Security-based resilient event-triggered control of networked control systems under denial of service attacks

Article (Accepted Version)

Security-based Resilient Event-triggered Control of Networked Control Systems under Denial of Service Attacks

Hongtao Sun[1], Chen Peng[1], Weidong Zhang[2], Taicheng Yang[3], Zhiwen Wang[4]

[1] *Department of Automation, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China, 200072.*

[2] *Department of Automation, Shanghai JiaoTong University, Shanghai, China, 200240*

[3] *Department of Engineering and Design, University of Sussex, Brighton BN1 9QT, UK*

[4] *College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou, China, 730050*

Abstract

This paper is concerned with the security control problem of the networked control system (NCSs) subjected to denial of service (DoS) attacks. In order to guarantee the security performance, this paper treats the influence of packet dropouts due to DoS attacks as a uncertainty of triggering condition. Firstly, a novel resilient triggering strategy by considering the uncertainty of triggering condition caused by DoS attacks is proposed. Secondly, the event-based security controller under the resilient triggering strategy is designed while the DoS-based security performance is preserved. At last, the simulation results show that the proposed resilient triggering strategy is resilient to DoS attacks while guaranteeing the security performance.

Keywords: Networked control systems, Security control, Resilient Event-triggering strategy, Denial of service

☆Corresponding author: Chen Peng, E-mail:c.peng@shu.edu.cn

1. Introduction

In the past few decades, considerable research effects have been made on the control issues of the NCSs where physical process, sensors and actuators are linked together through communication network [1]. Modeling, analysis and synthesis for the NCSs have been received great attention with its extensively applied in many potential areas such as internet of things (IoT), smart grids and unmanned aerial vehicles [2, 3].

Because of the deep integration of physical systems and networks, communication resources, as the medium of signal transmission, become more and more important for control implementations and many works devote themselves to save network bandwidth and reduce communication load [4, 5]. With the development of digital circuits and networked control technologies, the event-based control scheme has been paid more and more attentions from the control engineering community [6, 7, 8, 9, 10]. This event-based strategy implement their control actions as they need which lead to a less communication consumption. Recent years has witnessed significant advances on the event-triggered control scheme and many results are discussed such as [11, 12, 13] and there references in.

Obviously, these event-triggered control strategies are sensitive to sampled-data while reducing the quantities of communication. These exchanged event-based data in the NCSs without security protection is easy attacked by malicious adversaries [14, 15, 16] and this lead to time delay, packet dropouts and disorder problems. Although such problems have been studied from different perspectives for the traditional NCSs, they may be not suitable for safety constraint scenarios. Hence,the NCSs are more and more vulnerable to various malicious attacks due to the ever-increasing openness of communication networks [17]. Recently, there are some works have been drawn attention to this raw field such as [18, 19, 20, 21] and there references in and the most studies focus on two common attack types, namely, DoS attacks [22, 23, 24, 25, 26] to communication networks and physical attacks [27, 28, 29, 30] to industrial process.

In this paper, we will discuss the DoS attacks for the NCSs. As well known, time delays would be caused by DoS attacks. Although periodic attacks [23], Bernoulli process [31, 24, 26], (hiden) Markov process [32, 33], zero-sum stochastic game [34], time delay approach [35, 36], switched system model [24] are often used to modeling the effects of DoS attacks in the NCSs, the time delay caused by DoS attacks is different from traditional ones caused by network uncertainties. An DoS attacker may not follow any deterministic manners or specific rules such as periodic behavior or probability distribution. Based on this view point, the time delay approach is more suitable for describing the DoS attack behaviors. By considering the energy-constraint of DoS attacks, the less conservative for the time delay, the longer DoS duration can be tolerated for the system. Therefore, it is necessary to design a security controller to tolerant a more larger time delay or packet dropouts. For triggered-packet dropouts, Sun et. al [37] investigate the stability of event-triggered control system subject to one-step packet dropout with the concept of average dwell time in switched systems. Dimarogonas et. al [38] proposed a non-monotonic approach to cope with the triggered-packet dropouts case. Perisis et. al [25] characterize the relationship between frequency and duration of DoS attacks while preserving ISS stability by estimating the system evolution with/without DoS attacks. Peng et. al [36] proposed a co-design method for a resilient event-triggering strategy to tolerant a degree of packet dropouts by adjusting the triggering parameter. Girard [39] proposed dynamic triggering mechanism for event-triggered control when the event-triggered condition is violated. When a larger time delay caused by DoS attacks, on the one hand, it is very conservative for solving LMIs and hard to design a larger time delay tolerable controller, on the other hand, it is also not applicable for changing controller when the system is running although such a larger time delay tolerable controller can be designed.

In fact, there always exist such a time delay caused by DoS attacks that the system can not be tolerated for a given controller. Then the system have to degrade running under this circumstance. By considering that the DoS attacks will lead to lost of security performance through altering the previous triggering condition, the main contributions of this technical note can be summarized as

- According to the alteration of triggering condition due to DoS attacks, a novel security-performance-based resilient triggering strategy is proposed under the DoS attack scenario.
- The corresponding security performance analysis and event-triggered controller design under the proposed resilient triggering strategy are discussed in order to guarantee the NCSs security performance.

The reminder of this paper is organised as follows. Section 2 gives some preliminaries of event-triggered control framework as well as the proposed resilient triggering strategy under DoS attack scenario. The main results are presented in Section 3 where sufficient conditions are derived to guarantee the security performance under the DoS attack. The Section 4 presents the security controller design under the resilient triggering strategy and some simulation results are shown in the following Section 5. The last Section 6 concludes this paper.

2. Preliminaries and Problem Formulation

2.1. System framework

Consider a class of continuous time linear dynamics with exogenous disturbances as follows

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + B_w w(t) \\ z(t) = Cx(t) + Du(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $w(t) \in \mathcal{L}_2[0, \infty)$ and $z(t) \in \mathbb{R}^p$ are state input vector, input vector, disturbance and regulated output vector, respectively. A, B, B_w, C, D are constant matrices with compatible dimensions. The initial condition of the system (1) is given by $x(t_0) = x_0$.

The NCS framework is shown as in Fig. 1 where the control implementation are relay on a shared communication network. Owing to the opening of network, there are also some malicious attacks will imposed on the NCSs. It easy

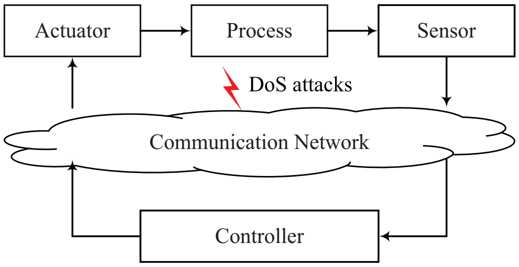

Figure 1 Diagram of the NCSs under DoS attacks

to see that the DoS attacks will affect both measurement channel (sensor-to-controller) and control channel (controller channel) and one of them attacked will block the control update.

