Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

# On Event-Triggered Implementation of Moving Target Defense Control

**Tua A. Tamba** * **Bin Hu** ** **Yul Y. Nazaruddin** ***

* *Dept. of Electrical Engineering, Parahyangan Catholic University, Bandung 40141, Indonesia (e-mail: ttamba@unpar.ac.id).*
** *Dept. of Engineering Technology, Old Dominion University, Norvolk, VA 23529, USA (e-mail: bhu@odu.edu)*
*** *Instrumentation & Control Research Group, Institut Teknologi Bandung, Bandung 40132, Indonesia (e-mail: yul@tf.itb.ac.id)*

**Abstract:** This paper proposes an event-triggered switched control system (ET-SCS) scheme for the implementation of moving target defense (MTD) control strategy in cyber-physical system (CPS). The proposed scheme uses the ET-SCS to obfustace the system structure/appearance while at the same time renders the closed loop CPS trajectories stable in the presence of cyber intrusion on the CPS actuator. The paper develops a mechanism for detecting the presence of such intrusions and then shows the asymptotic stability of the closed loop CPS.

*Keywords:* Secure control, moving target defense, event-triggered, switched control systems.

## 1. INTRODUCTION

A cyber-physical system (CPS) is an emerging framework for modern control systems which provides seamsless integration of the involved *physical* (e.g. plant, sensors, actuators) and *cyber* (e.g. computational engine, communication networks) elements. The application of CPS framework relies heavily on the performance of its cyber element to ensure real time and fast control computation, transmission and execution tasks. Alas, the last few decades have also witnessed the increased potential vulnerability of CPS' cyber systems to malicious attacks from adversaries (Humayed et al., 2017; Cardenas et al., 2009), especialy those CPSs which manage national critical infrastructures (cf. e.g. (Lun et al., 2019; Chong et al., 2019; Hu et al., 2018; Ding et al., 2018; Humayed et al., 2017; Yampolskiy et al., 2013; Cheminod et al., 2012; Yampolskiy et al., 2012)). Since both its physical and cyber elements are tightly integrated, any occuring fault/trouble in either of them will eventualy affect the overall performance of and the services provided by the CPS. It is thus crucial to take into account the potential occurrence of such cyber attacks in the design and development of CPS.

Most of the current cyber security strategies are developed under the so-called *static defense* mechanism (SDM) which essentially deploys heavily secured perimeter firewalls and intrusion detection systems to minimize the risk of being attacked/compromised by adversaries (Jajodia et al., 2011; Cardenas et al., 2009; Chong et al., 2019). It is now understood, however, that SDM-based cyber protection often fails when the so-called *information asymmetry* on the defender side is present during the defender-attacker interaction (Jajodia et al., 2011). To address this issue, one alternative approach called *moving target defense* (MTD) has been proposed (Cyberspace, 2011; Jajodia et al., 2011; Okhravi et al., 2013; Zhuang et al., 2014). The MTD scheme basically aims to obscure a cyber system's actual appearance (i.e. *surface*) by creating a moving target which produces a time-variant service availability under different system configurations. In this way, the adversary is blocked (or at least forced to spend significant amount of time and resources) from tracking the system configuration when trying to carry out the attacks (Wang and Lu, 2019). The end goal is thus to balance the constraints on information availability among players in the attacker-defender game by imposing comparable information asymmetry on the attacker side. In recent years, various studies have reported how the MTD scheme can outperform/overcome the SDM limitations and suggested its potential as the future cyber security implementation scheme (Wang and Lu, 2018; Lei et al., 2018; Britton, 2019; DHS, 2013; Burshteyn, 2018). Considering the tight coupling between CPS' communication and control elements, it is then of particular interest to examine ways by which it can benefit from MTD scheme.

This paper examines the use of an event-triggered (ET) strategy to further develop the MTD-based control scheme proposed in (Kanellopoulos and Vamvoudakis, 2020). Note that the basic idea of the MTD scheme in (Kanellopoulos and Vamvoudakis, 2020) is to impose information asymmetry on the attacker side by increasing the defender's closed loop system's entropy through the use of a family of switching controllers (Hespanha and Morse, 1999). This paper extends such a scheme by introducing an ET control scheduling approach (Tabuada, 2007; Lemmon, 2010; Marchand et al., 2012; Heemels et al., 2012) to the defender's control design strategy. The proposed use of ET control scheduling scheme is intended to examine possible reduction on the computational/communication loads of the CPS in securing its functionalities and at the

⋆ This research was funded by Kemenristek/BRIN of the Republic of Indonesia under the Fundamental Research (PDUPT) scheme.

same time guaranteeing its stability. This paper derives conditions on the switching frequency of the designed ET switching controllers that renders the closed loop CPS asymptotically stable, and then proposes a mechanism to detect potential cyber intrusions on the CPS' actuators.

The rest of the paper is structured as follows. Section 2 formulates the system setup and the MTD-based secure control framework. Section 3 analyzes the CPS stability under the proposed ET-based MTD scheme. An intrusion detection scheme and its impact on closed loop CPS stability under cyber intrusion are discussed in Section 4 and Section 5, respectively. Section 6 concludes the paper.

