Optimal Control of an Uncertain Linear Networked Control System Under Denial of Service Attacks

Tua Agustinus Tamba

***Abstract*—Controller design based on networked control system (NCS) framework combines sensing, control, and actuation tasks using shared channel of communication network. Such a use of communication channel often makes the NCS design more challenging due to the presence of system uncertainties, limitation on available computational/communication systems resources, as well as possible occurrences of data transmission failures or cyber attacks. This paper develops mathematical grounds for dynamic event-triggered control design method for an uncertain linear NCS with matched uncertainties whose communication channel undergoes cyber attaks in the form of *Denial-of-Service* (DoS). The DoS attacks are assumed to halt the execution of control update tasks that was scheduled by the dynamic event-triggered control scheme. Under such possible occurrences of DoS attacks, this paper bounds the allowable duration of the DoS presence and derives suitable control signals which can guarantee the closed loop NCS remains stable.**

***Index Terms*—Optimal Control, Uncertain Linear Networked, Networked Control System.**

I. Introduction

NCS typically uses a network of computers and dedicated communication system to regulate the data interactions/exchanges between the plant, sensor, controller and actuator elements [1]. This coupling between physical, computational and communication components often makes the NCS implementation becomes more challenging. Over the last two decades, significant studies and researches on NCS design are continuously done to improve NCS' resource utilization efficiency as well as robustness to cyber attacks.

To improve the efficiency of NCS' resource utilization, a new control scheduling approach based on a static event-triggered scheme (SETS) was proposed recently [2], [3]. The SETS is essentially an *aperiodic* sampling strategy which updates the control signals only when some predefined conditions (events) on the systems are satisfied. When compared to the commonly practiced periodic update schemes, the SETS-based method is shown to be more *resource-aware* as it utilizes the computational resource more efficiently [4], [5].

With regard to the used communication systems, previous studies on NCS design have commonly focused on examining the effects of communication system constraints (such as transmission delay, data quantization, or packet drops) on the closed loop NCS stability and performances (cf. [6] and references therein). Such studies on NCS communication constraints are usually done under the assumption that the used communication channels are predesigned such that their models and bounded uncertainties are known [7], [8].

In recent years, increased attentions have been given to explore and address related issues on NCS security to cyber attacks. This new research trend is particularly driven by real life observation of NCS applications which demonstrate their vulnerability to unpredictable cyber attacks [9], [10], [11], [12], [13]. One of such attacks is the well-known *denial-of service* (DoS) attack which can reduce or even diminish the timeliness of data transmission between different elements of the NCS. When coupled with possible uncertainties on the NCS model, the occurrence of DoS attacks can significantly deteriorate both the performance and stability of NCS. These thus suggest the need for NCS design frameworks which can ensure not only the efficiency of resource utilization but also the resiliency towards possible cyber attacks [14], [15], [16].

This paper presents mathematical grounds of a dynamic event-triggered scheme (DETS) for the design of uncertain linear NCS which is subjected to DoS attacks. The considered model uncertainty is assumed to be of *matched uncertainty* type [17], while the DoS attack is modeled as in [18], [19] which only assumes limited information about attacks' duration and frequency. This paper presents DETS formulation of the optimal control solution to uncertain linear systems as developed in [17], and then derives an update scheme for control signals that can guarantee the input-to-state stability (ISS) property of the closed loop system. In particular, the derived control signal and its update scheme illustrate the impacts of DoS attacks' presence/absence on the ISS property of the NCS.

Notations: $\mathbb{I}$ denotes the set of nonnegative integers. $\mathbb{R}$ and $\mathbb{R}_0^+$, respectively, are the sets of real and nonnegative real numbers, while $\mathbb{R}^n$ is Euclidean space of dimension n. $\|x\|$ is the norm of a vector $x \in \mathbb{R}^n$. $\overline{\lambda}(M)$ and $\underline{\lambda}(M)$, respectively, are the maximum and minimum of the eigenvalues $\lambda(M)$ of matrix M. $M \succeq 0$ means matrix M is positive semidefinite. $F(\cdot) \in \mathcal{K}$ means $F(\cdot)$ belongs to class $\mathcal{K}$ function such that it is continuous, strictly increasing, and $F(0) = 0$. $F(\cdot) \in \mathcal{K}_\infty$ means $F(\cdot)$ is of class $\mathcal{K}$ function which further satisfies $F(\zeta) \to +\infty$ as $\zeta \to +\infty$. For a function $F(t),\ t > 0$, $F(t^-)$ denotes the limit of $F(\tau)$ as $\tau \rightsquigarrow t$ from the left, such that $F(t^-) := F(t)$ when F is continuous at t.

II. Problem Setup and Formulation

We first recall the model of an uncertain linear NCS with its corresponding optimal controller, and then presents the closed loop control problem to be considered in this paper when DoS attacks occurrences are taken into consideration.

Tua Agustinus Tamba is with Department of Electrical Engineering, Parahyangan Catholic University, Bandung 40132, West Java, Indonesia e-mail: ttamba@unpar.ac.id.