Suppose that the sensor is time triggered with sampling period h and its sampling sequence is described by the set $\mathcal{S}_1 = \{0, h, 2h, \cdots kh\}, k \in \mathbb{N}$. By collecting these sampling data, the event trigger will transmit such sample data $x(kh)$ if the pre-designed triggering condition is violated. We denote these triggered sampling sequence as the set $\mathcal{S}_2 = \{0, t_1h, t_2h, \cdots t_kh\}$. Obviously, $\mathcal{S}_2 \subset \mathcal{S}_1$. Then the actuators will implement their control actions with these successfully transmitted sampled data, namely,

$$u(t) = Kx(t_k), t \in [t_kh, t_{k+1}h) \tag{2}$$

However, the transmission failure will occur for these triggered packets when they are suffering from DoS attacks. So, the control action will hold until the DoS ceased and this leads to unexpected control performance.

2.2. Security-oriented Resilient Triggering Strategy

In engineering practice, DoS attacks are hard to defense because it is often posterior or unpredictable. Therefore, it is impracticable to change controller or sampling frequency temporarily to tolerate such a attack. On the one hand, the DoS attacks will caused bad control performance, but on the other hand, not all DoS attacks will lead to the system crash. That is, the NCSs may run in degrade model with a certain security performance when DoS attacks happened.

That is, the actual error between the value of the last successful transmitted state and the value of the current state is beyond the expected range due to DoS attacks. So, we will focus on the excessive error which caused the alteration of the triggering condition. As shown in Fig. 2, there are three work models

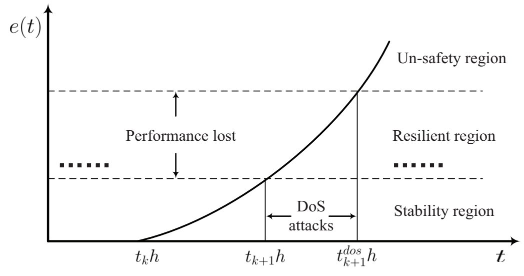

Figure 2 Diagram of the NCSs under DoS attacks

according to the event-based triggering conditions

- Safety region. In this region, there are no DoS attacks and every triggered packets can be transmitted successfully.
- Resilient region. In this region, there are DoS attacks and an extra triggered error is generated. However, this error can be tolerable for the NCSs.
- Un-safety region. In this region, there are DoS attacks and an intolerable error for the NCSs is generated.

In order to describe the performance lost caused by DoS attacks in more detail, it is necessary to illustrate the proposed resilient triggering strategy based on the security-based performance. For clear exposition, we first denote the last successful control update time instant as $t_k h$ and the future transmitted sampling instant according to the security event-triggered condition (no extra triggered error) as $t_{k+1}h$. However, $t_{k+1}h$ may be prolong to $t^{dos}_{k+1}h$ ($t^{dos}_{k+1}h > t_{k+1}h$) due to DoS attack with limited energy. If denote $i_k h$ as the current sampling instant during the k-th time interval, then the following expression $\xi(i_k h)$ is given to indicate an DoS attack behavior for each sampling instant

$$\xi(i_k h) = \begin{cases} 1 & \text{DoS attack} \\ 0 & \text{No DoS attack} \end{cases} \tag{3}$$

In general, one can launch their DoS attacks at any time but limit duration. Therefore, we can described the limited energy of DoS attacks by

$$\Delta^{dos}_{t_{k+1}h} = t^{dos}_{k+1}h - t_{k+1}h \tag{4}$$

and

$$\Delta^{dos}_{t_{k+1}h} \leq \Delta_{dos} \tag{5}$$

where Δ_{dos} represents the maximum duration of DoS attacks.
Let

$$e(i_k h) = x(i_k h) - x(t_k h) \tag{6}$$

where $e(i_k h)$ represent the error between the value of process state $x(t_k h)$ at the last successful control update and the value of process state $x(i_k h)$ at the current time.
In order to record the pre-designed triggered instant $t_{k+1}h$ and $x(t_{k+1})$, an buffer is needed for the event-trigger. Then, the extra error due to DoS attacks can be calculated by

$$e^{dos}(i_k h) = x(i_k h) - x(t_{k+1}h) \tag{7}$$

where $e^{dos}(i_k h)$ represent the error between the value of process state $x(t_{k+1}h)$ according to previous triggering condition and the value of process state $x(i_k h)$ at the current time. Obviously, the introduction of error $e^{dos}(i_k h)$ will lead to a bad control performance, even security problem. Based on the above analysis, we will illustrate our proposed security-orient resilient triggering strategy as follows

$$\begin{aligned} t^{dos}_{k+1}h =& t_k h + \min_t \{t \wedge i_k h | \delta x^T(t_k)\Phi x(t_k) - e^T(i_k h)\Phi e(i_k h) \\ & + \xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h}) \leq 0\} \end{aligned} \tag{8}$$

where $\Upsilon(\Delta^{dos}_{t_{k+1}h})$ represent the variation of triggering condition with $\Upsilon(\Delta^{dos}_{t_{k+1}h}) = (e^{dos}(i_kh))^T\Phi e^{dos}(i_kh)$ due to DoS attack.

According to (5), one can obtain that the uncertain of triggering condition should be constrained by limited energy of DoS attacks, namely,

$$\Upsilon(\Delta^{dos}_{t_{k+1}h}) \leq \Upsilon \tag{9}$$

In addition, we can divide the holding interval of the $t \in \mathcal{I}$ into subsets $\mathcal{I}_\ell = [i_kh + \tau_{i_k}, i_kh + h + \tau_{i_k+1})$ with $\mathcal{I} = \cup\mathcal{I}_\ell$ according to [40], and the delay version of system can be constructed for every two successfully transmitted instants by defining $\eta(t) \triangleq t - i_kh$. Then, the controller can be transformed into

$$u(t) = K(x(t - \eta(t)) - e(i_kh)) \tag{10}$$

and the actual control action with sample-error-dependent model is given as follows

$$\begin{cases} \dot{x}(t) = Ax(t) + BK(x(t - \eta(t)) - e(i_kh)) + B_w w(t) \\ z(t) = Cx(t) + DK(x(t - \eta(t)) - e(i_kh)), t \in \mathcal{I}_\ell \end{cases} \tag{11}$$

