quad\leqslant \alpha_{N_p}\left(\|f^{k_{j+1}-k_j}(x_{k_j}) - \bar{f}^{k_{j+1}-k_j}(x_{k_j})\|\right) \\
&\quad\leqslant \alpha_{N_p}(\|f(f^{k_{j+1}-k_j-1}(x_{k_j}), \hat{u}^B_{k_{j+1}-1|k_j}) \\
&\qquad - f(\bar{f}^{k_{j+1}-k_j-1}(x_{k_j}), \hat{u}^B_{k_{j+1}-1|k_j})\| + \|w_{k_{j+1}-1}\|) \\
&\quad\leqslant \alpha_{N_p}(L_f\|f^{k_{j+1}-k_j-1}(x_{k_j}) - \bar{f}^{k_{j+1}-k_j-1}(x_{k_j})\| + \|\mathbb{W}\|) \\
&\quad\leqslant \alpha_{N_p}\left(\sum_{i=0}^{k_{j+1}-k_j-1} L_f^i\|\mathbb{W}\|\right).
\end{aligned} \tag{39}$$

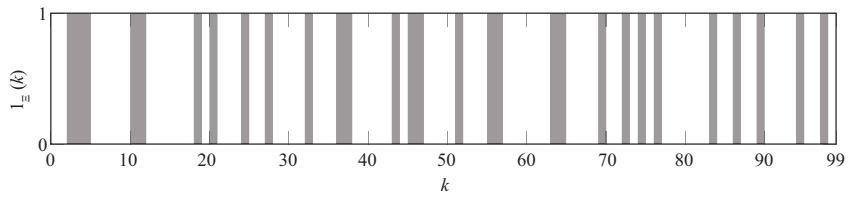

Figure 2 The DoS attack sequence for 100 time steps.

Combining (38) and (39), one can obtain

$$V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j}) \leqslant -\bar{\alpha}(\|x_{k_j}\|) + \bar{\gamma}(\|w\|) + \bar{c}, \tag{40}$$

where $\bar{\alpha} = \alpha_L$, $\bar{\gamma} = \alpha_{N_p} \circ \sum_{i=0}^{k_{j+1}-k_j-1} L_f^i$ and $\bar{c} = \bar{\alpha}_{V_f}(\|\mathbb{X}_f\|) + \alpha_{N_p}(\sum_{i=0}^{k_{j+1}-k_j-1} L_f^i \|\mathbb{W}\|)$. In addition, we have $\alpha_L(\|x\|) \leqslant V_{N_p}(x) \leqslant \alpha_{N_p}(\|x\|)$ by Assumptions 1 and 3. Together with (40), it follows that V_{N_p} is an ISpS-Lyapunov function for the closed-loop system in (17). Summarizing all the above statements, the closed-loop system is input-to-state practical stable in $\mathbb{X}_N$ at the triggered time instant k_j.

6 Simulation results

In this section, we apply the proposed scheme to a CPS-based control application. It includes a remotely-controlled nonlinear cart-damper-spring system, a remote MPC controller, and an Ethernet-like network environment that might be exposed to DoS attacks. The proposed scheme can also be applied to mechatronics systems. The NMPC algorithms are implemented using CasADi [36].

6.1 System model and parameter configuration

The dynamic model of nonlinear cart-damper-spring system is given by

$$\begin{cases} p_{k+1} = p_k + T_c v_k, \\ v_{k+1} = v_k - T_c \dfrac{\tau}{M_c} e^{-p_k} p_k - T_c \dfrac{h_d}{M_c} v_k + T_c \dfrac{u(k)}{M_c} + T_c \dfrac{w(k)}{M_c}, \end{cases}$$

where p_k and v_k denote the cart displacement and the cart velocity, $T_c = 0.2$ s is the sampling period, and the other coefficients represent physical parameters including the cart mass $M_c = 1.25$ kg, the nonlinear factor $\tau = 0.9$ N/m and the damping factor $h_d = 0.42$ Ns/m. The state and control input constraints are respectively given by $\mathbb{X} = \{[p, v]^{\mathrm{T}} | -2 \leqslant p \leqslant 2, -2 \leqslant v \leqslant 2\}$ and $\mathbb{U} = \{u | -1.5 \leqslant u \leqslant 1.5\}$. The DoS attack sequence is depicted in Figure 2, where the maximum attack duration can be identified as $N_a = 3$.