Manuscript received February 27, 2023; accepted August 4, 2023.

A. An Uncertain Linear NCS Model

We consider an uncertain linear NCS model below.

$$\dot{x}(t) = A(p)x(t) + Bu(t), \qquad x(0) = x_0, \tag{1}$$

with state $x(t) \in \mathbb{R}^n$ and input $u(t) \in \mathbb{R}^m$. B is the input matrix, and the system matrix $A(p)$ with uncertain parameter $p \in \mathcal{P}$ satisfies the *matched uncertainty* below [20]:

- for a nominal parameter $p_0 \in p$, the pair $\{A(p_0), B\}$ is stabilizable
- given some matrices R, $S \succeq 0$, there is a matrix $\zeta(p)$ such that: $\zeta^T(p)R\zeta(p) \leq S$. Also, for some known p_0:

$$A(p) - A(p_0) = B\zeta(p). \tag{2}$$

The matched uncertainty property allows (1) to be written as

$$\dot{x}(t) = A(p_0)x(t) + Bu(t) + B\zeta(p)x(t). \tag{3}$$

The controls of NCS (3) can be done using LQR design approach to ensure the closed loop asymptotic stability for all $p \in \mathcal{P}$ [17]. In particular, a feedback control signal of the form $u(t) = K^\intercal x(t)$ can be searched through the minimization of the following cost function.

$$J = \int_0^\infty \left(x(t)^\intercal \left(\mathcal{S} + Q\right) x(t) + u(t)^\intercal(t) R u(t)\right) dt, \tag{4}$$

in which $\mathcal{S} := \inf\{S : \zeta(p)^\intercal\zeta(p) \leq S\}$. In this regard, an optimal control law for (3) is of the following form

$$u(t) = -R^{-1}B^\intercal P x(t) = K^\intercal x(t), \tag{5}$$

with $P \succeq 0$ satisfies an algebraic Riccati equation below.

$$P^\intercal A(p_0) + A^\intercal(p_0)P + \mathcal{S} + Q - PBR^{-1}B^\intercal P = 0. \tag{6}$$

B. Problem Formulation

Consider the NCS setup of (3)–(5) as shown in Fig. 1. Assume the control signal (5) is generated using a zero-order hold sampler and then transmitted through a communication channel to the plant/actuator. Let $\{t_i\}_{i\in\mathbb{I}}$ with $t_0 := 0$ denotes the sequence of control signal update times. Then for two successive update times, the control signal (5) satisfies

$$u(t) = K^\intercal x(t_i), \qquad \forall t \in [t_i, t_{i+1}), \tag{7}$$

such that the closed loop NCS model (3) can be written as

$$\dot{x}(t) = A(p_0)x(t) + BK^\intercal x(t_i) + B\zeta(p)x(t). \tag{8}$$

Define the error $e(t)$ between the values of NCS states at the last control update time and at the current time t below.

$$e(t) = x(t_i) - x(t), \qquad \forall t \in [t_i, t_{i+1}). \tag{9}$$

Using (9), model (8) can be rewritten for all $t \in [t_i, t_{i+1})$ as

$$\dot{x}(t) = \left(A(p_0) + BK^\intercal\right) x(t) + BK^\intercal e(t) + B\zeta(p)x(t). \tag{10}$$

The objective of this paper is to study the stability property of NCS model (10) when its communication channels are subjected to DoS attacks (cf. Fig. 1). For this purpose, our analysis will use a DoS attack model developed in [18].

Let $\{\delta_n\}_{n\in\mathbb{I}}$ be the sequence of times when DoS attacks occur. Define $\mathcal{D}_n := [\delta_n, \delta_{n+1})$ as the time interval of the

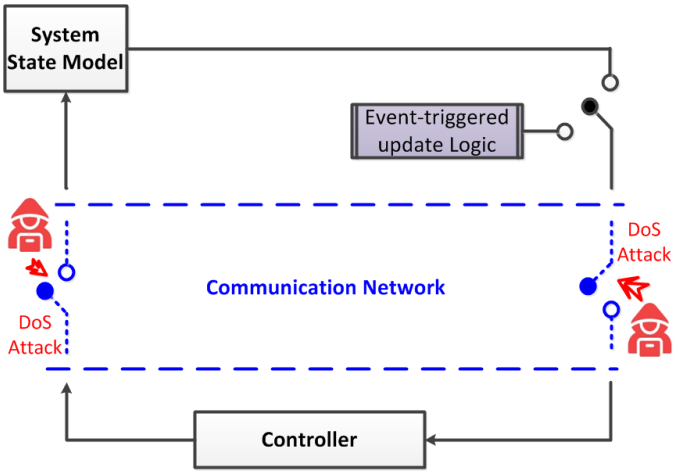

Fig. 1. NCS schematic of (3) and (5) under DoS attacks.