Remark 1: We refer to an effective DoS attack as the fact that may prevent control update from being executed at desired time. In fact, the control performance lost is caused by this triggering variation (9) due to DoS attacks. In order to indicate the maximum allowable performance lost for control system, the triggering variation $\Upsilon(\Delta^{dos}_{t_{k+1}h})$ should be limited by (9) for the control system. Noticed that if $\xi(i_kh) = 1$ for $t \in (t_kh, t_{k+1}h)$, the DoS attacks will not make any difference to control update. Likewise, if $\xi(i_kh) = 1$ for $t \in (t_{k+1}h, t^{dos}_{k+1}h)$, this implies there are triggered packets dropped by the DoS attacker with its duration $\Delta^{dos}_{t_{k+1}h}$ and this would to the extra triggering error $\Upsilon(\Delta^{dos}_{t_{k+1}h})$. If $\xi(i_kh) = 0$ for $t \in (t_{k+1}h, t^{dos}_{k+1}h)$, there is no effective DoS attacks and the event triggering strategy will degenerate into the common static triggering condition such as in [40].

2.3. Control objectives

Take the variation of triggered condition caused by DoS attacks into consideration, the problem of interest is that of finding a appropriate control gain under the above resilient triggering strategy (8) while ensuring a certain security performance. In detail, the following two states are shown to reflect our control goals

1. When there are no DoS attacks, the system (11) is asymptotically stable with H_∞ performance.
2. When there are DoS attacks, the security performance with uniformly ultimately bounded is achieved, i.e. the performance lost $||L(x(t))|| \leq \mathcal{B}$.

Here, $||L(x(t))||$ is the performance lost due to DoS attacks with its upper bound $\mathcal{B}$.

3. security-orient analysis under DoS attacks

In this section, the security performance analysis are given by some mathematical derivation. The following Proposition 1 shows that the uncertain of triggering condition with extra error will arouse a large time delay.

Proposition 1. *Let $\Upsilon(\Delta^{dos}_{t_{k+1}h}) > 0$ be the control performance lost under DoS attacks. Then $t_{k+1}h \leq t^{dos}_{k+1}h$ for the resilient triggering rule in (8).*

Proof: Let $\zeta^T(i_kh)\Phi\zeta(i_kh) = \delta x^T(t_k)\Phi x(t_k) + \Upsilon(\Delta^{dos}_{t_{k+1}h})$ with $\Upsilon(\Delta^{dos}_{t_{k+1}h}) \geq 0$. Assume that $t_{k+1}h > t^{dos}_{k+1}h$, then

$$\delta x^T(t_k)\Phi x(t_k) - e^T(i^{dos}_k h)\Phi e(i^{dos}_k h) > 0 \tag{12}$$

However, recalling the prescribed resilient event-triggering condition in (8), the following inequality

$$\begin{aligned} 0 &\geq \Upsilon(\Delta^{dos}_{t_{k+1}h}) + \delta x^T(t_k)\Phi x(t_k) - e^T(i^{dos}_k h)\Phi e(i^{dos}_k h) \\ &\geq \delta x^T(t_k)\Phi x(t_k) - e^T(i^{dos}_k h)\Phi e(i^{dos}_k h) \end{aligned} \tag{13}$$

will make a contradiction with (12). Therefore, we can easily obtained that $t_{k+1}h \leq t^{dos}_{k+1}h$.

Subsequently, we will carry out the robust H_∞ and security performance analysis for the NCSs subjected to DoS attacks and the result is shown by the following Theorem 1.

Theorem 1. *For some given positive constants h, $\eta_m \geq 0$, $\eta_M(\geq \eta_m)$ and a controller K, if there exist real matrices $P > 0$, $\Phi > 0$, $Q_i > 0$, $R_i > 0$ $(i = 1, 2)$ and S of appropriate dimensions such that*

$$\begin{bmatrix} Z_2 & S \\ S^T & Z_2 \end{bmatrix} > 0 \quad , \quad \Xi = \begin{bmatrix} \Xi_{11} & \Xi_{12} \\ * & \Xi_{22} \end{bmatrix} < 0 \tag{14}$$

where $\Xi_{22} = diag[-Z_1^{-1}, -Z_2^{-1}, -R^{-1}, -I]$,

$$\Xi_{11} = \begin{bmatrix} \varphi_{11} & Z_1 & \varphi_{13} & 0 & -PBK & PB_w \\ * & \varphi_{22} & \varphi_{23} & S & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & -\delta\Phi & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & -\Phi + \delta\Phi & 0 \\ * & * & * & * & * & -\gamma^2 I \end{bmatrix}$$

and

$$\Xi_{12} = \begin{bmatrix} \eta_m A^T & \eta A^T & \eta_M A^T & C^T \\ 0 & 0 & 0 & 0 \\ \eta_m (BK)^T & \eta (BK)^T & \eta_M (BK)^T & (DK)^T \\ 0 & 0 & 0 & 0 \\ -\eta_m (BK)^T & -\eta (BK)^T & -\eta_M (BK)^T & -(DK)^T \\ \eta_m B_w^T & \eta B_w^T & \eta_m B_w^T & 0 \end{bmatrix}$$

with

$\eta = \eta_M - \eta_m$

$\varphi_{11} = A^T P + PA + Q_1 - Z_1 - \frac{\pi^2}{4} R$

$\varphi_{13} = PBK + \frac{\pi^2}{4} R + \delta\Phi$

$\varphi_{22} = Q_2 - Q_1 - Z_1 - Z_2$

$\varphi_{23} = Z_2 - S$

$\varphi_{33} = -2Z_2 + S + S^T - \frac{\pi^2}{4} R + \delta\Phi$

$\varphi_{34} = Z_2 - S$

$\varphi_{44} = -Z_2 - Q_2$

Then, under the resilient triggering strategy (8), the system (11) is with the following property

- *When there are no DoS attacks, the system (11) is asymptotic stable with H_∞ performance.*
- *When there are DoS attacks, the security performance with uniformly ultimately bounded $||x(t)|| \leq \sqrt{\frac{V(0)+\frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho}}{\lambda(P)}}$ is achieved with performance lost $\mathcal{B} = \{||L(x(t))|| \leq \sqrt{\frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho\lambda(P)}}\}$.*

where ρ is related to Ξ and $\lambda(P)$ is the minimum eigenvalue of P.

