https://dx.doi.org/10.1016/j.ins.2022.08.093

Dynamic Event-Triggered Security Control for Networked Control Systems with Cyber-Attacks: A Model Predictive Control Approach

Bin Li[a], Xinglian Zhou[a], Zhaoke Ning[a,c,*], Xiaoyi Guan[b], Ka-Fai Cedric Yiu[b]

[a]*School of Aeronautics and Astronautics, Sichuan University, Chengdu, 610207, China*
[b]*Department of Applied Mathematics, The Hong Kong Polytechnic University, Hong Kong, China*
[c]*College of Information Engineering, Henan University of Science and Technology, Luoyang, 471023, China*

Abstract

In this study, a dynamic event-triggered security control problem for networked control systems was subject to deception attacks and packet dropouts. First, a combined cyber-attack model is proposed, which utilises two sets of independent stochastic sequences to reflect randomly occurring cyber-attacks. Subsequently, a dynamic event-triggered protocol is constructed to relieve the restricted bandwidth pressure by reducing the data transmission of the communication channel from the plant to the controller. With the consideration of randomly occurring deception attacks, packet dropouts, and dynamic event-triggered protocols, an online model predictive control algorithm is established to ensure the stochastic stability of the closed-loop model with expected H_2/H_∞ performance. Finally, two examples are simulated to interpret the validity and effectiveness of the proposed design strategy.

Keywords: Dynamic event-triggered protocol, security control, model predictive control, deception attacks, packet dropouts.

1. Introduction

Cyber-physical systems (CPSs) have generated an army of studies in the last few years with the development of network technology and communication requirements for large-scale plant equipment. From the attackers' perspective, scholars are interested in optimizing the attack strategy to achieve greater damage to CPSs with limited energy [38]. From the perspective of defenders, some scholars have been interested in the detection of attacks. In [7], a set-based attack detection mechanism and remedial measures were designed to provide timely alerts for attack occurrence. Other researchers have studied the networked security control from the perspective of protectors, aiming to design a control strategy to reduce the impact of network attacks on system performances. As one of the most famous CPSs, networked control systems (NCSs) play an increasingly important role in many fields, such as manufacturing plants, aircrafts remote operations, and power systems [11, 16, 18, 31]. The NCSs use networks as the communication channel, which connects the sensors, actuators, and controllers of the plant. Owing to the broadcast characteristics of communication networks, NCSs are vulnerable to various attacks and interference. Attackers can break into the system in a highly concealed manner to realise damage to the control system or theft of information. Common network problems include time delay, packet disordering, quantization, and cyber-attacks [12, 25, 35], among which cyber-attacks mainly include deception [4, 21, 32], replay [3, 44], and denial-of-service (DoS) attacks [1, 30, 33, 38], which may lead to poor system performance and even result in system instability.

Network attacks are usually carried out in a random manner and Bernoulli and Markov processes are proposed to describe random network attacks [2, 45]. The authors in [37] studied the design of a proportional-integral controller for the height adjustment task of direct-drive-wheel systems in an environment with delay and random packet dropouts. In [41], a logic processor was introduced to obtain the duration information of a DoS attack, which was fully utilised to derive the elastic state feedback controller and stability criteria. With the growth of network scale

*Corresponding author: Zhaoke Ning. E-mail: zhaokening2018@163.com

and the amount of distributed information being processed, the data during network transmission easily suffer from different types of attacks; thus, it is increasingly necessary to consider the combination of network problems [15, 39]. Therefore, this study investigates the security control issue for NCSs with random packet dropouts and deception attacks simultaneously.

As a matter of fact, the data transmission capacity of practical network should not be ignored. The bandwidth resources of NCSs are limited by the complex environment, communication materials, and systems cost; therefore, the efficient utilisation of network resources has become a research hotspot. Because not all sampled data are valuable, it will cause problems such as low efficiency and waste of communication resources if all sampled data are transmitted through network channels. As one of the most useful strategies, the event-triggered control has been widely applied to save network resources. The difficulty of the event-triggered control lies in balancing control performance and satisfactory network resource utilisation efficiency. According to the types of triggering thresholds, the event-triggered protocol can be classified as the static event-triggered protocol (SETP) [13, 40] and the dynamic event-triggered protocol (DETP) [9, 10]. Compared with the former, the triggering threshold of DETP is adjusted with internal dynamic variables or the bandwidth status, which can further reduce the communication pressure and has received much research attention recently. For instance, the authors in [22] discussed a fault detection design approach for a nonlinear stochastic model that interfered with transmission delays and packet dropouts. The authors in [8] discussed the collaborative design of the dynamic event-triggered scheduling and formation control for vehicles with limited communication resources, as well as the formation control performance and communication efficiency. In [6], the authors provide an overview of the motivations, techniques and challenges of dynamic event-triggered distributed cooperative control problems. In [29], a adaptive fuzzy event-triggered controller was provided to address the consensus control problem of high-order nonlinear systems and to reduce the number of data transmissions. In [42], a PID controller design strategy was provided to guarantee the stability of linear systems subjected to cyberattacks under DETP. In addition the network security control issue was researched in [14] for T-S fuzzy systems against deception attacks and DoS attacks, where the DETP was applied to reduce the communication usage.

Model predictive control (MPC), a widely accepted control method, can solve optimization control problems with constraints. They have been broadly applied to contemporary industrial control systems [19, 20, 27]. The main idea of MPC is to repeatedly solve rolling optimization problems and take the first variable the control sequences as the current control input. Networked MPC inherits the advantages of NCSs and MPC; however, the introduction of network communication also results in communication problems and limited bandwidth resources. For instance, scholars have studied the design of fuzzy predictive control for nonlinear systems with packet dropouts that can ensure the stochastic stability of a closed-loop system [43]. The authors in [17] designed an observer to estimate the actuator fault signal of a plant, and applied an event-triggered model predictive tolerant controller to compensate the estimated fault signal. In [36], an output-based predictive control strategy was investigated for NCSs under SETP, which can save restricted network resources and achieve the anticipated control performance. A resilient MPC framework was presented to compensate for the adverse influence of DoS attacks and guarantee the exponential stability of the CPSs [26]. In [28], the security control problem was studied for linear parameter-varying systems subject to random deception attacks, and the sufficient conditions for the mean-square quadratic boundedness were deduced to ensure the stability of the system. After extensive research, it was found that there were not yet detailed findings on MPC for NCSs with combined network attacks and DETP. Compared with the traditional MPC strategy, the dynamic event-triggered MPC strategy can effectively reduce the data transmission of the feedback channel, which motivated this study.

The major challenge of this study is to design a dynamic event-triggered model predictive controller, that can guarantee the stochastic stability of a system subject to combined network attacks. The main contributions of this study are as follows.

- A dynamic event-triggered MPC strategy is developed to obtain the desired control objective, as well as to effectively save restricted network bandwidth resources.
- Two independent stochastic sequences are offered to represent the occurrence of hybrid cyber-attacks.
- A novel online-solved MPC optimization problem is proposed to guarantee the stochastic stability of a system subject to randomly occurring deception attacks and packet dropouts simultaneously.

2. Problem formulation

2.1. Model description

Consider a cyber-physical system that is characterized by the following linear discrete-time model:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + B_d d(k), \\ z(k) = Cx(k) + Du(k), \end{cases} \tag{1}$$

where A, B, B_d, C and D are the known parameters of the plant, $x(k) \in \mathbb{R}^{n_x}$ represents the state vector, $z(k) \in \mathbb{R}^{n_z}$ stands for the controlled output, $u(k) \in \mathbb{R}^{n_u}$ denotes the control input, and $d(k) \in \mathbb{R}^{n_d}$ is the bounded disturbance term, which is supposed to satisfy

$$\sum_{n=0}^{\infty} d^T(k)d(k) \leq \bar{d}, \tag{2}$$

where $\bar{d} > 0$ is a given constant.

We then consider the following MPC-based state feedback controller to achieve the expected control performance:

$$u(k+n|k) = F(k)x(k+n|k), \tag{3}$$

where $x(k+n|k)$ and $u(k+n|k)$ are the n-th step predictions for the state vector and control input, respectively. $F(k)$ is the unknown feedback gain that can be obtained.

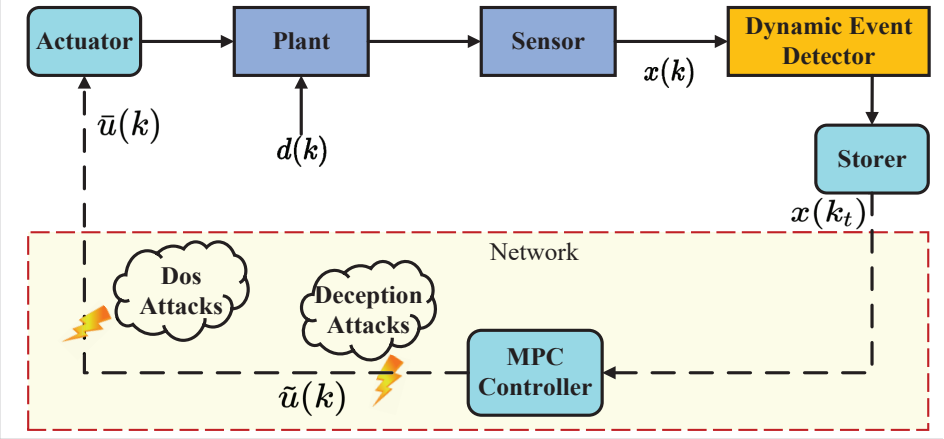


Figure 1: The framework of dynamic event-triggered model predictive security control.

