2015 IEEE 54th Annual Conference on Decision and Control (CDC)
December 15-18, 2015. Osaka, Japan

Output-based Event-triggered Control Systems under Denial-of-Service Attacks

V.S. Dolk, P. Tesi, C. De Persis and W.P.M.H. Heemels

Abstract— **In this paper, we propose a dynamic event-triggered control (ETC) strategy for output-based feedback systems in the presence of Denial-of-Service (DoS) attacks. These malicious DoS attacks aim to impede the communication of measurement data in order to endanger the functionality of the closed-loop system. We show that the proposed ETC scheme, if well designed, can tolerate a class of DoS signals characterized by frequency and duration properties without jeopardizing the stability, performance and Zeno-freeness of the ETC system.**

I. Introduction

The rapidly emerging field of *cyber-physical systems* (CPS) and, in particular, networked control systems (NCSs), require a paradigm shift in control theory to guarantee safe and secure operation despite the presence of possible malicious attacks [20]. One of the main concerns in NCSs regarding security are so-called *denial-of-service* (DoS) attacks. These DoS attacks, which are often induced by radio interference signals (also referred to as *jamming* signals), typically cause periods in time at which communication is not possible, see, for instance, [22]. In the present paper, we are interested in control strategies that are resilient to DoS attacks that aim to impede the networked communication with an *unknown* jamming strategy.

Besides the resilience requirement described above, the control strategy also needs to deal with the facts that networked communication is inherently digital (packet-based) and that the communication resources are limited. Hence, there is a strong need for a *resource-aware resilient* control strategy that only transmits the required measurements when necessary to maintain the desired stability and performance criteria. This is exactly the problem setting considered in this paper. In particular, we are interested in developing a design framework for control laws that limits the transmission of sensor data while realizing desired closed-loop stability and performance criteria despite the presence of DoS attacks. The proposed solution to this challenging problem relies on an event-triggered control (ETC) strategy which allows to balance the utilization of communication resources and control performance by letting the transmission times depend on, *e.g.*, sensor measurements of the system. Although many ETC strategies were proposed before, see [14] for a recent overview, only a few consider cyber-security issues like DoS attacks. Notable exceptions are [3]–[5], [11]. In [11], a method was proposed to identify features of DoS attacks in order to improve the scheduling of transmissions in the sense that the DoS periods are being avoided. However, this approach turns out to be effective only when the DoS attacks are "well- structured" over time, e.g., in case of a periodic jamming signal. In [3]–[5] a more general and realistic DoS attack model is employed based on the frequency and duration of the attacker's actions. In contrast to stochastic packet dropout models, this characterization allows to capture a wide class of DoS attacks including *trivial*, *periodic*, *random* and *protocol-aware* jamming attacks [6], [22].

A significant drawback of the approaches in [3]–[5], [11] is that the control strategies rely on the availability of full state information. This is in general a strong assumption as in practice full state measurements are rarely available. For this reason, it is of importance to address the design of *resource-aware* control laws dealing with DoS attacks for the output-feedback case. To the best of our knowledge, this case has never been addressed in the literature which is probably due to the complexity of developing output-based ETC schemes robust to the presence of disturbances is (even in absence of DoS attacks) as shown in [1], [10]. In this paper, we propose a novel systematic design methodology for *output-based*, *resilient* and *resource-aware* dynamic ETC strategies. Under the proposed design conditions, we prove that the resulting closed-loop system is input-to-output stable with finite induced $\mathcal{L}_\infty$-gains (*peak-to-peak gains*) and induced $\mathcal{L}_2 \to \mathcal{L}_\infty$-gains (also known as the *energy-to-peak* gains). Interestingly, this result is of independent interest in the context of switched systems under average-dwell time conditions, see also [16]. Furthermore, we show that the proposed ETC scheme, despite the presence of disturbances and/or DoS attacks, guarantees the existence of a strictly positive lower-bounded on the time in between two consecutive transmission attempts, also referred to as the minimal-inter event time (MIET).

The remainder of this paper is organized as follows. After presenting the necessary preliminaries and notational conventions in Section II, we introduce the networked control setup subject to DoS attacks and the problem statement in Section III. In Section IV, we formalize the event-triggered NCS setup by means of hybrid models leading to a mathematically rigorous problem formulation. In Section V, we characterize the DoS attacks and, based on this characterization, we

This work is supported by the STW project "Integrated design approach for safety-critical real-time automotive systems" (No. 12698) and the Innovational Research Incentives Scheme under the VICI grant "Wireless control systems: A new frontier in automation" (No. 11382) awarded by NWO (The Netherlands Organisation for Scientific Research) and STW (Dutch Technology Foundation).Victor Dolk and Maurice Heemels are with the Control Systems Technology group, Dept. of Mechanical Eng., Eindhoven University of Technology, Eindhoven 5600 MB, The Netherlands, e-mail: {v.s.dolk,m.heemels@tue.nl}. Claudio De Persis and Pietro Tesi are with Faculty of Mathematics and Natural Sciences, University of Groningen, the Netherlands, email: {c.de.persis,p.tesi@rug.nl}

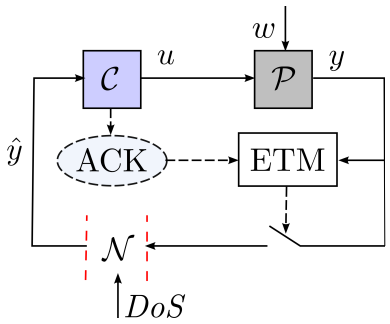

Fig. 1. Schematic representation of an event-triggered control configuration of an NCS consisting of the interconnection of $\mathcal{P}$, $\mathcal{C}$ and $\mathcal{N}$.

present design conditions for the proposed event-triggering strategy such that stability and performance properties are satisfied. Finally, we state the concluding remarks in Section VI.

