2021 IEEE International Conference on Predictive Control of Electrical Drives and Power Electronics (PRECEDE) | 978-1-6654-2557-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/PRECEDE51386.2021.9680921

Resilient MPC under DoS Attacks

1st Shuyou Yu, 2nd Zhuqing Shi, 3rd Yulei Wang
State Key Laboratory of Automotive Simulation and Control
Department of Control Science and Engineering
Jilin University
Changchun, P. R. China
{shuyou, wangyulei}@jlu.edu.cn, shizq18@mails.jlu.edu.cn

4th Yongfu Li
College of Automation
Chongqing University of Posts and Telecommunications
Chongqing, P. R. China
liyongfu@cqupt.edu.cn

5th Hong Chen
College of Electronics & Information Engineering
Tongji University
Shanghai, P. R. China
chenhong2019@tongji.edu.cn

***Abstract*—In this paper, resilient model predictive control (MPC) of the cyber-physical systems under denial-of-service (DoS) attacks is proposed, where the system dynamics is modelled as a discrete-time linear system, and the jamming strategy is not prefixed. Recursive feasibility as well as stability with respect to DoS attacks are guaranteed with the price of a little bit heavy communication load. The allowable duration of DoS attacks, which defined as a prescribed and finite control horizon of jamming action, is estimated. The effectiveness of the proposed resilient MPC scheme is verified by a simulation example.**

***Index Terms*—Robust predictive control, Resilient control, Denial-of-service attacks.**

I. Introduction

A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the internet and its users. CPS brings advances in personalized heath care, emergency response, traffic flow management, autonomous driving, and electric power generation and delivery. A cyber attack is any types of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems. A denial-of-service (DoS) attack, one of the top 10 most common type of cyber attacks, occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

Analysis of a database which tracks cyber-incidents offering industrial control systems shows that DoS attacks are the most likely threat to industrial control systems [1]. DoS attacks will force the systems to work in an open-loop status which may cause a serious threat to the control system, in particular, if the system under control is open-loop unstable.

Optimal control of a scalar discrete time LTI system in the presence of a strategic but action-limited jammer potentially disrupting the communication between the controller and the plant is considered in [2]. This leads to a zero-sum dynamic game for which the existence of saddle-point equilibrium strategies is established. A resilient control method against DoS attacks is proposed by recurring to the delta operator, which has been well recognized to overcome numerical illness for discrete-time systems with fast sampling rate [3]. The attacking scenario is considered where the defender and attacker possess asymmetric information. At the side of the defender, the inverse game approach is proposed to compensate for the attack-induced performance loss. The problem of secure control for discrete-time systems is formulated in [4]. A performance function is minimized such that a safety specification is satisfied with high probability and power limitations are obeyed in expectation when the sensor and control packets can be dropped by a random or a resource-constrained attacker. Networked systems subject to DoS attacks from the perspective of designing maximally robust controller is studied in [5, 6]. A measure of robustness against DoS attacks which is related to the average percentage of transmission failures or jamming rate is introduced. It is shown that asymptotic stability can be ensured under additional conditions, which are needed to avoid finite time phenomena during DoS attacks [6]. An explicit characterization of the frequency and duration of DoS attacks under which closed-loop stability can be preserved is investigated [7]. The result is intuitive for it relates stability with the ratio between the on/off periods of jamming. An output-based dynamic event-triggered control strategy is proposed [8], in which transmission times are determined online by means of well-design triggering rules. Additionally, desired stability and performance criteria can be guaranteed based on the natural assumption that DoS attacks are restricted in terms of frequency and duration. A resilient dual-mode model predictive control (MPC) algorithm is proposed [9] to compensate the effect induced by DoS attacks, where the input and state constraints are fulfilled by introducing the modified initial feasible set to the optimization problem.

This work is supported by the National Natural Science Foundation of China (U1964202), and Key Laboratory of New Energy Vehicle Power System in Jiangsu Province (JKLNEVPS201901).

In this contribution, we propose an event-trigger MPC scheme for constrained linear discrete-time systems under DoS attacks, in which the event is treated as the individual event. That is, if there is no attack, the involved optimization problem is solved online based on the updated measurement, and the first item of the obtained control sequence will be applied directly to systems; if on the contrary, there is a DoS attack, the shifted control sequence obtained at the former instant will be applied instead. Furthermore, both recursive feasibility of the involved optimization problem and asymptotic stability of the system are guaranteed, i.e., the DoS attack characterized by frequency and duration properties can be "tolerated". The numerical example reveals robustness to DoS attacks and performance guarantees.