2.2. Dynamic event-triggered protocol

As shown in Fig.1, the signal transmission capacity of a realistic network cannot ignored. In certain cases, restricted bandwidth resources are not sufficient for massive data transmissions. Therefore, reducing the communication of unnecessary data is worth investigating. The event-triggered data-transmission protocol is widely accepted as an effective strategy for saving limited network resources.

For convenience, we refer the triggering time instants as $\{k_1, k_2, k_3, ..., k_t, ...\}$. Subsequently, a predefined dynamic event-triggered function $f(\phi, \zeta)$ is constructed in the following form:

$$f(\varrho, \varsigma) \triangleq \varrho(k)^T \varrho(k) - \frac{1}{\delta}\varsigma(k) - \varepsilon x(k)^T x(k), \tag{4}$$

where ε and δ are specified positive scalars; $\varrho(k)$ represents the difference in system state value at the current time k and the latest triggering k_t, that is $\varrho(k) \triangleq x(k_t) - x(k), k \in [k_t, k_{t+1})$. $\varsigma(k)$ is an internal dynamic variable that is defined as follows:

$$\begin{cases} \varsigma(k+1) = \beta\varsigma(k) + \varepsilon x(k)^T x(k) - \varrho(k)^T \varrho(k), \\ \varsigma(0) = \bar{\varsigma}, \end{cases} \tag{5}$$

where $\bar{\varsigma} > 0$ is the initial value of $\varsigma(k)$, and $\beta \in (0, 1)$ is constant scalar. Event-triggered instants can then be obtained using the following function:

$$k_{t+1} = \inf \{k \in \mathbb{N} \mid k > k_t, f(\varrho, \varsigma) > 0\}. \tag{6}$$

Based on the event-triggered conditions (4)-(6), we can determine that the sampled data will not be triggered when the following inequality is satisfied:

$$\varrho(k)^T \varrho(k) - \frac{1}{\delta}\varsigma(k) - \varepsilon x(k)^T x(k) \leq 0.$$

Combined with (4)-(5), under the conditions of $\theta\delta \geq 1$ and $\bar{\zeta} \geq 0$, we can obtain the following formulation:

$$\varsigma_{k+1} \geq \left(\theta - \frac{1}{\delta}\right)\varsigma_k \geq \ldots \geq \left(\theta - \frac{1}{\delta^{k+1}}\right)\varsigma_0 \geq 0.$$

Therefore, the dynamic event-triggered conditions (4)-(6) will be more effective in saving network resources than the static event-triggered mechanism (10)-(12) in [5].

Remark 1. It is noteworthy that the threshold in the dynamic event-triggered function (4) can be adjusted by the dynamic function $\varsigma(k)$, which is more effective in reducing network communication resources than the traditional fixed threshold method. If we set $\delta \to \infty$, the variable $\frac{1}{\delta}\varsigma(k)$ tends to 0. The proposed DETP is similar to the traditional method with a fixed threshold [5].

In this study, a dynamic event-triggered protocol was designed to reduce the information exchanged between the sensor and the controller. The storer can only retransmit the latest state information to the controller at trigger instants. The controllers only have state information of the latest triggering moment between the two triggering moments.

The model predictive controller under the dynamic event-triggered communication protocol can be formulated as follows:

$$u(k+n|k) = F(k)x(k_t + n|k_t) = F(k)\left[x(k+n|k) + \varrho(k+n|k)\right], \quad k \in [k_t, k_{t+1}). \tag{7}$$

2.3. Cyber-attacks model

Physical CPSs can bring great convenience in realising wireless data communication via networks, but they can also result in network-induced security problems. In this study, we assume that the network link from the controller to the actuator is vulnerable to cyber-attacks, which consist of DoS attacks and deception attacks.

First, when the communication network from the controller to the actuator suffers from malicious deception attacks, a malicious signal is transmitted to the actuator instead of the real control signal. Obviously, the deception attack behaviour can be easily discovered and detected if the a malicious attacker keeps sending deception signals. Otherwise, a continuous deception attack consumes more energy than an intermittent attack. Therefore, we assume that the deception signals attack the control system randomly, and the controller output can be rewritten as follows:

$$\tilde{u}(k) = u(k) + \mu(k)\zeta(k), \tag{8}$$

where $\zeta(k)$ represents the malicious deception variable launched by adversaries, which can be constructed as:

$$\zeta(k) = -u(k) + \upsilon(k),$$

where $\mu(k)$ is an independently distributed Bernoulli sequence with a value of 0 or 1. $\mu(k) = 1$ indicates that the network control system is attacked by deception signals, and $\mu(k) = 0$ signifies no deception information. $\bar{\mu}$ represents the probability of deception attacks; that is,

$$\begin{cases} \text{Prob}\{\mu(k) = 1\} = \bar{\mu}, \\ \text{Prob}\{\mu(k) = 0\} = 1 - \bar{\mu}, \end{cases} \tag{9}$$

where $\bar{\mu}$ represents the probability of deception attacks, and we assume that $\sum_{k=0}^{\infty} \upsilon^T(k)\upsilon(k) \leq \bar{\upsilon}$.

Remark 2. As shown in Fig.1, the data may be attacked on the communication link from the controller to the actuator. If the attacker can eavesdrop the information transmitted by the system, a smart attacker will send attack signals, which can be divided into two parts: one part $-u(k)$ is used to offset the control signal transmitted by the system, and the other part $\upsilon(k)$ is applied to deceive the actuator of the control system. Therefore, we assume that the $\zeta(k) = -u(k) + \upsilon(k)$ is reasonable. In addition, the attacker's energy is limited; thus, it is feasible to assume that deception signals have upper bounds.

Moreover, denial of service attacks are another common type of cyber-attack behaviour. Malicious attackers generate a large number of interference signals and transmit them to the network channel, which may block the network channel and result in the dropout of useful data packets. For the same reason, this study provides a stochastic sequence with a known probability to describe the random occurrence of packet dropouts caused by DOS attacks [34]. Therefore, by considering the cyber-attacks model and proposed dynamic event-based MPC protocol, the realistic signals received by the actuator of the plant are as follows:

$$\begin{aligned} \overline{u}(k+n|k) &= (1-\theta(k))\left[(1-\mu(k))\,u(k+n|k) + \mu(k)\upsilon(k+n|k)\right] \\ &= (1-\theta(k))\,(1-\mu(k))\,F\left[x(k+n|k) + \varrho(k+n|k)\right] + (1-\theta(k))\,\mu(k)\upsilon(k+n|k), \end{aligned} \tag{10}$$

where $\theta(k)$ is a stochastic variable with value of 0 or 1, i.e.

$$\begin{cases} \text{Prob}\{\theta(k) = 1\} = \overline{\theta}, \\ \text{Prob}\{\theta(k) = 0\} = 1 - \overline{\theta}, \end{cases}$$

where $\overline{\theta}$ is a given scalar.

Substitute Eq.(10) into Eq.(1), we can establish a closed-loop predictive control system, as described below:

$$\begin{aligned} x(k+n+1|k) = &\left[A + B\,(1-\theta(k))\,(1-\mu(k))\,F(k)\right] x(k+n|k) + B\,(1-\theta(k))\,(1-\mu(k)) \\ &\times F(k)\varrho(k+n|k) + B\,(1-\theta(k))\,\mu(k)\upsilon(k+n|k) + B_d d(k+n|k), \\ z(k+n|k) = &\left[C + D\,(1-\theta(k))\,(1-\mu(k))\,F(k)\right] x(k+n|k) + D\,(1-\theta(k)) \times (1-\mu(k)) \\ &\times F(k)\varrho(k+n|k) + B\,(1-\theta(k))\,\mu(k)\upsilon(k+n|k). \end{aligned} \tag{11}$$

Then, we define $\eta(k+n|k) = \begin{bmatrix} d^T(k+n|k) & \upsilon^T(k+n|k) \end{bmatrix}^T$, and this article explores the design of a dynamic event-triggered model prediction controller (10) for NCSs interfered with cyber-attacks, which satisfies the following:

- The closed-loop predictive control system (11) has stochastic stability for all $\eta(k+n|k) = 0$.
- H_∞ performance: For a given scalar $\alpha > 0$ and $\eta(k+n|k) \neq 0$, the controlled output satisfies the following inequality:

$$\sum_{\mathrm{n}=0}^{\infty} \| z(k+n|k)\|_2^{\,2} < \alpha^2 \sum_{n=0}^{\infty} \| \eta(k+n|\mathrm{k})\|_2^{\,2}. \tag{12}$$