**Notations:** $\mathbb{R}$ and $\mathbb{R}^n$ denote the set of real numbers and an $n$ dimensional vector space, respectively. For a vector $x \in \mathbb{R}^n$ whose its $i$th element is denoted $x_i$ $(i = 1, \ldots, n)$, then $\|x\|$ and $\texttt{supp}(x)$ denote, respectively, the Euclidean norm and the support of $x$. $\lambda(A)$, $\texttt{rank}(A)$, and $\texttt{diag}(A)$ denote the eigenvalues, rank and diagonal elements of a matrix $A \in \mathbb{R}^{n\times n}$, respectively. $\bar{\lambda}(A)$ and $\underline{\lambda}(A)$ are the maximum and minimum of $\lambda(A)$, respectively. For $A \in \mathbb{R}^{n\times n}$, then $A \succeq 0$ means $A$ is positive semi definite.

## 2. SETUP & PRELIMINARIES

### 2.1 System Description

Consider the linear time-invariant (LTI) model of a CPS

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{1a}$$
$$= Ax(t) + b_i u_i(t), \qquad x(0) = x_0, \tag{1b}$$

for all $t \geq 0$, where $x \in \mathbb{R}^n$ and $u \in \mathbb{R}^m$ are the state and input vectors with state and input matrices $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$, respectively, and $b_i$ is the $i$th column of $B$ which corresponds to the $i$th control signal $u_i(t)$ acting on the $i$th actuator. We assume that the actuators of (1) is subject to potential cyber attacks such that (1a) satisfies

$$\dot{x}(t) = Ax(t) + B\tilde{u}(t), \tag{2a}$$
$$\tilde{u}(t) := \gamma(t)u(t) = (\texttt{diag}\{\gamma_{ii}(t)\}_{i=1}^m)\, u(t), \tag{2b}$$

where $\tilde{u}(t)$ is the potentially attacked input with a time-varying attack parameter $\gamma(t)$ satisfying Assumption 1. Thus, $\gamma_{ii} = 1$ implies the system is not being compromised.

*Assumption 1.* For any closed time interval $[t_1, t_2], 0 \leq t_1 \leq t_2$, (i) $\gamma(t)$ is locally integrable, (ii) $\texttt{supp}(\gamma(t)) < m$.

Let $\mathcal{B} := \{b_i\}_{i=1}^m$ be the set of actuators of (1). Define a set $\mathcal{P}(\mathcal{B}) = 2^{\mathcal{B}}$ of possible actuator combinations. Then each matrix $B_j$ $(j = 1, \ldots, 2^m)$ with column elements $b_i$ in (1) is an element of $\mathcal{P}(\mathcal{B})$. We will consider the set $\mathcal{B}_c$ below

$$\mathcal{B}_c = \left\{B_j \,\middle|\, \texttt{rank}\left([B_j\ AB_j\ \cdots\ A^{n-1}B_j]\right) = n\right\} \tag{3}$$

which denotes the set of *candidate actuating modes* which renders the closed loop system (1) fully controllable.

Now, for a set of actuating modes $B_i \in \mathcal{B}_c$, (1) reads

$$\dot{x}(t) = Ax(t) + B_i u_i(t), \quad \forall t \geq 0,\ x(0) = x_0. \tag{4}$$

Assume each pair $(A, B_i)$ is stabilizable and control $u_i(t)$ is generated by ET-based LQR method with cost $J_i$ below

$$J_i = \min_{u_i} \int_0^\infty \left(x^T(t)Q_i x(t) + \rho_i u_i^T(t) R_i u_i(t)\right) d\tau, \tag{5}$$

for all $x_0,\ Q_i \succeq 0,\ R_i \succ 0, \rho_i > 0$ and $i = \{1, 2, \ldots, |\mathcal{B}_c|\}$. The ET control scheme uses two functions: (i) a *feedback control law* $u_i(t) : \mathbb{R}^n \mapsto \mathbb{R}^m$, and (ii) an *event function* $\xi : \mathbb{R}^n \times \mathbb{R}^n \mapsto \mathbb{R}$ which decides if the control input should be updated (if $\xi \leq 0$) or not (if $\xi > 0$).

Let $t_k$ be the update time instant (*event*) of the $k$th control such that the control signal in (5) is of the form $u_i(t),\ \forall t \in [t_k, t_{k+1})$. By the stabilizability assumption of (4), it was shown in Marchand et al. (2012) that an optimal controller $u_i(t)$ for each actuating mode can be obtained using an event-triggered mechanism (ETM) below:

- *event function:*

$$\begin{aligned}\xi(x) = (\nu - 1)x^T(t)\left[A^T P_i + P_i A\right] x(t) \\ - 4\rho_i x^T(t) P_i B_i R_i^{-1} B_i^T P_i \left[\nu x(t) - x(t_k)\right]\end{aligned} \tag{6}$$

- *feedback control law:*

$$\hat{u}_i(t) = -K_i x(t_k) = -2\rho R_i^{-1} B_i^T P_i x(t_k), \tag{7}$$

with $\nu \in (0, 1)$ is a parameter, while the symmetric matrix $P_i \succeq 0$ satisfies the algebraic Riccati equation (ARE):

$$A^T P_i + P_i A - 4\rho P_i B_i R_i^{-1} B_i^T P_i + Q_i = 0. \tag{8}$$

Under the ETM (6)-(7), then (4) with $x(0) = x_0$ becomes

$$\dot{x}(t) = Ax(t) - B_i K_i x(t_k), \quad \forall t \in [t_k, t_{k+1}[, \tag{9}$$

with a time sequence of control updates of the form

$$t_0 := 0,\ \ t_{k+1} = \{t > t_k \,|\, \xi\left(x(t), x(t_k)\right) \geq 0\}. \tag{10}$$

We denote as $\mathcal{K}$ the set of $K_i$s in (7) which forms the set of actuating modes in (3) (note that this implies $|\mathcal{K}| = |\mathcal{B}_c|$).