II. Definitions and Preliminaries

The following notational conventions will be used in this paper. $\mathbb{N}$ denotes the set of all non-negative integers, $\mathbb{N}_{>0}$ the set of all positive integers, $\mathbb{R}$ the field of all real numbers and $\mathbb{R}_{\geqslant 0}$ the set of all non-negative reals. For $N \in \mathbb{N}$, we write the set $\{1, 2, \ldots, N\}$ as $\bar{N}$. For N vectors $x_i \in \mathbb{R}^{n_i}, i \in \bar{N}$, we denote the vector obtained by stacking all vectors in one (column) vector $x \in \mathbb{R}^n$ with $n = \sum_{i=1}^{N} n_i$ by $(x_1, x_2, \ldots, x_N)$, *i.e.* $(x_1, x_2, \ldots, x_N) = \begin{bmatrix} x_1^\top & x_2^\top & \cdots & x_N^\top \end{bmatrix}^\top$. The vectors in $\mathbb{R}^N$ consisting of all ones and zeros are denoted by $\mathbf{1}_N$ and $\mathbf{0}_N$, respectively. By $|\cdot|$ and $\langle \cdot, \cdot \rangle$ we denote the Euclidean norm and the usual inner product of real vectors, respectively. For a real symmetric matrix A, $\lambda_{\max}(A)$ denotes the largest eigenvalue of A. I_N denotes the identity matrix of dimension $N \times N$ and if N is clear for the context, we write I. A function $\alpha : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is said to be of class $\mathcal{K}$ if it is continuous, strictly increasing and $\alpha(0) = 0$. It is said to be of class $\mathcal{K}_\infty$ if it is of class $\mathcal{K}$ and it is unbounded. A continuous function $\beta : \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is said to be of class $\mathcal{KL}$ if, for each fixed s, the mapping $r \mapsto \beta(r, s)$ belongs to class $\mathcal{K}$, and for each fixed r, the mapping $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \to 0$ as $s \to 0$. A function $f : \mathbb{R}^n \to \mathbb{R}^n$ is said to be locally Lipschitz continuous if for each $x_0 \in \mathbb{R}^n$ there exist constants $\delta > 0$ and $L > 0$ such that for all $x \in \mathbb{R}^n$ we have that $|x - x_0| \leqslant \delta \Rightarrow |f(x) - f(x_0)| \leqslant L|x - x_0|$.

III. NCS Model and Problem Statement

In this section, we introduce the event-triggered NCS setup subject to *denial-of-service* (DoS) attacks. Based on this description, we also provide the problem statement considered in this paper.

A. Networked Control configuration

In this paper, we consider a control configuration in which the sensor measurements of plant $\mathcal{P}$ are transmitted to the controller $\mathcal{C}$ over a network $\mathcal{N}$, as shown in Figure 1. The continuous-time plant $\mathcal{P}$ is described by

$$\mathcal{P} : \begin{cases} \dot{x}_p = f_p(x_p, u, w) \\ y = g_p(x_p, w), \\ z = q(x_p), \end{cases} \tag{1}$$

where $w \in \mathbb{R}^{n_w}$ is a disturbance input, $x_p \in \mathbb{R}^{n_p}$ the state vector, $u \in \mathbb{R}^{n_u}$ is the control input, $y \in \mathbb{R}^{n_y}$ is the measured output of plant $\mathcal{P}$ and $z \in \mathbb{R}^{n_z}$ the performance output. The controller $\mathcal{C}$ is given by

$$\mathcal{C} : \begin{cases} \dot{x}_c = f_c(x_c, \hat{y}) \\ u = g_c(x_c, \hat{y}), \end{cases} \tag{2}$$

where $x_c \in \mathbb{R}^{n_c}$ denotes the controller state, $\hat{y} \in \mathbb{R}^{n_y}$ represents the most recently received output measurement of the plant at the controller $\mathcal{C}$ and $u \in \mathbb{R}^{n_u}$ is the controller output.

As already mentioned, the output y is transmitted over the network $\mathcal{N}$ to the controller $\mathcal{C}$ in a package-based manner. In other words, transmissions containing output measurements y can only occur at discrete instants in time, *i.e.*, at times t_j, $j \in \mathbb{N}$, satisfying $0 \leqslant t_0 < t_1 < t_2 < \ldots$. At each transmission instant t_j, $j \in \mathbb{N}$, $y(t_j)$ is transmitted and the value of $\hat{y}$ is updated, *i.e.*, $\hat{y}(t_j^+) = y(t_j)$, for all $j \in \mathbb{N}$ (assuming for the moment that DoS attacks are absent). For simplicity of exposition, we assume that the value of $\hat{y}$ evolves in a zero-order-hold (ZOH) fashion in the sense that in between updates, the variable $\hat{y}$ is held constant, *i.e.*, $\dot{\hat{y}} = 0$ for all $t \in (t_j, t_{j+1})$ with $j \in \mathbb{N}$, although (model-based) holding devices can be included as well. The functions f_p and f_c are assumed to be continuous and the functions g_p and g_c are assumed to be continuously differentiable.

