Resilient self-triggered model predictive control strategy against replay attack

Ning He[1], Shixuan Lin[1], Kai Ma[1*], Shuoji Chen[1]

[1]School of Mechanical and Electrical Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China
[*] E-mail: makai@xauat.edu.cn

Abstract. In this paper, contrapose cyber-physical system (CPS), a resilient control strategy based on input sample reconstruction is proposed to solve the security problem of self-triggered model predictive control (STMPC) in the presence of malicious replay attacks. Firstly, a novel replay attack model is established by considering the STMPC non-periodic sampling features. Secondly, by analyzing the characteristics of established replay attack model, an input reconstruction mechanism based on key data is designed, which ensures that even if the optimal control sample is attacked, the controlled system can still generate feasible control samples to preserve the system. In addition, closed-loop stability of the system under replay attacks is strictly demonstrated. Finally, the effectiveness of the developed resilient control mechanism is verified by a robotic system.

Keywords: Cyber-physical System, Replay Attack, Self-triggered Model Predictive Control, Input Sample Reconstruction

1. INTRODUCTION

Cyber-physical system (CPS) plays an important part in supporting and leading the new generation of industrial transformation. However, due to the interactive nature of the network, CPS is inevitably subject to malicious cyber attacks during operation, e.g., false data injection （FDI） attacks, denial-of-service (DoS) attacks, replay attacks, etc[1]. Therefore, CPS's security has attracted extensive attention. The research areas on security of CPS in the literature involve attack detection and identification, optimal attack scheduling, resilient control under attacks and so on[2].

Model predictive control (MPC) is good at dealing with complex constrained optimization control problems and has been widely applied in CPS, such as under water robot[3], intelligent robot[4], intelligent grid[5] etc. However, because frequent solving of optimization problems and data transmission restrict the application of the periodic MPC mechanism in resource-constrained CPSs, event-triggered and self-triggered mechanism is imported to diminish the communication resources[6]. STMPC incorporates an active triggering mechanism. Rely on closed-loop system stability analysis, an self-triggered condition is designed, and the next update instant is determined in advance at the current update moment. Based on the above ideas, different STMPC mechanisms have been proposed. In [7], authors propose a STMPC mechanism aimed at discrete time Markov jump linear systems. The algorithm uses the error between the current sampling information and the prediction message to calculate the next sampling time. In [8], a STMPC based on approximation is proposed aimed at sampled data systems with system constraints.

In networked MPC, not only resource consumption needs to be considered, but also security issues have raised great concerns. Recently, the responses strategies for MPC under replay attacks have been widely discussed. Replay attacks record a set of transmitted data and then replay the recorded messages into the system to achieve the purpose of attack[9]. Compared to other types of cyber attacks, replay attacks only need to replay data at certain moments to compromise the system, therefore replay attacks could directly skip the verification process that the device has been installed and have a strong stealthy nature [10]. In recent years, research on replay attack has become one of the most popular research field of industry and academia. In [11], for replay attacks, the authors design a distributed control scheme for multi-agent networked systems which subject to input and state constraints. In [12], by making clever use of set-theoretic of the receding control horizon philosophy, authors design model predictive control schemes for detection attack and resilient control action purposes. However, few schemes that simultaneously consider the response to replay attacks and resource constraints have been developed. Therefore, a resilient STMPC mechanism based on data reconstruction is put forward to balance the contradiction between security and resources. The core contributions of this paper can be summed up as follows：

1). An input sample reconstruction mechanism based on key data is proposed by analyzing replay attack characteristics, and a resilient STMPC algorithm is developed depended on this mechanism to weaken the impact of replay attack on CPS.

2). Computational principles of key data are given, and the system's closed-loop stability is demonstrated, despite the presence of replay attacks.

Notations : In this paper, all adopted symbols are characterized as follows: R , R^+ are set of real numbers and non-negative real numbers respectively. N^+ is the set of positive integers. $\| n \|$ is the Euclidean norm of n . Given two different sets Ω_1 and Ω_2 , $\Omega_1 \setminus \Omega_2 = \{x \mid x \in \Omega_1, x \in \Omega_2\}$.

