Event-triggered control systems under denial-of-service attacks

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

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 systematic design framework for output-based dynamic event-triggered control (ETC) systems under Denial-of-Service (DoS) attacks. These malicious DoS attacks are intended to interfere with the communication channel causing periods in time at which transmission of measurement data is impossible. 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. In fact, the design procedure of the ETC condition allows trade-offs between performance, robustness to DoS attacks and utilization of communication resources. The main results will be illustrated by means of a numerical example.**

I. Introduction

The field of *cyber-physical systems* (CPS) and, in particular, networked control systems (NCSs) is rapidly emerging due to a wide range of potential applications. However, there is a strong need for novel analysis and synthesis tools in control theory to guarantee safe and secure operation despite the presence of possible malicious attacks [2]. Especially for safety-critical applications such as intelligent transport systems and power grids, this is of high importance and requires the integration of cyber-security and control strategies.

One of the main concerns in NCSs with respect to security are *deception* attacks and *denial-of-service* (DoS) attacks. Deception attacks are intended to tamper transmitted data packages causing false feedback information, see for more details, *e.g.*, [3] and the reference therein, whereas DoS attacks, 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, [4]. In the present paper, we focus on the latter type of attack. To be more concrete, we are interested in creating control strategies that render the overall closed-loop system resilient to DoS attacks which occur according to some *unknown* strategy with the aim to impede the communication of sensor measurements.

In addition to this resilience requirement described above, the control strategy needs to deal with the inherent imperfections of networked communication. Communication in NCSs is in general packet-based and thus measurement data can only be transmitted at discrete time instants. Moreover, especially since a communication network is often shared with multiple devices, the communication resources are restricted. Hence, a *resource-aware* and *resilient* control approach, which aims to only schedule the transmission of data when needed to maintain the desired stability and performance criteria, is a requisite. In a nutshell, the control problem addressed in this paper is to design a control law 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 design problem is to adopt an event-triggered control (ETC) strategy, in which transmission times are determined online by means of well-design triggering rules which rely on, *e.g.*, sensor measurements of the system. The introduction of this feedback in the sampling process enables ETC schemes to reduce the utilization of communication resources without jeopardizing control performance. In contrast to periodic time-triggered control schemes, ETC schemes aim to only transmit data when needed to maintain desired closed-loop properties. However, the majority of the literature on ETC strategies do not consider cyber-security issues like DoS attacks. Notable exceptions are [5]–[7]. In [7], 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 [5], [6], a more general and more realistic DoS attack model is used based on the frequency and duration of the attacker's actions. These constraints are quite natural, as in reality, also the jammers resources are not infinite and several provisions can be taken to mitigate these DoS attacks. Additionally, no assumptions regarding the underlying jamming strategy of the attacker are made. Moreover, 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 [4], [8].

A drawback of the approaches in [5]–[7] is that these approaches are restricted to the case of static state feedback which requires the availability of full state information. Clearly, in practice, this is a strong assumption as only in very rare cases the full state variable is available for feedback. For this reason, it is of interest to study event-triggered NCSs subject to DoS attacks that rely on output measurements only. To the best of our knowledge, the output feedback case in the context of DoS attacks has never been addressed in literature. This is not surprising as, especially in the presence

A preliminary and much shorter version of this work was accepted for presentation at the 54th IEEE Conference on Decision and Control [1].

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}

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

of disturbances, extending existing ETC schemes that rely on state-feedback to the *output-based* ETC schemes (even without DoS attacks) is far from trivial as shown in [9], [10]. Therefore, we propose in this paper a novel systematic design methodology for *output-based resilient* and *resource-aware* dynamic ETC strategies for a class of non-linear systems subject to disturbances. We prove that under the proposed design conditions, the resulting closed-loop system is input-to-output stable with finite induced $\mathcal{L}_\infty$-gains (*peak-to-peak gains*). Interestingly, this result is of independent interest in the context of switched systems under average-dwell time conditions, see also [11].

To enable practical implementation of the ETC scheme, it is important to guarantee that the time between consecutive transmission attempts is strictly positive and preferably lower bounded by a positive constant. By exploiting the Zeno-freeness property of the ETC scheme presented in [12], [13], we show that for the proposed ETC scheme, such a positive minimal-inter event time (MIET) exists by design despite the presence of disturbances and/or DoS attacks. By employing the DoS characterization as presented in [5], [6], the obtained results hold for wide classes of relevant DoS attacks. As a matter of fact, as already mentioned, no assumptions regarding the underlying strategy of the attacker are needed, which makes the proposed scheme applicable in many contexts. The design procedure is demonstrated on a case study of cooperative adaptive cruise control. The numerical example reveals that illustrates a tradeoff between robustness with respect to DoS attacks, network utilization and performance guarantees.

The remainder of this paper is organized as follows. After presenting the necessary preliminaries and notational conventions in Section II, we introduce the event-triggered networked control setup subject to DoS attacks in Section III leading to the problem statement. This event-triggered NCS setup is formalized in Section IV by means of hybrid models resulting in a mathematically rigorous problem formulation. In Section V, we characterize DoS attacks in terms of frequency and duration and, based on this characterization, we provide design conditions for the proposed dynamic event-triggered strategy such that stability and performance properties are satisfied. The obtained design framework is illustrated by means of a numerical example in Section VI. Finally, we provide the concluding remarks in Section VII.

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 $s \to \infty$. A continuous function $\gamma : \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is said to be of class $\mathcal{KLL}$ if, for each $r \geqslant 0$, both $\gamma(\cdot, \cdot, r)$ and $\gamma(\cdot, r, \cdot)$ belong to class $\mathcal{KL}$. 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 $|x - x_0| \leqslant \delta \Rightarrow |f(x) - f(x_0)| \leqslant L|x - x_0|$.

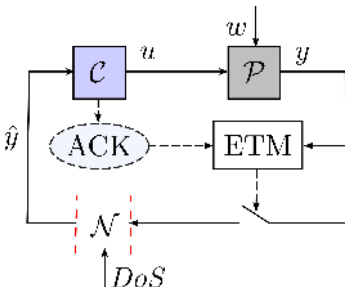

Figure 1. Schematic representation of the event-triggered NCS considered in this paper which consists of the interconnection of $\mathcal{P}$, $\mathcal{C}$ and $\mathcal{N}$ and where the transmission instants are determined by an event-triggering mechanism (ETM). Moreover, we assume an acknowledgement scheme is available meaning that the ETM has knowledge about reception of packages at the controller side.

III. NCS Model and Problem Statement

In this section, we present the networked control setup and the dynamic event-triggering mechanism employed by this NCS. Moreover, we describe how this NCS is affected by *denial-of-service* (DoS) attacks. Based on these descriptions, we formulate the problem statement.

A. Networked Control Configuration

Consider the feedback control configuration depicted in Figure 1. In this configuration, the sensor measurements of a plant $\mathcal{P}$ are being transmitted to a (dynamic) *output-based* controller $\mathcal{C}$ over a network $\mathcal{N}$. The continuous-time plant $\mathcal{P}$ is given by

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

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 $\mathcal{P}$. The (dynamic) output-based 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

output. The performance output is given by $z = q(x)$, where $z \in \mathbb{R}^{n_z}$ and $x = (x_p, x_c)$.

Typically, the communication over the network $\mathcal{N}$ is packet-based, which implies that the output measurements y can only be transmitted at discrete instants in time, *i.e.*, at times t_j, $j \in \mathbb{N}$, satisfying $0 \leqslant t_0 < t_1 < t_2 < \ldots$. Hence, at each transmission instant t_j, $j \in \mathbb{N}$, the value of $\hat{y}$ is updated/jumps according to $\hat{y}(t_j^+) = y(t_j)$, for all $j \in \mathbb{N}$ (assuming for the moment that no DoS attacks are present). Here we consider $\hat{y}$ as a left-continuous signal in the sense that $\hat{y}(t) = \lim_{s \to t} \hat{y}(s)$. Furthermore, 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.*, $\dot{\hat{y}}(t) = 0$ for all $t \in (t_j, t_{j+1})$ with $j \in \mathbb{N}$. 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.