The reminder of this paper is organized as follows. In Section II, the framework of interest is described and the control problem is formulated. Event-triggered MPC of network control systems under DoS attacks is proposed, and the characterization of the systems under control is discussed in Section III. The obtained design framework is illustrated by means of a numerical example in Section IV. Section V ends the paper with concluding remarks.

A. Notations and Basic Definitions

Let $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{R}^n$ denote the field of real numbers, positive numbers and the n-dimensional Euclidean space, $\mathbb{N}$ and $\mathbb{N}^+$ the sets of all natural numbers and all positive numbers. Let $N_{[k,k+N]} \triangleq \{a \in \mathbb{N} \mid k \leq a \leq k+N\}$ and $N_{[k,k+N)} \triangleq \{a \in \mathbb{N} \mid k \leq a < k+N\}$. The union, intersection and complement of two sets $\mathbb{X}$ and $\mathbb{Y}$ are denoted by $\mathbb{X} \bigcup \mathbb{Y}$, $\mathbb{X} \bigcap \mathbb{Y}$ and $\mathbb{X} \setminus \mathbb{Y}$. Denote a positive definite matrix and positive semi-definite matrix as $P \succ 0$ and $P \succeq 0$. Moreover, $\star$ is used to denote the symmetric part of a matrix, i.e., $\begin{bmatrix} a & b^T \\ b & c \end{bmatrix} = \begin{bmatrix} a & \star \\ b & c \end{bmatrix}$.

II. Problem Setup & Preliminaries

Consider discrete-time linear systems

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

where $x \in R^{n_x}$ is the system state and $u \in R^{n_u}$ the control input. The state and input constraints are defined by a polyhedral set

$$\mathcal{C} := \left\{ \begin{bmatrix} x_k \\ u_k \end{bmatrix} \in \mathcal{R}^{n_x+n_u} \mid c_j x_k + d_j u_k \leq 1, j = 1, \ldots, p \right\} \tag{2}$$

where $c_j \in \mathcal{R}^{1\times N_u}$ and $d_j \in \mathcal{R}^{1\times n_u}$. For simplicity in writing, the state and control constraints are as follows

$$x \in \mathcal{X} \tag{3a}$$

$$u \in \mathcal{U} \tag{3b}$$

where both $\mathcal{X}$ and $\mathcal{U}$ are compact set, and each set contains the origin in its interior. That is, $\mathcal{X} \times \mathcal{U} \subseteq \mathcal{C}$ and $\mathcal{X} \times \mathcal{U} \supseteq \mathcal{C}$.

Assumption 1: The pair (A, B) is stabilizable.

Suppose that the sampling period is δ, i.e., the system only exchanges information with its actuator and surrounding environment at each time instant $\Gamma\delta$ with $\Gamma \in \mathbb{N}$.

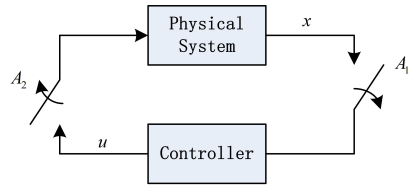

Fig. 1: DoS attacks on a control system: at the measured portion or the control input portion

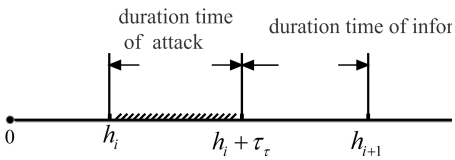

Fig. 2: DoS attacks on a control system: at the measured portion or the control input portion

A. DoS attacks on control systems

Since the controller and physical system are not integrated together physically in the controls on data in the cloud computing environment or in the real time remote control based on internet, communication between the controller and physical system plays an important role. Information availability of the control system refers to the ability of all components of being accessible in the sense of information or status. Lack of availability results in a DoS of sensor and control data, i.e., information can not transfer correctly and timely. To launch a DoS the adversary can jam the communication channels, comprise devices and prevent them from sending data, attack the routing protocols, flood with network traffic [4]. DoS attacks are represented in Fig.1 where the adversary prevents two entities of the physical system and controller from communication.