- H_2 performance: The controlled output $z(k)$ established in model (11) with disturbance, randomly occurring deception attacks and packet dropouts satisfies the following:

$$\sum_{n=0}^{\infty} \| z(k+n \mid k)\|_2^{\,2} < \rho. \tag{13}$$

- The input is constrained as follows:

$$\| u(k+n|k) \|_2^2 \leq u_{\max}^2. \tag{14}$$

Furthermore, we can obtain the optimized feedback gain control parameter $F(k)$ and H_2 performance index ρ by solving the following problem:

$$\begin{aligned} &\min_{F(k)} \quad \rho \\ &\text{s.t.} \quad J(k) \leq \rho \end{aligned}$$

where the cost function $J(k)$ is considered as following form:

$$J(k) = \sum_{n=0}^{\infty} z^T(k+n|k) z(k+n|k).$$

Remark 3. Owing to the complex network communication environment, the actual bandwidth resource is limited and the existence of cyber-attacks will degrade the system performance and even lead to instability of the control system. Therefore, the main challenge of this study is to design a dynamic event-triggered model predictive controller to save limited network resources, ensure the stochastic stability of networked control systems subject to cyber-attacks, and achieve a balance between the control performance and communication efficiency.

3. Main results and proofs

This section provides a theorem to guarantee the stochastic stability of the established model (11) with the desired security control performance (12)-(13). The designed dynamic event-triggered MPC law can be determined by solving the linear matrix inequalities(LMIs) problem.

Theorem 1. For a given H_∞ performance index α and the dynamic event-triggered threshold parameters δ, β, and ε in (4)-(6), the established model (11) with bounded disturbances, random deception attacks and packet dropouts is of stochastic stability with expected H_2/H_∞ performance if there exist parameters $\rho > 0$, matrices $Q > 0$, $Y(k)$ and $\Phi(k)$ such that the following optimization problem is feasible:

$$\min \quad \rho \tag{15}$$

$$s.t. \begin{cases} \begin{bmatrix} \Xi & \Theta^T \\ \Theta & \Lambda \end{bmatrix} < 0, & (16a) \\ \begin{bmatrix} -1 & * & * & * \\ \alpha^2 \bar{d} & -\rho\alpha^2 \bar{d} & * & * \\ \alpha^2 \bar{v} & \mathbf{0}_{n_u \times 1} & -\rho\alpha^2 \bar{v} & * \\ x(k_t) & \mathbf{0}_{n_x \times 1} & \mathbf{0}_{n_x \times 1} & -Q \end{bmatrix} \leq 0, & (16b) \\ \begin{bmatrix} -Q & * \\ Y & -u_{\max}^2 I \end{bmatrix} \leq 0, & (16c) \end{cases}$$

where

$$\Xi = \begin{bmatrix} -Q + (\frac{\varepsilon}{\delta} + \varepsilon\pi)\Phi & * & * & * & * \\ \mathbf{0}_{n_d \times n_x} & -\alpha^2\rho I & * & * & * \\ \mathbf{0}_{n_x \times n_x} & \mathbf{0}_{n_x \times n_d} & \left(-\frac{1}{\delta} - \pi\right)\Phi & * & * \\ \mathbf{0}_{n_u \times n_x} & \mathbf{0}_{n_u \times n_d} & \mathbf{0}_{n_u \times n_x} & -\alpha^2\rho I & * \\ \mathbf{0}_{1 \times n_x} & \mathbf{0}_{1 \times n_d} & \mathbf{0}_{1 \times n_x} & \mathbf{0}_{1 \times n_u} & \frac{\beta+\pi-1}{\delta}\rho \end{bmatrix},$$

$$\Theta = \begin{bmatrix} \Pi_{11} & \Pi_{12} & \Pi_{13} & \Pi_{14} & \mathbf{0}_{n_x\times 1} \\ \Pi_{21}\hat{\mu} & \Pi_{22}\hat{\mu} & \Pi_{23}\hat{\mu} & \Pi_{24}\hat{\mu} & \mathbf{0}_{n_x\times 1} \\ \Pi_{31}\hat{\theta} & \Pi_{32}\hat{\theta} & \Pi_{33}\hat{\theta} & \Pi_{34}\hat{\theta} & \mathbf{0}_{n_x\times 1} \\ \Pi_{41}\hat{\theta}\hat{\mu} & \Pi_{42}\hat{\theta}\hat{\mu} & \Pi_{43}\hat{\theta}\hat{\mu} & \Pi_{44}\hat{\theta}\hat{\mu} & \mathbf{0}_{n_x\times 1} \\ \digamma_{11} & \digamma_{12} & \digamma_{13} & \digamma_{14} & \mathbf{0}_{n_z\times 1} \\ \digamma_{21}\hat{\mu} & \digamma_{22}\hat{\mu} & \digamma_{23}\hat{\mu} & \digamma_{24}\hat{\mu} & \mathbf{0}_{n_z\times 1} \\ \digamma_{31}\hat{\theta} & \digamma_{32}\hat{\theta} & \digamma_{33}\hat{\theta} & \digamma_{34}\hat{\theta} & \mathbf{0}_{n_z\times 1} \\ \digamma_{41}\hat{\theta}\hat{\mu} & \digamma_{42}\hat{\theta}\hat{\mu} & \digamma_{43}\hat{\theta}\hat{\mu} & \digamma_{44}\hat{\theta}\hat{\mu} & \mathbf{0}_{n_z\times 1} \end{bmatrix},$$

$$\Lambda = \mathrm{diag}\left(-Q,-Q,-Q,-Q,-\rho,-\rho,-\rho,-\rho\right),$$

$$\Pi_{11} = AQ + BY\left(1-\bar{\theta}\right)(1-\bar{\mu}),\ \Pi_{21} = -BY\left(1-\bar{\theta}\right),\ \Pi_{31} = -BY\left(1-\bar{\mu}\right),\ \Pi_{41} = BY,$$

$$\Pi_{12} = B_dQ,\ \Pi_{22} = 0,\ \Pi_{32} = 0,\ \Pi_{42} = 0,\ \Pi_{13} = BY\left(1-\bar{\theta}\right)(1-\bar{\mu}),\ \Pi_{23} = -BY\left(1-\bar{\theta}\right),$$

$$\Pi_{33} = -BF\left(1-\bar{\mu}\right),\ \Pi_{43} = BY,\ \Pi_{14} = BQ\left(1-\bar{\theta}\right)\bar{\mu},\ \Pi_{24} = BQ\left(1-\bar{\theta}\right),\ \Pi_{34} = -\bar{\mu}BQ,$$

$$\Pi_{44} = -BQ,\ \digamma_{11} = CQ + D(1-\bar{\theta})(1-\bar{\mu})Y,\ \digamma_{21} = -D(1-\bar{\theta})Y,\ \digamma_{31} = -D(1-\bar{\mu})Y,$$

$$\digamma_{41} = DY,\ \digamma_{12} = 0,\ \digamma_{22} = 0,\ \digamma_{32} = 0,\ \digamma_{42} = 0,\ \digamma_{13} = DQ(1-\bar{\theta})(1-\bar{u}),\ \digamma_{23} = -DQ(1-\bar{\theta}),$$

$$\digamma_{33} = -DQ(1-\bar{u}),\ \digamma_{43} = DQ,\ \digamma_{14} = DQ(1-\bar{\theta})\bar{\mu},\ \digamma_{24} = DQ(1-\bar{\theta}),\ \digamma_{34} = -\bar{\mu}DQ,$$

$$\digamma_{44} = -DQ,\ \Phi = \rho P^{-1}P^{-1},\ \hat{\theta} = \sqrt{\bar{\theta}(1-\bar{\theta})},\ \hat{\mu} = \sqrt{\bar{\mu}(1-\bar{\mu})}.$$

Then, the feedback gain of the designed predictive controller can be computed as $F(k) = Y(k)Q^{-1}(k)$.