B. DoS attacks

A *denial-of-service* (DoS) attack is defined as a period in time at which no communication is possible from sensor to controller due to a malicious attacker. To be more concrete, when a transmission of $y(t_j)$ is attempted at time t_j while a DoS attack is present, the attempt fails and the value of $\hat{y}$ can not be updated to $y(t_j)$. Clearly, these attacks can endanger the stability and performance of the closed-loop system and it is important to design control systems that are resilient to them.

To model DoS attacks, we use a sequence of time intervals $\{H_n\}_{n \in \mathbb{N}}$ where H_n represents the n-th DoS interval and is given by $H_n := \{h_n\} \cup [h_n, h_n + \tau_n)$. Hence, $h_n \in \mathbb{R}_{\geqslant 0}$ denotes the time instant at which the n-th DoS interval commences and where $\tau_n \in \mathbb{R}_{\geqslant 0}$ denotes the length of the n-th DoS interval. The collection of sequences of DoS intervals $\{H_n\}_{n \in \mathbb{N}}$ that satisfy $0 \leqslant h_0 \leqslant h_0 + \tau_0 < h_1 \leqslant h_1 + \tau_1 < h_2 < \ldots$ (hence, no overlapping DoS intervals), is denoted by $\mathcal{I}_{DoS}$.

Moreover, for a given $\{H_n\}_{n \in \mathbb{N}} \in \mathcal{I}_{DoS}$, we define the collection of times at which DoS attacks are active as

$$\mathcal{T} := \bigcup_{n \in \mathbb{N}} H_n,$$

where we do not explicitly write the dependency of $\mathcal{T}$ on $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ assuming it is clear from the context. Given this definition, for each transmission attempt at time $t_j \in \mathbb{R}_{\geqslant 0}$, $j \in \mathbb{N}$, the jump/update of $\hat{y}$ as in (2) and the update of the transmission error $e := \hat{y} - y$, according to the hybrid modelling framework advocated in [13], can now be described as

$$\hat{y}^+ = \begin{cases} y, & \text{when } t_j \notin \mathcal{T} \\ \hat{y}, & \text{when } t_j \in \mathcal{T}, \end{cases}, \; e^+ = \begin{cases} 0, & \text{when } t_j \notin \mathcal{T} \\ e, & \text{when } t_j \in \mathcal{T}, \end{cases} \quad (3)$$

for each $j \in \mathbb{N}$, respectively.

C. Event-based communication

Stability analysis for time-triggered NCSs, see, *e.g.*, [2], [15], [17], [21], typically results in so-called *maximum allowable transmission interval* (MATI) bounds, which are upper bounds for the inter-transmission times $t_{j+1} - t_j$, $j \in \mathbb{N}$ such that desired stability and/or performance properties are guaranteed. This time-based specification does not depend on the state of the system and therefore corresponds to the worst-case situation of the system. For this reason, time-triggered control schemes often lead to redundant utilization of the communication resources. To deal with scarcity of the communication resources, it seems more natural to determine transmissions on the basis of available measurements instead of using these worst-case time bounds. This can lead to significant prolongations of the transmission intervals and thus to reduced utilization of communication resources while desired stability and performance criteria are still guaranteed, see [14].

In this paper, we will follow a design philosophy based on a *dynamic* event-triggered control schemes [7], [12], [18], [19] which have several advantages over the commonly studied *static* counterparts, see [7], [9], [12] for more details. In a *dynamic* event-trigger mechanism (ETM), the transmission instants are determined according to the rule

$$t_0 = 0,\, t_{j+1} := \inf\{t > t_j + \tau_{miet} \mid \eta(t) \leqslant 0\}, \quad (4)$$

for all $j \in \mathbb{N}$, $t_0 = 0$, $\eta(0) = 0$ and where $\tau_{miet} \in \mathbb{R}_{>0}$ is an (enforced) lower bound on the *minimum inter-event time* (MIET) and $\eta \in \mathbb{R}$ is an auxiliary variable. The evolution of the triggering variable η can be expressed in terms of flow and jump equations according to the hybrid modelling framework advocated in [13], as

$$\begin{cases} \dot{\eta} & = \tilde{\Psi}(m, o, \eta), \text{ when } \eta \geqslant 0 \\ \eta^+ & = \eta_0(e), \text{ when } \eta \leqslant 0, \end{cases} \quad (5)$$

where o represents the information *locally* available at the ETM (see Figure 1) such as the output measurements $y \in \mathbb{R}^{n_y}$ and the transmission error $e := \hat{y} - y$ and $m \in \{0, 1\}$ is an auxiliary variable used to keep track on whether the most recent transmission attempt was successful ($m = 0$) or not ($m = 1$) (due to DoS attacks). Observe that the presence of Zeno-behavior is prevented if we select $\tau_{miet} \in \mathbb{R}_{>0}$, as the adopted time regularization enforces then that the next event only occurs after at least τ_{miet} time units have elapsed, *i.e.*, $t_{j+1} - t_j \geqslant \tau_{miet}$, for each $j \in \mathbb{N}$. Of course, the event-triggered closed-loop system only results in desired stability and performance guarantees if τ_{miet}, $\tilde{\Psi}$ and η_0 are selected according to design conditions which are developed in Section V-B and Section V-C.