Remark 1. *For the sake of brevity, we consider the control configuration presented in Figure 1 in which we consider dynamic controllers as in (2) and only sensor measurements are transmitted over the network. However, the framework presented in this paper also applies to other configurations such as decentralized control setups as described in [13], [14].*

B. DoS Attacks

A *denial-of-service* (DoS) attack is defined as a period in time at which the communication is blocked by a malicious attacker. Hence, when a transmission of $y(t_j)$ is attempted at transmission time t_j and a DoS attack is active, the attempt will fail and thus the value of $\hat{y}$ can not be updated to $y(t_j)$. Obviously, this can have detrimental effects on the stability and performance of the closed-loop system.

In general, DoS attacks lead to a sequence of time intervals $\{H_n\}_{n \in \mathbb{N}}$, where the n-th time interval H_n, given by $H_n := \{h_n\} \cup [h_n, h_n + \tau_n)$, represents the n-th DoS attack (period). Hence, $h_n \in \mathbb{R}_{\geqslant 0}$ denotes the time instant at which the n-th DoS interval commences and $\tau_n \in \mathbb{R}_{\geqslant 0}$ denotes the length of the n-th DoS interval. The collection of all sequences $\{H_n\}_{n \in \mathbb{N}}$ of DoS attacks without overlap, *i.e.*, satisfy $0 \leqslant h_0 \leqslant h_0 + \tau_0 < h_1 \leqslant h_1 + \tau_1 < h_2 < \ldots$, 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 a DoS attack is active by

$$\mathcal{T} := \bigcup_{n \in \mathbb{N}} H_n, \tag{3}$$

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. By means of this definition, we can now describe the jump/update of $\hat{y}$ as in (2) for each transmission attempt at time $t_j \in \mathbb{R}_{\geqslant 0}$, $j \in \mathbb{N}$ as

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

and, accordingly, the update of the transmission error $e := \hat{y} - y$ as

$$e(t_j^+) = \begin{cases} 0, & \text{when } t_j \notin \mathcal{T} \\ e(t_j), & \text{when } t_j \in \mathcal{T}, \end{cases} \tag{4}$$

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

C. Event-based Communication

As already mentioned in the introduction, in comparison with time-triggered control, event-triggered control (ETC) is much more suitable for balancing network utilization and control performance. See also [15]–[18] for some early approaches of ETC and see [19] for a recent overview.

In this paper, we we follow a design philosophy based on a *dynamic* event-triggered control scheme [12], [13], [20]–[23], which has several advantages over their *static* counterparts, see [1], [12], [20], [22], [23] for more details on these advantages. A dynamic triggering condition in the context of this paper will take the form

$$t_0 = 0,\ t_{j+1} := \inf \left\{ t > t_j + \tau_{miet}^{m(t)} \mid \eta(t) < 0 \right\}, \tag{5}$$

for all $j \in \mathbb{N}$, $\eta(0) = 0$, where $m(t) \in \{0, 1\}$ is an auxiliary variable used to keep track of whether the most recent transmission attempt at time $t \in \mathbb{R}_{\geqslant 0}$ was successful ($m(t) = 0$) or not ($m(t) = 1$) (due to DoS attacks), $\tau_{miet}^0, \tau_{miet}^1 \in \mathbb{R}_{>0}$ are (enforced) lower bounds on the *minimum inter-event times* (MIETs) for the cases that $m(t) = 0$ and $m(t) = 1$, respectively, and $\eta \in \mathbb{R}$ is an auxiliary variable. Let us remark that in general, if possible, it is helpful to schedule transmission attempts more often when a DoS attack is active in order to determine earlier when the DoS attack is over. For this reason, we consider two different waiting times τ_{miet}^0, τ_{miet}^1 and we choose $\tau_{miet}^1 \leqslant \tau_{miet}^0$. The variable η evolves according to

$$\dot{\eta}(t) = \tilde{\Psi}(m(t), o(t), \eta(t)), \text{ when } t \in (t_j, t_{j+1}] \tag{6}$$

$$\eta(t_j^+) = \begin{cases} \eta_0(e(t_j)), & \text{when } t_j \notin \mathcal{T} \\ \eta(t_j), & \text{when } t_j \in \mathcal{T}, \end{cases} \tag{7}$$

where $o = (y, e, \tau, \phi) \in \mathbb{O} := \mathbb{R}^{n_y} \times \mathbb{R}^{n_y} \times \mathbb{R}_{\geqslant 0} \times \left[\lambda, \lambda^{-1}\right]$ with $\lambda \in (0, 1)$ representing the information *locally* available at the event-triggering mechanism (ETM) (see Figure 1) including the output measurements $y \in \mathbb{R}^{n_y}$, the transmission error $e := \hat{y} - y$ and the auxiliary variables $\tau \in \mathbb{R}_{\geqslant 0}$ and $\phi \in \left[\lambda, \lambda^{-1}\right]$. The variables τ and ϕ are discussed in more detail in Section IV. Observe that by taking $\tau_{miet}^0, \tau_{miet}^1 \in \mathbb{R}_{>0}$ Zeno-behavior is excluded from the ETC system since the next event can only occur after at least τ_{miet}^1 time units have elapsed, *i.e.*, $t_{j+1} - t_j \geqslant \tau_{miet}^1$, for each $j \in \mathbb{N}$. In Section V-B and Section V-C, we specify how to select τ_{miet}^0, τ_{miet}^1, $\tilde{\Psi}$ and η_0 such that desirable closed-loop stability and performance requirements are met.

D. Problem Formulation

Given the descriptions above, the problem considered in this work can now roughly be stated as follows: *Propose a systematic design procedure for $\tilde{\Psi}$, η_0, τ_{miet}^0 and τ_{miet}^1 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 (5)-(7), satisfies desired asymptotic stability criteria and performance criteria, in terms of the so-called* peak-to-peak

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

gain despite the presence of the DoS attacks $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ *that satisfy constraints in terms of frequency and duration.*

In the next section, we introduce a complete mathematical (hybrid) model for the event-triggered closed-loop NCS setup, definitions of DoS frequency and duration, and relevant stability and performance notions, leading to a more formal problem formulation.

IV. Mathematical Formulation of the Event-triggered Control Setup

In this section, we reformulate the dynamics of the event-triggered NCS subject to DoS attacks in the form of the hybrid model $\mathcal{H}_{\mathcal{T}}$ given by,

$$\dot{\xi} = F(\xi, w), \quad \text{when } \xi \in C, \tag{8a}$$

$$\xi^+ = G_{\mathcal{T}}(\xi), \quad \text{when } \xi \in D, \tag{8b}$$

see [24] for details on this hybrid modelling framework.

Let us remark that the hybrid systems considered in this paper have time regularization (or dwell time) and external inputs only appearing in the flow map. The latter allow us to employ the following signal norm definitions inspired by [21]. For any hybrid signal $\zeta(\cdot,\cdot)$ defined on dom $\zeta \subset \mathbb{R}_{\geqslant 0} \times \mathbb{N}$ we define the $\mathcal{L}_\infty$-norm of ζ as $\|\zeta\|_\infty := \sup_{j\in\mathbb{N}} \left(\operatorname{ess\,sup}_{\{t\in\mathbb{R}|(t,j)\in\text{dom }\zeta\}} |\zeta(t,j)|\right)$. Observe that this signal norm definition is similar to the corresponding classical continuous-time norm. In this paper, we employ the same notation for the $\mathcal{L}_\infty$-norm of hybrid time signals and conventional continuous-time signals. Moreover, due to the aforementioned properties and notational convenience, we consider the disturbance input $w : \mathbb{R}_{\geqslant 0} \to \mathbb{R}^{n_w}$ to be a time signal instead of a hybrid signal and use the usual definition for $\mathcal{L}_\infty$-norm.