nth DoS with duration τ_n during which the communication between controller and system actuator is compromised. During such a duration, the system actuator is assumed to implement the last succesfully received control signal. By the definitions of such $\delta_n, \mathcal{D}_n$ and t_n, the time duration $[0, t]$ can be partitioned into the following elements:

- The set $\Omega(t)$ denoting the period up to time "t" at which the controller–actuator communication exists, i.e.:

$$\Theta(t) := [0, t] \backslash \cup_{n\in\mathbb{I}}\, \mathcal{D}_n. \tag{11}$$

  The control signal (7) is implemented during $\Theta(t)$.
- The set $\Omega(t)$ denoting the instances of DoS occurrences when controller–actuator communication do not exist:

$$\Omega(t) := \cup_{n\in\mathbb{I}}\, \mathcal{D}_n \cap [0, t]. \tag{12}$$

  The control signal at each element of $\Omega(t)$ is:

$$u(t) = K^\intercal x\left(t_{i(t)}\right) \tag{13}$$

  where the subscript $i(t)$ is defined as:

$$i(t) := \begin{cases} -1, & \text{if } \theta(t) = \emptyset \\ \sup\left(i \in \mathbb{I} : t_i \in \Theta(t)\right), & \text{otherwise} \end{cases} \tag{14}$$

  It can be seen that (13) essentially defines the latest control signal received and updated by the actuators.

It is also assumed that the DoS sequence $\{d_n\}_{n\in\mathbb{I}}$ satisfies

$$\inf_{n\in\mathbb{I}}\, \tau_n > 0, \tag{15}$$

and that the following holds on $\Omega(t)$ for a constant $\kappa > 0$:

$$|\Omega(t)| \leq \kappa + \frac{t}{T}. \tag{16}$$

Condition (15) basically assumes that the occurrence of DoS is *regular* (i.e. the occurrence frequency is finite and *non-Zeno*), while (16) sets the DoS' *slow-on-the-average* property with *average dwell-time* parameter of T (cf. [21]).

Given NCS model (10) and DoS characteristics (11)-(16), we aim to bound the allowable time duration of DoS presence as well as suitable control signals that can stabilize the closed loop NCS. In [18], this problem was first examined for LTI

systems of the form $\dot{x}(t) = Ax(t) + Bu(t)$ using SETS [2] with control update time logic as follows: $t_0 = 0$, and

$$t_{i+1} = \inf\big\{t \in \mathbb{R} \;\big|\; t > t_i \wedge \sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t^-)] \leq 0\big\} \quad (17)$$

with $\sigma \in (0,1)$. Choosing a Lyapunov function $V(x(t)) = x(t)^\intercal P x(t)$ with $P \succeq 0$, [18] showed that LTI systems with control update logic (17) that are attacked by DoS satisfying (15)-(16) will remain GAS if the conditions below hold:

$$\text{(i) } \gamma_1 > \sigma\gamma_2, \;\; \text{and} \;\; \text{(ii) } \tau > 1 + \frac{\alpha_2\gamma_2\,(2+\sigma)}{\alpha_1\,(\gamma_1 - \sigma\gamma_2)} \quad (18)$$

with $\gamma_1 = \underline{\lambda}(Q), \gamma_2 = 2\|PBK^\intercal\|$, $\alpha_1 = \underline{\lambda}(P)$, $\alpha_2 = \overline{\lambda}(P)$, and $Q \succeq 0$ satisfies $(A+BK^\intercal)^\intercal P + P^\intercal(A+BK^\intercal) = -Q$. The work in [22] extends the results in [18] for uncertain linear NCS of the form (10) using update logic in (17), while [23] examined similar problem as in [18] but using a DETS that was proposed in [24] as the control update time logic.

This paper essentially further develops the results in [18], [22], [23] by addressing DoS-resilient control design problem for uncertain linear NCS of the form (10) using DETS framework. The inclusion of system uncertainties in NCS model and analysis makes the proposed method more realistic/applicative. Furthermore, as shown in [24], the use of DETS also provides a sequence of control update times with longer inter-sampling intervals and therefore ensures more efficient utilization of the available NCS resources.

The DETS that is used in this paper assumes the following sequence of control update times [24]: $t_0 = 0$, and

$$t_{i+1} = \inf\{t \in \mathbb{R} \,|\, t > t_i \,\wedge\, \eta(t) + \theta[\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t^-)] \leq 0\} \quad (19)$$

where the dynamic variable $\eta(t)$ satisfies equation below.

$$\dot{\eta}(t) = -\varphi\eta(t) + \sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t) \quad (20)$$

with $\eta(0) = \eta_0$. This paper's objective is to examine required conditions under which the closed loop NCS (10) maintains an ISS property when using DETS (19)-(20) and is subjected to DoS attacks. Definition 1 formalizes such an ISS concept.