2. PROBLEM FORMULATION

2.1. STMPC

Given the CPS system shown in FIG. 1, the controlled system model is described by following continuous nonlinear input system:

$$\dot{x} = \phi(x,u) = f(x) + g(x)u \,, \tag{1}$$

$x \in R^n$ is the system state and $u \in R^m$ is input.

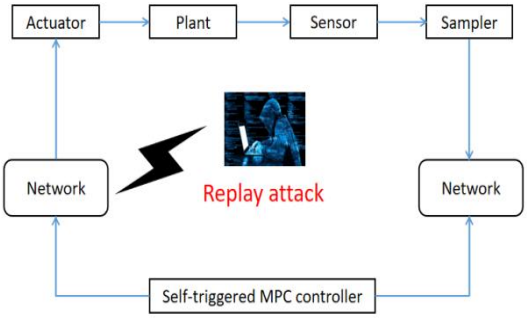


Fig. 1 STMPC

Note that the control objective of this work is: when $t \to \infty$, $x(t) \to 0$. To satisfy the ambition, first introduce Assumption 1:

Assumption 1. System $\phi(x,u)$ is Lipschitz continuous for $x \in R^n$ and exists Lipschitz constant L_ϕ .

The following optimal control problem (OCP) is considered:

$$\min_u J[x(t_k),u] = \int_{t_k}^{t_k+T_P} F[x(s),u(s)]\, ds + V_f[x(t_k+T_P)] \,, \tag{2}$$

$$s.t. \qquad \dot{x} = \phi(x,u),\ s \in [t_k, t_k+T_p] \,, \tag{3}$$

$$u(s) \in \mathcal{U} \,, \tag{4}$$

$$x(t_k+T_P) \in \Omega(\varepsilon_f) \,. \tag{5}$$

The sequence $\{ t_k \}$ represents the sampling time of MPC, T_P is the prediction horizon. $F(x,u)$ reprents the stage cost functions and $V_f(x)$ is defined as the terminal cost functions.

$\mathcal{U}$ represents set of control input constraint, which is defined in following way:

$$\mathcal{U} = \{u(s) \in R^m : \| u(s) \| \le u_{\max}, \| \dot{u}(s) \| \le K_u\} \,.$$

Moreover, $\Omega(\varepsilon_f)$ is terminal constraints:

$$\Omega(\varepsilon_f) = \{x(s) \in R^n : V_f[x(s)] \le \varepsilon_f\} \,, \tag{6}$$

where $\varepsilon_f > 0$. And, $\Omega(\bullet)$ satisfies the following assumptions:

Assumption 2. Given $\Omega(\varepsilon_f)$, there has a feedback control law $\kappa(x) \in \mathcal{U}$ satisfies:

$$\frac{\partial V_f}{\partial x}[f(x) + g(x)\kappa(x)] \le -F[x, \kappa(x)] \,, \tag{7}$$

Note that, $J^*(x)$ is defined as the optimal cost function, collected by solving OCP, and the following regions is set as MPC stable regions:

$$\Omega_V = \{x \in R^n,\ J^*(x) \le J_0\} \,, \tag{8}$$

where J_0 can be obtained by system performance[13] and $\Omega(\varepsilon_f) \in \Omega_V$.

The MPC control mentioned above is to actuate the system begins from $\Omega(\varepsilon_f) \setminus \Omega_V$ to $\Omega(\varepsilon_f)$ in a limited time. Further more, assume F and V_f satisfy the following conditions:

Assumption 3. Given α_1 and α_2, $F(x,u) \ge \alpha_1(\| x \|)$, $V_f(x) \le \alpha_2(\| x \|)$ are satisfied, where α is K_∞ function. Furthermore, $F(x,u)$ and $V_f(x)$ are Lipschitz continuous on $x \in \Omega_V$. And there exists Lipschitz constant L_F and L_{V_f} which satisfy $0 < L_F < \infty$, $0 < L_{V_f} < \infty$.