Proof 1. Define the following Lyapunov function:

$$\mathrm{V}(k+n\mid k) = x^T(k+n\mid k)P\left(k\right)x(k+n\mid k) + \frac{1}{\delta}\varsigma(k+n\mid k) \tag{17}$$

where $P(k)$ is a positive definite symmetric matrix. Subsequently, along the trajectory of (11), the derivative of $V(k+n\mid k)$ can be obtained as follows:

$$\begin{aligned}
\mathbb{E}\{\Delta V(k+n\mid k)\} =& \mathbb{E}\{V(k+n+1\mid k) - V(k+n+1\mid k)\} \\
=& \mathbb{E}\{\{\{A + B[1-\bar{\theta}-(\theta(k)-\bar{\theta})][1-\bar{\mu}-(\mu(k)-\bar{\mu})]F(k)\}x(k+n\mid k) \\
&+ B[1-\bar{\theta}-(\theta(k)-\bar{\theta})][1-\bar{\mu}-(\mu(k)-\bar{\mu})]F(k)\phi(k+n\mid k) + B[1-\bar{\theta}-(\theta(k)-\bar{\theta})] \\
&\times[\bar{\mu}+(\mu(k)-\bar{\mu})]v(k+n\mid k) + B_dd(k+n\mid k)\}^TP(k)\{A + B[1-\bar{\theta}-(\theta(k)-\bar{\theta})] \\
&\times[1-\bar{\mu}-(\mu(k)-\bar{\mu})]F\}x(k+n\mid k) + B[1-\bar{\theta}-(\theta(k)-\bar{\theta})][1-\bar{\mu}-(\mu(k)-\bar{\mu})]F \\
&\times\phi(k+n\mid k) + B[1-\bar{\theta}-(\theta(k)-\bar{\theta})][\bar{\mu}(k_t+n\mid k) + (\mu(k)-\bar{\mu})]v(k+n\mid k) \\
&+ B_dd(k+n\mid k)\} + \frac{1}{\delta}[\beta\varsigma(k+n\mid k) + \varepsilon x^T(k+n\mid k)x(k+n\mid k) - \varrho^T(k+n\mid k) \\
&\times\varrho(k+n\mid k)] - x(k+n\mid k)^TP(k)x(k+n\mid k) - \frac{1}{\delta}\varsigma(k+n\mid k)\}.
\end{aligned} \tag{18}$$

The following results can be easily derived:

$$\mathbb{E}\{\mu(k)-\bar{\mu}\} = 0,\quad \mathbb{E}\{\theta(k)-\bar{\theta}\} = 0,\quad \mathbb{E}\{(\mu(k)-\bar{\mu})^2\} = \bar{\mu}(1-\bar{\mu}),\quad \mathbb{E}\{(\theta(k)-\bar{\theta})^2\} = \bar{\theta}(1-\bar{\theta}),$$

$$\mathbb{E}\{(\mu(k)-\bar{\mu})(\theta(k)-\bar{\theta})^2\} = 0,\quad \mathbb{E}\{(\mu(k)-\bar{\mu})^2(\theta(k)-\bar{\theta})\} = 0,\quad \mathbb{E}\{(\mu(k)-\bar{\mu})^2(\theta(k)-\bar{\theta})^2\} = \bar{\theta}(1-\bar{\theta})\bar{\mu}(1-\bar{\mu}).$$

In the following, by defining $\Gamma(k+n|k) = \left[x^T(k+n|k) \quad d^T(k+n|k) \quad \varrho^T(k+n|k) \quad \upsilon^T(k+n|k) \quad \sqrt{\varsigma^T(k+n|k)}\right]^T$

and considering the dynamic event-triggered protocol (4)-(6), one can readily obtain:

$$\begin{aligned}
&\mathbb{E}\{\Delta V(k+n \mid k)\}+\| z(k+n \mid k)\|^2-\alpha^2\| \eta(k+n \mid k)\|^2 \\
&\leq \mathbb{E}\{\Delta V(k+n \mid k)\}+\| z(k+n \mid k)\|^2-\alpha^2\| \eta(k+n \mid k)\|^2 \\
&\quad+\pi[-\varrho^T(k+n \mid k) \varrho(k+n \mid k)+\frac{1}{\delta} \varsigma(k+n \mid k)+\varepsilon x^T(k+n \mid k) x(k+n \mid k)] \\
&=\Gamma^T(k+n \mid k)\left({\Theta_1}^T \Lambda_1 \Theta_1+\Xi_1\right) \Gamma(k+n \mid k)=\Gamma^T(k+n \mid k) \Upsilon \Gamma(k+n \mid k)
\end{aligned} \tag{19}$$

where

$$\Xi_1=\begin{bmatrix}
-P+(\frac{\varepsilon}{\delta}+\pi \varepsilon) I & * & * & * & * \\
\mathbf{0}_{n_d \times n_x} & -\alpha^2 I & * & * & * \\
\mathbf{0}_{n_x \times n_x} & \mathbf{0}_{n_x \times n_d} & \left(-\frac{1}{\delta}-\pi\right) I & * & * \\
\mathbf{0}_{n_u \times n_x} & \mathbf{0}_{n_u \times n_d} & \mathbf{0}_{n_u \times n_x} & -\alpha^2 I & * \\
\mathbf{0}_{1 \times n_x} & \mathbf{0}_{1 \times n_d} & \mathbf{0}_{1 \times n_x} & \mathbf{0}_{1 \times n_u} & \frac{\beta+\pi-1}{\delta}
\end{bmatrix},$$

$$\Theta_1=\begin{bmatrix}
A_1 & \mathrm{B}_1 & \mathrm{C}_1 & \mathrm{D}_1 & \mathbf{0}_{n_x \times 1} \\
\mathrm{A}_2 \hat{\mu} & \mathrm{B}_2 \hat{\mu} & \mathrm{C}_2 \hat{\mu} & \mathrm{D}_2 \hat{\mu} & \mathbf{0}_{n_x \times 1} \\
\mathrm{A}_3 \hat{\theta} & \mathrm{B}_3 \hat{\theta} & \mathrm{C}_3 \hat{\theta} & \mathrm{D}_3 \hat{\theta} & \mathbf{0}_{n_x \times 1} \\
\mathrm{A}_4 \hat{\theta} \hat{\mu} & \mathrm{B}_4 \hat{\theta} \hat{\mu} & \mathrm{C}_4 \hat{\theta} \hat{\mu} & \mathrm{D}_4 \hat{\theta} \hat{\mu} & \mathbf{0}_{n_x \times 1} \\
\mathrm{A}_{11} & \mathrm{B}_{11} & \mathrm{C}_{11} & \mathrm{D}_{11} & \mathbf{0}_{n_u \times 1} \\
\mathrm{A}_{22} \hat{\mu} & \mathrm{B}_{22} \hat{\mu} & \mathrm{C}_{22} \hat{\mu} & \mathrm{D}_{22} \hat{\mu} & \mathbf{0}_{n_u \times 1} \\
\mathrm{A}_{33} \hat{\theta} & \mathrm{B}_{33} \hat{\theta} & \mathrm{C}_{33} \hat{\theta} & \mathrm{D}_{33} \hat{\theta} & \mathbf{0}_{n_u \times 1} \\
\mathrm{A}_{44} \hat{\theta} \hat{\mu} & \mathrm{B}_{44} \hat{\theta} \hat{\mu} & \mathrm{C}_{44} \hat{\theta} \hat{\mu} & \mathrm{D}_{44} \hat{\theta} \hat{\mu} & \mathbf{0}_{n_u \times 1}
\end{bmatrix},$$

$$\Lambda_1=\operatorname{diag}\left(-P^{-1},-P^{-1},-P^{-1},-P^{-1},-I,-I,-I,-I\right), \Upsilon=\begin{bmatrix}\Xi_1 & {\Theta_1}^T \\ \Theta_1 & \Lambda_1\end{bmatrix},$$

$$A_1=A+BF\left(1-\bar{\theta}\right)(1-\bar{\mu}),\ A_2=-BF\left(1-\bar{\theta}\right),\ A_3=-BF\,(1-\bar{\mu}),\ A_4=BF,$$

$$B_1=B_d,\ B_2=0,\ B_3=0, B_4=0,\ C_1=BF\left(1-\bar{\theta}\right)(1-\bar{\mu}),\ C_2=-BF\left(1-\bar{\theta}\right),$$

$$C_3=-BF\,(1-\bar{\mu}),\ C_4=BF,\ D_1=B\left(1-\bar{\theta}\right)\bar{\mu},\ D_2=B\left(1-\bar{\theta}\right),\ D_3=-\bar{\mu}B,$$

$$D_4=-B,\ A_{11}=C+D(1-\bar{\theta})(1-\bar{\mu})F,\ A_{22}=-D(1-\bar{\theta})F,\ A_{33}=-D(1-\bar{\mu})F,$$

$$A_{44}=DF,\ B_{11}=0,\ B_{22}=0, B_{33}=0,\ B_{44}=0,\ C_{11}=D(1-\bar{\theta})(1-\bar{u}),\ C_{22}=-D(1-\bar{\theta}),$$

$$C_{33}=-D(1-\bar{u}),\ C_{44}=D,\ D_{11}=D(1-\bar{\theta})\bar{\mu},\ D_{22}=D(1-\bar{\theta}),\ D_{33}=-\bar{\mu}D,\ D_{44}=-D.$$

Next, pre- and post-multiplying ρ by $\operatorname{diag}\left(-\rho^{\frac{1}{2}}P^{-1},-\rho^{\frac{1}{2}}I,-\rho^{\frac{1}{2}}P^{-1},\rho^{\frac{1}{2}}I,-\rho^{\frac{1}{2}}I,-\rho^{\frac{1}{2}}I,-\rho^{\frac{1}{2}}I,-\rho^{\frac{1}{2}}I\right)$ and its transpose, respectively, and by setting $Y(k)=F(k)Q(k)$, $Q(k)=\rho P^{-1}$, we can calculate $\Upsilon<0$ based on the inequality (16a), which can also derive that:

$$\mathbb{E}\{\Delta V(k+n)\}+z^T(k+n \mid k) z(k+n \mid k)-\alpha^2 \eta^T(k+n \mid k) \eta(k+n \mid k)<0, \tag{20}$$

Adding from $t=0$ to $t=\infty$ on both sides of (20) , we can obtain:

$$\sum_{\mathrm{n}=0}^{\infty} z^T(k+n \mid k) z(k+n \mid k)<x^T P x+\alpha^2 \sum_{n=0}^{\infty} \eta^T(k+n \mid k) \eta(k+n \mid k). \tag{21}$$

Under zero initial condition, we can achieve:

$$\sum_{\mathrm{n}=0}^{\infty} z^T(k+n \mid k) z(k+n \mid k)<\alpha^2 \sum_{n=0}^{\infty} \eta^T(k+n \mid k) \eta(k+n \mid k), \tag{22}$$

which implies that the H_∞ performance is guaranteed.