To exploit the proposed event-triggered NMPC algorithm, we first need to tune the OCP parameters. The prediction horizon is set as $N_p = 15$; the stage cost is selected as $L(x, u) = x^{\mathrm{T}} Q x + u^{\mathrm{T}} R u$ where $Q = [0.1, 0.0; 0.0, 0.1]$ and $R = 0.1$; the terminal cost is $V_f(x) = x^{\mathrm{T}} P x$ where $P = [0.1967, 0.0734; 0.0734, 0.1737]$; the terminal law is $\kappa_f(x) = Kx$ where $K = [-0.3169, -1.1566]$; the terminal constraint is defined as $\xi \mathbb{X}_f, \xi = 0.8$ where $\mathbb{X}_f = \{x | x^{\mathrm{T}} P x \leqslant 0.01\}$ is the positively invariant set via the method in [37]; the scaling ratio for the shrinking state constraint is set as $\zeta = 0.2$. The disturbance bound $\|\mathbb{W}\|$ is 0.0312. It is worthwhile to point out that $L, V_f, \kappa_f, \mathbb{X}_f$ fulfill Assumption 3 with $\alpha_L(s) = 0.1(\|s\|)^2$, $\underline{\alpha}_{V_f}(s) = 0.11(\|s\|)^2$, $\overline{\alpha}_{V_f}(s) = 0.26(\|s\|)^2$. Then according to the conditions in Lemma 2, we can configure the triggering level σ as 0.01. It can be verified that the prediction horizon N_p, the triggered level σ, and the scaling parameters for the state constraint and terminal constraint $\zeta, \xi \in (0, 1)$ obey the recursive feasibility conditions given the pre-defined state constraint $\mathbb{X}$, the terminal constraint $\mathbb{X}_f$, the disturbance bound $\|\mathbb{W}\|$, and the DoS attack parameter N_a. The initial state of the system is given as $x_0 = [-1.2, 1.2]$. The total simulation step is configured as $N_{\mathrm{sim}} = 100$.

6.2 Results and comparisons

The simulation results and comparisons with a conventional ET-MPC in [14] are shown in Figure 3, where the state trajectories, control input sequences, and event-triggered intervals are thoroughly compared. Note that we have used the same ET-MPC parameter settings including the OCP parameters and the

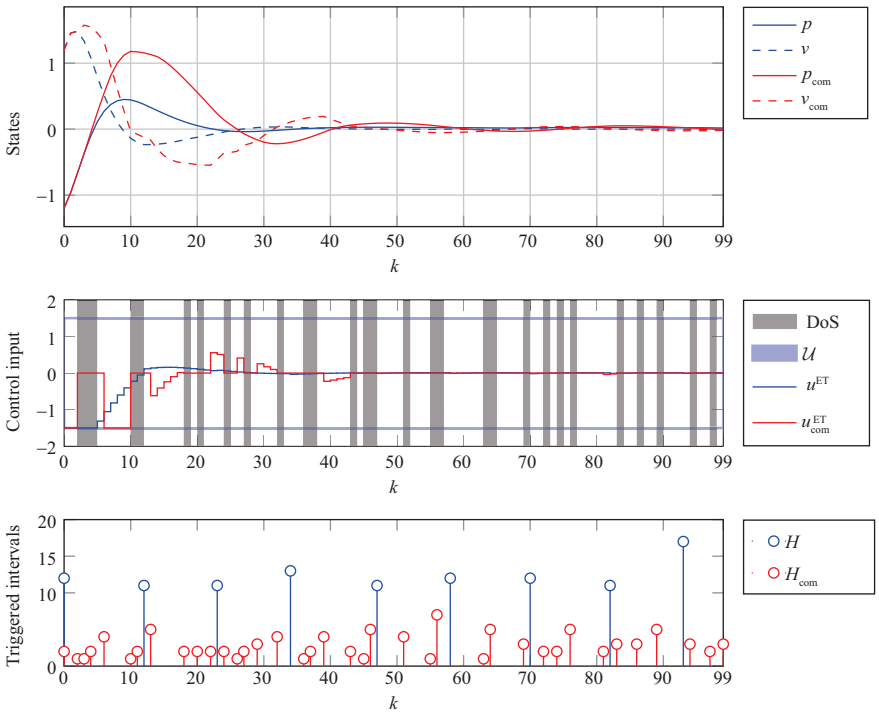

Figure 3 (Color online) The numerical comparisons between our proposed method and the ET-MPC strategy in [14]. The state trajectories (p, v and $p_{\rm com}$, $v_{\rm com}$), control input sequences ($u^{\rm ET}$ and $u^{\rm ET}_{\rm com}$), and event-triggered intervals (H and $H_{\rm com}$) in 100 time steps are respectively shown in the above three subfigures. The blue colored lines represent the results of our work, whereas the red colored lines denote the results of [14].

triggering level when conducting the simulation comparisons. Also, all the comparisons are conducted under the DoS attacks shown in Figure 2 and the same disturbance sequence.