Based on the above settings, the optimal control input $u^*(s)$ and optimal state trajectory $x^*(s)$ is defined as:

$$u^*(s), x^*(s)\ \ s \in [t_k, t_k+T_P],\ x^*(t_k) = x(t_k) \,. \tag{9}$$

Based on the above OCP, in traditional MPC, only $u^*(t_k)$ is applied to the system (1). Periodic MPC needs to consume more resources compared to other control methods. For balancing the conflict between control performance and resource consumption, an effective solution scheme is to introduce a self-triggered mechanism. STMPC use the previously received data and system dynamics, predicts next triggering moment t_{k+1} at the triggering moment t_k , and apply $u^*(s)$ to

system until the t_{k+1}. Consider $u^*(s)$ as continuous input data, and transmitting continuous data in a wireless network requires wireless bandwidth, therefore, in industrial applications, continuous control samples need to be discretized and sent just N control samples U^*, which means:

$$U^* = \{u^*(t_k), u^*(t_k + \delta_1), ..., u^*(t_k + \delta_i), ...u^*(t_k + \Delta_n)\}, \quad (10)$$

that $\Delta_n = \sum_{i=1}^{N} \delta_i < T_P$, $1 \le n \le N$. Actuator applies U^* in sampling-hold mode between the triggering moment t_k and $t_k + \sum_{i=1}^{N} \delta_i$.

2.2. Replay attack

According to STMPC strategy above, U^* is packaged and transmitted through the network. During transmission, the control sample $u^*(s)$ in packet U^* may be attacked by malicious replay. Define the control signal after attack as $u_a(s)$:

$$u_a(s) = \begin{cases} u^*(s); & t_k < s < t_g \\ u^*(t_g); & t_g \le s < t_{k+1} \end{cases},$$

Define U_a as the control sequence actually obtained by the actuator after the system is attacked:

$$U_a = \{u_a(t_k), u_a(t_k + \Delta_1), ..., u_a(t_g), u_a(t_g), ...\}. \quad (11)$$

If U_a is applied directly, the system will be directly affected and even unstable. For the purpose of keeping the stability of system, it is necessary to put forward a resilient control strategy to stabilize the system. For the purpose of achieving this goal, following assumption are mentioned. In resilient controller design, the existence of Assumption 4 is reasonable, because the main work is to solve the attack response problem. Detection can be achieved by watermark or observer-based signature compensation.

Assumption 4. The controlled system can effectively detect replay attacks in network channels.

3. RESILIENT CONTROL STRATEGY

This section put forward a resilient strategy for the CPS as shown in FIG. 1 after being subjected to replay attack. The developed resilient control strategy mainly includes the following key steps:1) the self-triggered input is sampled, and key reconstruction parameter K is obtained, 2) the reconstruction parameter K and the self-triggered sequence are transmitted to the actuator through the network, and the key parameter K is extra protected, 3) the controlled system applies parameter K to reconstruction the feasible control sample to ensure system stability when a replay attack is detected by the controlled system. Before the resilient STMPC is proposed, a control sample reconstruction mechanism is first designed.

3.1. Control sample reconstruction method

If the system is attacked at t_g, the actuator constructs a continuous control sample $u'(s)$ based on control samples U_a and K:

$$u'(s) = \frac{[u^*(t_q) - u^*(t_k)]}{t_q - t_k}(s - t_k) + u^*(t_k) - Ks, \quad s \in [t_g, t_k + \Delta_n] \quad (12)$$

where $t_q = t_{g-1}$, K is a set encrypted parameter, which will be discussed in detail in subsection 3.2. At this point, (13) will be applied to system, and actual state $x(s)$ can be obtained based on (13):

$$U' = \{u^*(t_k), ..., u^*(t_q), u'(t_g), ..., u'(t_k + \Delta_n)\}. \quad (13)$$

FIG. 2 is a schematic diagram of control input under different conditions. The black curve $u^*(s)$ represents the optimal solution obtained by solving OCP problem at t_k, and the black dot represents N control samples selected from $u^*(s)$ by SFMPC. Blue curve $u_{a1}(s)$ represents the control curve after the replay attack. The red curve $u'(s)$ represents the reconstructed control sequence curve, and the red dot represents the reconstructed new control data points. It is worth noting that $t_g = t_q + \delta_4$.

