Zhiwen Wang; Xiangnan Xu; Hongtao Sun; Long Li

Dual-terminal event triggered control for cyber-physical systems under false data injection attacks

Kybernetika, Vol. 56 (2020), No. 2, 323–339

Persistent URL: http://dml.cz/dmlcz/148303

KYBERNETIKA — VOLUME *56* (2020), NUMBER 2, PAGES 323–339

DUAL-TERMINAL EVENT TRIGGERED CONTROL FOR CYBER-PHYSICAL SYSTEMS UNDER FALSE DATA INJECTION ATTACKS

Zhiwen Wang, Xiangnan Xu, Hongtao Sun and Long Li

This paper deals with the problem of security-based dynamic output feedback control of cyber-physical systems (CPSs) with the dual-terminal event triggered mechanisms (DT-ETM) under false data injection (FDI) attacks. Considering the limited attack energy, FDI attacks taking place in transmission channels are modeled as extra bounded disturbances for the resulting closed-loop system, thus enabling H_∞ performance analysis with a suitable ϱ attenuation level. Then two buffers at the controller and actuator sides are skillfully introduced to cope with the different transmission delays in such a way to facilitate the subsequent security analysis. Next, a dynamic output feedback security control (DOFSC) model based on the DT-ETM schemes under FDI attacks is well constructed. Furthermore, novel criteria for stability analysis and robust stabilization are carefully derived by exploiting Lyapunov–Krasovskii theory and LMIs technique. Finally, an illustrative example is provided to show the effectiveness of the proposed method.

Keywords: cyber-physical system, FDI attacks, Event-triggered mechanisms, dynamic output feedback security control

Classification: 93C05, 93B36, 93D15

1. INTRODUCTION

In the past decades, CPSs have been widely applied to many fields, such as smart grid, smart transportation and smart city. However, the recent incidents, such as 'Stuxnet' and 'WannaCry', have led to intensive attention on security issues from different communities [1, 9, 10, 18, 19, 20, 24]. Owing to software vulnerabilities and hardware backdoor, it is necessary to develop new strategies or methods to fulfill the full-dimensional security defense.

FDI attacks, as one of the major attacks in CPSs, have been found in several major power grid accidents around the world. For example, the power blackout of Ukraine, in 2015, caused a worldwide concern as the power data was compromised by malicious attacks [14]. The serious damages are not only in power communication network but also in power grid hardware architecture [3, 10, 26]. Several incidents show that physical defense can not provide comprehensive protection for CPSs. Since the lack of attention to

DOI: 10.14736/kyb-2020-2-0323

the communication security for a long time, FDI attacks have become a real threat to the safe and stable operation of CPSs [2, 13, 28]. Therefore, many works devote themselves to the following security issues: 1) how to design an intelligent attack strategy to impair CPSs without detection; and 2) how to protect the CPSs from being injured by these malicious attacks.

FDI attacks are designed to exploit the vulnerabilities of network and hardware backdoor so as to compromise CPSs real data by passing the given bad data detection mechanism without being perceived [8, 10, 18, 25]. For example, Liang et al. illustrated that attackers could take advantage of the network vulnerability to implement FDI attacks which led to the blackout of smart grid [10]. In [13], Liu et al. showed that the attackers could launch their FDI attacks through manipulating state estimation results and avoiding bad data detection. Similarly, a more practical FDI attack, which named load redistribution attack, was proposed in [16], then two mathematical models under the consideration of the direct impacts and delay caused by such attacks were established. In [15], the necessary and sufficient condition for the existence of perfect malicious attacks was proved and designed two attack regimes against the distributed control systems. In [23], a further illustration of FDI model was proposed under the CPSs framework, while no discussion on the stable operation control strategy was given.

From the perspective of defense, one should spare no efforts on stability and optimal control strategies for CPSs. In [16], Pang et al. investigated the influence of the system output tracking error under the two-channels data injection attacks based on output tracking control law. In [19], the authors proposed an FDI attack model and an attack collaboration strategy. An optimal ellipsoidal state prediction and estimation method was presented in [6] for resisting certain attacks. In [21], a cooperative design method of output feedback controller based on the two-side asynchronous events triggering was proposed such that one can save communication resources, but they did not refer to some security issues. In [27], random cyber-attacks in communication channel were taken into account and described by a stochastic variable subject to Bernoulli distribution.

In this paper, we study the secure event-triggered control problem of a resource-limited CPS under dual terminal time-delays and energy-constrained FDI attacks. Note that limited communication resources, transmission delays and attacks are not rare in practical networked systems [4, 5, 7, 22, 29, 31]. To the best of our knowledge, dual terminal transmission delays have not been considered in designing event-triggered controller methods with energy-constrained FDI attacks. Therefore, the operation interval should be afresh divided into a series equal intervals when FDI attack and short time-delay exists at the same time, and a novel DOFSC is proposed to reduce communication burden with the DT-ETM. In particular, under the same time sequence, robust H_∞ tools are used to make the impact of FDI attacks on the system within a controllable range. By considering the energy-constrained FDI attacks, the dynamic output-based security control strategy is proposed in this paper. The main contributions of this paper can be summarized as:

1) A novel DOFSC model which includes bounded FDI attacks is well constructed under DT-ETM.

2) Under the constructed model, FDI attacks are converted into extra external disturbances of the resulting closed-loop system such that the security issue of the

studied CPS can be handled under H_∞ performance analysis and synthesis.

The remainder of this paper is organized as follows. The framework of the studied CPSs and some preliminaries are formulated in Section 2. In Section 3, the stability analysis of the system under the limited attack energy is presented. Then the co-design of security and control is given in Section 4; The following Section 5 shows the numerical and simulation results which can verify the given results; The last section 6 concludes this paper.

2. PROBLEM FORMULATION

2.1. The framework description

The framework of the proposed dual-terminal event triggered dynamic output feedback control scheme is shown in Figure 1, where the plant, controller, sensor and actuators are communicated with wireless network channel. Here, the data packets are transmitted in a single packet manner and there is no data loss or disorder, the bad data tampered by FDI is integrated with the normal packets. In order to prevent information of sensor and actuator from being lost, buffers whose lengths are greater than the biggest delay should be separately setting at the sending points of the sensor and controller. In particular, the length of buffer is predefined by comparing with the average delay of the system test operation and engineer experience to choose a suitable solution.

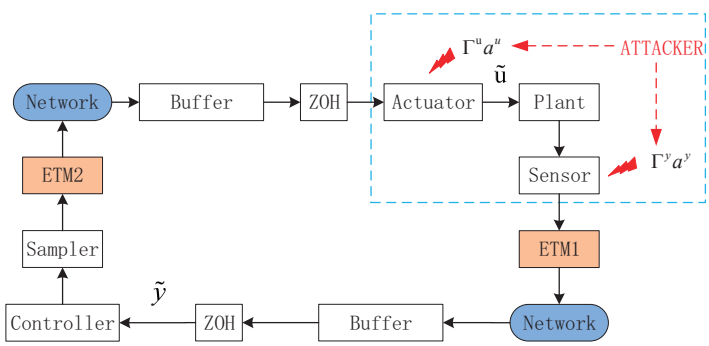

Fig. 1: The CPSs block diagram under FDI.