Definition 1. *Dynamical systems of the form (10) is said to satisfy the ISS property if for all $x(0) := x_0 \in \mathbb{R}^n$, there exist an ISS Lyapunov function $V(x(t)) : \mathbb{R}^n \times \mathbb{R}_+ \to \mathbb{R}_+$ and functions $\alpha_1, \alpha_2, \varphi, \xi \in \mathcal{K}_\infty$ of class $\mathcal{K}_\infty$ such that:*

1) $\alpha_1\left(\|x(t)\|^2\right) \leq V(x(t)) \leq \alpha_2\left(\|x(t)\|^2\right)$,
2) $\dot{V}(x(t)) \leq -\varphi\left(\|x(t)\|\right) + \xi\left(\|e(t)\|\right)$.

III. Main Results

This section presents this paper's main results regarding properties of DETS (19)-(20) and their use to derive conditions for ISS of NCS (10) when DoS attacks are present.

A. Properties of Dynamic Event-Triggered Scheme

Lemma 1 below shows that the dynamic variable $\eta(t)$ in DETS (19)-(20) is always non-negative. Such a property will be useful for deriving the ISS conditions of NCS (10).

Lemma 1. *Consider the DETS in* (19)-(20)*. Then for all $t \in [t, \infty)$, the following inequalities hold for $\eta(t)$:*

1) $\eta(t) + \theta\left(\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t)\right) \geq 0$
2) $\eta(t) \geq 0$

Proof. We first show that condition 1) in Lemma 1 is true. The construction of the DETS update times logic (19) implies that the following holds for all $t \in [0, \infty)$.

$$\eta(t) + \theta\left(\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t^-)\right) \geq 0 \quad (21)$$

By noting that $e(t) \geq e(t^-)$ holds for all $t \in [0, \infty)$, then (21) implies that the following also true.

$$\eta(t) + \theta\left(\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t)\right) \geq 0, \quad (22)$$

which is statement 1) in Lemma 1. Now we show 2) by examining (22) when $\theta = 0$ and $\theta \neq 0$. If $\theta = 0$, (22) reads

$$\eta(t) \geq 0 \quad (23)$$

Next, if $\theta \neq 0$, then (22) becomes

$$\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t) \geq -\frac{1}{\theta}\eta(t). \quad (24)$$

Based on (23) and (24), the dynamics of $\eta(t)$ in (20) becomes

$$\dot{\eta}(t) \geq -\left(\varphi + 1/\theta\right)\eta(t), \qquad \eta(0) \geq 0. \quad (25)$$

By the comparison lemma [25], then (25) implies that

$$\eta(t) \geq \eta(0)e^{-(\varphi+1/\theta)t}, \qquad \eta(0) \geq 0 \quad (26)$$

which proves $\eta(t) \geq 0$ as in statement 2) of Lemma 1. □

Next, Lemma 2 shows that the inter-execution time (t_{i+1}) of DETS (19)-(20) is greater than that of the SETS in (17).

Lemma 2. *Let t^s_{i+1} be the next $(i+1)$th control update time of SETS* (17)*, and t^d_{i+1} be the next $(i+1)$th control update time of DETS* (19)*. Then, it holds that: $t^d_{i+1} \geq t^s_{i+1}$.*

Proof. Assume for the moment that $t^s_{i+1} \geq t^d_{i+1}$. Then the SETS update logic (17) implies the following must hold.

$$\sigma x(t^d_{i+1})^\intercal Q x(t^d_{i+1}) - 2x(t^d_{i+1})^\intercal PBK^\intercal e(t^d_{i+1}) > 0 \quad (27)$$

Now, consider the DETS update logic (19) for two cases of θ values. Firstly, if $\theta > 0$, then the update time logic (19) and the non-negativity of $\eta(t)$ showed in Lemma 1 imply:

$$\begin{aligned} 0 \geq \eta(t^d_{i+1}) + \theta\big[&\sigma x(t^d_{i+1})^\intercal Q x(t^d_{i+1}) \\ &- 2x(t^d_{i+1})^\intercal PBK^\intercal e(t^d_{i+1})\big], \\ \geq \theta\big[&\sigma x(t^d_{i+1})^\intercal Q x(t^d_{i+1}) - 2x(t^d_{i+1})^\intercal PBK^\intercal e(t^d_{i+1})\big]. \end{aligned} \quad (28)$$

Since $\theta \geq 0$, then (28) will hold only if (29) below is true.

$$\sigma x(t^d_{i+1})^\intercal Q x(t^d_{i+1}) - 2x(t^d_{i+1})^\intercal PBK^\intercal e(t^d_{i+1}) < 0. \quad (29)$$

Note that (29) contradicts (27), so $t^d_{i+1} \geq t^s_{i+1}$ should instead be true. Secondly, if $\theta = 0$, the DETS update logic in (19) implies $\eta^d_{t+1} \leq 0$, and so the $\eta(t)$ dynamics in (20) becomes

$$\dot{\eta}(t) \leq 0 \;\Rightarrow\; \sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t) \leq 0. \quad (30)$$

Again, (30) contradicts the assumption in (27) and therefore $t^d_{i+1} \geq t^s_{i+1}$ should instead be true as stated in Lemma 2. □

Lastly, we present in Lemma 3 below an upper bound for the functional of the error $e(t)$ when DoS attacks are present.