Proof: Firstly, we consider the following candidate Lyapunov-Krasovskii function $V_x(t; x(t))$ such that

$$V_x(t; x(t)) = V_1(t; x(t)) + V_2(t; x(t)) + V_3(t; x(t)) + V_4(t; x(t)) \tag{15}$$

where

$$\begin{aligned}
V_1(t; x(t)) =& x^T(t)Px(t) \\
V_2(t; x(t)) =& \int_{t-\eta_m}^{t} x^T(s)Q_1x(s)ds + \int_{t-\eta_M}^{t-\eta_m} x^T(s)Q_2x(s)ds \\
V_3(t; x(t)) =& \eta_m \int_{-\eta_m}^{0}\int_{t+\theta}^{t} \dot{x}^T(s)Z_1\dot{x}(s)dsd\theta + \\
& (\eta_M - \eta_m)\int_{-\eta_M}^{-\eta_m}\int_{t+\theta}^{t} \dot{x}^T(s)Z_2\dot{x}(s)dsd\theta \\
V_4(t; x(t)) =& \eta_M^2 \int_{i_k h}^{t} \dot{x}^T(s)R\dot{x}(s)ds \\
& -\frac{\pi^2}{4}\int_{i_k h}^{t} [x(s) - x(i_k h)]^T R[x(s) - x(i_k h)]ds
\end{aligned}$$

Then, taking the time derivative along the trajectory of system (11) yields

$$\begin{aligned}
\dot{V}_1(t; x(t)) =& 2x^T(t)P[Ax(t) + BKx(t - \eta(t)) \\
& - BKe(i_k h) + B_w w(t)]
\end{aligned} \tag{16}$$

$$\begin{aligned}
\dot{V}_2(t; x(t)) =& x^T(t)Q_1x(t) - x^T(t - \eta_M)Q_2x(t - \eta_M) + \\
& x^T(t - \eta_m)(Q_2 - Q_1)x(t - \eta_m)
\end{aligned} \tag{17}$$

$$\begin{aligned}\dot{V}_3(t;x(t)) =&\dot{x}^T(t)(\eta_m^2 Z_1 + (\eta_M - \eta_m)^2 Z_2)\dot{x}(t)\\ &- \eta_m \int_{t-\eta_m}^{t} \dot{x}^T(s) Z_1 \dot{x}(s) ds\\ &- (\eta_M - \eta_m) \int_{t-\eta_M}^{t-\eta_m} \dot{x}^T(s) Z_2 \dot{x}(s) ds\end{aligned} \tag{18}$$

$$\begin{aligned}\dot{V}_4(t;x(t)) =& -\frac{\pi^2}{4}[x(t) - x(t-\eta(t))]^T R[x(t) - x(t-\eta(t))]\\ &+\eta_M^2 \dot{x}^T(t) R \dot{x}(t)\end{aligned} \tag{19}$$

By using Jessen inequality, the following relationship hold

$$\begin{aligned}&-\eta_m \int_{t-\eta_m}^{t} \dot{x}^T(s) Z_1 \dot{x}(s) ds \leq\\ &- [x(t) - x(t-\eta_m)]^T Z_1 [x(t) - x(t-\eta_m)]\end{aligned} \tag{20}$$

Since $\begin{bmatrix} Z_2 & S \\ S^T & Z_2 \end{bmatrix} > 0$, it follows that

$$\begin{aligned}&- (\eta_M - \eta_m) \int_{t-\eta_M}^{t-\eta_m} \dot{x}^T(s) Z_2 \dot{x}(s) ds \leq\\ &- [x(t-\eta_m) - x(t-\eta(t)]^T Z_2 [x(t-\eta_m) - x(t-\eta(t)]\\ &- [x(t-\eta(t)) - x(t-\eta_M)]^T Z_2 [x(t-\eta(t)) - x(t-\eta_M)]\\ &+ 2[x(t-\eta_m) - x(t-\eta(t)]^T S [x(t-\eta(t)) - x(t-\eta_M)]\end{aligned} \tag{21}$$

Define $\chi^T(t) = [x(t), x(t-\eta_m), x(t-\eta(t)), x(t-\eta_M), e(i_k h), w(t)]$ for the augmented dynamical system given by (11). Thus, substituting (16)-(19) into (15), taking (20) and (21) into account, we can find that

$$\frac{d}{dt}V(t;x(t)) \leq \chi^T(t)[\Xi_1 + \Gamma_1^T(\eta_m^2 Z_1 + \eta_M^2 R(\eta_M - \eta_m)^2 Z_2)\Gamma_1]\chi(t) \tag{22}$$

where

$\Gamma_1 = [A, 0, BK, 0, -BK, B_w]$

and

$$\Xi_1 = \begin{bmatrix} \varphi_{11} & Z_1 & \varphi_{13} & 0 & -PBK & PB_w \\ * & \varphi_{22} & \varphi_{23} & S & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & 0 & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 \end{bmatrix}$$

with

$\varphi_{11} = A^TP + PA + Q_1 - Z_1 - \frac{\pi^2}{4}R$

$\varphi_{13} = PBK + \frac{\pi^2}{4}R$

$\varphi_{22} = Q_2 - Q_1 - Z_1 - Z_2$

$\varphi_{23} = Z_2 - S$

$\varphi_{33} = -2Z_2 + S + S^T - \frac{\pi^2}{4}R$

$\varphi_{34} = Z_2 - S$

$\varphi_{44} = -Z_2 - Q_2$

In what follows, we consider the robust H_∞ performance for the studied system with external disturbance. Recalling the fact that $||z(t)|| \leq \gamma||w(t)||$, it is easily to see that

$$\frac{d}{dt}V(t;x(t)) + z^T(t)z(t) - \gamma w^T(t)w(t) \leq 0 \tag{23}$$

Further,

$$\begin{aligned} \frac{d}{dt}V(t;x(t)) \leq \chi^T(t)[\Xi_2 + \Gamma_1^T(\eta_m^2 Z_1 + \eta_M^2 R + \\ (\eta_M - \eta_m)^2 Z_2 + \eta_M^2 R)\Gamma_1 + \Gamma_2^T\Gamma_2]\chi(t) \end{aligned} \tag{24}$$

where $\Gamma_2 = [C, 0, DK, 0, -DK, 0, 0]$ and

$$\Xi_2 = \begin{bmatrix} \varphi_{11} & Z_1 & \varphi_{13} & 0 & -PBK & PB_w \\ * & \varphi_{22} & \varphi_{23} & S & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & 0 & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & 0 & 0 \\ * & * & * & * & * & -\gamma^2 \end{bmatrix}$$

with

$\varphi_{11} = A^TP + PA + Q_1 - Z_1 - \frac{\pi^2}{4}R$

$\varphi_{13} = PBK + \frac{\pi^2}{4}R$

$\varphi_{22} = Q_2 - Q_1 - Z_1 - Z_2$

$\varphi_{23} = Z_2 - S$

$\varphi_{33} = -2Z_2 + S + S^T - \frac{\pi^2}{4}R$

$\varphi_{34} = Z_2 - S$

$\varphi_{44} = -Z_2 - Q_2$

It is clear that

$$\Xi_2 + \Gamma_1^T(\eta_m^2 Z_1 + (\eta_M - \eta_m)^2 Z_2)\Gamma_1 + \Gamma_2^T\Gamma_2 < 0 \tag{25}$$

and this means that there is a positive scalar ε such that $\frac{d}{dt}V(t;x(t)) < ||\chi(t)||^2 < -\varepsilon||x(t)||$. Therefore, one can conclude that the system (11) is asymptotically stable and H_∞ performance of the studied system.