The sensor measures output $y(t)$ with a constant sampling period h and we denote the discrete measurement output $y(kh)$ from the sensor to controller channel. The dynamics of the CPS are described by

$$\begin{cases} \dot{x}(t) &= Ax(t) + B\tilde{u}(t) + B_w w(t) \\ z(t) &= C_1 x(t) + D_1 w(t) \\ y(t) &= Cx(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the system state vector, $\tilde{u}(t) \in \mathbb{R}^{n_u}$ is the control input vector, $z(t) \in \mathbb{R}^{n_z}$ is the controlled output vector, and $y(t) \in \mathbb{R}^{n_y}$ is the measured output vector,

$w(t) \in \ell_2[0,\infty)$ is the exogenous disturbance. A, B, B_w, C, C_1 and D_1 are constant matrices with appropriate dimensions. The initial condition of the system (1) is given by $x(0) = x_0$.

The dual-terminal event triggered mechanisms, equipped with the interested framework, are used to reduce the data transmission. To facilitate description, we denote the sampling set as $\mathbb{S}_s = \{0, h, 2h, \ldots, kh, \ldots\}$ $(k \in \mathbb{N})$, the successful transmitted set of sensor side as $\mathbb{S}_y = \{0, i_1h, i_2h, \ldots\}(i_k \in \mathbb{N})$, the successful transmitted set of controller side as $\mathbb{S}_u = \{0, d_1h, d_2h, \ldots\}(d_k \in \mathbb{N})$, and the arrival time set of each packet as $\mathbb{S}_z = \{t_0 = \tau, t_1, t_2, \ldots\}(t_k \in \mathbb{N})$.

In addition, the attacker selects sensor and actuator locations to inject false data $\Gamma^u a^u$ and $\Gamma^y a^y$, respectively.

2.2. Dual-terminal event triggered

For clear purpose, we denote i_kh as the latest transmission instants of ETM1 and i_kh+jh is the current triggering instant. Thus, the event triggered condition for ETM1 can be designed as

$$\|\Omega_y^{\frac{1}{2}}[y(i_kh) - y(i_kh + jh)]\|_2 \geq \delta_y \|\Omega_y^{\frac{1}{2}} y(i_kh)\|_2 \tag{2}$$

where scalar $0 \leq \delta_y < 1$ is threshold, and positive definite matrix $\Omega_y > 0$ is weight matrix. Once the trigger condition (2) is satisfied, the current packet is immediately released through the communication network, otherwise, the current packet is discarded. Therefore, the successful transmitted set of ETM1 is a subset of the sampling time, i. e., $\mathbb{S}_y \subseteq \mathbb{S}_s$. According to the event-triggered condition (2), the next release instant of ETM1 can be described as

$$i_{k+1}h = i_kh + \min_{j\in\mathbb{N}}\{jh | \|\Omega_y^{\frac{1}{2}}[y(i_kh) - y(i_kh + jh)]\|_2 > \delta_y \|\Omega_y^{\frac{1}{2}} y(i_kh)\|_2\}.$$

Similarly, we denote as d_kh as the latest transmission instants of ETM2 and d_kh+jh is the current triggering instant of ETM2. Then the next release instant of ETM2 can be designed as

$$d_{k+1}h = d_kh + \min_{j\in\mathbb{N}}\{jh | \|\Omega_y^{\frac{1}{2}}[u(d_kh) - u(d_kh + jh)]\|_2 > \delta_u \|\Omega_u^{\frac{1}{2}} u(d_kh)\|_2\} \tag{3}$$

where scalar $0 \leq \delta_u < 1$ is threshold, and positive definite matrix $\Omega_u > 0$ is weight matrix. $u(d_kh)$ and $u(d_kh + jh)$ represents the latest triggered moment and the current triggering instant of the control law $u(t)$, respectively.

Remark 2.1. The smaller δ_y, δ_u, the more sensitive to the state change, and the more frequently control updates. It is obvious that if $\delta_y \to 0, \delta_u \to 0$, the event trigger will operate in the periodic sampling style, i. e., $\mathbb{S}_y = \mathbb{S}_u = \mathbb{S}_s$.

Remark 2.2. It is different to cope with dual time delays for each side because the values of τ_k^u and τ_k^y are different and unpredictable. However, the uncertain delay can be converted to the maximum delay by setting up data center buffer at the controller

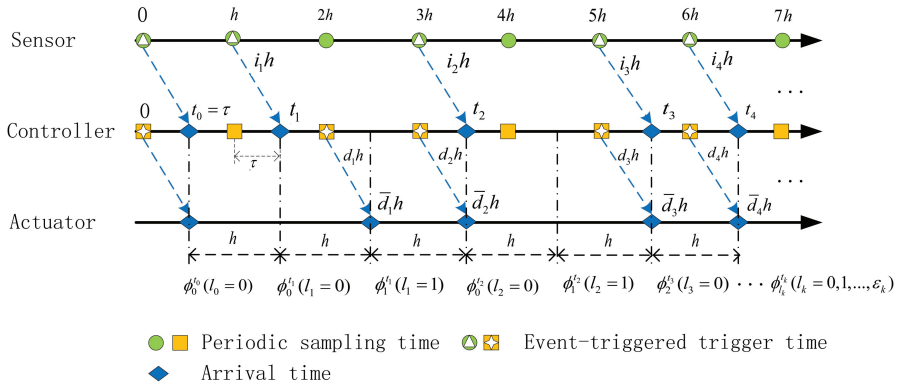

Fig. 2: The operation interval division diagram.

and the actuator side since $0 \le \tau_k^y \le \tau^y, 0 \le \tau_k^u \le \tau^u$, and the corresponding controller design parameters can be calculated. Therefore, the maximum induced delay in dual-terminal communication network can be defined as $\tau = \max\{\tau^y, \tau^u\}$.

Considering the time delay τ_k^y, τ_k^u of communication network for each side, we define $\epsilon_k = i_{k+1} - i_k - 1$. Then zero-order holder(ZOH) interval of the sensor point $[t_k, t_{k+1})$ can be divided as:

$$[t_k, t_{k+1}) = \bigcup_{\ell_k=0}^{\epsilon_k} \phi_{\ell_k}^{t_k}$$

where $\phi_{\ell_k}^{t_k} = [t_k + \ell_k h, t_k + (\ell_k + 1)h)$, $\ell_k = 0, 1, \ldots, \epsilon_k$. Further, it is clear that

$$\phi_{\ell_k}^{t_k} \subseteq [\bar{d}_k h + \tau, \bar{d}_{k+1} h + \tau) \tag{4}$$

where $\bar{d}_k h = \max\{d_k h | d_k h \le i_k h + \ell_k h\}$ represents the latest triggered time of the controller side up to the current triggering instant $i_k h + \ell_k h$ with $\bar{d}_{k+1} h \ge i_k h + (\ell_k + 1)h$. Considering the dynamic variability of the time delay, it is difficult to realize the time-varying division of operation interval. In general, the value of τ can always be selected as the maximum time delay collected during test operation.