Lemma 3. *Consider NCS* (10) *under DETS control update time logic* (19)-(20)*. Assume the NCS is subjected to DoS attacks with properties as in* (11)–(16)*. Then for all $t \in \Omega(t)$, the inequality below holds regarding the error $e(t)$ in* (9)*.*

$$\begin{aligned} 2\gamma_2\|x(t)\|\|e(t)\| \leq (\sigma\gamma_1 + 2\gamma_2)\|x(\delta_n)\|^2 \\ + 2\gamma_2\|x(t)\|^2 + \frac{1}{\theta}\|\eta(\delta_n)\| \end{aligned} \quad (31)$$

Proof. On the one hand, note for the error $e(t)$ in (9) that the following can be written for all $t \in \Omega(t)$.

$$e(t) = x(t_{i(\delta_n)}) - x(t) \quad (32)$$

On the other hand, the construction of control update time logic (19) implies the following also holds for all $t \in \Omega(t)$.

$$2x(\delta_n)^\intercal PBK^\intercal e(\delta_n) \leq \sigma x(\delta_n)^\intercal Q x(\delta_n) + \frac{1}{\theta}\eta(\delta_n) \quad (33)$$

Consequently, we can write the norm of (33) as below.

$$\begin{aligned} &2\|PBK\|\|x(\delta_n)\|\|e(\delta_n)\| \leq \sigma\underline{\lambda}(Q)\|x(\delta_n)\|^2 + \frac{1}{\theta}\|\eta(\delta_n)\| \\ &2\gamma_2\|x(\delta_n)\|\left(\|x(t_{i(\delta_n)}) - x(d_n)\|\right) \leq \sigma\gamma_1\|x(\delta_n)\|^2 \\ &\qquad + \frac{1}{\theta}\|\eta(\delta_n)\| \\ &2\gamma_2\|x(\delta_n)\|\|x(t_{i(\delta_n)})\| \leq 2\gamma_2\|x(\delta_n)\|^2 + \sigma\gamma_1\|x(\delta_n)\|^2 \\ &\qquad + \frac{1}{\theta}\|\eta(\delta_n)\| \end{aligned} \quad (34)$$

As a result, the following functional relationship can be obtained based on the error $e(t)$ definition in (32).

$$2x(t)^\intercal PBK^\intercal e(t) = 2x(t)^\intercal PBK^\intercal\left(x(t_{i(\delta_n)}) - x(t)\right) \quad (35)$$

By taking the norm of (34), we then have that:

$$\begin{aligned} 2\|PBK^\intercal\|\|x(t)\|\|e(t)\| &\leq 2\|PBK\|\|x(t)\|\|x_{t_{i(\delta_n)}}\| \\ &\quad + 2\|PBK\|\|x(t)\|^2 \\ &\leq 2\|PBK\|\|x(d_n)\|\|x_{t_{i(\delta_n)}}\| \\ &\quad + 2\|PBK\|\|x(t)\|^2 \end{aligned} \quad (36)$$

The substitution of (35) into (36) allows us to write (36) as

$$\begin{aligned} 2\gamma_2\|x(t)\|\|e(t)\| &\leq 2\gamma_2\|x(\delta_n)\|^2 + \sigma\gamma_1\|x(\delta_n)\|^2 \\ &\quad + \frac{1}{\theta}\|\eta(\delta_n)\| + 2\gamma_2\|x(t)\|^2 \\ &\leq (\sigma\gamma_1 + 2\gamma_2)\|x(\delta_n)\|^2 \\ &\quad + 2\gamma_2\|x(t)\|^2 + \frac{1}{\theta}\|\eta(\delta_n)\| \end{aligned} \quad (37)$$

which is as stated in the lemma. The proof is completed. □

In subsections III-B-III-C, we use the DETS properties derived in this subsection to characterize conditions which will guarantee the ISS property of uncertain linear NCS (10) in the absence or presence of DoS attacks.

B. NCS Stability Analysis: DoS Attacks are Absent

We first derive required conditions to ensure ISS property of the uncertain linear NCS (10) when DoS attacks are absent on the communication channels. Proposition 4 below states such conditions.