From the first two subfigures in Figure 3, it can be observed that the proposed ET-MPC strategy can not only fulfill the state and control input constraints but also stabilize the closed-loop system despite the existence of DoS attacks and additive disturbances. The last subfigure in Figure 3 illustrates the triggered time instants and intervals generated by the proposed ETM. Note that we have solved OCP and transmitted control packet only on 9 triggered time instants, which can save a lot of communication resource compared with periodic sampling based NMPC. In addition, it can be verified that the triggered intervals satisfy the condition (18) in Lemma 2. Another interesting fact is that our ETM does permit sampling intervals larger than the NMPC prediction horizon, which can further reduce communication cost compared with traditional ETMs in [14, 15].

In order to further compare our proposed method with the one in [14], we introduce two quantitative indices to respectively evaluate its network and control performance. Specifically, we take the average sampling interval ($\frac{N_{\rm sim}}{\text{The Number of Samplings}}$) as the network performance index, and the total cost ($\sum_0^{N_{\rm sim}}(x^{\rm T}Qx + u^{\rm T}Ru)$) as the control performance index. It is worth pointing out that: the larger the average sampling interval is, the better the network performance will be. Then, we can obtain that the network performance index of our method is 11.11 while the one of the comparison work is 2.28, which shows that our method is superior than the comparison work in terms of network performance. It is also worthwhile noting that the last sampling interval of our method is 17, which is larger than the prediction horizon N_p and hence verifies the superiority of our ETM on generating larger sampling intervals. Besides, the simulation comparison also shows that the control performance index of our method (3.01) is better than the one of the comparison work (5.19). In summary, the comparison results have shown that our method has significant advantages over conventional ET-MPC in terms of both the network and control performance.

In the following, we provide a Monte-Carlo simulation in order to show how the proposed ET-MPC strategy behaves under different DoS attacks. The group of different DoS attacks are configured as $N_a = 3, 5, 7, 9$. Under each DoS attack configuration, we conduct 200 different samples of implementing Algorithm 1. Then, we investigate the network and control performance indices as described in the

Table 1 The performance comparison under different DoS attacks

DoS (N_a)	Network performance index	Control performance index
3	13.3733	3.0085
5	13.8014	3.0090
7	14.3713	3.0102
9	15.6394	3.0127

aforementioned. The simulation results are shown in Table 1. As seen in Table 1, the network performance index increases as N_a increases, whereas the control performance index increases very slightly as N_a increases. This interesting result may actually reveal that our proposed resilient ETM contributes more significantly to dealing with DoS attacks. In other words, our proposed ET-MPC tends to sacrifice its network performance to compensate the adverse effect caused by DoS attacks. In addition, the control performance seems to be largely maintained from unreliable communication network without significant performance degradation.

7 Conclusion

We have studied the resilient control problem for resource-aware CPSs under duration-constrained DoS attacks and additive disturbances. An event-triggered robust NMPC framework has been proposed to achieve the resilient and resource-aware control objectives. In particular, we have designed an effective packet transmission strategy and a novel robustness constraint to simultaneously deal with DoS attacks and additive disturbances. The recursive feasibility of the NMPC optimization and ISpS of the resulting closed-loop system have been guaranteed with some sufficient conditions. Finally, the effectiveness of the proposed NMPC strategy has been verified by a nonlinear CPS application example. In the future work, we will apply the event-triggered robust NMPC strategy to a more general case where the DoS attacks occur at both the C-A communication channel and the sensor-to-controller (S-C) communication channel.

References

1 Colombo A W, Karnouskos S, Kaynak O, et al. Industrial cyberphysical systems: a backbone of the fourth industrial revolution. IEEE Ind Electron Mag, 2017, 11: 6–16
2 Khaitan S K, McCalley J D. Design techniques and applications of cyberphysical systems: a survey. IEEE Syst J, 2015, 9: 350–365
3 Cárdenas A A, Amin S, Sastry S. Secure control: towards survivable cyber-physical systems. In: Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, 2008. 495–500
4 Rieger C G, Gertman D I, McQueen M A. Resilient control systems: next generation design research. In: Proceedings of the 2nd Conference on Human System Interactions, Catania, 2009. 632–636
5 Dolk V S, Tesi P, de Persis C, et al. Event-triggered control systems under denial-of-service attacks. IEEE Trans Control Netw Syst, 2017, 4: 93–105
6 Amin S, Cárdenas A A, Sastry S S. Safe and secure networked control systems under denial-of-service attacks. In: Proceedings of the 12th International Conference on Hybrid Systems: Computation & Control, San Francisco, 2009. 31–45
7 Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Automat Contr, 2013, 58: 2715–2729
8 Zhang H, Cheng P, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans Automat Contr, 2015, 60: 3023–3028
9 Zhang D, Feng G, Shi Y, et al. Physical safety and cyber security analysis of multi-agent systems: a survey of recent advances. IEEE/CAA J Autom Sin, 2021, 8: 319–333
10 Zhang D, Wang Q G, Feng G, et al. A survey on attack detection, estimation and control of industrial cyber—physical systems. ISA Trans, 2021, 116: 1–16
11 Zhou C, Hu B, Shi Y, et al. A unified architectural approach for cyberattack-resilient industrial control systems. Proc IEEE, 2021, 109: 517–541
12 Mayne D Q, Rawlings J B, Rao C V, et al. Constrained model predictive control: stability and optimality. Automatica, 2000, 36: 789–814
13 Gommans T M P, Heemels W P M H. Resource-aware MPC for constrained nonlinear systems: a self-triggered control approach. Syst Control Lett, 2015, 79: 59–67
14 Li H, Shi Y. Event-triggered robust model predictive control of continuous-time nonlinear systems. Automatica, 2014, 50: 1507–1513
15 Sun Q, Chen J, Shi Y. Integral-type event-triggered model predictive control of nonlinear systems with additive disturbance. IEEE Trans Cybern, 2020. doi: 10.1109/TCYB.2019.2963141
16 Foroush H S, Martinez S. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In: Proceedings of the 51st IEEE Conference on Decision and Control (CDC), Maui, 2012. 2551–2556
17 Hu S, Yue D, Xie X, et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybern, 2019, 49: 4271–4281