A. Hybrid Model

To describe the NCS setup as discussed before in terms of flow equations (8a) and jump equations (8b), we first need to introduce a few auxiliary variables, namely, 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. Moreover, we we also introduce an additional auxiliary variable $\phi \in \left[\lambda, \lambda^{-1}\right]$, where $\lambda \in (0,1)$ is a tuning parameter to be specified, used in the triggering condition and part of o as already mentioned in Section III-C. By combining these auxiliary variables with (1), (2) and (7), the flow map of the interconnection $(\mathcal{P}, \mathcal{C}, \mathcal{N})$ can be defined as

$$F(\xi, w) := \Big(f(x,e,w), g(x,e,w), 1, 1, 0, \tilde{\Psi}(m,o,\eta), f_\phi(\tau,m,\phi)\Big), \tag{9}$$

where $\xi = (x, e, \tau, s, m, \eta, \phi) \in \mathbb{X} := \mathbb{R}^{n_x} \times \mathbb{R}^{n_y} \times \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \times \{0,1\} \times \mathbb{R}_{\geqslant 0} \times \left[\lambda, \lambda^{-1}\right]$ with $n_x = n_p + n_c$ and $\lambda \in (0,1)$. Moreover, the functions f and g follow from (1) and (2) and are given by

$$f(x,e,w) = \begin{bmatrix} f_p(x_p, g_c(x_c, g_p(x_p) + e), w) \\ f_c(x_c, g_p(x_p) + e) \end{bmatrix}, \tag{10}$$

$$g(x,e,w) = -\frac{\partial g_p}{\partial x_p}(x_p) f_p(x_p, g_c(x_c, g_p(x_p) + e), w), \tag{11}$$

and f_ϕ will be specified later. In accordance with (5), we define the flow set as

$$C := \{\xi \in \mathbb{X} \mid \tau \leqslant \tau^m_{miet} \vee \eta \geqslant 0\}. \tag{12}$$

Based on (7) and (4), we specify the jump map as

$$G_{\mathcal{T}}(\xi) := \begin{cases} G_0(\xi), & \text{when } \xi \in D \wedge s \notin \mathcal{T} \\ G_1(\xi), & \text{when } \xi \in D \wedge s \in \mathcal{T}, \end{cases} \tag{13}$$

where

$$G_0(\xi) = (x, 0, 0, s, 0, \eta_0(e), \lambda) \tag{14}$$

$$G_1(\xi) = (x, e, 0, s, 1, \eta, \phi), \tag{15}$$

such that $\xi^+ = G_0(\xi)$ corresponds to a successful transmission attempt and $\xi^+ = G_1(\xi)$ to a failed transmission attempt.

Finally, the jump set is given by

$$D := \{\xi \in \mathbb{X} \mid \tau \geqslant \tau^m_{miet} \wedge \eta \leqslant 0\}. \tag{16}$$

The time-constants τ^0_{miet} and τ^1_{miet} and the functions $\tilde{\Psi}$, η_0 and f_ϕ are specified in Section V. Observe that the hybrid system description presented above leads to more solutions than induced by the triggering condition given by (5) and (7).[1]

Moreover, observe that the hybrid system $\mathcal{H}_{\mathcal{T}}$ as described by (8)-(16) is parameterized by the collection of time-intervals at which DoS attacks are active as defined in (3). Therefore, we write explicitly the dependence of $\mathcal{H}_{\mathcal{T}}$ on $\mathcal{T}$.

B. Constraints on DoS Sequence

Since it is reasonable to assume that the attacker's resources are not infinite and measures can be taken to mitigate malicious DoS attacks, a natural characterization of DoS attacks can be given in terms of both the DoS *frequency* and the DoS *duration* as in [5], see also Remark 2 below. Therefore, we define the collection of times within the interval $[T_1, T_2]$, with $T_2 \geqslant T_1 \geqslant 0$, at which DoS attacks are active as

$$\Xi(T_1, T_2) := [T_1, T_2] \cap \mathcal{T} \tag{17}$$

with $\mathcal{T}$ as in (3) and the collection of time instants within the interval $[T_1, T_2]$ at which communication is possible as

$$\Theta(T_1, T_2) := [T_1, T_2] \backslash \Xi(T_1, T_2).$$

Consider a collection $\{I_i\}$, $i \in \bar{N}$ of N intervals that do not overlap, *i.e.*, $I_i \cap I_j = \emptyset$ for all $i, j \in \bar{N}$, $i \neq j$, and let $I = \bigcup_{i\in\bar{N}} I_i$. We denote with $|I|$ the sum of the lengths of all intervals I_i, $i \in \bar{N}$. Consequently, $|\Xi(T_1, T_2)|$ denotes the total length of the DoS attacks within the interval $[T_1, T_2]$. Consider the following definitions.

Definition 1. [6], [11] (DoS frequency). *Let* $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ *and let* $n(T_1, T_2)$ *denote the number of DoS* off/on *transitions*

[1] We foresee that the results in [24, Chapter 6, Chapter 7] on well-posed hybrid systems can relatively easily be used to obtain robustness properties with respect to arbitrarily small vanishing perturbations on the flow map jump map and all states. Note, however, that the focus of this paper is to obtain robustness result with respect to DoS attacks, which require different and new techniques. To not complicate the exposition of the novel techniques by introducing more technicalities needed to address also the robustness properties studied in [24], we describe only the new results, although they can be combined with the existing robustness results of [24].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

occurring in the interval $[T_1, T_2)$, i.e., $n(T_1, T_2) = card\{n \in \mathbb{N} \mid h_n \in [T_1, T_2)\}$, *where card denotes the number of elements in the set. We say that a given sequence of DoS attacks* $\{H_n\}_{n\in\mathbb{N}}$ *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* $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ *with* $T_2 \geqslant T_1$

$$n(T_1, T_2) \leqslant \nu + \frac{T_2 - T_1}{\tau_D}. \tag{18}$$

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. [6] (DoS duration). *We say that a 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* $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ *with* $T_2 \geqslant T_1$

$$|\Xi(T_1, T_2)| < \varsigma + \frac{T_2 - T_1}{T}. \tag{19}$$

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. Moreover, we also define the class of hybrid systems, which are generated by $(\nu, \tau_D, \varsigma, T)$-DoS sequences as $\mathcal{H}(\nu, \tau_D, \varsigma, T) := \{\mathcal{H}_\mathcal{T} \mid \mathcal{T}$ as in (3) with $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}(\nu, \tau_D, \varsigma, T)\}$.

Remark 2. *Observe that Definition 1 and Definition 2 make no assumptions regarding the attacker's underlying strategy as they only indicate limitations in terms of the frequency and duration of DoS attacks. From a practical point of view, Definition 1 and Definition 2 are natural as well since there exist several techniques to* mitigate *jamming attacks, for example, spreading techniques and high-pass filtering. As a consequence, the frequency and duration of DoS attacks can indeed be restrained by exploiting such techniques, see,* e.g., *[4], [8].*

Of course, desired control objectives can in general not be achieved in case the DoS frequency and/or DoS duration can be arbitrarily large, *i.e.*, in case $\tau_D \to 0$ or $T = 1$, respectively, as in that case every communication attempt can be blocked by the attacker with the consequence that the system is in open loop all the time. Fortunately, as already mentioned in Remark 2, several provisions can be taken in order to mitigate DoS attacks with the aim to limit the frequency and duration of the time intervals over which communication is effectively denied.

C. Mathematical Problem Formulation

To specify desirable stability and performance properties, we introduce the following definitions that use the concepts of hybrid time domains and corresponding solutions [24]. In this paper, we assume that all hybrid trajectories start in the set

$$\mathbb{X}_0 := \{\xi \in \mathbb{X} \mid \tau \geqslant \tau^0_{miet}, s = 0, \eta = 0, \phi = \phi_{miet}\}, \tag{20}$$

where ϕ_{miet} will be specified in Section V-B. Observe that this assumption only reflects the initialization of the ETM variables, which can be freely chosen, while we do not put any (initial) constraints on the plant and the controller states $x = (x_p, x_c)$ and the initial knowledge of $\hat{y}$ at the controller side.