### 2.2 Switching Controller Modes for Moving Target Defense

When a sequence of several $K_i$s are used in (9), it forms a switched control system and can be used to develop an MTD strategy against cyber intrusions/attacks. By using an appropriate switching rule that orchestrates the activation sequence of $K_i \in \mathcal{K}$, then (9) creates a surface randomization which complicates an attacker's task/goal.

Let $\sigma(t) : [0, \infty) \to \mathcal{I}$ with $\mathcal{I} = \{1, \ldots, |\mathcal{K}|\}$ be a piecewise constant and right continuous switching signal. For each $\sigma(t) = i$ with $i \in \mathcal{I}$, then (9) can be rewritten as an event-triggered switched control systems (ET-SCS) model below.

$$\dot{x}(t) = Ax(t) - B_{\sigma(t)} K_{\sigma(t)} x(t_k), \quad \forall t \in [t_k, t_{k+1}[. \tag{11}$$

The control objective is then to design a switching rule $\sigma(t)$ which minimizes the cost in (5) while at the same time maximizes the unpredictability of the resulting switched systems as captured by the system's information entropy (Kanellopoulos and Vamvoudakis, 2020). This thus creates a trade-off between system optimality (defined by optimal cost $J_i^*$) and unpredictability (defined by system entropy $\mathcal{H}(p) = -p^T \log(p)$ for a simplex $p$ describing the probability that each $K_i$ is active). Such a trade-off can be captured as the probability measure $\mathbb{P}_i$ that the $i$th control gain $K_i$ is active below (Kanellopoulos and Vamvoudakis, 2020).

$$\mathbb{P}_i = \exp\left[-\frac{J_i^*}{\epsilon} - 1 - \epsilon \log\left(e^{-1}\Sigma_{i=1}^{|\mathcal{K}|} e^{\frac{J_i^*}{\epsilon}}\right)\right], \tag{12}$$

with $\epsilon > 0$ is a weighting parameter of the entropy of (11).

### 2.3 Problem Formulation

Motivated by (Kanellopoulos and Vamvoudakis, 2020), this paper aims to investigate the stability of and develop an intrusion detection scheme for (11). To this end, define

for all $t \in [t_k, t_{k+1}[$ the error signal $e(t) = x(t_k) - x(t)$ between the state values at time $t$ and that at the last control update instant $t_k$. Then (11) can be rewritten as

$$\dot{x}(t) = \mathcal{A}_{\sigma(t)}x(t) - B_{\sigma(t)}K_{\sigma(t)}e(t), \quad \forall t \in [t_k, t_{k+1}[, \quad (13)$$

with $\mathcal{A}_{\sigma(t)} = A - B_{\sigma(t)}K_{\sigma(t)}$. We use Assumption 2 below.

*Assumption 2.* (Hespanha and Morse (1999)). The number of switchings $N_\sigma(t_1, t_2)$ of $\sigma(t)$ in the ET-SHS (13) over a time interval $(t_1, t_2)$ with $t_2 \geq t_1 \geq 0$ satisfies

$$N_\sigma(t_1, t_2) \leq N_0 + (t_2 - t_1)/\tau_D, \quad (14)$$

where $N_0 > 0$ and $\tau_D > 0$ denote the *chatter bound* and the *average dwell time* of $\sigma(t)$, respectively.

Given the ET-SHS (13), this paper derives conditions on the switching signal $\sigma(t)$ which ensure the closed loop system is stable and develops an intrusion detection mechanism to identify potential cyber attacks from malicious adversaries. Definition 1 will be used for such purposes.

*Definition 1.* (Exponential Stability). System (13) is said to be *globally exponentially stable* (GES) under the switching signal $\sigma(t)$ if, for any initial condition $x(t_0) := x(0)$ and constants $c_1 \geq 0$ and $c_2 > 0$, the solution $x(t)$ satisfies

$$\|x(t)\| \leq c_1 e^{-c_2(t-t_0)}\|x(0)\|, \qquad \forall t \geq t_0. \quad (15)$$

## 3. STABILITY IN THE ABSENCE OF INTRUSION

This section analyzes the stability of (13). First, we show in Lemma 1 below that the inter-event time of (13) under the ETM in (10) is lower bounded by a positive constant.

*Lemma 1.* Consider system (13) under the ETM in (10) in the absence of attacks. Then for any event time instant $t_k$ and all $t \in [t_k, t_{k+1}[$, the inter-event time $t_{k+1} - t_k$ is lower bounded by a strictly positive constant of the form

$$\triangle t_k^{k+1} = \frac{\ln(1 + \kappa_1\kappa_2)}{\theta_1}, \quad (16)$$

where $\kappa_1 = \frac{\omega_1}{\omega_1+\omega_2}$, $\kappa_2 = \frac{\theta_1}{\theta_1+\theta_2}$, $\omega_1 = \|4\rho P_i B_i R_i^{-1} B_i^T P_i$, $\omega_2 = \|(\nu-1)Q_i\|$, $\theta_1 = \|A\|$, and $\theta_2 = \max_{i\in\mathcal{I}}\|B_iK_i\|$.