In this paper, we are interested in constructing a dynamic output feedback controller of the following form

$$\begin{cases} \dot{x}_c(t) &= A_c x_c(t) + A_{cd} x_c(t - \eta(t)) + B_c \tilde{y}(t) \\ u(t) &= C_c x_c(t) \end{cases} \tag{5}$$

where $x_c(t) \in \mathbb{R}^n, \tilde{y}(t), u(t)$ represents state, input and output vector, respectively. A_c, A_{cd}, B_c, C_c are the real matrix with appropriate dimension.

The actual feedback action is given by

$$\tilde{y}(t) = y(i_k h), t \in \phi_{\ell_k}^{t_k}. \tag{6}$$

Then we can define a function $\eta(t)$ and $e_y(t)$ as

$$\eta(t) = t - (i_k h + \ell_k h),\ e_y(t) = y(i_k h) - y(i_k h + \ell_k h), t \in \phi_{\ell_k}^{t_k}. \tag{7}$$

Obviously, $\eta(t)$ is a piecewise linear function with the following characteristics:

$$0 \leq \tau = \eta_1 \leq \eta(t) \leqslant \eta_2 = h + \tau, t \in \phi_{\ell_k}^{t_k}.$$

Remark 2.3. If $\tau = 0$, there is no induction delay existing or the induction delay ignored, and the η_2 indicates the maximum check update period. From Figure 2, it can be observed that the presence of Zeno behavior is prevented as $(t_{k+1} - t_k)_{min} = h > 0$ can guarantee that the inter-event interval is strictly positive [11, 12].

From (4),(6),(7), we have the controller input $\tilde{y}(t)$ and the control output $\tilde{u}(t)$,

$$\tilde{y}(t) = y(i_k h) = e_y(t) + y(t - \eta(t)),\ \tilde{u}(t) = u(\bar{d}_k h), t \in \phi_{\ell_k}^{t_k}. \tag{8}$$

Similar to (7), we can obtain the $\tilde{u}(t)$ as follows

$$e_u(t) = u(\bar{d}_k h) - u(i_k h + \ell_k h), \tilde{u}(t) = u(\bar{d}_k h) = e_u(t) + u(t - \eta(t)), t \in \phi_{\ell_k}^{t_k}. \tag{9}$$

2.3. Data injection model

In order to characterize the FDI attacks, the channel selection matrix is defined as

$$\Gamma^y = diag(\gamma_1^y, \ldots, \gamma_s^y, \ldots, \gamma_n^y), \Gamma^u = diag(\gamma_1^u, \ldots, \gamma_s^u, \ldots, \gamma_n^u)$$

where $\gamma_s^y \in \{0, 1\}$ and $\gamma_s^u \in \{0, 1\}$ represent whether the channel is attacked, $\gamma_s^y = 1$ and $\gamma_s^u = 1$ denote that the s channel is attacked and the data is compromised.

Then the false data injected by an attacker is descried as

$$a^y(t) = [a_1^y(t), \ldots, a_s^y(t), \ldots, a_n^y(t)]^T, a^u(t) = [a_1^u(t), \ldots, a_s^u(t), \ldots, a_n^u(t)]^T$$

where $a_s^y(t)$ and $a_s^u(t)$ represent the injection bias of the s channel at the time instant t.

Therefore, the compromised data can be expressed as

$$\tilde{y}(t) = e_y(t) + y(t - \eta(t)) + \Gamma^y a^y(t), t \in \phi_{\ell_k}^{t_k}; \tag{10}$$

$$\tilde{u}(t) = e_u(t) + u(t - \eta(t)) + \Gamma^u a^u(t), t \in \phi_{\ell_k}^{t_k}. \tag{11}$$

Setting the attack vector $\omega(t) = \begin{bmatrix} w(t) & a^y(t) & a^u(t) \end{bmatrix}^T$ and combining (1), (9), (10), (11) together, we have the following closed-loop system

$$\begin{cases} \dot{\tilde{x}}(t) = \bar{A}\tilde{x}(t) + \bar{A}_d\tilde{x}(t - \eta(t)) + \bar{B}_u e_u(t) + \bar{B}_y e_y(t) + \bar{B}_w\omega(t) \\ z(t) = \bar{C}_1\tilde{x}(t) + \bar{D}_1\omega(t) \end{cases} \tag{12}$$

where

$$\bar{A} = \begin{bmatrix} A & 0 \\ 0 & A_c \end{bmatrix}, \bar{A}_d = \begin{bmatrix} 0 & BC_c \\ B_c C & A_{cd} \end{bmatrix}, \bar{B}_y = \begin{bmatrix} 0 \\ B_c \end{bmatrix}, \bar{B}_u = \begin{bmatrix} B \\ 0 \end{bmatrix},$$

$$\bar{B}_w = \begin{bmatrix} B_w & 0 & B\Gamma^u \\ 0 & B_c\Gamma^y & 0 \end{bmatrix}, \bar{C}_1 = \begin{bmatrix} C_1 & 0 \end{bmatrix}, \bar{D}_1 = \begin{bmatrix} D_1 & 0 & 0 \end{bmatrix}.$$

Note from above equation that $e_u(t)$, $e_y(t)$ satisfy the following constraints under the same sequence $\phi_{\ell_k}^{t_k}$, namely, the event-triggered mechanisms follow the below conditions

$$\begin{aligned} e_y^T(t)\Omega_y e_y(t) \leq & \delta_y(e_y(t) + CE_1\tilde{x}(t-\eta(t)))^T\Omega_y(e_y(t) + CE_1\tilde{x}(t-\eta(t))), \\ e_u^T(t)\Omega_u e_u(t) \leq & \delta_u(e_u(t) + C_cE_2\tilde{x}(t-\eta(t)))^T\Omega_u(e_u(t) + C_cE_2\tilde{x}(t-\eta(t))). \end{aligned} \tag{13}$$

The objective of this paper is to synthesize DOFSC for the closed-loop system (12) under DT-ETM such that:

- The closed-loop system is asymptotically stable when neither disturbance nor attack exists, i. e., $\omega(t) = 0$.
- Under zero initial condition, the closed-loop system guarantees that $\|z(t)\|_2 \leq \varrho\|w(t)\|_2$ for all nonzero $w \in L_2[0, +\infty)$, where $\varrho > 0$ is a prescribed scalar.

Because of the energy limitation of FDI attacks, $a^y(t)$ and $a^u(t)$ are bounded by $a(t) = \begin{bmatrix} a^y(t) & a^u(t) \end{bmatrix}^T$ with $\|a(t)\|_2 \leq \varpi\|z(t)\|_{2max} \leq \varpi\varrho\|\omega(t)\|_2 = \gamma\|\omega(t)\|_2$, where ϖ is a given constant greater than zero in relation to attack energy and $\gamma = \varpi\varrho$.

3. STABILITY ANALYSIS OF THE DUAL-TERMINAL EVENT TRIGGERED CLOSED-LOOP SYSTEM

In this section, Lyapunov–Krasovskii theory and LMIs method are exploited to analyze the stability of the proposed framework of DT-ETM CPS under FDI attacks.