According to the Schur complement principle, (16b) can be converted into:

$$\begin{aligned}
\begin{bmatrix} -1 & * & * & * \\ \alpha^2\bar{d} & -\rho\alpha^2\bar{d} & * & * \\ \alpha^2\bar{\upsilon} & \mathbf{0}_{n_u\times 1} & -\rho\alpha^2\bar{\upsilon} & * \\ x(k_t) & \mathbf{0}_{n_x\times 1} & \mathbf{0}_{n_x\times 1} & -Q \end{bmatrix} &= -1 - \begin{bmatrix} \alpha^2\bar{d} & \alpha^2\bar{\upsilon} & x^T(k_t) \end{bmatrix} \begin{bmatrix} \frac{1}{-\rho\alpha^2\bar{d}} & * & * \\ \mathbf{0}_{n_u\times 1} & \frac{1}{-\rho\alpha^2\bar{\upsilon}} & * \\ \mathbf{0}_{n_x\times 1} & \mathbf{0}_{n_x\times 1} & -Q^{-1} \end{bmatrix} \begin{bmatrix} \alpha^2\bar{d} \\ \alpha^2\bar{\upsilon} \\ x(k_t) \end{bmatrix} \\
&= -1 - \begin{bmatrix} \frac{1}{-\rho} & \frac{1}{-\rho} & -x^T(k_t)\ Q^{-1} \end{bmatrix} \begin{bmatrix} \alpha^2\bar{d} \\ \alpha^2\bar{\upsilon} \\ x(k_t) \end{bmatrix} \\
&= -1 + \frac{1}{\rho}\alpha^2\bar{d} + \frac{1}{\rho}\alpha^2\bar{\upsilon} + x^T(k_t)Q^{-1}x(k_t) \qquad (23)
\end{aligned}$$

By multiplying both sides of (23) by ρ, the following inequality can be derived:

$$x^T Px + \alpha^2\bar{d} + \alpha^2\bar{\upsilon} \le \rho. \qquad (24)$$

According to (21) and (24), we have:

$$\sum_{\mathrm{n}=0}^{\infty} z^T(k+n\mid k)z(k+n\mid k) < x^T Px + \alpha^2\bar{\eta} \le \rho. \qquad (25)$$

where $\bar{\eta} = \left[\bar{d}^T, \bar{\upsilon}^T\right]^T$.

Therefore, the H_2 performance is satisfied.

In the following, pre- and post-multiplying (16c) by $\mathrm{diag}(\rho^{-\frac{1}{2}}P, \rho^{-\frac{1}{2}}I)$ and its transpose, (16c) can be transformed into:

$$\begin{bmatrix} -P & * \\ F & -u_{\max}^2\frac{1}{\rho}I \end{bmatrix} \le 0. \qquad (26)$$

By the Schur complement, we can derive:

$$\begin{aligned}
&-P + F^T\frac{1}{u_{\max}^2}F\rho \le 0, \\
&-x^T(k+n\mid k)Px(k+n\mid k) + \frac{1}{u_{\max}^2}\rho x^T(k+n\mid k)F^TFx(k+n\mid k) \le 0. \qquad (27)
\end{aligned}$$

Based on (10), the above inequality can be converted to:

$$\begin{aligned}
-x^T(k+n\mid k)Px(k+n\mid k) + \frac{\rho u^T(k+n\mid k)u(k+n\mid k)}{u_{max}^2} &\le 0, \\
\frac{u^T(k+n\mid k)u(k+n\mid k)}{u_{\max}^2} &\le x^T(k+n\mid k)Q^{-1}x(k+n\mid k).
\end{aligned}$$

Considering (24), we have:

$$u^T(k+n\mid k)u(k+n\mid k) \le u_{\max}^2,$$

which satisfies the input constraint (14).

When the distribution $d(k+n\mid k) = 0$ and the deception attack $\upsilon(k+n\mid k) = 0$, one can also see that the closed-loop predictive control system (11) is stochastically stable based on (16a). Therefore, the proof is completed.

4. Illustrative example

The primary purpose of this section is to provide two physical examples to prove the feasibility of the designed dynamic event-based model predictive control method for NCSs with hybrid cyber-attacks.

4.1. Example 1

In this case, the angular positioning system is considered in the following form [24]:

$$x_p(k+1) = \begin{bmatrix} 1 & 0.1 \\ 0 & 1-0.1\partial(k) \end{bmatrix} x_p(k) + \begin{bmatrix} 0.1\kappa & 0 \\ 0 & 0.1\kappa \end{bmatrix} u(k),$$

where $x_p(k) = \begin{bmatrix} \theta(k) \\ \dot{\theta}(k) \end{bmatrix}$ stands for angular position and velocity of antenna, respectively; $\partial(k)$ is the coefficient of viscous friction and satisfies $0.1s^{-1} \leq \partial(k) \leq 10s^{-1}$. We assume that $\partial(k) = 0.1$ and $\kappa = 0.787 rad^{-1}V^{-1}s^{-2}$ and have the following model parameters:

$$A = \begin{bmatrix} 1 & 0.1 \\ 0 & 0.99 \end{bmatrix}, B = \begin{bmatrix} -0.0787 & 0 \\ 0 & 0.0787 \end{bmatrix},$$

and other system matrices are assumed as follows:

$$B_d = \begin{bmatrix} -0.061 \\ 0.09504 \end{bmatrix}, C = \begin{bmatrix} 0.1 & 0 \\ 0.1 & 0.1 \end{bmatrix}, D = \begin{bmatrix} 0.2 & 0.1 \\ 0.2 & 0.1 \end{bmatrix}.$$

In this example, we assume that the occurrence probabilities of deception attacks and packet dropout are $\bar{\mu} = 0.2$ and $\bar{\theta} = 0.11$, respectively. The other parameters are selected as $\delta = 8$, $\varepsilon = 0.6$, $\beta = 0.8$, $\bar{\eta} = [150, 120]$, $\alpha = 0.8$. In addition, we choose the initial value of state as $x_0 = [-5 \quad 5]^T$. The disturbance and deception signals are described as:

$$d(k) = 0.5 * \sin(0.3k),$$
$$\upsilon(k) = 0.4 * \sin(0.5k).$$

Figs.2-4(b) show the simulation results. The controlled output of the open-loop system is shown in Fig.2, which shows that the open-loop model is unstable. The instant and value of the deception signal are shown in Fig.3(a), and Fig.3(b) shows when the control signal is not successfully transmitted to the actuator of the plant. Fig.4(a) depicts the triggering instants of the DETP proposed in this paper, which shows that only 56 sampling moments satisfy dynamic triggered conditions (4)-(6) and should be transmitted through the network. Communication resources can be effectively reduced. The controlled output response of the closed-loop model is shown in Fig.3(c), from which we can easily determine that the system can be stabilised, and the controlled output is robust to randomly occurring deception attacks, packet dropouts and external disturbances by applying the designed MPC strategy. Therefore, the proposed model predictive control approach can achieve security control under DETP, randomly occurring deception attacks and packet dropouts.

To further verify the advantages of the proposed DETP, we considered the static event-triggered design approach in [5]. The simulation result is shown at the bottom of Fig.4(b), which indicates that 94 sampling moments satisfy the static event-triggered condition, and are transmitted through the network. We can observe that the transmitted data of the proposed DETP is $(94-56)/94 = 40.43\%$ less than that of the SETP. The next table presents a detailed comparison of the results of the two data transmission schemes.