**Proof.** Since $e(t) = x(t_k) - x(t)$, we have $\forall t \in [t_k, t_{k+1}[$

$$\begin{aligned}\dot{e}(t) &= -\dot{x}(t) = \mathcal{A}_{\sigma(t)}x(t) - B_{\sigma(t)}K_{\sigma(t)}e(t)\\ &= -\left(A - B_{\sigma(t)}K_{\sigma(t)}\right)x(t) + B_{\sigma(t)}K_{\sigma(t)}e(t)\\ &= -Ax(t) + B_{\sigma(t)}K_{\sigma(t)})\left(x(t) + e(t)\right)\\ &= -Ax(t) + B_{\sigma(t)}K_{\sigma(t)})x(t_k).\end{aligned} \quad (17)$$

In this regard, we may write that

$$\begin{aligned}\frac{d}{dt}\|e(t)\| \leq \|\dot{e}(t)\| &= \| - Ax(t) + B_{\sigma(t)}K_{\sigma(t)})x(t_k)\|\\ &\leq \|Ax(t)\| + \|B_{\sigma(t)}K_{\sigma(t)})x(t_k)\|\\ &\leq \|A\|\|x(t)\| + \|B_{\sigma(t)}K_{\sigma(t)})\|\|x(t_k)\|\\ &\leq \theta_1\|x(t)\| + \theta_2\|x(t_k)\|.\end{aligned} \quad (18)$$

As $x(t) = x(t_k) - e(t) \Rightarrow \|x(t)\| \leq \|e(t)\| + \|x(t_k)\|$, then

$$\begin{aligned}\frac{d}{dt}\|e(t)\| &\leq \theta_1\left(\|e(t)\| + \|x(t_k)\|\right) + \theta_2\|x(t_k)\|\\ &\leq \theta_1\|e(t)\| + (\theta_1 + \theta_2)\|x(t_k)\|.\end{aligned} \quad (19)$$

Thus, in the time interval $[t_k, t_{k+1}[$, the dynamics of $\|e(t)\|$ with initial condition $e(t_k) = 0$ can be upper bounded as

$$\|e(t)\| \leq e^{\theta_1(t-t_k)}\|e(t_k)\| + \int_{t_k}^{t} e^{\theta_1(t-\tau)}(\theta_1 + \theta_2)\|x(t_k)\|\, d\tau. \quad (20)$$

Also, since $e(t) = x(t_k) - x(t)$, then the ETM in (10) can be written in the form $\omega_1\|e(t)\| \leq \omega_2\|x(t)\|$ if it holds that

$$\|e(t)\| \leq \frac{\omega_1}{\omega_1 + \omega_2}\|x(t_k)\|. \quad (21)$$

Thus, if $x(t_k) \neq 0$, before an event is generated, it can be concluded from (20)-(21) that the following must hold.

$$\begin{aligned}\frac{\omega_1}{\omega_1+\omega_2}\|x(t_k)\| &= \int_{t_k}^{t} e^{\theta_1(t-\tau)}(\theta_1 + \theta_2)\|x(t_k)\|\, d\tau\\ &= (\theta_1 + \theta_2)\|x(t_k)\|\int_{t_k}^{t} e^{\theta_1(t-\tau)}\, d\tau\\ &= (\theta_1 + \theta_2)\|x(t_k)\|\left[\frac{1}{\theta_1}\left(e^{\theta_1(t-\tau)}\Big|_{\tau=t}^{\tau=t_k}\right)\right]\\ &= \frac{(\theta_1 + \theta_2)}{\theta_1}\left(e^{\theta_1(t-t_k)} - 1\right)\|x(t_k)\|.\end{aligned}$$

By comparing the coefficients on the left- and right-hand sides of the above equation and simplifying, we have that

$$\frac{\omega_1}{\omega_1 + \omega_2} = \frac{(\theta_1 + \theta_2)}{\theta_1}\left(e^{\theta_1(t-t_k)} - 1\right), \quad (22)$$

which after rearrangement can be written as

$$e^{\theta_1(t-t_k)} = 1 + \frac{\theta_1\omega_1}{(\theta_1 + \theta_2)(\omega_1 + \omega_2)} := 1 + \kappa_1\kappa_2, \quad (23)$$

By defining $\triangle t_k^{k+1} = t_{k+1} - t_k$, we may conclude that

$$\theta_1 \triangle t_k^{k+1} = \ln(1 + \kappa_1\kappa_2), \quad (24)$$

which is the result stated in (16). The proof is complete.

Having shown that the ET-SHS (13) excludes zeno behavior, we now proceed to the derivation of conditions on the switching signal $\sigma(t)$ that will guarantee it to be GES.