Theorem 3.1. For given scalars $h > 0, \tau > 0, \varrho > 0, \varpi > 0$, the close-loop system (12), which subjects FDI attacks (10), (11), under the communication scheme (13) is asymptotically stable with H_∞ performance index ϱ, if there exist scalars $0 < \delta_y < 1, 0 < \delta_u < 1$, real matrices $\Omega_y > 0$, $\Omega_u > 0, P > 0, U > 0, Q > 0, R_i > 0 (i = 1, 2, 3)$, and S_2, S_3 of appropriate dimensions such that

$$\Upsilon_1 := \begin{bmatrix} R_i & * \\ S_i & R_i \end{bmatrix} > 0, \quad i = 2, 3, \tag{14}$$

$$\Upsilon_2 := \begin{bmatrix} \Xi_{11}^i & * \\ \Xi_{21} & \Xi_{22} \end{bmatrix} < 0, \quad i = 2, 3 \tag{15}$$

where

$$\begin{cases} \Xi_{21} = col\{\lambda_2, \lambda_3, \eta_{1m}\lambda_1, \eta_{2m}\lambda_1, \lambda_4\}, \\ \Xi_{22} = diag\{-(\delta_y\Omega_y)^{-1}, -(\delta_u\Omega_u)^{-1}, -R_1^{-1}, -R_2^{-1} - R_3^{-1}, -I\} \\ \Xi_{11}^i = \Theta^i - \lambda_1(\eta_1^2R_1 + \eta_{1m}^2R_2 + \eta_{2m}^2R_3)\lambda_1^T - e_6\Omega_y e_6^T - e_7\Omega_u e_7^T - \varrho^2 e_8 e_8^T. \end{cases}$$

P r o o f. Choose the Lyapunov–Krasovskii functional candidate as

$$V(t) \triangleq V_1(t) + V_2(t) + V_3(t) + V_4(t) + V_5(t) + V_6(t),$$

$$
\begin{aligned}
V_1(t) &= \tilde{x}^T(t)P\tilde{x}(t), P > 0,\\
V_2(t) &= \int_{t-\eta_1}^{t} \tilde{x}^T(s)U\tilde{x}(s)\,\mathrm{d}s, U > 0,\\
V_3(t) &= \int_{t-\rho}^{t} \zeta^T(s)Q\zeta(s)\,\mathrm{d}s, Q > 0,\\
V_4(t) &= \eta_1 \int_{-\eta_1}^{0}\int_{t+\theta}^{t} \dot{\xi}^T(s)R_1\dot{\xi}(s)\,\mathrm{d}s\mathrm{d}\theta, R_1 > 0,\\
V_5(t) &= \eta_{1m} \int_{-\eta_m}^{-\eta_1}\int_{t+\theta}^{t} \dot{\tilde{x}}^T(s)R_2\dot{\tilde{x}}(s)\,\mathrm{d}s\mathrm{d}\theta, R_2 > 0,\\
V_6(t) &= \eta_{2m} \int_{-\eta_2}^{-\eta_m}\int_{t+\theta}^{t} \dot{\tilde{x}}^T(s)R_3\dot{\tilde{x}}(s)\,\mathrm{d}s\mathrm{d}\theta, R_3 > 0
\end{aligned}
$$

where $\eta_{1m} = \eta_m - \eta_1$, $\eta_{2m} = \eta_2 - \eta_m$, $\rho = \frac{\eta_2-\eta_1}{2}$, $\eta_m = \frac{\eta_1+\eta_2}{2}$, $\zeta(t) = \mathrm{col}\{\tilde{x}\,(t-\eta_1)\,, \tilde{x}\,(t-\eta_m)\}$.

Defining $\chi(t) = \{\tilde{x}(t), \tilde{x}\,(t-\eta_1)\,, \tilde{x}(t-\eta(t)), \tilde{x}(t-\eta_m), \tilde{x}\,(t-\eta_2)\,, e_y(t), e_u(t), \omega(t)\}$ and the following associated with the unit matrices, so the system (12) can be written as $\dot{\tilde{x}}(t) = \lambda_1^T\chi(t)$.

$$
\begin{aligned}
e_1 &\triangleq \begin{bmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T, e_2 \triangleq \begin{bmatrix} 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T,\\
e_3 &\triangleq \begin{bmatrix} 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T, e_4 \triangleq \begin{bmatrix} 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \end{bmatrix}^T,\\
e_5 &\triangleq \begin{bmatrix} 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \end{bmatrix}^T, e_6 \triangleq \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \end{bmatrix}^T,\\
e_7 &\triangleq \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \end{bmatrix}^T, e_8 \triangleq \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \end{bmatrix}^T,
\end{aligned}
$$

$$
\lambda_1 \triangleq \left(\bar{A}e_1^T + \bar{A}_d e_3^T + \bar{B}_y e_6^T + \bar{B}_u e_7^T + \bar{B}_w e_8^T\right)^T.
$$

Taking the time derivative along the trajectory of system (12) yields

$$
\begin{aligned}
\dot{V}_1(t) &= 2\chi^T(t)\lambda_1 P e_1^T\chi(t),\\
\dot{V}_2(t) &= \chi^T(t)\left\{e_1Ue_1^T - e_2Ue_2^T\right\}\chi(t),\\
\dot{V}_3(t) &= \chi^T(t)\left\{[e_2\ e_4]Q[e_2\ e_4]^T - [e_4\ e_5]Q[e_4\ e_5]^T\right\}\chi(t),\\
\dot{V}_4(t) &= -\eta_1\int_{t-\eta_1}^{t} \dot{\tilde{x}}^T(\theta)R_1\dot{\tilde{x}}(\theta)\,\mathrm{d}\theta + \dot{\tilde{x}}^T(t)\eta_1^2R_1\dot{\tilde{x}}(t),\\
\dot{V}_5(t) &= -\eta_{1m}\int_{t-\eta_m}^{t-\eta_1} \dot{\tilde{x}}^T(\theta)R_2\dot{\tilde{x}}(\theta)\,\mathrm{d}\theta + \dot{\tilde{x}}^T(t)\eta_{1m}^2R_2\dot{\tilde{x}}(t),\\
\dot{V}_6(t) &= -\eta_{2m}\int_{t-\eta_2}^{t-\eta_m} \dot{\tilde{x}}^T(\theta)R_3\dot{\tilde{x}}(\theta)\,\mathrm{d}\theta + \dot{\tilde{x}}^T(t)\eta_{2m}^2R_3\dot{\tilde{x}}(t).
\end{aligned}
$$

Based on the values of $\eta(t)$, we consider the following two conditions.