At last, considering the resilient triggering condition in (8), it is clear that

$$e_{i_kh}^T(t)\Phi e_{i_kh}(t) \leq \delta x^T(t_k)\Phi x(t_k) + \xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos}) \tag{26}$$

thus, we obtain that

$$\begin{aligned} \frac{d}{dt}V(t;x(t)) \leq& \frac{d}{dt}V(t;x(t)) + \xi_{i_kh}(t)\Upsilon(\Delta_{t_{k+1}h}^{dos}) + \delta x^T(t_k)\Phi x(t_k) - e_{i_kh}^T(t)\Phi e_{i_kh}^T(t) \\ \leq& \chi^T(t)\Xi\chi^T(t) + \xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos}) \end{aligned} \tag{27}$$

where Ξ is defined in (14).

Because of $\Xi < 0$, there must be a appropriate positive ρ such that $\chi^T(t)\Xi\chi^T(t) \leq -\rho V(t)$. From (27),

$$\frac{d}{dt}V(t;x(t)) \leq -\rho V(t) + \xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos}) \tag{28}$$

Multiply $e^{\rho t}$and integral on both sides of (28), then

$$\begin{aligned} V(t) \leq& e^{\rho t}V(0) + \frac{\xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos})}{\rho}(1 - e^{-\rho t}) \\ \leq& V(0) + \frac{\xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos})}{\rho} \end{aligned} \tag{29}$$

It is clear that

$$x^T(t)Px(t) \leq V(t) \leq V(0) + \frac{\xi(i_kh)\Upsilon(\Delta_{t_{k+1}h}^{dos})}{\rho} \tag{30}$$

So,

$$||x(t)|| \leq \sqrt{\frac{V(0) + \frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho}}{\lambda(P)}} \tag{31}$$

where $\lambda(P)$ is the minimum eigenvalue of P.

Obviously, the performance lost is only related to the last term of (30) and it satisfy that

$$\mathcal{B} \in \{L(x(t)) : ||L(x(t))|| \leq \sqrt{\frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho\lambda(P)}}\} \tag{32}$$

with $\mathcal{B} = \sqrt{\frac{\xi_{i_k h}(t)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho\lambda(P)}}$

Remark 2: Theorem 1 shows that the security of network would affect the control performance of the NCSs. In fact, we can see that the control performance is DoS-depended from (32). The bigger $\Upsilon(\Delta^{dos}_{t_{k+1}h})$, the more performance lost. In addition, the performance is also related to parameter ρ. The bigger ρ, the less performance lost. As well known, ρ is regard to the converge rate of the system. Intuitively, a fast converge rate will be more robust to DoS attack.

4. Security Controller Design under the Resilient Triggering Strategy

In this section, the event-based controller under the proposed resilient triggering is discussed. Based on Theorem. 1, we found that only the term Ξ is related to controller K. So, the following Theorem 2 is used to controller design in order to achieve the above two goals.

Theorem 2. *For some given positive constants h, $\eta_m \geq 0$, $\eta_M(\geq \eta_m)$, if there exist real matrices $\overline{P} > 0$, $\overline{\Phi} > 0$, $\overline{Q}_i > 0$, $\overline{Z}_i > 0$ $(i = 1, 2)$ and $\overline{S}$ of appropriate dimensions such that*

$$\begin{bmatrix} \overline{Z}_2 & \overline{S} \\ * & \overline{Z}_2 \end{bmatrix} > 0, \quad \Xi = \begin{bmatrix} \overline{\Xi}_{11} & \overline{\Xi}_{12} \\ * & \overline{\Xi}_{22} \end{bmatrix} < 0 \tag{33}$$

where $\Xi_{22} = diag[\overline{Z}_1 - 2X, \overline{Z}_2 - 2X, \overline{R}_1 - 2X, -I]$,

$$\Xi_{11} = \begin{bmatrix} \varphi_{11} & \overline{Z}_1 & \varphi_{13} & 0 & -BY & PB_w \\ * & \varphi_{22} & \varphi_{23} & \overline{S} & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & -\delta\overline{\Phi} & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & -\overline{\Phi} + \delta\overline{\Phi} & 0 \\ * & * & * & * & * & -\gamma^2 I \end{bmatrix}$$

and

$$\Xi_{12} = \begin{bmatrix} \eta_m A^T & \eta A^T & \eta_M A^T & C^T \\ 0 & 0 & 0 & 0 \\ \eta_m (BY)^T & \eta (BY)^T & \eta_M (BY)^T & (DY)^T \\ 0 & 0 & 0 & 0 \\ -\eta_m (BY)^T & -\eta (BY)^T & -\eta_M (BY)^T & -(DY)^T \\ \eta_m B_w^T & \eta B_w^T & \eta_m B_w^T & 0 \end{bmatrix}$$

with

$\eta = \eta_M - \eta_m$

$\overline{\varphi}_{11} = X\overline{A}^T + AX + Q_1 - \overline{Z}_1 - \frac{\pi^2}{4}\overline{R}$

$\overline{\varphi}_{13} = BY + \frac{\pi^2}{4}\overline{R} + \delta\overline{\Phi}$

$\overline{\varphi}_{22} = \overline{Q}_2 - \overline{Q}_1 - \overline{Z}_1 - \overline{Z}_2$

$\overline{\varphi}_{23} = \overline{Z}_2 - \overline{S}$

$\overline{\varphi}_{33} = -2\overline{Z}_2 + \overline{S} + \overline{S}^T - \frac{\pi^2}{4}\overline{R} + \delta\overline{\Phi}$

$\overline{\varphi}_{34} = \overline{Z}_2 - \overline{S}$

$\overline{\varphi}_{44} = -\overline{Z}_2 - \overline{Q}_2$

then, the controlled system (11) can be secured by $K = YX^{-1}$ *under the resilient triggering strategy (8), namely,*