Proposition 4. *Consider the uncertain linear NCS in* (10)*. Assume the DETS control update logic* (19)-(20) *is used. Then the closed loop NCS (10) is GAS when DoS is absent.*

Proof. For $P \succeq 0$, consider the quadratic Lyapunov function $V(x(t)) = x(t)^\intercal P x(t)$ for NCS (10). Thus:

$$\alpha_1\|x(t)\|^2 \leq V(x(t)) \leq \alpha_2\|x(t)\|^2, \quad (38)$$

where $\alpha_1 = \underline{\lambda}(P), \alpha_2 = \overline{\lambda}(P)$. On the state trajectories of (10), the time derivative $\dot{V}$ of $V(x(t))$ can be written as

$$\begin{aligned} \dot{V} &= V_x\left\{[A(p_0) + BK^\intercal]\,x(t) + BK^\intercal e(t) + B\zeta(p)x(t)\right\}, \\ &= V_x\left[(A(p_0) + BK^\intercal)\,x(t)\right] + V_x BK^\intercal e(t) \\ &\quad + V_x B\zeta(p)x(t). \end{aligned} \quad (39)$$

where $V_x := (\partial V(x)/x)$. Using (6), (39) can be rewritten as

$$\begin{aligned} \dot{V} &= -x\left(\mathcal{S} + Q + K^\intercal RK\right)x + 2x(t)^\intercal PBK^\intercal e(t) \\ &\quad - 2x(t)^\intercal K^\intercal R\zeta(p)x(t), \\ &= -x\left(\mathcal{S} + Q + K^\intercal RK + K^\intercal R\zeta(p) + \zeta^\intercal(p)R^\intercal K\right)x \\ &\quad + 2x^T PBK^\intercal e, \end{aligned} \quad (40)$$

Now add $x^T(t)\zeta^T(p)R\zeta(p)x(t)$ to and substract it from the right hand side of (40). We can then write the following.

$$\begin{aligned} \dot{V} &= -x(t)\left(\mathcal{S} + Q + K^\intercal RK\right)x(t) + 2x(t)^\intercal PBK^\intercal e(t) \\ &\quad - 2x(t)^\intercal K^\intercal R\zeta(p)x(t), \\ &= -x\big[\left(\mathcal{S} - \zeta^T(p)R\zeta(p)\right) + Q + K^\intercal RK + K^\intercal R\zeta(p) \\ &\quad + \zeta(p)^\intercal R^\intercal K^\intercal + \zeta(p)^\intercal R\zeta(p)\big]x + 2x(t)^\intercal PBK^\intercal e(t), \\ &= -x(t)\big[\left(\mathcal{S} - \zeta(p)^\intercal R\zeta(p)\right) + Q \\ &\quad + \left(K + \zeta(p)\right)^\intercal R\left(K + \zeta(p)\right)\big]x(t) + 2x(t)^\intercal PBK^\intercal e(t), \\ &= -x(t)^\intercal\Phi x(t) + 2x(t)^\intercal PBK^\intercal e(t), \\ &\leq -\gamma_\Phi\|x(t)\|^2 + 2\|PBK^\intercal\|\|x(t)\|\|e(t)\|, \end{aligned} \quad (41)$$

where $\gamma_\Phi = \underline{\lambda}(\Phi)$ in which $\Phi = \mathcal{S} - \zeta^T(p)R\zeta(p) + Q + \left(K + \zeta(p)\right)^T R\left(K + \zeta(p)\right)$.

When there are no DoS attacks, the DETS control update time logic (19)-(20) imply that the following holds.

$$\eta(t) + \theta\left(\sigma x(t)^\intercal Q x(t) - 2x(t)^\intercal PBK^\intercal e(t)\right) \geq 0. \quad (42)$$

Taking the norm of (42) and substituting it into (41) allow us to write (41) into the following.

$$\begin{aligned} \dot{V}(x(t)) &\leq -\gamma_\Phi\|x(t)\|^2 + \sigma\underline{\lambda}(Q)\|x(t)\|^2 + \frac{1}{\theta}\|\eta(t)\|, \\ &\leq -\omega_1 V(x(t)) + \xi\|\eta(t)\|^2, \end{aligned} \quad (43)$$

which satisfies Definition 1 in which $\varphi := \omega_1 = (\gamma_\Phi - \sigma\gamma_1)/\alpha_1$ and $\xi = 1/\theta$. This thus shows the ISS property of the closed loop NCS (10) when DoS attacks are absent. □

C. NCS Stability Analysis: DoS Attacks are Present

Next, we examine the stability of NCS (10) when DoS attacks are present. During such DoS occurrences (i.e $\forall t \in \Omega(t)$ defined in (12)), the DETS control update time logic (19)-(20) cannot be carried out. In this regard, one instead may examines the upperbound of the error functional term $2\|PBK^\intercal\|\|x(t)\|\|e(t)\|$ of the time derivative $\dot{V}(x)$ in (41). This can be done using the result in (31) of Lemma 3. More specifically, the substitution of (31) into (41) allows us to write the time derivative in (41) as follows.

$$\begin{aligned}\dot{V} &\leq -\gamma_\Phi\|x(t)\|^2 + 2\|PBK^\intercal\|\|x(t)\|\|e(t)\| \\ &\leq -\gamma_\Phi\|x(t)\|^2 + (\sigma\gamma_1 + 2\gamma_2)\|x(\delta_n)\|^2 \\ &\quad + 2\gamma_2\|x(t)\|^2 + \frac{1}{\theta}\|\eta(\delta_n)\| \\ &\leq (2\gamma_2 - \gamma_\Phi)\|x(t)\|^2 + (\sigma\gamma_1 + 2\gamma_2)\|x(\delta_n)\|^2 \\ &\quad + \frac{1}{\theta}\|\eta(\delta_n)\|^2\end{aligned} \tag{44}$$

