Robust Model Predictive Control of Resilient Cyber-Physical Systems: Security and Resource-Awareness

by

Qi Sun
B.Sc., Northwestern Polytechnical University, 2013
M.Sc., Northwestern Polytechnical University, 2016

A Dissertation Submitted in Partial Fulfillment of the
Requirements for

DOCTOR OF PHILOSOPHY

in the Department of Mechanical Engineering

Robust Model Predictive Control of Resilient Cyber-Physical Systems: Security and Resource-Awareness

by

Qi Sun
B.Sc., Northwestern Polytechnical University, 2013
M.Sc., Northwestern Polytechnical University, 2016

Supervisory Committee

Dr. Yang Shi, Supervisor
(Department of Mechanical Engineering)

Dr. Daniela Constantinescu, Departmental Member
(Department of Mechanical Engineering)

Dr. Lin Cai, Outside Member
(Department of Electrical & Computer Engineering)

ABSTRACT

Cyber-physical systems (CPS), integrating advanced computation, communication, and control technologies with the physical process, are widely applied in industry applications such as smart production and manufacturing systems, robotic and automotive control systems, and smart grids. Due to possible exposure to unreliable networks and complex physical environments, CPSs may simultaneously face multiple cyber and physical issues including cyber threats (e.g., malicious cyber attacks) and resource constraints (e.g., limited networking resources and physical constraints). As one of the essential topics in designing efficient CPSs, the controller design for CPSs, aiming to achieve secure and resource-aware control objectives under such cyber and physical issues, is very significant yet challenging. Emphasizing optimality and system constraint handling, model predictive control (MPC) is one of the most widely used control paradigms, notably famous for its successful applications in chemical process industry. However, the conventional MPC methods are not specifically tailored to tackle cyber threats and resource constraints, thus the corresponding theory and tools to design the secure and resource-aware controller are lacking and need to be developed. This dissertation focuses on developing MPC-based methodologies to address the i) secure control problem and ii) resource-aware control problem for CPSs subject to cyber threats and resource constraints.

In the resource-aware control problem of CPSs, the nonlinear system with additive disturbance is considered. By using an integral-type event-triggered mechanism and an improved robustness constraint, we propose an integral-type event-triggered MPC so that smaller sampling frequency and robustness to the additive disturbance can be obtained. The sufficient conditions for guaranteeing the recursive feasibility and the closed-loop stability are established.

For the secure control problem of CPSs, two aspects are considered. Firstly, to achieve the secure control objective, we design a secure dual-mode MPC framework, including a modified initial feasible set and a new positively invariant set, for constrained linear systems subject to Denial-of-Service (DoS) attacks. The exponential stability of the closed-loop system is guaranteed under several conditions. Secondly, to deal with cyber threats and take advantage of the cloud-edge computing technology, we propose a model predictive control as a secure service (MPCaaSS) framework, consisting of a double-layer controller architecture and a secure data transmission protocol, for constrained linear systems in the presence of both cyber threats and ex-

ternal disturbances. The rigorous recursive feasibility and robust stability conditions are established.

To simultaneously address the secure and resource-aware control problems, an event-triggered robust nonlinear MPC framework is proposed, where a new robustness constraint is introduced to deal with additive disturbances, and a packet transmission strategy is designed to tackle DoS attacks. 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. The recursive feasibility and the closed-loop stability in the sense of input-to-state practical stable (ISpS) are guaranteed under the established sufficient conditions.

Table of Contents

List of Tables

List of Figures

List of Acronyms

C-A	Controller-to-actuator.
CPS	Cyber-physical system.
DoS	Denial-of-Service.
DP	Dynamic Programming.
ECC	Elliptic curve cryptography.
ECDLP	Elliptic curve discrete logarithm problem.
ETC	Event-triggered control.
ETM	Event-triggered mechanism.
ET-MPC	Event-triggered model predictive control.
ICS	Industrial control system.
IoT	Internet-of-Things.
ISpS	Input-to-state practical stable.
ISS	Input-to-state stable.
IT	Information technology.
LQG	Linear quadratic Gaussian.
LQR	Linear quadratic regulator.
LTI	Linear time-invariant.

MPC	Model predictive control.
MPCaaSS	Model predictive control as a secure service.
NMPC	Nonlinear model predictive control.
OCP	Optimization control problem.
PID	Proportional integral derivative.
PLC	Programmable logic controller.
RPI	Robust positively-invariant.
RSA	Rivest–Shamir–Adleman.
S-C	Sensor-to-controller.
SCADA	Supervisory control and data acquisition.
STM	Self-triggered mechanism.
ST-MPC	Self-triggered model predictive control.

ACKNOWLEDGEMENTS

First of all, I would like to express my deepest thanks to my supervisor Dr. Yang Shi who has given me his continuous, intensive and patient guidance, encouragement, and support during the last several years. His remarkable knowledge and insightful vision have always steered me in the right research direction; his valuable suggestions to academic problems have inspired me to solve challenging problems; his world-class research taste and passion have directed me to confidently pursue better and higher academic achievements. Dr. Yang Shi is not only a great advisor but also a lifelong mentor to me. He always provided me sincere, timely and selfless assistance whenever I got lost in confusion, has been offering constructive advice to my career development since the beginning of the Ph.D. program, and most importantly has been always teaching me how to become a decent researcher. I hereby greatly appreciate him and feel so fortunate to become his student.

I would like to express my sincere gratitude to the supervisory committee members Dr. Lin Cai and Dr. Daniela Constantinescu, and the external member Dr. Ya-Jun Pan for reviewing this dissertation and providing constructive comments.

I am also very lucky to have had such excellent teammates in the Applied Control and Information Processing Lab at the University of Victoria. I am particularly grateful to Dr. Binxian Mu for his help on experimental software and hardware, to Dr. Chao Shen for the discussions on optimization techniques and tools, to Dr. Yuanye Chen for sharing his experiences on MASs with me, to Dr. Jicheng Chen for his discussions on MPC, and to Dr. Yuan Yang for the discussions on the MAS experiments. I also greatly thank Kunwu Zhang, Qian Zhang, Changxin Liu, Henglai Wei, Tianyu Tan, Xiang Sheng, Xinxin Shang, Yaning Guo, Tianxiang Lu, Binyan Xu, Yufan Dai, Yue Song, Dr. Zhuo Zhang, Dr. Chuixi Yang, Dr. Fengqiu Xu, Dr. Songlin Zhuang, Dr. Kenan Yong, and Dr. Xiaodong Shao for their valuable discussions and comments in the group meetings, which have helped me to come up with some of the greatest ideas and solutions. Those memorable days that we shared together will be one of the most precious memories in all my life.

Finally, I gratefully acknowledge the financial support from the Chinese Scholarship Council, the Natural Science and Engineering Council of Canada, the Mitacs Accelerate Program, the Department of Mechanical Engineering and the Faculty of Graduate Studies at the University of Victoria.

Chapter 1

Introduction

This chapter depicts some introductory information about cyber-physical systems (CPS). Then cyber threats and resource constraints to CPSs are introduced along with the corresponding control objectives for achieving security and resource-awareness. Next, the existing methodologies and state-of-the-art research results on resource-aware and/or secure control are reviewed and categorized. Finally, the thesis outline and contributions are summarized for each thesis work.

1.1 Overview

1.1.1 Cyber-Physical System

CPSs are characterized as a new generation of engineered systems in which the operations for monitoring, coordinating, and controlling the physical process are generated and transmitted by a (remote) computing and communication core. With the rapid development of wireless embedded sensors and actuators, CPSs have been utilized in many emerging applications such as remote medical services, autonomous vehicles, smart grids, and nuclear power plants [1, 2]. As shown in Fig. 1.1, the typical architecture of the CPS framework consists of a physical process and several other components such as distributed sensors, actuators, embedded control units, communication links, etc. Like the World-Wide Web, which enables the world-wide communication through a set of universal communication technologies, CPSs integrate cyber abstractions with engineered systems in order to provide humans a revolutionary way of interacting with and controlling the physical world.

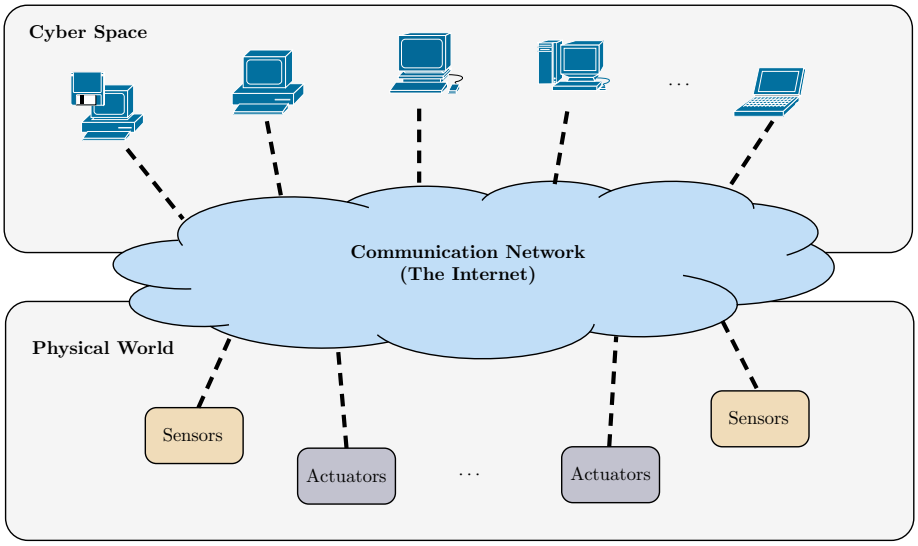

Fig. 1.1: The cyber-physical system architecture.

Control is embedded in many CPSs and has been playing a fundamental role, which particularly benefits from advanced CPS networking technologies in terms of reducing system cost and increasing structural flexibility. However, the integration of physical layers and cyber layers has inevitably made CPS-based control systems confront joint challenges from the physical environment and the cyber space (e.g., disturbances, model uncertainties, resource constraints, and malicious cyber attacks [3]). The presence of these challenges in CPSs may cause severe consequences such as dramatic performance degradation or even system failure [4], and consequently lead to economic and ecological crises [5–7].

1.1.2 Cyber Threats and Resource Constraints

Due to extensive exploitation of wireless communication technologies [8], CPSs are vulnerable to some network-induced issues, e.g., malicious cyber attacks such as denial-of-service (DoS) and deception attacks [9] and resource-constrained networking conditions such as limited bandwidth [10], etc. In addition, the physical environment induced issues such as physical constraints and uncertainties existing widely in physical process may also pose serious threats to CPS-based control applications.

Cyber Threats

Security challenges have grown exponentially when integrating cyber layers to CPS-based control systems [11]. In 2010, the Stuxnet Worm hit centrifuges at a uranium enrichment facility in Iran [12], which infected targets including Windows, industrial control systems (ICS) and programmable logic controllers (PLC) connected to variable-frequency drives. These attacks were delivered with USB stick and can replay the measurements to control center and execute harmful controls. In 2014, it was reported that the attackers targeted several sensitive organizations including the North Atlantic Treaty Organization, Ukrainian and Polish government agencies, and a variety of sensitive European industries. The attack strategy was using booby-trapped macro functions embedded in Microsoft Office documents. These malicious macros can render infected computers unbootable, destroy critical parts of a computer hard drive, and even back-door secure shell (SSH) utility that gave attackers permanent access to infected computers. A more advanced, more autonomous, follow-up attack called "Crash Override" was launched by malicious adversaries in 2016 [13].

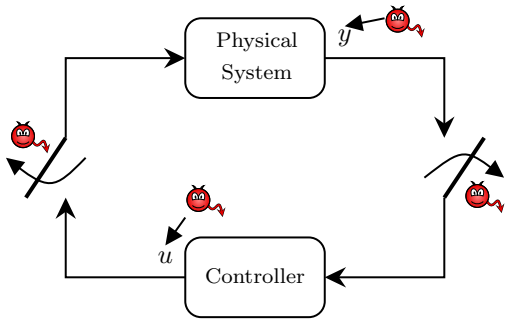

Fig. 1.2: The possible cyber threats.

Various cyber attacks have been reported to threaten the new generation of CPSs under the thriving usage of the Internet infrastructure [11]. According to the exposure of the information and resources to the adversaries, cyber attacks can be classified as either deception attacks or DoS attacks as shown in Fig. 1.2. The former one is usually caused by information disruption, while the latter one implies the unavailability of the necessary communication channel. A detailed explanation of cyber attacks are stated as follows:

- **DoS attacks** are usually rendered as the jamming of communication channels from sensors to controllers, or controllers to actuators. Vicious adversary uses

this type of attack to block the normal communications between these system components. Obviously, DoS attacks can be categorized to the disruption resources attacks. It is also reported that some DoS attacks can also use the model knowledge.

- **Deception attacks** are usually conducted by the adversary through false information injection to communication channels. The false information is usually an incorrect measurement or a series of fake control signals corrupted by the malicious adversary. These attacks can be launched by replacing the corresponding sensor measurements and control sequences with false ones, which might induce the system performance degradation or even the instability of the closed-loop system. Replay attacks are a kind of deception attacks, where the system data is intercepted and stored by the attacker. The stored data can be used to imitate the correct information by the attacker, which can also cause severe damage to the system.

Resource Constraints

CPS-based control systems can also be affected by some resource constraints. Specifically, the integration of the cyber and physical components inevitably causes networking limitations including limited data transmission bandwidth and physical constraints (e.g., control saturation, state constraint). The resource constraints include:

- **Networking limitations** denote insufficient communication resources due to the imperfect communication channel or limited communication bandwidth [14]. Since communication in CPSs is generally realized by data packets transmitted at discrete-time instants, the communication resource can become rather restricted especially when multiple devices share one communication channel.

- **Physical constraints** are usually imposed on the physical process such that the states and control actions of that process fulfill operational safety and actuator saturation [15, 16]. The violation of these constraints may cause damage to the system.

Besides, the other issues such as parametric uncertainties and external disturbances existing widely in physical process also need to be considered for controller design especially in a CPS-based context.

1.1.3 Secure and Resource-Aware Control Objectives

The concept of secure control systems compromising measurement and actuator data integrity and availability has been initially reported in [9]. Due to the utilization of wireless communication technologies such as 3G/4G networks, WiFi, GPRS, and WiMax [17], many of the threats are exacerbated by the utilization of these communication networks. The wireless communication technologies are the key components for CPSs to conduct control tasks and operations remotely. However, these technologies will inevitably increase the architectural complexity, thus introducing additional vulnerabilities and security risks. For example, many critical infrastructures are operated through supervisory control and data acquisition (SCADA) systems, where the unprotected communication channels expose the whole system to various cyber threats [18].

Traditional information technology (IT) infrastructures characterize security requirements as availability, integrity and confidentiality. These security requirements can also be found necessary for securing CPSs. The interpretation of security requirements for CPSs can be roughly categorized into the following sections:

- **Integrity** refers to trustworthiness of information flowing through communication channels between sensors, controllers and actuators of CPSs [19], which means that the transmitted data cannot be disrupted by unauthorized operations [19]. A lack of integrity usually leads to corrupted data which might be eroded by deception attacks. In the CPS framework, integrity can be therefore interpreted as the capabilities of keeping the operational goals from interference by malicious deception attackers.

- **Availability** refers to the fact that CPSs have timely access to essential control, performance and information resources [20]. For example, if a critical physical process is unstable in an open-loop fashion but can be stabilized by state/output feedback, DoS attacks on the control signal sending to the remote actuators may render the closed-loop system unstable under the state/output feedback controller.

- **Confidentiality** relates to the non-disclosure of private information [20]. CPSs are also required to prevent an unauthorized party from eavesdropping on the state of the physical system through the communication channels between the system components.

Other than the security requirements, the more important goals for secure control of CPSs include **stability**, **robustness** [21], and **optimality** [15, 22], which inherit naturally from classical control design. All of these designed goals are referred to as the operational goals, and our secure control design is to prevent these operational goals from malicious adversaries and limited resources.

Besides, it is also important to consider the resource constraints when designing a functional and economic controller for CPSs. Hence, the resource-aware control objectives include:

- **Communication reduction** signifies the lower packet transmission rate at the controller-to-actuator (C-A) and sensor-to-controller (S-C) communication channels, as well as the smaller packet size. Thus, the average sampling time can be used as a metric to represent communication reduction. The larger the average sampling time is, the more communication resource will be saved.

- **Constraint satisfaction** means that the designed controller can proactively handle the control input saturation and the resulting closed-loop system obeys state constraints at all time steps [15].

Therefore, in order to simultaneously fulfill those aforementioned control objectives, we in this thesis will develop secure and resource-aware control strategies for CPS-based control systems in the presence of cyber threats and resource constraints.

1.2 Model Predictive Control

Model predictive control (MPC) is an advanced optimization-based control methodology that has been widely used in industry applications such as chemical control process, supply chain, aerospace engineering and automotive industry [16, 23]. The essence of MPC is to optimize an objective function over a series of state and control input forecasts based on system dynamics, and therefore the model is an essential element of an MPC controller. The main advantage of MPC is that it can take into account future model predictions and constraint satisfaction, which grants MPC the ability of anticipating future events and taking admissible control actions accordingly. MPC controllers are steered by a finite-time horizon constrained optimization, relying on the dynamic model of the process often obtained by using system identification. At each sampling time instant, the optimization problem is solved and then

the MPC feedback control law, generated by using the optimal decision variables, is implemented until the control objectives, e.g., stability [15] and robustness [22], are achieved.

In order to briefly describe the MPC framework, we use the nonlinear time-invariant system as an example to show the essence of a typical MPC problem. The nonlinear state-space model is given as follows:

$$\dot{x} = f(x, u) \tag{1.1}$$

$$x \in \mathcal{X}, \quad u \in \mathcal{U} \tag{1.2}$$

where $x \in \mathbb{R}^n$ is the state variable, $u \in \mathbb{R}^m$ is the control input, $\mathcal{X} \subseteq \mathbb{R}^n$ is the state constraint set, and $\mathcal{U} \subseteq \mathbb{R}^m$ is the control input constraint set. The finite horizon cost being minimized can be defined by

$$J\left(x(s;t), u(s;t)\right) = \int_t^{t+T} L(x(s;t), u(s;t))\mathrm{d}s + F(x(t+T;t)), \tag{1.3}$$

where $x(s;t)$ and $u(s;t)$ are respectively the predicted state and control input at the prediction time s, T is the prediction horizon, $L(\cdot,\cdot)$ is the stage cost function, and $F(\cdot)$ is the terminal cost function. Then, the MPC optimization problem over a finite horizon T is given by

$$\begin{aligned} \boldsymbol{u}^*(x(t)) = &\arg\min_{u\in\mathcal{U}} J\left(x(s;t), u(s;t)\right) \\ \text{s.t.} \quad &\dot{x}(s;t) = f(x(s;t), u(s;t)), \\ &u(s;t) \in \mathcal{U}, \quad s \in [t, t+T], \\ &x(s;t) \in \mathcal{X}, \quad s \in [t, t+T], \\ &x(t+T;t) \in \Omega \end{aligned} \tag{1.4}$$

where $\Omega \subset \mathbb{R}^n$ is the terminal set and $\boldsymbol{u}^*(x(t)) = \{u^*(s;t) | s \in [t, t+T]\}$. The terminal set will be properly designed such that any state of the nonlinear system (1.1) starting in Ω will remain in Ω by a terminal feedback control. This important configuration enables that the closed-loop stability can be achieved for a large class of nonlinear systems. The MPC control law can be implemented by using $\boldsymbol{u}^*(x(t))$. For example, we can take the first portion (from t to $t+\delta$) of $\boldsymbol{u}^*(x(t))$ as the MPC control law [24].

Compared with the classic control methodologies such as proportional integral derivative (PID) and linear quadratic regulator (LQR), MPC has many advantages

especially in terms of handling constraints explicitly. Since MPC is an optimization-based control method, the computational load is hard to neglect especially when dealing with high dimensional nonlinear models at high sampling frequency. Therefore, in real applications where the computational resource is scarce, it is common to use a simpler model (i.e., a linear model) at a lower sampling frequency. In this dissertation, we focus on utilizing MPC on both linear and nonlinear models while reducing energy consumption and preserving control performance.

1.3 Problem Formulation

Throughout the thesis, we focus on designing secure and/or resource-aware MPC methodologies for compensating adverse effects in application scenarios where the cyber threats and resource constraints are present. A typical secure and resource-aware MPC framework is illustrated in Fig. 1.3, where two types of cyber attacks (i.e., deception attacks and DoS attacks) erode the communication channel (e.g., the C-A channel and the S-C channel). The following elements of the control framework include: 1) the model of the physical plant; 2) the formulation of resource constraints; 3) the model of cyber attacks; 4) the MPC optimization problem; and 5) the state feedback control law.

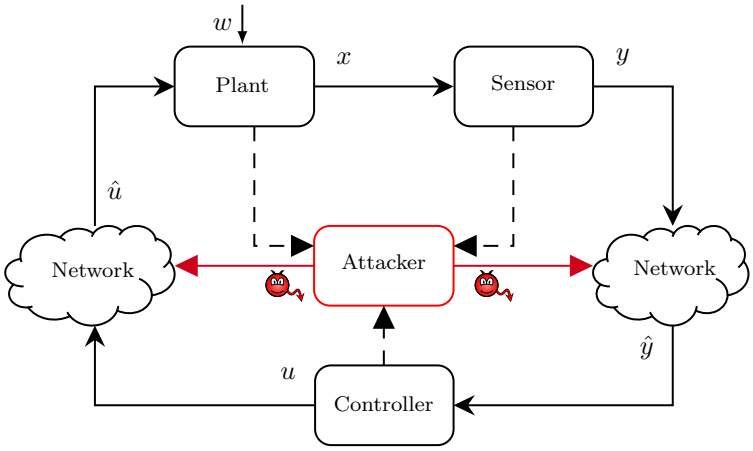

Fig. 1.3: The secure control system diagram under malicious attacks.

- **Model of the physical plant**

The physical plant is considered as a perturbed nonlinear differential equation:

$$\dot{x}(t) = f(x(t), u(t), w(t)) \tag{1.5}$$

where x is the system state, u is the control input, and w is unknown but bounded parametric uncertainty or external disturbance. Note that all of these variables have appropriate dimensions. In a CPS context, it is usually more common to use the discrete-time version of (1.5), i.e., $x_{k+1} = f_d(x_k, u_k, w_k)$. Besides, the physical plant can be simplified as a linear state-space model if the nonlinearity can be neglected.

- **Formulation of resource constraints**

  The resource constraints are formulated in set-based approaches. In particular, the physical constraints include: $x \in \mathcal{X}$ is the state constraint set and $u \in \mathcal{U}$ is the control input constraint set, where both of the sets are compact; the network limitation is treated as an upper bound of transmission bandwidth for sending the control packets from the controller to the physical plant.

- **Model of cyber attacks**

  We consider the case that the DoS attack can block the control packet transmission on the C-A channel and the deception attack can inject false information into the control packet.

  In order to model DoS attacks, we first introduce the following notations of DoS attack launching time instants and durations, i.e., $\mathcal{T}^a \triangleq \{k_\ell^a \in \mathbb{N}_{\geq 0}, \ell \in \mathbb{N}_{\geq 0}\}$ and $\mathcal{D}^a \triangleq \{d_\ell^a \in \mathbb{N}_{>0}, \ell \in \mathbb{N}_{\geq 0}\}$ where ℓ denotes the ℓth launching (see, e.g., [25]). Then, we can define the *total activation time* and *overall successful transmission time* of the DoS attack as

$$\Xi(0, \infty) \triangleq \bigcup_{\ell \in \mathbb{N}} \mathbb{N}_{[k_\ell^a, k_\ell^a + d_\ell^a)} \tag{1.6}$$

$$\Theta(0, \infty) \triangleq \mathbb{N}_{[0,\infty)} \backslash \Xi(0, \infty) \tag{1.7}$$

  Using the above configurations, the DoS attack effect on the communication

network can be conveniently formulated as an indicator function, i.e.,

$$\mathbf{1}_{\Xi}(k) = \begin{cases} 1, & k \in \Xi(0,\infty) \\ 0, & k \in \Theta(0,\infty) \end{cases} \tag{1.8}$$

where $\mathbf{1}_{\Xi}(k) = 1$ represents the communication channel is blocked and $\mathbf{1}_{\Xi}(k) = 0$ indicates a possible successful transmission can be made through this channel. Moreover, for any specific time interval $[k_0, k] \subset [0, \infty)$, we introduce the following similar notations:

$$\Xi(k_0, k) \triangleq \Xi(0,\infty) \bigcap \mathbb{N}_{[k_0,k)} \tag{1.9}$$

$$\Theta(k_0, k) \triangleq \mathbb{N}_{[k_0,k)} \backslash \Xi(k_0, k) \tag{1.10}$$

where $k_0 \in \mathbb{N}_{\geq 0}, k \in \mathbb{N}_{>0}$ and $k > k_0$. Then, the DoS attack capability (or energy) can be naturally measured by $\mathrm{card}\,(\Xi(k_0, k))$, which denotes the total duration of DoS attacks between time instants k_0 and k.

The deception attack can be modeled as a bounded signal $a(t)$ representing the attack effect targeting at the control packet transmission, i.e., the control signal received by the physical plant will be added by $a(t)$. Due to that the adversaries only have limited capability for attacking the communication channel, it is reasonable to assume that both of the DoS attack and the deception attack have energy constraints.

- **MPC optimization problem**

The finite-horizon cost to be minimized can be given by

$$J\left(x(s;t), u(s;t)\right) = \int_{t}^{t+T} L(x(s;t), u(s;t))\mathrm{d}s + F(x(t+T;t)) \tag{1.11}$$

where t is the current sampling time, T is the prediction horizon, $L(\cdot,\cdot)$ is the stage cost function, and $F(\cdot)$ is the terminal cost function. The discrete-time version of (1.11) can be formulated as

$$J_d\left(x_{k+i|k}, u_{k+i|k}\right) = \sum_{i=0}^{N} L(x_{k+i|k}, u_{k+i|k}) + F(x_{k+N|k}) \tag{1.12}$$

where k is the sampling time step and N is the prediction horizon. The MPC

optimization problem over a finite horizon T is therefore given by

$$\begin{aligned} & \min J\left(x(s;t), u(s;t)\right) \\ \text{s.t.} \quad & \dot{x}(s;t) = f(x(s;t), u(s;t)), \\ & u(s;t) \in \mathcal{U}, \quad s \in [t, t+T], \\ & x(s;t) \in \mathcal{X}, \quad s \in [t, t+T], \\ & x(t+T;t) \in \Omega \end{aligned} \tag{1.13}$$

where Ω is the terminal set.

- **State feedback control law**

  The control law is solely dependent on the system state of the physical plant. In particular, the control law derived throughout this thesis belongs to the following general state feedback form:

$$u^*(t) = \mu(x(t)) \tag{1.14}$$

  where the mapping μ can be obtained through secure and/or resource-aware MPC controller design methodologies. The closed-loop stability and optimal control performance will be investigated and analyzed for the closed-loop system by using $u^*(t)$ as a state-feedback control.

This thesis focuses on the following groups of questions related to the CPS-based control system in Fig. 1.3:

Q1 **Resource-aware MPC framework**: How to improve the network transmission efficiency for CPS-based control systems while fulfilling the resource constraints and achieving the closed-loop stability? What core techniques should be developed for adapting the conventional MPC?

Q2 **Secure MPC framework**: How to model cyber attacks for the MPC framework? How to guarantee the secure control objectives for CPS-based control systems while using MPC to deal with the physical constraints? How to protect the private information transmission from the eavesdropper?

1.4 Related Work

In this section, we provide an overview of existing research results related to this thesis from the following two aspects: event-triggered control of CPSs and secure control of CPSs.

1.4.1 Event-Triggered Control of CPSs

For resource-aware CPSs, event-triggered control (ETC) is a useful control paradigm to achieve the resource-aware control objectives [26]. In general, ETC features an event-triggered mechanism (ETM) to determine the sampling time instants. The main benefit of ETC is the communication reduction, which is of practical importance especially for CPSs with rather limited communication resources. Hence, there are numerous research interests and efforts on reducing the communication load in control systems by using the event-triggered scheme [26–37]. The work [26] firstly proposed a constant threshold-based event-triggered scheme, which executes the next sampling when the norm of state or estimation error exceeds a certain constant bound. Compared with the conventional periodic control, this method is shown to have great advantages in terms of reducing communication rate [26]. In another early work [27], the proposed event-triggered scheme adopted a so-called relative threshold policy for a class of nonlinear systems. In addition, a lower bound for the inter-execution time is proved to exist for avoiding the Zeno behavior. Input-to-state stability of the integral-based event-triggered control is investigated in [36]. The study of state-based event-triggered control can be found in [30], and output-based event-triggered control has been reported in [31].

As a promising research direction in ETC, event-triggered MPC (ET-MPC) implements ETM by continuously checking the discrepancy between the real state trajectory and the optimal predicted state trajectory. The advantage of MPC is that it can simultaneously handle the system constraints and take the future system behavior into account. Compared with other well-known networked control strategies such as networked proportional-integral control [38] and event-triggered fuzzy control [39], the MPC-based method provides constraint satisfaction and better performance guarantees in the control design of networked control systems [40–43]. In particular, the integration of ETM into MPC can significantly reduce not only the communication but also the computation load, given the fact that MPC usually consumes more computational power. Therefore, by using the event-triggered scheme,

ET-MPC can reduce the frequency of state sampling, optimization solving, and information transmission. The concept of ET-MPC is firstly studied in [41] and then received continuous research efforts in [43–48], to name a few.

In the existing literature, some promising results on ET-MPC have been reported in [41–46, 48–57]. Roughly speaking, the research on ET-MPC can be generally classified into two categories, e.g., for linear [45, 54] and nonlinear systems [43, 44, 53, 55, 56], respectively. (1) ET-MPC for linear systems. For example, the authors in [54] studied the ET-MPC of linear systems with additive disturbances by using a tube-based approach. (2) ET-MPC for nonlinear systems. In [44], an event-triggered scheme was proposed for nonlinear systems with additive disturbances by continuously measuring the discrepancy between the actual and the predicted trajectories. In order to acquire the benefit of avoiding the Zeno behavior, the authors in [43] proposed an ETM design that can guarantee that the inter-execution time is lower bounded. In [53], a self-triggered MPC framework is proposed for nonlinear affine systems to further reduce the communication load. The control signal is a piecewise constant signal by using sample-and-hold on the optimal control sequence, where each sampling interval is chosen by an adaptive selection scheme. It is worthwhile to note that ET-MPC has also been applied to decentralized systems [42] and distributed systems [49, 52]. In particular, we can categorize the related ET-MPC literature according to the different ETMs they used, i.e., the absolute threshold based ETM [41, 43, 45–48, 51, 58–60], the relative threshold based ETM [49, 61, 62], and the Lyapunov based ETM [44, 63–66].

The first type of ET-MPC uses a triggering condition with a constant threshold to generate the sampling instants at which the triggering condition violates the predesigned threshold. In [41], the authors first proposed an implicit event-based MPC algorithm for nonlinear continuous systems. If the inter-execution time interval (i.e., the time interval between two consecutive triggering time instants) is both upper and lower bounded, the feasibility and convergence of this algorithm can be guaranteed. In a later work [45], the authors studied the trade-off between the threshold of the triggering condition and the control performance for discrete-time linear systems subject to disturbances. The authors in [43] introduced a constant threshold event-triggered dual-mode MPC framework in order to further reduce the communication and computation power consumption. In [48], the ET-MPC framework was extended by using the integral-type ETM, where the communicational and computational resource consumption can be further reduced. After that, a new event-triggering condition for

the dual-mode MPC was introduced by [47], which designed the threshold of the condition as a function of the minimum time interval. This method guarantees that the controller will switch from MPC to the local stabilizing controller after the state enters the terminal set. Recently, the authors in [58] investigated the ISS properties of the ET-MPC for uncertain nonlinear systems. In addition, the constant threshold ET-MPC can also find application in tracking control systems and distributed control systems. For example, the work [59] designed a constant threshold ET-MPC strategy for tracking control of nonholonomic systems. In [51], the authors applied the absolute threshold triggering condition to a distributed MPC framework for nonlinear systems. Generally speaking, the first type of ET-MPC has the advantage of easier implementation, but the disadvantages of more resource consumption due to the design conservativeness brought by the constant threshold.

To provide more resource-aware control performance, the second type of ET-MPC exploits triggering conditions using a relative threshold based on the system state, thus introducing another degree of freedom when designing more efficient ET-MPC strategies. For example, the authors in [61] proposed a robust ET-MPC for linear systems under matched model uncertainties by using the integral sliding mode control and the relative threshold-based event-triggering condition. The designed triggering condition used a threshold that is the product of the norm of the system state and a given real constant. In [49], an ET-MPC framework was developed for cooperative control of decoupled nonlinear multi-agent systems. In this framework, each of the subsystems had its triggering condition based on the local real state and the errors between the predicted and the real state trajectories of the neighboring agents. In particular, the relative thresholds of the triggering conditions are designed as the non-decreasing and radially unbounded function of the norm of the local real state. Although it may bring better resource-awareness, this kind of ET-MPC is relatively hard to implement and can also easier lead to the infinite number of state sampling, i.e., the so-called Zeno behavior [43].

The third type of ET-MPC derives its triggering condition based on the analysis of the descent property of the Lyapunov function. That is to say, the triggering condition is designed as certain conditions for guaranteeing the closed-loop stability. In the literature, an early work [44] first applied a Lyapunov based triggering condition to an event-triggered NMPC framework for uncertain nonlinear systems subject to additive disturbances. This triggering condition was derived to ensure that the Lyapunov function was decreasing at each triggering instant. The authors

in [64] proposed a robust ET-MPC framework for nonlinear continuous-time systems with additive disturbances. In the framework, two different event-triggering conditions were designed based on a non-monotonic Lyapunov function approach. Using these conditions and applying piecewise constant control law, this work showed that there existed a trade-off between the frequency of event triggering and the control performance. Besides, this type of ET-MPC finds increasing attention in designing event-triggered distributed MPC. For example, the work [65] studied a distributed event-based MPC framework for linear time-invariant multi-agent systems, where a cost-based event-triggering condition was designed based on locally comparing the cost before and the cost after the local optimization. In another work [63], the authors proposed a triggering condition for distributed MPC framework, which only used the local information for generating the event-triggered time instants. In [66], a novel triggering condition involving the neighbours' information was introduced to achieve a trade-off between the resource consumption and the control performance. Since all of these triggering conditions are derived based on the Lyapunov function, the closed-loop stability can be more easily guaranteed, however, at the cost of increasing the complexity of the triggering condition.

Despite considerable reduction of the resource consumption, the aforementioned ET-MPC strategies generally achieve better resource-awareness at the expense of sacrificing the control performance. Therefore, the trade-off between the resource-awareness and the control performance must be considered in order to design more efficient ET-MPC strategies for CPSs.

1.4.2 Secure Control of CPSs

Recently, secure control systems have drawn many research interests and attention since they can provide CPSs (especially critical CPSs) necessary and important protection against malicious cyber attacks [6, 67]. The secure concept arises originally in the computer science society, focusing mainly on data and IT services [19]. Unlike the computer and IT systems targeting data security, the secure control systems are designed to achieve more operational goals such as stability and optimal control performance, see survey papers [68–73] and references therein. The existing results on secure control can be classified into two categories in terms of the different adversarial attacks, i.e. DoS attacks [10, 11, 25, 74–91] and deception attacks [11, 92–106]. In [11], different counter mechanisms and resulting analysis strategies were summarized and

categorized in terms of dealing with deception attacks and DoS attacks.

As for secure control under deception attacks, a linear quadratic Gaussian (LQG) regulation problem equipped with a so-called $\mathcal{X}^2$ failure detector was studied in [101]. The performance degradation of CPSs under stealthy deception attacks was investigated in [94], where the effect of attacks was considered as the maximum perturbation by using a reachable set computation. In [104], a dynamic output feedback controller was designed for stochastic nonlinear systems such that the prescribed security using probability and input-to-state stability were guaranteed. Secure consensus under deception attacks was addressed in [105]. A trade-off between the performance degradation and deception attacks can also be found in [94]. The malicious adversary can inject false data into the C-A and S-C channels of an LTI system without incurring detection from an anomaly detector. The maximum perturbation induced by the deception attack can be achieved by using the reachable set computation. For a stochastic control system, the largest performance degradation was derived under a so-called ϵ-stealthiness attack [98]. The effect of replay attacks on the sensor measurements was analyzed in [101], where all the information of the system and sensor measurements were eavesdropped by the adversary. In addition, an output feedback control law was proposed for the linear system under deception attacks on both S-C and C-A channels [97], where only the appropriate chosen feedback control can make the closed-loop system more secure to sensor attacks.

Compared with deception attacks, DoS attacks require much less prior information of the control system, but they can seriously damage the system by tampering availability of the communication channel. In [75], the authors proposed a secure constrained optimal control framework for discrete-time linear time-invariant (LTI) systems. An optimal casual feedback controller that minimizes the cost function subject to DoS attacks was obtained by transforming the original problem into a semi-definite programming optimization. In [25], a new DoS attack model characterized by attack frequency and duration was proposed. The closed-loop stability can be guaranteed by using state-feedback control related to the explicit duration and frequency of DoS attacks. To handle the DoS attack and external disturbance simultaneously, the authors in [107] considered the input-to-state stable (ISS) property for nonlinear systems by using a frequency and duration measured DoS attack model. By using the same DoS attack model, the robust control design was proposed in [84] for maximizing the duration and frequency of the DoS attacks without destabilizing the resulting closed-loop system. Besides, the ISS property under multiple transmission

S-C channels in the presence of DoS attack was investigated in [88], where sufficient conditions on the duration and frequency can be achieved under the prerequisite of the closed-loop stability. A two-player zero-sum game-based model was introduced for LTI systems in [76], where the first player acted as a controller, while the other one played like a jammer. Saddle-point equilibrium based control and jamming strategies were derived under the prerequisite of full state information. In [89], a unified game framework was proposed for linear systems under DoS attacks, where the optimal attack and defense strategies were studied respectively.