- *When there are no DoS attacks, the system (11) is asymptotically stable with* H_∞ *performance.*
- *When there are DoS attacks, the security performance with uniformly ultimately bounded* $||x(t)|| \leq \sqrt{\frac{V(0) + \frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}} h)}{\rho}}{\lambda(P)}}$ *and the performance lost*

$$\mathcal{B} \in \{L(x(t)) : ||L(x(t))|| \leq \sqrt{\frac{\xi(i_k h)\Upsilon(\Delta^{dos}_{t_{k+1}h})}{\rho\lambda(P)}}\}$$ *is achieved.*

Proof: Define $X = P^{-1}$, $\overline{Q}_i = XQ_iX$, $\overline{Z}_i = XZ_iX$ $(i = 1, 2)$, $\overline{S}_i = XSX$, $\overline{\Phi}_i = X\Phi X$ and $Y = KX$. Then pre- and post- multiplying both sides of left term of inequality with $diag[X, X]$ and right term of inequality with $diag[X, X, X, X, X, I, X, X, X, I]$ for the second condition in (14), we can arrive at the second condition in Theorem 2 by using the fact that $-HG^{-1}H \leq G-2H$ for appropriate matrices to deal with the non-linear terms. Then the system (11) is asymptotically stable with H_∞ performance index γ for the disturbance attenuation when there are no DoS attacks. Based on the designed controller, the second goal can be easily obtained.

Based on the above the designed controller, we will describe the system workflow as the following Fig.3. In fact, the controller K, δ and Φ can be designed according to [40]. Once there parameters are given, the system will be run in an excepted performance.

But the error $e(i_kh)$ will keep increasing regardless the $e^T(i_kh)\Phi e(i_kh) > \delta x^T(t_k)\Phi x(t_k)$ or not when there are DoS attacks. However, when $e^T_{i_kh}(t)\Phi e_{i_kh}(t) >$

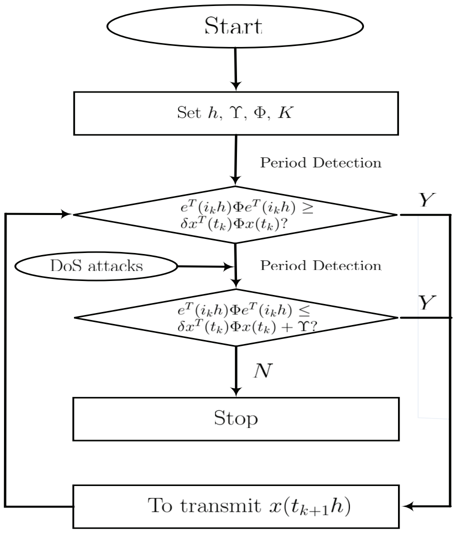
Start
Set h, Υ, Φ, K
Period Detection
$e^T(i_kh)\Phi e^T(i_kh) \geq \delta x^T(t_k)\Phi x(t_k)$?
Y
DoS attacks
Period Detection
$e^T(i_kh)\Phi e^T(i_kh) \leq \delta x^T(t_k)\Phi x(t_k) + \Upsilon$?
Y
N
Stop
To transmit $x(t_{k+1}h)$

Figure 3 Workflow of the NCSs under DoS attacks

$\delta x^T(t_k)\Phi x(t_k)+\Upsilon(\Delta^{dos})$, the state must be transmitted. If not, an un-tolerable performance lost will be caused and this may be lead to the system crash.

5. Illustrative example

In this section, a simulation example is used to illustrate the security control method under the resilient triggering strategy.

Let us consider the pendulum example borrowed from [40] with its plant dynamics given by

$$\dot{x}(t)=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{mg}{M} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -\frac{g}{l} & 0 \end{bmatrix} x(t)+\begin{bmatrix} 0 \\ \frac{1}{M} \\ 0 \\ -\frac{1}{Ml} \end{bmatrix} u(t)+\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} w(t) \tag{34}$$

where $M=10$ is the cart mass, $m=1$ is the mass of the pendulum bob, $l=3$ is the length of the pendulum arm and $g=10$ is the gravitational acceleration. For simplicity and clearly, the external disturbance is neglected here and the initial state is $x(0)=\begin{bmatrix} 0.98 & 0 & 0.2 & 0 \end{bmatrix}^T$. Taking the sampling period $h=0.01s$. It is easy to see that the system is unstable when there are no control input. According to the controller design method in this paper, we choose the following parameters as $\delta=0.1$, $\gamma=200$, $\eta_1=0$ and $\eta_2=0.05$. Then the corresponding feedback controller and the triggered matrix are obtained as

$$K=\begin{bmatrix} 2.9972 & 11.0572 & 297.9713 & 166.0562 \end{bmatrix} \tag{35}$$

and

$$\overline{\Phi}=\begin{bmatrix} 1.4640 & -3.5258 & -7.7964 & 14.0335 \\ -3.5258 & 19.8779 & 39.2554 & -71.6757 \\ -7.7964 & 39.2554 & 79.5624 & -144.9050 \\ 14.0335 & -71.6757 & -144.9050 & 263.9816 \end{bmatrix} \tag{36}$$

Case I: No DoS attacks

When there are no DoS attacks, the response of system (34) with the designed controller under the event-triggered communication scheme are depicted in Fig.4

and the release instants and release intervals for the event-triggered communication strategy without resilience are shown in Fig.5, respectively.

The statistics shows that 234 packets are transmitted and the average period

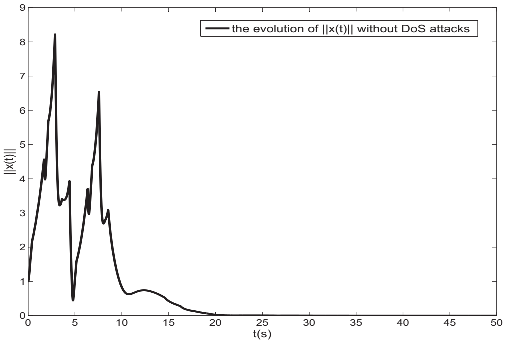

Figure 4 State response without DoS attacks

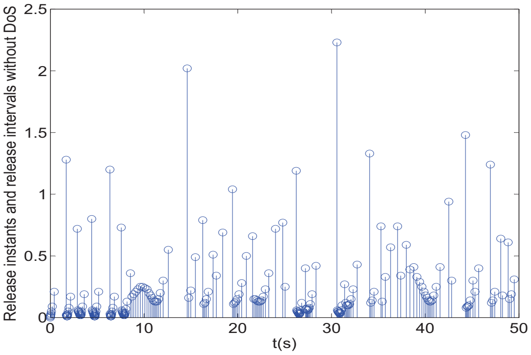

Figure 5 Release intervals without DoS attacks

is 0.2115s. Also, Fig.4 shows that the system state converges to zero with a good performance. 205

Case II: Probabilistic DoS attacks

When there are DoS attacks imposed on the system (34), the aforemention event-triggered communication scheme is violated. Suppose that the upper bound of the uncertain of DoS attacks $\Upsilon = 10$. In what follows, a probabilistic DoS attack and the worst case DoS attack are shown.