Note on one hand that if $\|x(\delta_n)\| \leq \|x(t)\|$, (44) becomes

$$\begin{aligned}\dot{V} &\leq (\sigma\gamma_1 - \gamma_\Phi + 4\gamma_2)\|x(t)\|^2 + \frac{1}{\theta}\|\eta(t)\|^2 \\ &\leq \omega_2 V(x(t)) + \xi\|\eta(t)\|^2\end{aligned} \tag{45}$$

with $\omega_2 = (\sigma\gamma_1 - \gamma_\Phi + 4\gamma_2)/\alpha_1$. On the other hand, inequality (46) below instead will hold if $\|x(\delta_n)\| \geq \|x(t)\|$.

$$\dot{V} \leq \omega_2 V(x(d_n)) + \xi\|\eta(t)\|^2 \tag{46}$$

Using the obtained results in (43), (45), and (46), Theorem 5 below states the conditions which will guarantee the ISS property of the closed loop NCS (10) for all time $t \geq 0$.

Theorem 5. *Consider the uncertain NCS* (10) *with DETS control update time logic* (19)-(20)*. Assume the NCS is being attacked by DoS phenomenon with properties as in* (11)–(16)*. Then the closed loop NCS* (10) *maintains ISS property for any DoS satisfying* (15)-(16) *with a constraint of the form*

$$\tau > \frac{\omega_1 + \omega_2}{\omega_1}, \tag{47}$$

in which ω_1 and ω_2 are as in (43) *and* (46)*, respectively.*

Proof. Define $\delta_{n-1} = 0$, $\tau_{n-1} = 0$. Then (43) allows us to write the following for all $t \in [\delta_{n-1} + \tau_{n-1}, \delta_n)$,

$$\begin{aligned}V(x(t)) \leq e^{-\omega_1(t-(\delta_n+\tau_n))}V(x(\delta_{n-1}+\tau_{n-1})) \\ + \frac{\xi}{\omega_1}\|\eta(t)\|_\infty^2\end{aligned} \tag{48}$$

Similarly, we have the following from (46) for all $t \in \mathcal{D}_n$.

$$V(x(t)) \leq e^{\omega_2(t-\delta_n)}V(x(\delta_n)) + \frac{\xi}{\omega_2}\|\eta(t)\|_\infty^2, \tag{49}$$

Now note that (11)–(12) imply $|\Theta(t)| = t - |\Omega(t)|$. Thus for all $t \geq 0$, one may combines (48) and (49) as follows.

$$\begin{aligned}V(x(t)) &\leq e^{-\omega_1|\Theta(t)|}e^{\omega_2|\Omega(t)|}V(x_0) + \varpi\|\eta(t)\|_\infty^2 \\ &\leq e^{-\omega_1 t}e^{(\omega_2+\omega_1)|\Omega(t)|}V(x_0) + \varpi\|\eta(t)\|_\infty^2\end{aligned} \tag{50}$$

in which $\varpi := \max(\xi/\omega_1, \xi/\omega_2)$. Substituting the constraint (16) on DoS occurrences into (50), we have that

$$\begin{aligned}V(x(t)) &\leq e^{-\omega_1 t}e^{(\omega_1+\omega_2)(\kappa+(t/T))}V(x_0) + \varpi\|\eta(t)\|_\infty^2 \\ &\leq e^{\kappa(\omega_1+\omega_2)}e^{-(\omega_1-(\omega_1+\omega_2)/T)t}V(x_0) + \varpi\|\eta(t)\|_\infty^2\end{aligned} \tag{51}$$

Using property (38) of $V(x(t))$, we may write from (51) that

$$\begin{aligned}\|x(t)\|^2 \leq \left(\frac{\alpha_2}{\alpha_1}e^{\kappa(\omega_1+\omega_2)}\right)e^{-\left(\omega_1-\frac{\omega_1+\omega_2}{T}\right)t}\|x_0\|^2 \\ + \frac{\varpi}{\alpha_1}\|\eta(t)\|_\infty^2\end{aligned} \tag{52}$$

Now note that an inequality of the form $a^2 + b^2 \leq (a+b)^2$ holds for any pair of real numbers $a > 0$ and $b > 0$. Using this fact on (52), we may infer the following inequality.

$$\begin{aligned}\|x(t)\| &\leq \underbrace{\sqrt{\frac{\alpha_2}{\alpha_1}e^{\kappa(\omega_1+\omega_2)}}\,e^{-\left[\omega_1-\left(\frac{\omega_1+\omega_2}{T}\right)\right]\frac{t}{2}}\|x_0\|}_{-\Psi(\|x_0\|,t)} \\ &\quad + \underbrace{\sqrt{\frac{\phi}{\alpha_1}}\,\|\eta(t)\|_\infty}_{\Gamma(\|\eta(t)\|_\infty)} \\ &\leq -\Psi(\|x_0\|,t) + \Gamma(\|\eta(t)\|_\infty)\end{aligned} \tag{53}$$