D. Problem formulation

Roughly speaking, the problem considered in this work can now be stated as follows. *Propose a systematic design procedure for $\tilde{\Psi}$, η_0 and τ_{miet} such that the interconnection $(\mathcal{P}, \mathcal{C}, \mathcal{N})$ with $\mathcal{P}$ and $\mathcal{C}$ as in (1) and (2), respectively, and the transmission attempts being generated by (4) and (5), satisfies desired stability and performance criteria despite the presence of the DoS attacks $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ that are restricted in terms of frequency and duration.*

The problem will be posed more formally in the next section, based on a complete mathematical (hybrid) model for the event-triggered closed-loop NCS, definition of DoS frequency and duration, and stability and performance notions.

IV. Mathematical formulation of the event-triggered control setup

In this section, we formulate the dynamics of the event-triggered NCS subject to DoS attacks in terms of the hybrid model $\mathcal{H}_{\mathcal{T}}$ [13] of the form

$$\dot{\xi} = F(\xi, w), \quad \text{when } \xi \in C, \quad (6a)$$
$$\xi^+ = G_{\mathcal{T}}(\xi), \quad \text{when } \xi \in D. \quad (6b)$$

Moreover, we present a natural characterization of DoS sequences. These descriptions lead to a more formal problem formulation.

A. Hybrid model

To model the NCS setup as discussed in the previous section in terms of flow and jump equations as in (6), we introduce the timer variables $s, \tau \in \mathbb{R}_{\geqslant 0}$ representing the overall time and the time elapsed since the most recent transmission attempt, respectively. By combining (1), (2) and (5), the flow map in (6) of the interconnection $(\mathcal{P}, \mathcal{C}, \mathcal{N})$ can be written as

$$F(\xi, w) := \Big(f(x, e, w), g(x, e, w), 1, 1, 0, \tilde{\Psi}(m, o, \eta), f_\phi(\tau, m, \phi)\Big), \quad (7)$$

where $x = (x_p, x_c)$, $\xi = (x, e, \tau, s, m, \eta, \phi) \in \mathbb{X} := \mathbb{R}^{n_x} \times \mathbb{R}^{n_y} \times \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \times \{0, 1\} \times \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{>0}$ with $n_x = n_p + n_c$ and $o = (y, e, \tau, \phi) \in \mathbb{O} := \mathbb{R}^{n_y} \times \mathbb{R}^{n_y} \times \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{>0}$. Here, $\phi \in \mathbb{R}_{>0}$ is an additional auxiliary variable used in the triggering condition which we initialized on $\phi(0, 0) = \phi_{miet}$, where $\phi_{miet} \in \mathbb{R}_{>0}$ is a design variable. The functions f and g are given by

$$f(x, e, w) = \begin{bmatrix} f_p(x_p, g_c(x_c), w) \\ f_c(x_c, g_p(x_p) + e, w) \end{bmatrix}, \quad (8)$$

$$g(x, e, w) = \begin{bmatrix} -\frac{\partial g_p}{\partial x_p}(x_p) f_p(x_p, g_c(x_c), w) \end{bmatrix}. \quad (9)$$

On the basis of the ETM given in (4), the flow set in (6) is given by

$$C := \{\xi \in \mathbb{X} \mid \tau \leqslant \tau_{miet} \vee \eta \geqslant 0\}. \tag{10}$$

Based on (5) and (3), we define the following

$$G_\Theta(\xi) := (x, 0, 0, s, 0, \eta_0(e, s), \phi_0) \tag{11a}$$

$$G_\Xi(\xi) := (x, e, 0, s, 1, \eta_0(e, s), \phi). \tag{11b}$$

Observe that $\xi^+ = G_\Theta(\xi)$ corresponds to a successful transmission attempt and $\xi^+ = G_\Xi(\xi)$ to a failed transmission attempt. Hence, the jump map in (6) is given by

$$G_\mathcal{T}(\xi) := \begin{cases} G_\Theta(\xi), & \text{when } \xi \in D \wedge s \notin \mathcal{T} \\ G_\Xi(\xi), & \text{when } \xi \in D \wedge s \in \mathcal{T}. \end{cases} \tag{12}$$

Based on (5), the jump set in (6) is given by

$$D := \{\xi \in \mathbb{X} \mid \tau \geqslant \tau_{miet} \wedge \eta \leqslant 0\}. \tag{13}$$

The function $f_\phi : \mathbb{R} \to \mathbb{R}$ and constant $\phi_0 \in \mathbb{R}_{>0}$ are to be designed and will be specified in Section V (just as τ_{miet}, $\tilde{\Psi}$ and η_0). By means of (7)-(13) presented above, we can now, according to the framework presented in [13], represent the ETC setup as illustrated in Figure 1

B. Constraints on DoS sequence

In practice, the resources of the attacker are limited and measures can be taken to mitigate malicious DoS attacks. For this reason, the DoS attacks are typically constrained in terms of both the DoS *frequency* and the DoS *duration*, see also [3], [4] and Remark 1. To do so, we define the collection of times within the interval $[\tau, t]$, with $t \geqslant \tau$, at which DoS attacks are active as

$$\Xi(\tau, t) := [\tau, t] \cap \mathcal{T}, \tag{14}$$

and the collection of time instants within the interval $[\tau, t]$ at which communication is possible as

$$\Theta(\tau, t) := [\tau, t] \backslash \Xi(\tau, t).$$

In this paper, we employ the following definitions.