1) If $\eta(t) \in [\eta_1, \eta_m)\,, t \in \phi_{\ell_k}^{t_k}$, we use Jensen's inequality for $\dot{V}_4(t), \dot{V}_5(t), \dot{V}_6(t)$ to get

$$
\dot{V}_4(t) \le \chi^T(t)\left\{\lambda_1\eta_1^2R_1\lambda_1^T - [e_1 - e_2]R_1[e_1 - e_2]^T\right\}\chi(t),
$$

$$\begin{aligned}
\dot{V}_6(t) &\le \chi^T(t)\left\{\lambda_1\eta_{2m}^2 R_3\lambda_1^T - [e_4-e_5]R_1[e_4-e_5]^T\right\}\chi(t),\\
\dot{V}_5(t) &= \chi^T(t)\left\{\lambda_1\eta_{1m}^2 R_2\lambda_1^T\right\}\chi(t) - \int_{t-\eta_m}^{t-\eta_t}\dot{\tilde{x}}^T(\theta)R_2\dot{\tilde{x}}(\theta)\,\mathrm{d}\theta\\
&\quad + \int_{t-\eta_t}^{t-\eta_1}\dot{\tilde{x}}^T(\theta)R_2\dot{\tilde{x}}(\theta)\,\mathrm{d}\theta\\
&\le \chi^T(t)\{\lambda_1\eta_{1m}^2 R_2\lambda_1^T - \frac{\eta_{1m}}{\eta(t)-\eta_1}[e_2-e_3]R_2[e_2-e_3]^T\\
&\quad - \frac{\eta_{1m}}{\eta_m-\eta(t)}[e_3-e_4]R_2[e_3-e_4]^T\}\chi(t).
\end{aligned}$$

If the condition (14) is satisfied, we use the reciprocally convex method in [17] for $\dot{V}_5(t)$ and obtain

$$\begin{aligned}
\dot{V}_5(t) \le &\chi^T(t)\{\lambda_1\eta_{1m}^2 R_2\lambda_1^T + sym\{[e_3-e_4]S_2[e_2-e_3]^T\}\\
&- [e_2-e_3]R_2[e_2-e_3]^T - [e_3-e_4]R_2[e_3-e_4]^T\}\chi(t)
\end{aligned}$$

where $sym\{X\} = X + X^T$.

2) Similarly, if $\eta(t)$ satisfies $\eta(t) \in [\eta_m, \eta_2]$. By applying the Jensen's inequality and reciprocally convex method for $\dot{V}_4(t), \dot{V}_5(t), \dot{V}_6(t)$ respectively, we have that

$$\begin{aligned}
\dot{V}(t) = \chi^T(t)\Theta^i\chi(t) = &\dot{V}(t) - e_y^T(t)\Omega_y e_y(t) + e_y^T(t)\Omega_y e_y(t)\\
&- e_u^T(t)\Omega_u e_u(t) + e_u^T(t)\Omega_u e_u(t) - z^T(t)z(t)\\
&+ z^T(t)z(t) - \varrho^2\omega^T(t)\omega(t) + \varrho^2\omega^T(t)\omega(t), \quad i = 2,3
\end{aligned} \tag{16}$$

where

$$\Theta^i = \begin{cases}
sym\{\lambda_1 P e_1^T\} + (e_1-e_2)R_1(e_1-e_2)^T - e_1 U e_1^T - e_2 U e_2^T + [e_2 \quad e_4]Q[e_2 \quad e_4]^T\\
\quad - [e_4 \quad e_5]Q[e_4 \quad e_5]^T + \lambda_1^T(\eta_1^2 R_1 + \eta_{1m}^2 R_2 + \eta_{2m}^2 R_3)\lambda_1\\
-(3-i)(e_4-e_5)R_3(e_4-e_5)^T - (i-2)(e_4-e_3)R_3(e_4-e_3)^T\\
\quad - (i-2)(e_3-e_5)R_3(e_3-e_5)^T\\
-(3-i)(e_2-e_3)R_2(e_2-e_3)^T - (3-i)(e_3-e_4)R_2(e_3-e_4)^T\\
\quad - (i-2)(e_2-e_4)R_2(e_2-e_4)^T\\
+(3-i)sym\{(e_3-e_4)S_2(e_2-e_3)^T\} + (i-2)sym\{(e_3-e_5)S_3(e_4-e_3)^T\}
\end{cases}$$

Substituting (13) and H_∞ performance for both disturbance and FDI attacks into (16), we have that

$$\dot{V}(t) \le \chi^T(t)\bar{\Theta}^i\chi(t) - z^T(t)z(t) + \varrho^2\omega^T(t)\omega(t), i = 2,3, \tag{17}$$

where $\bar{\Theta}^i = \Theta^i - e_6\Omega_y e_6^T - e_7\Omega_u e_7^T - \varrho^2 e_8 e_8^T + \delta_y\lambda_2\Omega_y\lambda_2^T + \delta_u\lambda_3\Omega_u\lambda_3^T + \lambda_4\lambda_4^T, \lambda_2 = CE_1e_3 + e_6, \lambda_3 = C_cE_2e_3 + e_7, \lambda_4 = \bar{C}_1e_1 + D_1e_8$.

By using Schur complement, we have $\bar{\Theta}^i < 0, i = 2,3$. Therefore, for $t \in \phi_{\ell_k}^{t_k}$, we have

$$\dot{V}(t) \le -z^T(t)z(t) + \varrho^2\omega^T(t)\omega(t). \tag{18}$$

Then we manipulate integration for both sides of (18) from 0 to $+\infty$, yielding

$$V(+\infty) - V(0) \leq \int_0^{+\infty} [-z^T(t)z(t) + \varrho^2\omega^T(t)\omega(t)]\,\mathrm{d}t \tag{19}$$

for all $w(t) \in L_2[0, +\infty)$.

Under zero initial condition, it follows from (19) that

$$\int_0^{+\infty} z^T(t)z(t)\,\mathrm{d}t \leq \int_0^{+\infty} \varrho^2\omega^T(t)\omega(t)]\,\mathrm{d}t.$$

That is, $\|a(t)\|_2 \leq \varrho\|\omega(t)\|_2$. This completes the proof.

□

4. EVENT-TRIGGERED DOFSC DESIGN

In this section, the following theorem is given to design the event-triggered DOFSC.

Theorem 4.1. For given scalars $h > 0, \tau > 0, \varrho > 0$, the DOFSC of the closed-loop system (12) subject to FDI attacks (10), (11) under the communication scheme (13) is solvable with H_∞ performance index ϱ, if there exist scalars $0 < \delta_y < 1, 0 < \delta_u < 1$, and real matrices $\Omega_y > 0, \Omega_u > 0, \bar{U} > 0, X > 0, Y > 0$, $\bar{Q} > 0, \bar{R}_i > 0 (i = 1, 2, 3), \bar{S}_2, \bar{S}_3$, and $W_j (j = 1, ...4)$ of compatible dimensions such that

$$Z := \begin{bmatrix} X & * \\ I & Y \end{bmatrix} > 0, \Upsilon_3 := \begin{bmatrix} \bar{R}_i & * \\ \bar{S}_i & \bar{R}_i \end{bmatrix} > 0, \quad i = 2, 3, \tag{20}$$

$$\Upsilon_4 := \begin{bmatrix} \bar{\Xi}_{11}^i & * \\ \bar{\Xi}_{21} & \bar{\Xi}_{22} \end{bmatrix} < 0, \quad i = 2, 3 \tag{21}$$