Let h_l with $l \in \mathbb{N}$ denote the time while the attacker launching a DoS attack on the system. For each distinct attack instant, the duration time of attack is denoted by $\tau_l \in \mathbb{R}^+$ and

$$\tau_l \leq h_{l+1} - h_l, \qquad \forall l \in \mathbb{N}. \tag{4}$$

Accordingly, denote η_l with $l \in \mathbb{N}$ as the duration time of information availability, where

$$\eta_l = h_{l+1} - h_l - \tau_l \quad \forall l \in \mathbb{N}. \tag{5}$$

Note that the DoS attack might be launched on the system during the sampling period. The relationship of the time while attacker launching a DoS attack on the system, duration time of attack and duration time of information availability are depicted in Fig.2.

B. Goal and requirements

Suppose that x_k can be measured in real time at the measured portion.

Remark 2.1: Systems know instantaneously the value of their state no matter whether there exist attacks or not.

The goal is to design a control law for a discrete-time linear system with respect to DoS attacks, such that

(i) The system is asymptotically stable,
(ii) Both state and input constraints are satisfied.

That is, we are interested in designing a control law that render the overall closed-loop system resilient to DoS attacks which occur according to some unknown strategy with the purpose to impede the communication of system and its remote controller.

Note that the allowed duration and the frequency of DoS attacks depend on both the system dynamics and the proposed control scheme. The control objective is to "maximize" in some sense the frequency and duration of the DoS attacks under which the closed-loop stability is not destroyed.

III. MPC SECURE AGAINST DOS ATTACKS

Define $\bar{x}_k$ and $\bar{u}_k$ as the state and control input of the predicted model

$$\bar{x}_{k+1} = A\bar{x}_k + B\bar{u}_k, \tag{6}$$

respectively.

Since the pair of (A, B) is staibilizable, for the given positive definite weighting matrices $Q \in$ and $R \in R^{n_u \times n_u}$, the following Lyapunov inequality

$$(A + BF)^T P(A + BF) - P \leq -Q - F^T RF$$

admits a unique positive definite matrix $P \in R^{n_x \times n_x}$, where $A + BF$ is stabilizable.

Lemma 1: There exists $\alpha > 0$ which specifies an ellipsoid

$$X_f := \{\xi \in R^{n_x} \mid \xi^T P\xi \leq \alpha\}$$

such that

- $X_f \subseteq \mathcal{X}$
- $Fx \in \mathcal{U}$ for all $x \in \mathcal{X}$
- X_f is positive invaraint for the nominal system (6) with the linear control law $F\bar{x}$

MPC can take constraints explicitly into account in the process of controller design, thus it is a suitable choice to achieve the given tasks. The key idea of MPC is to solve at each time instant k an open-loop optimization problem based on the measured system state x_k.

Denote the sequence

$$\bar{U}_k := \left[\bar{u}_{k|k}, \bar{u}_{k+1|k}, \cdots, \bar{u}_{k+N-1|k}\right]$$

as the control input trajectory and N as the prediction horizon.

The following finite horizon quadratic cost function is considered in MPC

$$J(x_k, \bar{U}_k) := \bar{x}^T_{k+N|k} P \bar{x}_{k+N|k} + \sum_{i=0}^{N-1} \bar{x}^T_{k+i|k} Q \bar{x}_{k+i|k} + \bar{u}^T_{k+i|k} Q \bar{u}_{k+i|k}$$

The optimization problem involved in MPC is as follows

Problem 1:

$$\underset{\bar{U}_k}{\text{minimize}} \quad J(x_k, u_k) \tag{7a}$$

subject to

$$\bar{x}_{k|k} = x_k, \quad \bar{u}_{k|k} = u_k \tag{7b}$$

$$\bar{x}_{k+i+1|k} = A\bar{x}_{k+i|k} + B\bar{x}_{k+i|k}, \tag{7c}$$

$$\bar{x}_{k+i|k} \in \mathcal{X}, \qquad i \in [0, N-1], \tag{7d}$$

$$\bar{u}_{k+i|k} \in \mathcal{U}, \qquad i \in [0, N-1], \tag{7e}$$

$$\bar{x}_{k+N|k} \in \mathbb{X}_f, \tag{7f}$$

where $X_f \subseteq \mathcal{X}$ is assumed to have an interior.

The set X_f is the terminal set, $\xi^T P\xi$ and $F\xi$ with $\xi \in X_f$ are the terminal penalty and the terminal control law, respectively.