Table 1: The comparison between two kinds of data transmission scheme

Transmission methods	transfer rate	ρ
SETP	31.33%	172.8766
DETP	18.67%	172.8502

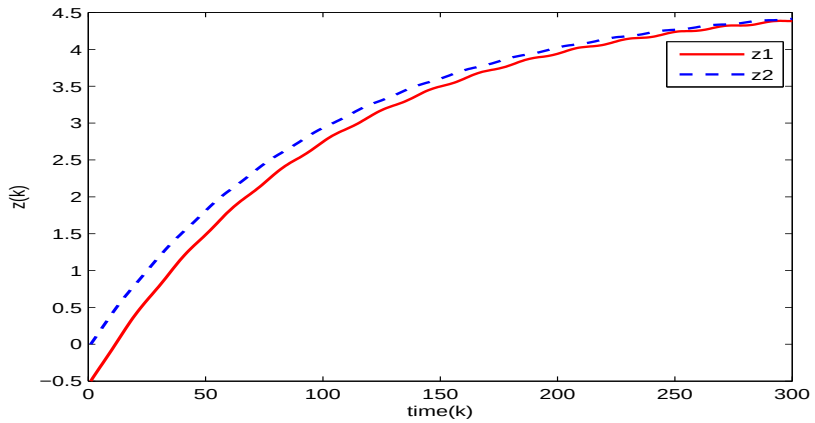
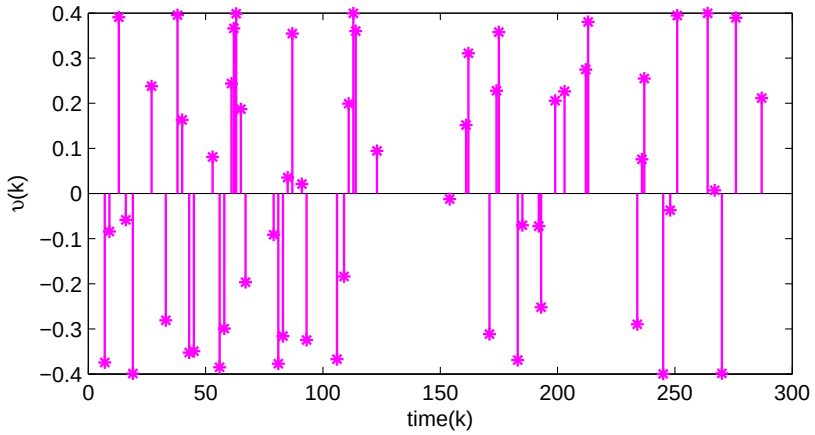
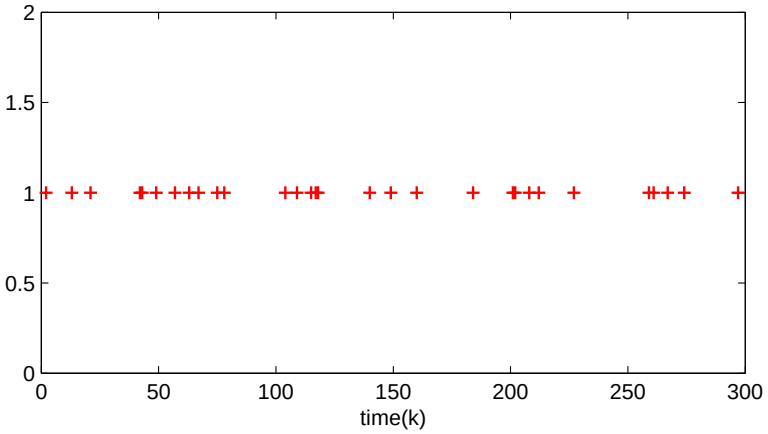


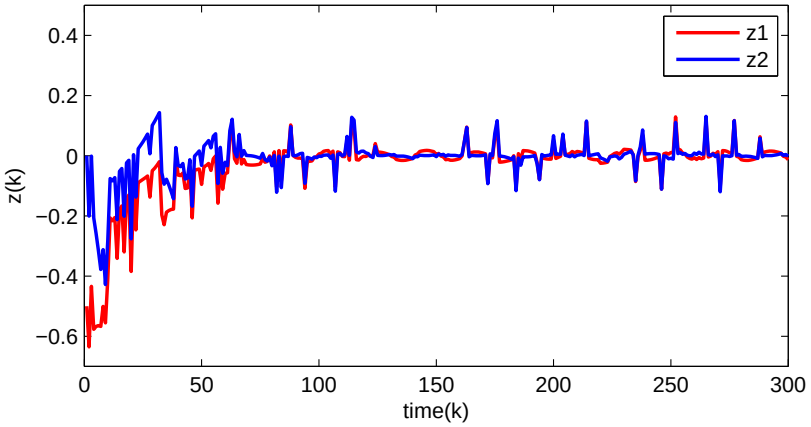
Figure 2: Controlled output responses of open-loop system



(a) The attack instant and value of deception signal

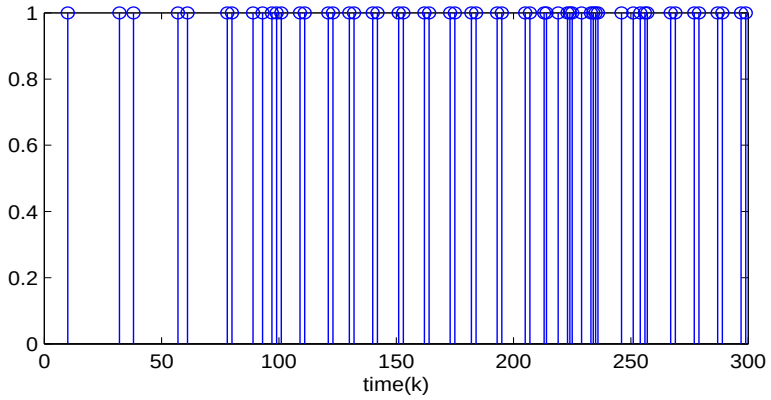


(b) The instants of packet dropout

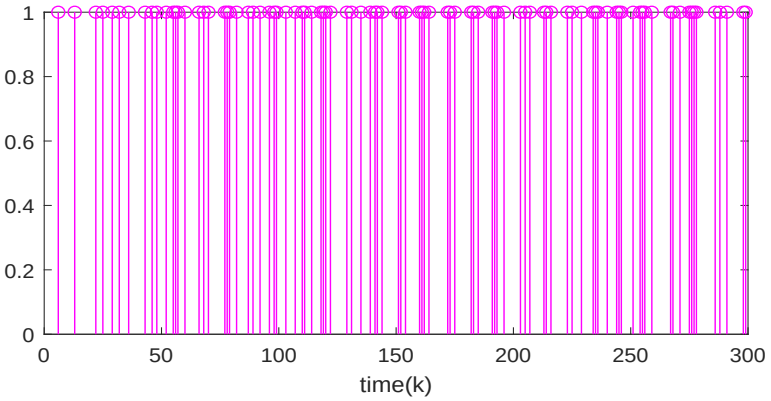


(c) Controlled output trajectories of closed-loop system

Figure 3: The trajectories of controlled output subject to deception attacks and packet dropout



(a) The triggering instants under dynamic event-triggered MPC strategy



(b) The triggering instants under static event-triggered MPC strategy

Figure 4: The triggering instants under dynamic and static event-triggered MPC strategy

4.2. Example 2

In this example, the linearized model of the vertical take-off and landing (VTOL) control system is given to evaluate the proposed design strategy, where the model parameters are as follows [23]:

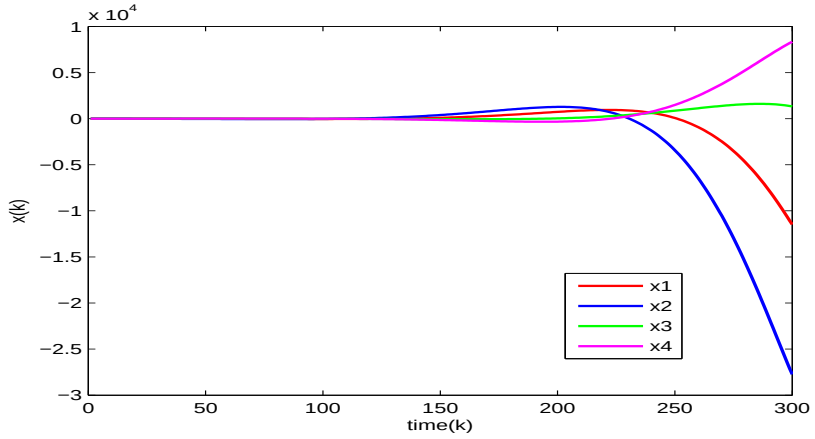
$$A = \begin{bmatrix} 0.9964 & 0.0026 & -0.0004 & -0.0460 \\ 0.0045 & 0.9037 & -0.0188 & -0.3834 \\ 0.0098 & 0.0339 & 0.9383 & 0.1302 \\ 0.0005 & 0.0017 & 0.0968 & 1.0067 \end{bmatrix}, B = \begin{bmatrix} 0.0445 & 0.0167 \\ 0.3407 & -0.7249 \\ -0.5278 & 0.4214 \\ -0.0268 & 0.0215 \end{bmatrix}$$

$$B_d = \begin{bmatrix} 0.0297 \\ 0.0353 \\ 0.0221 \\ 0.0147 \end{bmatrix}, C = \begin{bmatrix} 0.1 & 0.1 & 0.1 & 1 \end{bmatrix}, D = \begin{bmatrix} 1.33 & 0.106 \end{bmatrix}.$$