Definition 1. [5], [16] (DoS frequency*). Let $n(\tau, t)$ denote the number of DoS* off/on *transitions occurring on the interval $[\tau, t)$,* i.e.*, $n(\tau, t) = card\{n \in \mathbb{N} \mid h_n \in [\tau, t)\}$, where card denotes the number of elements in the set. We say that the sequence of DoS attacks specified by $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ satisfies the* DoS frequency *constraint for a given $\tau_D \in \mathbb{R}_{>0}$, and a given $\nu \in \mathbb{R}_{\geqslant 0}$, if for all $\tau, t \in \mathbb{R}_{\geqslant 0}$ with $t \geqslant \tau$*

$$n(\tau, t) \leqslant \nu + \frac{t - \tau}{\tau_D}. \tag{15}$$

We denote the class of sequences of DoS intervals that satisfy this DoS frequency *constraint by $\mathcal{I}_{DoS,freq}(\nu, \tau_D)$.*

Definition 2. [5] (DoS duration*). We say that the sequence of DoS attacks specified by $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ satisfies the* DoS duration *constraint for a given $T \in \mathbb{R}_{>1}$ and a given $\varsigma \in \mathbb{R}_{\geqslant 0}$, if for all $\tau, t \in \mathbb{R}_{\geqslant 0}$ with $t \geqslant \tau$*

$$|\Xi(\tau, t)| \leqslant \varsigma + \frac{t - \tau}{T}. \tag{16}$$

We denote the class of all sequences of DoS intervals that satisfy this DoS duration *constraint by $\mathcal{I}_{DoS,dur}(\varsigma, T)$.*

We will also use the notation $\mathcal{I}_{DoS}(\nu, \tau_D, \varsigma, T)$ for $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$ and $T \in \mathbb{R}_{>1}$ to denote the intersection $\mathcal{I}_{DoS,freq}(\nu, \tau_D) \cap \mathcal{I}_{DoS,dur}(\varsigma, T)$. We call a sequence of DoS attacks that satisfies $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}(\nu, \tau_D, \varsigma, T)$, a $(\nu, \tau_D, \varsigma, T)$-DoS sequence for short.

Remark 1. *From a practical point of view, Definition 1 and Definition 2 are natural since measures can be taken to* mitigate *jamming attacks, for example, spreading techniques and high-pass filtering, such that the frequency and duration of DoS attacks are limited see,* e.g.*, [6], [22].*

Let us remark that in case the DoS frequency or DoS duration can be arbitrarily large, *i.e.*, in case $\tau_D = 0$ or $T = 1$, desired performance and stability criteria can in general not be met as in that case, all communication attempts can be blocked with the consequence that the system is in open loop all the time. Fortunately, as already mentioned in Remark 1, this will typically be not the case in practice.

C. Mathematical problem formulation

Consider the following definitions where we use the terminology of [13].

Definition 3. *The hybrid system $\mathcal{H}_\mathcal{T}$ is said to be* persistently flowing *if all maximal solutions ξ have unbounded domains in the t-direction, i.e., $\sup_t dom\, \xi = \infty$.*

In this paper, we assume all hybrid trajectories start in the set $\mathbb{X}_0 := \{\xi \in \mathbb{X} \mid \tau = \tau_{miet}, s = 0, \eta = 0, \phi = \phi_{miet}\}$ with $\phi_{miet} \in \mathbb{R}_{>0}$ which is specified in Section V-B. Observe that this assumption only reflects the initialization of the ETM variables.

Definition 4. *Let $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$ and $T \in \mathbb{R}_{>1}$ be given. The hybrid system $\mathcal{H}_\mathcal{T}$ is said to be* uniformly globally asymptotically stable *(UGAS) with respect to $\xi(0, 0) \in \mathbb{X}_0$ for $(\nu, \tau_D, \varsigma, T)$-DoS sequences if the system is persistently flowing and there exists a function $\beta \in \mathcal{KL}$ such that, for any initial condition $\xi(0, 0) \in \mathbb{X}_0$ and all $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}(\nu, \tau_D, \varsigma, T)$, all corresponding solutions ξ of $\mathcal{H}_\mathcal{T}$ with $w = 0$ satisfy*

$$|\,(x(t, j), e(t, j))\,| \leqslant \beta\,(|\,(x(0, 0), e(0, 0))\,|, t)\,, \tag{17}$$

for all $(t, j) \in dom\, \xi$. The set $\mathcal{E}$ is said to be uniformly globally exponentially stable *(UGES) for $(\nu, \tau_D, \varsigma, T)$-DoS sequences, if β can be taken as $\beta(r, t) = Mr \exp(-\varrho t)$ for some $M \geqslant 0$ and $\varrho > 0$ in the above property.*

Definition 5. *Let $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>\tau_{miet}}$ and $T \in \mathbb{R}_{>1}$ be given. The hybrid system $\mathcal{H}_\mathcal{T}$ is said to be $(\mathcal{L}_p \to \mathcal{L}_\infty)$-stable ($p \in [1, \infty)$) with an induced $(\mathcal{L}_p \to \mathcal{L}_\infty)$-gain less than or equal to ϑ under $(\nu, \tau_D, \varsigma, T)$-DoS sequences, if there exists a $\mathcal{K}_\infty$-function β such that for any exogenous input $w \in \mathcal{L}_p$, and any initial condition $\xi(0, 0) \in \mathbb{X}_0$, each corresponding solution to $\mathcal{H}_\mathcal{T}$ satisfies*

$$\|z\|_{\mathcal{L}_\infty} \leqslant \beta(|\,(x(0, 0), e(0, 0))\,|) + \vartheta \|w\|_{\mathcal{L}_p}. \tag{18}$$

The hybrid system $\mathcal{H}_\mathcal{T}$ is said to be $\mathcal{L}_\infty$-stable with an induced $\mathcal{L}_\infty$-gain less than or equal to ϑ if it is $(\mathcal{L}_\infty \to \mathcal{L}_\infty)$-stable with an induce $(\mathcal{L}_\infty \to \mathcal{L}_\infty)$-gain less than or equal to θ.