First, we simulate the probabilistic DoS attack with manipulate parameter $\xi(i_kh)$. Take $\xi(i_kh) = 1$ with probability $\alpha = 0.02$ with its attack sequence is shown as following Fig. 6. With the above designed controller and the resilient triggering bound, the response of system (34) under the probabilistic is depicted in Fig.7 and the release instants and release intervals are shown in Fig.8, respectively.

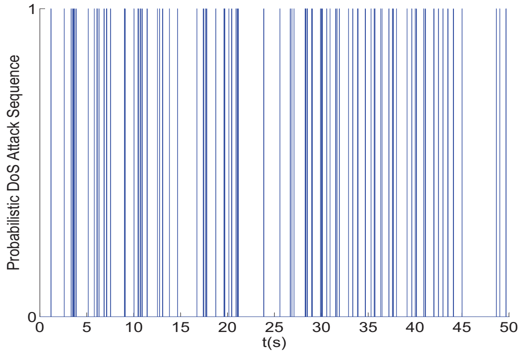

Figure 6 Probabilistic DoS attacks with $\alpha(\xi(i_kh) = 1) = 0.02$

The statistics shows that 246 packets are transmitted and the average period is 0.2029s. Here, the smaller average transmission period is shown. However, a

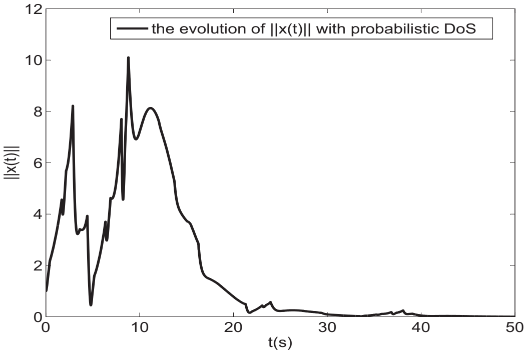

Figure 7 State response with probabilistic DoS attacks

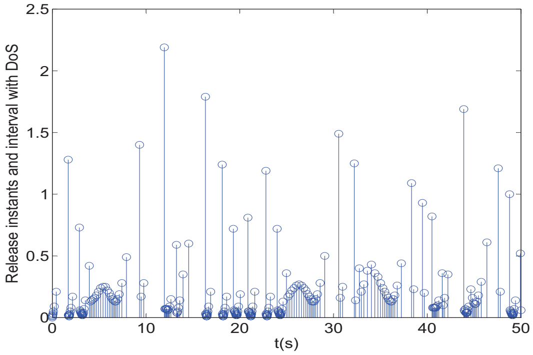

Figure 8 Release intervals with DoS attacks

worse performance during such DoS style is presented by comparing Fig.4 and Fig.7 which implies that a DoS attacks can lead to a bad performance indeed.

Case III: The worst DoS attacks case

The last scenario consider the worst DoS attack. Under such attack case, $\xi(i_k h) = 1$ is always hold except the instants which reach the up bound of the resilient region. Similarly, we can obtain the following figures on $||x(t)||$ and release intervals.

The statistics shows that 145 packets are transmitted and the average period

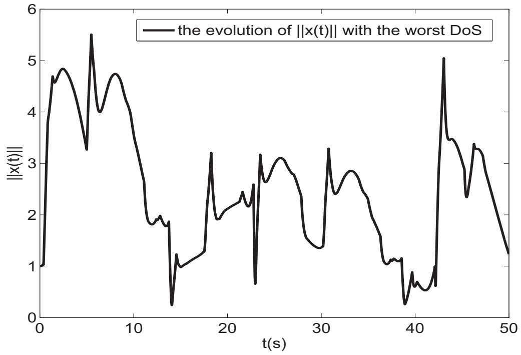

Figure 9 State response with DoS attacks

is $0.3277s$. The less sample data are transmitted and a larger average transmis-

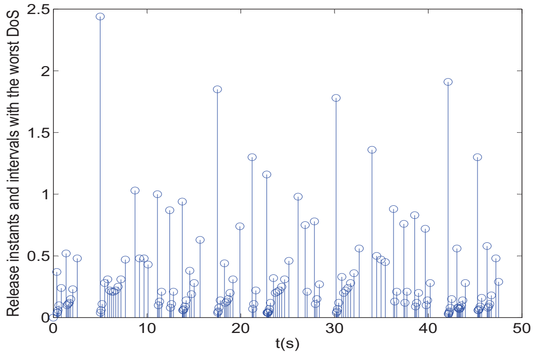

Figure 10 Release intervals with the worst DoS attacks

sion period is obtained. Although $||x(t)||$ is bounded, a worse performance is presented by comparing Fig.7 and Fig.9 which implies that one should trade-off between control performance and network security.

6. Conclusions

As so far, we have investigated the resilient triggering strategy for the event-based NCSs under DoS attacks. For the NCSs, the following three facts are: the DoS attacks is unpredictable, 2) it is impractical to change a controller when system is running, and 3) the network security will propagate to the physical system which will lead to the lost of control performance. Based on the above facts, the NCSs must be capable to tolerate a certain degree of DoS attacks. In this paper, a novel resilient triggering strategy caused by DoS attacks is proposed and the control performance lost is well confined according to the designed event-based controller. It is worthy noting that the proposed resilient triggering strategy takes the relationship between the uncertain of triggering condition and the control performance lost into consideration while dealing with the DoS attacks. For the proposed resilient triggering strategy, we must guarantee the successful transmission of the control signal which reach to the up bound of the uncertain of the triggering condition. Or the NCSs may be crashed by DoS attacks. The simulation result shows the validity of our theorem results.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61673255, the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning, the Key Project of Science and Technology Commission of Shanghai Municipality under Grant 10JC1405000, Shanghai Young Eastern Scholar Program under Grant QD2016030, A Project of Shandong Province Higher Educational Science and Technology Program under Grant J17KA084.

References

[1] A. Bemporad, M. Heemels, M. Johansson, Networked Control Systems, Springer London, 2010.

[2] D. Zhang, P. Shi, Q. G. Wang, L. Yu, Analysis and synthesis of networked control systems: A survey of recent advances and challenges., ISA Transactions 66 (2017) 376–392.