Definition 3. *A hybrid system* $\mathcal{H}_\mathcal{T}$ *is said to be* persistently flowing *with respect to initial state set* $\mathbb{X}_0$ *if all maximal solutions*[2] ξ *with* $\xi(0,0) \in \mathbb{X}_0$ *have unbounded domains in the* t*-direction, i.e.,* $\sup_t dom\, \xi = \infty$.

Definition 4. *Let* $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$ *and* $T \in \mathbb{R}_{>1}$ *be given. A closed set* $\mathcal{A} \subset \mathbb{X}$ *is said to be* uniformly globally asymptotically stable *(UGAS) for the class of hybrid systems* $\mathcal{H}(\nu, \tau_D, \varsigma, T)$ *with respect to initial state set* $\mathbb{X}_0$ *if all systems* $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ *are persistently flowing with respect to initial state set* $\mathbb{X}_0$ *and there exists a function* $\beta \in \mathcal{KLL}$ *such that for any* $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ *and for any initial condition* $\xi(0,0) \in \mathbb{X}_0$, *all corresponding solutions* ξ *of* $\mathcal{H}_\mathcal{T}$ *with* $w = 0$ *satisfy*

$$|\xi(t,j)|_\mathcal{A} \leqslant \beta\left(|\xi(0,0)|_\mathcal{A}, t, j\right) \tag{21}$$

for all $(t,j) \in dom\, \xi$. *The closed set* $\mathcal{A}$ *is said to be* uniformly globally exponentially stable *(UGES) for the class of hybrid systems* $\mathcal{H}(\nu, \tau_D, \varsigma, T)$, *if the above holds with* $\beta(r, t, j) = Mr\exp(-\varrho(t + j))$ *for some* $M \geqslant 0$ *and* $\varrho > 0$.

Definition 5. *Let* $\vartheta, \nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$ *and* $T \in \mathbb{R}_{>1}$ *be given. A closed set* $\mathcal{A} \subset \mathbb{X}$ *is said to be* $\mathcal{L}_\infty$*-stable with an induced* $\mathcal{L}_\infty$*-gain less than or equal to* ϑ *for the class of hybrid systems* $\mathcal{H}(\nu, \tau_D, \varsigma, T)$, *if all systems* $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ *are persistently flowing with respect to initial state set* $\mathbb{X}_0$ *and there exists a* $\mathcal{K}_\infty$*-function* β *such that for any* $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$, *exogenous input* $w \in \mathcal{L}_\infty$, *and any initial condition* $\xi(0,0) \in \mathbb{X}_0$, *each corresponding solution to* $\mathcal{H}_\mathcal{T}$ *satisfies*

$$\|z\|_{\mathcal{L}_\infty} \leqslant \beta(|\xi(0,0)|_\mathcal{A}) + \vartheta\|w\|_{\mathcal{L}_\infty}. \tag{22}$$

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

Problem 1. *Given* $\nu \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}, \varsigma \in \mathbb{R}_{\geqslant 0}$ *and* $T \in \mathbb{R}_{>1}$, *provide design conditions for the values of* $\tau^0_{miet}, \tau^1_{miet} \in \mathbb{R}_{>0}$ *and the functions* $\tilde{\Psi}$, η_0 *as in the event generator given by (5) and (7) and* f_ϕ *as in (9), such that the closed set* $\mathcal{A} := \{\xi \in \mathbb{X} \mid x = 0, e = 0\}$ *is UGES and/or, in the presence of disturbances, has a finite induced* $\mathcal{L}_\infty$*-gain for the class of hybrid systems* $\mathcal{H}(\nu, \tau_D, \varsigma, T)$.

V. Design Conditions and Stability Guarantees

In Section V-B and Section V-C, the time-constants τ^0_{miet} and τ^1_{miet}, and the function f_ϕ are specified and design conditions for the functions $\tilde{\Psi}$ and η_0 are presented leading

[2][24, Chapter 2] A solution ξ to $\mathcal{H}_\mathcal{T}$ is maximal if there does not exist another solution $\bar{\xi}$ to $\mathcal{H}_\mathcal{T}$ such that dom ξ is a proper subset of dom $\bar{\xi}$ and $\xi(t,j) = \bar{\xi}(t,j)$ for all $(t,j) \in$ dom ξ.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

to a solution for Problem 1. In order to specify the design conditions, we first start with the required preliminaries consisting of stability and performance conditions for *time-triggered* NCSs taken from [25], [26] in Section V-A.

A. Preliminaries

Consider the following condition.

Condition 1. *([25], [26]) 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 $L \geqslant 0$, $\underline{c}_W$, and $\bar{c}_W$, such that*

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

$$\underline{c}_W |e| \leqslant W(e) \leqslant \bar{c}_W |e|, \tag{23}$$

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

$$\left\langle \frac{\partial W(e)}{\partial e}, g(x,e,w) \right\rangle \leqslant LW(e) + H(x,w). \tag{24}$$

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

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

$$\underline{c}_V |x|^2 \leqslant V(x) \leqslant \bar{c}_V |x|^2,\ c_z |q(x)|^2 \leqslant V(x), \tag{25}$$

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

$$\begin{aligned} \langle \nabla V(x), f(x,e,w) \rangle \leqslant -\rho_V V(x) - \varrho(|y|) - H^2(x,w) \\ + (\gamma^2 - \rho_W) W^2(e) + \theta^2 |w|^2, \end{aligned} \tag{26}$$

- *the constants ρ_W and γ satisfy $\rho_W \leqslant \gamma^2$.*

Let us remark that for linear systems the conditions above can be obtained systematically by solving a multi-objective linear matrix inequality (LMI) problem, see [12], [13], [26] for more details. Also several classes of nonlinear systems satisfy these conditions, see [13].

B. Minimal Inter-event Time

As already mentioned, τ^0_{miet} and τ^1_{miet} (and ϕ_{miet}, $\tilde{\Psi}$, f_ϕ and η_0) should be chosen appropriately in the sense that desirable closed-loop stability and performance requirements can be achieved. To do so, we specify the function[3] $f_\phi : \mathbb{R}_{\geqslant 0} \times \mathbb{N} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}$, as

$$f_\phi(\tau, m, \phi) := \begin{cases} (m-1)\left(2L\phi + \gamma(\phi^2+1)\right), & \text{for } \tau \leqslant \tau^0_{miet}, \\ 0, & \text{for } \tau > \tau^0_{miet}, \end{cases} \tag{27}$$

with L and γ as given in Condition 1. The time-constants τ^0_{miet} and τ^1_{miet} can be chosen less than or equal to the *maximally allowable transmission interval* bound (in this work referred to as $\bar{\tau}_{miet}$) given in [25] as

$$\bar{\tau}_{miet} := \begin{cases} \frac{1}{Lr} \arctan\left(\frac{r(1-\lambda)}{2\frac{\lambda}{1+\lambda}\left(\frac{\gamma}{L}-1\right)+1+\lambda} \right), & \gamma > L \\ \frac{1}{L}\frac{1-\lambda}{1+\lambda}, & \gamma = L \\ \frac{1}{Lr} \operatorname{arctanh}\left(\frac{r(1-\lambda)}{2\frac{\lambda}{\lambda+1}\left(\frac{\gamma}{L}-1\right)+1+\lambda} \right), & \gamma < L, \end{cases} \tag{28}$$

where $r = \sqrt{|(\gamma/L)^2 - 1|}$. Note that by selecting τ^0_{miet} and τ^1_{miet} equal to the right-hand side of (28) indeed longer (average) transmission intervals are realized compared to time-based (worst-case) specifications as discussed in Section III-C.