In Problem 1 the index $k + i|k$ denotes the predicted states and inputs of the predicted model at the time instant $k + i$, where the prediction has been calculated at the current time instant k. The solution to Problem 1 at time k is the open-loop input trajectory

$$\{\bar{x}^*_{k|k}, \bar{U}^*_k\} = \arg\min_{\bar{U}_k} J(x_k, \bar{U}_k),$$

and the optimal predicted state sequence accordingly is

$$\bar{X}^*_k := \left[\bar{x}^*_{k|k}, \bar{x}^*_{k+1|k}, \cdots, \bar{x}^*_{k+N-1|k}\right].$$

Denote the optimal value of the optimal cost function at the time instant k by

$$J^*(x_k) := J(x_k, \bar{U}^*_k)$$

A. Algorithm secure against DoS attacks

If the information of the system state can be obtained by controller at each time instant k, then the optimization problem 1 will be solved with the new updated system state x_k. Furthermore, if the solution of the optimization problem is obtained as well by the physical system, then the control input applied to the system (1) will be updated at each time instant k, i.e., the applied input is

$$u_k = \bar{u}^*_{k|k}$$

where $\bar{u}^*_{k|k}$ is the first item of the optimal input sequence U^*_k. However, since the system under control and the controller are not integrated physically, DoS attack might cut the channel of the information exchanges for a while. That is, information exchanges either from physical system to controller or from controller to physical system is cut down.

Definition 1: A time instant k is an effective communication time instant in control systems if the communication between the physical system and MPC is accessible, smooth and timely (instantaneously).

Note that an effective communication time instant means that at that time instant, information exchanges both from the physical system to controller and from controller to the physical system are effective, lossless and no delay.

While a successful transmission is conducted, instead of sending only the current control signal $\bar{u}^*_{k|k}$, the current

optimal control sequence $\bar{U}_k^*$ is sent to the actuator. Thus, a buffer installed on the actuator side is needed to store the latest control signal and the predicted state.

Assumption 2: suppose that $k = 0$ is an effective communication time instant, and the duration time of attack and duration time of information availability satisfy, respectively

$$\tau_l \leq \max\{h_{l+1} - h_l,\ (N-1)\delta\} \tag{8}$$

$$\eta_l \geq \delta \tag{9}$$

Note that Assumption 2 implies that one effective information exchange between the system under control and the actuator will happen in one prediction horizon $N\delta$, and the frequency of DoS attack is less than the sampling rate of systems.

The following algorithm will be used to regulate the physical system even while DoS attacks might occur.

Data: N, Q, R and P
Result: the control input u_k
Initialization:
- At the time instant 0, solve Problem 1 with x_0, send $\bar{U}_0^*$ to the physical systems and store it at the control portion;
- Apply $u_0 = \bar{u}_{0|0}^*$ to the physical system, and set $k_e = 0$;
for $k = 1 \to \infty$ **do**
  if *k is an effective communication time instant* **then**
    - Solve Problem 1 with x_k, send $\bar{U}_k^*$ to the physical systems and store it at the control portion;
    - Apply directly $u_k = \bar{u}_{k|k}^*$ to the physical system, and set $k_e = k$;
  else
    Apply $u_k = \bar{u}_{k|k_e}^*$ to the physical system, and set $k_e = k$;
  end
end

Algorithm 1: Algorithm secure against DoS attacks

Remark 3.1: Resilient dual-mode model predictive control is presented to attenuate adverse effects of DoS attacks for the cyber-physical systems in [9]. Control action obtained by receding horizon optimization switches to the terminal control law once the closed-loop trajectory is driven to the terminal set around the origin in the presence of DoS attacks. In general switch from one controller to the others might induce chatter changes problem.

Remark 3.2: Transmission times are determined by well-defined triggering rule in [8]. Instead, in this paper, DoS attacks or loss of information exchanges will trigger systems to implement the control actions obtained in former times.

Remark 3.3: DoS attacks might not trigger the event if the interval of attacks are short enough, i.e., it is in between of information exchanges of the actuator and the plant. Thus, we care only about detected DoS attacks.

B. Recursive feasibility & Asymptotic stability

Note that in this paper, only DoS attacks are considered. The following theorem states the properties of the proposed scheme.

Theorem 1: Suppose that

- at the initial time instant, there is no DoS attack on system (1) and Problem 1 admits a feasible solution
- the duration of suffered DoS attacks is less than $(N-1)\delta$, and the frequency of DoS attacks is lower than the sampling frequency.