[3] R. M. Murray, Future directions in control, dynamics, and systems: overview, grand challenges, and new courses, European Journal of Control 9 (2) (2003) 144–158.

[4] L. Zhang, H. Gao, O. Kaynak, Network-induced constraints in networked control systemsa survey, IEEE Transactions on Industrial Informatics 9 (1) (2012) 403–416.

[5] L. Hetel, C. Fiter, H. Omran, A. Seuret, E. Fridman, J. P. Richard, S. I. Niculescu, Recent developments on the stability of systems with aperiodic sampling: An overview , Automatica 76 (2017) 309–335.

[6] P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, IEEE Transactions on Automatic Control 52 (9) (2007) 1680–1685.

[7] D. Yue, E. Tian, Q. L. Han, A delay system method to design of event-triggered control of networked control systems, in: Decision and Control and European Control Conference, 2011, pp. 1668–1673.

[8] D. Zhang, Q. L. Han, X. Jia, Network-based output tracking control for t-s fuzzy systems using an event-triggered communication scheme, Fuzzy sets and systems 273 (2015) 26–48.

[9] C. Peng, S. Ma, X. Xie, Observer-based non-pdc control for networked t-s fuzzy systems with an event-triggered communication, IEEE Transactions on Cybernetics 47 (8) (2017) 2279–2287.

[10] Z. Wu, Y. Wu, Z. G. Wu, J. Lu, Event-based synchronization of heterogeneous complex networks subject to transmission delays, IEEE Transactions on Systems Man & Cybernetics Systems (2017) DOI:10.1109/TSMC.2017.2723760.

[11] X. M. Zhang, Q. L. Han, B. L. Zhang, An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems, IEEE Transactions on Industrial Informatics 13 (1) (2017) 4–16.

[12] C. Peng, J. Zhang, H. Yan, Event-triggered communication and H_∞ control co-design for networked control systems, IEEE Transactions on Industrial Electronics 65 (2) (2018) 1685–1694.

[13] C. Peng, M. Wu, X. Xie, Y. Wang, Event-triggered predictive control for networked nonlinear systems with imperfect premise matching, IEEE Transactions on Fuzzy Systems (2018) DOI:10.1109/TFUZZ.2018.2799187.

[14] H. Sandberg, S. Amin, K. Johansson, Cyberphysical security in networked control systems: An introduction to the issue, Control Systems IEEE 35 (1) (2015) 20–23.

[15] S. Mclaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, R. Karri, The cybersecurity landscape in industrial control systems, Proceedings of the IEEE 104 (5) (2016) 1039–1057.

[16] A. A. C, S. Amin, B. Sinopoli, A. Perrig, S. Sastry, Challenges for securing cyber physical systems, In First Workshop on Cyber-physical Systems Security (2006) 363 – 369.

[17] J. P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (1) (2011) 23–40.

[18] I. Shames, H. Sandberg, K. H. Johansson, A secure control framework for resource-limited adversaries, Automatica 51 (C) (2015) 135–148.

[19] F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems, Control Systems IEEE 35 (1) (2015) 110–127.

[20] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, T. Hayat, Recent advances on filtering and control for cyber-physical systems under security and resource constraints , Journal of the Franklin Institute 353 (11) (2016) 2451–2466.

[21] C. Shen, T. Yu, H. Xu, G. Yang, X. Guan, User practice in password security: an empirical study of real-life passwords in the wild, Computers & Security 61 (2016) 130–141.

[22] S. Amin, S. S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: International Conference on Hybrid Systems: Computation and Control, 2009, pp. 31–45.

[23] H. S. Foroush, S. Martnez, On triggering control of single-input linear systems under pulse-width modulated dos signals, Siam Journal on Control & Optimization 54 (6) (2016) 3084–3105.

[24] Y. Yuan, F. Sun, Q. Zhu, Resilient control in the presence of dos attack: Switched system approach, International Journal of Control Automation & Systems 13 (6) (2015) 1423–1435.

[25] C. D. Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (11) (2015) 2930–2944.

[26] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Transactions on Automatic Control 60 (11) (2015) 3023–3028.

[27] Z. H. Pang, G. P. Liu, Design and implementation of secure networked predictive control systems under deception attacks, IEEE Transactions on Control Systems Technology 20 (5) (2012) 1334–1342.

[28] T. Rhouma, K. Chabir, M. N. Abdelkrim, Resilient control for networked control systems subject to cyber/physical attacks, International Journal of Automation & Computing (1) (2017) 1–10.

[29] K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using kalman filter, Control of Network Systems IEEE Transactions on 1 (4) (2014) 370–379.

[30] J. Y. Keller, K. Chabir, D. Sauter, Input reconstruction for networked control systems subject to deception attacks and data losses on control signals, International Journal of Systems Science 47 (4) (2016) 814–820.

[31] D. Ding, Z. Wang, G. Wei, F. E. Alsaadi, Event-based security control for discrete-time stochastic systems, Iet Control Theory & Applications 10 (15) (2016) 1808–1815.

[32] H. Sun, C. Peng, T. Yang, H. Zhang, W. He, Resilient control of networked control systems with stochastic denial of service attacks, Neurocomputing 270 (2017) 170–177.

[33] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies, IEEE Transactions on Automatic Control 60 (12) (2015) 3299–3304.

[34] K. Ding, Y. Li, D. E. Quevedo, S. Dey, L. Shi, A multi-channel transmission schedule for remote state estimation under dos attacks , Automatica 78 (2017) 194–201.

[35] R. Cao, J. Wu, C. Long, S. Li, Stability analysis for networked control systems under denial-of-service attacks, in: IEEE Conference on Decision and Control, 2015, pp. 7476–7481.

[36] C. Peng, J. Li, M. R. Fei, Resilient event-triggered H_∞ load frequency control for networked power systems with energy-limited dos attacks, IEEE Transactions on Power Systems 32 (5) (2017) 4110–4118.

[37] D. Wu, X. M. Sun, Y. Tan, W. Wang, On designing event-triggered schemes for networked control systems subject to one-step packet dropout, IEEE Transactions on Industrial Informatics 12 (3) (2016) 902–910.

[38] S. Linsenmayer, D. V. Dimarogonas, F. Allg?wer, A non-monotonic approach to periodic event-triggered control with packet loss, in: Decision and Control, 2016, pp. 507–512.

[39] A. Girard, Dynamic triggering mechanisms for event-triggered control, IEEE Transactions on Automatic Control 60 (7) (2015) 1992–1997.

[40] C. Peng, T. C. Yang, Event-triggered communication and H_∞ control co-design for networked control systems, Automatica 49 (5) (2013) 1326–1332.