18 Zhu Y, Zheng W X. Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy. IEEE Trans Automat Contr, 2020, 65: 3714–3721
19 de Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Automat Contr, 2015, 60: 2930–2944
20 Feng S, Tesi P. Resilient control under denial-of-service: robust design. Automatica, 2017, 79: 42–51
21 Cetinkaya A, Kikuchi K, Hayakawa T, et al. Randomized transmission protocols for protection against jamming attacks in multi-agent consensus. Automatica, 2020, 117: 108960
22 Liu S, Li S, Xu B. Event-triggered resilient control for cyber-physical system under denial-of-service attacks. Int J Control, 2020, 93: 1907–1919
23 Befekadu G K, Gupta V, Antsaklis P J. Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies. IEEE Trans Automat Contr, 2015, 60: 3299–3304
24 Åström K J, Bernhardsson B. Comparison of Riemann and Lebesgue sampling for first order stochastic systems. In: Proceedings of the 41st IEEE Conference on Decision and Control, Las Vegas, 2002. 2011–2016
25 Tabuada P. Event-triggered real-time scheduling of stabilizing control tasks. IEEE Trans Automat Contr, 2007, 52: 1680–1685
26 Varutti P, Kern B, Faulwasser T, et al. Event-based model predictive control for networked control systems. In: Proceedings of the 48th IEEE Conference on Decision & Control and 28th Chinese Control Conf (CDC/CCC), Shanghai, 2009. 567–572
27 Eqtami A, Dimarogonas D V, Kyriakopoulos K J. Novel event-triggered strategies for model predictive controllers. In: Proceedings of the 50th IEEE Conference on Decision & Control and European Control Conference (CDC/ECC), Orlando, 2011. 3392–3397
28 Lehmann D, Henriksson E, Johansson K H. Event-triggered model predictive control of discrete-time linear systems subject to disturbances. In: Proceedings of European Control Conference (ECC), Zurich, 2013. 1156–1161
29 Sun Q, Zhang K, Shi Y. Resilient model predictive control of cyber-physical systems under DoS attacks. IEEE Trans Ind Inf, 2020, 16: 4920–4927
30 Wang J, Ding B, Hu J. Security control for LPV system with deception attacks via model predictive control: a dynamic output feedback approach. IEEE Trans Automat Contr, 2021, 66: 760–767
31 Sun Y C, Yang G H. Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. Int J Robust Nonlin Control, 2019, 29: 4797–4811
32 Sontag E D, Wang Y. New characterizations of input-to-state stability. IEEE Trans Automat Contr, 1996, 41: 1283–1294
33 Li H, Shi Y. Network-based predictive control for constrained nonlinear systems with two-channel packet dropouts. IEEE Trans Ind Electron, 2014, 61: 1574–1582
34 Quevedo D E, Nesic D. Input-to-state stability of packetized predictive control over unreliable networks affected by packet-dropouts. IEEE Trans Automat Contr, 2011, 56: 370–375
35 Rawlings J B, Mayne D Q. Model Predictive Control: Theory and Design. Madison: Nob Hill Publishing, 2009
36 Andersson J A E, Gillis J, Horn G, et al. CasADi: a software framework for nonlinear optimization and optimal control. Math Prog Comp, 2019, 11: 1–36
37 Li H P, Shi Y. Robust Receding Horizon Control for Networked and Distributed Nonlinear Systems. Berlin: Springer, 2017