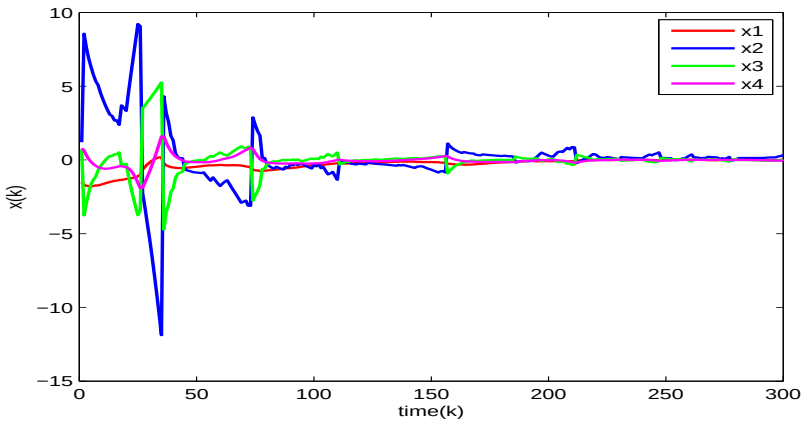
where the system state $x(t) = [v_h, v_v, q, \theta]^T$, v_h, v_v, q, θ represent the horizontal speed, vertical speed, pitch rate and pitch angle of the VTOL helicopter, respectively. The controllers $u(t) = [\delta_c, \delta_l]^T$, where δ_c is collective pitch controller, and δ_l is longitudinal cyclic pitch controller.

We assume the occurring probability of deception attacks and packet dropouts are 0.2 and 0.11, respectively. Assume that the initial state $x(0) = [-1.5, 1.2, 0.7, 0.8]^T$. The other variables and parameters are selected as $d(k) = 0.1 * \sin(0.3k), \upsilon = 0.25 * \cos(0.6k), \delta = 10, \varepsilon = 0.6, \beta = 0.8, \bar{\eta} = [30, 75]$, and $\alpha = 0.66, u_{\max} = 25$.

Fig.5(a) depicts the state trajectory of the open-loop model, and it can can be observed that the helicopter dynamic system is unstable without control. The state response under the proposed control policy is shown in Fig.5(b), which demonstrates that the designed strategy can achieve the desired security control performance. Fig.6(a) shown the random deception signal initiated by the attacker, where the instants of packet dropout are depicted in Fig.6(b). The controlled output of the closed-loop system subjected to a deception attack and packet dropout is shown in Fig.6(c). The triggering instants of the DETP are shown in Fig.7, and it can be observed that 78 of the 300 sampled data are transmitted through the network. Based on the above results, the designed dynamic event-based model prediction control approach can achieve the desired security control purpose and save network communication resources.

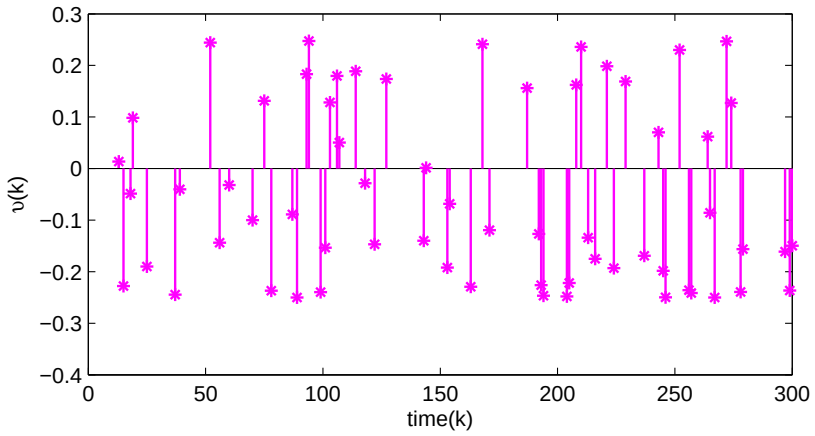


(a) State trajectories of open-loop system with cyber-attacks

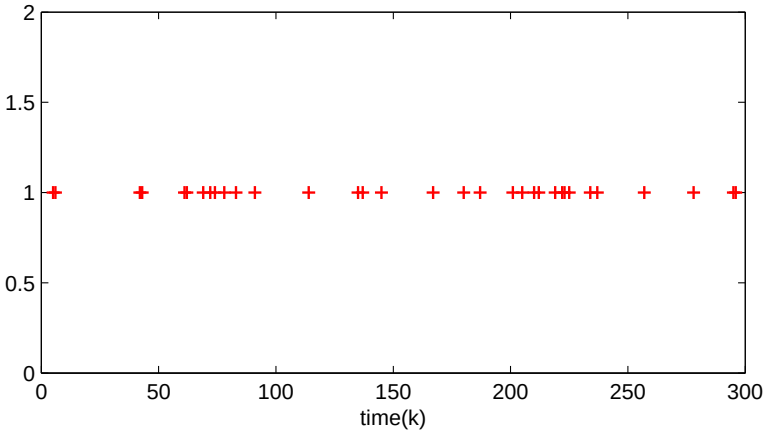


(b) State trajectories of closed-loop system with cyber-attacks

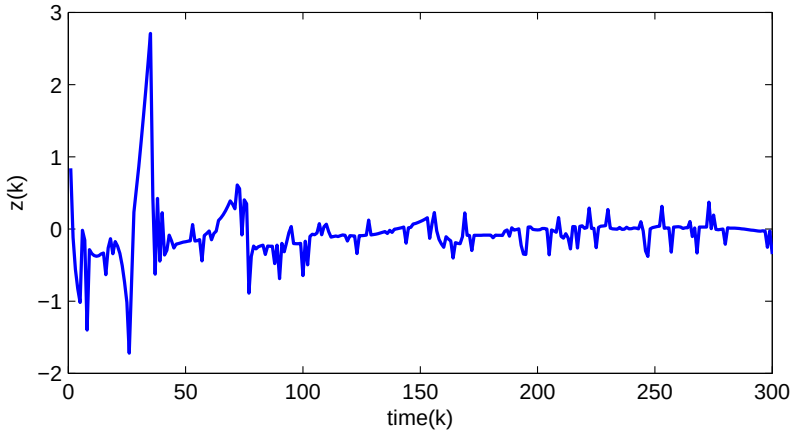
Figure 5: State trajectories of open-loop and closed-loop system with cyber-attacks



(a) The attack instant and value of deception signal



(b) The instants of packet dropout



(c) The controlled output trajectories of closed-loop system

Figure 6: The trajectories of controlled output subject to deception attacks and packet dropout

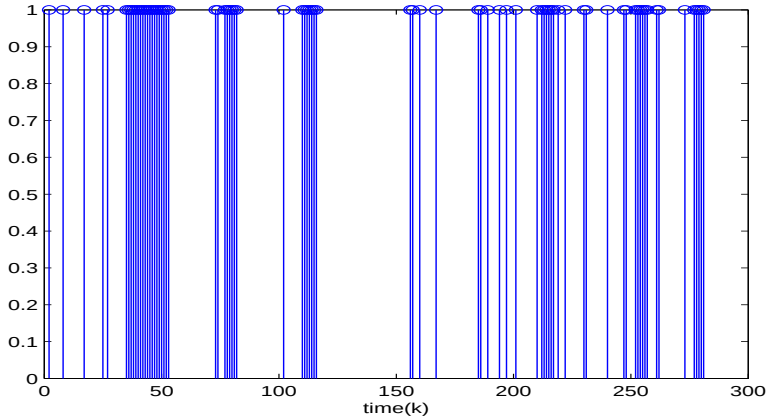


Figure 7: The triggering instants under dynamic event-triggered MPC strategy

5. Conclusion

This paper discusses the model predictive control and dynamic event-triggered protocol design problem for NCSs with deception attacks and packet dropouts. A combined cyber-attack problem is considered to stochastically destroy a realistic communication network. A novel DETP was adopted to mitigate network communication pressure, and the threshold was adjusted by the internal dynamic variable of the plant over time. Subsequently, an MPC method with H_2/H_∞ performance is designed by solving an optimal control problem that interferes with deception attacks and packet dropouts. Solvability algorithms are provided to obtain the designed controller gain, which can guarantee the stochastic stability of a closed-loop system with the expected security control objective. Finally, two practical physical models were presented to demonstrate the effectiveness of the designed strategy. Future works will focus on fault-tolerant control problems of multi-agent systems subjected to cyber-attacks.