*Theorem 1.* Given the ET-SHS (13) with switching signal $\sigma(t) = i$, $(i \in \mathcal{I})$, and the corresponding control gain $K_i$ in (7). Then (13) is GES for any $\sigma(t)$ satisfying (14) if the average dwell time $\tau_D$ of $\sigma(t)$ is bounded from below as

$$\tau_D > \frac{\ln\alpha}{\beta_i} := \frac{\ln\left[\max_{(i,i')\in\mathcal{I}}\left(\overline{\lambda}(P_i)/\underline{\lambda}(P_{i'})\right)\right]}{\nu\max_{i\in\mathcal{I}}\left(\overline{\lambda}(Q_i)/\underline{\lambda}(P_i)\right)}. \quad (25)$$

**Proof.** Set $\sigma(t) = i \in \mathcal{I}$. Consider the Lyapunov function $V_i(x) = x^T(t)P_ix(t)$ for the $i$th actuating mode of (13). Then for any $i, i' \in \mathcal{I}$, it holds for each $V_i(x)$ that

$$\underline{\lambda}(P_i)\|x(t)\|^2 \leq V_i(x) = x^T P_i x \leq \overline{\lambda}(P_i)\|x(t)\|^2 \quad (26)$$

$$\underline{\lambda}(P_{i'})\|x(t)\|^2 \leq V_{i'}(x) = x^T P_{i'} x \leq \overline{\lambda}(P_{i'})\|x(t)\|^2 \quad (27)$$

such that the following relationship can be obtained

$$V_i(x) \leq \overline{\lambda}(P_i)\|x(t)\|^2 \leq \overline{\lambda}(P_i)\left(V_{i'}(x)/\underline{\lambda}(P_{i'})\right) \quad (28)$$

Thus for arbitrary pairs of elements $(i, i') \in \mathcal{I}$, it holds that $V_i(x) \leq \alpha V_{i'}(x)$, where $\alpha = \max_{(i,i')\in\mathcal{I}}\left(\overline{\lambda}(P_i)/\underline{\lambda}(P_{i'})\right)$. Below, the dynamics of (13) are examined for a particular actuating mode, and then continued for different modes.

The time derivative of $V_i(x)$ along (13) can be written as

$$\begin{aligned}\dot{V}_i(x) &= \dot{x}^T(t)P_ix(t) + x^T(t)P_i\dot{x}(t)\\ &= \left[\mathcal{A}_ix(t) - B_iK_ie(t)\right]^T P_ix(t)\\ &\qquad + x^T(t)P_i\left[\mathcal{A}_ix(t) - B_iK_ie(t)\right]\end{aligned} \quad (29)$$

Since $\mathcal{A}_i = A - B_iK_i$ with $K_i$ as in (7), then (29) becomes

$$\begin{aligned}\dot{V}_i &= x^T(t)\big[(A^T - 2\rho P_i B_i R_i^{-1} B_i^T)P_i \\ &\quad + P_i\left(A - 2\rho B_i R_i^{-1} B_i^T P_i\right)\big]x(t) \qquad (30)\\ &\quad - 2x^T(t)P_i B_i\left(2\rho R_i^{-1} B_i^T P_i\right)e(t),\\ &= -x^T(t)Q_i x(t) - 4\rho x^T(t)P_i B_i R_i^{-1} B_i^T P_i e(t) \qquad (31)\end{aligned}$$

where the ARE ($A^T P_i + P_i A - 4\rho P_i B_i R_i^{-1} B_i^T P_i = -Q_i$) in (8) has been used in (30). To examine (31) under possible control updates, consider the period $[t_s,\, t_{s+1}[$ and the inter-event period $[t_k,\, t_{k+1}[$ of the ETM in (10). Assume (13) switches from mode $i$ to $i'$ with $(i, i') \in \mathcal{I}$ at time $t_s$. Then two possible dynamic cases below can be identified.

- *Case 1:* The event where $t_k \le t_s$ and $t_{k+1} \ge t_{s+1}$ such that $[t_s, t_{s+1}[$ contains no triggering time. From (10) and (6), the equality below holds for $t \in [t_k, t_{k+1}[$:
$$\begin{aligned}(\nu-1)x^T(t)\Phi_i x(t) &= 4\rho x^T(t)P_i B_i R_i^{-1} B_i^T P_i \\ &\quad \times \left[\nu x(t) - x(t_k)\right],\end{aligned}$$
with $\Phi_i := A^T P_i + P_i A$. As $e(t) = x(t_k) - x(t)$, then
$$\begin{aligned}(\nu-1)x^T(t)\Phi_i x(t) &= 4\rho x^T(t)P_i B_i R_i^{-1} B_i^T P_i \\ &\quad \times \left[(\nu-1)x(t) - e(t)\right],\end{aligned}$$
which when combined with (8) can be rearranged as
$$4\rho_i x^T(t)P_i B_i R_i^{-1} B_i^T P_i = (\nu-1)x^T(t)Q_i x(t). \quad (32)$$
As a result, (31) becomes
$$\dot{V}_i(x) \le -\nu\overline{\lambda}(Q_i)\|x(t)\|^2, \qquad (33)$$
where $\nu \in (0,1)$ whereas $\overline{\lambda}(Q_i) > 0$ is the largest eigenvalue of the matrix $Q_i \succ 0$. Now note that the following inequalities also hold for $V_i(x)$.
$$\underline{\lambda}(P_i)\|x(t)\|^2 \le V_i(x) = x^T P_i x \le \overline{\lambda}(P_i)\|x(t)\|^2. \quad (34)$$
Taking (26) into account, (33) may be written as
$$\dot{V}_i(x) \le -\nu\overline{\lambda}(Q_i)\left(\frac{V_i(x)}{\underline{\lambda}(P_i)}\right) = -\nu\frac{\overline{\lambda}(Q_i)}{\underline{\lambda}(P_i)}V_i(x). \quad (35)$$
For (35) to hold for any $i \in \mathcal{I}$, it must hold that
$$\dot{V}_i(x) \le -\beta_i V_i(x), \qquad (36)$$
where $\beta_i = \nu \max_{i\in\mathcal{I}}\left(\overline{\lambda}(Q_i)/\underline{\lambda}(P_i)\right) > 0$.
- *Case 2:* The event where $[t_s, t_{s+1}[$ contains (possibly many) control update instances (e.g. $t_k \le t_s < t_{k+1} < \cdots < t_{k+q} \le t_{s+1}$ for $q$ times of control updates during $[t_s, t_{s+1}[$). In this case, (32) remains valid for each inter-event subinterval, implying (36) also holds.