Notice that $\Gamma(\cdot)$ in (53) is of class $\mathcal{K}_\infty$. In order for (53) to satisfy the second ISS condition in Definition 1 (i.e. guarantee the ISS property of NCS (10)), then $\Psi(\|x_0\|, t)$ should also be of class $\mathcal{K}_\infty$ which can be ensured if condition (47) in the theorem is satisfied. The proof is completed. □

Condition (47) in Theorem 5 suggests that the ISS property of DoS-attacked uncertain NCS in (10) is dependent on both the frequency and individual duration of DoS occurrences. Consequently, such a condition can also be viewed/used as a measure of the NCS' resiliency to DoS attacks which occurr in the NCS' communication channels.

IV. Conclusion

This paper has presented mathematical grounds for DETS-based optimal control design approach to maintain an ISS property of a class of NCS which satisfies the matched uncertainty condition and undergoes DoS attacks. Under the assumption that the DoS attacks occur in a regular manner, this paper uses Lyapunov's stability analysis method to derive conditions for the proposed DETS-based control that will produce a sequence of control update times which can preserve the ISS property of the closed loop NCS. Future works will be directed toward examining and implementing the proposed resilient optimal control design method in practical and real life NCS applications under uncertainties.

Acknowledgment

This research was supported by the Directorate General for Higher Education, Research, and Technology of the Ministry of Education, Culture, Research, and Technology (Kemendikbudristek) of the Republic of Indonesia under the Regular Fundamental Research grant year 2023.

REFERENCES

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. ISORC*, 2008, pp. 363–369.

[2] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE T. Automat. Contr.*, vol. 52, no. 9, pp. 1680–1685, 2007.

[3] M. D. Lemmon, "Event-triggered feedback in control, estimation, and optimization," in *Networked Control Systems*. Springer, 2010.

[4] A. Cervin, D. Henriksson, B. Lincoln, J. Eker, and K.-E. Årzén, "How does control timing affect performance?" *IEEE Contr. Syst. Mag.*, vol. 23, no. 3, pp. 16–30, 2003.

[5] X. Ge, Q.-L. Han, X.-M. Zhang, and D. Ding, "Dynamic event-triggered control and estimation: A survey," *Int. J. Autom. Comput.*, vol. 18, no. 6, pp. 857–886, 2021.

[6] E. Garcia and P. J. Antsaklis, "Model-based event-triggered control for systems with quantization and time-varying delays," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 422–434, 2013.

[7] K. Liu, E. Fridman, and Y. Xia, *Networked Control Under Communication Constraints*. Springer, 2020.

[8] 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. Autom. Sin.*, vol. 7, no. 1, pp. 1–17, 2019.

[9] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proc. ACM Symp. Inform., Comp. & Comm. Security*, 2011, pp. 355–366.

[10] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[11] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[12] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[13] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, p. 210, 2019.

[14] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," in *Proc. Conf. Human System Interactions*, 2009, pp. 632–636.

[15] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. Int. Conf. Dist. Comput. Syst. Wksp.*, 2008, pp. 495–500.

[16] T. A. Tamba, "A metaheuristic scheme for secure control of cyber-physical systems," in *Metaheuristic Algorithms in Industry 4.0*. CRC Press, 2021, pp. 47–72.

[17] F. Lin and A. W. Olbrot, "An LQR approach to robust control of linear systems with uncertain parameters," in *Proc. IEEE Conf. Decision & Control*, vol. 4, 1996, pp. 4158–4163.

[18] C. De Persis and P. Tesi, "Resilient control under denial-of-service," *IFAC Proc. Vol.*, vol. 47, no. 3, pp. 134–139, 2014.

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

[20] F. Lin, R. D. Brandt, and J. Sun, "Robust control of nonlinear systems: compensating for uncertainty," *Int. J. Control*, vol. 56, no. 6, pp. 1453–1459, 1992.

[21] J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Proc. IEEE Conf. Decision & Control*, 1999, pp. 2655–2660.

[22] T. A. Tamba and Y. Y. Nazaruddin, "Event-triggered resilient control of a class of cyber-physical systems under denial-of-service," in *Proc. 5th Int. Conf. Instrum. Control Autom.*, 2017, pp. 41–46.

[23] T. A. Tamba, Y. Y. Nazaruddin, and B. Hu, "Resilient control under denial-of-service via dynamic event triggering," in *Proc. 11th Asian Control Conf.*, 2017, pp. 1749–1754.

[24] A. Girard, "Dynamic triggering mechanisms for event-triggered control," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1992–1997, 2015.

[25] H. K. Khalil, *Nonlinear Control*, 3rd ed. Pearson New York, 2015.