We can now formalize the problem loosely stated at the end of Section III.

Problem 1. Given the system $\mathcal{H}_\mathcal{T}$ as in (6) and $\nu \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}, \varsigma \in \mathbb{R}_{\geqslant 0}$ and $T \in \mathbb{R}_{>1}$, provide design conditions for the values of $\tau_{miet} \in \mathbb{R}_{>0}$ and the functions $\tilde{\Psi}$, η_0, ϕ_0 and f_ϕ as in the event generator given by (4) and (5), such that the system $\mathcal{H}_\mathcal{T}$ is UGES and/or, in the presence of disturbances, has a finite induced $\mathcal{L}_\infty$-gain and/or a finite induced $(\mathcal{L}_2 \to \mathcal{L}_\infty)$-gain under $(\nu, \tau_D, \varsigma, T)$-DoS sequences, with large (average) inter-event times $t_{j+1} - t_j$, $j \in \mathbb{N}$.

V. Design Conditions and Stability Guarantees

In Section V-B and Section V-C, design conditions will be presented for constant τ_{miet}, ϕ_{miet}, ϕ_0 and the functions $\tilde{\Psi}$, η_0 and f_ϕ leading to a solution for Problem 1. In order to specify these design conditions, we first present required preliminaries based on the work in [2], [15].

A. Preliminaries

Condition 1. *([2], [15]) There exist a locally Lipschitz function $W : \mathbb{R}^{n_y} \to \mathbb{R}_{\geqslant 0}$, a continuous function $H : \mathbb{R}^{n_x} \times \mathbb{R}^{n_w} \to \mathbb{R}$, and constants $L \geqslant 0$, $\underline{c}_W, \bar{c}_W > 0$, and $0 < \lambda < 1$ such that*

- *for all $e \in \mathbb{R}^{n_e}$ it holds that*

$$\underline{c}_W |e| \leqslant W(e) \leqslant \bar{c}_W |e|, \tag{19}$$

- *for all $x \in \mathbb{R}^{n_x}$, and almost all $e \in \mathbb{R}^{n_y}$ it holds that*

$$\left\langle \frac{\partial W}{\partial e}, g(x, e, w) \right\rangle \leqslant LW(e) + H(x, w). \tag{20}$$

In addition, there exist a locally Lipschitz function $V : \mathbb{R}^{n_x} \to \mathbb{R}_{\geqslant 0}$, class $\mathcal{K}_\infty$-functions $\rho : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ and $\sigma_1 : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$, a positive semi-definite function $\varrho : \mathbb{R}^{n_y} \to \mathbb{R}_{\geqslant 0}$ and constants $\gamma, \underline{c}_V, \bar{c}_V, c_z > 0$, such that

- *for all $x \in \mathbb{R}^{n_x}$*

$$\underline{c}_V |x|^2 \leqslant V(x) \leqslant \bar{c}_V |x|^2, \; c_z |q(x)|^2 \leqslant V(x), \tag{21}$$

- *for all $e \in \mathbb{R}^{n_y}$, and almost all $x \in \mathbb{R}^{n_x}$*

$$\begin{aligned} \langle \nabla V(x), f(x, e, w) \rangle \leqslant -\rho(|x|) - \varrho(|y|) - H^2(x, w) \\ - \sigma_1(W(e)) + \gamma^2 W^2(e) + \theta^2 |w|^2. \end{aligned} \tag{22}$$

Note that for linear systems the functions V and W that satisfy Condition 1 can be constructed systematically by means of linear matrix inequalities (LMIs), see [7], [15] for more details. Also several classes of nonlinear systems satisfy these conditions, see [8].

B. Minimal inter-event time

As already mentioned, τ_{miet}, ϕ_{miet}, f_ϕ, ϕ_0 (and $\tilde{\Psi}$, η_0) have to be designed such that desirable closed-loop stability and performance requirements as specified in Definition 5 are met. Consider the function $f_\phi : \mathbb{R}_{\geqslant 0} \times \mathbb{N} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}$, which is defined as

$$f_\phi(\tau, m, \phi) := \begin{cases} (m-1)\left(2L\phi + \gamma(\phi^2 + 1)\right), & \text{for } \tau \leqslant \tau_{miet}, \\ 0, & \text{for } \tau > \tau_{miet}. \end{cases} \tag{23}$$

where L and γ are constants as given in Condition 1. Moreover, we select

$$\phi_0 := \lambda^{-1}, \tag{24}$$

as initial value for ϕ after a successful transmission attempt as described by (11)-(6) with $\lambda \in (0, 1)$. The time-constant τ_{miet} can be taken less than or equal to the MATI bound given in [2] as

$$\tau_{mati} = \begin{cases} \frac{1}{Lr} \text{arctan}\left(\frac{r(1-\lambda)}{2\frac{\lambda}{1+\lambda}\left(\frac{\gamma}{L} - 1\right) + 1 + \lambda} \right), & \gamma > L \\ \frac{1}{L} \frac{1-\lambda}{1+\lambda}, & \gamma = L \\ \frac{1}{Lr} \text{arctanh}\left(\frac{r(1-\lambda)}{2\frac{\lambda}{\lambda+1}\left(\frac{\gamma}{L} - 1\right) + 1 + \lambda} \right), & \gamma < L, \end{cases} \tag{25}$$

where $r = \sqrt{|(\gamma/L)^2 - 1|}$. Note that by selecting τ_{miet} equal to τ_{mati} indeed longer (average) transmission intervals are realized compared to time-based (worst-case) specifications as discussed in Section III-C.