Based on (36), the solution $V_i(x)$ for Case 1 satisfies
$$V_i(x(t)) \le e^{-\beta_i(t-t_s)}V_{i(t_s)}(x(t_s)), \qquad (37)$$
As for Case 2, the solution $V_i(x)$ for each subinterval can be obtained in a similar manner and is given as
$$V_i(x(t)) \le \begin{cases} e^{-\beta_i(t-t_s)}V_{i(t_s)}(x(t_s)),\ t \in [t_s, t_{k+1}[ \\ e^{-\beta_i(t-t_{k+1})}V_{i(t_{k+1})}(x(t_{k+1})),\ t \in [t_{k+1}, t_{k+2}[ \\ \vdots \\ e^{-\beta_i(t-t_{k+q})}V_{i(t_{k+q})}(x(t_{k+q})),\ t \in [t_{k+q}, t_{q+1}[ \end{cases} \quad (38)$$
Note that $e(t)$ is bounded and piecewise continuous (possibly with a finite number of jump discontinuities) on $[t_s, t_{s+1}[$. Since $\sigma(t_s) = \sigma(t_{k+1}) = \cdots = \sigma(t_{k+q})$, it can be inferred that (38) is essentially of the form (37).

We now examine $V_i(x)$ when switchings between different actuating modes exist. For any $t > 0$ and by (14), let $0 := t_0 \le t_1 \le t_2 \le \cdots \le t_s = t_{N_\sigma(0,t)} \le t$ be the time sequence of mode switchings during $[0, t]$. Since $V_i(x) \le \alpha V_{i'}(x)$, we may rewrite (36) as follows.
$$\begin{aligned}V_i(x(t)) &\le \alpha e^{-\beta_i(t-t_s)}V_{i(t_s^-)}(x(t_s^-)) \\ &\le \alpha e^{-\beta_i(t-t_s)}e^{-\beta(t_s-t_{s-1})}V_{i(t_{s-1})}(x(t_{s-1})) \\ &\le \alpha^2 e^{-\beta_i(t-t_{s-1})}V_{i(t_{s-1}^-)}\left(x(t_{s-1}^-)\right) \\ &\le \cdots \\ &\le \alpha^{N_\sigma(t_0,t)}e^{-\beta_i(t-t_0)}V_{i(t_0)}(x(t_0)) \qquad (39)\\ &= e^{\left(-\beta_i(t-t_0)+\ln\alpha^{N_\sigma(t_0,t)}\right)}V_{i(t_0)}(x(t_0)) \\ &\le e^{\left(-\beta_i(t-t_0)+\left(N_0+\frac{t-t_0}{\tau_D}\right)\ln\alpha\right)}V_{i(t_0)}(x(t_0)) \\ &\le e^{(N_0\ln\alpha)}e^{-\left(\beta_- \frac{\ln\alpha}{\tau_D}\right)(t-t_0)}V_{i(t_0)}(x(t_0)).\end{aligned}$$
As a result, (39) can be used to obtain
$$\|x(t)\| \le \sqrt{\frac{\overline{\lambda}(P_i)}{\underline{\lambda}(P_i)}}e^{\left(\frac{N_0\ln\alpha}{2}\right)}e^{-\frac{1}{2}\left(\beta_i - \frac{\ln\alpha}{\tau_D}\right)(t-t_0)}\|x(t_0)\|. \quad (40)$$
Letting $c_1 = \sqrt{\frac{\overline{\lambda}(P_i)}{\underline{\lambda}(P_i)}}e^{\left(\frac{N_0\ln\alpha}{2}\right)}$ and $c_2 = \frac{1}{2}\left(\beta_i - \frac{\ln\alpha}{\tau_D}\right)$, then the system is GES as per Definition 1 if the average dwell time $\tau_D$ of (13) satisfies condition (25) in the theorem.

## 4. AN INTRUSION DETECTION SCHEME

This section derives an upper bound for the system trajectories under actuator intrusion event and the deviation bound of such trajectories from the optimal one when no intrusion is present. A mechanism to detect potential presence of such intrusions is also presented.