In the vast majority of literature on secure 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 [108–110] and time-sequence based attacks [25, 84, 111]), whereas the latter focuses on the stochastic nature of some malicious attackers (e.g., Bernoulli attacks [112] and Markov-modulated attacks [113]). Deterministic DoS attacks are often believed to be more realistic since attackers do have clear incentives to sabotage control objectives [25]. 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 [25]. In [110], the periodic DoS attacks are characterized by a cyclic dwell-time switching strategy, by which the resulting augmented system can be transformed into a stable and an unstable subsystem. Based on a Markov modulated DoS attack model, the risk-sensitive stochastic control problem was tackled by proposing an optimal control policy for mitigating the adverse effect [78].

MPC has drawn great attention in the past decades due to its wide applications in many industrial systems, see [16, 114]. The MPC-based methodology for securing CPSs is also shown great advantages compared with other approaches. In this context, the generated control sequence can be more useful to compensate for the various security issues such as DoS attacks and deception attacks by using appropriate compensating mechanisms. These features brought by utilizing MPC methods have shown great potential in achieving the secure control objectives for CPSs. In addition, the MPC-based methods can inherit the benefits of dealing with a variety of system constraints, i.e., control input and state constraints. These naturally grant CPSs the designing advantages capable of taking into account the controller energy conservation and communication resource limitation. Therefore, the study of MPC-based control for CPSs is able to facilitate and advance the demanding applications

for such systems under security-aware communication networks and controller energy restrictions.

There have been some interesting research works reported on MPC of CPSs for handling various cyber attacks [79–81, 95, 103, 115, 116]. The MPC problem of stochastic systems over bit-rate limited channels with limited energy DoS attack has been investigated in [79, 80], where the DoS attack was modeled as a Bernoulli process. In [95], the authors proposed a secure networked predictive control system framework, which was an integration method of several advanced techniques including the Data Encryption Standard algorithm, Message Digest algorithm, and recursive networked predictive control method, etc. This method was proposed to compensate for the adverse effects brought by deception attacks and the network constraints, such as network-induced delays and packet dropouts. The authors in [117] proposed a Lyapunov-based based MPC framework for the networked nonlinear systems subject to DoS attacks. A recent work [115] has shown that the designed MPC algorithm for hybrid NCSs was capable of compensating the effect of DoS attacks while preserving the ISS property of the closed-loop system. The authors in [103] proposed a slightly revised receding-horizon control law for alleviating the replay and DoS attacks occurring at the C-A channel. The system performance degradation was also studied, where a set of sufficient conditions between the infinite-horizon cost and the attacking horizons was investigated to ensure asymptotical and exponential stability, respectively. In addition to MPC-based approaches, there have been research efforts on secure control using resource-aware control approaches [10, 108, 118, 119] and game theoretic approaches [76, 77, 120, 121].

1.5 Thesis Outline and Contributions

This thesis focuses on a group of research questions on resource-awareness and security of CPS-based control systems. In **Chapter 2**, an ET-MPC strategy on dealing with **Q1** of nonlinear CPSs is studied. The MPC-based secure control problem (**Q2**) of CPSs subject to DoS attacks is investigated in **Chapter 3**. In **Chapter 4** and **Chapter 5**, the resource-aware and secure control problems (both **Q1** and **Q2**) subject to cyber attacks is respectively considered via an ET-MPC based strategy and an ST-MPC based strategy. **Chapter 6** presents a cloud-based MPC strategy on addressing secure and resource-aware control problems (both **Q1** and **Q2**) in a cloud-edge computing architecture. Finally, in **Chapter 7**, a summary of this thesis

is presented and the possible future research opportunities are listed.

Now we summarize the contributions of each thesis work.

Chapter 2 presents an integral-type ET-MPC framework of continuous-time nonlinear systems. An integral-type ETM is proposed by incorporating the integral of errors between the actual and predicted state sequences, leading to the reduced average sampling frequency. Besides, a new and improved robustness constraint is introduced to handle the additive disturbances, rendering the MPC problem with a potentially enlarged initial feasible region. Furthermore, the feasibility of the designed MPC and the stability of the closed-loop system are rigorously investigated. Several sufficient conditions to guarantee these properties are established, which are related to factors such as the prediction horizon, the disturbance bound, the triggering level, and the contraction rate for the robustness constraint.

In **Chapter 3**, we present a secure MPC framework to attenuate adverse effects of DoS attacks for CPSs, where the system dynamics is modeled by a linear time-invariant system. A DoS attacker aims at blocking the C-A channel by launching adversarial jamming signals. We show that, in order to guarantee exponential stability of the closed-loop system, several conditions for secure MPC should be satisfied. And these established conditions are explicitly related to the duration of DoS attacks and MPC parameters such as the prediction horizon and the terminal constraint. Two key techniques including the μ-step positively invariant set and the modified initial feasible set are exploited for achieving exponential stability in the presence of DoS attacks. Moreover, the maximum allowable duration of the DoS attacker is also obtained by using the μ-step positively invariant set.

Chapter 4 introduces a robust ET-MPC framework for CPSs in the presence of 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 ETM, 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 (ISpS) under some sufficient conditions.

In **Chapter 5**, we propose a self-triggered min-max MPC framework for constrained uncertain nonlinear cyber-physical systems in the presence of deception attacks and DoS attacks. In the proposed framework, a new min-max MPC optimiza-

tion problem is formulated with a new control variable parameterized by a series of radial basis functions. Then, a novel self-triggered mechanism is developed by comparing the optimal value functions of the new min-max optimization problem and the original min-max optimization problem. By using the min-max technique, we can optimize the control performance over the worst case of all possible uncertainty and deception attack realizations. In addition, DoS attacks can be tackled with the control sequence based on the new min-max MPC optimization problem. By using the proposed MPC strategy, we can guarantee that the closed-loop system is ISpS.

Chapter 6 describes a model predictive control as a secure service (MPCaaSS) framework for CPSs in the presence of cyber threats and external disturbance. By introducing a double-layer controller architecture, we are able to formulate an optimization control problem which permits not only the computationally-heavy optimization-based controller profile update in the cloud node but also the real-time control law implementation in the edge node. Besides, in order to securely transmit the controller profile and the state measurement, we integrate an encoding scheme and elliptic curve cryptography (ECC) into the proposed MPCaaSS framework such that no malicious attackers or eavesdroppers can corrupt and intercept these private signals. It is shown that the recursive feasibility of MPCaaSS is achieved under some sufficient conditions. Moreover, the robust stability of the closed-loop system is guaranteed if the optimization problem is recursively feasible.

Chapter 2

Resource-Aware Model Predictive Control of Nonlinear CPSs under External Disturbance

2.1 Introduction

In this chapter, we investigate the resource-aware control problem for continuous-time nonlinear systems with additive disturbance, aiming at alleviating the communication load while ensuring the closed-loop stability and resource awareness. Recent research interests and efforts have been directed towards reducing the communication load in control systems by using the event-triggered scheme [26, 27, 30, 31, 34–37]. Such a control paradigm employs the so-called ETM to reduce the frequency of state sampling and information transmission while maintaining expected performance. Compared with the conventional periodic control, event-triggered control treats sampling instants as a design factor, whereas the periodic scheme samples the states at fixed time instants. The event-triggered paradigm features the design of an appropriate scheduling mechanism with the capability of determining when the states or sensor outputs should be sampled. The benefit of such an effective scheduling can lead to a reduced communication rate and thus decrease the communication load, especially in cases where the communication resources are limited.

In control applications, MPC has been one of the most successful control methodologies. The basic and essential idea of MPC framework is to solve optimization problems online at each sampling instant, and apply the optimized control action

to the plant. The advantages of MPC is that it can simultaneously handle the system constraints and take the future system behavior into account. Compared with other well-known networked control strategies such as networked PID control [38] and event-triggered fuzzy control [39], the MPC-based method provides constraint satisfactions and better performance guarantees in the control design of networked control systems [40–43].

In particular, the incorporation of the event-triggered scheme into MPC can significantly alleviate the communication and computation load, especially considering that MPC features relatively heavier computational complexity. Therefore, ET-MPC has received many research efforts [41–45, 49, 52–56]. Specifically, by using the event-triggered scheme, ET-MPC can reduce the frequency of state sampling, optimization solving, and information transmission. In [43], the authors proposed an event-triggered scheme for reducing the communication load for a dual-mode MPC framework, where the event-triggering condition is designed based on the discrepancy between the real state and the predicted optimal state. To further reduce the communication rate, the authors in [35] proposed an integral-based event-triggered scheme by incorporating the integral of estimated errors to the event-triggering condition. Inspired by these works, we propose an integral-type ET-MPC framework to achieve the desired control objectives. The main contributions are three-fold: 1) An integral-type ET-MPC algorithm for the continuous-time nonlinear system with additive disturbance is proposed, where the integral of errors between the actual and predicted state sequences is used as the triggering condition for saving more communication resources. 2) A new and improved robustness constraint on the system states, rendering the MPC problem with a potentially enlarged initial feasible region compared with the existing one, is proposed to the MPC problem. 3) The feasibility of the designed MPC and the stability of the closed-loop system are thoroughly studied, theoretically showing that both of these important properties are related to the factors including the prediction horizon, the bound of disturbance, the triggering level, and the contraction rate of the robustness constraint.

The remainder of this chapter is organized as follows. Section 2.2 describes the problem formulation. Section 2.3 proposes the integral-type ET-MPC scheme. Section 2.4 presents feasibility of the MPC problem and stability of the closed-loop system. Section 2.5 illustrates a simulation example to verify the effectiveness of the proposed scheme and algorithm. Finally, we conclude this work in Section 2.6.

Notations: The real space is denoted by $\mathbb{R}$ and the set of all positive integers is

given by $\mathbb{N}$. For a given matrix X, $X^\top$ and X^{-1} denote its transpose and inverse (if invertible), respectively. For a symmetric matrix $S \in \mathbb{R}^{n\times n}$, $S \succ 0$ and $S \succeq 0$ is used as a common notation for positive definite and positive semidefinite matrices; the largest and smallest eigenvalues of S are denoted by $\overline{\lambda}(S)$ and $\underline{\lambda}(S)$. Given a column vector $x \in \mathbb{R}^n$, $\|x\| := \sqrt{x^\top x}$ represents the Euclidean norm and $\|x\|_P := \sqrt{x^\top P x}$ is the P-weighted norm.

2.2 Problem Formulation

We consider a continuous-time nonlinear system with additive disturbance as follows

$$\dot{x}(t) = f(x(t), u(t)) + \omega(t) \tag{2.1}$$

where $x(t) \in \mathbb{R}^n$ is the state variable, $u(t) \in \mathbb{R}^m$ is the control input, and $\omega(t) \in \mathbb{R}^n$ is unknown but bounded additive disturbance. The system satisfies $f(0,0) = 0$ and has a Lipschitz constant L. The control input constraint is $u(t) \in \mathcal{U}$, where $\mathcal{U} \subseteq \mathbb{R}^m$ is a compact set containing the origin. Moreover, the disturbance $\omega(t)$ belongs to a compact set $\mathcal{W}$ and its upper bound is given by $\rho \overset{\triangle}{=} \sup_{\omega(t)\in\mathcal{W}} \|\omega(t)\|$. The nominal system of (2.1) can be given as

$$\dot{x}(t) = f(x(t), u(t)) \tag{2.2}$$

where this system dynamics (2.2) will be used for constructing the equality constraint of the optimization problem. By linearizing the nonlinear system in (2.2) at the equilibrium $(0,0)$, we can obtain the linearized state-space model:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{2.3}$$

where $A = \frac{\partial f}{\partial x}|_{(0,0)}$ and $B = \frac{\partial f}{\partial u}|_{(0,0)}$.

In the following, we introduce a conventional assumption for the linearized model in (2.3), which will be used in the following lemma.

Assumption 2.1. *There exists a state-feedback gain K such that $A + BK$ is stable.*

Then, a conventional result regarding the control invariant property of the nonlinear system (2.2) is stated as follows.

Lemma 2.2. *[24] If $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is twice continuously differentiable, $f(0,0) = 0$, $u(t)$ is piece-wise right-continuous and Assumption 2.1 holds, then given two PD matrices Q and R, there exist a state-feedback gain K and a constant $\kappa > 0$ such that: 1) The Lyapunov equation $(A+BK+\kappa I)^\top P + P(A+BK+\kappa I) = -Q^*$ admits a unique solution $P \succ 0$, where $Q^* = Q + K^\top RK \in \mathbb{R}^{n\times n}$ and κ is smaller than the real part of $-\overline{\lambda}(A+BK)$; 2) $\Omega(\epsilon) := \{x \in \mathbb{R}^n | V(x(t)) \leq \epsilon\}$ is control invariant by the feedback control law $u(t) = Kx(t)$ for the system in (2.2); 3) $\dot{V}(x(t)) \overset{\triangle}{=} \|x(t)\|_P^2 \leq -\|x(t)\|_{Q^*}^2$ and $u(t) = Kx(t) \in \mathcal{U}$ for $x(t) \in \Omega(\epsilon)$.*

In the networked control system as illustrated in Fig. 2.1, the sampling time instants are denoted by $\{t_0, t_1, \ldots, t_k, \ldots\}$ for the nonlinear system in (2.1). At each sampling time instant t_k, the MPC controller generates an optimal control sequence $\hat{u}^*(s; t_k)$ and a corresponding optimal predicted state sequence $\hat{x}^*(s; t_k)$ by solving an online optimization problem, where $s \in [t_k, t_k + T]$. In order to save communication resources, we propose to use the event-triggered MPC strategy, where the control inputs are updated aperiodically with larger time intervals rather than periodically with a fixed small time interval. In particular, we aim at designing a more efficient event-triggered MPC scheme for the system in (2.1) such that the better communication performance and the closed-loop stability can be obtained.

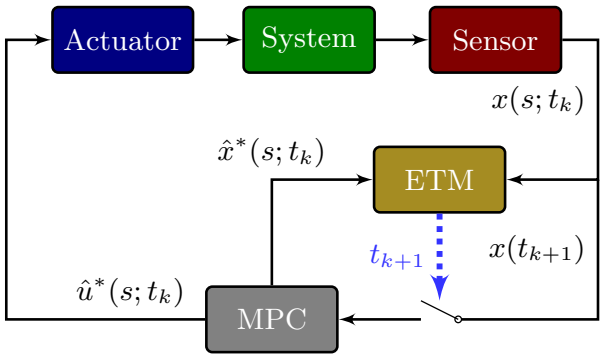

Fig. 2.1: An overview of the event-triggered network control system.

2.3 Integral-type Event-Triggered MPC

2.3.1 Optimization Problem

In order to avoid ambiguity, we take explicit notations $\hat{u}(s; t_k)$ and $\hat{x}(s; t_k)$ as the control and predicted state sequence at the kth sampling instant, respectively. Then,

the MPC optimization problem at t_k can be designed as

$$\hat{u}^*(s;t_k) = \arg\min_{\hat{u}\in\mathcal{U}} J\left(\hat{x}(s;t_k),\hat{u}(s;t_k)\right) \tag{2.4}$$

$$\text{s.t.} \quad \dot{\hat{x}}(s;t_k) = f(\hat{x}(s;t_k),\hat{u}(s;t_k)) \tag{2.5}$$

$$\hat{u}(s;t_k) \in \mathcal{U}, \quad s \in [t_k, t_k+T] \tag{2.6}$$

$$\|\hat{x}(s;t_k)\|_P \leq \frac{(t_k+T-s)M + s - t_k}{T}\alpha\epsilon \tag{2.7}$$

where the cost function in (4) is defined by

$$J\left(\hat{x}(s;t_k),\hat{u}(s;t_k)\right) \triangleq \int_{t_k}^{t_k+T} \|\hat{x}(s;t_k)\|_Q^2 + \|\hat{u}(s;t_k)\|_R^2 \mathrm{d}s + \|\hat{x}(t_k+T;t_k)\|_P^2 \tag{2.8}$$

Note that $Q \succeq 0$, $R \succ 0$, $\mathbf{I}_n$ is the $n \times n$ identity matrix, P is defined by using the method from Lemma 2.2, T is the prediction horizon, ϵ is the designed parameter for defining the terminal set, $\alpha \in (0,1)$ is the scaling ratio, and M is the contraction rate for the robustness constraint (2.7). It is also worthwhile pointing out that the terminal constraint is $\hat{x}(t_k+T;t_k) \in \Omega(\alpha\epsilon) \triangleq \{x : \|x\|_P \leq \alpha\epsilon\}$ by the robustness constraint (2.7). After solving the optimization problem at t_k, the optimal control sequence can be expressed as $\hat{u}^*(s;t_k)$, and the corresponding optimal predicted state sequence can be given as $\hat{x}^*(s;t_k)$, where $s \in [t_k, t_k+T]$.

Remark 2.3. *In the optimization problem (2.4), the robustness constraint (2.7) is used for tightening the P-weighted norm of state predictions, which grants MPC capability of compensating the additive disturbance. The robustness constraint-based method for MPC has been firstly proposed in [43], where its contraction speed is proportional to the prediction time. In our configuration, the less-conservative robustness constraint is designed with a constant contraction speed as the predicted state trajectory shrink into the terminal set. Compared with the conventional one, our proposed robustness constraint can provide a larger initial feasible set for solving the optimization problem.*

2.3.2 Integral-type Event-Triggered Mechanism

In order to more efficiently reduce the frequency of solving the optimization, state sampling, and information transmission from the controller to the actuator, an integral-type ETM is introduced for scheduling and implementing these tasks, i.e. determining

the event-triggered instants $\{t_0, t_1, \ldots, t_k, \ldots\}$. At the kth sampling instant t_k, from the system in (2.1) and the MPC optimization problem in (2.4), one can get the real state sequence $x(s;t_k)$ and the optimal predicted state sequence $\hat{x}^*(s;t_k)$ for $s \in [t_k, t_k+T]$, where T denotes the prediction horizon defined in the MPC optimization problem. Due to the additive disturbance in the system, the two sequences $x(s;t_k)$ and $\hat{x}^*(s;t_k)$ cannot coincide with each other. Motivated by this fact, the discrepancy of these two sequences can be used to construct conditions for triggering the next sampling instant. Therefore, the triggering condition for the integral-type ETM is designed as

$$\begin{aligned} H_k &= \inf_{h>0}\left\{h : \int_{t_k}^{t_k+h} \|x(s;t_k) - \hat{x}^*(s;t_k)\|_P \mathrm{d}s = \delta\right\} \\ t_{k+1} &= \min\{t_k + H_k, t_k + T\} \end{aligned} \tag{2.9}$$

where δ is the triggering level and h is the time variable to be determined for satisfying the equality in the triggering condition (2.9) at t_k. If the integral of errors in (2.9) is large enough to reach a specific threshold at some time instant $t_k + H_k$ between t_k and $t_k + T$, then this $t_k + H_k$ will be the next sampling instant t_{k+1}. It is worth noting that the triggering level δ will dramatically affect both the communication and control performance. Roughly speaking, the larger δ will lead to better communication performance but worse control performance. Thus, it should be carefully designed.

Remark 2.4. *Note that the designed ETM is based on the integral of errors between actual state sequence and optimal predicted state sequence, which is different from the event-triggered setting in [43]. The benefit of introducing the integral of errors to the triggering condition lies in that the average of errors between two consecutive event-triggered instants is taken into consideration, leading to some advantages in terms of reducing inter-execution sampling intervals, which will be illustrated in the simulation study in Section 2.5.*

The following theorem shows some important properties of the proposed integral-type ETM on avoiding the Zeno behavior.

Theorem 2.5. *For the nonlinear system in (2.1), if the event-triggered time instants t_k, $k \in \mathbb{N}$ are implemented according to (2.9), then the following properties hold: 1) The upper bound on the inter-execution time is $\sup_{k\in\mathbb{N}}(t_{k+1} - t_k) = T$; 2) the lower bound $\inf_{k\in\mathbb{N}}(t_{k+1} - t_k) = \beta T$ can be guaranteed by properly designing the triggering*

level δ *as*

$$\delta = \rho\overline{\lambda}(\sqrt{P})\left[e^{L\beta T}\left(\frac{\beta T}{L} - \frac{1}{L^2}\right) + \frac{1}{L^2}\right] \tag{2.10}$$

where $\beta \in (0, 1)$ *is a scaling parameter.*

Proof. This proof can be done by two steps.

Step 1: The upper bound of inter-execution intervals is T. From the design of the integral-type ETM, it can be directly deduced that all the intervals $t_{k+1} - t_k$ is less than or equal to the prediction horizon T.

Step 2: The inter-execution intervals can be lower bounded to βT by properly designing the triggering level δ according to (2.10). To prove this result, we firstly consider the upper bound for $\|x(s;t_k) - \hat{x}^*(s;t_k)\|_P$ at t_k. We assume here that the sensor measurements are accurate. Thus, it follows that $x(t_k;t_k) - \hat{x}^*(t_k;t_k) = 0$. By using the triangle inequality, we have $\|x(s;t_k) - \hat{x}^*(s;t_k)\|_P \leq \|x(t_k;t_k) - \hat{x}^*(t_k;t_k) + \int_{t_k}^{s} \dot{x}(\tau;t_k) - \dot{x}^*(\tau;t_k)\mathrm{d}\tau\|_P \leq \int_{t_k}^{s} L\|x(\tau;t_k) - \hat{x}^*(\tau;t_k)\|_P + \|\omega(\tau)\|_P\mathrm{d}\tau \leq \int_{t_k}^{s} L\|x(\tau;t_k) - \hat{x}^*(\tau;t_k)\|_P\mathrm{d}\tau + \rho\overline{\lambda}(\sqrt{P})(s - t_k)$. Then by applying the integral form of Gronwall-Bellman inequality, it can be obtained that $\|x(s;t_k) - \hat{x}^*(s;t_k)\|_P \leq \rho\overline{\lambda}(\sqrt{P})(s - t_k)e^{L(s-t_k)}$. Substituting the previous inequality to (2.9), we can deduce that $\int_{t_k}^{t_{k+1}} \|x(s;t_k) - \hat{x}^*(s;t_k)\|_P\mathrm{d}s \leq \int_{t_k}^{t_{k+1}} \rho\overline{\lambda}(\sqrt{P})(s - t_k)e^{L(s-t_k)}\mathrm{d}s = \rho\overline{\lambda}(\sqrt{P}) \cdot \left[e^{L(t_{k+1}-t_k)}\left(\frac{t_{k+1}-t_k}{L} - \frac{1}{L^2}\right) + \frac{1}{L^2}\right]$. Since $\overline{\lambda}(\sqrt{P})(s - t_k)e^{L(s-t_k)}$ is strictly larger than zero for $s > t_k$, we can choose δ as (2.10) such that the lower bound of the triggered time interval is $\inf_{k\in\mathbb{N}}(t_{k+1} - t_k) = \beta T$. The proof is completed. □

2.3.3 The Closed-Loop System

By implementing the generated optimal control sequence into the system model in (2.1), we write the resulting closed-loop system as

$$\dot{x}(t) = f(x(t), \hat{u}^*(t;t_k)) + \omega(t), \quad k \in \{0, 1, 2, \ldots\} \tag{2.11}$$

where t_k is the kth event-triggered instant generated by (2.9). The feasibility of MPC problem (2.4) and the closed-loop stability of (2.11) will be respectively analyzed in the following section. For a clear view of the aforementioned integral-type ET-MPC, we design the ET-MPC algorithm as described in Algorithm 2.1.

Algorithm 2.1: Integral-type ET-MPC

```
while The control action is not stopped do
    if k = 0 then
        Solve the optimization problem in (2.4) at t_0;
    end
    while The ETM condition (2.9) is not triggered do
        Apply optimal control input û*(s; t_k), where s ∈ [t_k, t_k + T];
    end
    Obtain t_{k+1} according to (2.9);
    Solve the optimization problem in (2.4) at t_{k+1};
end
```

2.4 Main Results

2.4.1 Feasibility Analysis

Following a conventional setup for MPC framework, we construct a classical feasible control sequence for the optimization problem (2.4) as follows:

$$\tilde{u}(s;t_k) = \begin{cases} \hat{u}^*(s;t_{k-1}) & \text{if } s \in [t_k, t_{k-1}+T] \\ Kx(s;t_k) & \text{if } s \in (t_{k-1}+T, t_k+T] \end{cases} \tag{2.12}$$

Then the candidate state sequence evolves as

$$\dot{\tilde{x}}(s;t_k) = f(\tilde{x}(s;t_k), \tilde{u}(s;t_k)) \tag{2.13}$$

Before presenting the result of this section, we introduce a lemma that will be useful in the following analysis.

Lemma 2.6. *Let $g : \mathbb{R} \to \mathbb{R}^N$ be a differentiable vector-valued function defined on $t \in [a,b]$. Then the following inequality holds:*

$$\sup_{t\in[a,b]} \|g(t)\| \leq \frac{1}{2}\int_a^b \|g^{'}(t)\|dt + \frac{1}{2}\|g(a)+g(b)\| \tag{2.14}$$

where $g^{'}$ is the derivative of g.

Proof. For every $t \in [a,b]$, we have two results: $g(t) = g(a) + \int_a^t g^{'}(\tau)\mathrm{d}\tau$, $\quad g(b) =$

$g(t)+\int_t^b g^{'}(\tau)\mathrm{d}\tau$. Subtracting the aforementioned two equations yields $2g(t)=g(a)+g(b)+\int_a^t g^{'}(\tau)\mathrm{d}\tau+\int_b^t g^{'}(\tau)\mathrm{d}\tau$. By employing the triangle inequality, we can deduce from the above equality that $\|g(t)\| \leq \frac{1}{2}\|g(a)+g(b)\|+\frac{1}{2}\int_a^t \|g^{'}(\tau)\|\mathrm{d}\tau+\frac{1}{2}\int_t^b \|g^{'}(\tau)\|\mathrm{d}\tau = \frac{1}{2}\int_a^b \|g^{'}(t)\|\mathrm{d}t+\frac{1}{2}\|g(a)+g(b)\|$. Since every $g(t)$ defined on the closed interval $[a,b]$ is equal to or less than the right side of the above inequality, the result in (2.14) thus holds. □

To facilitate the analysis of integral-type event-triggered configuration, we make use of a term $e(s;t_k)=\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})$ for $s\in[t_k,t_{k-1}+T]$. Note that $\tilde{x}(s;t_k)$ is defined as the candidate state sequence generated by the nominal system (2.13), and $\hat{x}^*(s;t_{k-1})$ is the solution of the optimization problem (2.4). In addition, we let $\tilde{x}(t_k;t_k)=x(t_k)$ by sampling the state at the kth triggered time instant t_k, since we assume that there is no measurement inaccuracy. Then we can propose the following result.

Corollary 2.6.1. *Given $e(s;t_k)$ defined on $s\in[t_k,t_{k-1}+T]$, the following inequality holds*

$$\sup_{s\in[t_k,t_{k-1}+T]}\|e(s;t_k)\|_P \leq \frac{L^2\beta T}{L\beta T-1}e^{L(1-\beta)T}\delta \tag{2.15}$$

under the condition that $L\beta T>1$.

Proof. By Lemma 2.6, we can obtain that

$$\begin{aligned}\sup_{s\in[t_k,t_{k-1}+T]}\|\sqrt{P}e(s;t_k)\| \leq & \frac{1}{2}L\int_{t_k}^{t_{k-1}+T}\|\sqrt{P}e(s;t_k)\|\mathrm{d}s \\ & +\frac{1}{2}\|\sqrt{P}e(t_k;t_k)+\sqrt{P}e(t_{k-1}+T;t_k)\|\end{aligned} \tag{2.16}$$

Note that $\|e(s;t_k)\|_P=\|\sqrt{P}e(s;t_k)\|$. Then it can be deduced from the above inequality that

$$\begin{aligned}\sup_{s\in[t_k,t_{k-1}+T]}\|e(s;t_k)\|_P \leq & \frac{1}{2}L\int_{t_k}^{t_{k-1}+T}\|e(s;t_k)\|_P\mathrm{d}s \\ & +\frac{1}{2}\|2e(t_k;t_k)+\int_{t_k}^{t_{k-1}+T}\dot{e}(s;t_k)\mathrm{d}s\|_P \\ \leq & L\int_{t_k}^{t_{k-1}+T}\|e(s;t_k)\|_P\mathrm{d}s+\|e(t_k;t_k)\|_P\end{aligned} \tag{2.17}$$

Next we show that the upper bound of $\|e(t_k;t_k)\|_P$ is related to the triggering level δ.

By using the result from Theorem 2.5, the upper bound of $\|x(s;t_{k-1}) - \hat{x}^*(s;t_{k-1})\|_P$ is $\rho\overline{\lambda}(\sqrt{P})(s-t_{k-1})e^{L(s-t_{k-1})}$ for $s \in [t_{k-1}, t_k]$. Suppose that there exists a maximum value of $\|x(s;t_{k-1}) - \hat{x}^*(s;t_{k-1})\|_P$ such that $\|x(t_{k-1}+h;t_{k-1}) - \hat{x}^*(t_{k-1}+h;t_{k-1})\|_P \geq \|x(s;t_{k-1}) - \hat{x}^*(s;t_{k-1})\|_P$ for $s \in [t_{k-1}, t_k]$. Here $h \in [\beta T, T]$ is some positive real number. Note from Theorem 2.5 that we also have $\delta = \rho\overline{\lambda}(\sqrt{P})\left[e^{Lh}\left(\frac{h}{L} - \frac{1}{L^2}\right) + \frac{1}{L^2}\right]$, where the triggering level δ is designed as the integral of $\|x(s;t_{k-1}) - \hat{x}^*(s;t_{k-1})\|_P$ from t_{k-1} to $t_{k-1} + h$. By following some calculation, we can obtain that

$$\rho\overline{\lambda}(\sqrt{P})\left[e^{Lh}(h - \frac{1}{L}) + \frac{1}{L}\right] = L\delta \tag{2.18}$$

and consequently it follows that

$$\sigma(t_{k-1}+h;t_{k-1}) \leq \rho\overline{\lambda}(\sqrt{P})e^{Lh}h \leq L\delta\frac{h}{h - \frac{1}{L}} \tag{2.19}$$

where $\sigma(t_{k-1}+h;t_{k-1}) \triangleq \|x(t_{k-1}+h;t_{k-1}) - \hat{x}^*(t_{k-1}+h;t_{k-1})\|_P$ and $L\beta T > 1$. Since the function $\frac{h}{h-\frac{1}{L}}$ gets its maximum at $h = \beta T$, the above inequality becomes

$$\|e(t_k;t_k)\|_P \leq \sigma(t_{k-1}+h;t_{k-1}) \leq \frac{L^2\beta T}{L\beta T - 1}\delta \tag{2.20}$$

According to Gronwall-Bellman inequality, one can obtain (2.15) by substituting (2.20) to (2.17). The proof is thus completed. □

Now we can analyze the iterative feasibility of the MPC problem (2.4), implying that if the MPC problem admits a solution at current time instant then a feasible solution exists for the next time instant. To prove this result, we use a conventional feasible control sequence candidate $\tilde{u}(s;t_k)$ at time instant t_k defined in (2.12), where $\tilde{u}(s;t_k) = \hat{u}^*(s;t_{k-1})$ for $s \in [t_k, t_{k-1}+T]$ and $\tilde{u}(s;t_k) = K\tilde{x}(s;t_k)$ for $s \in (t_{k-1}+T, t_k+T]$. In the following theorem, we will show that the designed control sequence candidate $\tilde{u}(s;t_k)$ can steer the feasible state $\tilde{x}(s;t_k)$ into $\Omega(\alpha\epsilon)$ if some conditions can be satisfied. In addition, it is also necessary to show that the candidate state $\tilde{x}(s;t_k)$ will fulfill the designed state constraint (2.7).

Assumption 2.7. *The optimization problem (2.4) admits a feasible solution $\hat{u}^*(s;t_0)$ at the initial time t_0.*

Theorem 2.8 (Feasibility)**.** *Suppose that Assumptions 2.1 and 2.7 hold. The MPC problem (2.4) is iteratively feasible under the following conditions:*

$$\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\rho\overline{\lambda}(\sqrt{P})\left[e^{L\beta T}\left(\frac{\beta T}{L}-\frac{1}{L^2}\right)+\frac{1}{L^2}\right]\leq(1-\alpha)\epsilon \tag{2.21}$$

$$T\geq\max\left\{-2\frac{\overline{\lambda}(P)}{\underline{\lambda}(Q^*)\beta}\ln\alpha,\frac{1}{L\beta}\right\} \tag{2.22}$$

$$M\geq\max\left\{\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\frac{\delta}{\alpha\epsilon}+1,1-\frac{1}{\beta}+\frac{1}{\alpha\beta}\right\} \tag{2.23}$$

Moreover, the maximum allowable disturbance can be given as

$$\rho\leq\frac{(1-\alpha)\epsilon}{\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\overline{\lambda}(\sqrt{P})\left[e^{L\beta T}\left(\frac{\beta T}{L}-\frac{1}{L^2}\right)+\frac{1}{L^2}\right]} \tag{2.24}$$

Proof. First, we show that the designed control sequence $\tilde{u}(s;t_k)$ for $s\in[t_k,t_{k-1}+T]$ drives $\tilde{x}(s;t_k)$ into $\Omega(\epsilon)$, i.e. $\|\tilde{x}(s;t_k)\|_P\leq\epsilon$. Let us construct an error norm $\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_P$ for $s\in[t_k,t_{k-1}+T]$. By using Corollary 2.6.1, we can obtain that

$$\sup_{s\in[t_k,t_{k-1}+T]}\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_P\leq\frac{L^2\beta T}{L\beta T-1}e^{L(1-\beta)T}\delta \tag{2.25}$$

which turns out that $\|\tilde{x}(t_{k-1}+T;t_k)-\hat{x}^*(t_{k-1}+T;t_{k-1})\|_P\leq\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\delta$. With help of the Triangle inequality, we have

$$\|\tilde{x}(t_{k-1}+T;t_k)\|_P\leq\|\hat{x}^*(t_{k-1}+T;t_{k-1})\|_P+\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\delta \tag{2.26}$$

which implies that $\|\tilde{x}(t_{k-1}+T;t_k)\|_P\leq\alpha\epsilon+\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\delta$.

Note from Theorem 2.5 that the triggering level is designed as $\delta=\rho\overline{\lambda}(\sqrt{P})\cdot\left[e^{L\beta T}\left(\frac{\beta T}{L}-\frac{1}{L^2}\right)+\frac{1}{L^2}\right]$. In order to steer the candidate state sequence $\tilde{x}(t_{k-1}+T;t_k)$ into $\Omega(\epsilon)$, one can simply deduce that the following inequality must hold:

$$\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\rho\overline{\lambda}(\sqrt{P})\left[e^{L\beta T}\left(\frac{\beta T}{L}-\frac{1}{L^2}\right)+\frac{1}{L^2}\right]\leq(1-\alpha)\epsilon \tag{2.27}$$

From (2.27), it can be also obtained that the maximum bound for disturbance satisfies (2.24).

Second, we consider the candidate sequence $\tilde{x}(s;t_k)$ for $s \in (t_{k-1}+T, t_k+T]$. Then using Lemma 2.2, we can verify that $\Omega(\epsilon)$ is an invariant set for the closed-loop system $\dot{\tilde{x}}(s;t_k) = f\left(\tilde{x}(s;t_k), K(\tilde{x}(s;t_k))\right)$. Consequently, we can deduce that $\dot{V}(\tilde{x}(s;t_k)) \leq -\|\tilde{x}(s;t_k)\|^2_{Q^*}$. By the virtue of comparison principle, it follows that

$$V(\tilde{x}(s;t_k)) \leq \epsilon^2 e^{-\frac{\underline{\lambda}(Q^*)}{\overline{\lambda}(P)}(s-t_{k-1}-T)} \tag{2.28}$$

for $s \in (t_{k-1}+T, t_k+T]$, which indicates that $V(\tilde{x}(t_k+T;t_k)) \leq \epsilon^2 e^{-\frac{\underline{\lambda}(Q^*)}{\overline{\lambda}(P)}(t_k-t_{k-1})}$. By using Theorem 2.5, we can have $\inf(t_k - t_{k-1}) = \beta T$. To obtain $\|\tilde{x}(t_k+T;t_k)\|_P \leq \alpha\epsilon$, it is equivalent to show that $V(\tilde{x}(t_k+T;t_k)) \leq \alpha^2\epsilon^2$. With some calculation, one can have $T \geq -2\frac{\overline{\lambda}(P)}{\underline{\lambda}(Q^*)\beta}\ln\alpha$ such that the previous inequality holds. Similar argument can be found in [43].

Third, we show that $\tilde{x}(s;t_k)$ satisfies the state constraint (2.7). For $s \in (t_k, t_{k-1}+T]$, one can get

$$\|\tilde{x}(s;t_k)\|_P \leq \|\hat{x}^*(s;t_{k-1})\|_P + \frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T - 1}\delta \tag{2.29}$$

which can be derived from (2.15). Then we need to prove

$$\frac{(t_k+T-s)M + s - t_k}{T}\alpha\epsilon \leq \frac{(t_{k-1}+T-s)M + s - t_{k-1}}{T}\alpha\epsilon + \frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T - 1}\delta \tag{2.30}$$

By some calculation, it can be obtain that $M \geq \frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T - 1}\frac{\delta}{\alpha\epsilon} + 1$. For $s \in (t_{k-1}+T, t_k+T]$, it can be deduced from (2.28) that

$$\|\tilde{x}(s;t_k)\|_P \leq \epsilon e^{-\frac{\underline{\lambda}(Q^*)}{\overline{\lambda}(P)}(s-t_{k-1}-T)/2} \tag{2.31}$$

In order to prove $\|\tilde{x}(s;t_k)\|_P \leq \frac{(t_k+T-s)M+s-t_k}{T}\alpha\epsilon$, it is equivalent to show

$$\frac{(t_k+T-s)M + s - t_k}{T}\alpha\epsilon \geq \epsilon e^{-\frac{\underline{\lambda}(Q^*)}{\overline{\lambda}(P)}(s-t_{k-1}-T)/2} \tag{2.32}$$

For brevity, we denote $F(s) = \frac{T/\alpha\cdot e^{-\frac{\underline{\lambda}(Q^*)}{\overline{\lambda}(P)}(s-t_{k-1}-T)/2} + t_k - s}{t_k+T-s}$, and it turns out that $M \geq F(s)$. By evaluating the derivative of $F(s)$, it can be verified that $F'(s)$ is non-positive for $s \in (t_{k-1}+T, t_k+T]$, which indicates $M \geq 1 - \frac{1}{\beta} + \frac{1}{\alpha\beta}$. Finally, the

designing parameter should be configured as $M \geq \max\{\frac{L^2\beta T e^{L(1-\beta)T}}{L\beta T-1}\frac{\delta}{\alpha\epsilon}+1, 1-\frac{1}{\beta}+\frac{1}{\alpha\beta}\}$ for guaranteeing the satisfaction of the proposed robustness constraint. The proof is completed. □

Remark 2.9. *Note from Theorem 2.8 that the feasibility can be affected by the prediction horizon T, the Lipschitz constant L, and the disturbance bound ρ. In order to achieve the recursive feasibility, the prediction horizon T and the design parameter M in (2.7) should be both lower bounded. It should be also noted that the maximum allowable disturbance bound can be estimated according to (2.24).*

2.4.2 Stability Analysis

In this part, we investigate the closed-loop stability by applying the proposed integral-type ET-MPC. It is worthwhile to point out that, due to the disturbance, the established closed-loop stability property can steer system states into an invariant set. Under the MPC configuration, the analysis for stability can be divided into two steps: 1) The first step is to ensure that the system trajectory will enter the terminal set in finite time; 2) the second step is to prove that the closed-loop system is stable after the state enters the terminal set.