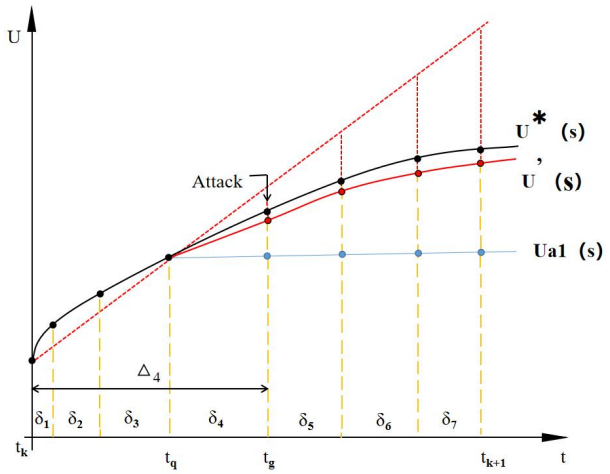


Fig. 2 Diagram of control input

3.2. Resilient STMPC Strategy

According to Lemma 1, the analytic upper bound of system state error when control data $u^*(s)$ changes to $u'(t_k + \Delta_j)$ can be obtained.

Lemma 1. The upper bound value of $\| x(t_k+\Delta_1)-x^*(t_k+\Delta_1)\|$, described as $E(\Delta_1)$, and let $t_k+\Delta_{G+1}=t_g$:

When $i=1$,

$$E(\Delta_1)=\| x(t_k+\Delta_1)-x^*(t_k+\Delta_1)\| \le L_G\Delta_u(t_k+\delta_1)e^{L_\phi\delta_1}, \quad (14)$$

When $1<i\le G$,

$$E(\Delta_i)=\| x(t_k+\Delta_i)-x^*(t_k+\Delta_i)\| \le E(\Delta_{i-1})e^{L_\phi\delta i}+L_G\Delta_u(t_k+\delta_i)e^{L_\phi\delta_i}, \quad (15)$$

where:

$$\Delta u(t_k+\delta_i)=\| \int_{t_k+\delta_{i-1}}^{t_k+\delta_i} u(t_k+\Delta_{i-1})-u^*(s)ds\|. \quad (16)$$

When $G<i\le N$,

$$E(\Delta_i)=\| x'(t_k+\Delta_i)-x^*(t_k+\Delta_i)\| \le E(\Delta_{i-1})e^{L_\phi\delta i}+L_G\Delta_q(t_k+\delta_i)e^{L_\phi\delta_i}, \quad (17)$$

where:

$$\Delta q(t_k+\delta_i)=\| \int_{t_k+\delta_{i-1}}^{t_k+\delta_i} u'(t_k+\Delta_{i-1})-u^*(s)ds\|. \quad (18)$$

Proof:

First, for $\Delta_i=\delta_1$, $s\in[t_k,t_k+\delta_1]$,

$$x(t_k+\delta_1)=x(t_k)+\int_{t_k}^{t_k+\delta_1}\phi[x(s),u^*(t_k)]\,ds,$$

$$x^*(t_k+\delta_1)=x^*(t_k)+\int_{t_k}^{t_k+\delta_1}\phi[x^*(s),u^*(s)]\,ds.$$

where $x(t_k)=x^*(t_k)$. Thus

$$E(\Delta_1)=\| x(t_k+\delta_1)-x^*(t_k+\delta_1)\| \le \int_{t_k}^{t_k+\delta_1} L_\phi\| x(s)-x^*(s)\|\,ds + L_G\Delta u(t_k+\delta_1).$$