where

$$\begin{cases} \bar{\Xi}_{21} = \mathrm{col}\{\bar{\lambda}_2, \bar{\lambda}_3, \eta_1\bar{\lambda}_1, \eta_{1m}\bar{\lambda}_1, \eta_{2m}\bar{\lambda}_1, \bar{\lambda}_4\}, \\ \bar{\Xi}_{22} = \mathrm{diag}\{\Omega_y - 2\delta_y^{-\frac{1}{2}} I, \Omega_u - 2\delta_u^{-\frac{1}{2}} I, \bar{R}_1 - 2Z, \bar{R}_2 - 2Z, \bar{R}_3 - 2Z, -I\}, \\ \bar{\Xi}_{11}^i = \begin{cases} sym\left\{\bar{\lambda}_1 e_1^T\right\} \\ +e_1\bar{U}e_1^T - e_2\bar{U}e_2^T \\ -(e_1 - e_2)\bar{R}_1(e_1 - e_2)^T \\ -e_6\Omega_y e_6^T - e_7\Omega_u e_7^T - \varrho^2 e_8 e_8^T \\ +[e_2 \quad e_4]\bar{Q}[e_2 \quad e_4]^T - [e_4 \quad e_5]\bar{Q}[e_4 \quad e_5]^T \\ -(3-i)(e_4 - e_5)\bar{R}_3(e_4 - e_5)^T - (i-2)(e_4 - e_3)\bar{R}_3(e_4 - e_3)^T \\ \quad -(i-2)(e_3 - e_5)\bar{R}_3(e_3 - e_5)^T \\ -(3-i)(e_2 - e_3)\bar{R}_2(e_2 - e_3)^T - (3-i)(e_3 - e_4)\bar{R}_2(e_3 - e_4)^T \\ \quad -(i-2)(e_2 - e_4)\bar{R}_2(e_2 - e_4)^T \\ +(3-i)sym\{(e_3 - e_4)\bar{S}_2(e_2 - e_3)^T\} + (i-2)sym\{(e_3 - e_5)\bar{S}_3(e_4 - e_3)^T\} \end{cases} \end{cases}$$

with

$$\begin{cases} \bar{\lambda}_1 = \phi_1 e_1 + \phi_2 e_3 + \phi_3 e_6 + \phi_4 e_7 + \phi_5 e_8, \\ \bar{\lambda}_2 = \phi_6 e_3 + e_6, \bar{\lambda}_3 = \phi_7 e_3 + e_7, \\ \bar{\lambda}_4 = \phi_8 e_1 + D_1 e_8, \end{cases}$$

and

$$\phi_1 = \begin{bmatrix} AX & A \\ W_4 & YA \end{bmatrix}, \phi_2 = \begin{bmatrix} BW_1 & 0 \\ W_3 & W_2 C \end{bmatrix}, \phi_3 = \begin{bmatrix} 0 \\ W_2 \end{bmatrix}, \phi_4 = \begin{bmatrix} B \\ YB \end{bmatrix},$$

$$\phi_5 = \begin{bmatrix} B_\omega \\ YB_\omega \end{bmatrix}, \phi_6 = \begin{bmatrix} CX & C \end{bmatrix}, \phi_7 = [W_1 \quad 0], \phi_8 = \begin{bmatrix} C_1 X & C_1 \end{bmatrix}.$$

Proof. Introduce $X > 0$ such that $Y_1 = N^T (Y - X^{-1})^{-1} N$. Clearly ,$Y - X^{-1} > 0$ because of $Y_1 > 0$ and N is non-singular. By Schur complement, we can obtain that $Y - X^{-1} > 0 \Leftrightarrow Z > 0$, where Z is defined in (20).

Let

$$\Psi_1 = \begin{bmatrix} X & I \\ N^{-1}(I - YX) & 0 \end{bmatrix}, \Psi_2 = P\Psi_1 = \begin{bmatrix} I & Y \\ 0 & N^T \end{bmatrix},$$

and Ψ_1 Ψ_2 are non-singular. Denote $J_1 = \text{diag}\{\Psi_1, \Psi_1\}, J_2 = \text{diag}\{J_1, J_1, \Psi_1, I, I, I, I, I, \Psi_2, \Psi_2, \Psi_2, I\}$ and

$$\begin{cases} W_1 = C_c N^{-1}(I - YX), \quad W_2 = NB_c, \\ W_3 = W_2 CX + YBW_1 + NA_{cd} N^{-1}(I - YX), \\ W_4 = YAX + NA_c N^{-1}(I - YX). \end{cases} \tag{22}$$

With a congruence transformation on Υ_1 and Υ_2, which are defined in (14) (15) by non-singular matrix J_1 and J_2, we can obtain that

$$J_1^T \Upsilon_1 J_1 = \Upsilon_3 J_2^T \Upsilon_2 J_2 = \Upsilon_4 \tag{23}$$

after some simple algebraic manipulations. Here, Υ_3 and Υ_4 are defined in (20) (21).

Therefore, if Theorem 3.1 is satisfied, there exist real matrices $\bar{U} = \Psi_1^T U \Psi_1 > 0, \bar{Q} = J_1^T Q J_1 > 0, \bar{R}_i = \Psi_1^T R_i \Psi_1 > 0 (i = 1, 2, 3), \bar{S}_i = \Psi_1^T S_i \Psi_1 (i = 2, 3)$ and W_1, W_2, W_3, W_4 such that the matrix inequalities in (22) is satisfied.

With the aid of $x_c(t) = N^{-1} \bar{x}_c(t)$ in (5), the DOFC gain matrices are given as

$$\begin{cases} \bar{A}_c = (W_4 - YAX)(I - YX)^{-1}, \\ \bar{C}_c = W_1 (I - YX)^{-1}, \bar{B}_c = W_2, \\ \bar{A}_{cd} = (W_3 - W_2 CX - YBW_1)(I - YX)^{-1}. \end{cases}$$

The proof is completed. □

5. SIMULATION EXAMPLE

In this section, we use a simulation example, which is borrowed from [30], to demonstrate the effectiveness of the proposed DOFSC method. The system matrices are given as follows

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -\frac{k}{J_2} & -\frac{d}{J_2} & \frac{k}{J_2} & \frac{d}{J_2} \\ 0 & 0 & 0 & 1 \\ \frac{k}{J_1} & \frac{d}{J_1} & -\frac{k}{J_1} & -\frac{d}{J_1} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{J_1} \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Set $J_1 = J_2 = 1, k = 0.09$ and $d = 0.0219$. The system initial condition is $x_0 = [0.2, -0.3, 0.3, -0.2]^T$, and the system aims to move states to the original point x_e. Obviously, the eigenvalues of A are $0.0219 + 0.4237j, 0, -0.0219 - 0.4237j$ and 0, which means that the open-loop system is unstable.

Suppose that there are two measurement output channels and one actuator input channel. Therefore, the false data injected channels $\{\Gamma^y, \Gamma^u\}$ follow the form of

$$\Gamma^y \in \{\text{diag}(0,0), \text{diag}(1,0), \text{diag}(0,1), \text{diag}(1,1)\}$$
$$\Gamma^u \in \{0, 1\}.$$

The other parameters are $C_1 = [\ 1 \quad 0 \quad 0 \quad 0\ ], D_1 = 0, \omega(t) = 0.01 * \sin(2\pi t), h = 100\text{ms}, \tau_{min} = 20\text{ms}, \tau_{max} = 600\text{ms}, \varrho = 100$, and the simulation time is $100s$. More information about controller matrices A_c, A_{cd}, B_c, C_c can be found in [30].

We select channels $\Gamma^y = diag(1,1), \Gamma^u = 1$, and attack signals a^y, a^u satisfying $\|a^y(t)\| \leq 0.5, \|a^u(t)\| \leq 0.2$. The biased attack signals are arbitrarily and continuously injected between $70 - 100s$.