Theorem 2.10 (Stability)**.** *Suppose that Assumptions 2.1 and 2.7 hold, and the conditions in Theorem 2.8 are satisfied. The state of the closed-loop system (2.11) enters the designed terminal set in finite time and converges to $\Omega(\bar{\epsilon})$ if the following condition holds for some $n \in \mathbb{N}$:*

$$\begin{aligned}&\frac{\overline{\lambda}(Q)}{\underline{\lambda}(P)}\frac{L^2(1-\beta)T}{L\beta T-1}e^{L(1-\beta)T}\delta\left[\frac{L^2\beta T}{L\beta T-1}e^{L(1-\beta)T}\delta+2[(1-\beta)M+\beta]\alpha\epsilon\right]\\&+\frac{L^4\beta T}{(L\beta T-1)^2}e^{2L(1-\beta)T}\delta^2\leq\frac{\underline{\lambda}(Q)n}{\overline{\lambda}(P)(n+1)}\left(\alpha\epsilon-\frac{L^2\beta T}{L\beta T-1}\delta\right)^2\end{aligned}\tag{2.33}$$

Proof. This theorem will be proved by two steps.

Step 1: For all initial state $x(t_0) \in \mathcal{X} \setminus \Omega(\alpha\epsilon)$ where $\mathcal{X}$ is the initial feasible set for system state, we aim to show the state trajectory enters $\Omega(\alpha\epsilon)$ in finite time. In this situation, we construct an error term as $\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right) := J\left(\tilde{x}(s;t_k),\tilde{u}(s;t_k)\right)-$

$J\left(\hat{x}^*(s;t_{k-1}),\hat{u}^*(s;t_{k-1})\right)$. Expanding this term yields

$$\begin{aligned}
&\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right)\\
=&\int_{t_k}^{t_k+T}\|\tilde{x}(s;t_k)\|_Q^2+\|\tilde{u}(s;t_k)\|_R^2\mathrm{d}s+\|\tilde{x}(t_k+T;t_k)\|_P^2\\
&-\int_{t_{k-1}}^{t_{k-1}+T}\|\hat{x}^*(s;t_{k-1})\|_Q^2+\|\hat{u}^*(s;t_{k-1})\|_R^2\mathrm{d}s\\
&-\|\hat{x}^*(t_{k-1}+T;t_{k-1})\|_P^2
\end{aligned}\tag{2.34}$$

Substituting $\tilde{u}(s;t_k)$ in (2.12) to the above equation, we can obtain that

$$\begin{aligned}
\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right)=&\int_{t_{k-1}+T}^{t_k+T}\|\tilde{x}(s;t_k)\|_{Q^*}^2\mathrm{d}s\\
&+\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)\|_Q^2-\|\hat{x}^*(s;t_{k-1})\|_Q^2\\
&\qquad+\|\tilde{u}(s;t_k)\|_R^2-\|\hat{u}^*(s;t_{k-1})\|_R^2\mathrm{d}s\\
&-\int_{t_{k-1}}^{t_k}\|\hat{x}^*(s;t_{k-1})\|_Q^2+\|\hat{u}^*(s;t_{k-1})\|_R^2\mathrm{d}s\\
&+\|\tilde{x}(t_k+T;t_k)\|_P^2-\|\hat{x}^*(t_{k-1}+T;t_{k-1})\|_P^2
\end{aligned}\tag{2.35}$$

Note from Lemma 2.2 that $\dot{V}(\tilde{x}(s;t_k))\le-\|\tilde{x}(s;t_k)\|_{Q^*}^2$. Taking integral from $t_{k-1}+T$ to t_k+T of the above inequality yields

$$\begin{aligned}
&\int_{t_{k-1}+T}^{t_k+T}\dot{V}(\tilde{x}(s;t_k))\mathrm{d}s\\
=&\|\tilde{x}(t_k+T;t_k)\|_P^2-\|\tilde{x}(t_{k-1}+T;t_k)\|_P^2\\
\le&-\int_{t_{k-1}+T}^{t_k+T}\|\tilde{x}(s;t_k)\|_{Q^*}^2\mathrm{d}s
\end{aligned}\tag{2.36}$$

Applying this fact to $\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right)$, it can be shown that

$$\begin{aligned}
&\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right)\\
\leq&\underbrace{\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)\|_Q^2-\|\hat{x}^*(s;t_{k-1})\|_Q^2\mathrm{d}s}_{\Delta\tilde{J}_1}\\
&\underbrace{-\int_{t_{k-1}}^{t_k}\|\hat{x}^*(s;t_{k-1})\|_Q^2+\|\hat{u}^*(s;t_{k-1})\|_R^2\mathrm{d}s}_{\Delta\tilde{J}_2}\\
&+\underbrace{\|\tilde{x}(t_{k-1}+T;t_k)-\hat{x}^*(t_{k-1}+T;t_{k-1})\|_P^2}_{\Delta\tilde{J}_3}
\end{aligned}\tag{2.37}$$

To analyze the above inequality, we firstly consider the term

$$\Delta\tilde{J}_1=\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)\|_Q^2-\|\hat{x}^*(s;t_{k-1})\|_Q^2\mathrm{d}s\tag{2.38}$$

By using the triangle inequality, we have

$$\begin{aligned}
\Delta\tilde{J}_1\leq&\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_Q^2\mathrm{d}s\\
&+2\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_Q\cdot\|\hat{x}^*(s;t_{k-1})\|_Q\mathrm{d}s
\end{aligned}\tag{2.39}$$

Then apply Holder inequality, and it follows that

$$\begin{aligned}
\Delta\tilde{J}_1\leq&\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_Q\mathrm{d}s\\
&\cdot\max_s\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_Q\\
&+2\int_{t_k}^{t_{k-1}+T}\|\tilde{x}(s;t_k)-\hat{x}^*(s;t_{k-1})\|_Q\mathrm{d}s\cdot\max_s\|\hat{x}^*(s;t_{k-1})\|_Q
\end{aligned}\tag{2.40}$$

Using the result in Corollary 2.6.1 and the robustness constraint (2.7), it can be calculated that

$$\Delta\tilde{J}_1\leq\frac{\overline{\lambda}(Q)}{\underline{\lambda}(P)}\frac{L^2\beta T(1-\beta)T}{L\beta T-1}e^{L(1-\beta)T}\delta\cdot\left[\frac{L^2\beta T}{L\beta T-1}e^{L(1-\beta)T}\delta+2[(1-\beta)M+\beta]\alpha\epsilon\right]\tag{2.41}$$

For the second term

$$\Delta\tilde{J}_2 = -\int_{t_{k-1}}^{t_k} \|\hat{x}^*(s;t_{k-1})\|_Q^2 + \|\hat{u}^*(s;t_{k-1})\|_R^2 \mathrm{d}s \tag{2.42}$$

it follows that

$$\Delta\tilde{J}_2 \leq -\int_{t_{k-1}}^{t_k} \|\hat{x}^*(s;t_{k-1})\|_Q^2 \mathrm{d}s \tag{2.43}$$

Since $x(t_0) \in \mathcal{X} \setminus \Omega(\alpha\epsilon)$, we can have $\Delta\tilde{J}_2 \leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\beta T(\alpha\epsilon - \frac{L^2\beta T}{L\beta T-1}\delta)^2$. By Corollary 2.6.1, one can get the following result for the third term:

$$\Delta\tilde{J}_3 \leq \frac{L^4\beta^2T^2}{(L\beta T-1)^2} e^{2L(1-\beta)T}\delta^2 \tag{2.44}$$

Consequently, it can be obtained that

$$\Delta\tilde{J}\left(x(s;t_k),u(s;t_k)\right) \leq \sum_{\ell=1}^{3}\Delta\tilde{J}_i \leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)(n+1)}\beta T(\alpha\epsilon - \frac{L^2\beta T}{L\beta T-1}\delta)^2 \tag{2.45}$$

if the stability condition (2.33) is satisfied. Due to the sub-optimality of the designed control $\tilde{u}(s;t_k)$ at t_k, we can achieve that the deceasing properties of the optimal cost function at t_{k-1} and t_k is guaranteed by $\Delta J\left(\hat{x}^*(s;t_{k-1}),\hat{u}^*(s;t_{k-1})\right) \leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)(n+1)}\beta T(\alpha\epsilon - \frac{L^2\beta T}{L\beta T-1}\delta)^2$, which consequently shows that the optimal cost functional J^* is decreasing as t approaches to infinity. Since the nominal state $\tilde{x}$ stays outside $\Omega(\alpha\epsilon)$, it thus follows that the lower bound for the decreasing of optimal functional J^* is a positive constant. Assume that the nominal state $\tilde{x}$ cannot converge to the terminal set $\Omega(\alpha\epsilon)$ in finite time, then the optimal functional will decrease to $-\infty$ as time evolves to infinity, which is a contradiction to the fact that the optimal functional is quadratic. Similar argument can be found in [24, 43].

Step 2: For all initial state $x(t_0) \in \Omega(\alpha\epsilon)$, we need to prove that the closed-loop system (2.11) converges to $\Omega(\bar{\epsilon})$. Using the fact that $\hat{x}^*(s;t_{k-1}) \in \Omega(\alpha\epsilon)$, $\Delta\tilde{J}_1$ in (2.40) can be rewritten as

$$\Delta\tilde{J}_1 \leq \frac{\overline{\lambda}(Q)}{\underline{\lambda}(P)}\frac{4\alpha\epsilon L^2\beta T(1-\beta)T}{L\beta T-1} e^{L(1-\beta)T}\delta \tag{2.46}$$

For the second term $\Delta\tilde{J}_2$ in (2.43), we have the following inequality hold by Lemma 2.2:

$$\Delta\tilde{J}_2 \leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\beta T\|\hat{x}^*(t_k;t_{k-1})\|_P^2 \tag{2.47}$$

According to the event-triggering condition, we can have $\|x(t_k)-\hat{x}^*(t_k;t_{k-1})\|_P^2 \leq \left(\frac{L^2\beta T}{L\beta T-1}\delta\right)^2$ by following a similar procedure in Corollary 2.6.1. Then applying the above inequality to (2.47) yields

$$\begin{aligned}\Delta\tilde{J}_2 &\leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\beta T\left[\|x(t_k)\|_P^2-\left(\frac{L^2\beta T}{L\beta T-1}\delta\right)^2\right]\\ &\leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\beta T\|x(t_k)\|_P^2+\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\frac{L^4\beta^2T^2}{(L\beta T-1)^2}\delta^2\end{aligned} \tag{2.48}$$

Combining (2.46), (2.48) and (2.44), it follows that $\Delta J \leq \Delta\tilde{J}_1+\Delta\tilde{J}_2+\Delta\tilde{J}_3 \leq -\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\beta T\|x(t_k)\|_P^2+\frac{\underline{\lambda}(Q)}{\overline{\lambda}(P)}\frac{L^4\beta^2T^2}{(L\beta T-1)^2}\delta^2+\frac{\overline{\lambda}(Q)}{\underline{\lambda}(P)}\frac{4\alpha\epsilon L^2\beta T(1-\beta)T}{L\beta T-1}e^{L(1-\beta)T}\delta+\frac{L^4\beta^2T^2}{(L\beta T-1)^2}e^{2L(1-\beta)T}\delta^2$, which implies that the sate will converge to the set $\Omega(\bar{\epsilon})$ with $\bar{\epsilon}=\left(1+\frac{\overline{\lambda}(P)}{\underline{\lambda}(Q)}e^{2L(1-\beta)T}\right)\frac{L^4\beta T}{(L\beta T-1)^2}\delta^2+\frac{\overline{\lambda}(P)}{\underline{\lambda}(Q)}\frac{\overline{\lambda}(Q)}{\underline{\lambda}(P)}\frac{4\alpha\epsilon L^2(1-\beta)T}{L\beta T-1}e^{L(1-\beta)T}\delta$. Then the proof is completed by summarizing Step 1 and Step 2. □

Remark 2.11. *The inequality (2.33) shows that the stability can be guaranteed by properly designing the prediction horizon T, the triggering level δ, and the contraction rate M for the robustness constraint. The larger triggering level δ leads to less frequent sampling events by sacrificing the control performance, whereas the larger prediction horizon T usually provides better control performance due to the fact that longer state evolution is considered in the optimization. However, solving the MPC problem with larger prediction horizon T consumes more computation resources. Thus, a trade-off should be considered when designing the parameters T and δ in terms of the control performance.*

2.5 Simulation Results

Consider a nonlinear cart-damper-spring system with the following dynamics [43]:

$$\begin{cases}\dot{x}_1(t)=x_2(t)\\ \dot{x}_2(t)=-\frac{\tau}{M_c}e^{-x_1(t)}x_1(t)-\frac{h_d}{M_c}x_2(t)+\frac{u(t)}{M_c}+\frac{\omega(t)}{M_c}\end{cases}$$

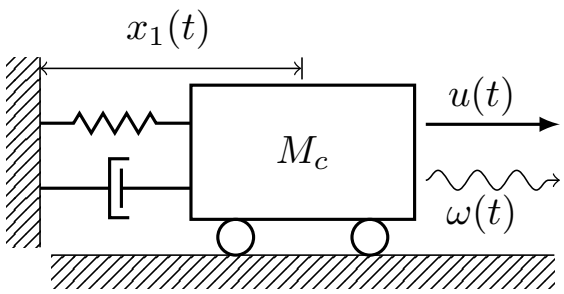

Fig. 2.2: The schematic illustration of a cart-damper-spring system.

where $x_1(t)$ denotes the displacement of the cart, $x_2(t)$ is the velocity, its mass $M_c = 1.25\,\text{kg}$, the nonlinear factor $\tau = 0.9\,\text{N/m}$, the damping factor $h_d = 0.42\,\text{N*s/m}$, and the constrained control input $u(t) \in [-1, 1]$. The Lipschitz constant L is 1.4. For this integral-type ET-MPC, we choose the weighted matrices $Q = [0.1, 0.0; 0.0, 0.1]$ and $R = 0.1$. Then the LQR feedback gain for (2.3) can be calculated as $K = [-0.4454, -1.0932]$. According to Lemma 2.2, the corresponding P matrix is designed as $P = [0.1692, 0.0572; 0.0572, 0.1391]$ and the terminal set level is determined as $\epsilon = 0.03$. We choose the scaling ratio of the terminal set as $\alpha = 0.8$ and the parameter as $\beta = 0.6$. In addition, $T = 2.0\,\text{s}$ and $M = 10$ are chosen to satisfy the feasibility and stability conditions (2.21), (2.22), (2.33). Therefore, the minimum inter-execution time is $\beta T = 1.2\,\text{s}$. By using (2.24) in Theorem 2.8, the maximum allowable disturbance is calculated as $\rho_{\max} = 0.00058$. Thus the additive disturbance can be configured as $\rho = 0.00031$. The triggering level is chosen as $\delta = 8.1 \times 10^{-5}$ in order to satisfy the stability condition (2.33).

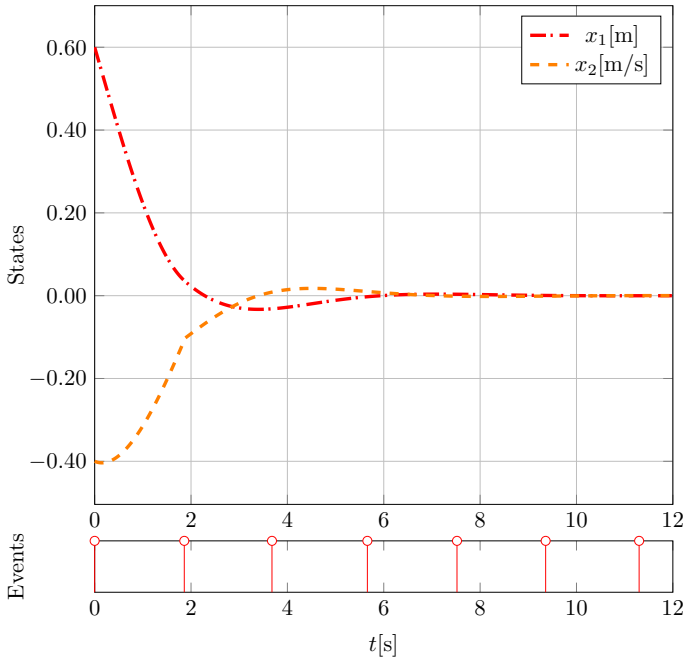

Fig. 2.3: States trajectories of the closed-loop system (2.11) driven by integral-type ET-MPC (2.4), and event-triggering instants with condition (2.9). The red circle denotes the event-triggering instant.

We use IPOPT [122] to solve the online optimization problem. Fig. 2.3 shows the state trajectory and event-triggering instants by using Algorithm 2.1 given the initial state $x_0 = [0.6, -0.4]$. Under the same initial state, the ET-MPC algorithm in [43] is not feasible, which might indicate that the proposed integral-type ET-MPC scheme with less-conservative robustness constraint can admit an enlarged initial feasible region. For comparison purposes, we conduct another numerical example in Fig. 2.4, where the initial states are set as $x_0 = [0.3, -0.2]$ to satisfy the initial feasibility of both the conventional ET-MPC and the integral-type ET-MPC. In order to further show the advantages of the proposed integral-type ET-MPC scheme, we have also done two Monte-Carlo simulations to compare the communication performance with that of the conventional ET-MPC, where the communication performance is measured by the average sampling time of all the simulations. The simulation results show that the average sampling time of our approach is 6.38 which outperforms 6.66 of the conventional ET-MPC. One can see that the integral-type ET-MPC can save considerable communication resource by performing less frequent event-triggered samplings, which is more efficient than the conventional ET-MPC.

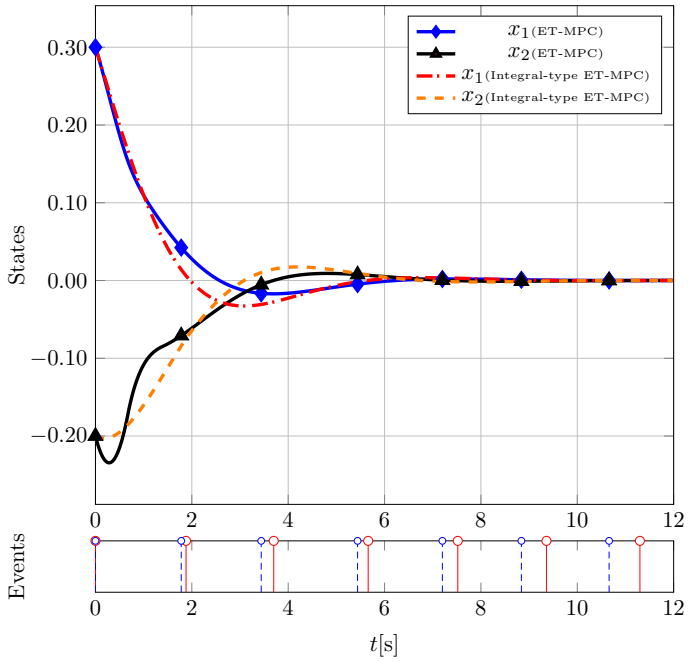

Fig. 2.4: Comparison of state trajectories and event-triggering instants by the integral-type ET-MPC and the conventional ET-MPC in [43]. The red circle denotes the event-triggering instant by our method and the blue one denotes the event-triggering instant by the conventional ET-MPC.

2.6 Conclusion

In this chapter, an integral-type ET-MPC scheme has been designed for nonlinear systems with additive disturbance. The integral-type ETM has shown considerable improvement on avoiding unnecessary communication. A new less conservative robustness constraint was proposed to handle the additive disturbance. In addition, we showed that the feasibility and stability properties were related to the prediction horizon, the disturbance bound, the triggering level, and the contraction rate for the robustness constraint. The simulation and comparison study demonstrated the effectiveness of proposed method.

Chapter 3

Secure Model Predictive Control of CPSs under DoS Attacks

3.1 Introduction

In this chapter, we aim to design secure control strategies for constrainedCPSs with actuator saturations and state constraints in the presence of DoS attacks. With the rapid development of IT and industrial informatics, the combination of physical layers and cyber layers has inevitably left CPSs exposed to the joint effects of disturbances from the physical environment and malicious cyber attacks from the cyber space (e.g., deception attacks and DoS attacks [3]), which might cause severe issues such as dramatic performance degradation or even system failure [4]. These critical issues give rise to a new type of controller design problems for CPSs in response to those joint effects from the cyber-physical world. Recently, secure control, as a new concept to control systems, is proposed as an important tool to tackle such issues [9, 21], aiming at keeping an acceptable level of operational normalcy in the presence of these attacks while maintaining system robustness against disturbances. Recent results to secure control of CPSs can be found in [11, 25, 74, 75, 88, 89, 101].

The objectives are to design and analyze secure controllers that can simultaneously handle both DoS attacks and physical system constraints. We consider a networked control system, in which the plant, along with a sensor and an actuator, and the controller are interconnected via communication networks. The controller receives sensor measurements and sends control signals both through communication networks. The DoS attacks corrupt the communication channel between the controller and the ac-

tuator, by which the malicious adversaries is able to degrade the control performance or even destabilize the overall system. There have been many research efforts focused on stability of networked control systems under DoS attacks [25, 75, 84, 88]. However, these results may not be applied to the case when physical system constraints are present. Hence, we propose a variant of dual-mode MPC to address this problem. The main contributions include: 1) A dual-mode MPC algorithm is proposed to compensate the effect induced by the DoS attacks, where the control input and state constraints are fulfilled by introducing the modified initial feasible set to the MPC optimization problem. 2) The maximum allowable duration of DoS attacks is obtained for the closed-loop system by using the μ-step positively invariant set. We theoretically show that, under the DoS attacks, the state trajectories, commencing in a given ellipsoidal set, will enter this set after μ steps. 3) Exponential stability of the closed-loop system with the dual-mode MPC control law is also proved under conditions that the duration of DoS attacks is constrained and the MPC parameters are properly designed.

The reminder of this chapter is organized as follows. In Section 3.2, we describe the secure MPC framework. Section 3.3 gives the main theoretical results of this chapter. In Section 3.4, we conduct numerical examples and comparisons to illustrate the effectiveness of the proposed method. Finally, we conclude this work in Section 3.5.

Notations: The symbols $\mathbb{R}$, $\mathbb{N}$ and $\mathbb{N}^+$ represent the sets of all real numbers, all natural numbers and all positive integers. Let $\mathbb{N}_{[k,k+N]} \triangleq \{a \in \mathbb{N} | k \leq a \leq k+N\}$ and $\mathbb{N}_{[k,k+N)} \triangleq \{a \in \mathbb{N} | k \leq a < k+N\}$, where $k \in \mathbb{N}, N \in \mathbb{N}^+$. The union, intersection and complement of two sets $\mathcal{X}$ and $\mathcal{Y}$ are denoted by $\mathcal{X} \bigcup \mathcal{Y}$, $\mathcal{X} \bigcap \mathcal{Y}$ and $\mathcal{X} \backslash \mathcal{Y}$. Let $A \in \mathbb{R}^{n \times n}$ be a square matrix, then A^n is defined as the matrix product of n copies of A. The spectral norm of A is denoted by $\|A\|_2 = \sqrt{\lambda_{\max}(A^\top A)} = \sigma_{\max}(A)$, where $\lambda_{\max}(\cdot)$ and $\sigma_{\max}(\cdot)$ denote the largest eigenvalue and the largest singular value of a matrix. We denote a positive definite matrix and positive semi-definite matrix as $P \succ 0$ and $P \succeq 0$. Given a vector $x \in \mathbb{R}^n$ and $P \succ 0$, the following vector norms will be used throughout this chapter: Euclidean norm $\|x\|_2 := \sqrt{\sum_{i=1}^{n} |x_i|^2}$ and P-weighted norm $\|x\|_P^2 := x^\top P x$. The cardinality of a given set $\mathcal{X}$ is defined as card $(\mathcal{X})$ denoting the number of its basic elements.

3.2 Secure MPC Framework

3.2.1 System Setup

We consider the following LTI system

$$x_{k+1} = Ax_k + Bu_k \tag{3.1}$$

where $x_k \in \mathbb{R}^n$ is the system state, $u_k \in \mathbb{R}^m$ is the control input and k is the time. The system state and control input satisfy the state constraint and control input constraint as $x_k \in \mathcal{X}$ and $u_k \in \mathcal{U}$, where $\mathcal{X}$ and $\mathcal{U}$ are compact sets containing the origin as an interior point.

Assumption 3.1. *For the system in (3.1), there exists a linear state-feedback gain K such that $A + BK$ is stable.*

For each $x_k \in \mathcal{X}$, the $N \in \mathbb{N}^+$ steps state prediction can be obtained iteratively by using the system model in (3.1), i.e.,

$$x_{k+i+1|k} = Ax_{k+i|k} + Bu_{k+i|k},\ i \in \mathbb{N}_{[0,N-1]} \tag{3.2}$$

where $u_{k+i|k}$ denotes the control variable to be determined and $x_{k+i|k}$ represents the resulting predicted state at the $(k+i)$th prediction step. It should be noted that the prediction model in (3.2) and the control variables $u_{k|k}, u_{k+1|k}, \ldots, u_{k+N-1|k}$ will be used as the equality constraint and decision variables in the optimization problem, which will be later introduced in Section 3.2.2.

The DoS attacks that might be occurring in the C-A communication channel is considered in this chapter. The attacker is only capable of launching limited times attacks due to its finite power energy.

Definition 3.2 (DoS Attack Duration Constraint)**.** *Given the DoS attack sequence defined by (1.8), the DoS attack is said to be duration-constrained on the time interval from k_j to $k_j + N - 1$ if*

$$\text{card}\left(\Xi(k_j, k_j + N - 1)\right) = M < N \tag{3.3}$$

Remark 3.3. *The DoS attack duration denotes the total time on which the C-A communication channel is jammed. Specifically, the DoS attack having larger duration*

can make the communication channel unavailable for more time. In addition, there might exist some extreme cases where the C-A channel can be totally disabled such that any control input cannot be transmitted. Thus, it is reasonable to assume that the DoS attack is constrained by (3.3), which indicates that the total duration of DoS attacks cannot exceed the time horizon N.

3.2.2 Secure Control Law

The secure control law implements a dual-mode MPC strategy, which combines an optimization-based control law and a state-feedback control law. The optimization-based control is firstly used to steer the system state into a predefined set, and the state-feedback control law is applied after the state enters this set. Due to the presence of DoS attacks in the C-A channel, the conventional dual-mode MPC needs to be adapted to the adverse network environment.

Let us first introduce the optimization problem for obtaining the optimal control law. For the system in (3.1), the MPC cost function is defined as

$$V_N(x_k, \boldsymbol{u}_k) \triangleq \sum_{i=0}^{N-1} L(x_{k+i|k}, u_{k+i|k}) + V_f(x_{k+N|k}) \tag{3.4}$$

where $i \in \mathbb{N}_{[0,N-1]}$, $x_k = x_{k|k}$, and $\boldsymbol{u}_k = \{u_{k|k}, u_{k+1|k}, \ldots, u_{k+N-1|k}\}$. We use a quadratic form for the stage cost and terminal cost functions, i.e.,

$$\begin{aligned} L(x_{k+i|k}, u_{k+i|k}) &\triangleq \|x_{k+i|k}\|_Q^2 + \|u_{k+i|k}\|_R^2 \\ V_f(x_{k+N|k}) &\triangleq \|x_{k+N|k}\|_P^2 \end{aligned} \tag{3.5}$$

where $Q, R, P \succ 0$. $\mathcal{X}_f$ and $V_f(\cdot)$ are the terminal constraint set and terminal cost function. The following assumptions are introduced for the terminal cost $V_f(\cdot)$ and terminal constraint $\mathcal{X}_f$, which can guarantee exponential stability of the linear system (see details in [15, 24, 123, 124]).

Assumption 3.4. *There exists a local control law $u_k = Kx_k$ for $x_{k+1} = Ax_k + Bu_k$ and a subset $\mathcal{X}_f$ of $\mathcal{X}$ such that, for all $x_k \in \mathcal{X}_f$,*

A1: $(A + BK)x_k \in \mathcal{X}_f$ and $Kx_k \in \mathcal{U}$;

A2: $V_f((A + BK)x_k) + L(x_k, Kx_k) \leq V_f(x_k)$.

Remark 3.5. *In particular, when the terminal cost function $V_f(x)$ is chosen as the value function of the unconstrained infinite-horizon optimal control problem (i.e., $V_f(x) = x^\top P_f x$ and P_f is the solution of the discrete-time algebraic Riccati equation), the above two assumptions can be satisfied (A2 is satisfied with equality) under the condition that the system in (3.1) is controllable (see details in [15]).*

Then the MPC optimization problem can be formulated as

$$\boldsymbol{u}_k^* = \arg\min_{\boldsymbol{u}_k \in \mathcal{U}} V_N(x_k, \boldsymbol{u}_k) \tag{3.6a}$$

$$\text{s.t.} \quad x_{k|k} = x_k \tag{3.6b}$$

$$x_{k+i+1|k} = Ax_{k+i|k} + Bu_{k+i|k} \tag{3.6c}$$

$$u_{k+i|k} \in \mathcal{U} \tag{3.6d}$$

$$x_{k+i|k} \in \mathcal{X} \tag{3.6e}$$

$$x_{k+N|k} \in \mathcal{X}_f \tag{3.6f}$$

Conventionally, the optimization-based control law can be obtained by iteratively implementing the first control signal $u_{k|k}^*$ of the current optimal control sequence $\boldsymbol{u}_k^*$. However, it might not be always viable to send $u_{k|k}^*$ owing to the DoS attack presence in the C-A channel. In order to maintain the system stability and control performance, we choose to send to the actuator the current optimal control sequence $\boldsymbol{u}_k^*$ instead of sending only one control signal. Because it is generally impossible to successfully send all the optimal control sequences, a buffer $\boldsymbol{u}_s^*$ installed on the actuator side is used to store the latest successfully transmitted optimal control sequence $\boldsymbol{u}_{k_j}^*$, where k_j represents the sampling time to be able to conduct a successful transmission. Since the optimization is solved at all time, all the successful sampling time $k_j, j = 0, 1, 2, \ldots$ constitute a set denoting as $\mathbb{N}\backslash\Xi(0, \infty)$.

Therefore, the dual-mode control signal applied to the open-loop system in (3.1) at the time k can be designed as

$$\kappa(k; k_j) = \begin{cases} u_{k|k_j}^* \\ K\nu_k x_k \text{ after } x_k \text{ enters } \mathcal{X}_f \end{cases} \tag{3.7}$$

where $k_j \in \mathbb{N}\backslash\Xi(0, \infty)$. With (3.7) and (3.1), the closed-loop system can be thus given by

$$x_{k+1} = Ax_k + B\kappa(k; k_j),\ j \in \{0, 1, 2, \ldots\} \tag{3.8}$$

The main objective of this chapter is to study stability of the closed-loop system in (3.8) under DoS attacks and to investigate the maximum allowable duration of DoS attacks.

Remark 3.6. *In fact, the constructed control law exploits the dual-mode control policy for the MPC problem (see, e.g, in [125]). In the dual-mode MPC design, the generated optimal control input $u^*_{k|k_j}$ will be applied to the system until the state enters $\mathcal{X}_f$. After the system state enters $\mathcal{X}_f$, the dual-mode MPC controller then operates in a linear state-feedback fashion permanently. The main advantages of using the dual-mode control for the proposed secure MPC framework are: 1) To guarantee exponential stability of the closed-loop system under DoS attacks, while maintaining the constraint satisfaction; 2) To save computation resource since the linear feedback control is used after the state enters the terminal set.*

3.3 Theoretical Results

3.3.1 Attack-Secure Terminal Constraint Set Design

In this section, a new terminal constraint set for dual-mode MPC will be designed for dealing with DoS attacks. This new set is a μ-step positively invariant set for the closed-loop system with linear state-feedback control. Specifically, we expect that, for any initial state in this predefined set, the linear state-feedback control law can steer state trajectories into this set after μ steps even in the presence of DoS attacks.

Let us firstly recall a well-known definition for the conventional positively invariant set.

Definition 3.7 (Positively Invariant Set [126])**.** *A set $\Omega \subseteq \mathbb{R}^n$ is said to be positively invariant for $x_{k+1} = f(x_k)$ if $x_0 \in \Omega$ implies that $x_k \in \Omega$ for all $k \in \mathbb{N}$.*

In general, it is always possible to find a positively invariant set for the system in (3.1). However, it may be impossible to find such a set for the system under DoS attacks. Thus, we introduce a relaxed version of the positively invariant set, which only requires the system state to be inside the set after several steps.

Definition 3.8 (μ-step Positively Invariant Set)**.** *Given a dynamic system $x_{k+1} = f(x_k)$ and trajectory x_k with the initial state $x_0 \in \Omega \subseteq \mathbb{R}^n$, if $x_0 \in \Omega$ implies that $x_{k+\mu} \in \Omega$ for some $\mu \in \mathbb{N}^+$ and all $k \in \mathbb{N}$, then Ω is said to be μ-step positively invariant for the dynamic system.*

Note that this concept of μ-step positively invariant set provides a general way for characterizing the set invariance property of the system under study. It is also worthwhile to point out that the intermediate states between step x_0 and x_μ can be either inside or outside the predefined invariant set Ω. That is to say, a μ-step positively invariant set is also a $(\mu+m)$-step positively invariant set, where $m \in \mathbb{N}^+$. The conventional positively invariant set can be regarded as a typical μ-step positively invariant set by letting $\mu = 1$.

Now we can present the main result of this section. A useful lemma is firstly recalled here.

Lemma 3.9. *[127] Let $Q \in \mathcal{C}^{n\times n}$ be a unitary matrix with its conjugate transpose Q^H, then $Q^H A Q = T = D + N$ is a Schur decomposition of $A \in \mathbb{R}^{n\times n}$, where D and N are, respectively, a diagonal matrix and a strictly upper triangular matrix. If $\gamma \geq 0$, then for all $k \in \mathbb{N}$ we have*

$$\|A^k\|_2 \leq (1+\gamma)^{n-1}\left(|\lambda_{\max}(A)| + \frac{\|N\|_F}{1+\gamma}\right)^k \tag{3.9}$$

where $\|\cdot\|_F$ denotes the Frobenius norm of a matrix.

In the following, we show that, under the duration-constrained DoS attacks, the controlled system by using linear state feedback control law admits a μ-step positively invariant set.

Lemma 3.10. *For the system in (3.1) under the DoS attack modeled by (1.8), suppose that there exist a stabilizable K satisfying Assumption 3.1, $Q \succ 0$, $R \succ 0$, the associated Lyapunov equation $(A+BK)^\top P(A+BK) - P = -(Q + K^\top R K)$, and an ellipsoidal set $\Omega_\alpha \triangleq \{x \in \mathbb{R}^n | \|x\|_P^2 \leq \alpha, \alpha > 0\}$ satisfying Assumption 3.4 (A1). If the inequality in (3.19) holds, then the following statements are true:*

1) There exists an ellipsoidal neighbourhood of the origin, i.e.,

$$\Omega_{\bar{\alpha}} \triangleq \left\{x \in \mathbb{R}^n | \|x\|_P^2 \leq \bar{\alpha}, \bar{\alpha} = \frac{\alpha}{h_* \lambda_*}\right\} \tag{3.10}$$

such that $\Omega_{\bar{\alpha}}$ serves as a μ-step positively invariant set for the underlying closed-loop system

$$x_{k+1} = (A + \nu_k BK)x_k \tag{3.11}$$

2) Kx_k belongs to $\mathcal{U}$, where x_k is the solution of (3.11) with the initial state $x_0 \in \Omega_{\bar{\alpha}}$.

Proof. First, we show that the conventional positively invariance does not hold when A is unstable. We first show that $\Omega_{\bar{\alpha}}$ is not a positively invariant set for the closed-loop system (3.11) under DoS attacks. Without loss of generality, we set $\nu_k = 0$ to indicate that the controller cannot send the kth control packet to the plant. Assume that x_k is on the boundary of $\Omega_{\bar{\alpha}}$ (i.e., $x_k \in \{x \in \mathbb{R}^n | \|x\|_P^2 = \bar{\alpha}\}$), then there must exist some x_k such that the next state $x_{k+1} = Ax_k$ is outside $\Omega_{\bar{\alpha}}$. This result can be proved by contradiction. Assuming that the next state x_{k+1} is inside $\Omega_{\bar{\alpha}}$, the following equation

$$x_k^\top A^\top P A x_k - x_k^\top P x_k < 0 \tag{3.12}$$

is true. By (3.12), we can have the equality

$$A^\top P A - P = -\xi I \tag{3.13}$$

holds for some $\xi \in (0, \infty)$, where I is the identity matrix. Note that $P \succ 0$ is the unique solution of (3.13). Then the existence of P requires that all the eigenvalues of A lie in the open unit disc, which contradicts the fact that A is not stable. Thus, the closed-loop system (3.11) is not positively invariant in $\Omega_{\bar{\alpha}}$ when A is not stable. Then consider the case when A is stable. Since $A + BK$ is also stable, then $\Omega_{\bar{\alpha}}$ is a positively invariant set for (3.11) under the condition that the equation (3.13) has a solution.