Let

$$\Delta u(t_k+\delta_1)=\| \int_{t_k}^{t_k+\delta_1}[u(t_k)-u^*(s)ds]\|.$$

$E(\Delta_1)$ can be rewritten as:

$$\| x(t_k+\delta_1)-x^*(t_k+\delta_1)\| \le \int_{t_k}^{t_k+\delta_1} L_\phi\| x(s)-x^*(s)\|\,ds + L_G\Delta u(t_k+\delta_1).$$

Using Gronwall-Bellman inequality can acquire:

$$E(\Delta_1)=\| x(t_k+\delta_1)-x^*(t_k+\delta_1)\| \le L_G\Delta u(t_k+\delta_1)e^{L_\phi\delta_1}.$$

For $1<i\le G$, Gronwall-Bellman inequality is also used to obtain:

$$E(\Delta_i)\le E(\Delta_{i-1})e^{L_\phi\delta_i}+L_G\Delta u(t_k+\delta_i)e^{L_\phi\delta_i}.$$

For $G<i<N+1$,

$$x(t_k+\Delta_{G+1})=x(t_k+\Delta_G)+\int_{t_k+\Delta_G}^{t_k+\Delta_{G+1}}\phi[x(s),u'(t_k+\Delta_G)]\,ds,$$

$$x^*(t_k+\Delta_{G+1})=x^*(t_k+\Delta_G)+\int_{t_k+\Delta_G}^{t_k+\Delta_{G+1}}\phi[x^*(s),u^*(s)]\,ds.$$

Thus $E(\Delta_{G+1})=\| x(t_k+\Delta_{G+1})-x^*(t_k+\Delta_{G+1})\| \le E(\Delta_G)e^{L_\phi\delta_{G+1}}+L_G\Delta_q(t_k+\Delta_{G+1})e^{L_\phi\delta_{G+1}}$.

where $\Delta q(t_k+\Delta_{G+1})=\| \int_{t_k+\delta_G}^{t_k+\delta_{G+1}}[u'(t_k+\Delta_G)-u^*(s)]ds\|$.

In the same way, for $i>G+1$,

$$E(\Delta_i)=\| x(t_k+\Delta_i)-x^*(t_k+\Delta_i)\| \le E(\Delta_{i-1})e^{L_\phi\delta_i}+L_G\Delta q(t_k+\delta_i)e^{L_\phi\delta_i}.$$

Note that $\Delta u(t_k+\delta_i)$ and $\Delta q(t_k+\Delta_{G+1})$ can be obtained by online calculation.

Based on Lemma 1, parameter K is calculated in the way of the following formula:

$$E(\Delta_{N-1})e^{L_\phi\delta_N}+L_G\Delta q(t_k+\delta_N)e^{L_\phi\delta_N}=\frac{1}{L_J}\sigma_J(t_k+\delta_N), \quad (19)$$

where $\sigma_J=\gamma\int_{t_k}^{t_k+s}F[x^*(s),u^*(s)]\,ds$, $\gamma\in(0,1)$. L_J is the Lipschitz constant, and it can be seen from reference [6] that:

$$L_J=(\frac{L_F}{L_\phi}+L_{V_f})e^{(L_\phi T_p)}-\frac{L_F}{L_\phi}.$$

It is worth noting that in equation (19), $\Delta q(t_k+\delta_N)$ is a setting symbol including parameter K.

Assumption 5. It is assumed that equation (19) has a solution.

Through the above analysis, the resilient STMPC strategy is summarized as Algorithm 1 as follows.

Table. Algorithm 1

Algorithm 1.Adaptive selection algorithm
i. while $x(t_k)\notin\Omega_{\varepsilon_f}$ **do**
ii. Calculate control sample U^* by STMPC and a encrypted parameter K by formula (19).
iii. Transmit U^* and K to actuator by network.
iii. **if** replay attack is launched. **then**
iv. The controlled system obtains the control sample U' through formula (12).
v. The actuator applies the control sample U' in a zero-order holding manner.
vi. **else**
The actuator applies the sample U^* in a zero-order hold.

vii. **end if**.
viii. Pass $x_{t_{k+1}}$ to controller when advanced present state for dealing with OCP problem.
end while
The local feedback controller $K(x)$ is utilized.