Acknowledgment

This work was partially supported by the National Natural Science Foundation of China (62071317,61903125), National Defense Basic Research Program (JCKY2021204B051), Huiyan Project for Research on Innovation and

Application of Space Science and Technology (CD2B65B6), Key Scientific Research Project of Colleges and Universities in Henan Province (20A413001).

[1] An, L., Yang, G., 2019. Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. IEEE Transactions on Cybernetics 49 (3), 827–838.
[2] Befekadu, G., Gupta, V., Antsaklis, P., 2015. Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies. IEEE Transactions on Automatic Control 60 (12), 3299–3304.
[3] Chen, B., Ho, D., Hu, G., Yu, L., 2018. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. IEEE Transactions on Cybernetics 48 (6), 1862–1876.
[4] Cui, Y., Liu, Y., Zhang, W., Alsaadi, F., 2021. Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method. IEEE Transactions on Systems Man Cybernetics:Systems 51 (1), 561–573.
[5] Dong, H., Wang, Z., Shen, B., Ding, D., 2016. Variance-constrained H_∞ control for a class of nonlinear stochastic discrete time-varying systems: The event-triggered design. Automatica 72, 28–36.
[6] Ge, X., Han, Q., Ding, L., Wang, Y., Zhang, X., 2020. Dynamic event-triggered distributed coordination control and its applications: A survey of trends and techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems 50 (9), 3112–3125.
[7] Ge, X., Han, Q., Zhang, X., Ding, D., Yang, F., 2020. Resilient and secure remote monitoring for a class of cyber-physical systems against attacks. Information sciences 512, 1592–1605.
[8] Ge, X., Xiao, S., Han, Q., Zhang, X., Ding, D., 2021. Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks. IEEE/CAA Journal of Automatica Sinica 9 (1), 31–46.
[9] Gu, Z., Shi, P., Yue, D., Ding, Z., 2019. Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems. IEEE Transactions on Cybernetics 49 (5), 1570–1579.
[10] Guan, Y., Han, Q., Yao, H., Ge, X., 2018. Robust event-triggered H_∞ controller design for vehicle active suspension systems. Nonlinear Dynamics 94 (1), 627–638.
[11] Gupta, R., Chow, M., 2010. Networked control system: Overview and research trends. IEEE Transactions on Industrial Electronics 57 (7), 2527–2535.
[12] Jin, Z., Gupta, V., Murray, R., 2006. State estimation over packet dropping networks using multiple description coding. Automatica 42 (9), 1441–1452.
[13] Li, L., Zou, W., Fei, S., 2017. Event-based dynamic output-feedback controller design for networked control systems with sensor and actuator saturations. Journal of the Franklin Institute 354 (11), 4331–4352.
[14] Liu, J., Yin, T., Cao, J., Yue, D., Karimi, H., 2021. Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks. IEEE Transactions on Systems Man Cybernetics:Systems 51 (10), 6544–6554.
[15] Liu, J., Yin, T., Yue, D., Karimi, H., 2021. Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks. IEEE Transactions on Cybernetics 51 (1), 162–173.
[16] Liu, Y., Peng, Y., Wang, B., Yao, Y., Liu, Z., 2017. Review on cyber-physical systems. IEEE/CAA Journal of Automatica Sinica 4 (1), 27–40.
[17] Lu, Q., Shi, P., Wu, L., Lim, C., 2020. Event-triggered estimation and model predictive control for linear systems with actuator fault. IET Control Theory & Applications 14 (16), 2406–2412.
[18] Ma, Z., Liu, Z., Huang, P., 2021. Fractional-order control for uncertain teleoperated cyber-physical system with actuator fault. IEEE/ASME Transactions on Mechatronics 26 (5), 2472–2482.
[19] Manzoor, T., Sun, Z., Xia, Y., Ma, D., 2020. MPC based compound flight control strategy for a ducted fan aircraft. Aerospace Science and Technology 107, 106264.
[20] Munoz-Carpintero, D., Cannon, M., Kouvaritakis, B., 2015. Robust MPC strategy with optimized polytopic dynamics for linear systems with additive and multiplicative uncertainty. Systems & Control Letters 81, 34–41.
[21] Ning, Z., Wang, T., Zhang, K., 2022. Dynamic event-triggered security control and fault detection for nonlinear systems with quantization and deception attack. Information Sciences 594, 43–59.
[22] Ning, Z., Yu, J., Pan, Y., Li, H., 2018. Adaptive event-triggered fault detection for fuzzy stochastic systems with missing measurements. IEEE Transactions on Fuzzy Systems 26 (4), 2201–2212.
[23] Parlakci, M., 2006. Improved robust stability criteria and design of robust stabilizing controller for uncertain linear time-delay systems. International Journal of Robust and Nonlinear Control 16 (13), 599–636.
[24] Qiu, L., Shi, Y., Yao, F., Xu, G., Xu, B., 2015. Network-based robust H_2/H_∞ control for linear systems with two-channel random packet dropouts and time delays. IEEE Transactions on Cybernetics 45 (8), 1450–1462.
[25] Song, H., Yu, L., Zhang, W., 2009. H_∞ filtering of network-based systems with random delay. Signal processing 89 (4), 615–622.
[26] Sun, Q., Zhang, K., Shi, Y., 2020. Resilient model predictive control of cyber-physical systems under DoS attacks. IEEE Transactions on Industrial Informatics 16 (7), 4920–4927.
[27] Wada, N., Saito, K., Saeki, M., 2006. Model predictive control for linear parameter varying systems using parameter dependent lyapunov function. IEEE Transactions on Circuits and Systems-II:Express Briefs 53 (12), 1446–1450.
[28] Wang, J., Ding, B., Hu, J., 2021. Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach. IEEE Transactions on Automatic Control 66 (2), 760–767.
[29] Wang, W., Li, Y., Tong, S., 2020. Adaptive fuzzy event-triggered control for leader-following consensus of high-order nonlinear systems. IEEE Transactions on Fuzzy Systems 28 (10), 2389–2400.
[30] Wang, X., Ding, D., Ge, X., Han, Q., 2022. Neural-network-based control for discrete-time nonlinear systems with denial-of-service attack: The adaptive event-triggered case. International Journal of Robust and Nonlinear Control 32 (5), 2760–2779.
[31] Wang, Y., Han, Q., 2018. Network-based modelling and dynamic output feedback control for unmanned marine vehicles in network environments. Automatica 91, 43–53.
[32] Xiao, S., Han, Q., Ge, X., Zhang, Y., 2020. Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks. IEEE Transactions on Cybernetics 50 (3), 1220–1229.
[33] Yang, C., Yang, W., Shi, H., 2018. DoS attack in centralised sensor network against state estimation. IET Control Theory & Applications

12 (9), 1244–1253.
[34] Yang, H., Li, Y., Dai, L., Xia, Y., 2019. MPC-based defense strategy for distributed networked control systems under DoS attacks. Systems & Control Letters 128, 9–18.
[35] Yang, R., Shi, P., Liu, G., 2011. Network-based feedback control for systems with mixed delays based on quantization and dropout compensation. Automatica 47 (12), 2805–2809.
[36] Yang, R., Wei, X., 2020. Output-based event-triggered predictive control for networked control systems. IEEE Transactions on Industrial Electronics 67 (12), 10631–10640.
[37] Zhang, D., Han, Q.-L., Zhang, X.-M., 2020. Network-based modeling and proportional-integral control for direct-drive-wheel systems in wireless network environments. IEEE Transactions on Cybernetics 50 (6), 2462–2474.
[38] Zhang, H., Qi, Y., Wu, J., Fu, L., He, L., 2018. DoS attack energy management against remote state estimation. IEEE Transactions on Control of Network Systems 5 (1), 383–394.
[39] Zhang, W., Yu, L., 2008. Modelling and control of networked control systems with both network-induced delay and packet-dropout. Automatica 44 (12), 3206–3210.
[40] Zhang, X., Han, Q., Zhang, B., 2017. An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems. IEEE Transactions on Industrial Informatics 13 (1), 4–16.
[41] Zhang, X.-M., Han, Q.-L., Ge, X., Ding, L., 2020. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. IEEE Transactions on Cybernetics 50 (8), 3616–3626.
[42] Zhao, D., Wang, Z., Wei, G., Han, Q., 2020. A dynamic event-triggered approach to observer-based PID security control subject to deception attacks. Automatica 120, 109128.
[43] Zhao, Y., Gao, H., Chen, T., 2010. Fuzzy constrained predictive control of non-linear systems with packet dropouts. IET Control Theory and Applications 4 (9), 1665–1677.
[44] Zhu, M., Martinez, S., 2014. On the performance analysis of resilient networked control systems under replay attacks. IEEE Transactions on Automatic Control 59 (3), 804–808.
[45] Zhu, Y., Yang, F., Li, C., Zhang, Y., Han, Q., 2019. Strong $\gamma_c - \gamma_{cl}$ H_∞ stabilization for networked control systems under denial of service attacks. Journal of the Franklin Institute 356 (5), 2723–2741.