Then we show that $\Omega_{\bar{\alpha}}$ is a μ-step positively invariant set for (3.11) under the condition $A + BK$ is stable. First, we investigate the bound for the state trajectories of the open-loop system $x_{k+1} = Ax_k$ and the closed-loop system $x_{k+1} = (A + BK)x_k$, respectively. Since $A + BK$ is stable, based on Lemma 3.9, there always exist positive scalars $h_1 > h_2 \in (1, \infty)$, $|\lambda_{\max}(A)| < \lambda_1 < \sigma_{\max}(A)$ and $|\lambda_{\max}(A + BK)| < \lambda_2 < 1$ such that the following inequalities hold for all $k \in \mathbb{N}$, i.e.,

$$\|A^k\|_2 \leq h_1 \lambda_1^k, \quad \|(A + BK)^k\|_2 \leq h_2 \lambda_2^k \tag{3.14}$$

It is worthwhile to point out that h_1, λ_1 can be obtained by properly configuring γ according to Lemma 3.9, and h_2, λ_2 can be achieved by using Gelfand's Formula.

Based on the above results, we next estimate the finite-time state evolution under DoS attacks. For a fixed interval N from k_j to $k_j + N - 1$, the state at $k_j + N$ can

be calculated by

$$x_{k_j+N} = \left(\prod_{k=k_j}^{k_j+N-1} A + \nu_k BK \right) x_{k_j} \tag{3.15}$$

According to (3.3), there exist at most M distinct DoS attack instances on this fixed interval. Thus we have the following result by substituting (3.14) to (3.15):

$$\|x_{k_j+N}\|_2 \leq h_1^M h_2^{M+1} \lambda_1^M \lambda_2^{N-M} \|x_{k_j}\|_2 \tag{3.16}$$

Next we show that, if M is upper bounded, $h_1^M h_2^{M+1} \lambda_1^M \lambda_2^{N-M}$ can be approximated by $h_* \lambda_*^N < 1$, where $\lambda_* \in (\lambda_2, 1)$ and $h_* \in (1, \infty)$. Assume that

$$h_1^M h_2^{M+1} \lambda_1^M \lambda_2^{N-M} \leq h_* \lambda_*^N \tag{3.17}$$

and we have

$$h_1^M h_2^{M+1} \left(\frac{\lambda_1}{\lambda_2} \right)^M \leq h_* \left(\frac{\lambda_*}{\lambda_2} \right)^N \tag{3.18}$$

Consequently, the upper bound for M can be obtained as

$$M \leq \frac{-N \ln(\lambda_2) - \ln(h_2)}{\ln(h_1 h_2 \lambda_1) - \ln(\lambda_2)} \tag{3.19}$$

Then the μ-step invariance of (3.11) can be discussed as follows. Combining (3.16) with (3.17), we can get the relation between x_{k_j} and $x_{k_j+\mu}$, i.e.,

$$\|x_{k_j+\mu}\|_2 \leq h_* \lambda_*^\mu \|x_{k_j}\|_2 \tag{3.20}$$

Since the initial state $x_{k_j} \in \Omega_{\bar{\alpha}}$, there always exists a $\mu \leq N$ such that $h_* \lambda_*^\mu < 1$, and the system state will enter $\Omega_{\bar{\alpha}}$ after μ steps. That is to say, the system in (3.11) is μ-step positively invariant in $\Omega_{\bar{\alpha}}$. Based on Assumption 3.4 (A1), we have $Kx \in \mathcal{U}$ for all $x \in \Omega_\alpha$. Because the upper bound for the state trajectory of (3.11) evolves as (3.20), we have $\bar{\alpha} = \frac{\alpha}{\max\limits_{\mu} h_* \lambda_*^\mu} = \frac{\alpha}{h_* \lambda_*}$ such that $Kx_k \in \mathcal{U}$ for the trajectory x_k of (3.11) with the initial state $x_0 \in \Omega_{\bar{\alpha}}$. □

Remark 3.11. *Note from (3.16) and (3.20) that the upper bound for Euclidean norm of the terminal state x_{k_j+N} is given with respect to that of the initial state x_{k_j}. This bound is related to the system matrices A, B, feedback gain K and the DoS attack*

duration M. Lemma 3.10 also states that, for a stabilizable feedback gain K, the maximum allowable DoS attack duration can be given by (3.19) such that the system in (3.11) admits a μ-step positively invariant set. The state trajectories of the system, commencing in this set, are guaranteed to enter this set after μ steps.

3.3.2 Stability Analysis

In this section, we study the closed-loop stability by using the dual-mode control policy in (3.7). For the MPC optimization problem in (3.6), we can find an admissible control set $\mathcal{U}_N(x)$ along with an initial feasible set $\mathcal{X}_N$ (see details in [15]). For this purpose, we use a notation $x_i = \phi(i; x, \boldsymbol{u})$ to represent the ith solution of (3.1), where the control sequence $\boldsymbol{u} \stackrel{\triangle}{=} \{u_0, u_1, \ldots, u_{N-1}\}$ satisfies the control input constraint. Note that we omit the subscripts denoting the sampling time for the sake of simplicity. Hence, the admissible control set can be defined as

$$\mathcal{U}_N(x) = \{\boldsymbol{u} | u_i \in \mathcal{U}, \phi(i; x, \boldsymbol{u}) \in \mathcal{X}, \forall i \in \mathbb{N}_{[0,N-1]}, \phi(N; x, \boldsymbol{u}) \in \mathcal{X}_f\} \tag{3.21}$$

The initial feasible set can be therefore given by

$$\mathcal{X}_N \stackrel{\triangle}{=} \{x | \mathcal{U}_N(x) \neq \emptyset\} \tag{3.22}$$

It is worth pointing out that $\mathcal{X}_N$ is the region of attraction for the system in (3.1) by applying the calculated optimal control sequence [15]. However, $\mathcal{X}_N$ cannot be directly used as an initial feasible set for the closed-loop system in the presence of DoS attacks.

In the following, we will introduce a modified admissible control set to deal with DoS attacks. Note from (3.3) that there exist at most M consecutive attacks after a new sampling of the state is received by the MPC controller. When there is no optimal control sequence stored in actuator, the system operates in an open-loop fashion with the control input being zero. Hence, we introduce a new control sequence $\boldsymbol{u}^M = \{\underbrace{0, \ldots, 0}_{M}, \underbrace{u_M, u_{M+1}, \ldots, u_{N-1}}_{N-M}\}$, where the first M elements are zeros and the rest are required to satisfy the input constraint $\mathcal{U}$. Now, based on this new control

sequence, the modified admissible control set can be defined as

$$\begin{aligned}\mathcal{U}_N^M(x) = \{\boldsymbol{u} | u_i = 0, \forall i \in \mathbb{N}_{[0,M-1]}, u_i \in \mathcal{U}, \forall i \in \mathbb{N}_{[M,N-1]}, \\ \phi(i; x, \boldsymbol{u}) \in \mathcal{X}, \forall i \in \mathbb{N}_{[0,N-1]}, \phi(N; x, \boldsymbol{u}) \in \mathcal{X}_f\}\end{aligned} \tag{3.23}$$

Accordingly, the corresponding initial feasible set can be given by

$$\mathcal{X}_N^M \triangleq \left\{x | \mathcal{U}_N^M(x) \neq \emptyset\right\} \tag{3.24}$$

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

Assumption 3.12 (Existence of $\mathcal{X}_N^M$)**.** *There exists a maximum allowable M satisfying the duration constraint of DoS attacks in (3.3) such that $\mathcal{X}_N^M$ is nonempty.*

Remark 3.13. *This assumption guarantees that the MPC optimization problem in (3.6) is feasible in the presence of the duration-constrained DoS attacks. Note from (3.3) that there exist at most M consecutive DoS attacks such that the first M control input will be zero. Then by (3.24), a feasible control sequence $\boldsymbol{u}^M$ with its first M elements being zeros can be found, which can steer the state, starting from $\mathcal{X}_N^M$, into the terminal set $\mathcal{X}_f$ in N steps.*

Based on Assumption 3.12, we have the following result.

Lemma 3.14. *If Assumption 3.12 is satisfied, the following statement is true*

$$\mathcal{X}_N^M \subseteq \mathcal{X}_N^{M-1} \subseteq \ldots \subseteq \mathcal{X}_N^0 = \mathcal{X}_N \tag{3.25}$$

Proof. The proof begins with investigating the inclusion relation between the first two sets $\mathcal{X}_N^M$ and $\mathcal{X}_N^{M-1}$. By Assumption 3.12, there exists a feasible control sequence candidate $\hat{\boldsymbol{u}}^M = \{\hat{u}_0^M, \hat{u}_1^M, \ldots, \hat{u}_{N-1}^M\}$ such that $\mathcal{X}_N^M$ is nonempty, i.e., $x \in \mathcal{X}_N^M$ implies $x_N \in \mathcal{X}_f$ for all $\hat{\boldsymbol{u}}^M \in \mathcal{U}_N^M(x)$. From (3.23), we can get

$$\begin{aligned}&\hat{u}_i^M = 0, \forall i \in \mathbb{N}_{[0,M-1]}, \hat{u}_i^M \in \mathcal{U}, \forall i \in \mathbb{N}_{[M,N]}, \\ &\phi(i; x, \hat{\boldsymbol{u}}^M) \in \mathcal{X}, \forall i \in \mathbb{N}_{[0,N-1]}, \phi(N; x, \hat{\boldsymbol{u}}^M) \in \mathcal{X}_f\end{aligned} \tag{3.26}$$

Since the control input constraint $\mathcal{U}$ contains the origin, it thus follows that $\hat{u}_{M-1}^M = 0 \in \mathcal{U}$. Hence,

$$\begin{aligned}&\hat{u}_i^M = 0, \forall i \in \mathbb{N}_{[0,M-2]}, \hat{u}_i^M \in \mathcal{U}, \forall i \in \mathbb{N}_{[M-1,N]}, \\ &\phi(i; x, \hat{\boldsymbol{u}}^M) \in \mathcal{X}, \forall i \in \mathbb{N}_{[0,N-1]}, \phi(N; x, \hat{\boldsymbol{u}}^M) \in \mathcal{X}_f\end{aligned} \tag{3.27}$$

which shows that $\hat{\boldsymbol{u}}^M \in \mathcal{U}_N^{M-1}(x)$ and then consequently $\mathcal{U}_N^M(x) \subseteq \mathcal{U}_N^{M-1}(x)$. Similarly, we have $\mathcal{U}_N^M \subseteq \mathcal{U}_N^{M-1} \subseteq \ldots \subseteq \mathcal{U}_N^0 = \mathcal{U}_N$. By definitions of (3.22) and (3.24), we can deduce that (3.25) is valid. □

Remark 3.15. *Note that the modified admissible set $\mathcal{X}_N^M(x)$ is a subset of the original admissible set $\mathcal{X}_N(x)$. In the dual-mode MPC policy design, all the initial states starting from $\mathcal{X}_N^M$ are guaranteed to enter the terminal set $\mathcal{X}_f$ in finite time even in the presence of DoS attacks occurring at the C-A channel. However, $\mathcal{X}_N^M$ might be conservative due to the fact that the worst case of DoS attacks is considered.*

The exponential stability result are investigated in the following theorem.

Theorem 3.16 (Exponential Stability)**.** *For the system in (3.1) under the duration-constrained DoS attack modeled by (1.8), suppose that the Assumptions 3.4, 3.12 hold, and the control input is generated by (3.7). If the conditions in Lemma 3.10 are satisfied and the terminal set $\mathcal{X}_f$ is configured as (3.10), then the system in (3.8) is exponentially stable with a region of attraction $\mathcal{X}_N^M$.*

Proof. We first show feasibility of the secure MPC problem. It should be noticed from [15] that recursive feasibility of nominal MPC (without DoS attacks) can be guaranteed when the initial state $x_0 \in \mathcal{X}_N$. Then combining with Lemma 3.14, the proposed secure MPC problem admits feasible solutions for every time given all initial states commencing in $\mathcal{X}_N^M$. Therefore, the recursive feasibility of the proposed secure MPC is guaranteed. The proof of the closed-loop exponential stability can be divided into two steps. Step 1): All trajectories of the controlled system, starting from $\mathcal{X}_N^M \backslash \mathcal{X}_f$, are guaranteed to enter $\mathcal{X}_f$ in finite time; and Step 2): The closed-loop system is exponentially stable after the state enters $\mathcal{X}_f$.

Step 1): $x_0 \in \mathcal{X}_N^M \backslash \mathcal{X}_f$. In this situation, there always exists a positive real constant r such that $\|x_k\| \geq r$. Since we choose $L(x_k, u_k)$ as a quadratic function, it thus follows that $\|L(x_k, u_k)\| \geq \ell(r)$, where $\ell(0) = 0$, $\ell(r) > 0, \forall r \neq 0$ and $\lim_{r\to\infty} \ell(r) = \infty$. For the optimal control problem, we next show the monotonic property of the following value function $V_N^*(x_k) \triangleq V_N(x_k, \boldsymbol{u}_k^*)$, where $\boldsymbol{u}_k^* = \{u_{k|k}^*, u_{k+1|k}^*, \ldots, u_{k+N-1|k}^*\}$. By constructing a feasible control sequence candidate for the next step $k+1$, i.e.,

$$\tilde{\boldsymbol{u}}_{k+1} = \{u_{k+1|k}^*, u_{k+2|k}^*, \ldots, Kx_{k+N|k}\} \tag{3.28}$$

we have $V_N^*(x_k) - V_N^*(x_{k+1}) \geq V_N^*(x_k) - V_N(x_{k+1}, \tilde{\boldsymbol{u}}_{k+1}) = \sum_{i=0}^{N-1} L(x_{k+i|k}, u_{k+i|k}^*) + V_f(x_{k+N|k}) - \sum_{i=0}^{N-2} L(x_{k+i+1|k+1}, u_{k+i+1|k}^*) - L(x_{k+N|k+1}, Kx_{k+N|k}) - V_f(x_{k+N+1|k+1})$.

Due to the absence of state measurement inaccuracy, it follows that $x_{k+i+1|k+1} = x_{k+i+1|k}$ and $x_{k+N+1|k+1} = (A + BK)x_{k+N|k}$. Therefore, we can obtain $V_N^*(x_k) - V_N^*(x_{k+1}) \geq L(x_k, u_{k|k}^*) + V_f(x_{k+N|k}) - V_f((A + BK)x_{k+N|k}) - L(x_{k+N|k}, Kx_{k+N|k}) \geq L(x_k, u_{k|k}^*)$, which implies, according to Assumption 3.4, that the value function $V_N^*(x_k)$ is monotonically decreasing at least $L(x_k, u_{k|k}^*)$ for each step as $k \to \infty$. Assume that the system trajectory x_k, commencing in $\mathcal{X}_N^M$, cannot enter $\mathcal{X}_f$ in finite time. Then there must exist a $k_m \in (0, \infty)$ such that $V_N^*(x_0) < k_m \ell(r)$, which consequently results in a contradiction, i.e., $V_N^*(x_k) < 0$ for $k > k_m$. Therefore, we conclude that all trajectories of the controlled system, commencing in $\mathcal{X}_N^M$, enter $\mathcal{X}_f$ in finite time.

Step 2): $x_0 \in \mathcal{X}_f$. In this case, the closed-loop system will be $x_{k+1} = (A + \nu_k BK)x_k$. The exponential stability in the presence of DoS attacks can be obtained by using Lemma 3.10. Specifically, according to Lemma 3.10, we can obtain that $\mathcal{X}_f$ is a μ-step positively invariant set for the system $x_{k+1} = (A+\nu_k BK)x_k$, and the state evolution of the closed-loop system is bounded by an exponentially decay function with represent to the initial state. The state constraint satisfaction and control input

Algorithm 3.1: Secure MPC

Require: Initial state x_0; the DoS attack v_k modeled by (1.8) and M by (3.3); the MPC parameters $N, Q, R, K, P, \bar{\alpha}$ according to Theorem 3.16; the time $k = 0$; the buffer state $\boldsymbol{u}_s^* = 0$.;
repeat
  Sample system state at k;
  Solve Optimization Problem $\mathcal{P}$ at k;
  if $\nu_k = 1$ **then**
    Send control sequence $\boldsymbol{u}_k^*$ to the actuator;
    Apply $u_{k|k}^*$ to the system;
    $\boldsymbol{u}_s^* = \boldsymbol{u}_k^*$;
  else
    Use the latest stored control sequence $\boldsymbol{u}_s^*$;
    Apply $u_{k|s}^*$ to the system;
  end
  $k = k + 1$;
  Apply the feedback control law $u_k = Kx_k$.;
until $x_k \in \Omega_{\bar{\alpha}}$;

satisfaction are also fulfilled by Lemma 3.10. This completes the proof. □

For a clear view of the proposed secure MPC framework, we design the secure MPC algorithm as described in Algorithm 3.1.

3.4 Numerical Examples

Consider a constrained stabilizable linear process defined by

$$x_{k+1} = Ax_k + Bu_k \tag{3.29}$$

where $x \triangleq [x_1, x_2]^\top$ and $A = \begin{bmatrix} 1.0 & -1.2 \\ 1.2 & 1.1 \end{bmatrix}$, $B = \begin{bmatrix} 1 \\ 0.5 \end{bmatrix}$. The state constraint is given by $\mathcal{X} \triangleq \{[x_1, x_2]^\top | -10 \leq x_1 \leq 10, -8 \leq x_2 \leq 2\}$ and the control input is bounded by $u \in \mathcal{U} \triangleq \{u | \|u\|_\infty \leq 1\}$. The stage cost function $L(x, u)$ and the terminal cost function $V_f(x)$ are chosen to be quadratic functions as (3.5), where Q is the identity matrix and $R = 0.1$. Then we can calculate K and P for the system in (3.29) as $P = \begin{bmatrix} 1.9385 & 1.7088 \\ 1.7088 & 5.0552 \end{bmatrix}$ and $K = \begin{bmatrix} -1.5718 & -0.2611 \end{bmatrix}$. The terminal set is defined as $\mathcal{X}_f \triangleq \{x | \|x\|_P^2 \leq \bar{\alpha}\}$. Here we set $\bar{\alpha} = 0.1$. The prediction horizon for the MPC problem is set as $N = 10$. The initial feasible set $\mathcal{X}_N \subset \mathcal{X}$ is calculated by using the MPT toolbox [128].

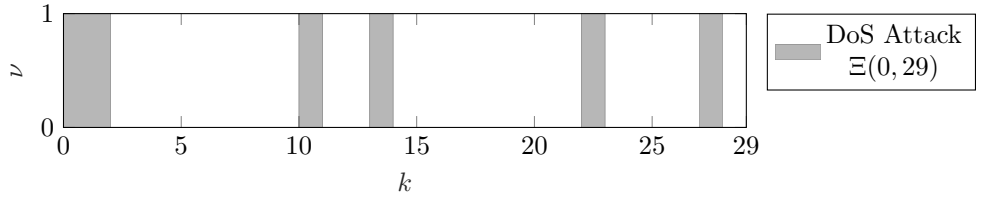

Fig. 3.1: The DoS attack sequence for 30 times. The grey area denotes the DoS attack activation times.

Fig. 3.1 shows the DoS attack sequence in 30 times. We use the duration constraint (3.3) to model DoS attacks occurring at the C-A channel, where the maximum DoS attack duration is determined as $M = 2$ for every N steps. Based on this formulation, the modified initial feasible set $\mathcal{X}_N^M$ with respect to M can be calculated by using a similar approach for obtaining $\mathcal{X}_N$. For the comparison purpose, we illustrate

these two initial feasible sets along with the terminal set in Fig. 3.2. Note from this figure that the modified set $\mathcal{X}_N^M$ is a subset of the original initial feasible set $\mathcal{X}_N$. In addition, this set is shrinking with respect to M, i.e., $\mathcal{X}_{10}^2 \subset \mathcal{X}_{10}^1$ as shown in Fig. 3.2.

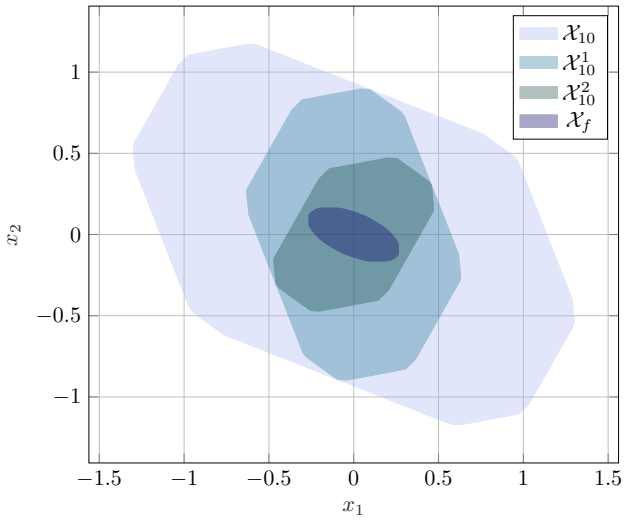

Fig. 3.2: The comparison of $\mathcal{X}_N$, $\mathcal{X}_N^M$ and $\mathcal{X}_f$ with $N = 10$, $M = 1$ and $M = 2$.

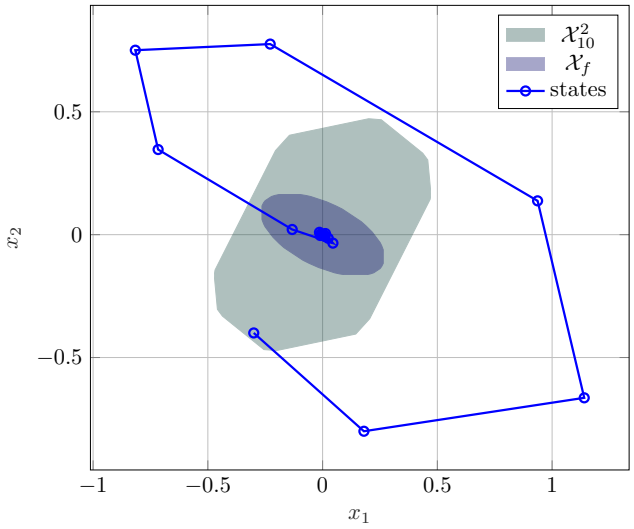

Fig. 3.3: State trajectories by using the secure MPC under DoS attacks.

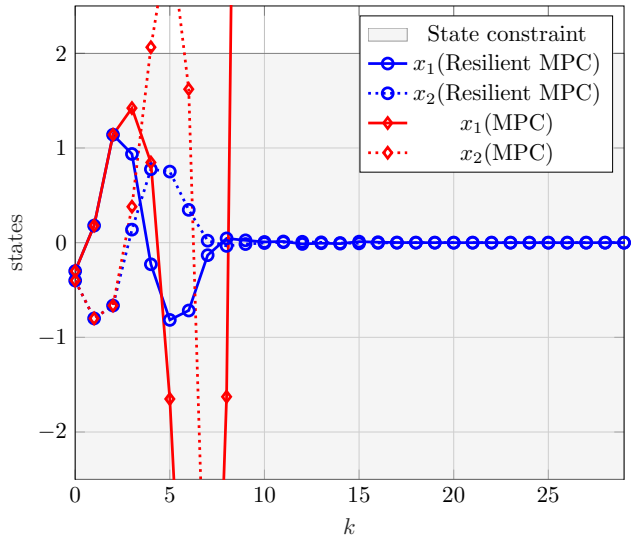

Fig. 3.4: Comparison of state trajectories by using the secure MPC and the conventional MPC under DoS attacks.

The online MPC optimization is formulated as a quadratic programming problem, which is solved by using an efficient QP solver (qpOASES [129]). The initial state is configured as $[-0.3, -0.4]$ and the total simulation time is 30. Fig. 3.3 shows the state trajectory driven by the secure MPC. The comparison of state evolution by using the proposed secure MPC and the conventional MPC is also provided in Fig. 3.4. It shows that the proposed method outperforms the conventional MPC in terms of both constraint satisfaction and control performance. It is worthwhile to point out that, by setting different M, the performance degradation or even instability of the closed-loop system could be induced by the effect of DoS attacks on the C-A channel. Taking the finite horizon cost $\sum_{k=0}^{30} L(x_k, u_k)$ as the performance index, we illustrate the performance degradation with respect to the different DoS attack duration in Table 3.1. As seen in this table, the finite horizon cost is increasing when the DoS attack duration is increasing. Due to the joint effects of physical system constraints and DoS attacks, it should be also noticed that the MPC optimization problem might not be feasible when the DoS attack duration is too large.

Table 3.1: The performance index under different DoS attacks.

DoS Attack Duration	Performance Index	Feasibility
$M = 0$	1.3972	Yes
$M = 1$	3.5134	Yes
$M = 2$	6.5142	Yes
$M \geq 3$	N/A	No

3.5 Conclusion

In this chapter, we have designed a secure MPC algorithm for CPSs under DoS attacks without considering model uncertainties and measurement noises. The CPS has been modeled as an LTI system equipped with a dual-mode MPC controller. A malicious attacker with the constrained duration can send jamming signals to block control signal transmission. We have shown that, by virtue of the dual-mode MPC strategy, the closed-loop system trajectories can be driven to the origin in the presence of DoS attacks. Conditions for the closed-loop exponential stability have been also derived, which rely on the duration of DoS attacks and MPC parameters such as the prediction horizon and the terminal constraint. In addition, the maximum allowable duration of the DoS attacker has been also obtained. Simulation results and comparisons have been provided for verifying the effectiveness of the proposed secure MPC framework.

Chapter 4

Resource-Aware Robust Nonlinear Model Predictive Control of CPSs under DoS Attacks

4.1 Introduction

In this chapter, we propose an event-triggered robust NMPC strategy for nonlinear CPSs in the presence of DoS attacks and additive disturbances, where the packet transmission time instants are determined using an ETM. The ETM triggering rules rely on state or output measurements, leading to the so-called Lebesgue sampling-based control, i.e., event-triggered control [26, 27].

The major objectives of secure control include security and robustness [21]. Security refers to the operational normalcy under malicious attacks [75]. In particular, two of the main concerns with respect to security are deception attacks and DoS attacks. Deception attackers intend to manipulate the data transmission by injecting false and interpolated data packets into the communication channel (see, e.g., [130] and references therein), whereas DoS attackers typically aim at jamming communication channel such that the data transmission can be disabled for some time periods (see, for instance, [75]). In this chapter, 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 survey papers [131–134] and reference therein.

In addition to security, 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. 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 obtained by repeatedly solving constrained optimization problems with future system performance as objective functions [15]. Secondly, networking limitations reveal insufficient communication resources due to imperfect communication channel or limited communication bandwidth [14]. 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 secure 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.

However, very few MPC research efforts have concentrated on security, except the following literature [90, 91, 106]. Specifically, DoS attacks and deception attacks have been respectively studied by [91] and [106] in periodic sampling-based MPC settings. In order to save the communication resource, the authors in [90] has 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 ISpS. However, due to fixed-length control packets induced by MPC controller, the packet transmission strategy in [90] may not fit well with secure and resource-aware control objectives. Hence, we aim to design event-triggered robust NMPC strategy for nonlinear CPSs with additive disturbances in order to achieve these control objectives. In summary, the main contributions are listed 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 [43, 48], 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 conven-

tional 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 recursive feasibility of event-triggered robust NMPC and 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.

The remainder of this chapter is organized as follows. In Section 4.2, we describe the problem formulation. The event-triggered NMPC scheme is introduced in Section 4.3. Section 4.4 presents some sufficient conditions under which the MPC optimization problem is recursively feasible and the closed-loop system is ISpS. In Section 4.5, simulation and comparison examples are presented to verify the effectiveness of the proposed strategy. Finally, we conclude this work in Section 4.6.

Notations: All real numbers and all the nonnegative real numbers are respectively denoted by $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$. The symbols $\mathbb{N}_{\geq 0}$ 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 $X^\top$ 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 $\|x\|_P := \sqrt{x^\top P x}$ is the P-weighted norm. For any set $\mathcal{X} \subseteq \mathbb{R}^n$, we define a metric on $\mathbb{R}^n$ as $\|\mathcal{X}\| \triangleq \sup_{x \in \mathcal{X}} \|x\|$. Note that $a\mathcal{X} \triangleq \{ax : x \in \mathcal{X}\}$ is elementary-wise multiplication of $\mathcal{X}$, where $a \in (0, 1)$. Given two functions α_1 and α_2, $\alpha_1 \circ \alpha_2$ denotes the function composition of these two functions.

4.2 Problem Formulation

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

$$x_{k+1} = f(x_k, u_k) + w_k \tag{4.1}$$

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

Assumption 4.1. *For the system in (4.1), the following condition holds for all $x, z \in \mathcal{X}$ and $u \in \mathcal{U}$:*

$$\|f(x,u) - f(z,u)\| \leq L_f(\|x - z\|) \tag{4.2}$$

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 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 [111] is introduced to characterize DoS attacks in terms of the total attack duration.

Assumption 4.2. *Given the DoS attack induced activation time sequence in (1.9), there exist two constants $\pi \geq 0$ and $\rho \in (0,1)$ such that*

$$\text{card}\left(\Xi(k_0,k)\right) = \sum_{i=k_0}^{k} \mathbf{1}_{\Xi}(i) \leq \pi + \rho(k - k_0) \tag{4.3}$$

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

Remark 4.3. *Under the configuration of Assumption 4.2, DoS attacks considered in this chapter 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., $\lim\limits_{k\to\infty} \frac{\text{card}(\Xi(k_0,k))}{k-k_0} = \rho$. 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 OCP is solved. At each sampling time instant k_j,

the cost function of the OCP is defined by

$$J\left(x_{k_j}, \boldsymbol{u}_{k_j}\right) \triangleq \sum_{i=0}^{N_p-1} L(x_{i+k_j|k_j}, u_{i+k_j|k_j}) + V_f(x_{N_p+k_j|k_j}), \tag{4.4}$$

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, $L : \mathcal{X} \times \mathcal{U} \mapsto \mathbb{R}_{\geq 0}$ is the stage cost function, $V_f : \mathcal{X}_f \mapsto \mathbb{R}_{\geq 0}$ 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 chapter is to design an event-triggered robust NMPC law $u_k^{ET} = \mu_{k-k_j}(x_{k_j})$, which is obtained by minimizing the finite-horizon cost J in (4.4) 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 (4.1) in the presence of 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 4.4. *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. Then, 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. 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 and system destabilization.*

4.3 Event-Triggered NMPC under DoS Attacks

In this section, we propose an ET-MPC framework under DoS attacks (see Fig. 4.1). 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 communi-

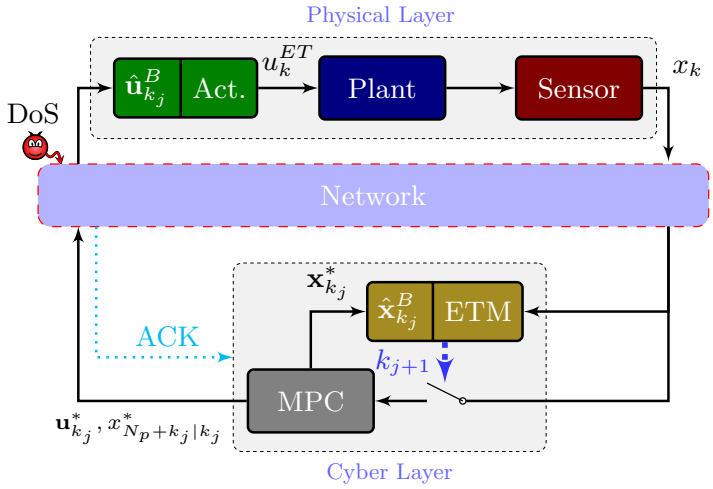

Fig. 4.1: The ET-MPC scheme under DoS attacks. The physical layer consists of the plant, the actuator and the sensor. The cyber layer includes the MPC controller and the ETM. Two dynamic buffers are located respectively in the actuator and the ETM in order to provide real-time control signals and the reference states.

cation network. Secondly, the packet transmission strategy is presented, where the dynamic buffer mechanism is introduced to compensate the adverse effect induced by DoS attacks. 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.

4.3.1 Constrained Optimization Problem

For the nonlinear system in (4.1), the corresponding OCP can be formulated as

$$\boldsymbol{u}_{k_j}^* = \arg \min_{\boldsymbol{u} \in \mathcal{U}^{N_p}} J\left(x_{k_j}, \boldsymbol{u}_{k_j}\right) \tag{4.5a}$$

$$\text{s.t.} \quad x_{k_j|k_j} = x_{k_j} \tag{4.5b}$$

$$x_{i+1+k_j|k_j} = f(x_{i+k_j|k_j}, u_{i+k_j|k_j}) \tag{4.5c}$$

$$x_{i+k_j|k_j} \in (1 - \frac{i}{N_p}\zeta)\mathcal{X} \tag{4.5d}$$

$$u_{i+k_j|k_j} \in \mathcal{U},\ i \in \mathbb{N}_{[0,N_p)} \tag{4.5e}$$

$$x_{N_p+k_j|k_j} \in \xi\mathcal{X}_f \tag{4.5f}$$

where $\mathcal{U}$ is the control constraint; $\mathcal{X}$ is the state constraint; $\xi\mathcal{X}_f$ is the terminal constraint; $\zeta, \xi \in (0, 1)$ are scaling parameters for the robustness constraint in (4.5d) and terminal constraint. It is worth noting that we require the proper design for ζ such that $\mathcal{X}_f \subset (1-\zeta)\mathcal{X}$, since the robustness constraint needs to obey the terminal constraint. In addition, we also have $\|\xi\mathcal{X}_f\| = \xi\|\mathcal{X}_f\|$. 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 direct multiple shooting method, where all the elements in two sequences are treated as decision variables.

4.3.2 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 [135]. 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 reference state for the ETM. How the mechanism

works with the actuator and the ETM will be introduced later in Section 4.3.3 and Section 4.3.4. 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:

$$\hat{u}^B_{k|k_j} = \begin{cases} u^*_{k|k_j}, & \text{if } k \in \mathbb{N}_{[k_j, N_p+k_j)} \\ \kappa_f(\hat{x}_{k|k_j}), & \text{if } k \in \mathbb{N}_{[N_p+k_j, \infty)} \end{cases} \tag{4.6}$$

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

$$\hat{x}^B_{k|k_j} = \begin{cases} x^*_{k|k_j}, & \text{if } k \in \mathbb{N}_{[k_j+1, N_p+1+k_j)} \\ \hat{x}_{k|k_j}, & \text{if } k \in \mathbb{N}_{[N_p+1+k_j, \infty)} \end{cases} \tag{4.7}$$

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 4.10. 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 4.5. *Different from the conventional buffer mechanisms in [79, 91, 135], 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 due to that 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.*

4.3.3 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

$$k_{j+1} = \inf \left\{ k \in \Theta(k_j + 1, \infty) : \|x_k - \hat{x}^B_{k|k_j}\| \geq \sigma \right\} \tag{4.8}$$

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 (4.5) has to be frequently solved. Similar event-triggering conditions can be found in [43, 48]. 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 4.6. *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 due to that the DoS attack may occur between the triggered time instants. STM can not handle this behavior since it lacks of the proactive state measuring capability like ETM. Although STM may provide better network performance, we use ETM in order to deal with DoS attacks.*

4.3.4 Explicit Control Law

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

$$u_k^{ET} \triangleq \hat{u}_{k|k_j}^B,\ k \in \mathbb{N}_{[k_j,k_{j+1})} \tag{4.9}$$

where $\{k_0, k_1, \ldots, k_j, \ldots\}$ denote all the triggering time instants generated by (4.8). Then the closed-loop system can be formally given by

$$x_{k+1} = f(x_k, u_k^{ET}) + w_k,\ k \in \mathbb{N}_{[k_j,k_{j+1})} \tag{4.10}$$

For a clear view of the event-triggered robust NMPC framework, we provide the detailed procedures as shown in Algorithm 4.1.

Algorithm 4.1: event-triggered robust NMPC under DoS attacks

Require: Initial state x_0; the DoS attack satisfying (4.3); 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 (4.6) and (4.7);
  while *The condition in (4.8) is not triggered* **do**
    Apply $\hat{u}_{k|k_j}^B$ to the system in (4.1);
    $k = k + 1$;
  end
  Obtain next triggered time instant k_{j+1} using (4.8);
  $j = j + 1$;
until *The control objective is achieved*;

Remark 4.7. *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 secure 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 to the case of applying conventional ET-MPC.

4.4 Theoretical Analysis

In this section, we first derive sufficient conditions for ensuring the recursive feasibility of OCP (4.5). 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 4.8. *Suppose that Assumptions 4.1 and 4.2 hold. Given the ETM (4.8) and the DoS attack duration constraint (4.3), the following two statements hold true:*
(a) the time interval between any two consecutive triggered time instants k_{j+1} and k_j satisfies:

$$\inf_{j\in\mathbb{N}}\{k_{j+1}-k_j\} \geq \begin{cases} \frac{\ln\left(\sigma(L_f-1)/\|\mathcal{W}\|+1\right)}{\ln(L_f)} & \text{if } L_f \neq 1 \\ \frac{\sigma}{\|\mathcal{W}\|} & \text{if } L_f = 1 \end{cases} \tag{4.11}$$

(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:

$$\sup_{j\in\mathbb{N}}\{\|x_{k_{j+1}}-\hat{x}^B_{k_{j+1}|k_j}\|\} \leq L_f^{N_a+1}\sigma + \sum_{i=0}^{N_a} L_f^i\|\mathcal{W}\| \tag{4.12}$$

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 $w_k \in \mathcal{W}$.

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

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

Combining the triggering condition (4.8) with the above inequality yields

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

for $L_f \neq 1$, and

$$(k_{j+1} - k_j)\|\mathcal{W}\| \geq \sigma$$

for $L_f = 1$. From the above inequalities, we can obtain (4.11).