Then, although there exist DoS attacks,

(i) Problem 1 is feasible for all $k \geq 0$,
(ii) the system under event-triggered model predictive control is asymptotically stable.

Proof 1: (1) Suppose that no DoS attack is detected for all $k \geq 0$, i.e., both the system state and the obtained control action can be transmitted correctly, then no event is triggered. Thus, event-triggered MPC is reduced to conventional model predictive control. Therefore, both recursive feasibility and asymptotic stability can be guaranteed [10, 11].

(2) Suppose that at time instant k, with the measured system state x_k, Problem 1 has a feasible solution

$$\left[\bar{u}_{k|k}, \bar{u}_{k+1|k}, \cdots, \bar{u}_{k+N-1|k}\right]$$

and the predicted state sequence is

$$\left[\bar{x}_{k|k}, \bar{x}_{k+1|k}, \cdots, \bar{x}_{k+N-1|k}\right]$$

where $\bar{x}_{k|k} = x_k$. Note that (a) $\bar{u}_{k+i|k} \in \mathcal{U}$, $\bar{u}_{k+1|k} \in \mathcal{X}$ and $\bar{x}_{k+N|k} \in \Omega$, i.e., state constraints, input constraints and terminal constraint are satisfied. (b) Attack will be detected only at the time instant $k+1$. Otherwise, new control sequence can be obtained with the new measurement.

Without loss of generality, assume that m-consecutive signals are blocked and $m < N-1$, i.e., in that period, either control action or system state is transmitted correctly. Since neither model-plant mismatches or disturbances is considered, the predicted state is equal to the actual system state.

(2.1) At time instant $k+1$,

$$\left[\bar{u}_{k+1|k}, \cdots, \bar{u}_{k+N-1|k}, F\bar{x}_{k+N-1|k}\right]$$

is a feasible solution to Problem 1, and the predicted system state sequence is

$$\left[\bar{x}_{k+1|k}, \cdots, \bar{x}_{k+N-1|k}, \bar{x}^{k+1}\right]$$

where $\bar{x}^{k+1} \in \Omega \subseteq \mathcal{X}$. The cost function satisfies

$$J(x_{k+1}) - J(x_k) \leq -x_{k+1|k}^T Q x_{k+1|k} - u_{k+1|k}^T R u_{k+1|k}$$

which is decreasing monotonically along the predicted trajectory. (2.2) At time instant $k+h$ with $h \leq m$ and $h > 1$,

$$\left[\bar{u}_{k+h|k}, \cdots, \bar{u}_{k+N-1|k}, F\bar{x}_{k+N-1|k}, F\bar{x}^{k+1}, \cdots, F\bar{x}^{k+h-1}\right]$$

is a feasible solution to Problem 1, and the predicted system state sequence is

$$\left[\bar{x}_{k+h|k}, \cdots, \bar{x}_{k+N-1|k}, \bar{x}^{k+1}, \bar{x}^{k+2}, \cdots \bar{x}^{k+h}\right]$$