It is noted that the feed back controller $K(x)$ is set at the actuator side which not participating in communications.

4. STABILITY ANALYSIS

In the sector, we analyze the stability of above algorithm.

Theorem 1. Given the system in (1), if Algorithm 1 is applied, then any state trajectory starting from $x(t_k) \in \Omega_V \setminus \Omega_{\varepsilon_f}$ will enter Ω_{ε_f} within finite time, and remain in Ω_{ε_f} for all future times.

Proof:

The proof adopts method of contradiction. First, assume: $x(t_0) \in \Omega_V \setminus \Omega_{\varepsilon_f}$ and $x(s), s > t_0$ is always outside of Ω_{ε_f}. It is that, when $t \to \infty$, the system state x still being outside the constraint Ω_{ε_f} under control of the designed algorithm. Then it proves that the controlled system can still run stably under the action of Algorithm 1 by proving that the assumption is not tenable.

Firstly, the optimization conditions based on design are:

$$J^*[x(t_{k+1})] - J^*[x(t_k)] \le (\gamma - 1) \int_{t_k}^{t_{k+1}} F[x^*(s), u^*(s)]\, ds < 0 .$$

$J^*[x(s)]$ presents the solution of the optimal cost function depended on optimal control input $u^*(s)$.

Meanwhile, $J^*[x(s)]$ is also regarded as the closed-loop Lyapunov function of system (1). Therefore, based on Lyapunov stability theory, stability can be guaranteed when $J^*[x]$ is guaranteed to decrease with triggering time t_k. Because $\Delta_n = t_{k+1} - t_k > 0$, So

$$\begin{aligned} J^*[x(t_k)] - J^*[x(t_{k-1})] &\le (\gamma - 1) \int_{t_{k-1}}^{t_k} F[x^*(s), u^*(s)]\, ds \\ &< (\gamma - 1) \int_{t_{k-1}}^{t_{k-1}+\Delta_n} \alpha_1[\alpha_2^{-1}(\varepsilon_f)]\, ds \\ &= -(1-\gamma)\alpha_1[\alpha_2^{-1}(\varepsilon_f)]\Delta_n \triangleq -\zeta < 0 \end{aligned}$$

Because $F(x,u) \ge \alpha_1(\| x \|)$, $V_f(x) \le \alpha_2(\| x \|)$, we can get $\varepsilon_f < V_f[x(t_k + \zeta)] \le \alpha_2[\| x(t_k + \zeta) \|]$. So:

$$F[x^*(s), u^*(s)] \ge \alpha_1[\| x(t_k + \zeta) \|] > \alpha_1[\alpha_2^{-1}(\varepsilon_f)] > 0$$

where $t_{k-1} < s < t_{k-1} + \Delta_i, 0 < \zeta < \Delta_i$. Then we can get:

$$J^*[x(t_k)] - J^*[x(t_{k-1})] < -\zeta$$

$$\vdots$$

$$J^*[x(t_1)] - J^*[x(t_0)] < -\zeta .$$

And summing left and right:

$$J^*[x(t_k)] < -k\zeta + J^*[x(t_0)] < -k\zeta + J_0 ,$$

that J_0 has been given in formula (8). It means that $J^*[x(t_k)] < 0$ when $k \to \infty$. It contradicts $J^*[x(t_k)] > 0$. So the above assumption is not valid. Thus, the state is proved to enters Ω_{ε_f} in a finite time.

Note that when the state reaches Ω_{ε_f}, the local control law $K(x)$ is applied. Therefore, the control goal of asymptotically stabilizing the system to the origin can be accomplished, that is, $x(t) \to 0$ when $t \to \infty$.

5. SIMULATION EXAMPLES

In this part, applied the designed algorithm to the two-position nonholonomic vehicle system to verify its effectiveness. Driving the system from its initial position to the target position is the corresponding control objective.