To prove the second result in (4.12), we use contradiction. Suppose that k_j and k_{j+1} are a pair of two consecutive triggered time instants such that (4.12) does not hold. Due to Lipschitz continuity, one can obtain

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

Since we assume that (4.12) does not hold, it follows

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

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 (4.12) holds. □

Remark 4.9. *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 (4.8) compared with the other existing ETM designs for MPC [43, 48]. 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.

4.4.1 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

$$\tilde{u}_{k|k_{j+1}} \triangleq \begin{cases} \hat{u}^B_{k|k_j} & \text{if } k \in \mathbb{N}_{[k_{j+1},N_p+k_j)} \\ \kappa_f(\tilde{x}_{k|k_j}) & \text{if } k \in \mathbb{N}_{[N_p+k_j,N_p+k_{j+1})} \end{cases} \tag{4.13}$$

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.,

$$\tilde{x}_{k+1|k_{j+1}} = f(\tilde{x}_{k|k_{j+1}}, \tilde{u}_{k|k_{j+1}}) \tag{4.14}$$

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; see, e.g., [43, 48].

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

Assumption 4.10. *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 $\mathcal{X}_f \subseteq \mathcal{X}$ containing origin such that

$$L(x,u) \geq \alpha_L(\|x\|),\ \forall x \in \mathcal{X}, u \in \mathcal{U} \tag{4.15}$$

$$\underline{\alpha}_{V_f}(\|x\|) \leq V_f(x) \leq \bar{\alpha}_{V_f}(\|x\|),\ \forall x \in \mathcal{X}_f \tag{4.16}$$

$$\kappa_f(x) \in \mathcal{U}, f(x,\kappa_f(x)) \in \mathcal{X}_f,\ \forall x \in \mathcal{X}_f \tag{4.17}$$

$$V_f(f(x,\kappa_f(x))) - V_f(x) \leq -L(x,\kappa_f(x)),\ \forall x \in \mathcal{X}_f \tag{4.18}$$

$$\|V_{N_p}(x) - V_{N_p}(z)\| \leq \alpha_{N_p}(\|x-z\|),\ \forall x,z \in \mathcal{X} \tag{4.19}$$

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 chapter defined by OCP in (4.5).

The conditions (4.15)-(4.18) in Assumption 4.10 are necessary for proving stability for general nonlinear MPC formulations [136]. It is also worth noting that continuity of the optimal value function in (4.19) is often used to show robust stability of nonlinear CPSs with constraints; see, e.g., [79].

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

Assumption 4.11 (Initially feasible region)**.** *There exists an initially feasible region $\mathcal{X}_N \subseteq \mathcal{X}$ such that for all $x_0 \in \mathcal{X}_N$ the OCP in (4.5) admits a feasible solution with its initial value being x_0.*

Due to the formulation of the candidate control sequence in (4.13), the control input constraint in the OCP is trivially satisfied. Then, to establish the recursive feasibility, it is equivalent to show that $\tilde{\boldsymbol{x}}_{k_{j+1}}$ obeys the state constraint and enters the terminal set under Assumption 4.11.

Lemma 4.12. *For the system in (4.1) under DoS attacks satisfying duration constraints in (4.3), suppose that Assumptions 4.1–4.11 hold. The OCP (4.5) is recursively feasible at the triggered time instants k_j generated by the proposed ETM (4.8) if the following conditions are satisfied:*

$$L_f^{(1-\beta)N_p}\left(\sum_{i=0}^{N_a} L_f^i\|\mathcal{W}\| + L_f^{N_a+1}\sigma\right) \leq \max\{\zeta\|\mathcal{X}\|, (1-\xi)\|\mathcal{X}_f\|\} \tag{4.20}$$

$$N_p \geq \frac{\overline{\alpha}_{V_f}(\|\mathcal{X}_f\|) - \underline{\alpha}_{V_f}(\xi\|\mathcal{X}_f\|)}{\beta\alpha_L(\xi\|\mathcal{X}_f\|)} \tag{4.21}$$

where

$$\beta \triangleq \left\lfloor \frac{\ln\left(\sigma(L_f-1)/\|\mathcal{W}\|+1\right)}{\ln(L_f)}+1 \right\rfloor /N_p \tag{4.22}$$

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 (4.6), 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 prove that $\tilde{\boldsymbol{x}}_{k_{j+1}}$ fulfills:

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

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

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 $\mathcal{X}_f$ 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 $\xi\mathcal{X}_f$ (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 $\tilde{x}_{N_p+k_j|k_{j+1}} \in \mathcal{X}_f$. At the current triggered time instant k_{j+1} that is generated by the ETM in (4.7), we have $\tilde{x}_{k_{j+1}|k_{j+1}} = x_{k_{j+1}}$. Then using (4.12) in Lemma 4.8 and the Lipschitz continuity by Assumption 4.1, one can obtain

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

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

$$\|\tilde{x}_{k|k_{j+1}}\| \le \|\hat{x}^B_{k|k_j}\| + L_f^{k-k_{j+1}}\bar{\sigma} \tag{4.23}$$

In order to satisfy the tightened state constraint, we require

$$\|\tilde{x}_{k|k_{j+1}}\| \le (1-\frac{k-k_{j+1}}{N_p}\zeta)\|\mathcal{X}\|$$

for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$. Since $\|\hat{x}^B_{k|k_j}\| \le (1-\frac{k-k_j}{N_p}\zeta)\|\mathcal{X}\|$, by combining the above two equations with (4.23), one can obtain

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

which consequently reveals

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

Note from Lemma 4.8 that $k_{j+1} - k_j \geq \beta N_p$. Applying this fact into the above inequality, one can obtain

$$L_f^{(1-\beta)N_p}\bar{\sigma} \leq \zeta\|\mathcal{X}\| \tag{4.24}$$

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

$$\|\hat{x}^B_{N_p+k_j|k_j}\| + L_f^{(1-\beta)N_p}\bar{\sigma} \leq \|\mathcal{X}_f\|$$

From the OCP in (4.5) and the buffer design, we can know $\hat{x}^B_{N_p+k_j|k_j} \in \xi\mathcal{X}_f$. To ensure that $\tilde{x}_{N_p+k_j|k_{j+1}}$ is driven into $\mathcal{X}_f$, the following condition needs to be satisfied:

$$L_f^{(1-\beta)N_p}\bar{\sigma} \leq (1-\xi)\|\mathcal{X}_f\| \tag{4.25}$$

Combining the two conditions (4.24) and (4.25), we can obtain (4.20) such that the tightened state constraint satisfaction is guaranteed for $k \in \mathbb{N}_{[k_{j+1},N_p+k_j)}$ and $\tilde{x}_{N_p+k_j|k_{j+1}} \in \mathcal{X}_f$.

For $k \in \mathbb{N}_{[N_p+k_j,N_p+k_{j+1})}$, it can be seen from Assumption 4.10 that

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

Note that the tightened state constraint (C1) is satisfied because $\mathcal{X}_f$ is an invariant set for (4.14) and $\mathcal{X}_f \subset (1-\zeta)\mathcal{X}$. In addition, we need to show the terminal constraint satisfaction, i.e., $\tilde{x}_{N_p+k_{j+1}|k_{j+1}} \in \xi\mathcal{X}_f$. In order to achieve this, it needs to satisfy the following inequality:

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

Then using (4.15) and (4.16) in Assumption 4.10, the following inequality can be obtained:

$$\overline{\alpha}_{V_f}(\|\mathcal{X}_f\|) - \beta N_p\alpha_L(\xi\|\mathcal{X}_f\|) \leq \underline{\alpha}_{V_f}(\xi\|\mathcal{X}_f\|) \tag{4.26}$$

which can guarantee that the candidate state enters the terminal constraint set. As

a result, we can readily establish the condition in (4.21), from (4.26), such that the candidate state enters $\xi\mathcal{X}_f$ at $k = k_{j+1} + N_p$.

Case 2: $k_{j+1} \geq k_j + N_p$. Recalling the dynamic buffer design, the reference state trajectory after N_p steps remains inside $\xi\mathcal{X}_f$ due to (4.18) in Assumption 4.10, i.e., $\hat{x}^B_{k_{j+1}|k_j} \in \xi\mathcal{X}_f$. 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 $\mathcal{X}_f$ and last component $\tilde{x}_{k_{j+1}+N_p|k_{j+1}}$ enters $\xi\mathcal{X}_f$. To achieve this objective, we should have

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

which shows

$$\bar{\sigma} \leq (1-\xi)\|\mathcal{X}_f\| \tag{4.27}$$

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

$$\overline{\alpha}_{V_f}(\|\mathcal{X}_f\|) - N_p\alpha_L(\xi\|\mathcal{X}_f\|) \leq \underline{\alpha}_{V_f}(\xi\|\mathcal{X}_f\|) \tag{4.28}$$

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

By combining (4.24)-(4.28), we can conclude that the OCP is recursively feasible if the conditions (4.20) and (4.21) are satisfied. This completes the proof. □

Remark 4.13. *When choosing the terminal cost function V_f and the stage cost function L as quadratic functions such as $x^\top Px$ and $\|x\|_Q^2 + \|u\|_R^2$, 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 triggering time instants under the prerequisite of satisfying the established feasibility conditions.*

4.4.2 Input-to-State Stability Analysis

For the proposed robust NMPC algorithm for 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 Section 4.4.1.

Theorem 4.14. *Suppose that Assumptions 4.1–4.11 hold. If the conditions in Lemma 4.12 are satisfied, then given any $x_{k_0} \in \mathcal{X}_N$ where k_0 is the first triggered time instant, the closed-loop system in (4.10) is ISpS in the presence of DoS attacks subject to (4.3) 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

$$\begin{aligned} V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j}) =& \Big(V_{N_p}(x_{k_{j+1}}) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) \Big) \\ &+ \Big(V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \Big) \end{aligned}$$

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

$$\begin{aligned} & V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\ & \leq J(\bar{f}^{k_{j+1}-k_j}(x_{k_j}), \tilde{\boldsymbol{u}}_{k_{j+1}}) - V_{N_p}(x_{k_j}) \\ & = \sum_{k=k_{j+1}}^{N_p-1+k_{j+1}} L(\bar{f}^{k-k_j}(x_{k_j}), \hat{u}^B_{k|k_j}) + V_f(\bar{f}^{N_p+k_{j+1}-k_j}(x_{k_j})) \\ & \quad - \left(\sum_{k=k_j}^{N_p-1+k_j} L(x^*_{k|k_j}, u^*_{k|k_j}) + V_f(x^*_{N_p+k_j|k_j}) \right) \\ & = - \sum_{k=k_j}^{\min\{k_{j+1}, N_p+k_j\}} L(x^*_{k|k_j}, u^*_{k|k_j}) \\ & \quad + \sum_{k=\max\{k_{j+1}, N_p+k_j\}}^{N_p-1+k_{j+1}} L(\bar{f}^{k-k_j}(x_{k_j}), \kappa_f(\bar{f}^{k-k_j}(x_{k_j}))) \\ & \quad + V_f(\bar{f}^{N_p+k_{j+1}-k_j}(x_{k_j})) - V_f(x^*_{N_p+k_j|k_j}) \end{aligned} \tag{4.29}$$

Now consider two different cases of the above inequality when $k_{j+1} < N_p + k_j$ and $k_{j+1} \geq N_p + k_j$. For $k_{j+1} < N_p + k_j$, applying (4.18) in Assumption 4.10 and the fact $x^*_{N_p+k_j|k_j} = \bar{f}^{N_p}(x_{k_j})$ to (4.29) yield

$$\begin{aligned} & V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\ & \leq -\sum_{k=k_j}^{k_{j+1}} L(x^*_{k|k_j}, u^*_{k|k_j}) \\ & \leq -L(x^*_{k_j|k_j}, u^*_{k_j|k_j}) \\ & \leq -\alpha_L(\|x_{k_j}\|) \end{aligned} \tag{4.30}$$

For $k_{j+1} \geq N_p + k_j$, we can rewrite (4.29) as

$$\begin{aligned} & V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(x_{k_j}) \\ & \leq -\sum_{k=k_j}^{N_p-1+k_j} L(x^*_{k|k_j}, u^*_{k|k_j}) \\ & \quad + \left| V_f(\bar{f}^{k_{j+1}-k_j}(x_{k_j})) - V_f(x^*_{N_p+k_j|k_j}) \right| \\ & \leq -L(x^*_{k_j|k_j}, u^*_{k_j|k_j}) \\ & \quad + \max\{V_f(\bar{f}^{k_{j+1}-k_j}(x_{k_j})), V_f(x^*_{N_p+k_j|k_j})\} \\ & \leq -\alpha_L(\|x_{k_j}\|) + \bar{\alpha}_{V_f}(\|\mathcal{X}_f\|) \end{aligned} \tag{4.31}$$

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

$$f^{i+1}(x_{k_j}) = f(f^i(x_{k_j}), \hat{u}^B_{i+k_j|k_j}) + w_{i+k_j}$$

with $f^0(x_{k_j}) \stackrel{\triangle}{=} x_{k_j}$. In the above equation, $f^{k-k_j}(x_{k_j})$ denotes the real trajectory of the perturbed nonlinear dynamics (4.1) with the initial state x_{k_j} under the disturbance

w_k. Then, we can have

$$\begin{aligned}
&\|V_{N_p}(x_{k_{j+1}}) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))\| \\
&= \|V_{N_p}(f^{k_{j+1}-k_j}(x_{k_j})) - V_{N_p}(\bar{f}^{k_{j+1}-k_j}(x_{k_j}))\| \\
&\leq \alpha_{N_p}\left(\|f^{k_{j+1}-k_j}(x_{k_j}) - \bar{f}^{k_{j+1}-k_j}(x_{k_j})\|\right) \\
&\leq \alpha_{N_p}\Bigg(\|f(f^{k_{j+1}-k_j-1}(x_{k_j}), \hat{u}^B_{k_{j+1}-1|k_j}) \\
&\quad - f(\bar{f}^{k_{j+1}-k_j-1}(x_{k_j}), \hat{u}^B_{k_{j+1}-1|k_j})\| + \|w_{k_{j+1}-1}\|\Bigg) \\
&\leq \alpha_{N_p}\Bigg(L_f\|f^{k_{j+1}-k_j-1}(x_{k_j}) - \bar{f}^{k_{j+1}-k_j-1}(x_{k_j})\| + \|\mathcal{W}\|\Bigg) \\
&\leq \alpha_{N_p}\Bigg(\sum_{i=0}^{k_{j+1}-k_j-1} L_f^i\|\mathcal{W}\|\Bigg)
\end{aligned} \tag{4.32}$$

Then combining (4.31) and (4.32), one can obtain

$$\|V_{N_p}(x_{k_{j+1}}) - V_{N_p}(x_{k_j})\| \leq -\bar{\alpha}(\|x_{k_j}\|) + \bar{\gamma}(\|w\|) + \bar{c} \tag{4.33}$$

where $\bar{\alpha} = \alpha_L$, $\bar{\gamma} = \alpha_{N_p} \circ \sum_{i=0}^{k_{j+1}-k_j-1} L_f^i$ and $\bar{c} = \bar{\alpha}_{V_f}(\|\mathcal{X}_f\|) + \alpha_{N_p}\Bigg(\sum_{i=0}^{k_{j+1}-k_j-1} L_f^i\|\mathcal{W}\|\Bigg)$. In addition, we have $\alpha_L(\|x\|) \leq V_{N_p}(x) \leq \alpha_{N_p}(\|x\|)$ by Assumptions 4.1 and 4.10. Together with (4.33), it follows that V_{N_p} is an ISpS-Lyapunov function for the closed-loop system in (4.10). Summarizing all the above statements, the closed-loop system is ISpS in $\mathcal{X}_N$ at the triggered time instants k_j. □

4.5 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 [137].

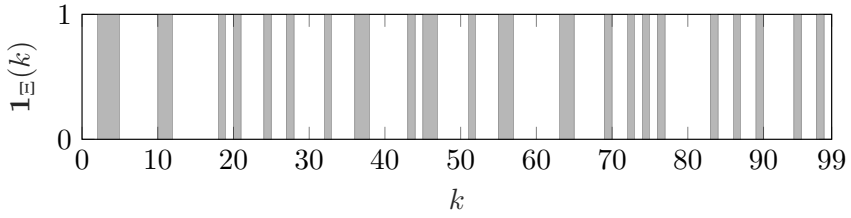

Fig. 4.2: The DoS attack sequence for 100 time steps.

4.5.1 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; the other coefficients represent physical parameters including the cart mass $M_c = 1.25\,\mathrm{kg}$, the nonlinear factor $\tau = 0.9\,\mathrm{N/m}$ and the damping factor $h_d = 0.42\,\mathrm{Ns/m}$. The state and control input constraints are respectively given by $\mathcal{X} = \{[p, v]^\top : -2 \leq p \leq 2, -2 \leq v \leq 2\}$ and $\mathcal{U} = \{u : -1.5 \leq u \leq 1.5\}$. The DoS attack sequence is depicted in Fig. 4.2, 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 $L(x, u) = x^\top Q x + u^\top R u$ where $Q = [0.1, 0.0; 0.0, 0.1]$ and $R = 0.1$; the terminal cost is $V_f(x) = x^\top P x$ where $P = [0.1967, 0.0734; 0.0734, 0.1737]$; the terminal control law is chosen as $\kappa_f(x) = Kx$ where $K = [-0.3169, -1.1566]$; the terminal constraint is defined as $\xi\mathcal{X}_f, \xi = 0.8$ where $\mathcal{X}_f = \{x : x^\top P x \leq 0.01\}$ is the positively invariant set via the method in [138]; the scaling ratio for the shrinking state constraint is set as $\zeta = 0.2$. The disturbance bound $\|\mathcal{W}\|$ is 0.0312. It is worthwhile to point out that $L, V_f, \kappa_f, \mathcal{X}_f$ fulfill Assumption 4.10 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 4.8, 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 $\mathcal{X}$, the terminal constraint $\mathcal{X}_f$, the disturbance bound $\|\mathcal{W}\|$ and the

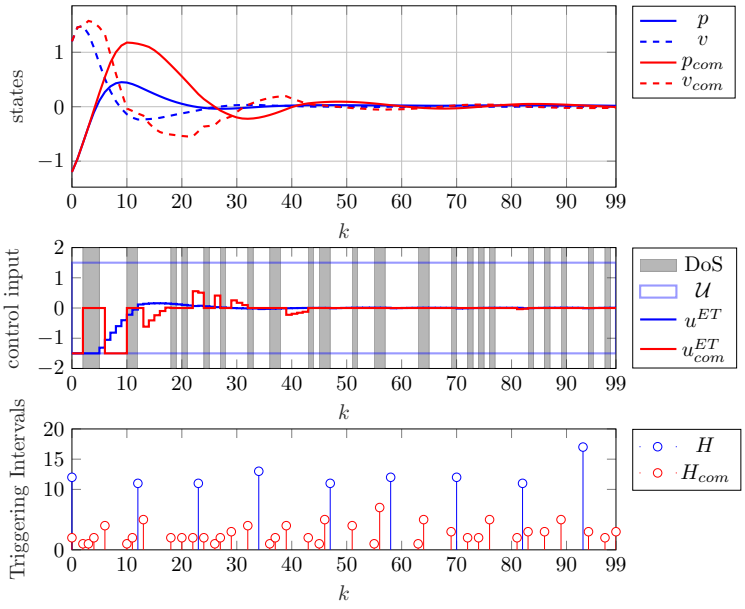

Fig. 4.3: The numerical comparisons between our proposed method and the ET-MPC strategy in [43]. The state trajectories (p, v and p_{com}, v_{com}), control input sequences (u^{ET} and u^{ET}_{com}), and event triggered intervals (H and H_{com}) in 100 time steps are respectively shown in the above three subfigures. The blue colored lines represent the results of our work, whereas the red colored lines denote the results of the other work.

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 $N_{\text{sim}} = 100$.

4.5.2 Results and Comparisons

The simulation results and comparisons with a conventional ET-MPC in [43] are shown in Fig. 4.3, where the state trajectories, control input sequences, and event-triggered intervals are thoroughly compared. Note that we have used same ET-MPC parameter settings including the OCP parameters and the triggering level when conducting the simulation comparisons. Also, all the comparisons are conducted under the DoS attack shown in Fig. 4.2 and the same disturbance sequence.

From the first two subfigures in Fig. 4.2, 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 Fig. 4.2 illustrates the triggering time instants & intervals generated by the proposed ETM. Note that we have solved OCP and

transmitted control packet only on 9 triggering time instants, which can save a lot of communication resource compared with periodic sampling based NMPC. In addition, it can be verified that the triggering intervals satisfy the condition (4.11) in Lemma 4.8. 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 [43, 48].

In order to further compare our proposed method with the one in [43], we introduce two quantitative indices to respectively evaluate its network and control performance. Specifically, we take the average sampling interval ($\frac{N_{\text{sim}}}{\text{The Number of Samplings}}$) as the network performance index, and the total cost ($\sum_0^{N_{\text{sim}}} \left(x^\top Q x + u^\top R u\right)$) 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 behave 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 4.1. Then, we investigate the network and control performance indices as described in the previous paragraph. The simulation results are shown in Table 4.1. As seen in this table, 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 secure ETM contribute 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.

Table 4.1: 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

4.6 Conclusion

In this chapter, we have studied secure 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 secure 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.

Chapter 5

Resource-Aware Min-Max Model Predictive Control of CPSs under Cyber Attacks

5.1 Introduction

In this chapter, a self-triggered MPC framework is proposed for achieving the resource-aware and secure control objectives. In particular, the control packet transmission is scheduled by an STM such that the better resource-awareness can be obtained. The benefits of using such mechanism are mainly focused on saving networking resources through less frequent sampling of states, however, without sacrificing too much control performance or even maintaining optimized control performance [139]. In addition, the integration of STM into MPC is even more profitable since less frequent sampling may lead to less computational power consumption. This is meaningful since solving MPC optimization problem usually consumes considerable computational resource.

The design objectives of secure control mainly concentrate on maintaining the operational normalcy against malicious attacks [75]. The recent research efforts on developing secure control strategies can be found in survey chapters [72, 73] and reference therein. In the existing literature, there are roughly two major security issues considered, i.e., deception attacks and DoS attacks. Specifically, deception attacks often refer to malicious data manipulation that can tamper with packets transmitted over the communication channel, while DoS attacks usually jam communication channel in order to completely disable the packet transmission for certain time in-

tervals [11]. There are plenty of research endeavours focused on developing control strategies against deception attacks [95, 104–106] and DoS attacks [25, 84, 89, 91], just to name a few. In [104], a dynamic output feedback controller is designed for stochastic nonlinear systems such that the prescribed security using probability and input-to-state stability is guaranteed. In [25], an input-to-state stabilizing control strategy is developed for nonlinear systems under DoS attacks, where a switching system approach is used for modeling DoS attack. A unified game theoretic secure control approach is presented in [89] in order to deal with DoS attacks, where the optimal control strategy is obtained using game theory in the delta domain. However, there are rarely research results on developing secure control strategies that can simultaneously tackle DoS attacks and deception attacks, let alone the ones that can also consider other cyber and physical issues such as constrained networking resource, physical constraints, and uncertainties. Therefore, we in this chapter aim at developing secure control strategies under DoS attacks and deception attacks while simultaneously considering such cyber and physical issues.

Due to its superior performance, MPC has not only been studied extensively for tackling physical issues via mature tools such as min-max MPC [55, 140] but also received recent research interests on designing secure control strategies, see, e.g., [91, 106]. The authors in [106] propose an MPC-based approach to obtain security objectives for linear parameter-varying systems under deception attacks. In [91], an MPC-based secure control strategy is developed to tackle DoS attacks while maintaining the closed-loop stability and constraint satisfaction. However, to the best of our knowledge, the research on secure MPC under deception and DoS attacks is still in its infancy. Besides, the conventional MPC (i.e., periodic sampling based MPC [106]) alone may not survive in CPS-based control scenarios where the other cyber issues such as constrained networking resource are present.

Hence, a self-triggered MPC framework might be a viable choice for dealing with such issues simultaneously. In this framework, the control packet transmission is scheduled by an STM. Unlike conventional MPC, self-triggered MPC uses STM to determine sampling time instants that are usually nonuniform over time. Such a mechanism is mainly focused on saving networking resources through less frequent sampling of states, however, without sacrificing too much control performance [139]. In addition, the integration of STM into MPC is even more beneficial since less frequent sampling may lead to less computational power consumption. This feature is meaningful since solving MPC optimization problem usually consumes consider-

able computational resource. Therefore, we design a self-triggered min-max MPC to address secure control problem for nonlinear CPSs in the presence of both cyber issues (i.e., both deception attacks and DoS attacks, limited networking resource) and physical issues (i.e., uncertainty and physical constraints). The main contributions are given as follows. 1) A self-triggered min-max MPC framework is proposed for uncertain nonlinear CPSs in the presence of deception and DoS attacks. In the proposed framework, a new min-max optimization problem is formulated by means of radial basis function and then a novel STM is designed based on the discrepancy between the original optimal value function and the new optimal value function. We take advantage of min-max optimization over all possible deception attacks and uncertainties such that the resulting control law can maintain optimized control performance against cyber attacks. 2) The closed-loop stability in the sense of ISpS is derived by showing that the optimal value function of the new min-max optimization problem is an ISpS-Lyapunov function at the triggered time instants. The established theoretical results reveal that not only the state and control input constraints are satisfied but also the closed-loop system sate trajectory converges despite the presence of deception attacks and DoS attacks.

The outline of this chapter is given as follows. The problem formulation is presented in Section 5.2. The main control algorithm design is introduced in Section 5.3. Section 5.4 presents the stability analysis. In Section 5.5, simulated examples are given in order to verify the effectiveness of the proposed control algorithm. Finally, this work is concluded by Section 5.6.

Notations: All the real numbers, nonnegative integers and positive integers are denoted by $\mathbb{R}$, $\mathbb{N}_{\geq 0}$ and $\mathbb{N}_{>0}$. We use $\mathbb{N}_{[k_1,k_2)}$ to denote all the integers in $[k_1, k_2)$. We use $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ to represent all real column vectors of length n and all real matrices of size n by m, where $m, n \in \mathbb{N}_{>0}$. For a given matrix $X \in \mathbb{R}^{n\times m}$, its transpose is represented by $X^\top$; a matrix is called symmetric if its transpose is identical with itself. For a symmetric matrix $S \in \mathbb{R}^{n\times n}$, $S \succ 0$ (or $S \succeq 0$) means that S is positive definite (or positive semidefinite). For any $x \in \mathbb{R}^n$, $\|x\|$ represents the Euclidean norm. For a set $\mathcal{X} \subseteq \mathbb{R}^n$, we define $\|\mathcal{X}\| \triangleq \sup_{x\in\mathcal{X}} \|x\|$ and $\mathcal{X}^N$ as the Nth Cartesian product of $\mathcal{X}$. The distance from a point $z \in \mathbb{R}$ to a set $\mathcal{X} \subseteq \mathbb{R}^n$ is denoted by $\text{dist}(z, \mathcal{X}) \triangleq \inf_{x\in\mathcal{X}} \|x - z\|$. $\otimes$ is the Kronecker product.

5.2 Problem Formulation

Consider a CPS deployed over wireless communication networks, where its physical process is modeled by the following discrete-time nonlinear system:

$$x_{k+1} = f(x_k, u_k, w_k) \tag{5.1}$$

where $x_k \in \mathcal{X} \subseteq \mathbb{R}^n$ denotes the constrained system state, $u_k \in \mathcal{U} \subseteq \mathbb{R}^m$ represents the constrained control input that may be affected by the DoS attack and deception attack, and $w_k \in \mathcal{W} \subseteq \mathbb{R}^q$ is the parametric uncertainty; $f : \mathcal{X} \times \mathcal{U} \times \mathcal{W} \mapsto \mathbb{R}^n$ is a continuous mapping with $f(0, 0, 0) = 0$; $\mathcal{X}, \mathcal{U}$ and $\mathcal{W}$ are all compact sets containing the origin as their interior point. It is also further assumed that the state measurement can be acquired accurately at any given sampling time.

Since the adversaries usually have limited energy to launch cyber attacks, it is reasonable to assume that DoS and deception attacks fulfill some energy constraints, i.e., the attackers cannot have arbitrary attack abilities.

Assumption 5.1. *The cyber attacks considered throughout this chapter are subject to the following conditions:*
***DoS attack**: There exist two constants $\pi \geq 0$ and $\rho \in (0, 1)$ such that*

$$\text{card}\left(\Xi(k_0, k)\right) = \sum_{i=k_0}^{k} \mathbf{1}_{\Xi}(i) \leq \pi + \rho(k - k_0) \tag{5.2}$$

where $\text{card}\left(\Xi(k_0, k)\right)$ *is defined using (1.9).*
***Deception attack**: Consider the deception attack occurs in the communication channels. We introduce a set-based model*

$$\sup_{\iota \in \mathbb{N}_{\geq 0}} \|a_\iota\|_\infty < \theta_a \tag{5.3}$$

where θ_a denotes the maximum attack level to the system.

Based on (5.3), it is natural to define a set $\mathcal{A} \triangleq \{a_\iota : \sup_{\iota \in \mathbb{N}_{\geq 0}} \|a_\iota\|_\infty < \theta_a\}$, which represents all possible deception attacks. Note that, under Assumption 5.1, DoS attacks considered in this chapter are allowed to launch at arbitrary time instants. Moreover, ρ depicts the average attack duration, i.e., $\lim_{k\to\infty} \frac{\text{card}(\Xi(k_0,k))}{k-k_0} = \rho$, while the other constant π reveals the maximum duration of consecutive DoS attacks. 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 $N_a \triangleq \lceil \pi/(1-\rho) \rceil$ (see, e.g., [111]).

Problem 1: The control objective is to design a self-triggered min-max MPC control law such that the controlled system is ISpS despite DoS attacks and deception attacks. Let $k_j, j \in \mathbb{N}_{\geq 0}$ denote all the sampling time instants at which the optimization problems are solved and the corresponding control packets are successfully transmitted. Then the control law can be designed as

$$\hat{u}_k = \mu_{k-k_j}(x_{k_j}),\ k \in \mathbb{N}_{[k_j,k_{j+1})} \tag{5.4}$$

where $\mu : \mathbb{R}^n \times \mathbb{N}_{\geq 0} \mapsto \mathbb{R}^m$. In addition, the next sampling time instant is determined by the following self-triggered scheduler:

$$k_{j+1} = k_j + H_j^*, j \in \mathbb{N}_{\geq 0} \tag{5.5}$$

where $H^* : \mathbb{R}^n \mapsto \mathbb{N}_{>0}$.

5.3 Secure Min-Max MPC under Cyber Attacks

5.3.1 Min-Max Optimization Control Problem

We first introduce the conventional cost function of min-max MPC at the sampling instant k_j:

$$J_N(x_{k_j}, \boldsymbol{u}_{k_j}, \boldsymbol{w}_{k_j}, \boldsymbol{a}_{k_j}) \triangleq \sum_{i=0}^{N-1} L(x_{k_j+i|k_j}, u_{k_j+i|k_j}) + F(x_{k_j+N|k_j}) \tag{5.6}$$

where $N \in \mathbb{N}_{>0}$ is the prediction horizon, $x_{k_j+i|k_j}$ is the predicted state for the system in (5.1) with its initial state $x_{k_j|k_j} = x_{k_j}$, $\boldsymbol{u}_{k_j} = \{u_{k_j|k_j}, u_{k_j+1|k_j}, \ldots, u_{k_j+N-1|k_j}\}$ is the control input sequence, $\boldsymbol{w}_{k_j} = \{w_{k_j|k_j}, w_{k_j+1|k_j}, \ldots, w_{k_j+N-1|k_j}\}$ is the uncertainty sequence, $\boldsymbol{a}_{k_j} = \{a_{k_j|k_j}, a_{k_j+1|k_j}, \ldots, a_{k_j+N-1|k_j}\}$ is the deception attack sequence, $L : \mathbb{R}^n \times \mathbb{R}^m \mapsto \mathbb{R}_{\geq 0}$ with $L(0,0) = 0$ is the stage cost function, and $F : \mathbb{R}^n \mapsto \mathbb{R}_{\geq 0}$ with $F(0) = 0$ is the terminal cost function. Then, the optimization problem $\mathcal{P}_N$ for

min-max MPC can be defined as

$$V_N(x_{k_j}) = \min_{\boldsymbol{u}_{k_j}} \left\{ \max_{\boldsymbol{a}_{k_j}\in\mathcal{A}^N, \boldsymbol{w}_{k_j}\in\mathcal{W}^N} J_N \right\} \tag{5.7a}$$

$$\text{s.t.} \quad x_{k_j|k_j} = x_{k_j} \tag{5.7b}$$

$$x_{k_j+i+1|k_j} = f(x_{k_j+i|k_j}, \hat{u}_{k_j+i|k_j}, w_{k_j+i|k_j}) \tag{5.7c}$$

$$\hat{u}_{k_j+i|k_j} = u_{k_j+i|k_j} + a_{k_j+i|k_j} \tag{5.7d}$$

$$x_{k_j+i|k_j} \in \mathcal{X},\ u_{k_j+i|k_j} \in \mathcal{U},\ i \in \mathbb{N}_{[0,N-1]} \tag{5.7e}$$

$$x_{k_j+N|k_j} \in \mathcal{X}_f \tag{5.7f}$$

where $\mathcal{X}_f$ is the terminal set and $V_N(x_{k_j})$ is the optimal value function. As shown in the above optimization problem (5.7), the uncertainty and deception attack are explicitly handled via a min-max optimization. Besides, the DP equations for (5.7) can be shown as

$$\begin{aligned} &V_{N-i}(x_{k_j+i|k_j}) \\ &\triangleq \min_{u_{k_j+i|k_j}\in\mathcal{U}} \left\{ \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+i|k_j}, u_{k_j+i|k_j}) + V_{N-i-1}(x_{k_j+i+1|k_j}) \right\} \text{ such that} \right. \\ &\qquad \left. x_{k_j+i+1|k_j} \in \mathcal{X}_{N-i-1},\ \forall w_{k_j+i|k_j} \in \mathcal{W},\ \forall a_{k_j+i|k_j} \in \mathcal{A} \right\} \end{aligned}$$

with the boundary conditions

$$V_0(x_{k_j+N|k_j}) \triangleq F(x_{k_j+N|k_j})$$
$$\mathcal{X}_0 \triangleq \mathcal{X}_f$$

where $\mathcal{X}_f \subseteq \mathcal{X}_{N-i-1} \subseteq \mathcal{X}$ for $i = 0, 1, \ldots, N-1$. In addition, the control policy based on the optimization problem $\mathcal{P}_N$ can be given as

$$\hat{u}_k(x_{k_j}) \triangleq u^*_{k|k_j},\ \forall k \in \mathbb{N}_{[k_j,k_{j+1})} \tag{5.8}$$

5.3.2 Parameterized Min-Max Optimization Control Problem

In order to tackle DoS attacks, we propose to use a novel control sequence based on the following parameterization method:

$$u^r_{k_j+i|k_j} = \sum_{r=0}^{M-1} p_{(r,k_j)}\varphi_i(r),\ p_{(r,k_j)} \in \mathbb{R}^{m\times 1} \tag{5.9}$$

where $\varphi_i(r) \triangleq e^{-(i+1)\epsilon^2(r+1)^2}, \forall r \in \mathbb{N}_{[0,M-1]}$ denotes the rth linearly-independent Gaussian radial basis functions at the ith prediction step; $\epsilon \in (0,1)$ is a tuning parameter for shaping the Gaussian radial basis function; $p_{(r,k_j)}$ is the weight containing m real coefficients for the rth radial component. Consequently, we rewrite (5.9) into a more compact form:

$$u^r_{k_j+i|k_j} = \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_m\right)\boldsymbol{p}_{k_j} \tag{5.10}$$

where

$$\begin{aligned}\boldsymbol{p}_{k_j} &\triangleq \boldsymbol{p}^M_{k_j} = [p^\top_{(0,k_j)}, p^\top_{(1,k_j)}, p^\top_{(2,k_j)}, \ldots, p^\top_{(M-1,k_j)}]^\top \\ \boldsymbol{\varphi}_i &\triangleq \boldsymbol{\varphi}^M_i = [\varphi_i(0), \varphi_i(1), \ldots, \varphi_i(M-1)]^\top\end{aligned}$$

Then the parameterized control sequence can be denoted as

$$\boldsymbol{u}^r_{k_j} = \left(\boldsymbol{\phi}_N \otimes \mathbf{I}_m\right)\boldsymbol{p}_{k_j} \tag{5.11}$$

where

$$\boldsymbol{\phi}_N \triangleq \boldsymbol{\phi}^M_N = [\boldsymbol{\varphi}_0, \boldsymbol{\varphi}_1, \boldsymbol{\varphi}_2, \ldots, \boldsymbol{\varphi}_{N-1}]^\top$$

Note that $\boldsymbol{\phi}_N$ is a matrix of size N by M. In the following discussion, we omit the superscript M of $\boldsymbol{p}^M$, $\boldsymbol{\varphi}^M_i$ and $\boldsymbol{\phi}^M_N$ for ease of exposition.