Lemma 2. *[2] If τ_{mati} is chosen according to (25), then the solution to*

$$\dot{\tilde{\phi}} = -2L\tilde{\phi} - \gamma\left(\tilde{\phi}^2 + 1\right) \tag{26}$$

with $\tilde{\phi}(0) = \lambda^{-1}$ satisfies $\tilde{\phi}(t) \in [\lambda, \lambda^{-1}]$ for all $t \in [0, \tau_{mati}]$, and $\tilde{\phi}(\tau_{mati}) = \lambda$.

Finally, we define

$$\phi_{miet} := \tilde{\phi}(\tau_{miet}), \tag{27}$$

where $\tilde{\phi}$ is the solution to (26) with $\tilde{\phi}(0) = \lambda^{-1}$.

C. Stability and Performance Guarantees

Theorem 3. *Given fixed DoS parameters $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$, $T \in \mathbb{R}_{>1}$ and system $\mathcal{H}_\mathcal{T}$ satisfying Condition 1 with $\tau_{miet} \leqslant \tau_{mati}$, where τ_{mati} as in (25), f_ϕ and ϕ_0 as in (23) and (24), respectively, and where ϕ_{miet} as in 27, and suppose that the following four conditions hold:*

i) The functions ρ and σ_1 satisfy $\rho(s) \geqslant c_1 s^2$ and $\sigma_1(s) \geqslant c_2 s^2$, respectively, for some constants c_1, $c_2 \in \mathbb{R}_{>0}$ and for all $s \in \mathbb{R}_{\geqslant 0}$.

ii) The DoS frequency parameter τ_D and the DoS duration parameter T satisfy

$$\frac{\tau_{miet}}{\tau_D} + \frac{1}{T} < \frac{\omega_1}{\omega_1 + \omega_2}, \tag{28}$$

where

$$\omega_1 = \min\left(\frac{c_1 + c_3}{\bar{c}_V}, \frac{\lambda c_2}{\gamma} \right), \; \omega_2 = \frac{(\bar{\gamma} - c_2)}{\gamma \phi_{miet}}, \tag{29}$$

with $\bar{\gamma} = \gamma\left(2\phi_{miet}L + \gamma(1+\phi_{miet}^2)\right)$.

iii) There exist a constant $c_3 \in \mathbb{R}_{\geqslant 0}$ *and a function* $\Psi : \mathbb{O} \to \mathbb{R}$*, such that for all* $o \in \mathbb{O}$*,* $x \in \mathbb{R}^{n_x}$*, and all* $\xi \in \mathbb{X}$

$$\Psi(o) + c_3|x|^2 \leqslant M(\xi, w), \tag{30}$$

and

$$\Psi(o) \geqslant 0, \text{ for } 0 \leqslant \tau \leqslant \tau_{miet} \tag{31}$$

with

$$M(\xi, w) = \begin{cases} M_1(\xi, w), & \text{for } 0 \leqslant \tau \leqslant \tau_{miet}, \\ M_2(\xi, w), & \text{for } \tau > \tau_{miet}, \end{cases} \tag{32}$$

and where

$$M_1(\xi, w) := \varrho(|y|) + \left(H(x, w) - \gamma\phi W(e)\right)^2, \tag{33}$$

$$M_2(\xi, w) := \varrho(|y|) + H^2(x, w) - 2\gamma\phi W(e)H(x, w) - \left(\gamma^2 + 2\gamma\phi L\right) W^2(e). \tag{34}$$

Moreover, η_0 *is given by* $\eta_0(e) = \gamma\phi_{miet}W^2(e)$.

iv) The function $\tilde{\Psi}$ *is given by*

$$\tilde{\Psi}(m, o, \eta) = (1 - m)\left(\Psi(o) - \sigma_2(\eta)\right), \tag{35}$$

where σ_2 *is a* $\mathcal{K}_\infty$*-function that satisfies* $\sigma_2(s) \geqslant \omega_1 s$ *for all* $s \in \mathbb{R}_{\geqslant 0}$.

Then the hybrid system $\mathcal{H}_\mathcal{T}$*, as described by (6) and (7)-(13), is UGES under* $(\nu, \tau_D, \varsigma, T)$*-DoS sequences and is* $(\mathcal{L}_2 \to \mathcal{L}_\infty)$*-stable and* $\mathcal{L}_\infty$*-stable with a finite induced* $(\mathcal{L}_2 \to \mathcal{L}_\infty)$*-gain and a finite induced* $\mathcal{L}_\infty$*-gain with respect to input* w *and output* z *are less than or equal to* $\sqrt{\frac{\kappa}{c_z}}\theta$ *and* $\sqrt{\frac{\kappa}{c_z\beta^*}}\theta$*, respectively, where* $\kappa := e^{\varsigma_*(\omega_1+\omega_2)}$*,* $\varsigma_* := \varsigma + \nu\tau_{miet}$*,* $\beta_* = \omega_1 - (\omega_1 + \omega_2)/T_*$ *and* $T_* := \tau_D T/(\tau_D + \tau_{miet}T)$.