### *4.1 Upper Bound of Trajectory Deviation Under Intrusion*

Let $\hat{x}(t)$ and $\tilde{x}(t)$ denote the closed loop trajectories in the absence and presence of actuator intrusion, respectively. Fix a time period $[t_0, t]$. Then $\hat{x}(t)$ is essentially an optimal trajectory under the optimal LQR control (7) of the form
$$\dot{\hat{x}}(t) = (A - B_i K_i)\hat{x}(t) - B_i K_i e(t), \quad x(t_0) = x_0. \quad (41)$$
Meanwhile, the trajectory under intrusion satisfies
$$\dot{\tilde{x}}(t) = (A - B_i\gamma(t)K_i)\tilde{x}(t) - B_i\gamma(t)K_i e(t), \qquad (42)$$
which through rearrangement can be rewritten as
$$\begin{aligned}\dot{\tilde{x}}(t) &= (A - B_i\gamma(t)K_i)\tilde{x}(t) - B_i\gamma(t)K_i e(t) \\ &\quad - B_i\gamma(t)K_i e(t) + B_i K_i e(t) - B_i K_i e(t) \\ &= (A - B_i K_i)\tilde{x}(t) - B_i K_i e(t) \\ &\quad + B_i\left[I - \gamma(t)\right]K_i\left[\tilde{x}(t) + e(t)\right] \\ &= \mathcal{A}_i\tilde{x}(t) - B_i K_i e(t) + B_i\left[I - \gamma(t)\right]K_i\left[\tilde{x}(t) + e(t)\right], \qquad (43)\end{aligned}$$
with $\mathcal{A}_i = A - B_i K_i$. We then have the following result whose proof can be found in (Tamba et al., 2019).

*Proposition 1.* The deviation $\varepsilon(t) = \tilde{x}(t) - \hat{x}(t)$ between the trajectories in (41) and (43) is bonded from above as
$$\|\varepsilon(t)\| \le \mathcal{E}(\gamma, \tau)\|x_0\|, \qquad (44)$$
where $\mathcal{E}(\cdot) = \frac{\xi_i}{\kappa_i}\int_{t_0}^{t}\mu_i(\tau)\|I - \gamma(\tau)\|e^{\frac{1}{\kappa_1}\int_{t_0}^{t}\mu_i(s)\|I-\gamma(s)\|ds}d\tau$.

From (44), one may sees for the case $\gamma(t) = I$ (no intrusion) that $\varepsilon(t)$ is zero, suggesting that such a deviation signal may be utilized to identify possible presence of actuator intrusion.

### *4.2 Trajectory Deviation-based Intrusion Detection Scheme*

By taking into account the derived trajectory deviation bound in (44), a detection scheme for the presence of actuator intrusion in the proposed ET MTD framework can be derived. This fact is formally state in Theorem 2 below (refer to (Tamba et al., 2019) for the proof).

*Theorem 2.* For the ET SHS (13) with control law (7) and a finite duration $\delta > 0$, define an intrusion detection signal

$$\pi(t) = V_i\left(\tilde{x}(t-\delta)\right) - V_i\left(\tilde{x}(t)\right) - \int_{t-\delta}^{t} \left(\tilde{x}(\tau)Q_i\tilde{x}(\tau) + \rho\hat{u}_i^T(\tau)R_i\hat{u}_i(\tau)\right) d\tau. \quad (45)$$

Then there exists an intrusion on the system if and only if $\pi(t) \neq 0$. In particular, the resulting optimality loss is bounded for any integrable injected intrusion signal as

$$\|\bar{\pi}(t)\| \leq \mathcal{B}(\gamma,\tau)\|x_0\|^2 \quad (46)$$

where for $\hat{\beta}_i = \|e^{-\beta(t-t_0)/2}\|$, the function $\mathcal{B}(\gamma,\tau)$ satisfies

$$\mathcal{B}(\gamma,\tau) = \|P_i\|\|\mathcal{E}(\gamma,t)\|^2 + 2\hat{\beta}_i\|P_i\|\|\mathcal{E}(\gamma,t)\| + \int_{t-\delta}^{t}\left(\|\Omega\|\|\mathcal{E}(\gamma,\tau)\|^2 + 2\hat{\beta}_i\|\mathcal{E}(\gamma,\tau)\|\|\Omega\|\right) d\tau \quad (47)$$

One may sees in the proof of Theorem 2 that the cost that results on the closed loop system is zero whenever $\gamma(t) = I$ (i.e. intrusion is absent). This suggests that any occuring change in the value of the cost function with respect to its nominal optimal value can be used as a detection signal for possible presence of actuator intrusion on the system.

## 5. STABILITY IN THE PRESENCE OF INTRUSION

Using the proposed intrusion detection scheme, one may further examines the stability of the closed loop system in the presence of actuator intrusion. To this end, note from (12) that the probability $\mathbb{P}_i > 0$ that each mode $i \in \mathcal{I}$ is active is greater than zero. This implies that there exists a final time $t_f^*$, sufficiently long enough after the initial time $t_0$, until which the system has been switched through all available modes. Then under the assumption that the attacker is not able to compromise all of the system actuators at once (cf. Assumption 1), the following result on the stability of the system in the presence of actuator intrusion may be stated. The proof of this theorem resembles that of (Kanellopoulos and Vamvoudakis, 2020, Theorem 4), and is thus omitted.