Then, by introducing (5.11) to the original cost function (5.6), we can design a new cost function as follows:

$$J^r_N(x_{k_j}, \boldsymbol{p}_{k_j}, \boldsymbol{w}_{k_j}, \boldsymbol{a}_{k_j}) \triangleq \sum_{i=0}^{N-1} L(x_{k_j+i|k_j}, \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_m\right)\boldsymbol{p}_{k_j}) + F(x_{k_j+N|k_j}) \tag{5.12}$$

Consequently, the parameterized optimization problem $\mathcal{P}_N^r$ for the proposed min-max MPC framework can be formulated as

$$V_N^r(x_{k_j}) = \min_{\boldsymbol{p}_{k_j}} \left\{ \max_{\boldsymbol{a}_{k_j}\in\mathcal{A}^N, \boldsymbol{w}_{k_j}\in\mathcal{W}^N} J_N^r \right\} \tag{5.13a}$$

$$\text{s.t.} \quad x_{k_j|k_j} = x_{k_j} \tag{5.13b}$$

$$x_{k_j+i+1|k_j} = f(x_{k_j+i|k_j}, \hat{u}_{k_j+i|k_j}, w_{k_j+i|k_j}) \tag{5.13c}$$

$$\hat{u}_{k_j+i|k_j} = \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_m\right) \boldsymbol{p}_{k_j} + a_{k_j+i|k_j} \tag{5.13d}$$

$$x_{k_j+i|k_j} \in \mathcal{X},\ \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_m\right) \boldsymbol{p}_{k_j} \in \mathcal{U} \tag{5.13e}$$

$$x_{k_j+N|k_j} \in \mathcal{X}_f \tag{5.13f}$$

where $\boldsymbol{p}_{k_j} \in \mathbb{R}^{mM}$ is the new decision variable and $V_N^r(x_{k_j})$ is the optimal value function for (5.13). Similarly, it is worthwhile noting that the DP equations for (5.13) can be given by

$$\begin{aligned} &V_{N-i}^r(x_{k_j+i|k_j}) \\ &\triangleq \min_{\boldsymbol{p}_{k_j}} \left\{ \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j}, \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_m\right) \boldsymbol{p}_{k_j}) + V_{N-i-1}^r(x_{k_j+i+1|k_j}) \right\} \text{ such that} \right. \\ &\qquad \left. x_{k_j+i+1|k_j} \in \mathcal{X}_{N-i-1},\ \forall w_{k_j+i|k_j} \in \mathcal{W},\ \forall a_{k_j+i|k_j} \in \mathcal{A} \right\} \end{aligned}$$

with the boundary conditions

$$V_0^r(x_{k_j+N|k_j}) \triangleq F(x_{k_j+N|k_j})$$
$$\mathcal{X}_0 \triangleq \mathcal{X}_f$$

$\mathcal{X}_f \subseteq \mathcal{X}_{N-i-1} \subseteq \mathcal{X}$ for $i = 0, 1, \ldots, N-1$.

Remark 5.2. *Note that we have introduced a novel control parameterization (5.9) to adapt the original optimization problem (5.7). Using this technique, we are able to obtain an optimal control sequence parameterized by just one decision variable* $\boldsymbol{p}_{k_j}^*$. *That is to say, this parameterized control sequence is irrelevant to the prediction horizon. This unique feature can help to generate the control law under DoS attacks occurring at the communication channel.*

5.3.3 Self-Triggered Min-Max MPC Control Law

To mitigate the communicational and computational overload, we introduce a STM for the proposed min-max MPC scheme in (5.13). The triggered time instants are denoted as $k_{j+1} = k_j + H_j^*$. H_j^* is the triggered interval determined by the following STM:

$$H_j^* \triangleq \max\{H \in \mathbb{N}_{[1,\bar{N}]} : V_N^r(x_{k_j}) - V_N(x_{k_j}) \leq Ce^{-H\delta}\} \tag{5.14}$$

It is worthwhile noting that the largest sampling intervals are configured as $\bar{N} \triangleq N - N_a > 1$ in order to tackle DoS attacks, δ and C are the tuning parameter. In addition, due to that the DoS attacks may hinder the data transmission from the controller to the actuator, it is highly possible that the control signal cannot be successfully sent to the controlled system at the generated triggered time instants. Thus, we impose an explicit upper bound $\bar{N}$ on the sampling interval between k_j and k_{j+1} in order to deal with such DoS attack induced issue. That is, even if the next triggered instant is attacked by the DoS adversary, the CPS's actuator can always use proper control signals in the last controller update under the proposed STM.

Then the control law can be given as

$$\hat{u}_k^{ST}(x_{k_j}) \triangleq \left(\boldsymbol{\varphi}_{k-k_j}^\top \otimes \mathbf{I}_m\right) \boldsymbol{p}_{k_j}^*, \, \forall k \in \mathbb{N}_{[k_j,k_{j+1})} \tag{5.15}$$

where $k_j \in \mathbb{N}_{\geq 0}, j \in \{0, 1, 2, \ldots\}$ are the time instants at which the optimization problems are solved and the DoS attack is absent. By applying (5.15) to the controlled system in (5.1), we can formulate the closed-loop system as

$$\begin{aligned} x_{k+1} &= f(x_k, u_k^{ST}, w_k) \\ u_k^{ST} &= \hat{u}_k^{ST}(x_{k_j}) + a_k, \, \forall k \in \mathbb{N}_{[k_j,k_{j+1})} \end{aligned} \tag{5.16}$$

The main objective of this chapter is to prove that the designed control law can render the nonlinear system ISpS. The self-triggered secure min-max MPC algorithm

is shown in Algorithm 5.1.

Algorithm 5.1: Self-triggered min-max MPC algorithm under DoS attacks and deception attacks

Require: The radial basis function parameter ϵ and the prediction horizon N.
Initialization: Set the initial time $k = 0$, the initial sampling time $k_0 = 0$, and $j = 0$;
while *The control action is not stopped* **do**
    Sample the system state x_{k_j} at k_j;
    Solve the optimization problem (5.13) to obtain $\boldsymbol{p}^*_{k_j}$;
    Use the STM (5.14) to determine the next sampling time k_{j+1};
    while $k < k_{j+1}$ **do**
        Apply the control law (5.15) to the system in (5.1);
        $k = k + 1$;
    end
    $j = j + 1$;
end

5.4 Stability Analysis

In this section, the theoretical properties of the proposed MPC scheme will be considered. First, the decreasing property of the optimal value function for $\mathcal{P}_N$ is investigated. Then, the closed-loop system, driven by the control law (5.15), is proved to be ISpS.

Before presenting the main analysis result, we introduce the conventional assumptions for the proposed min-max MPC framework, which have been widely used in state-of-the-art MPC literature such as [15, 140].

Assumption 5.3. *There exist a function $\kappa_f : \mathbb{R}^n \mapsto \mathbb{R}^m$ with $\kappa_f(0) = 0$ and $\alpha_L, \bar{\alpha}_F, \underline{\alpha}_F, \sigma \in \mathcal{K}_\infty$ such that:*

1) $\mathcal{X}_f$ is a subset of $\mathcal{X}$ containing the origin as its interior where

$$\kappa_f(x) \in \mathcal{U},\ f(x, \kappa_f(x) + a, w) \in \mathcal{X}_f \tag{5.17}$$

for all $x \in \mathcal{X}_f$, $a \in \mathcal{A}$, $w \in \mathcal{W}$.

2) The stage and terminal cost functions are bounded by

$$L(x,u) \geq \alpha_L(\|x\|),\ \forall x \in \mathcal{X}, u \in \mathcal{U} \tag{5.18}$$

$$\underline{\alpha}_F(\|x\|) \leq F(x) \leq \bar{\alpha}_F(\|x\|),\ \forall x \in \mathcal{X}_f \tag{5.19}$$

3) The terminal cost function satisfies

$$\begin{aligned} F(f(x,\kappa_f(x)+a,w)) - F(x) \leq -L(x,\kappa_f(x)) \\ + \sigma(\|\mathcal{A}\|) \end{aligned} \tag{5.20}$$

for all $x \in \mathcal{X}_f$, $a \in \mathcal{A}$, $w \in \mathcal{W}$.

Specifically, the first condition guarantees that the system in (5.1) controlled by $u = \kappa_f(x)$ will admit an invariant set despite the effect of uncertainty and deception attacks; the second condition states that both the stage cost function and terminal cost function should be bounded by some comparison functions; the third condition imposes additional local stabilizing requirement on the terminal cost function. The main difference to the standard assumption is that we consider an additional deception attack sequence.

Remark 5.4. *Assumption 5.3 is a special case of the standard MPC assumption (see, e.g., [15, 136]). It is also worthwhile to point out that Assumption 5.3 implies that F is an ISpS Lyapunov function for all $x \in \mathcal{X}_f$, all $w \in \mathcal{W}$, and all $a \in \mathcal{A}$.*

Assumption 5.5. *There exists a subset $\mathcal{X}_N$ of $\mathcal{X}$ such that for all initial state $x \in \mathcal{X}_N$ the set $\mathcal{U}_N(x) \triangleq \{(\boldsymbol{\phi}_N \otimes \mathbf{I}_m)\,\boldsymbol{p} \in \mathcal{U}^N : \text{(5.13b)-(5.13f) holds}\}$ is not empty.*

Remark 5.6. *Assumption 5.5 requires an initially feasible set $\mathcal{X}_N$ for the optimization problem (5.13) despite the presence of uncertainty and deception attacks, which guarantees that the OCP always gets at least one feasible control sequence provided the initial state starting from $\mathcal{X}_N$. In addition, Assumption 5.5 also reveals that there exists a $\boldsymbol{p}$ such that $\kappa_f(x) = \left(\boldsymbol{\varphi}_{N-1}^\top \otimes \mathbf{I}_m\right)\boldsymbol{p}$ for $x \in \mathcal{X}_f$.*

Lemma 5.7. *Suppose that Assumption 5.3 and 5.5 hold. Given the optimization control problem defined in (5.7), it follows that*

$$V_N(x_{k_{j+1}}) - V_N(x_{k_j}) \leq -\alpha_L(\|x_{k_j}\|) + \bar{N}\sigma(\|\mathcal{A}\|)$$

for all $x_{k_j} \in \mathcal{X}_N$.

Proof. First, we investigate the decreasing property of the optimal value function, which is proved by means of dynamic programming techniques applied to the min-max optimization problem. In order to show $V_{N-i}(x_{k_j+i|k_j})$ is monotonically decreasing with respect to i, we firstly take an error term $\Delta V_{N-i}(x_{k_j+i|k_j}) \triangleq V_{N-i}(x_{k_j+i|k_j}) - V_{N-i-1}(x_{k_j+i|k_j})$. Due to Assumption 5.3 and Assumption 5.5, we have $u_{k_j+N|k_j} = \kappa_f(x_{k_j+N|k_j})$ is feasible for the optimization problem such that

$$
\begin{aligned}
&\Delta V_1(x_{k_j+N|k_j}) \\
&= \max_{\substack{w_{k_j+N|k_j}\in\mathcal{W} \\ a_{k_j+N|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+N|k_j}, u^*_{k_j+N|k_j}) + F(x^+_{k_j+N|k_j}) \right\} - F(x_{k_j+N|k_j}) \\
&\leq \max_{\substack{w_{k_j+N|k_j}\in\mathcal{W} \\ a_{k_j+N|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+N|k_j}, \kappa_f(x_{k_j+N|k_j})) + F(x^+_{k_j+N|k_j}) \right\} - F(x_{k_j+N|k_j}) \leq \sigma(\|\mathcal{A}\|)
\end{aligned}
$$

where $x^+_{k_j+N|k_j}$ denotes the successive state by applying the corresponding control input, e.g., $x^+_{k_j+N|k_j} \triangleq f(x_{k_j+N|k_j}, u_{k_j+N|k_j} + a_{k_j+N|k_j}, w_{k_j+N|k_j})$.

Then, by using the induction method, we show the decreasing property of $V_{N-i}(x_{k_j+i|k_j})$ as follows. Assume that $\Delta V_{N-i}(x_{k_j+i|k_j}) \leq \sigma(\|\mathcal{A}\|)$ for all $x_{k_j+i|k_j} \in \mathcal{X}_{N-i-1}$. Since the control input $u^*_{k_j+i|k_j} = K_i(x_{k_j+i|k_j})$ is well-defined for $x_{k_j+i|k_j} \in \mathcal{X}_{N-i}$, it is also feasible for the optimization problem due to $x^+_{k_j+i|k_j} = f(x_{k_j+i|k_j}, K_i(x_{k_j+i|k_j}) + a_{k_j+i|k_j}, w_{k_j+i|k_j}) \in \mathcal{X}_{N-i-1} \subseteq \mathcal{X}_{N-i}$. Then, it follows

$$
V_{N-i+1}(x_{k_j+i|k_j}) \leq \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+i|k_j}, K_i(x_{k_j+i|k_j})) + V_{N-i}(x^+_{k_j+i|k_j}) \right\}
$$

Consequently, we have

$$
\begin{aligned}
&\Delta V_{N-i+1}(x_{k_j+i|k_j}) \\
&\leq \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+i|k_j}, K_i(x_{k_j+i|k_j})) + V_{N-i}(x^+_{k_j+i|k_j}) \right\} \\
&\quad - \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ L(x_{k_j+i|k_j}, K_i(x_{k_j+i|k_j})) + V_{N-i-1}(x^+_{k_j+i|k_j}) \right\} \\
&\leq \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \left\{ V_{N-i}(x^+_{k_j+i|k_j}) - V_{N-i-1}(x^+_{k_j+i|k_j}) \right\} \leq \max_{\substack{w_{k_j+i|k_j}\in\mathcal{W} \\ a_{k_j+i|k_j}\in\mathcal{A}}} \Delta V_{N-i}(x^+_{k_j+i|k_j}) \leq \sigma(\|\mathcal{A}\|)
\end{aligned}
$$

Therefore, it can be concluded that $V_{N-i}(x_{k_j+i|k_j}) - V_{N-i-1}(x_{k_j+i|k_j}) \leq \sigma(\|\mathcal{A}\|)$ for all $x_{k_j+i|k_j} \in \mathcal{X}_{N-i-1}$ where $i = 0, 1, \ldots, N-1$.

Second, we study the property of $V_N(x_{k_{j+1}}) - V_N(x_{k_j})$. It can be achieved that

$$
\begin{aligned}
& V_N(x_{k_{j+1}}) - V_N(x_{k_j}) \\
=& V_N(x_{k_{j+1}}) - \max_{\substack{w_{k_j+i|k_j} \in \mathcal{W} \\ a_{k_j+i|k_j} \in \mathcal{A}}} \left\{ \sum_{i=0}^{H_j^*-1} \left[L(x_{k_j+i|k_j}, u^*_{k_j+i|k_j}) \right] + V_{N-H_j^*}(x_{k_j+H_j^*|k_j}) \right\} \\
\leq & -\alpha_L(\|x_{k_j}\|) + V_N(x_{k_{j+1}}) - V_{N-H_j^*}(x_{k_{j+1}}) \\
\leq & -\alpha_L(\|x_{k_j}\|) + \bar{N}\sigma(\|\mathcal{A}\|)
\end{aligned}
$$

□

Note from the above lemma that we have established the decreasing property of the value function for $\mathcal{P}_N$. In the following, we will investigate the decreasing property of the value function for $\mathcal{P}_N^r$ based on the established results from the above lemmas and the self-triggered condition. In other words, we want to show the value function for $\mathcal{P}_N^r$ is an ISpS Lyapunov function for the closed-loop system in (5.16). Now, we can proceed to the stability analysis, which is the main objective of this section.

Theorem 5.8. *Suppose that the Assumptions 5.1-5.5 hold. Given the optimization control problem defined in (5.13) and the self-triggered min-max MPC algorithm in Algorithm 5.1, the closed-loop system in (5.16) is ISpS.*

Proof. This proof can be completed by showing the optimal value function $V_N^r(x_{k_j})$ is an ISpS Lyapunov candidate for the closed-loop system in (5.16). To this end, we first study the properties of the two value functions $V_N(x_{k_j})$ and $V_N^r(x_{k_j})$. Due to the triggered mechanism design, we can always guarrantee, if Assumption 5.1 is satisfied, there exists a sucessfull transmission time sequence $k_j, \forall j \in \mathbb{N}_{\geq 0}$ such that $\boldsymbol{u}^*_{k_j}$ and $\boldsymbol{p}^*_{k_j}$ are respectively the optimal solutions for $\mathcal{P}_N$ and $\mathcal{P}_N^r$ with the same state x_{k_j}. From the formulation of $\mathcal{P}_N^r$, one can see that $(\boldsymbol{\phi}_N \otimes \mathbf{I}_m)\, \boldsymbol{p}^*_{k_j}$ is also a feasible solution to $\mathcal{P}_N$. Due to optimality, we can conclude that $V_N(x_{k_j}) \leq V_N^r(x_{k_j}), \forall j \in \mathbb{N}_{\geq 0}$.

Then, by applying the above result and the triggered condition in (5.14), one can obtain

$$
V_N^r(x_{k_{j+1}}) - V_N^r(x_{k_j}) \leq V_N(x_{k_{j+1}}) + Ce^{-H_{j+1}^*\delta} - V_N(x_{k_j}) \tag{5.21}
$$

for all $x_{k_j} \in \mathcal{X}_N$. Since Assumptions 5.3 and 5.5 hold, we can further get

$$V_N^r(x_{k_{j+1}}) - V_N^r(x_{k_j}) \leq -\alpha_L(\|x_{k_j}\|) + \bar{N}\sigma(\|\mathcal{A}\|) + Ce^{-H_{j+1}^*\delta}, \forall x_{k_j} \in \mathcal{X}_N \tag{5.22}$$

by applying the established result in Lemma 5.7. Because $\alpha_L, \sigma \in \mathcal{K}_\infty$ and $\bar{N}, Ce^{-H_{j+1}^*\delta}$ are constants, we can conclude that the closed-loop system is ISpS. □

Remark 5.9. *Note that Thoerem 5.8 investigates the closed-loop stability at triggered time instants on which DoS attacks are absent. Besides, in order to let ISpS stability hold, we must carefully design the tuning parameters of the STM, i.e., C and δ. Generally speaking, we might need C to be sufficiently large in order to ensure that the STM work properly. However, large choice of C may lead to worse control performance. Therefore, there exists a performance trade-off when designing such parameters for the STM.*

5.5 Simulation Results

In this section, we give a numerical example of applying the proposed control algorithm to a CPS-based cart-damper-spring system. The optimization problem is formulated by using CasADi [137] and solved by using Ipopt [122].

5.5.1 Simulation Configurations

Consider a CPS whose physical process is a cart-damper-spring system:

$$\begin{cases} p_{k+1} = p_k + T_s v_k \\ v_{k+1} = v_k - T_s \dfrac{\tau}{M_c} e^{-p_k} p_k - T_s \dfrac{h_d}{M_c} v_k - T_s \dfrac{w_k}{M_c} v_k + T_s \dfrac{u_k}{M_c} \end{cases}$$

where $x_k = [p_k, v_k]^\top$ denote the cart displacement and the cart velocity; $T_s = 0.2$s is the sampling period; u_k is the control input that might be corrupted by deception attack a_k; w_k is the model uncertainty; the other coefficients represent physical parameters including the cart mass $M_c = 1.25\,\mathrm{kg}$, the nonlinear factor $\tau = 0.9\,\mathrm{N/m}$, and the damping factor $h_d = 0.42\,\mathrm{Ns/m}$. The state and control input constraints are respectively given by $\mathcal{X} = \{[p, v]^\top : -2 \leq p \leq 2, -2 \leq v \leq 2\}$ and $\mathcal{U} = \{u : -1 \leq u \leq 1\}$. In this simulation, the chosen trajectories of the model uncertainty, deception attack, and DoS attack are depicted in Fig. 5.1, where the model uncertainty is bounded by

$-0.05 \leq w \leq 0.05$, the maximum attack level for deception attacks is $\theta_a = 0.03$, and the maximum duration of DoS attacks is identified as $N_a = 3$. The tuning parameters for the optimization problem (5.13) are configured as $L(x,u) = x^\top Qx + u^\top Ru$ and $F(x) = x^\top Px$ where $Q = 0.1\mathbf{I}_2$, $R = 0.1$, and $P = [0.9836, 0.3671; 0.3671, 0.8686]$. The shaping parameter for $\boldsymbol{\varphi}_i$ in (5.9) is set as $\epsilon = 0.2$ and the basis dimension is selected as $M = 5$. The terminal set is given by $\mathcal{X}_f \triangleq \{x : x^\top Px \leq 0.8\}$. The prediction horizon is configured as $N = 30$. For the STM, we configure its parameters as $C = 5$ and $\delta = 0.4$. The total simulation step is set as $N_{sim} = 100$ and the initial state is $x_0 = [-1.3, 1.4]^\top$.

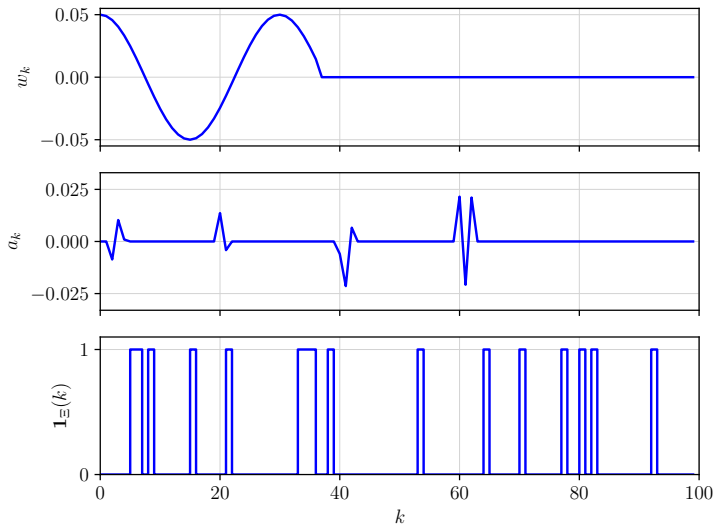

Fig. 5.1: The model uncertainty, deception attacks, and DoS attacks.

5.5.2 Results and Discussion

First, we show control performance of using the self-triggered secure min-max MPC under control sequence setup in (5.15). As shown in Fig. 5.2, it can be found that both the state trajectories and the control sequence fulfill the state and control input constraints, and the triggered time interval gradually increases to the maximum value as expected. Besides, the state trajectory converges into a small neighborhood around the origin. Therefore, the proposed control algorithm can render the closed-loop system ISpS even when the cyber attacks and uncertainty are present, which verifies the efficacy of Algorithm 5.1.

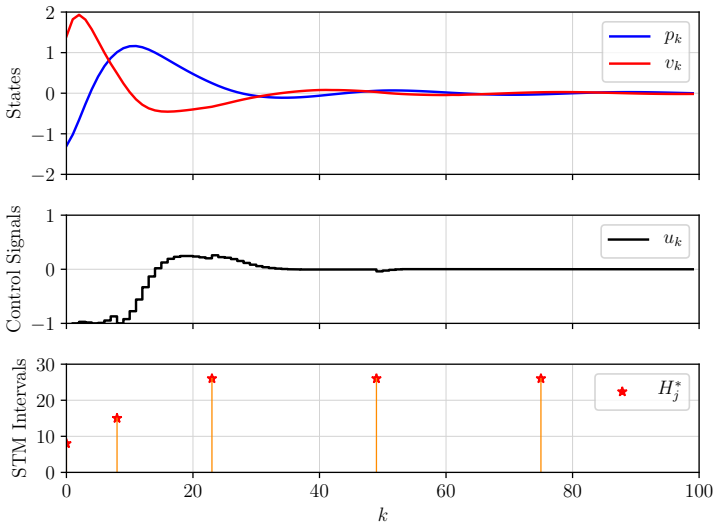

Fig. 5.2: The state trajectory, control input sequence, and self-triggered time intervals.

Second, we illustrate the performance comparison under different attack scenarios, which includes not only the control performance comparison but also the communication performance comparison. Note that the control performance is measured by averaging the cost over all simulation time step, i.e., $J_p = \frac{\sum_{k=0}^{N_{sim}} \left(x_k^\top Q x_k + u_k^\top R u_k\right)}{N_{sim}}$. The communication cost C_p is estimated by using the average sampling interval. Each set of cyber attacks are conducted in a Monte-Carlo simulation with 20 different samples. The simulation results are shown in Table 5.1, which indicates that the control performance index decreases as the deception attack level θ_a increases, while the communication performance index decreases as the DoS attack parameter N_a increases. These interesting facts reveal that our controller design in (5.15) can not only effectively maintain the control performance under DoS attacks thanks to the radial based design, but also degrade very little control performance in order to deal with deception attacks. What is even more surprising to see is that the deception attacks do not seem to affect the communication performance at all. That might be due to the specific design in the STM condition (5.14), that is, the subtraction of two value functions might minimize the effect of deception attacks to the STM.

Table 5.1: The performance comparison under different attack scenarios.

Deception (θ_a)	DoS (N_a)	J_p	C_p
0.03	3	0.0539	20.0
0.03	9	0.0541	16.67
0.03	15	0.0542	13.63
0.03	21	0.0541	10.38
0.03	3	0.0543	20
0.06	3	0.0548	20
0.09	3	0.0552	20
0.12	3	0.0559	20

5.6 Conclusion

In this chapter, we have designed a self-triggered min-max MPC framework for constrained uncertain nonlinear systems in the presence of the malicious deception attacks and DoS attacks occurring in the controller-to-actuator channel. A min-max MPC scheme has been introduced to optimize the control performance over the worst case of all possible uncertainty and deception attack realizations. In addition, a novel control sequence has been adapted for the min-max MPC in order to tackle DoS attacks. By using the proposed MPC strategy, the closed loop system has been guaranteed ISpS. The effectiveness of the proposed method has been verified by numerical examples.

Chapter 6

Model Predictive Control as A Secure Service for CPSs: A Cloud-Edge Framework

6.1 Introduction

In this chapter, the secure control problem has been investigated for CPSs assisted with the cloud-edge computing architecture. Recently, the rapid advancement of IoT and cloud-edge computing technologies have accelerated development of intelligent CPSs in many existing areas such as environmental monitoring [141], wearable IoT [142], smart transportation systems [143], and cloud-based robotic systems [144, 145]. The cloud-edge computing paradigm, by leveraging the powerful computing in the cloud node and the real-time task executing in the edge node, plays a key role in providing performance, reliability, flexibility and scalability for CPS. Emerging as one of important CPS applications, the cloud-based control system has increasingly drawn attention nowadays because of its powerful cloud computing capabilities (see, e.g., [143, 146, 147]). However, the integration of the cyber and physical components in cloud and edge layers inevitably causes various cyber-physical issues including cyber abnormalities (e.g., cyber security [148] and limited data transmission bandwidth) and physical limitations (e.g., control saturation, state constraint and external disturbance).

To deal with cyber-physical issues in the cloud-based control system, we propose an MPCaaSS framework which integrates with the cloud-edge computing technology

and ECC based encryption. However, there are two key practical issues when one applies conventional MPC to cloud-edge assisted control applications. The first major issue lies in the fact that constrained multi-parametric optimization problems may be computationally intractable for the edge nodes; the second one is the excessive data transmission (e.g., the optimal decision variables) of directly applying MPC in the cloud, which could lead to unnecessary waste of cloud network bandwidth resource especially when considering lots of requests from many edge nodes. In addition to the cloud-induced issues of applying MPC to cloud-based control systems, another significant problem is data security when transmitting data packets over unreliable network. The objective of data security is to make sure that no packet can be intercepted and corrupted by eavesdroppers and malicious attackers, leading to security enhancement in applying MPC to CPS over unreliable communication network. Therefore, it is desirable to develop a secure cloud-based robust MPC framework which can not only alleviate communication load on the cloud node, but also allow computationally tractable implementation for the edge node.

The research on cloud-based control of CPS can be categorized into two main directions in terms of considering the cloud computing paradigm [147, 149, 150] and the cloud-edge computing paradigm [151, 152]. In the first research direction, the control signals are directly generated in the cloud and transmitted to the controlled plant via communication network. For example, a cloud-service based robot control was proposed in [149], which can simultaneously tackle motion planning and control of the robots. In [150], the authors proposed a cloud-based event-driven control framework for large-scale industrial automation systems by embedding the event-driven controller as a cloud service. In the second research direction, the cloud is used for assisting the edge node to generate the real-time control law. For instance, the authors in [152] was able to design an adaptive control law by incorporating the cloud-side fuzzy rule-based systems with a locally deployed PID controller. Research interests on cloud-based MPC can be found in [153–156]. In [154], a concept and architecture of MPC as a service was proposed, where a feedback control was implemented in a cloud-based robot control application. In [155], a game-theoretical framework, describing bandwidth allocation based on a mutirate method, was introduced to MPC for dealing with the time-delay issues. One of the most recent work [156] proposed a cloud-based MPC framework by using variable horizon technique, where the cloud was utilized to implement a variable prediction horizon MPC while a local controller was introduced to ensure robustness. To the best of our knowledge, there are no research

results on simultaneously dealing with cyber abnormalities and physical limitations for CPSs.

In this work, we consider secure control problem of CPS while taking advantage of cloud-edge computing capabilities and ECC-based encryption. The contributions are summarized as follows. 1) An MPCaaSS framework is proposed to alleviate the data packet transmission load and provide real-time control performance for CPS in the presence of cyber threats and external disturbance. By formulating a new MPC optimization problem using Gaussian radial basis functions, an efficient cloud-based control law is designed which can make good use of the cloud computing advantage and real-time task executing of the edge node. 2) A secure data transmission protocol is designed for MPCaaSS framework by using ECC-based encryption method and a specifically-designed coding scheme. The ECC-based encryption consists of ECC shared key agreement and symmetric encryption, which is able to randomly update the key for symmetric encryption without sharing any sensitive information, and therefore provide superior security for CPS against various cyber threats. 3) The recursive feasibility of the MPCaaSS optimization problem is proved under several sufficient conditions. Moreover, the robust stability of the closed loop system is derived under conditions that the recursive feasibility is guaranteed and the Gaussian radial basis functions are properly designed.

The remainder of this chapter is organized as follows. Section 6.2 and Section 6.3 present preliminary results and the problem formulation, respectively. In Section 6.4, we describe the MPCaaSS framework. Main theoretical results are obtained in Section 6.5. In Section 6.6, we conduct numerical examples to illustrate effectiveness of the proposed method. Finally, we conclude this chapter in Section 6.7.

Notations: All the real numbers, nonnegative integers and positive integers are denoted by $\mathbb{R}$, $\mathbb{N}_{\geq 0}$ and $\mathbb{N}_{>0}$. We use $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ to represent all real column vectors of length n and all real matrices of size n by m, where $m, n \in \mathbb{N}_{>0}$. For a given matrix $X \in \mathbb{R}^{n\times m}$, its transpose is represented by $X^\top$; a matrix is called symmetric if its transpose is identical with itself. For a symmetric matrix $S \in \mathbb{R}^{n\times n}$, $S \succ 0$ (or $S \succeq 0$) means that S is positive definite (or positive semidefinite). For any $x \in \mathbb{R}^n$, $\|x\|$ represents the Euclidean norm. The distance from a point $z \in \mathbb{R}^n$ to a set $\mathcal{X} \subseteq \mathbb{R}^n$ is denoted by $\mathrm{dist}(z, \mathcal{X}) \triangleq \inf_{x\in\mathcal{X}} \|x - z\|$. Given two sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{R}^n$, the Minkowski sum of these two sets is $\mathcal{X} \oplus \mathcal{Y} \triangleq \{x + y : x \in \mathcal{X}, y \in \mathcal{Y}\}$; the Pontryagin difference is $\mathcal{X} \ominus \mathcal{Y} \triangleq \{z : z + y \in \mathcal{X}, \forall y \in \mathcal{Y}\}$.

6.2 Preliminaries

6.2.1 Elliptic Curve Cryptography

ECC is a well-known pub-key cryptography scheme that has been formally accepted as one of the main substitutions for the most widely used asymmetric cryptosystem, i.e., RSA. The security of RSA is based on the computational difficulty of large prime factorization. Unlike RSA, ECC derives its security using a completely different underlying mathematical property of elliptic curves, i.e., the difficulty of finding the discrete logarithm of a random point on the curve with respect to a base point. Compared with RSA, ECC offers better security and thus permits smaller key size for achieving comparative security [157].

Elliptic curves are a series of smooth cubic curves that have the following form:

$$e_y^2 = e_x^3 + ae_x + b, \tag{6.1}$$

where the condition $4a^3 + 27b^2 \neq 0$ is imposed on the fixed coefficients a and b in order to eliminate singularity. The set of points on the elliptic curve can be denoted by

$$\mathcal{E} \triangleq \{(e_x, e_y) \in \mathbb{R}^2 \big| e_y^2 = e_x^3 + ae_x + b\} \cup \{\mathcal{O}\}. \tag{6.2}$$

Note that $\mathcal{O}$ is defined as the point at infinity. Using this $\mathcal{O}$ as an identity element, one can define a *geometric addition* operation such that the set $\mathcal{E}$ forms a commutative group (also known as Abelian group) with respect to this addition operation.

Next, one can restrict the above elliptic curve over a finite field $\mathbb{F}_{e_p}$, i.e., the set of integers modulo a prime number e_p. The set of points now becomes

$$\mathcal{E}(\mathbb{F}_{e_p}) \triangleq \{(e_x, e_y) \in \mathbb{F}_{e_p}^2 \big| e_y^2 = e_x^3 + ae_x + b \pmod{e_p}\} \cup \{\mathcal{O}\}, \tag{6.3}$$

which is also a commutative group under the geometric addition. Then, the *scalar multiplication* is defined as

$$k_e \cdot G = \underbrace{G + G + \ldots + G}_{n \text{ times}} = S \in \mathcal{E}(\mathbb{F}_{e_p}), \tag{6.4}$$

where $G \in \mathcal{E}(\mathbb{F}_{e_p})$ is called a base point. As the most fundamental building block of the elliptic curve encryption, the ECDLP for (6.1) is defined as the inverse problem of scalar multiplication, i.e., given an $S \in \mathcal{E}(\mathbb{F}_{e_p})$ find the corresponding k_e such

that (6.4) holds. The ECDLP is known to take exponential time to solve, which permits its broad use in modern cryptography. Specifically, $k_e \in \mathbb{F}_{e_p}$ is the private key and $k_e \cdot G$ is the public key in an ECC-based context.

6.2.2 RPI-Based Constraint Tightening

In order to deal with external disturbances, the constraint tightening approaches based on the RPI set have been widely exploited in the existing MPC literature (e.g., [22, 158]). The problem of finding an RPI set can be given as follows.

Definition 6.1. *The set $\mathcal{R}$ is said RPI for the system*

$$x_{k+1} = \Phi x_k + w_k \tag{6.5}$$

if $\forall x \in \mathcal{R}$, $w \in \mathcal{W}$, $\Phi x + w \in \mathcal{R}$. Alternatively, $\mathcal{R}$ is called an RPI set for (6.5).

For a stabilizing feedback gain K, the maximum state deviation due to disturbance can be characterized by

$$\mathcal{R}_i \stackrel{\triangle}{=} \oplus_{\ell=0}^{i-1} \left(\Phi^\ell \mathcal{W}\right) \tag{6.6}$$

where $\Phi \stackrel{\triangle}{=} A + BK$. Due to existence of disturbance, the real state and applied control input can be given as

$$x_{k+i} \stackrel{\triangle}{=} x_{k+i|k} + \sum_{\ell=1}^{i} \Phi^\ell w_{k+\ell-1}, \tag{6.7a}$$

$$u_{k+i} \stackrel{\triangle}{=} u_{k+i|k} + \sum_{\ell=1}^{i} K\Phi^\ell w_{k+\ell-1} \tag{6.7b}$$

where $x_{k+i|k}$ and $u_{k+i|k}$ are predicted state and control input when applying the control law to the nominal system, i.e., neglect disturbance effect to the real system.

Note the state constraint set and control input constraint set can be denoted as $\mathcal{X}$ and $\mathcal{U}$, respectively. In addition, the tightened terminal set (i.e., the state constraint for the last state prediction) can be given as

$$\mathcal{X}_f \stackrel{\triangle}{=} \{x : \Phi^i x \in \mathcal{X}_i,\, K\Phi^i x \in \mathcal{U}_i \;\forall i \in \mathbb{N}_{\geq 0}\} \tag{6.8}$$

Based on (6.7) and (6.8), the corresponding tightened state and control input con-

straint sets are introduced as follows

$$\mathcal{X}_i \triangleq \mathcal{X} \ominus \mathcal{R}_i, \tag{6.9a}$$

$$\mathcal{U}_i \triangleq \mathcal{U} \ominus K\mathcal{R}_i \tag{6.9b}$$

$$\mathcal{X}_N \triangleq \mathcal{X}_f \ominus \mathcal{R}_N \tag{6.9c}$$

6.3 Problem Formulation

The control system is deployed in a CPS-based architecture, which has two layers in order to take advantage of the cloud-edge computing. The cloud layer includes powerful computing devices used for processing computationally heavy tasks, while the edge layer provides a computational unit with limited computational resources but better real-time performance. Both of the layers are installed with interfacing facilities that can support the data packet transmission over the network.

Consider the physical process modeled by the discrete-time LTI dynamics:

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{6.10}$$

where $x_k \in \mathcal{X} \subseteq \mathbb{R}^{n_x}$ denotes the constrained system state, $u_k \in \mathcal{U} \subseteq \mathbb{R}^{n_u}$ represents the constrained control input, $w_k \in \mathcal{W} \subseteq \mathbb{R}^{n_x}$ is the perturbed input due to disturbance and quantization error; $A \in \mathbb{R}^{n_x \times n_x}$ and $B \in \mathbb{R}^{n_x \times n_u}$ are the system matrices.

Assumption 6.2. *For the system in (6.10), it is assumed that*

A1: the pair (A, B) is stabilizable;

A2: $\mathcal{X}$, $\mathcal{U}$, and $\mathcal{W}$ are compact and convex sets containing the origin as their interior points.

It can be derived from Definition 6.1 and (6.6) that $\mathcal{R}_\infty$ is the smallest RPI set. Using the above information, the robust stability can be described in the following definition.

Definition 6.3. *For the system in (6.10) with the control law $u_k = \mu(x_k)$, if the following property holds:*

$$\lim_{k\to\infty} \operatorname{dist}(x_k, \mathcal{R}_\infty) = 0 \tag{6.11}$$

then the closed-loop system is robustly stable.

To facilitate the cloud-edge computing, the cloud-based control system needs to consider the following issues. The edge layer usually features a less powerful computing device, which does not suffice to perform computationally heavy tasks, e.g., solving constrained optimization problems. Although the cloud layer can alleviate the computational burden of the edge layer, the communicational load of the cloud layer will dramatically increase due to excessive information exchanges over the communication networks. Besides, the communication network between the cloud layer and edge layer may be exposed to various cyber threats such as malicious attackers and eavesdroppers.

In the cloud-based control system design, it is also important to consider physical constraints in terms of control input saturation and operational safety mainly due to the actuator saturation. These constraints naturally arise as one of the major practical issues in the controller design especially when one needs to implement a feasible control strategy. It is even more challenging to simultaneously consider the physical constraints and external disturbances in the cloud-based control framework. Therefore, the following three questions and objectives are to be addressed in this work.