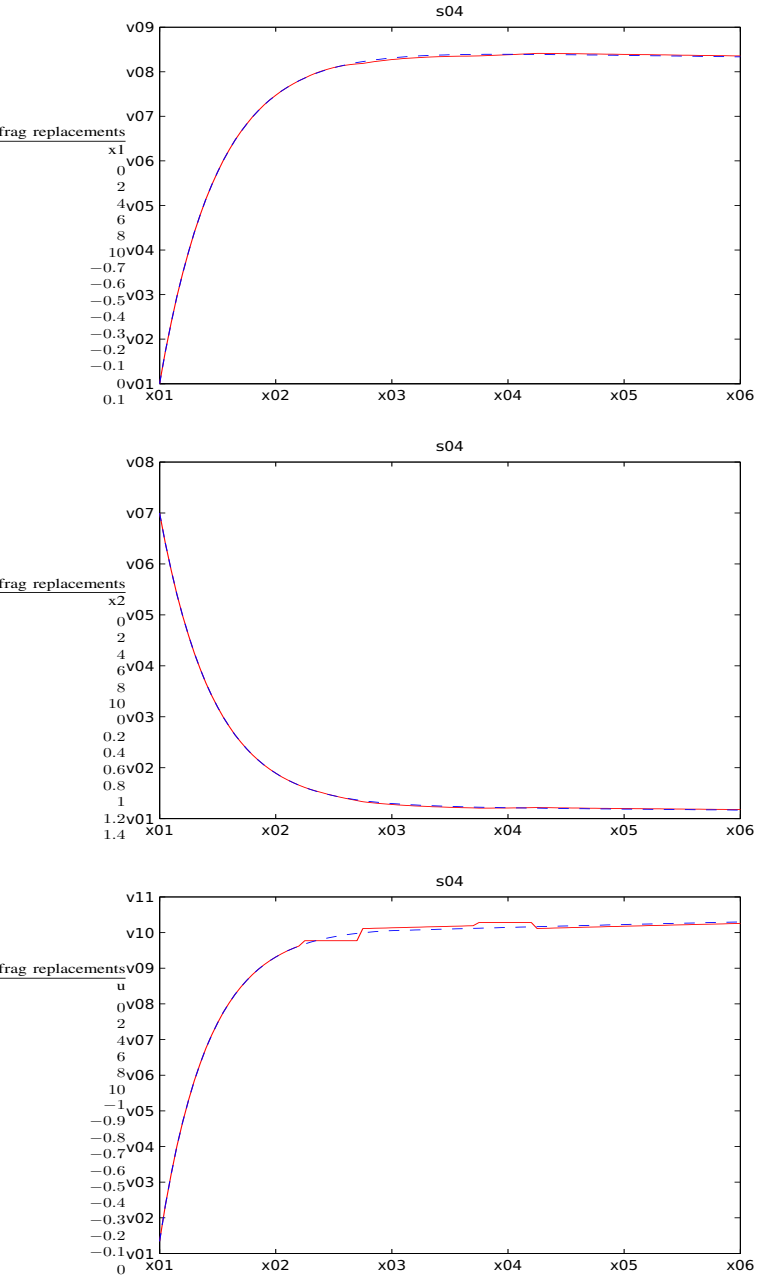

Fig. 3: Comparison of the system dynamics and control input with and without DoS attacks, Case 1 (without noises), blue line: conventional MPC without DoS attacks, solid line: event-triggered MPC with DoS attacks.

where $\bar{x}^{k+h} \in \Omega \subseteq \mathcal{X}$. The cost function satisfies

$$J(x_{k+h}) - J(x_{k+h-1}) \leq \\ - x^T_{k+h-1|k} Q x_{k+h-1|k} - u^T_{k+h-1|k} R u_{k+h-1|k}$$

which is decreasing monotonically along the predicted trajectory.

(2.3) Thus, although there is no information exchanges between the actuator and the plant, the shifted data buffered on the actuator side and the terminal control law together can guarantee the feasibility of the involved optimization problem, and the monotonically decreasing of system dynamics to the origin.

IV. Simulation Examples

In this section, a numerical example is investigated in order to verify the effectiveness of the proposed method.

The system is described by

$$x_{k+1} = \begin{bmatrix} 1 & 0.1 \\ 0.1 & 1 \end{bmatrix} x_k + \begin{bmatrix} 0.05 \\ 0.05 \end{bmatrix} u_k \tag{10}$$

which is unstable and controllable.

Consider the input constraint

$$-1 \leq u_k \leq 1, \qquad \forall k \geq 0.$$

Suppose that x_k can be measured, and choose the weighting matrices as $Q = \mathrm{diag}\{0.5, 0.5\}$, $R = 1$.

A terminal control law, a terminal penalty and a terminal constraint can be derived by solving the corresponding linear matrix inequalities (LMIs).

Lemma 2: [12, 13] For system (1), suppose that there exist a scale $\alpha > 0$, a matrix $X \succ 0$ and a matrix Y such that

$$\begin{bmatrix} X & \star & \star & \star \\ AX + BY & X & \star & \star \\ Q^{\frac{1}{2}} X & 0 & \alpha I & 0 \\ R^{\frac{1}{2}} Y & 0 & 0 & \alpha I \end{bmatrix} \succ 0 \\ \begin{bmatrix} 1 & \star \\ (c_j X + dY)^T & X \end{bmatrix} \succ 0, j = 1, \ldots, p \tag{11}$$

Then, $x^T P x$, Fx and $\Omega = \{x \in \mathcal{R}^{n_x} \mid x^T P x \leq \alpha\}$ can be chosen as the terminal penalty, terminal set and terminal control law, respectively, where $P = \alpha X^{-1}$ and $F = Y X^{-1}$. Thus, a linear state feedback control matrix $F = [-2.0107 - 2.0107]$, a terminal penalty $x^T P x$ with

$$P = \begin{bmatrix} 23.6835 & 21.0519 \\ 21.0519 & 23.6835 \end{bmatrix}$$

and a terminal set $\Omega = \left\{x \in \mathbb{R}^2 \mid x^T P x \leq 1\right\}$ are obtained accordingly by solving LMIs (11).