*Theorem 3.* Consider system (9) under the ETM (10) and the set of stabilizing controllers $\mathcal{K}$. Denote as $\mathcal{K}_c \subset \mathcal{K}$ the set of controllers that are compromised by the attacker such that $\mathcal{K} \setminus \mathcal{K}_c \neq \emptyset$. Assume the MTD strategy is designed such that whenever an intrusion on the $i$th actuator/mode is detected then the system switches to the controller with the best performance and the corresponding $i$th mode is taken out of the queue for the next actuator switchings. Then the closed loop system is asymptotically stable under the proposed MTD control strategy.

## 6. CONCLUDING REMARK

This paper has presented an ET-SCS method for implementing the MTD control strategy in CPS. More specifically, the proposed method uses an event triggered-based switching controller strategy to obfustace the system structure/appearance while at the same time render the closed loop system trajectories bounded from above in the presence of actuator intrusion. The paper also proposes a scheme to detect the presence of actuator intrusion on the system and analyzes the stability the resulting closed system. Future works will be aimed toward examining the implementation of the proposed MTD control framework in CPS with nonlinear dynamics.

## ACKNOWLEDGEMENTS

This research was funded by the Ministry of Research and Technology/ National Research and Innovation Agency (Kemenristek/BRIN) of the Republic of Indonesia under the Fundamental Research (PDUPT) scheme year 2020.

## REFERENCES

Britton, D. (2019). 3 reasons why moving target defense must be a priority. URL `https://gcn.com/articles/2019/06/10/moving-target- defense.aspx`.

Burshteyn, M. (2018). Moving target defense state of the field in 2018? URL `https://blog.cryptomove.com/`.

Cardenas, A. et al. (2009). Challenges for securing cyber physical systems. In *Proc. Wksh. Future Directions in Cyber-Physical Systems Security*, volume 5.

Cheminod, M., Durante, L., and Valenzano, A. (2012). Review of security issues in industrial networks. *IEEE Trans. Ind. Inform.*, 9(1), 277–293.

Chong, M.S., Sandberg, H., and Teixeira, A.M. (2019). A tutorial introduction to security and privacy for cyber-physical systems. In *Proc. 17th ECC*, 968–978.

Cyberspace, T. (2011). Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program. *National Science & Technology Council*.

DHS (2013). Moving target defense. URL `https://www.dhs.gov/science-and-technology/csd-mtd`.

Ding, D. et al. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275, 1674–1683.

Heemels, W., Johansson, K.H., and Tabuada, P. (2012). An introduction to event-triggered and self-triggered control. In *Proc. 51st IEEE CDC*, 3270–3285.

Hespanha, J.P. and Morse, A.S. (1999). Stability of switched systems with average dwell-time. In *Proc. 38th IEEE CDC*, 2655–2660.

Hu, Y. et al. (2018). A survey of intrusion detection on industrial control systems. *Int. J. Distrib. Sens. Net.*, 14(8), 1550147718794615.

Humayed, A., Lin, J., Li, F., and Luo, B. (2017). Cyber-physical systems securitya survey. *IEEE Internet Things J.*, 4(6), 1802–1831.

Jajodia, S. et al. (2011). *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer.

Kanellopoulos, A. and Vamvoudakis, K.G. (2020). A moving target defense control framework for cyber-physical systems. *IEEE Trans. Autom. Control*, 65(3), 1029–1043.

Lei, C. et al. (2018). Moving target defense techniques: A survey. *Security and Communication Networks*, 2018.

Lemmon, M. (2010). Event-triggered feedback in control, estimation, and optimization. In *Networked Control Systems*, 293–358. Springer.

Lun, Y.Z. et al. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *J. Syst. Software*, 149, 174–216.

Marchand, N., Durand, S., and Castellanos, J.F.G. (2012). A general formula for event-based stabilization of nonlinear systems. *IEEE Trans. Autom. Control*, 58(5), 1332–1337.

Okhravi, H., Hobson, T., Bigelow, D., and Streilein, W. (2013). Finding focus in the blur of moving-target techniques. *IEEE Secur. Priv.*, 12(2), 16–26.

Tabuada, P. (2007). Event-triggered real-time scheduling of stabilizing control tasks. *IEEE Trans. Autom. Control*, 52(9), 1680–1685.

Tamba, T.A., Hu, B., and Nazaruddin, Y.Y. (2019). An actuator intrusion detection mechanism for event-triggered moving target defense control. In *Proc. IEEE 6th ACDT*, 111–114.

Wang, C. and Lu, Z. (2018). Cyber deception: Overview and the road ahead. *IEEE Secur. Priv.*, 16(2), 80–85.

Wang, C. and Lu, Z. (2019). *Proactive and Dynamic Network Defense*. Springer.

Yampolskiy, M. et al. (2012). Systematic analysis of cyber-attacks on cps-evaluating applicability of DFD-based approach. In *Proc. 5th ISRCS*, 55–62.

Yampolskiy, M. et al. (2013). Taxonomy for description of cross-domain attacks on CPS. In *Proc. 2nd ACM HiCoNS*, 135–142.

Zhuang, R., DeLoach, S.A., and Ou, X. (2014). Towards a theory of moving target defense. In *Proc. 1st ACM Workshop on Moving Target Defense*, 31–40.