- How to design an efficient controller architecture while taking advantage of the cloud-edge computing paradigm?
- How to ensure secure data transmission over untrusted communication networks between the cloud and edge layers?
- How to guarantee the constraint satisfaction and robust stability of the closed-loop system in such a cloud-edge-based CPS setting?

To address the above problems, an MPCaaSS framework taking advantage of the cloud-edge computing will be proposed. Specifically, we will adapt a conventional robust MPC into a cloud-edge computing enabled CPS environment, which leads to secure, robust and efficient control strategy that can not only reduce the communicational load of the cloud layer, but also can be computationally tractable on the edge layer.

6.4 MPCaaSS Framework

In this section, we present the details of the MPCaaSS framework. As seen in Fig. 6.1, MPCaaSS exploits a double-layer secure controller architecture aiming to make full use of the cloud-edge computing advantages while preserving security against cyber threats. On the cloud layer, a cloud-side controller (CSC) based on a modified MPC is deployed in order to compute the optimal controller parameter that fulfills both the state and control constraints despite the effect of disturbances. While on the edge layer, an edge-side controller (ESC) is used to translate the controller parameter into real-time control law. In addition, in order to reduce the network bandwidth usage between the cloud layer and the edge layer, we explicitly adapt the control sequence of robust MPC by using a radial basis function based parameterization method permitting small basis dimensions.

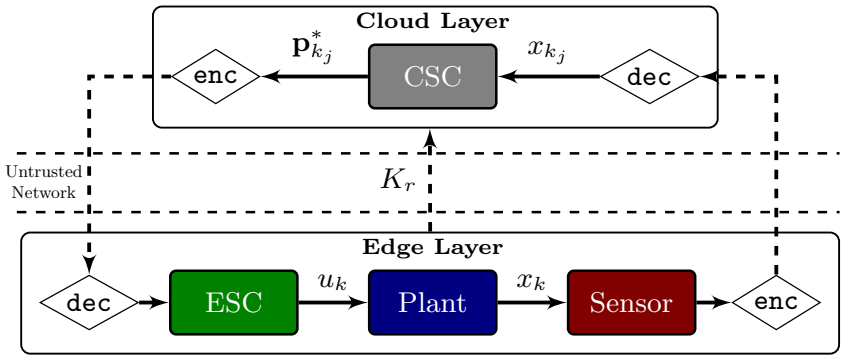

Fig. 6.1: The MPCaaSS framework.

6.4.1 Double-Layer Controller Architecture

In this part, we provide synthesis of the double-layer controller via Gaussian radial functions. At some time instant k_j, the cloud-based MPC solves an optimization control problem aiming to generate controller profile such that the control law can be implemented by the edge-side controller.

Edge-Side Controller

We take a controller architecture of the following form:

$$\mu_k = Kx_k + c_k \tag{6.12}$$

where $\mu : \mathcal{X} \mapsto \mathcal{U}$ is a mapping from state to control input. The first portion Kx_k is a stabilizing state-feedback controller for the system in (6.10), while the second portion c_k is designed as a vanishing term used to tackle the system constraint, i.e., make the control law (6.12) and the resulting closed-loop system obey control and state constraints. Note that obviously in our design, c_k consists of n_u components. Then, its ith component can be denoted as

$$c_{i,k} = \sum_{r=0}^{M-1} p_r \varphi_i(r) \tag{6.13}$$

where $p_r \in \mathbb{R}^{n_u \times 1}$ and

$$\varphi_i(r) \triangleq e^{-(i+1)\rho^2(r+1)^2} \tag{6.14}$$

with $\rho \in (0, 1)$. Using some matrix techniques, we can combine (6.12) and (6.13) into a compact form:

$$\mu_k(\boldsymbol{p}_{k_j}) = Kx_k + \left(\boldsymbol{\varphi}_{k-k_j}^\top \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}_{k_j} \tag{6.15}$$

where

$$\begin{aligned} \boldsymbol{p}_{k_j} &\triangleq \boldsymbol{p}_{k_j}^M = [p_{0,k_j}^\top, p_{1,k_j}^\top, p_{2,k_j}^\top, \ldots, p_{M-1,k_j}^\top]^\top, \\ \boldsymbol{\varphi}_i &\triangleq \boldsymbol{\varphi}_i^M = [\varphi_i(0), \varphi_i(1), \ldots, \varphi_i(M-1)]^\top. \end{aligned}$$

Note that $\boldsymbol{p}_{k_j}$ is the controller profile, $\boldsymbol{\varphi}_i$ is composed of Gaussian radial basis functions, and M is the basis dimension. It is worth noting that the controller profile $\boldsymbol{p}_{k_j}$ is designed as the coefficients of $\boldsymbol{\varphi}_i$. Hence, $p_{r,k_j} \in \mathbb{R}^{n_u}$ are the weights for the r-th component of $\boldsymbol{\varphi}_i$. Noting that M is clear from the context, thus with slight abuse of notation, the superscript of $\boldsymbol{p}^M$ and $\boldsymbol{\varphi}_i^M$ will be omitted for brevity.

Remark 6.4. *It is worth noting that the function $\varphi_i(r)$ gets its maximum value when $r = 0$. Specifically, $\varphi_i(r) \triangleq e^{-(i+1)\rho^2(r+1)^2}$ denotes the rth linearly-independent Gaussian radial basis function at the ith step, and ρ is a tuning parameter for shaping the Gaussian radial basis function.*

Cloud-Side Controller

By using (6.15) as the control decision variables, the optimization problem $\mathcal{P}$ for the MPCaaSS framework can be formulated as follows:

$$\boldsymbol{p}_{k_j}^* = \arg\min_{\boldsymbol{p}_{k_j}} V_N(x_{k_j}, \boldsymbol{p}_{k_j}) \tag{6.16a}$$

$$\text{s.t.} \quad x_{k_j|k_j} = x_{k_j} \tag{6.16b}$$

$$x_{k_j+i+1|k_j} = \Phi x_{k_j+i|k_j} + B\left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_{n_u}\right)\boldsymbol{p}_{k_j} \tag{6.16c}$$

$$u_{k_j+i|k_j} = K x_{k_j+i|k_j} + \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_{n_u}\right)\boldsymbol{p}_{k_j} \tag{6.16d}$$

$$x_{k_j+i|k_j} \in \mathcal{X}_i,\ u_{k_j+i|k_j} \in \mathcal{U}_i \tag{6.16e}$$

$$x_{k_j+N|k_j} \in \mathcal{X}_N \tag{6.16f}$$

where N is the prediction horizon, $\Phi \triangleq A + BK$, $\boldsymbol{p}_{k_j} \in \mathbb{R}^{Mn_u}$ is the decision variable, $\mathcal{X}_i, \mathcal{U}_i$, and $\mathcal{X}_N$ are defined in (6.9). Correspondingly, the cost function can be written as

$$V_N(x_{k_j}, \boldsymbol{p}_{k_j}) \triangleq \sum_{i=0}^{N-1} \left(\boldsymbol{p}_{k_j}^\top \left(\boldsymbol{\varphi}_i \otimes \mathbf{I}_{n_u}\right) \Psi_r \left(\boldsymbol{\varphi}_i^\top \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}_{k_j} \right) \tag{6.17}$$

where $\Psi_r \succ 0$. By applying some matrix techniques, we can obtain a compact matrix form of the cost function (6.17) as follows

$$V_N(x_{k_j}, \boldsymbol{p}_{k_j}) \triangleq \boldsymbol{p}_{k_j}^\top \left(\boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r\right) \boldsymbol{p}_{k_j} \tag{6.18}$$

where

$$\boldsymbol{\phi}_N \triangleq \boldsymbol{\phi}_N^M = \left[\boldsymbol{\varphi}_0, \boldsymbol{\varphi}_1, \boldsymbol{\varphi}_2, \ldots, \boldsymbol{\varphi}_{N-1}\right]^\top$$

Note that $\boldsymbol{\phi}_N$ is a matrix of size N by M. It is worthwhile noting that the optimization control problem (6.16) with the new cost function (6.18) has only one decision variable $\boldsymbol{p}_{k_j}$ no matter how large the prediction horizon N is chosen.

In the proposed controller architecture, there is no necessity to transmit the feedback gain and the Gaussian radial basis functions since both of them can be preset in controllers on both cloud and edge layers. The cloud layer only needs to receive the state measurement and then to send the controller parameter to the edge layer after solving each constrained optimization problem. Similarly, the edge layer receives the controller parameter for implementing the real-time control law, and sends the

current state measurement to the cloud layer upon request for updating controller parameters. In fact, the communication load of data transmission between the cloud and edge layers can be significantly reduced: Only the controller parameter $\boldsymbol{p}_{k_j}$ and the state measurement x_{k_j} need to be transmitted, which has a significant meaning in real-time control.

6.4.2 Secure Data Transmission Protocol

In order to securely transmit the necessary data (i.e., $\boldsymbol{p}_{k_j}$ and x_{k_j}) over unreliable communication channels, we propose an ECC-based secure transmission protocol and a specifically-designed quantization and encoding scheme for the MPCaaSS framework.

First, we need to encode the above real-valued vectors into binary representations, i.e., design a function $\mathscr{E} : \mathbb{R}^n \mapsto \mathbb{Z}$. The quantization and encoding scheme can be described by

$$\begin{aligned}
\mathscr{E}(\boldsymbol{p}_{k_j}): \quad & \underbrace{1 \sim 4}_{precision} \quad \underbrace{5 \sim 8}_{Mn_u} \quad \underbrace{9 \sim 24}_{\text{for } p_{0,k_j}} \ldots \underbrace{16i-7 \sim 8+16i}_{\text{for } p_{i-1,k_j}} \ldots \\
\mathscr{E}(x_{k_j}): \quad & \underbrace{1 \sim 4}_{precision} \quad \underbrace{5 \sim 8}_{n_x} \quad \underbrace{9 \sim 24}_{\text{for } x_{1,k_j}} \ldots \underbrace{16i-7 \sim 8+16i}_{\text{for } x_{i,k_j}} \ldots
\end{aligned}$$

where the first four digits represent the quantization precision; the next four digits denote sizes of $\boldsymbol{p}_{k_j}$ and x_{k_j}; the remaining digits characterize each element of $\boldsymbol{p}_{k_j}$ and x_{k_j} in 16−bit binary representations. However, due to the quantization error, we cannot transmit the exact controller profile and the state measurement using the above encoding scheme. Moreover, we can represent the decoding scheme with the quantization error as follows

$$\boldsymbol{p}_{k_j} = \underbrace{\mathscr{E}^{-1}\left(\mathscr{E}(\boldsymbol{p}_{k_j})\right)}_{\hat{\boldsymbol{p}}_{k_j}} + \epsilon_{\boldsymbol{p}} \tag{6.19}$$

$$x_{k_j} = \underbrace{\mathscr{E}^{-1}\left(\mathscr{E}(x_{k_j})\right)}_{\hat{x}_{k_j}} + \epsilon_x \tag{6.20}$$

where $\mathscr{E}^{-1} : \mathbb{Z} \mapsto \mathbb{R}^n$ is the inverse mapping of $\mathscr{E}$, $\epsilon_{\boldsymbol{p}}$ is the quantization error for encoding the controller profile, and ϵ_x is the quantization error for encoding the state measurement.

Remark 6.5. *It is noteworthy that, for every transmission, the controller profile and state measurement can be encoded in binary-valued packets with identical word length. In addition, from the encoding scheme, the highest and lowest quantization error can be identified as* $\frac{1}{2^{16}}$ *and* $\frac{1}{2^{1}}$*, respectively.*

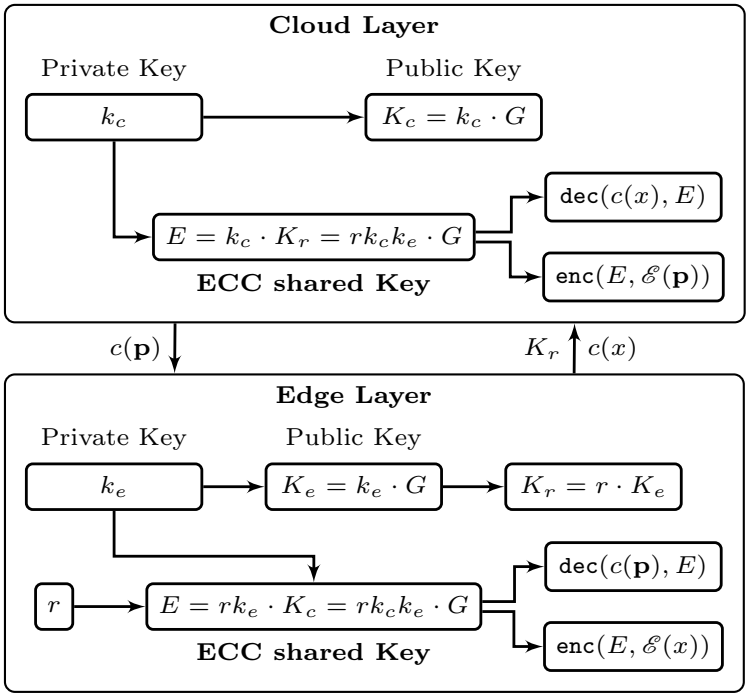

Fig. 6.2: ECC-based secure data transmission scheme.

Second, based on the quantization and encoding scheme, we introduce an ECC-based encryption method in order to securely transmit the encoded packets over unreliable communication networks. The ECC-based encryption consists of two processes, i.e., ECC shared key agreement and symmetric encryption. Specifically, the ECC shared key agreement is employed in order to achieve the same encryption keys in both the cloud and the edge layers, while the symmetric encryption is used to encrypt the packet transmission using the ECC shared key.

To fulfill the security objective, as shown in Fig. 6.2, the secure controller in the edge layer not only hold a private key k_e but also generate and send to the cloud layer a temporary public key K_r at each sampling time instant. With this temporary public key, the cloud-side controller is able to recover the ECC shared key E using its own private key k_c without knowing anything sensitive from the cloud layer. Moreover, due to the randomization of r, it can be guaranteed that the shared

keys used for encrypting $\mathscr{E}(\boldsymbol{p}_{k_j})$ and $\mathscr{E}(x_{k_j})$ at $k_j, j \in \mathbb{N}_{\geq 0}$ are different and unrelated with respect to the sampling time instants, which improves the security. In addition, the proposed encryption scheme is based on Advanced Encryption Standard (AES). Detailed procedures of the encryption scheme is illustrated in Algorithm 6.1.

Algorithm 6.1: Symmetric encryption

Require: The ECC shared key E_{k_j};

– ENCRYPTION:

Encode $\boldsymbol{p}_{k_j}, x_{k_j}$ to $\mathscr{E}(\boldsymbol{p}_{k_j}), \mathscr{E}(x_{k_j})$;

Compute $c(\boldsymbol{p}_{k_j}), \mathtt{tag}_{\boldsymbol{p}} \leftarrow \mathtt{enc}(E_{k_j}, \mathscr{E}(\boldsymbol{p}_{k_j}))$;

Compute $c(x_{k_j}), \mathtt{tag}_x \leftarrow \mathtt{enc}(E_{k_j}, \mathscr{E}(x_{k_j}))$;

– DECRYPTION:

Compute $\mathscr{E}(\boldsymbol{p}_{k_j}), \mathtt{tag}_{\boldsymbol{p}} \leftarrow \mathtt{dec}(c(\boldsymbol{p}_{k_j}), E_{k_j})$;

Compute $\mathscr{E}(x_{k_j}), \mathtt{tag}_x \leftarrow \mathtt{dec}(c(x_{k_j}), E_{k_j})$;

Verify $\mathtt{tag}_{\boldsymbol{p}}, \mathtt{tag}_x$ to see if data is corrupted;

if *Verification is passed* **then**

  Decode $\mathscr{E}(\boldsymbol{p}_{k_j}), \mathscr{E}(x_{k_j})$ to $\boldsymbol{p}_{k_j}, x_{k_j}$;

end

6.4.3 MPCaaSS Algorithm Design

Now, we present the overall design of the MPCaaSS algorithm based on the double-layer controller architecture and the secure data transmission protocol. At each sampling time k_j, the edge layer needs to first generate a new ECC shared key that is used to encrypt the state measurement. Then, the encrypted state is transmitted to the cloud layer. After receiving the encrypted state, the cloud layer first use the ECC shared key, obtained by using the method illustrated in Fig. 6.2, to decrypt the state for solving the MPC optimization problem. Finally, the calculated controller parameter will be encrypted and sent to the edge layer for implementing the edge-side

control law.

Algorithm 6.2: Model predictive control as a secure service

Require: Edge-side controller parameters $\rho, \boldsymbol{\varphi}_i, K$; Cloud-side controller parameters $N, \mathcal{X}_i, \mathcal{U}_i, \mathcal{X}_N$; ECC-based encryption parameters G, k_c, k_e, K_c, K_e;

Initialization: Set the initial time $k = 0$, the initial sampling time $k_0 = 0$, and $j = 0$;

while *The service is not stopped* **do**

– Cloud Layer:

Receive the encrypted state measurement $c(x_{k_j})$ and the temporary public key K_r at k_j;

Compute the ECC shared key E_{k_j} using k_c and K_r;

Decrypt $c(x_{k_j})$ to get x_{k_j} using the decryption method in Algorithm 6.1;

Obtain $\boldsymbol{p}^*_{k_j}$ by solving (6.16);

Encyrpt $\boldsymbol{p}^*_{k_j}$ to $c(\boldsymbol{p}^*_{k_j})$ using the encryption method in Algorithm 6.1;

– Edge Layer :

Decrypt $c(\boldsymbol{p}^*_{k_j})$ to get $\boldsymbol{p}^*_{k_j}$ using the decryption method in Algorithm 6.1;

while $k < k_{j+1}$ **do**

Apply the edge-side control law (6.22) to the system (6.10);

$k = k + 1$;

end

$j = j + 1$;

Generate the random number r;

Compute E_{k_j} using r, k_e and K_c;

Update K_r using r and k_e as shown in Fig. 6.2;

Sample and encrypt the state measurement x_{k_j};

Send $c(x_{k_j})$ and new K_r to the cloud-side controller;

end

In this part, we present the overall design of the MPCaaSS algorithm based on the double-layer controller architecture and the secure data transmission protocol.

By applying Algorithm 6.2 to the controlled system (6.10), the closed-loop system

can be formulated as

$$x_{k+1} = Ax_k + B\mu_k^{SC} + d_k \tag{6.21}$$

$$\mu_k^{SC} = Kx_k + \left(\boldsymbol{\varphi}_{k-k_j}^{\top} \otimes \mathbf{I}_{n_u}\right) \hat{\boldsymbol{p}}_{k_j}^{*} \tag{6.22}$$

where d_k is the disturbance, μ_k^{SC} is the edge-side control signal applied to the system in (6.10), and $\hat{\boldsymbol{p}}_{k_j}^{*} \triangleq \mathscr{E}^{-1}\left(\mathscr{E}(\boldsymbol{p}_{k_j}^{*})\right)$ is the optimal controller parameter after the quantization process according to (6.19). Note that $k_j \in \mathbb{N}_{\geq 0}, j \in \{0, 1, 2, \ldots\}$ are time instants when the optimization problems are solved. In addition, using (6.19), the closed-loop system can be rewritten as

$$x_{k+1} = Ax_k + B\mu_k^{SC} + \underbrace{\epsilon_k + d_k}_{w_k} \tag{6.23}$$

$$\mu_k^{SC} = Kx_k + \left(\boldsymbol{\varphi}_{k-k_j}^{\top} \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}_{k_j}^{*} \tag{6.24}$$

where $\epsilon_k = B\left(\boldsymbol{\varphi}_{k-k_j}^{\top} \otimes \mathbf{I}_{n_u}\right) \epsilon_{\boldsymbol{p}}$.

In the cloud-based MPC scheme, the cloud node firstly computes the optimal solution $\boldsymbol{p}_{k_j}^{*}$ of (6.16). Then, the optimal solution is encrypted and sent to the edge node at which the state-feedback gain K and the radial basis functions can be preset. Finally, the edge node can implement the control law (6.22) in real time.

6.5 Analysis

In this section, the theoretical properties regarding the recursive feasibility and the robust stability are considered. First, a candidate control sequence is introduced. Second, some sufficient conditions are developed for guaranteeing that the MPCaaSS optimization problem (6.16) is feasible at any subsequent sampling time instants. Third, the closed-loop system in (6.21) are proved to be robustly stable.

In the following, a new candidate control sequence for the optimization problem (6.16) at the next sampling time k_{j+1} is firstly introduced. By applying the widely used left-shifting technique (see, e.g., [15, 125, 159]) to the optimal control sequence generated at the last sampling time k_j, we formulate the candidate control sequence as

$$\tilde{\boldsymbol{c}}_{k_{j+1}} \triangleq \left(\tilde{\boldsymbol{\phi}}_N \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}_{k_j}^{*} \tag{6.25}$$

where

$$\tilde{\boldsymbol{\phi}}_N \triangleq \left[\boldsymbol{\varphi}_{k_{j+1}-k_j} \;\; \boldsymbol{\varphi}_{k_{j+1}-k_j+1} \;\; \cdots \;\; \boldsymbol{\varphi}_{k_{j+1}-k_j+N-1} \;\right]^\top$$

and $\boldsymbol{p}^*_{k_j}$ is the optimal solution obtained by solving the MPCaaSS optimization problem (6.16) at k_j. Based on the property of radial functions $\boldsymbol{\varphi}_i$, we have

$$\boldsymbol{\varphi}_{k_{j+1}-k_j+i} = \boldsymbol{\varphi}_i \,\mathrm{diag}\,(\boldsymbol{\varphi}_{k_{j+1}-k_j-1}) \tag{6.26}$$

By applying (6.26) to (6.25), one can obtain

$$\tilde{\boldsymbol{c}}_{k_{j+1}} \triangleq (\boldsymbol{\phi}_N \otimes \mathbf{I}_{n_u}) \left(\mathrm{diag}\,(\boldsymbol{\varphi}_{k_{j+1}-k_j-1}) \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}^*_{k_j} \tag{6.27}$$

where $\boldsymbol{\phi}_N$ is defined in (6.18). Finally, we can get the corresponding candidate solution $\tilde{\boldsymbol{p}}_{k_{j+1}}$ for (6.16):

$$\tilde{\boldsymbol{p}}_{k_{j+1}} = \left(\mathrm{diag}\,(\boldsymbol{\varphi}_{k_{j+1}-k_j-1}) \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}^*_{k_j} \tag{6.28}$$

which is based on the optimal solution of (6.16) at k_j. Then, we can analyze the recursive feasibility property by investigating the sufficient conditions under which $\tilde{\boldsymbol{p}}_{k_{j+1}}$ is a feasible solution for (6.16) at k_{j+1}.

Lemma 6.6. *Suppose that Assumptions A1 and A2 hold. For the system (6.10) under the control law (6.22), the candidate solution $\tilde{\boldsymbol{p}}_{k_{j+1}}$ is feasible for (6.16) at k_{j+1}, if the following conditions are satisfied:*

$$B e^{-(N-1)\rho^2} \mathcal{C} \subseteq \alpha \mathcal{W},\ \alpha > 0 \tag{6.29}$$

$$\Phi(\mathcal{X}_f \ominus \mathcal{R}_\iota) \oplus \alpha \mathcal{W} \subseteq \mathcal{X}_f \ominus \mathcal{R}_{\iota+1}, \forall \iota \geq N \tag{6.30}$$

where $\mathcal{C} \triangleq \{c : \|c\| \leq \sup_{u\in\mathcal{U}, x\in\mathcal{X}}\{\|u - Kx\|\}\}$.

Proof. Let $\tilde{x}_{k_{j+1}+i|k_{j+1}}$ and $\tilde{u}_{k_{j+1}+i|k_{j+1}}$ denote the predicted states and control inputs associated with the candidate control sequence (6.27) and the initial state $x_{k_{j+1}}$. Note that, $\forall i \geq 0$

$$\begin{aligned}
\tilde{x}_{k_{j+1}+i|k_{j+1}} &= x_{k_j+i+k_{j+1}-k_j|k_j} + \Phi^i \sum_{\iota=0}^{k_{j+1}-k_j-1} \Phi^\iota w_k \\
\tilde{u}_{k_{j+1}+i|k_{j+1}} &= u_{k_j+i+k_{j+1}-k_j|k_j} + K\Phi^i \sum_{\iota=0}^{k_{j+1}-k_j-1} \Phi^\iota w_k
\end{aligned} \tag{6.31}$$

where the predicted state and control input evolve according to

$$\begin{aligned} x_{k_j+\iota+1|k_j} &= \Phi x_{k_j+\iota|k_j} + B\left(\boldsymbol{\varphi}_\iota^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^* \\ u_{k_j+\iota|k_j} &= K x_{k_j+\iota|k_j} + \left(\boldsymbol{\varphi}_\iota^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^* \\ \iota \geq 0,\, x_{k_j|k_j} &= x_{k_j} \end{aligned}$$

Based on the new candidate control sequence (6.27), two cases will be investigated respectively for the above equations, i.e., $i < k_j + N - k_{j+1}$ and $i \geq k_j + N - k_{j+1}$. In the first case, the optimal state and control sequences at last sampling time k_j are obtained by solving the optimization problem (6.16), which obey the corresponding constraints $x_{k_j+i+k_{j+1}-k_j|k_j} \in \mathcal{X} \ominus \mathcal{R}_{i+k_{j+1}-k_j}$ and $u_{k_j+i+k_{j+1}-k_j|k_j} \in \mathcal{U} \ominus K\mathcal{R}_{i+k_{j+1}-k_j}$. While in the second case, there is no such explicit constraints for the appended state and control predictions defined in the optimization problem (6.16) due to the limited sequence length N.

Therefore, we first need to show how the appended $x_{k_j+i+1+k_{j+1}-k_j|k_j}$ and $u_{k_j+i+k_{j+1}-k_j|k_j}$ are constrained for $i \geq k_j + N - k_{j+1}$. Note that, for $x_{k_j+N|k_j} \in \mathcal{X}_f \ominus \mathcal{R}_N$, we have

$$x_{k_j+N+1|k_j} = \Phi x_{k_j+N|k_j} + B\left(\operatorname{diag}\left(\boldsymbol{\varphi}_{N-1}\right)\varphi_0^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^*$$

where

$$\|\left(\operatorname{diag}\left(\boldsymbol{\varphi}_{N-1}\right)\varphi_0^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^*\| \leq e^{-(N-1)\rho^2}\|\left(\varphi_0^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^*\|$$

It can be verified that

$$e^{-(N-1)\rho^2} \to 0 \text{ as } N \to \infty$$

and

$$\|\left(\varphi_0^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^*\| \leq \sup_{u\in\mathcal{U}, x\in\mathcal{X}}\{\|u - Kx\|\}$$

If condition (6.29) holds, one can have a sufficiently large N such that, $\forall i \geq 0$

$$B\left(\boldsymbol{\varphi}_{N+i}^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^* \in \alpha\mathcal{W}, \alpha > 0$$

Because of condition (6.30), it follows that

$$\begin{aligned} x_{k_j+N+i+1|k_j} &= \Phi x_{k_j+N+i|k_j} + B\left(\boldsymbol{\varphi}_{N+i}^\top \otimes \boldsymbol{I}_m\right)\boldsymbol{p}_{k_j}^* \\ \Longrightarrow x_{k_j+N+i+1|k_j} &\in \Phi(\mathcal{X}_f \ominus \mathcal{R}_{N+i}) \oplus \alpha\mathcal{W} \subseteq \mathcal{X}_f \ominus \mathcal{R}_{N+i+1} \end{aligned}$$

for all $i \geq 0$. Now, the constraint satisfaction problem of $\tilde{x}_{k_{j+1}+i|k_{j+1}}$ and $\tilde{u}_{k_{j+1}+i|k_{j+1}}$ can be readily addressed in the following discussion.

It follows from (6.31) that, for $i < k_j + N - k_{j+1}$

$$\begin{aligned}\tilde{x}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{X} \ominus \mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ \tilde{u}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{U} \ominus K\mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus K\Phi^i \mathcal{R}_{k_{j+1}-k_j}\end{aligned}$$

and consequently

$$\begin{aligned}\tilde{x}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{X} \ominus \mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ &= \left((\mathcal{X} \ominus \mathcal{R}_i) \ominus \Phi^i \mathcal{R}_{k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ &\subseteq \quad \mathcal{X} \ominus \mathcal{R}_i\end{aligned}$$

Similarly, for $i \geq k_j + N - k_{j+1}$, we have

$$\begin{aligned}\tilde{x}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{X}_f \ominus \mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ \tilde{u}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{U} \ominus K\mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus K\Phi^i \mathcal{R}_{k_{j+1}-k_j}\end{aligned}$$

and consequently

$$\begin{aligned}\tilde{x}_{k_{j+1}+i|k_{j+1}} &\in \left(\mathcal{X}_f \ominus \mathcal{R}_{i+k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ &= \left((\mathcal{X}_f \ominus \mathcal{R}_i) \ominus \Phi^i \mathcal{R}_{k_{j+1}-k_j}\right) \oplus \Phi^i \mathcal{R}_{k_{j+1}-k_j} \\ &\subseteq \quad \mathcal{X}_f \ominus \mathcal{R}_i \subseteq \mathcal{X} \ominus \mathcal{R}_i\end{aligned}$$

Combining the two cases, one can conclude $\tilde{x}_{k_{j+1}+i|k_{j+1}} \in \mathcal{X} \ominus \mathcal{R}_i$. Similarly, we also get $\tilde{u}_{k_{j+1}+i|k_{j+1}} \in \mathcal{U} \ominus K\mathcal{R}_i$. Therefore, $\tilde{\boldsymbol{p}}_{k_{j+1}}$ is a feasible solution for (6.16) at k_{j+1} under the condition that there exists an N such that (6.29) and (6.30) hold. □

Lemma 6.6 demonstrates that, if the MPCaaSS optimization problem (6.16) admits a feasible solution at the initial time k_0, then the problem is feasible at all time steps. Different from the classic robust MPC introduced by [22], our feasibility result shows that the optimization problem (6.16) is recursively feasible under some sufficient conditions related to system dynamics, constraints, disturbance set and the radial function parameter. It is also worthwhile noting that we do not impose an explicit bound on the two consecutive sampling time k_j and k_{j+1}, which provides more flexibility in designing scheduling mechanisms for the proposed MPCaaSS controller.

In order to design MPC parameters subject to conditions (6.29) and (6.30), the following procedures should be followed: Select a large N and a proper choice of $\rho \in (0,1)$; check the first condition (6.30) to find a largest possible α; then validate condition (6.29) with the previous determined α; choose the current N if all the conditions hold, otherwise increase N to do another check. In addition, the conditions (6.29) and (6.30) reduce to a set of linear inequalities and one quadratic inequality when all the sets are polytopes.

Now, we can proceed to the robust stability analysis.

Theorem 6.7. *Suppose that the Assumptions A1 and A2 are satisfied. If 1) the MPCaaSS optimization problem (6.16) is feasible at k_0, 2) the feasibility conditions in Lemma 6.6 are satisfied, and 3) $M < N$ for $\boldsymbol{\phi}_N$ in (6.17), then the closed-loop system (6.21) is robustly stable under the cloud-based control law (6.22).*

Proof. From Lemma 6.6, the first two conditions 1) and 2) guarantee that there always exists a feasible solution for the MPCaaSS optimization problem (6.16) at any time steps.

First of all, we need to show $\boldsymbol{p}_{k_j}^*$ converges to zero as $j \to \infty$. To this end, an optimal value function with respect to $\boldsymbol{p}_{k_j}^*$ is firstly established, which will be shown to have the monotonically decreasing property. The optimal value function is defined by

$$V(x_{k_j}) \triangleq V_N(x_{k_j}, \boldsymbol{p}_{k_j}^*) = {\boldsymbol{p}_{k_j}^*}^\top \left(\boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r\right) \boldsymbol{p}_{k_j}^*$$

Then, it follows from (6.28) that

$$\begin{aligned} V(x_{k_{j+1}}) \leq \tilde{V}(x_{k_{j+1}}) &= {\boldsymbol{p}_{k_j}^*}^\top \left(\operatorname{diag}\left(\boldsymbol{\varphi}_{k_{j+1}-k_j-1}\right) \otimes \mathbf{I}_{n_u}\right) \\ &\quad \cdot \left(\boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r\right) \left(\operatorname{diag}\left(\boldsymbol{\varphi}_{k_{j+1}-k_j-1}\right) \otimes \mathbf{I}_{n_u}\right) \boldsymbol{p}_{k_j}^* \\ &< {\boldsymbol{p}_{k_j}^*}^\top \left(e^{-2\rho^2} \boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r\right) \boldsymbol{p}_{k_j}^* \end{aligned}$$

Hence,

$$V(x_{k_{j+1}}) - V(x_{k_j}) < -{\boldsymbol{p}_{k_j}^*}^\top \left((1 - e^{-2\rho^2}) \boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r\right) \boldsymbol{p}_{k_j}^*$$

which implies that $V(x_{k_j}), j \geq 0$ is monotonically decreasing as $j \to \infty$. If $N > M$, $\boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N$ is strictly positive definite. Therefore, $(1 - e^{-2\rho^2}) \boldsymbol{\phi}_N^\top \boldsymbol{\phi}_N \otimes \Psi_r$ is also strictly positive definite since $\rho \in (0,1)$ and $\Psi \succ 0$, which indicates that $\boldsymbol{p}_{k_j}$ approaches to zero as $j \to \infty$.

Second, due to the fact that $\Phi \triangleq A + BK$ has all its eigenvalues inside the unit circle, one can obtain

$$\begin{aligned} x_k = \Phi^k x_0 + \sum_{\ell=1}^{j} \sum_{\iota=k_{\ell-1}}^{k_\ell - 1} \Phi^{k-\iota-1} B \left(\boldsymbol{\varphi}_{\iota-k_{\ell-1}}^\top \otimes \mathbf{I}_{n_u} \right) \boldsymbol{p}_{k_{\ell-1}}^* \\ + \sum_{i=0}^{k-1} \Phi^{k-i-1} w_i \end{aligned} \tag{6.32}$$

whose first two terms become zeros when $k \to \infty$. Thus, it is directly deduced from (6.32) that

$$\lim_{k\to\infty} x_k = \lim_{k\to\infty} \sum_{i=0}^{k-1} \Phi^{k-i-1} w_i \in \mathcal{R}_\infty$$

which completes the proof. □

Theorem 6.7 states that, under the established sufficient conditions, the state trajectory of the closed-loop system (6.21) can be driven into $\mathcal{R}_\infty$ eventually without violating the system constraints in the presence of disturbance and quantization error.

6.6 Simulation Results

In the section, we evaluate the proposed MPCaaSS via a CPS-based quadrotor attitude control system. In order to simulate the CPS architecture supporting the cloud-edge computing, we realize the cloud and edge layers as Python classes including the emulation of the quadrotor attitude system, integrations of the MPC problem formulation and the nonlinear programming solver, and efficient implementations of the ECC-based encryption and the encoding scheme. Besides, we also implement the interfacing functions for transmitting data packets in these Python classes, which simulates the untrusted communication network. The simulation is conducted by using Python 3.7 on a PC with a six-core Intel® Core™ CPU running at 2.90 GHz and 16.00 GB RAM.

6.6.1 Physical Model and Parameter Settings

Consider the quadrotor attitude error dynamics:

$$x_{k+1} = \left(\mathbf{I} + \Delta t \begin{bmatrix} \mathbf{0}_3 & \mathbf{I}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 \end{bmatrix}\right) x_k + \Delta t \begin{bmatrix} \mathbf{0}_3 \\ \mathbf{G} \end{bmatrix} u_k + w_k$$

where Δt is the sample period, $x \triangleq [\phi, \theta, \psi, \omega_x, \omega_y, \omega_z]^\top$ denote the roll, pitch and yaw errors and corresponding angular velocities, $u \triangleq [\tau_x, \tau_y, \tau_z]^\top$ represent control torques, w is disturbed input, and $\mathbf{G} = \text{diag}\left([\frac{1}{I_x}, \frac{1}{I_y}, \frac{1}{I_z}]\right)$ is the diagonal inertia matrix with $I_x = 8.1 \times 10^{-3}$, $I_y = 8.1 \times 10^{-3}$ and $I_z = 14.2 \times 10^{-3}$. The state and control input constraints are respectively $\mathcal{X} \triangleq \{x : -2 \cdot \mathbf{1} \leq x \leq 2 \cdot \mathbf{1}\}$ and $\mathcal{U} \triangleq \{u : -0.2 \cdot \mathbf{1} \leq u \leq 0.2 \cdot \mathbf{1}\}$. The disturbed input is upper bounded by $\mathcal{W} \triangleq \{w : \|w\|_\infty \leq 0.01\}$. We can choose a stabilizing controller gain as

$$K = \begin{bmatrix} -0.2042 & 0 & 0 & -0.2787 & 0 & 0 \\ 0 & -0.2042 & 0 & 0 & -0.2787 & 0 \\ 0 & 0 & -0.2107 & 0 & 0 & -0.3282 \end{bmatrix}$$

and the weighting matrix Ψ in (6.18) as

$$\Psi = \begin{bmatrix} 22.8506 & 0 & 0 \\ 0 & 22.8506 & 0 \\ 0 & 0 & 25.4356 \end{bmatrix}$$

The basis dimension M is chosen as 3, while the shaping parameter for the basis functions is configured as $\rho = 0.2$. The terminal set is given by $\mathcal{X}_f \triangleq \{x : x^\top P x \leq 0.05\}$, where P is the solution of Lyapunov matrix equation. The prediction horizon is set as $N = 60$, which can be verified to satisfy the recursive feasibility conditions (6.29) and (6.30). The total simulation steps is set to be 150 with the sample period $\Delta t = 0.05$s and the initial state $x_0 = [\pi/2, -\pi/3, \pi/4, 0.4, -0.1, 0.5]^\top$.