Choose the prediction horizon $N = 15$, and the sampling time $\delta = 0.1$. That is, the actuator and the plant will exchange information at the time instant $K\delta$ with $K \in \mathcal{N}^+$. Suppose that there exist DoS attacks during the intervals $[2.5, 3.5]$ and $[5.5, 6.5]$. Both of the two intervals are shorter than $N\delta = 1.5s$, and the gap between the two DoS attacks is larger than δ. Fig.3 shows the evolutions of state and control input of the considered system starting from $x_0 = [-0.7\ 1.2]'$. The red line shows the trajectory of the systems under the given DoS attacks with the proposed scheme, and the blue line shows the trajectory of the systems without DoS attacks under the conventional MPC scheme [14]. Although there exist DoS attacks, the proposed event-triggered MPC can drive the systems state to the origin, and guarantee the satisfaction of the input constraint. The achieved performance is close to the performance if there does not exist DoS attacks at all.

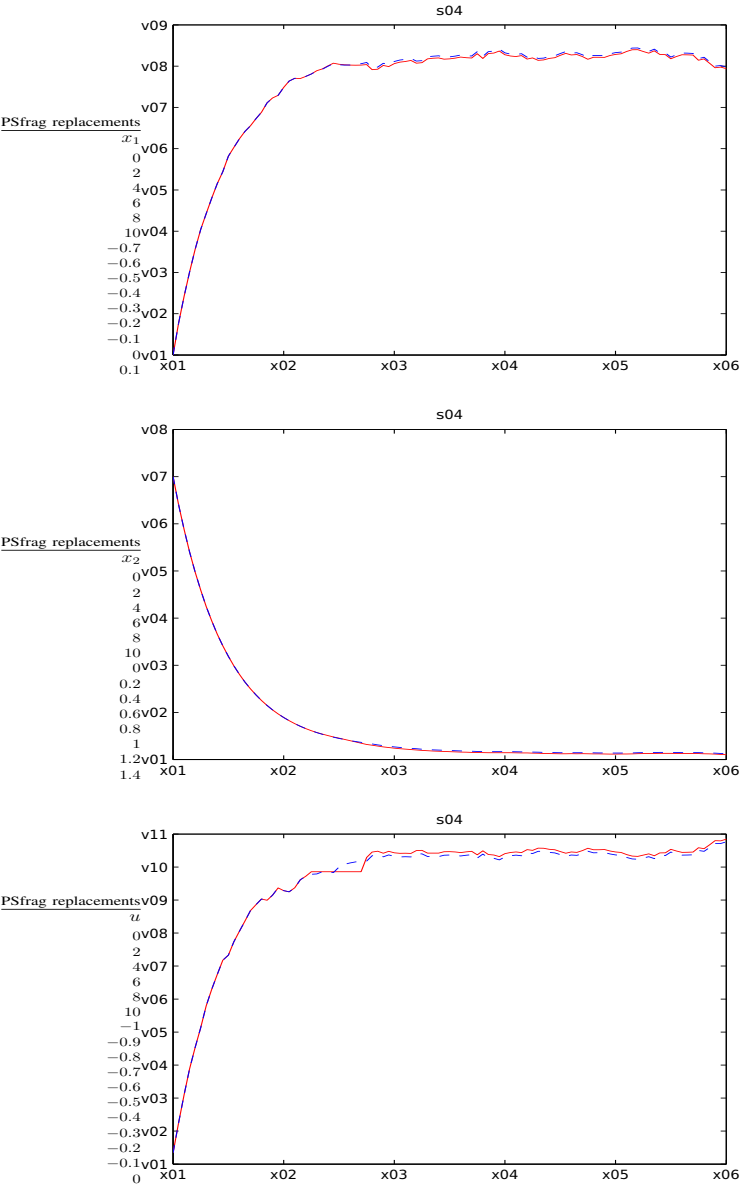

Fig. 4: Comparison of the system dynamics and control input with and without DoS attacks, Case 2 (with noises), blue line: conventional MPC without DoS attacks, solid line: event-triggered MPC with DoS attacks.