Lemma 1. *[25] Let $\bar{\tau}_{miet}$ be given by (28), then the solution to*

$$\dot{\tilde{\phi}} = -2L\tilde{\phi} - \gamma\left(\tilde{\phi}^2 + 1\right) \tag{29}$$

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

Finally, we define

$$\phi_{miet} := \tilde{\phi}(\tau^0_{miet}), \tag{30}$$

where $\tilde{\phi}$ is the solution to (29) with $\tilde{\phi}(0) = \lambda^{-1}$ and note again that $\tau^1_{miet} \leqslant \tau^0_{miet} \leqslant \bar{\tau}_{miet}$.

C. Stability and Performance Guarantees

Theorem 2. *Consider the class of hybrid systems $\mathcal{H}(\nu, \tau_D, \varsigma, T)$ with $\nu, \varsigma \in \mathbb{R}_{\geqslant 0}$, $\tau_D \in \mathbb{R}_{>0}$, $T \in \mathbb{R}_{>1}$ and let Condition 1 be satisfied with $\tau^1_{miet} \leqslant \tau^0_{miet} \leqslant \bar{\tau}_{miet}$ with $\bar{\tau}_{miet}$ as in (28) and with f_ϕ and ϕ_{miet} as in (27) and (30), respectively. Moreover, suppose that the following three conditions hold:*

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

$$\frac{\tau^1_{miet}}{\tau_D} + \frac{1}{T} < \frac{\omega_1}{\omega_1 + \omega_2}, \tag{31}$$

where

$$\omega_1 = \min\left(\rho_V, \frac{\lambda \rho_W}{\gamma}\right),\ \omega_2 = \frac{(\bar{\gamma} - \rho_W)}{\gamma \phi_{miet}} \tag{32}$$

and

$$\bar{\gamma} := \gamma\left(2\phi_{miet}L + \gamma(1 + \phi^2_{miet})\right). \tag{33}$$

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

$$\tilde{\Psi}(m, o, \eta) = \begin{cases} \Psi(o) - \sigma(\eta), & \text{when } m = 0, \\ -(1 - \omega(\tau, m)), & \text{when } m = 1, \end{cases} \tag{34}$$

where σ is a $\mathcal{K}_\infty$-function that satisfies $\sigma(s) \geqslant \omega_1 s$ for all $s \in \mathbb{R}_{\geqslant 0}$, the function $\Psi : \mathbb{O} \to \mathbb{R}$ is given by

$$\Psi(o) = \varrho(|y|) + \bar{\gamma}\omega(\tau, m) W^2(e) \tag{35}$$

with

$$\omega(\tau, m) \quad := \quad \begin{cases} 1, & \text{for } 0 \leqslant \tau \leqslant \tau^m_{miet} \\ 0, & \text{for } \tau > \tau^m_{miet}, \end{cases} \tag{36}$$

for $\tau \in \mathbb{R}_{\geqslant 0}$ and with $\bar{\gamma}$ as given in (33).

[3] Observe that the flow map F as given in (9) is discontinuous in τ due to (27). However, due to the facts that $\dot{\tau} = 1$ and the right hand-side of (27) is Lipschitz continuous, we find by means of the Carathéodory's existence theorem that this does not cause any problems in the uniqueness and existence of solutions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

iii) The function η_0 is given by $\eta_0(e) = \gamma\phi_{miet}W^2(e)$.

Then the closed set $\mathcal{A} = \{\xi \in \mathbb{X} \mid x = 0, e = 0\}$ is UGES and is $\mathcal{L}_\infty$-stable with a finite induced $\mathcal{L}_\infty$-gain less than or equal to $\theta\sqrt{\frac{\kappa}{c_z\beta^*}}$ with c_z as in (25) and where $\kappa := e^{\varsigma_*(\omega_1+\omega_2)}$, $\varsigma_* := \varsigma + \nu\tau^1_{miet}$, $\beta_* = \omega_1 - (\omega_1+\omega_2)/T_*$ and $T_* := \tau_D T/(\tau_D + \tau^1_{miet}T)$, for the class of hybrid systems $\mathcal{H}(\nu, \tau_D, \varsigma, T)$.

The proof is provided in the Appendix. Observe that the condition given in item i) imposes restrictions on the DoS parameters τ_D and T in terms of other system parameters. As such, the frequency and duration of the allowable DoS attacks are limited. Moreover, observe that the DoS parameters ν, τ_D, ς and T affect the guaranteed $\mathcal{L}_\infty$-gain of the system which illustrates the tradeoff between robustness with respect to DoS attacks and performance in the sense that in general, robustness comes at cost of performance.

Observe 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 again after τ^1_{miet} time units (to determine when the DoS attack is over) since when $m = 1$, which implies that $\eta = 0$ at the previous transmission attempt, $\tilde{\Psi}(m, o, \eta) = 0$ for $0 \leqslant \tau \leqslant \tau^1_{miet}$ and $\tilde{\Psi}(m, o, \eta) = -1$ for $\tau > \tau^1_{miet}$. Hence, when $m = 1$ and $\tau > \tau^1_{miet}$ a next jump occurs as flow condition $\eta \geqslant 0$ will be violated.

Remark 3. *Note that this implementation requires the knowledge about when DoS attacks are blocking transmissions, which could be realized by means of acknowledgements as illustrated in Figure 1. Let us remark that the ETM can easily be adjusted such that it is not required that acknowledgements are being received instantaneously. For example, the acknowledgement is allowed to be delayed with at most τ^1_{miet} time units if after each transmission instant, the ETM keeps track of the evolution of η for both the cases that the transmission has been successful or denied. For the brevity of exposition, this feature has, however, been omitted.*

The presented framework does not require an acknowledgement scheme when purely periodic sampling with inter-sampling time τ^1_{miet} is employed. The same design conditions lead to the same guarantees in this case.

Remark 4. *The proposed framework can also be used for the design of a* static *triggering mechanism, namely*

$$t_{j+1} := \inf\left\{t > t_j + \tau^{m(t)}_{miet} \mid \Psi(o) \leqslant 0\right\}, \qquad (37)$$

with $t_0 = 0$ and with Ψ as in (35).

VI. Case Study on Cooperative Adaptive Cruise Control

In this section, we illustrate the main result by means of a case study on cooperative adaptive cruise control (CACC). As shown in [27], in the context of vehicle platooning, wireless communication between vehicles can have a significant contribution to improving traffic throughput and safety. For a platoon of two identical vehicles equipped with CACC, the functions f and g as in (9) are given by $f(x, e, w) = A_{11}x + A_{12}e + A_{13}w$ and $g(x, e, w) = A_{21}x + A_{22}e + A_{23}w$, where

$$A_{11} = \begin{bmatrix} -\frac{1}{\tau_c} & \frac{1}{\tau_c} & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{h} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -h & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{\tau_c} & \frac{1}{\tau_c} \\ 0 & \frac{1}{h} & \frac{k_p}{h} & \frac{k_d}{h} & -k_d & -\frac{1}{h} \end{bmatrix}$$

$$A_{12} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{h} \end{bmatrix}^\top,$$

$$A_{13} = \begin{bmatrix} 0 & \frac{1}{h} & 0 & 0 & 0 & 0 \end{bmatrix}^\top,$$

$$A_{21} = \begin{bmatrix} 0 & \frac{1}{h} & 0 & 0 & 0 & 0 \end{bmatrix}, A_{22} = 0, A_{23} = -\frac{1}{h}$$

with $\tau_c \in \mathbb{R}_{>0}$ a time-constant corresponding to the driveline dynamics, $h \in \mathbb{R}_{>0}$ the time headway (desired time between the two vehicles) and $k_p, k_d \in \mathbb{R}_{>0}$ the controller gains. Moreover, the input w represents the control input of the leading vehicle. See, *e.g.*, [27] for more details. For this example, we use the following parameter values $\tau_c = 0.15$, $h = 0.6$, $k_p = 0.2$, $k_d = 0.7$. To comply with safety, one of the control objectives is to keep the error with respect to the vehicle desired distance small and therefore we define the performance output as $z = C_z x$, where

$$C_z = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

which corresponds to the spacing error between the two vehicles. The measured output y as in (1) is the desired acceleration of the leading vehicle and is given by $y = C_y x$, where

$$C_y = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and is available at the ETM to determine the transmission instants.