The proof is provided in [9]. In Section V of [7], a systematic procedure for finding a function Ψ that satisfies (30) and (31) is presented. Let us remark that in case communication is allowed, the transmissions are scheduled in an event-based fashion (to save valuable communication resources) whereas in case the communication is denied, the next transmission is scheduled after τ_{miet} has elapsed since $\tilde{\Psi}(m, o, \eta) = 0$ when $m = 1$.

VI. Conclusion

In this paper, we proposed a systematic design framework for *resource-aware* and *resilient* control strategies for networked control systems (NCSs) that are subject to disturbances and Denial-of-Service (DoS) attacks. The proposed control and communication strategy led to an *output-based* event-triggered control scheme applicable to a class of nonlinear feedback systems. Despite the presence of disturbances and DoS attacks, the proposed ETC scheme results in guarantees for a robust positive minimal inter event-time and stability and performance guarantees in terms of induced $\mathcal{L}_\infty$-gains and induced $(\mathcal{L}_2 \to \mathcal{L}_\infty)$-gains.

References

[1] D.P. Borgers and W.P.M.H. Heemels. Event-separation properties of event-triggered control systems. *IEEE Trans. Autom. Control*, 59(10):2644–2656, Oct 2014.

[2] D. Carnevale, A.R. Teel, and D. Nešić. A Lyapunov proof of an improved maximum allowable transfer interval for networked control systems. *IEEE Trans. Autom. Control*, 52(5):892–897, May 2007.

[3] C. De Persis and P. Tesi. On resilient control of nonlinear systems under denial-of-service. In *Proc. 53rd IEEE Conf. Decision and Control*, pages 5254–5259, Dec 2014.

[4] C. De Persis and P. Tesi. Resilient control under denial-of-service. In *Proc. 19th IFAC World Congress*, pages 134–139, 2014.

[5] C. De Persis and P. Tesi. Input-to-state stabilizing control under denial-of-service. 2015. In press.

[6] B. DeBruhl and P. Tague. Digital filter design for jamming mitigation in 802.15.4 communication. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pages 1–6, July 2011.

[7] V.S. Dolk, D.P. Borgers, and W.P.M.H. Heemels. Dynamic event-triggered control: Tradeoffs between transmission intervals and performance. In *Proc. 53rd IEEE Conf. Decision and Control*, pages 2764–2769, Dec 2014.

[8] V.S. Dolk, D.P. Borgers, and W.P.M.H. Heemels. Output-based and decentralized dynamic event-triggered control with guaranteed $\mathcal{L}_p$-gain performance and Zeno-freeness. 2015. Under review.

[9] V.S. Dolk, P. Tesi, C. De Persis, and W.P.M.H. Heemels. Event-triggered control systems under denial-of-service attacks. Under preparation.

[10] M.C.F Donkers and W.P.M.H Heemels. Output-based event-triggered control with guaranteed $\mathcal{L}_\infty$-gain and improved and decentralized event-triggering. *IEEE Trans. Autom. Control*, 57(6):1362–1376, June 2012.

[11] H. Foroush and S. Martinez. On triggering control of single-input linear systems under pulse-width modulated dos signals. *SIAM Journal on Control and Optimization*, 2014.

[12] A. Girard. Dynamic triggering mechanisms for event-triggered control. *IEEE Trans. Autom. Control*, 60(7):1992–1997, July 2015.

[13] R. Goebel, R.G. Sanfelice, and A.R. Teel. *Hybrid Dynamical Systems: Modeling, Stability, and Robustness*. Princeton University Press, 2012.

[14] W.P.M.H. Heemels, K.H. Johansson, and P. Tabuada. An introduction to event-triggered and self-triggered control. In *Proc. 51th IEEE Conf. Decision and Control*, pages 3270–3285, Dec 2012.

[15] W.P.M.H. Heemels, A.R. Teel, N. van de Wouw, and D. Nešić. Networked control systems with communication constraints: Tradeoffs between transmission intervals, delays and performance. *IEEE Trans. Autom. Control*, pages 1781–1796, 2010.

[16] J.P. Hespanha and A.S. Morse. Stability of switched systems with average dwell-time. In *Proc. 38th IEEE Conf. Decision and Control*, volume 3, pages 2655–2660 vol.3, 1999.

[17] D. Nešić and A.R. Teel. Input-output stability properties of networked control systems. *IEEE Trans. Autom. Control*, 49(10):1650–1667, October 2004.

[18] R. Postoyan, A. Anta, D. Nešić, and P. Tabuada. A unifying Lyapunov-based framework for the event-triggered control of nonlinear systems. In *Proc. 50th IEEE Conf. Decision and Control and European Control Conference*, 2011.

[19] R. Postoyan, P. Tabuada, D. Nešić, and A. Anta. Event-triggered and self-triggered stabilization of networked control systems. In *Proc. 50th IEEE Conf. Decision and Control and European Control Conference*, 2011.

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

[21] G.C. Walsh, Hong Ye, and L.G. Bushnell. Stability analysis of networked control systems. *IEEE Trans. on Control Systems Technology*, 10(3):438–446, May 2002.

[22] Wenyuan Xu, Ke Ma, W. Trappe, and Y. Zhang. Jamming sensor networks: Attack and defense strategies. *IEEE Network*, 20(3):41–47, May 2006.