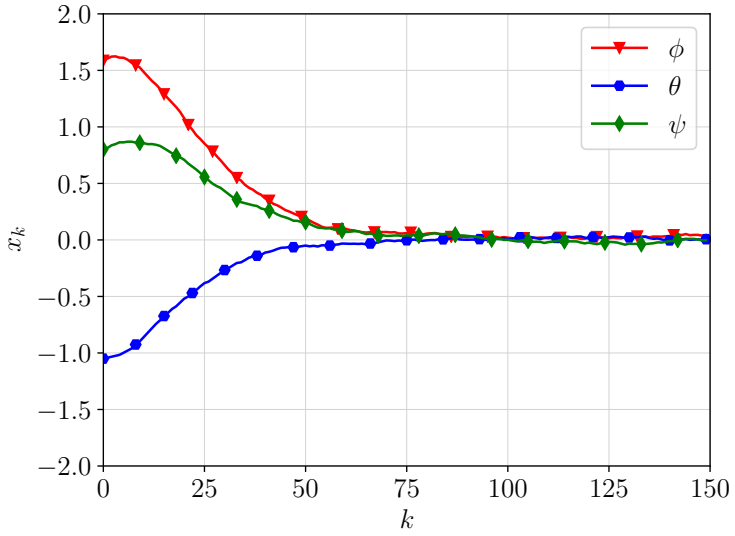

Fig. 6.3: The evolution of roll, pitch and yaw errors of the quadrotor system under MPCaaSS.

6.6.2 Secure Data Transmission Configurations

The secure data transmission configurations involve the ECC-based encryption and the quantization/coding scheme. First, we give detailed settings of the ECC-based encryption. The elliptic curve is chosen as `secp256k1`, i.e., $e_y^2 = e_x^3 + 7$ with $a = 0$ and $b = 7$, which is also used by Bitcoin [160]. The other parameters used by the ECC-based encryption are

$G =$ (`0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798`,
`0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8`)

$e_p =$ `0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f`

Then, the private and public key pairs for the cloud and edge layers, i.e., (k_c, K_c) and (k_e, K_e), can be generated by using scalar multiplication based on the above ECC parameters. In addition, the AES encryption algorithm is implemented using python library PyCryptodome [161].

Second, the settings for the quantization/coding scheme are introduced as follows. The precision for encoding the state measurement and the controller profile is set as $\frac{1}{2^8}$, which means that the left four digits of all encoded packets are `0b1000`. The data

length for representing each real value in the vectors is 16 bits. The overall packet length is set to be 256 bits in accordance to the ECC-based encryption. We can see that one packet can encode at most 15 real values, i.e., a real-valued vector with length smaller than 15. Note from the previous section that the controller profile and the state measurement need respectively 9 and 6 real values to represent. Thus, it is enough to use one packet for data transmission in the MPCaaSS framework.

6.6.3 Results and Analysis

To study the secure control performance of the proposed MPCaaSS framework, we conduct a numerical example using the cyber-physical settings and configurations as stated previously. It can be seen from Fig. 6.3 that, although there are disturbance and quantization error present, the Euler angles of the quadrotor can eventually converge into a small neighborhood around the desired attitude. Thus, the observation has verified the theoretical result presented in Theorem 6.7. The control torques generated by using the MPCaaSS controller are shown in Fig. 6.4. We can clearly observe from Fig. 6.3 and Fig. 6.4 that all the state and control input constraints are satisfied.

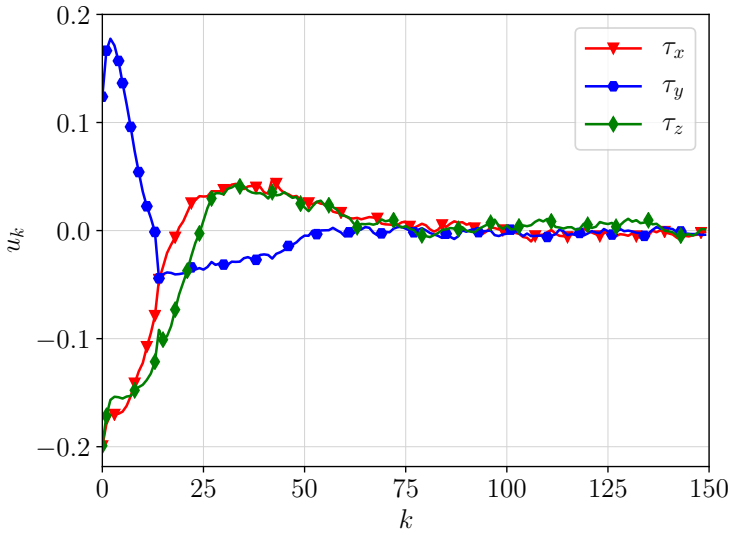

Fig. 6.4: The control torques generated by MPCaaSS.

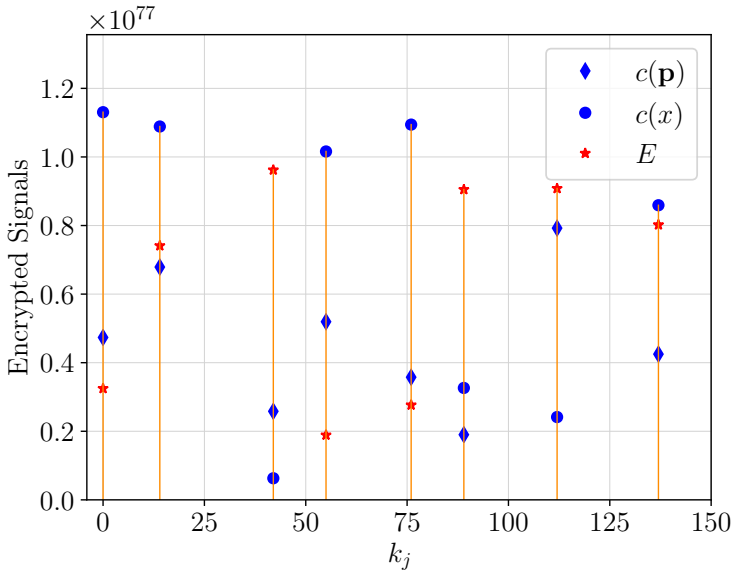

Fig. 6.5: The encrypted state measurements and controller profiles with the corresponding ECC shared key.

Fig. 6.5 demonstrates secure data transmission in MPCaaSS over unreliable network. The orange lines denote the sampling time instants at which the new ECC shared key is respectively generated in both cloud and edge layers, and thereafter the transmitted signals including controller profiles and state measurements are encrypted. Note that the sampling time instants are randomly generated to simulate the successful requests from the edge layer. It can be observed that the data transmission is well secured via the randomly-changing ECC shared key and AES-256 symmetric encryption. It is also worth noting that all the data shown in Fig. 6.5 are smaller than $2^{256} - 1 \approx 1.1579 \times 10^{77}$, which indicates that all the data packets are effectively encoded as 256-bit binary values. This fact verifies effectiveness of the designed packet transmission protocol. In addition, due to the verification process of AES in Algorithm 6.1, any unauthorized data modification by eavesdroppers and cyber attacks (e.g., deception attack and replay attack) by malicious adversaries can be detected by the receiver who has the only valid ECC shared key. Finally, we can conclude that the security issues of cloud-based control can be well addressed by the proposed MPCaaSS framework.

6.7 Conclusion

In this chapter, we have proposed an MPCaaSS framework for CPSs modeled by constrained linear time-invariant systems with external disturbance. In order to taking advantage of the cloud-edge computing, the proposed framework has used a double-layer controller architecture consisting of a cloud-side controller and an edge-side controller. Thanks to this unique controller design, the efficient real-time control performance and data transmission have been achieved. In addition, an encoding scheme and an ECC-based encryption scheme have been incorporated into the proposed framework in order to realize the secure data transmission. Moreover, we have derived several sufficient conditions for guaranteeing the recursive feasibility of the proposed MPC optimization problem and the robust stability of the closed-loop system. Finally, we have implemented the proposed framework to a CPS-based quadrotor attitude control system, which demonstrated the effectiveness of the proposed method. Future studies will be focused on extending this framework to distributed CPSs, which incorporates the network-enabled collaboration between multiple edge layers in order to fulfill more complex control tasks.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

In this thesis, several MPC based controller design problems have been studied for CPSs in the presence of cyber threats and resource constraints. Two fundamental problems, namely, the resource-aware control problem and secure control problem, are investigated and addressed with effective and efficient MPC based solutions.

Chapter 2 has been concerned with the resource-aware control problem for CPSs modeled by nonlinear systems with additive disturbances. An integral-type ET-MPC scheme was proposed, where an integral-type ETM is introduced to avoid unnecessary communication and a novel less conservative robustness constraint is proposed to handle the additive disturbance. It is shown that the feasibility of the MPC algorithm and the closed-loop stability is subject to several sufficient conditions.

In **Chapter 3**, the secure control problem has been investigated for CPSs modeled by linear systems subject to DoS attacks. A secure MPC algorithm has been designed using a novel positively invariant set and a dual-mode control scheme. It is shown that the closed-loop system is exponentially stable under the conditions relying on the duration of DoS attacks and the MPC parameters such as the prediction horizon. Besides, the maximum allowable duration of the DoS attacker has been also obtained through the novel positive invariance concept.

In **Chapter 4** and **5**, the secure and resource-aware control problems have been simultaneously studied for nonlinear CPSs in the presence of cyber attacks and additive disturbances. **Chapter 4** has presented an event-triggered robust NMPC framework in order to achieve the secure and resource-aware control objectives. In the pro-

posed framework, an efficient event-triggering condition is introduced to achieve better resource-awareness, an effective packet transmission strategy is used to deal with DoS attacks, and a novel robustness constraint is designed to handle additive disturbances. The recursive feasibility and the closed-loop stability have been guaranteed under some established sufficient conditions. **Chapter 5** has proposed a self-triggered min-max MPC framework for CPSs modeled by nonlinear systems in the presence of cyber attacks and uncertainties. A new min-max MPC scheme, parameterized by a novel control sequence in order to tackle DoS attacks, has been used to optimize the control performance over the worst case of all possible realizations of uncertainty and deception attack realizations. It is shown that the closed loop system is ISpS under the proposed MPC strategy.

In **Chapter 6**, the secure control problem has been investigated for CPSs assisted with the cloud-edge computing architecture. An MPC as a secure service framework has been proposed for CPSs modeled by constrained LTI systems subject to additive disturbances. In this framework, a double-layer controller architecture is developed by taking advantage of Gaussian radial functions; an encoding scheme and ECC-based encryption scheme are designed and integrated into the proposed MPC framework for achieving secure data transmission. It is proved that the proposed MPC algorithm is recursively feasible under sufficient conditions and the closed-loop system is robustly stable under the conditions that the MPC algorithm is recursively feasible.

7.2 Future Work

Since CPS-based resource-aware and secure control system design is an emerging and vibrant research topic, there are a lot of interesting and challenging topics worth studying in the future. In the following, we briefly discuss three potential future research directions derived from this dissertation.

- **Distributed MPC for cooperative resource-aware and secure control of CPSs.** The cooperative control of multi-agent systems has already received enormous research efforts during the last two decades. Due to the inherent distributed nature of CPSs, the cooperative control of CPSs is more appealing than the non-cooperative control used in this dissertation in order to complete cooperative control tasks. Since the multiple physical components (e.g., the controllers, actuators, and sensors) in CPSs can easily interact with each other,

the cooperative control of CPSs attracts more and more research attention in recent years, however, with much fewer efforts concentrated on achieving the resource-aware and secure control objectives. The original resource-aware and secure control objectives as we used in the previous chapters should be adapted to a cooperative setting since the communication can also occurs between the controllers. To obtain such control objectives, the distributed model predictive control (DMPC) can be used as an effective tool for cooperative control of CPSs. The biggest challenge in designing an effective DMPC framework may lie in the more complex scheduling design and attack-compensation design.

- **Learning-based MPC for resource-aware and secure control of CPSs.** The MPC algorithms developed in this dissertation need to repeatedly solve constrained optimization problems online, which could be however prohibitive for CPSs especially with less computational and communicational resources. On the one hand, the proposed MPC optimization problems cannot be solved fast enough in the low cost computing device, while the real time performance is required to maintain the control performance. On the other hand, the frequent transmission of the control signals and sensor measurements may cause the network congestion that can destabilize the controlled physical plant. Learning-based MPC is currently gaining increasingly research interests due to its powerful capability of directly searching for the optimal MPC control policy. In order to deal with these issues, we can use the learning-based MPC to transform the original MPC control law into an efficient control law that can be easily evaluated online. The main issue of applying learning-based MPC is how to consider the secure control objective. In addition, the study of the stability and constraint satisfaction of the learning-based MPC under resource constraints and cyber threats is also an interesting yet challenging topic.

- **Efficient and secure optimization methods for implementing MPC for CPSs.** Since the developed MPC algorithms use the general-purpose solvers, the secure and resource-aware control objectives are only guaranteed in the level of algorithm design. Moreover, the existing solvers are not aware of any possible cyber threats from the inside of the computing devices, which could possibly lead to dramatic control performance degradation or even cause the system failure. Therefore, an MPC optimization solver specifically designed for achieving security is particularly valuable.

Bibliography

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *Proceedings of the 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*. Orlando, USA: IEEE, May 2008, pp. 363–369.

[2] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proceedings of the 47th Design Automation Conference*. Anaheim, USA: ACM, Jun. 2010, pp. 731–736.

[3] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," *HotSec*, vol. 5, p. 15, 2008.

[4] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2012.

[5] U. GAO, "Critical infrastructure protection: Challenges and efforts to secure control systems," *U.S. GAO*, 2004.

[6] D. Powner and K. Rhodes, "Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain," 2007.

[7] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 53–66, 2015.

[8] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the internet-of-things," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38–60, 2017.

[9] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proceedings of the 28th International Conference*

on Distributed Computing Systems. Beijing, China: IEEE, Jun. 2008, pp. 495–500.

[10] V. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2017.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[12] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 3, no. 50, pp. 48–53, 2013.

[13] D. Goodin, "First known hacker-caused power outage signals troubling escalation," *Ars Technica*, vol. 4, 2016.

[14] T. Gommans and W. Heemels, "Resource-aware MPC for constrained nonlinear systems: A self-triggered control approach," *Systems & Control Letters*, vol. 79, pp. 59–67, 2015.

[15] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[16] S. J. Qin and T. A. Badgwell, "A survey of industrial model predictive control technology," *Control Engineering Practice*, vol. 11, no. 7, pp. 733–764, 2003.

[17] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Proceedings of the 2010 IEEE PES General Meeting*. Minneapolis, USA: IEEE, Jul. 2010, pp. 1–7.

[18] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in *Proceedings of the 2nd International Symposium on Resilient Control Systems*. Idaho Falls, USA: IEEE, Aug. 2009, pp. 31–35.

[19] M. A. Bishop, *Computer Security: Art and Science*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[20] R. Shirey, "Internet security glossary, version 2," RFC 4949, August, Tech. Rep., 2007.

[21] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," in *Proceedings of the 2nd Conference on Human System Interactions*. Catania, Italy: IEEE, 2009, pp. 632–636.

[22] L. Chisci, J. A. Rossiter, and G. Zappa, "Systems with persistent disturbances: predictive control with restricted constraints," *Automatica*, vol. 37, no. 7, pp. 1019–1028, 2001.

[23] D. Hrovat, S. Di Cairano, H. E. Tseng, and I. V. Kolmanovsky, "The development of model predictive control in automotive industry: A survey," in *Proceedings of the 2012 IEEE International Conference on Control Applications*. Dubrovnik, Croatia: IEEE, Oct. 2012, pp. 295–302.

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

[25] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[26] K. J. Åström and B. Bernhardsson, "Comparison of Riemann and Lebesgue sampling for first order stochastic systems," in *Proceedings of the 41st IEEE Conference on Decision and Control (CDC)*. Las Vegas, USA: IEEE, Dec. 2002, pp. 2011–2016.

[27] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1680–1685, 2007.

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

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

[30] J. Lunze and D. Lehmann, "A state-feedback approach to event-based control," *Automatica*, vol. 46, no. 1, pp. 211–215, 2010.

[31] M. Donkers and W. Heemels, "Output-based event-triggered control with guaranteed $\mathcal{L}_\infty$-gain and improved and decentralized event-triggering," *IEEE Transactions on Automatic Control*, vol. 57, no. 6, pp. 1362–1376, 2012.

[32] W. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proceedings of the 51st IEEE Conference on Decision and Control (CDC)*. Maui, Hawaii: IEEE, Dec. 2012, pp. 3270–3285.

[33] W. Heemels and M. Donkers, "Model-based periodic event-triggered control for linear systems," *Automatica*, vol. 49, no. 3, pp. 698–711, 2013.

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

[35] S. Mousavi and H. Marquez, "Integral-based event triggering controller design for stochastic LTI systems via convex optimisation," *International Journal of Control*, vol. 89, no. 7, pp. 1416–1427, 2016.

[36] H. Yu and F. Hao, "Input-to-state stability of integral-based event-triggered control for linear plants," *Automatica*, vol. 85, pp. 248–255, 2017.

[37] W. Hu, L. Liu, and G. Feng, "Consensus of linear multi-agent systems by distributed event-triggered strategy," *IEEE Transactions on Cybernetics*, vol. 46, no. 1, pp. 148–157, 2015.

[38] D. Zhang, Q.-L. Han, and X.-M. Zhang, "Network-based modeling and proportional-integral control for direct-drive-wheel systems in wireless network environments," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2462–2474, 2019.

[39] D. Zhang, Q.-L. Han, and X. Jia, "Network-based output tracking control for T–S fuzzy systems using an event-triggered communication scheme," *Fuzzy Sets and Systems*, vol. 273, pp. 26–48, 2015.

[40] C. K. Ahn, P. Shi, and L. Wu, "Receding horizon stabilization and disturbance attenuation for neural networks with time-varying delay," *IEEE Transactions on Cybernetics*, vol. 45, no. 12, pp. 2680–2692, 2014.

[41] P. Varutti, B. Kern, T. Faulwasser, and R. Findeisen, "Event-based model predictive control for networked control systems," in *Proceedings of the 48th IEEE Conference on Decision and Control and held jointly with the 28th Chinese Control Conference (CDC/CCC)*. Shanghai, China: IEEE, Dec. 2009, pp. 567–572.

[42] A. Eqtami, D. V. Dimarogonas, and K. J. Kyriakopoulos, "Event-triggered strategies for decentralized model predictive controllers," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 10 068–10 073, 2011.

[43] H. Li and Y. Shi, "Event-triggered robust model predictive control of continuous-time nonlinear systems," *Automatica*, vol. 50, no. 5, pp. 1507–1513, 2014.

[44] A. Eqtami, D. V. Dimarogonas, and K. J. Kyriakopoulos, "Novel event-triggered strategies for model predictive controllers," in *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC/ECC)*. Orlando, USA: IEEE, Dec. 2011, pp. 3392–3397.

[45] D. Lehmann, E. Henriksson, and K. H. Johansson, "Event-triggered model predictive control of discrete-time linear systems subject to disturbances," in *Proceedings of the 2013 European Control Conference (ECC)*. Zurich, Switzerland: IEEE, Jul. 2013, pp. 1156–1161.

[46] C. Liu, J. Gao, H. Li, and D. Xu, "Aperiodic robust model predictive control for constrained continuous-time nonlinear systems: An event-triggered approach," *IEEE Transactions on Cybernetics*, vol. 48, no. 5, pp. 1397–1405, 2017.

[47] K. Hashimoto, S. Adachi, and D. V. Dimarogonas, "Event-triggered intermittent sampling for nonlinear model predictive control," *Automatica*, vol. 81, pp. 148–155, 2017.

[48] Q. Sun, J. Chen, and Y. Shi, "Integral-type event-triggered model predictive control of nonlinear systems with additive disturbance," *IEEE Transactions on Cybernetics*, 2020.

[49] A. Eqtami, D. V. Dimarogonas, and K. J. Kyriakopoulos, "Event-based model predictive control for the cooperation of distributed agents," in *Proceedings of the 2012 American Control Conference (ACC)*. Montréal, Canada: IEEE, Jun. 2012, pp. 6473–6478.

[50] H. Li, Y. Shi, W. Yan, and R. Cui, "Periodic event-triggered distributed receding horizon control of dynamically decoupled linear systems," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 10 066–10 071, 2014.

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

[52] H. Li, Y. Shi, and W. Yan, "On neighbor information utilization in distributed receding horizon control for consensus-seeking," *IEEE Transactions on Cybernetics*, vol. 46, no. 9, pp. 2019–2027, 2015.

[53] K. Hashimoto, S. Adachi, and D. V. Dimarogonas, "Self-triggered model predictive control for nonlinear input-affine dynamical systems via adaptive control samples selection," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 177–189, 2016.

[54] F. D. Brunner, W. Heemels, and F. Allgöwer, "Robust event-triggered MPC with guaranteed asymptotic bound and average sampling rate," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 5694–5709, 2017.

[55] C. Liu, H. Li, J. Gao, and D. Xu, "Robust self-triggered min–max model predictive control for discrete-time nonlinear systems," *Automatica*, vol. 89, pp. 333–339, 2018.

[56] H. Li, W. Yan, and Y. Shi, "Triggering and control codesign in self-triggered model predictive control of constrained systems: With guaranteed performance," *IEEE Transactions on Automatic Control*, vol. 63, no. 11, pp. 4008–4015, 2018.

[57] M. Wang, J. Sun, and J. Chen, "Stabilization of perturbed continuous-time systems using event-triggered model predictive control," *IEEE Transactions on Cybernetics*, 2020.

[58] ——, "Input-to-state stability of perturbed nonlinear systems with event-triggered receding horizon control scheme," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 8, pp. 6393–6403, 2019.

[59] Z. Sun, L. Dai, Y. Xia, and K. Liu, "Event-based model predictive tracking control of nonholonomic systems with coupled input constraint and bounded disturbances," *IEEE Transactions on Automatic Control*, vol. 63, no. 2, pp. 608–615, 2018.

[60] D. Bernardini and A. Bemporad, "Energy-aware robust model predictive control based on noisy wireless sensors," *Automatica*, vol. 48, no. 1, pp. 36–44, 2012.

[61] A. Ferrara, G. P. Incremona, and L. Magni, "Model-based event-triggered robust MPC/ISM," in *Proceedings of the 2014 European Control Conference (ECC)*. Strasbourg, France: IEEE, Jun. 2014, pp. 2931–2936.

[62] F. Berkel and S. Liu, "An event-triggered output-based model predictive control strategy," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 822–832, 2019.

[63] K. Hashimoto, S. Adachi, and D. V. Dimarogonas, "Distributed aperiodic model predictive control for multi-agent systems," *IET Control Theory & Applications*, vol. 9, no. 1, pp. 10–20, 2014.

[64] N. He and D. Shi, "Event-based robust sampled-data model predictive control: A non-monotonic lyapunov function approach," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 10, pp. 2555–2564, 2015.

[65] D. Groß and O. Stursberg, "A cooperative distributed MPC algorithm with event-based communication and parallel optimization," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 3, pp. 275–285, 2015.

[66] Y. Zou, X. Su, S. Li, Y. Niu, and D. Li, "Event-triggered distributed predictive control for asynchronous coordination of multi-agent systems," *Automatica*, vol. 99, pp. 92–98, 2019.

[67] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, "Roadmap to secure control systems in the energy sector," *Energetics Incorporated. Sponsored by the US Department of Energy and the US Department of Homeland Security*, 2006.

[68] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, and T. Hayat, "Recent advances on filtering and control for cyber-physical systems under security and resource constraints," *Journal of the Franklin Institute*, vol. 353, no. 11, pp. 2451–2466, 2016.

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

[70] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

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

[72] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2019.

[73] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2021.

[74] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: Impact and mitigation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, 2005.

[75] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proceedings of the 12th International Workshop on Hybrid Systems: Computation and Control*. San Francisco, USA: Springer, Apr. 2009, pp. 31–45.

[76] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proceedings of the 49th IEEE Conference on Decision and Control*. Atlanta, USA: IEEE, Dec. 2010, pp. 1096–1101.

[77] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[78] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models," in *Proceedings of the 2011 American Control Conference (ACC)*. San Francisco, USA: IEEE, Jun. 2011, pp. 643–648.

[79] D. E. Quevedo and D. Nesic, "Input-to-state stability of packetized predictive control over unreliable networks affected by packet-dropouts," *IEEE Transactions on Automatic Control*, vol. 56, no. 2, pp. 370–375, 2011.

[80] D. E. Quevedo, J. Ostergaard, and D. Nesic, "Packetized predictive control of stochastic systems over bit-rate limited channels with packet loss," *IEEE Transactions on Automatic Control*, vol. 56, no. 12, pp. 2854–2868, 2011.

[81] Z.-H. Pang, G. Liu, and Z. Dong, "Secure networked control systems under denial of service attacks," in *Proceedings of the 18th IFAC World Congress*. Milano, Italy: IFAC, Aug. 2011, pp. 8908–8913.

[82] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2434–2449, 2017.

[83] S. Feng and P. Tesi, "Networked control systems under denial-of-service: Co-located vs. remote architectures," *Systems & Control Letters*, vol. 108, pp. 40–47, 2017.

[84] ——, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[85] P. K. Mishra, D. Chatterjee, and D. E. Quevedo, "Resource efficient stochastic predictive control under packet dropouts," *IET Control Theory & Applications*, vol. 11, no. 11, pp. 1666–1673, 2017.

[86] B. Demirel, V. Gupta, D. E. Quevedo, and M. Johansson, "On the trade-off between communication and control cost in event-triggered dead-beat control," *IEEE Transactions on Automatic Control*, vol. 62, no. 6, pp. 2973–2980, 2017.

[87] P. K. Mishra, D. Chatterjee, and D. E. Quevedo, "Stabilizing stochastic predictive control under bernoulli dropouts," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1579–1590, 2018.

[88] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1813–1820, 2018.

[89] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1786–1794, 2016.

[90] Y.-C. Sun and G.-H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *International Journal of Robust and Nonlinear Control*, vol. 29, no. 14, pp. 4797–4811, 2019.

[91] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4920–4927, 2020.

[92] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC)*. Atlanta, Georgia USA: IEEE, Dec. 2010, pp. 5967–5972.

[93] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, 2015.

[94] ——, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[95] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334–1342, 2012.

[96] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *Proceedings of the 51st IEEE Conference on Decision and Control (CDC)*. Maui, USA: IEEE, Dec. 2012, pp. 3412–3417.

[97] ——, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[98] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.

[99] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 6058–6064, 2017.

[100] Y. Chen, S. Kar, and J. M. Moura, "Cyber-physical attacks with control objectives," *IEEE Transactions on Automatic Control*, vol. 63, no. 5, pp. 1418–1425, 2018.

[101] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, USA: IEEE, Oct. 2009, pp. 911–918.

[102] M. Zhu and S. Martínez, "On distributed constrained formation control in operator–vehicle adversarial networks," *Automatica*, vol. 49, no. 12, pp. 3571–3582, 2013.

[103] ——, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

[104] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2016.

[105] W. Fu, J. Qin, Y. Shi, W. X. Zheng, and Y. Kang, "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4868–4877, 2019.

[106] J. Wang, B. Ding, and J. Hu, "Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, pp. 760–767, 2021.

[107] C. De Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," *Systems & Control Letters*, vol. 96, pp. 124–131, 2016.

[108] H. S. Foroush and S. Martinez, "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, USA: IEEE, 2012, pp. 2551–2556.

[109] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 12, pp. 4271–4281, 2018.

[110] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy," *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3714–3721, 2020.

[111] A. Cetinkaya, K. Kikuchi, T. Hayakawa, and H. Ishii, "Randomized transmission protocols for protection against jamming attacks in multi-agent consensus," *Automatica*, vol. 117, p. 108960, 2020.

[112] S. Liu, S. Li, and B. Xu, "Event-triggered resilient control for cyber-physical system under denial-of-service attacks," *International Journal of Control*, vol. 93, no. 8, pp. 1907–1919, 2020.

[113] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies," *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3299–3304, 2015.

[114] S. J. Qin and T. A. Badgwell, "An overview of nonlinear model predictive control applications," *Nonlinear Model Predictive Control*, pp. 369–392, 2000.

[115] W.-J. Ma and V. Gupta, "Input-to-state stability of hybrid systems with receding horizon control in the presence of packet dropouts," *Automatica*, vol. 48, no. 8, pp. 1920–1923, 2012.

[116] Z.-H. Pang, G.-P. Liu, D. Zhou, and D. Sun, "Data-based predictive control for networked nonlinear systems with network-induced delay and packet dropout," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 2, pp. 1249–1257, 2016.

[117] D. M. de la Pena and P. D. Christofides, "Lyapunov-based model predictive control of nonlinear systems subject to data losses," *IEEE Transactions on Automatic Control*, vol. 53, no. 9, pp. 2076–2089, 2008.

[118] D. Ding, Z. Wang, G. Wei, and F. E. Alsaadi, "Event-based security control for discrete-time stochastic systems," *IET Control Theory & Applications*, vol. 10, no. 15, pp. 1808–1815, 2016.

[119] D. Ding, Z. Wang, D. W. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Transactions on Cybernetics*, vol. 47, no. 8, pp. 1936–1947, 2017.

[120] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC/ECC)*. Orlando, Florida: IEEE, Dec. 2011, pp. 4066–4071.

[121] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, 2015.

[122] A. Wächter and L. T. Biegler, "On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming," *Mathematical Programming*, vol. 106, no. 1, pp. 25–57, 2006.

[123] L. Chisci, A. Lombardi, and E. Mosca, "Dual-receding horizon control of constrained discrete time systems," *European Journal of Control*, vol. 2, no. 4, pp. 278–285, 1996.

[124] P. O. Scokaert, D. Q. Mayne, and J. B. Rawlings, "Suboptimal model predictive control (feasibility implies stability)," *IEEE Transactions on Automatic Control*, vol. 44, no. 3, pp. 648–654, 1999.

[125] H. Michalska and D. Q. Mayne, "Robust receding horizon control of constrained nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 38, no. 11, pp. 1623–1633, 1993.

[126] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[127] G. H. Golub and C. F. Van Loan, *Matrix Computations*. JHU press, 2012, vol. 3.

[128] M. Herceg, M. Kvasnica, C. Jones, and M. Morari, "Multi-Parametric Toolbox 3.0," in *Proceedings of the 2013 European control conference (ECC)*. Zürich, Switzerland: IEEE, Jul. 2013, pp. 502–510.

[129] H. J. Ferreau, C. Kirches, A. Potschka, H. G. Bock, and M. Diehl, "qpOASES: A parametric active-set algorithm for quadratic programming," *Mathematical Programming Computation*, vol. 6, no. 4, pp. 327–363, 2014.

[130] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[131] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

[132] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[133] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Transactions*, 2021.

[134] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, 2021.

[135] H. Li and Y. Shi, "Network-based predictive control for constrained nonlinear systems with two-channel packet dropouts," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 3, pp. 1574–1582, 2014.

[136] J. B. Rawlings and D. Q. Mayne, *Model Predictive Control: Theory and Design*. Nob Hill Pub., 2009.

[137] J. A. E. Andersson, J. Gillis, G. Horn, J. B. Rawlings, and M. Diehl, "CasADi – A software framework for nonlinear optimization and optimal control," *Mathematical Programming Computation*, vol. 11, no. 1, pp. 1–36, 2019.

[138] H. Li and Y. Shi, *Robust Receding Horizon Control for Networked and Distributed Nonlinear Systems*. Springer, 2017.

[139] F. D. Brunner, M. Heemels, and F. Allgöwer, "Robust self-triggered MPC for constrained linear systems: A tube-based approach," *Automatica*, vol. 72, pp. 73–83, 2016.

[140] D. Limón, T. Alamo, F. Salas, and E. F. Camacho, "Input to state stability of min–max MPC controllers for nonlinear systems with bounded uncertainties," *Automatica*, vol. 42, no. 5, pp. 797–803, 2006.

[141] Z. Ji and Q. Anwen, "The application of internet of things (IoT) in emergency management system in china," in *Proceedings of the 19th IEEE International Conference on Technologies for Homeland Security (HST)*. Waltham, USA: IEEE, Nov. 2010, pp. 139–142.

[142] H. Huang, X. Li, S. Liu, S. Hu, and Y. Sun, "Tribomotion: A self-powered triboelectric motion sensor in wearable internet of things for human activity recognition and energy harvesting," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4441–4453, 2018.

[143] K. Sasaki, N. Suzuki, S. Makido, and A. Nakao, "Vehicle control system coordinated between cloud and mobile edge computing," in *Proceedings of the 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. Tsukuba, Japan: IEEE, Nov. 2016, pp. 1122–1127.

[144] B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, "A survey of research on cloud robotics and automation," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 2, pp. 398–409, 2015.

[145] P. Wu, F. Xiao, H. Huang, C. Sha, and S. Yu, "Adaptive and extensible energy supply mechanism for uavs-aided wireless-powered Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9201–9213, 2020.

[146] Y. Xia, "From networked control systems to cloud control systems," in *Proceedings of the 31st Chinese Control Conference*. Hefei, China: IEEE, Jul. 2012, pp. 5878–5883.

[147] H. Wu, L. Lou, C.-C. Chen, S. Hirche, and K. Kuhnlenz, "Cloud-based networked visual servo control," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 2, pp. 554–566, 2012.

[148] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[149] A. Vick, V. Vonásek, R. Pěnička, and J. Krüger, "Robot control as a service—towards cloud-based motion planning and control for industrial robots," in *Proceedings of the 10th International Workshop on Robot Motion and Control (RoMoCo)*. Poznan, Poland: IEEE, Jul. 2015, pp. 33–39.

[150] A. E. Abdelaal, T. Hegazy, and M. Hefeeda, "Event-based control as a cloud service," in *Proceedings of the 2017 American Control Conference (ACC)*. Seattle, USA: IEEE, May 2017, pp. 1017–1023.

[151] H. He, S. Kamburugamuve, G. C. Fox, and W. Zhao, "Cloud based real-time multi-robot collision avoidance for swarm robotics," *International Journal of Grid and Distributed Computing*, vol. 9, no. 6, pp. 339–358, 2016.

[152] G. Andonovski, S. Blažič, P. Angelov, and I. Škrjanc, "Analysis of adaptation law of the robust evolving cloud-based controller," in *Proceedings of the 2015 IEEE International Conference on Evolving and Adaptive Intelligent Systems (EAIS)*. Douai, France: IEEE, Dec. 2015, pp. 1–7.

[153] E. Biyik, J. D. Brooks, H. Sehgal, J. Shah, and S. Gency, "Cloud-based model predictive building thermostatic controls of commercial buildings: Algorithm and implementation," in *Proceedings of the 2015 American Control Conference (ACC)*. Chicago, USA: IEEE, Jul. 2015, pp. 1683–1688.

[154] A. Vick, J. Guhl, and J. Krüger, "Model predictive control as a service—concept and architecture for use in cloud-based robot control," in *Proceedings of the 21st International Conference on Methods and Models in Automation and Robotics (MMAR)*. Miedzyzdroje, Poland: IEEE, Sep. 2016, pp. 607–612.

[155] H. Yang, S. Ju, J. Zhang, and H. Yuan, "Model predictive control for cloud-integrated networked multiagent systems under bandwidth allocation," *Information Sciences*, vol. 500, pp. 156–172, 2019.

[156] P. Skarin, J. Eker, and K.-E. Årzén, "Cloud-based model predictive control with variable horizon," in *Proceedings of the 21st IFAC World Congress*. Berlin, Germany: IFAC, Jul. 2020.

[157] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta *et al.*, "Imperfect forward secrecy: How Diffie-Hellman fails in practice," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. New York, USA: ACM, Oct. 2015, pp. 5–17.

[158] D. Q. Mayne, M. M. Seron, and S. Raković, "Robust model predictive control of constrained linear systems with bounded disturbances," *Automatica*, vol. 41, no. 2, pp. 219–224, 2005.

[159] P. O. Scokaert and J. B. Rawlings, "Constrained linear quadratic regulation," *IEEE Transactions on Automatic Control*, vol. 43, no. 8, pp. 1163–1169, 1998.

[160] "Secp256k1 - bitcoin wiki," accessed on January 11, 2021. [Online]. Available: https://en.bitcoin.it/wiki/Secp256k1

[161] H. Eijs, "Pycryptodome: Cryptographic library for python," accessed on January 11, 2021. [Online]. Available: https://pypi.org/project/pycryptodomex/

Appendix A

Publications

- Refereed Journal Papers

  1. **Q. Sun** and Y. Shi (2021). "Model predictive control as a secure service for cyber-physical systems: A cloud-edge framework," *IEEE Internet of Things Journal*, published online on June 2021, doi: 10.1109/JIOT.2021.3091981.
  2. **Q. Sun**, J. Chen and Y. Shi (2021). "Event-triggered robust MPC of nonlinear cyber-physical systems against DoS attacks," *SCIENCE CHINA Information Sciences*, accepted, June 2021.
  3. **Q. Sun**, K. Zhang and Y. Shi (2020). "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4920–4927, July 2020, doi: 10.1109/TII.2019.2963294.
  4. **Q. Sun**, J. Chen and Y. Shi (2020). "Integral-type event-triggered model predictive control of nonlinear systems with additive disturbance," *IEEE Transactions on Cybernetics*, published online on January 2020, doi: 10.1109/TCYB.2019.2963141.
  5. K. Zhang, **Q. Sun** and Y. Shi (2021). "Trajectory tracking control of autonomous ground vehicles using adaptive learning MPC," *IEEE Transactions on Neural Networks and Learning Systems*, published online on January 2021, doi: 10.1109/TNNLS.2020.3048305.
  6. H. Wei, **Q. Sun**, J. Chen and Y. Shi (2021). "Distributed robust model predictive platooning control for heterogeneous autonomous surface ve-

hicles," *Control Engineering Practice*, vol. 107, pp. 104655, February 2021, doi: 10.1016/j.conengprac.2020.104655.

7. J. Chen, **Q. Sun**, and Y. Shi (2018). "Stochastic self-triggered MPC for linear constrained systems under additive uncertainty and chance constraints," *Information Sciences*, vol. 459, pp. 198–210, August 2018, doi: 10.1016/j.ins.2018.05.021.

- Journal Papers Under Preparation

1. **Q. Sun** and Y. Shi (2021). "Self-triggered MPC of cyber-physical systems under attacks: A min-max optimization approach," to be submitted.