Before the ETM design and the stability and performance analysis, we first have to guarantee that Condition 1 is met. For the vehicle platoon system described above, we can take $W(e) = |e|$. Observe that with this choice, (23) and (24) are met with $\underline{c}_W = \bar{c}_W = 1$, $L = 0$ and $H(x, w) = |A_{21}x + A_{21}w|$. To comply with (25) and (26), we take $\varrho(r) = qr^2$ and $V(x) = x^\top Px$, $\underline{c}_V = \lambda_{\min}(P)$ and $\bar{c}_V = \lambda_{\max}(P)$ where P can be obtained by minimizing $\gamma + \theta$ subject to the LMI given in (38).

To illustrate the design procedure, we take $\lambda = 0.7$ and compute $\bar{\tau}_{miet}$ (as in (28)) for various ρ_V and ρ_W. By taking $\lambda = 0.7$, $c_z = 1$ and $\tau^0_{miet} = \tau^1_{miet} = \frac{1}{2}\bar{\tau}_{miet}$, we obtain Figure 2 and Figure 3, which illustrate robustness in terms of $\frac{\omega_1}{\omega_1+\omega_2}$ which corresponds to the right-hand side of (31) and network utilization in terms of τ^1_{miet}, respectively.

Let us now study the influence of four DoS attacks of length zero on the performance of the system described above. For this reason, we take $\nu = 4$, $\varsigma = 0$ and we take $\beta^* = \frac{3}{4}\omega_1$ which implies that τ_D and T should satisfy $\frac{\tau_{miet}}{\tau_D} + \frac{1}{T} \leqslant \frac{1}{4}\frac{\omega_1}{\omega_1+\omega_2}$. The $\mathcal{L}_\infty$-gains for this case for various ρ_V and ρ_W are shown in Figure 4. Let us remark that other choices for ς and ν such as, *e.g.*, $\varsigma = \tau_{miet}$ and $\nu = 2\tau_{miet}$ lead to identical results in terms of the $\mathcal{L}_\infty$-gain but allow for different classes of DoS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

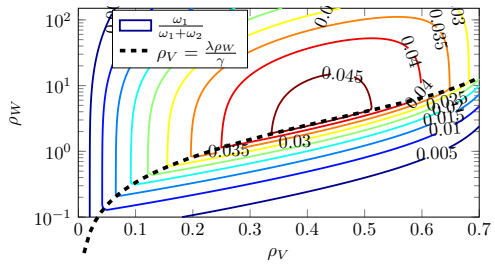

Figure 2. The achievable robustness in terms of $\frac{\omega_1}{\omega_1+\omega_2}$ for various values of ρ_V and ρ_W. The dashed line represents the points for which $\omega_1 = \rho_V = \frac{\lambda\rho_W}{\gamma}$

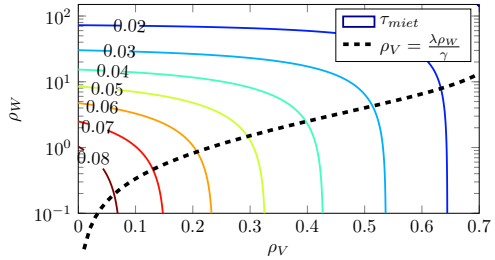

Figure 3. The minimal inter-event time for various values of ρ_V and ρ_W. The dashed line represents the points for which $\omega_1 = \rho_V = \frac{\lambda\rho_W}{\gamma}$

Attacks. The dashed-line In Figure 2, Figure 4 and Figure 3 represents the points at which $\omega_1 = \rho_V = \frac{\lambda\rho_W}{\gamma}$. Observe that below this line, the tradeoff between robustness, network utilization and performance is unfavorable for $\rho_V \geqslant \frac{\lambda\rho_W}{\gamma}$, since for this case, a smaller ρ_W leads to a relatively steep decline in both robustness and performance in contrast to the minimal inter-event time τ^1_{miet} that barely changes.

In Figure 5, the distance error/performance output z and the inter-event times $t_{j+1} - t_j$ are displayed for the case that $\rho_V = 0.5$, $\rho_W = 5$ and w as illustrated the figure resulting in an $\mathcal{L}_\infty$-gain less than or equal to 5.35, $\frac{\omega_1}{\omega_1+\omega_2} = 0.0454$ and $\tau^0_{miet} = \tau^1_{miet} = 0.0307$. Although in general, it is difficult to obtain the worst-case DoS attack and disturbance, the simulation results show that for this particular system, the derived $\mathcal{L}_\infty$-bound is a somewhat conservative. In fact, more consecutive transmission failures can be tolerated as shown in Figure 5. To obtain better performance in terms of lower $\mathcal{L}_\infty$-bounds, λ and/or c_z could be chosen larger and τ^0_{miet} and τ^1_{miet} could be chosen smaller. However, this comes at cost of increased network utilization and/or reduced robustness with respect to DoS attacks.

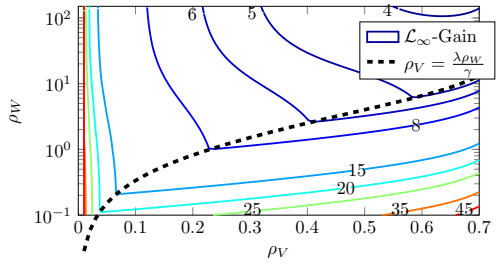

Figure 4. The $\mathcal{L}_\infty$-gain for various values of ρ_V and ρ_W. The dashed line represents the points for which $\omega_1 = \rho_V = \frac{\lambda\rho_W}{\gamma}$

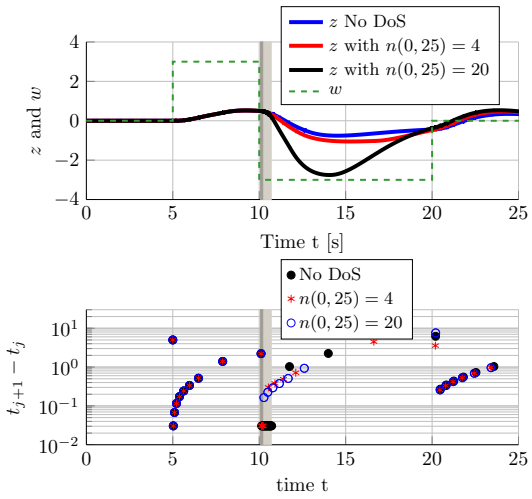

Figure 5. In the top plot, the trajectory of the distance error z of the vehicle platoon for DoS-attacks of various sizes and the input w are given. In the bottom plot, the inter-event times of the dynamic event triggering mechanism described by (5) and (7) are given. Both plots were generated by taking $\rho_V = 0.5$ and $\rho_W = 5$ resulting in $\mathcal{L}_\infty$-gain less than or equal to 5.35, $\frac{\omega_1}{\omega_1+\omega_2} = 0.0454$ and $\tau_{miet} = 0.0307$. The dark and light gray boxes show where the DoS attacks take place that block 4 and 20 consecutive transmissions, respectively.

VII. Conclusion

In this work, we addressed the design of *resource-aware* and *resilient* control strategies for networked control systems (NCS) subject to malicious *Denial-of-service* (DoS) attacks. In particular, the control and communication strategy was based on an *output-based* event-triggered control scheme applicable to a class of non-linear feedback systems that are subject to exogenous disturbances. The proposed framework led to guarantees regarding the existence of a robust strictly positive lower bound on the inter-event times despite the presence of disturbances and DoS attacks. Additionally, based on the natural assumption that DoS attacks are restricted in terms of frequency and duration, we showed that desired stability and performance criteria in terms of induced $\mathcal{L}_\infty$-gains can be guaranteed.