System equation is:

$$\begin{bmatrix} \dot{x}(t) \\ \dot{y}(t) \\ \dot{\theta}(t) \end{bmatrix} = \begin{bmatrix} \cos\theta(t) & 0 \\ \sin\theta(t) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v(t) \\ w(t) \end{bmatrix},$$

where $\chi = [x\ y\ \theta]^T$ represents variable of system state, $u = [v\ w]^T$ represents variable of control input, $[x, y]$ is the position of a vehicle, θ is the angle of the vehicle, $[v\ w]^T$ is the linear velocity and angular velocity respectively. First introduce STMPC algorithm in literature [14] to drive the system from the initial position [-5 4 -π/2] to the origin. Based on this STMPC, the controlled system is attacked by the replay attack method established in 2.3. Finally, the system is defended using the developed resilient control algorithm in Section 3. The parameters used in the simulation are described as follows: The constraint conditions is $\| v \| \le \overline{v}$ =1.5, $\| w \| \le \overline{w}$ =0.5, and the Lipschitz Constant $L_\phi = \sqrt{2}\overline{v}$, $L_G = 1.0$ [15]. Cost functions are $F = \chi^T Q \chi + u^T R u$ and $V_f = \chi^T \chi$, where $Q = 0.13 I_3$, $R = 0.05 I_2$. Set $\sigma = 0.99$, $\varepsilon_f = 0.4$, $N = 6$. The given design $\gamma = 0.99$.

As shown in FIG. 3, driven by the developed Algorithm 1 under replay attack, the running track of the vehicle (blue) and the standard STMPC algorithm without replay attack eventually tend to be stable. However, if no defensive measures are taken after the control data is maliciously tampered by subsection 2.2, the system will be in an unstable state, as shown in the red track in FIG. 3. The mark in FIG. 3 indicates that the controlled system is triggered and ought to communicate with controller in order to obtain control samples.

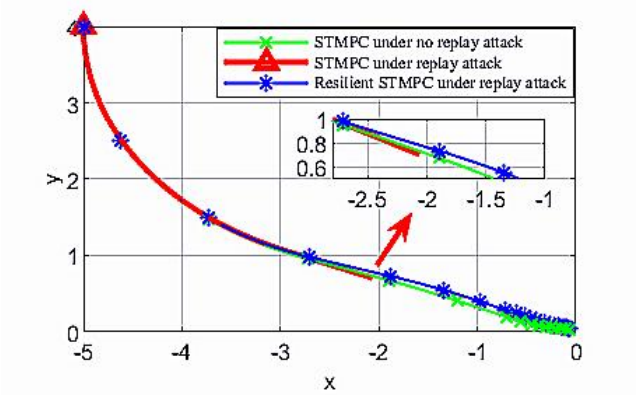


Fig. 3 Running track comparison diagram

FIG. 4 shows the comparison of triggering intervals between STMPC without replay attack and Algorithm 1under replay attack, marked in blue and green respectively. The frequency of triggering of Algorithm 1 under replay attack is not significantly increased compared to the standard STMPC under no attack.

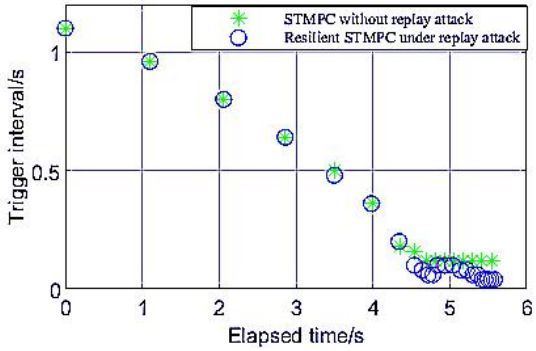


Fig. 4 Triggering interval comparison

6. CONCLUSION

In this paper, a resilient STMPC algorithm based on controlling sample reconstruction is developed, which can ensure the safety operation of the system when it is subjected to replay attacks. First, a controlling sample reconstruction method is designed based on the standard STMPC algorithm and the replay attack model, and the computation method of key parameters for the purpose of reconstructing the reconstructed samples is given. What is more, the stability of the system under the replay attack is strictly demonstrated. Finally, a nonlinear robot-based system is used to prove the validity of the developed resilient strategy.

7. ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (No.61903291), China Postdoctoral Science Foundation (No.2019M660257) and Key Research and Development Program of Shaanxi Province (No.2022NY-094).

REFERENCES:

[1] Li W F, Xie Z C, et al. Velocity-based robust fault tolerant automatic steering control of autonomous ground vehicles via adaptive event triggered network communication[J]. Mechanical Systems and Signal Processing, 2020, 143.

[2] Sun Y C, Yang G H. Robust event - triggered model predictive control for cyber - physical systems under denial - of - service attacks[J]. International Journal of Robust and Nonlinear Control, 2019, 29(14): 4797-4811.

[3] International Journal of Robust and Nonlinear Control, 2019, 29(14): 4797-4811.

[4] Mei M, Zhu D Q, Gan W Y, et al. The Tracking Control of Unmanned Underwater Vehicles Based on Model Predictive Control [J]. Control Engineering of China, 2019, 26 (10): 1917-1924.

[5] Zhao A J, Zhou M, et al. Study on Control and Optimization of Indoor Environmental Quality Based on Model Prediction[J]. Control Engineering of China, 2019, 26 (3): 570-577.

[6] Wang Y, Gai Y F, et al. Design of Intelligent and Connected Vehicle Path Tracking Controller Based on Model Predictive Control[J]. Control Engineering of China, 2019, 55 (8): 136-144+153.

[7] He N, Shi D W, et al. Self-triggered model predictive control for networked control systems based on first-order hold[J]. International Journal of Robust and Nonlinear Control, 2018, 28(4): 1303-1318.

[8] He N, Shi D W, et al. Event-Based Robust Sampled-Data Model Predictive Control: A Non-Monotonic Lyapunov Function Approach [J]. IEEE Transactions on Circuits and Systems—I: Regular Papers, 2017, 62(1): 177-189.

[9] Hashimoto K, Adachi S, Dimarogonas D V. Self-Triggered Model Predictive Control for Nonlinear Input-Affine Dynamical Systems via Adaptive Control Samples Selection[J]. IEEE Transactions on Automatic Control, 2015, 62(10): 2555-2564.

[10] Liu T, Tian J, Wang J Z, et al. Integrated Security Threats and Defense of Cyber-physical Systems[J]. Acta Automatica Sinica, 2019, 45 (1): 5-24.

[11] ASMAA A.Elsaeidy, Nishant Jagannath, et al. Replay attack detection in smart cities using deep learning[J]. IEEE Acess, 2020, 120.

[12] Giuesppe Frannze, Francesco Tedesco, et al. Resilience Against Replay Attacks：A Distributed Model Predictive Control Scheme for Networked Multi-Agent Systems[J]. IEEE JOURNAL OF AUTOMATICA SINICA, 2021, 117.

[13] Giuesppe Frannze, Francesco Tedesco, et al. Resilient Control for Cyber-Physical Systems Subject to Replay Attacks[J]. IEEE CONTROL SYSTEMS LETTERS, 2020, 97.

[14] Peng He, Jiwei Wen, et al. Model Predictive Control of Markov Jump Linear Systems an Error-based Self -triggered approach[J]. IEEE Transactions on Automatic Control, 2021, 37(8):2325-2330.

[15] Li H P, Shi Y. Event-triggered robust model predictive control of continuous-time nonlinear systems[J]. Automatica, 2014, 50(5): 1507-1513.

[16] Hashimoto K, Adachi S, Dimarogonas D V. Self-Triggered Model Predictive Control for Nonlinear Input-Affine Dynamical Systems via Adaptive Control Samples Selection[J]. IEEE Transactions on Automatic Control, 2015, 62(10): 2555-2564.