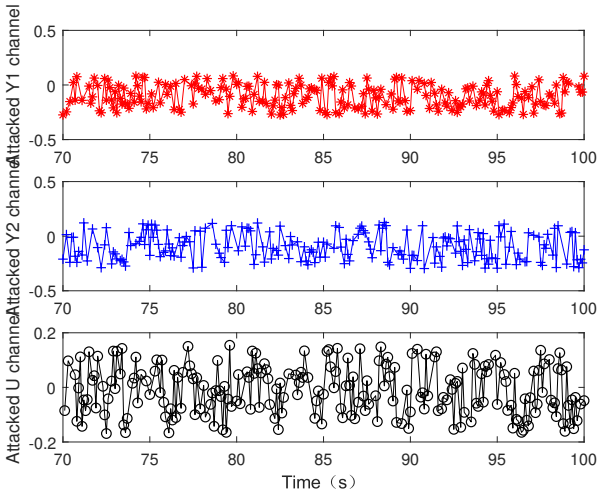

Fig. 3: The amount of data injected into different channels in 70-100s.

Based on the Theorem 4.1, the trigger mechanism parameters and the controller gain matrix are as follows $\Omega_u = 104.17, \Omega_y = \begin{bmatrix} 9.04 & -2.94 \\ -2.94 & 16.21 \end{bmatrix}, \delta_u = 0.04, \delta_y = 0.168$, and we select the DOFC for comparing the both state response in [30], where the event trigger parameters are $\delta_y = 0.0013$, $\Omega_y = \begin{bmatrix} 342.4817 & -13.7430 \\ -13.7430 & 322.9744 \end{bmatrix}$. Figure 4 shows the state response under the DOFC in [30].

From Figure 3, it is can be seen that FDI attacks are not continuous modification data in the channel, but launched at a random moment since 70s. Moreover, a^y, a^u signals are arbitrary within a limited range.

Figure 4 shows that the system state gradually shifts to the origin before 70s. However, the state $x(t)$ tends to be stable. Also, FDI attacks result in control performance deterioration between $[70, 100]$.

Figure 5 shows the state response under the proposed the DOFSC. It is clear that the system state changes slightly and the H_∞ control performance is achieved. The comparison shows that the proposed DOFSC can alleviate the effectiveness of FDI attacks.

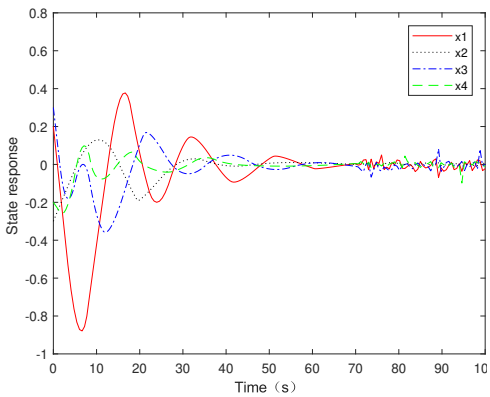

Fig. 4: State response under the DOFC1 in [30].

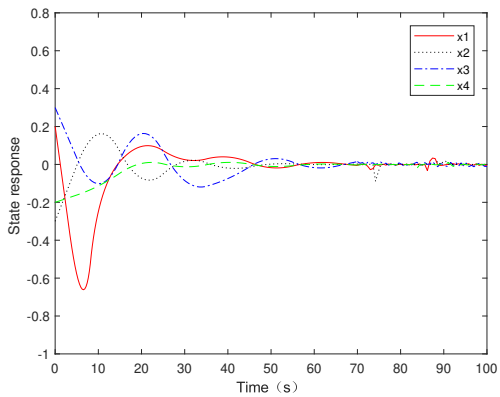

Fig. 5: State response under the DOFC.

The following Table 1 shows transmission rates of 62.4% (ETM2) and 33.7% (ETM1). The transmission rate of the system increases by 13.2% with FDI attacks.

	No FDI		FDI	
	Successful transmission	Bandwidth saving	Successful transmission	Bandwidth saving
Sensor side	337	66.3%	445	55.5%
Controller side	624	37.6%	779	22.1%

Tab. 1: The successful data packet transfer rate of FDI.

Figure 6 selects the event trigger interval diagrams between 55-70s and 70-85s for comparison. One can see from Figure 6 that the event trigger interval decreases and

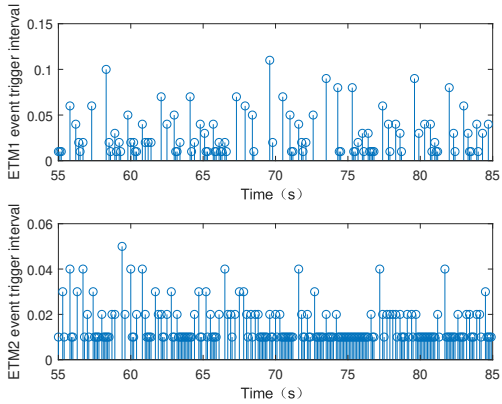

Fig. 6: Time interval between adjacent event triggers.

transmission frequency increases significantly. These results are consistent with the event triggered rules in Table 1. Although the transmission rate of the system is higher than FDI-free case, the closed-loop system stability is preserved.

6. CONCLUSION

In this paper, the dual event-triggered dynamic output feedback H_∞ control for CPSs under FDI attacks has been addressed. The comprehensive DT-ETM, which considers FDI attacks and transforms the attack into an 'extra' unknown disturbance, has been established to solve the security issues for the DOFSC of CPS. Then the Lyapunov theory and LMIs technique have been employed to formulate the proposed stability criterion. Also, the co-design of communication and security control law have been derived. Compared with state responses of simulations between traditional DOFC and the proposed DOFSC, the effectiveness of the proposed method is confirmed. In the future, combined with the attack and defense game, the optimal attack and defense model will be proposed , and the impact of FDI attacks on CPS security will be further explained.

ACKNOWLEDGEMENT

This work was supported in part by the Natural Natural Science Foundation of China under grants no. 61863026, 61751315, 61563031; in part by the Industrial Support and Guidance Project for Higher Education of Gansu Province (2019C-05); in part by the Open Fund Project of Key Laboratory of Gansu Advanced Control for Industrial Process (2019KFJJ03) and in part by the Program of Shandong Province Higher Educational Science and Technology under Grant no. J17KA084.