Suppose that a gaussian noise w_k with mean 0 and covariance 0.05 is added in the plant, i.e.,

$$x_{k+1} = \begin{bmatrix} 1 & 0.1 \\ 0.1 & 1 \end{bmatrix} x_k + \begin{bmatrix} 0.05 \\ 0.05 \end{bmatrix} u_k + \begin{bmatrix} 1 \\ 0 \end{bmatrix} w_k$$

In terms of the inherent robustness of MPC [15–17], conventional or named nominal MPC can be directly used to the control problem. Fig.4 shows the evolutions of state and control input of the considered system with disturbances starting from $x_0 = [-0.7\ 1.2]'$. The red line shows the trajectory of the systems under the given DoS attacks with the proposed scheme, and the blue line shows the trajectory of the systems without DoS attacks under the conventional MPC scheme. It shows that event-triggered MPC inherits the ability to deal with small disturbances as well.

V. Conclusions

In this paper, networked control systems in the presence of DoS attacks which prevent transmission over the communication network was studied. An event-triggered MPC was proposed to deal with DoS attacks that might be occurred in the communication and actuator channels. Furthermore, the allowed duration and frequency of DoS attacks are analyzed in terms of the stability guarantee and constraint satisfaction. The proposed scheme pays much attention on the final objective of the attack, but not on the particular mechanisms.

References

[1] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proceeding of the VDE Congress, VDE Association for Electrical Electronic & Informattion Technologies*, 2004, p. 1.

[2] A. Gupta, C. Langbort, and T. Baser, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. IEEE Conf. Decision Contr.* HIlton tlanta Hotel, Atlanta, GA, USA: IEEE, 2010, pp. 1096–1101.

[3] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control systems unde DoS attacks: A unifying game approach," *IEEE Transactions o Industrial Informatics*, vol. 12, no. 5, pp. 1786–1794, 2016.

[4] S. Smin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control. Lecture Notes in Computer Science, vol 5469.*, T. P. Majumdar R., Ed. Springer, Berlin, Heidelberg, 2009, pp. 31–45.

[5] S. Feng and P. Tesi, "Resilent control under denial-of-service: Robust design," *Automatica*, vol. 79, 2017.

[6] C. D. Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," vol. 96, pp. 124–131, 2016.

[7] ——, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Automat. Contr.*, vol. 60, no. 11, pp. 2930–2944, 2015.

[8] V. S. Dolk, P. Tesi, C. D. Persis, and W. P. M. H. 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.

[9] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber-physical systems under DoS attacks," *IEEE Transactions on Industrial Informatics*, 2020.

[10] J. B. Rawlings, D. Q. Mayne, and M. M. Diehl, *Model Predictive Control: Theory, Computation, and Design (2nd Edition)*. Madison, Wisconsin: Nob Hill Publishing, LLC, 2017.

[11] S. Yu, T. Qu, F. Xu, H. Chen, and Y. Hu, "Stability of finite horizon model predictive control with incremental input constraints," *Automatica*, vol. 79, pp. 265–272, 2017.

[12] C. Bohm, S. Yu, and F. Allgower, "Predictive control for constrained discrete-time periodic systems using a time-varying terminal region," in *14th International Conference on Methods and Models in Automation and Robotics*, Miedzyzdroje, Poland, 19 - 21, August 2009.

[13] Y. Liu, "Path following control of wheeled mobile robots based on model predictive control," Master Thesis, Jilin University, China, 2016.

[14] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. M. Scokaert, "Constrained model predictive control: stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[15] G. Grimm, M. J. Messina, S. Tuna, and A. R. Teel, "Examples when nonlinear model predictive control is nonrobust," *Automatica*, vol. 40, no. 10, pp. 1729–1738, 2004.

[16] S. Yu, M. Reble, H. Chen, and F. Allgöwer, "Inherent robustness properties of quasi-infinite horizon nonlinear model predictive control," *Automatica*, vol. 50, no. 9, pp. 2269–2280, 2014.

[17] D. A. Allan, C. N. Bates, M. J. Risbeck, and J. B. Rawlings, "On the inherent robustness of optimal and suboptimal nonlinear MPC," *Syst. Contr. Lett.*, vol. 106, pp. 68–78, 2017.