Appendix

Proof of Theorem 2: The main idea behind the proof is to regard the closed-loop system $\mathcal{H}_\mathcal{T}$ as a system switching between a stable hybrid model (when effectively no DoS attack is active) and an unstable mode (when effectively a DoS attack is active). Inspired by the concept of *average dwell-time* [11], we can then exploit the duration and frequency constraints of the DoS attacks to conclude UGES (or $\mathcal{L}_\infty$-stability a finite induced $\mathcal{L}_\infty$-gain) of the set $\mathcal{A}$ for the class of hybrid systems $\mathcal{H}(\nu, \tau_D, \varsigma, T)$. For clarity of exposition, the proof consists of four steps. In the proof, we often omit the time arguments of the solution ξ of a hybrid system $\mathcal{H}_\mathcal{T}$ and we do not mention dom ξ explicitly.

Step I. *Lyapunov/storage function analysis.* Let $\mathcal{R}(\mathbb{X}_0)$ denote all the reachable states of a hybrid system $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ for $\xi(0,0) \in \mathbb{X}_0$, see also [24, Chapter 6].

Lemma 3. *For any $\chi \in \mathcal{R}(\mathbb{X}_0)$ it holds that*

- $\{m = 1 \vee \tau \geqslant \tau^0_{miet}\} \Leftrightarrow \phi = \phi_{miet}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

$$\begin{pmatrix} A_{11}^\top P + PA_{11} + \rho_V P + A_{21}^\top A_{21} + C^\top QC & PA_{12} & PA_{13} + A_{21}^\top A_{23} \\ A_{12}^\top P & (\rho_W - \gamma^2)I & 0 \\ A_{13}^\top P + A_{23}^\top A_{21} & 0 & A_{23}^\top A_{23} - \theta^2 I \end{pmatrix} \preceq 0,\ P \succeq 0, C_y^\top C_y \preceq P. \tag{38}$$

- $\lambda^{-1} \geqslant \phi \geqslant \phi_{miet}$
- $\eta \geqslant 0$

Moreover, for all $\chi \in \mathcal{R}(\mathbb{X}_0)\backslash D$ there exists an $\varepsilon > 0$ and an absolutely continuous function $z : [0, \varepsilon] \to \mathbb{R}^n$ such that $z(0) = \chi$, $\dot{z}(t) = F(z(t))$ for almost all $t \in [0, \varepsilon]$ and $z(t) \in C$ for all $t \in (0, \varepsilon]$.

The proof is omitted for the sake of brevity. Consider the candidate Lyapunov/storage function,

$$U(\xi) = V(x) + \gamma\phi W^2(e) + \eta. \tag{39}$$

Given the second and third item of Lemma 3 and the fact that according to Condition 1, V and W satisfy (25) and (23), respectively, and $\gamma > 0$, we find that there exists a positive constant $\underline{c}_U \in \mathbb{R}_{\geqslant 0}$ such that

$$\underline{c}_U |\xi|_{\mathcal{A}}^2 \leqslant U(\xi), \tag{40}$$

for all $\xi \in \mathcal{R}(\mathbb{X}_0)$ where $\mathcal{A} = \{\xi \in \mathbb{X} \mid x = 0, e = 0\}$. Hence, U constitutes a suitable candidate Lyapunov/storage function for the cases $w = 0$ and $w \neq 0$, respectively.

To study the stability and the performance, we will discuss how the function U evolves over time by considering both jumps (when $\xi \in D$), and flows (when $\xi \in C$).

Jumps: We can see from (14) and (27) that at transmission events when communication is possible, *i.e.,* if $\xi \in \mathcal{R}(\mathbb{X}_0)$ and $\xi \in D$ and $s \notin \mathcal{T}$ (and thus $\eta = 0$), we have that $U(\xi^+) - U(\xi) = -\gamma\phi W^2(e) + \eta_0(e)$. By recalling that $\eta_0 = \gamma\phi_{miet} W^2(e)$, the first item of Lemma 3 and by using the fact that $\tau \geqslant \tau_{miet}^0$ when $\xi \in D$, we have that

$$U(\xi^+) - U(\xi) = 0, \tag{41}$$

when $\xi \in \mathcal{R}(\mathbb{X}_0) \cap D$ and $s \notin \mathcal{T}$ (and thus $\tau \geqslant \tau_{miet}^0$). At transmission times during a DoS attack, *i.e.,* when $\xi \in D$, and $s \in \mathcal{T}$, (41) holds as well since $e^+ = e$, $\phi^+ = \phi$, $\eta^+ = \eta = 0$ and $x^+ = x$.

Flows: For the bounds on U during flow we consider two cases depending on whether the most recent transmission attempt was successful ($m = 0$) or not ($m = 1$).

Case I ($m = 0$): From (24), (26) and (27), we can derive that for almost all $\xi \in \mathcal{R}(\mathbb{X}_0)$ with $m = 0$ and for $w \in \mathbb{R}^{n_w}$,

$$\begin{aligned} \langle \nabla U(\xi), F(\xi, w)\rangle &\leqslant -\varrho(|y|) - H^2(x,w) + \gamma^2 W^2(e) \\ &\quad +2\gamma\phi W(e)\left(LW(e) + H(x,w)\right) \\ &\quad -\omega(\tau,0)\gamma W^2(e)\left(2L\phi + \gamma\left(\phi^2+1\right)\right) \\ &\quad -\rho_W W^2(e) - \rho_V V(x) + \tilde{\Psi}(m,o,\eta) + \theta^2|w|^2 \\ &\leqslant -\rho_V V(x) - \rho_W W^2(e) - M(\xi,w) + \tilde{\Psi}(m,o,\eta) + \theta^2|w|^2, \end{aligned} \tag{42}$$

with $\omega(\tau, m)$ as in (36) and where M given by

$$M(\xi,w) = \begin{cases} M_1(\xi,w), & \text{for } 0 \leqslant \tau \leqslant \tau_{miet}^0, \\ M_2(\xi,w), & \text{for } \tau > \tau_{miet}^0, \end{cases} \tag{43}$$

where for all $\xi \in \mathbb{X}$ and $w \in \mathbb{R}^{n_w}$

$$M_1(\xi,w) := \varrho(|y|) + \left(H(x,w) - \gamma\phi W(e)\right)^2, \tag{44}$$

$$\begin{aligned} M_2(\xi,w) := \varrho(|y|) + H^2(x,w) - 2\gamma\phi W(e)H(x,w) \\ - \left(\gamma^2 + 2\gamma\phi L\right) W^2(e). \end{aligned} \tag{45}$$

By using the fact that $2\gamma\phi W(e)H(x,w) \leqslant \gamma^2\phi^2 W^2(e) + H^2(x,w)$, we can conclude from (35) and (43) that $\Psi(o) \leqslant M(\xi,w)$ for all $o \in \mathbb{O}$. Using the latter fact, we obtain from (34) and (42) that for $m = 0$, $\langle \nabla U(\xi), F(\xi,w)\rangle \leqslant -\rho_V V(x) - \rho_W W^2(e) - \omega_1\eta + \theta^2|w|^2$. By using Lemma 3 and the fact that $V(x) \leqslant c_{\bar{V}}|x|^2$ due to (25), we can conclude that for almost all $\xi \in \mathcal{R}(\mathbb{X}_0)$ with $m = 0$ and for $w \in \mathbb{R}^{n_w}$, we have that

$$\langle \nabla U(\xi), F(\xi,w)\rangle \leqslant -\omega_1 U(\xi) + \theta^2|w|^2, \tag{46}$$

with ω_1 as in (32).