(Received September 11, 2019)

REFERENCES

[1] Y. Ashibani and Q. H. Mahmoud: Cyber physical systems security: analysis, challenges and solutions. Computers Security *68* (2017), 81–97. DOI:10.1016/j.cose.2017.04.005

[2] D. Ding, Q.-L. Han, Z. Wang, and X. Ge: A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans. Industr. Inform. *15*(2019), 5, 2483–2499. DOI: 10.1109/TII.2019.2905295

[3] D. Ding, Z. Wang, D. Ho, and G. Wei: Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. Automatica *78* (2017), 231–240. DOI:10.1016/j.automatica.2016.12.026

[4] M. García-Rivera and A. Barreiro: Analysis of networked control systems with drops and variable delays. Automatica *43* (2007), 2054–2059. DOI:10.1016/j.automatica.2007.03.027

[5] X. Ge, Q.-L. Han, and Z. Wang: A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks. IEEE Trans. Cybernet. *49* (2019), 1148–1159. DOI:10.1109/TCYB.2017.2789296

[6] X. Ge, Q.-L. Han, X.-M. Zhang, D. Ding, and F. Yang: Resilient and secure remote monitoring for a class of cyber-physical systems against attacks. Inform. Sci. (2019). DOI: 10.1016/j.ins.2019.10.057

[7] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang: Distributed event-triggered estimation over sensor networks: A survey. IEEE Trans. Cybernet., to be published. DOI:10.1109/TCYB.2019.2917179

[8] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang: Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica *109* (2019), 108557. DOI:10.1016/j.automatica.2019.108557

[9] A. Humayed, J. Lin, F. Li, and B. Luo: Cyber-physical systems security – a survey. IEEE Internet Things J. *4* (2017), 1802–1831. DOI:10.1109/JIOT.2017.2703172

[10] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Dong: The 2015 ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Systems *32* (2017), 3317-.3318. DOI:10.1109/TPWRS.2016.2631891

[11] C. Liu, H. Li, Y. Shi, and D. Xu: Distributed event-triggered gradient method for constrained convex minimization. IEEE Trans. Automat. Control (2019). DOI:10.1109/TAC.2019.2916985

[12] C. Liu, H. Li, Y. Shi, and D. Xu: Co-design of event trigger and feedback policy in robust model predictive control. IEEE Trans. Automat. Control (2019). DOI:10.1109/TAC.2019.2914416

[13] Y. Liu, P. Ning, and M. Reiter: False data injection attacks against state estimation in electric power grids. ACM Trans. Inform. System Security *14* (2011), 1–33. DOI:10.1145/1952982.1952995

[14] A.-Y. Lu and G.-H. Yang: False data injection attacks against state estimation in the presence of sensor failures. Inform. Sci. *508* (2020), 92-104. DOI:10.1016/j.ins.2019.08.052

[15] A.-Y. Lu and G.-H. Yang: Malicious attacks on state estimation against distributed control systems. IEEE Trans. Automat. Control (2019). DOI: 10.1109/TAC.2019.2949877

[16] Z. Pang, G. Liu, D. Zhou, F. Hou, and D. Sun: Two-channel false data injection attacks against output tracking control of networked systems. IEEE Trans. Industr. Electron. *63* (2016), 3242–3251. DOI:10.1109/TIE.2016.2535119

[17] P. Park, J. W. Ko, and C. Jeong: Reciprocally convex approach to stability of systems with time-varying delays. Automatica *47* (2011), 235–238. DOI:10.1016/j.automatica.2010.10.014

[18] C. Peng, H. Sun, M. Yang, and Y. Wang: A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans. Systems Man Cybernet.: Systems. *49* (2019), 1554–1569. DOI: 10.1109/TSMC.2018.2884952

[19] D. Peng, J. Dong, Z. Cai, C. Zhang, and Q. Peng: A study on stability of cyber-physical systems under false data injection attacks. J. Automat. *45* (2019), 196–205. DOI:10.16383/j.aas.2018.c180331

[20] L. Shi, Q. Dai, and Y. Ni: Review of network attacks in power information physical fusion system environment. Electr. Power Syst. Res. *163* (2018), 396–412. DOI:10.1016/j.epsr.2018.07.015

[21] L. Song, J. Wu, C. Long, and S. Li: Asynchronous event-triggered output feedback control for cps under data injection attacks. In: 37th Chinese Automation Congress (2018), Xi'an, pp. 2530–2535. DOI:10.1109/CAC.2018.8623668

[22] Z. Song, J. Zhai, and H. Ye: Global adaptive output-feedback control for switched uncertain nonlinear systems. Kybernetika *53* (2017), 263–281. DOI:10.14736/kyb-2017-2-0263

[23] A. Teixeira, I. Shames, H. Sandberg, and K. H.Johansson: A secure control framework for resource-limited adversaries. Automatica *51* (2015), 135–148. DOI:10.1016/j.automatica.2014.10.067

[24] Q. Wang, W. Tai, Y. Tang, and M. Ni: A review of the false data injection attack against the cyber physical power system. J. Automat. *45* (2019), 72–83. DOI:10.16383/j.aas.2018.c180369

[25] D. Wang, S. Wu, W. Zhang, G. Wang, F. Wu, and S. Okubo: Model following control system with time delays. Kybernetika *52* (2016), 478–495. DOI:10.14736/kyb-2016-3-0478

[26] S. Xiao, Q.-L. Han, X. Ge, and Y. Zhang: Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks. IEEE Trans. Cybernet., to be published. DOI:10.1109/TCYB.2019.2900478

[27] S. Yan, S. K. Nguang, and L. Zhang: Nonfragile integral-based event-triggered control of uncertain cyber-physical systems under cyber-attacks. Complexity *ID 8194606* (2019), 14 pages. DOI:10.1155/2019/8194606

[28] W. Yu, Z. Deng, H. Zhou, and X. Zeng: Distributed event-triggered algorithm for optimal resource allocation of multi-agent systems. Kybernetika *53* (2017), 747–764. DOI: 10.14736/kyb-2017-5-0747

[29] W. Zeng and M.-Y. Chow: Optimal tradeoff between performance and security networked control systems based on coevolutionary algorithms. IEEE Trans. Industr. Electr. *59* (2012), 3016–3025. DOI:10.1109/TIE.2011.2178216

[30] X.-M. Zhang and Q.-L. Han: Event-triggered dynamic output feedback control for networked control systems. IET Control Theory Appl. *8* (2014), 226–234. DOI:10.1016/j.ins.2018.05.007

[31] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng: Networked control systems: a survey of trends and techniques. IEEE/CAA J. Automat. Sinica, to be published. DOI:10.1109/JAS.2019.1911651

Zhiwen Wang, Corresponding author. College of Electrical and Information Engineering, Lanzhou University of Technology, LanZhou, 730050. P. R. China; Key Laboratory of Gansu Advanced Control for Industrial Processes, Lanzhou University of Technology, Lanzhou 730050. P. R. China; National Demonstration Center for Experimental Electrical and Control Engineering Education, Lanzhou University of Technology, Lanzhou 730050. P. R. China.

e-mail: wwwzhiwen@163.com

Xiangnan Xu, College of Electrical and Information Engineering, Lanzhou University of Technology, LanZhou, 730050. P. R. China; Key Laboratory of Gansu Advanced Control for Industrial Processes, Lanzhou University of Technology, Lanzhou 730050. P. R. China; National Demonstration Center for Experimental Electrical and Control Engineering Education, Lanzhou University of Technology, Lanzhou 730050. P. R. China.

e-mail: idxuxn@163.com

Hongtao Sun, College of Electrical and Information Engineering, Lanzhou University of Technology, LanZhou, 730050. P. R. China

e-mail: huntsun@qfnu.edu.cn

Long Li, College of Electrical and Information Engineering, Lanzhou University of Technology, LanZhou, 730050. P. R. China

e-mail: 815345726@qq.com