Case II ($m = 1$): Observe that for $m = 1$, we have that $\dot{\phi} = 0$ and $\dot{\eta} = 0$ due to (7), (27) and (34), respectively. Hence, it holds that for almost all $\xi \in \mathcal{R}(\mathbb{X}_0)$ with $m = 1$ and for all $w \in \mathbb{R}^{n_w}$

$$\begin{aligned} \langle \nabla U(\xi), F(\xi,w)\rangle &\leqslant -\varrho(|y|) - H^2(x,w) + \gamma^2 W^2(e) \\ &\quad +2\gamma\phi W(e)\left(LW(e) + H(x,w)\right) \\ &\quad -\rho_W W(e) - \rho_V V(x) + \theta^2|w|^2. \end{aligned}$$

Using the fact that $2\gamma\phi W(e)H(x,w) \leqslant \gamma^2\phi^2 W^2(e) + H^2(x,w)$, and Lemma 3 we obtain that $\langle \nabla U(\xi), F(\xi,w)\rangle \leqslant (\bar{\gamma} - \rho_W)W^2(e) + \theta^2|w|^2$ with $\bar{\gamma}$ as in (33). Hence, it holds that for almost all $\xi \in \mathcal{R}(\mathbb{X}_0)$ with $m = 1$ and all $w \in \mathbb{R}^{n_w}$

$$\langle \nabla U(\xi), F(\xi,w)\rangle \leqslant \omega_2 U(\xi) + \theta^2|w|^2 \tag{47}$$

with ω_2 as in (32). In fact, observe that since $\omega_2 >$ due to Condition 1, (47) also holds when $m = 0$.

Observe that a system $\mathcal{H}_{\mathcal{T}} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ does not exhibit Zeno-behaviour due to a strictly positive MIET. Moreover, observe that finite escape-times are excluded from the system due to the bounds on the states x and e as in (40), (41), (46), (47) and the fact that the trajectories of the state variables τ, s, m, η, and ϕ do not exhibit finite escape-times. Given the aforementioned facts and the last property mentioned in Lemma 3, we can conclude that a system $\mathcal{H}_{\mathcal{T}} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$ with $\xi(0,0) \in \mathbb{X}_0$ is indeed persistently flowing with respect to initial state set $\mathbb{X}_0$.

Step II. *Characterization of stable and unstable modes.* In the previous step, we have shown how the Lyapunov/storage function behaves for both the cases where $m = 0$ and $m = 1$, see (46) ($m = 0$) and (47) ($m = 1$). To use average dwell-time arguments, it is needed to determine the collection of time instants at which either $m = 0$ or $m = 1$. Unfortunately, this can not directly be related to $\mathcal{T}$, since the value of $\hat{y}$ is typically not updated immediately after a DoS interval has ended due to τ_{miet}^1 being a lower bound on the inter-event times $t_{j+1} - t_j$, $j \in \mathbb{N}$, for which transmission time t_j corresponds to an

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

unsuccessful transmission attempt. For this reason, we will consider the "effective" DoS attacks, decompose the time axis accordingly and relate these "effective" DoS attacks to $\mathcal{T}$ via the collection of DoS intervals as given in (17). To do so, we first define for a given maximal solution ξ, the collection of time instants in the interval $[T_1, T_2]$, with $T_2 \geqslant T_1$, at which the most recent transmission attempt was successful and at which no DoS attack is active as

$$\bar{\Theta}_\xi(T_1,T_2) := \big\{\bar{t} \in (T_1,T_2) \mid \bar{t} \notin \mathcal{T} \text{ and } \forall j \in \mathbb{N}, (\bar{t},j) \in \text{dom } \xi \Rightarrow m(\bar{t},j) = 0\big\}. \quad (48)$$

The system $\mathcal{H}_\mathcal{T}$ is said to be in the *stable mode* (satisfying (46)) at a time instant t if $t \in \bar{\Theta}_\xi(0,\infty)$. In addition, we define the collection of "effective" DoS attacks in the interval $[T_1, T_2]$, with $T_2 \geqslant T_1$ as

$$\bar{\Xi}_\xi(T_1,T_2) := [T_1,T_2]/\bar{\Theta}_\xi(T_1,T_2). \quad (49)$$

Likewise, the system is said to be in the *unstable mode* (satisfying (47)) at a time instant t if $t \in \bar{\Xi}_\xi(0,\infty)$. Since for $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_2 \geqslant T_1$, $\bar{\Theta}_\xi(T_1,T_2) \cup \bar{\Xi}_\xi(T_1,T_2) = [T_1,T_2]$, we can write $\bar{\Theta}_\xi(T_1,T_2)$ and $\bar{\Xi}_\xi(T_1,T_2)$ as follows

$$\bar{\Xi}_\xi(T_1,T_2) := \bigcup_{k\in\mathbb{N}} Z_k \cap [T_1,T_2], \quad (50)$$

and

$$\bar{\Theta}_\xi(T_1,T_2) := \bigcup_{k\in\mathbb{N}} W_{k-1} \cap [T_1,T_2], \quad (51)$$

where for $k \in \mathbb{N}$

$$Z_k := \begin{cases} [\zeta_k, \zeta_k + v_k) & \text{when } v_k > 0, \\ \{\zeta_k\} & \text{when } v_k = 0, \end{cases}$$

$$W_k := \begin{cases} [\zeta_k + v_k, \zeta_{k+1}) & \text{when } v_k > 0, \\ (\zeta_k, \zeta_{k+1}) & \text{when } v_k = 0, \end{cases}$$

where v_k denotes the time elapsed between ζ_k and the next successful transmission attempt, and where $\zeta_0 := h_0$ where $W_{-1} = [0, \zeta_0)$ when $h_0 > 0$ and $W_{-1} = \emptyset$ when $h_0 = 0$. The collection of *effective* DoS attacks can be related to the *original* collection of DoS intervals as given in (17) as

$$|\bar{\Xi}_\xi(T_1,T_2)| \leqslant |\Xi(T_1,T_2)| + (1 + n(T_1,T_2))\tau^1_{miet}, \quad (52)$$

for all $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_2 \geqslant T_1$, where $n(T_1,T_2)$ denotes the number of DoS attacks in the interval $[T_1,T_2)$. Indeed, due to the finite sampling rate, the effective DoS interval $\bar{H}_n$ is extended with maximally τ^1_{miet} time units compared to H_n, $n \in \mathbb{N}$. Since this extension might also occur at the beginning of an interval $[T_1,T_2)$, the collection of effective DoS attacks over the interval $[T_1,T_2)$ is at most prolonged with $(1 + n(T_1,T_2))\tau^1_{miet}$ time units. Observe that the latter is not the case if $T_1 \in \big[\big(\bigcup_{k\in\mathbb{N}} W_{k-1}\big) \cup \{0\}\big] \cap [0,t]$, *i.e.*,

$$|\bar{\Xi}_\xi(T_1,T_2)| \leqslant |\Xi(T_1,T_2)| + n(T_1,T_2)\tau^1_{miet}, \quad (53)$$

for all $T_1 \in \big[\big(\bigcup_{k\in\mathbb{N}} W_{k-1}\big) \cup \{0\}\big] \cap [0,t]$ and all $T_2 \in \mathbb{R}_{\geqslant T_1}$. By means of Definition 1 and Definition 2 for the specific values of τ_D and T, we find that according to (53)

$$|\bar{\Xi}_\xi(T_1,T_2)| \leqslant \varsigma_* + \frac{T_2 - T_1}{T_*}, \quad (54)$$

where $\varsigma_* := \varsigma + \nu\tau^1_{miet}$ and $T_* := \tau_D T/(\tau_D + \tau^1_{miet} T)$ for all $T_1 \in \big[\big(\bigcup_{k\in\mathbb{N}} W_{k-1}\big) \cup \{0\}\big] \cap [0,t]$ and all $T_2 \in \mathbb{R}_{\geqslant T_1}$.

In summary, in this second step of the proof, we defined effective DoS sequences, which led to the intervals Z_k and W_k, $k \in \mathbb{N}$, representing the *stable* and (possibly) *unstable* mode of the system, respectively. Furthermore, we showed how this effective DoS is related to the original DoS sequence. This relation will be important in the stability and performance analysis.

Step III. *Time-trajectory bounds on Lyapunov/storage function.* As already mentioned, the collection of time instants at which either $m = 0$ or $m = 1$ can not directly be related to $\mathcal{T}$. However, we can deduce the following implications regarding a trajectory ξ with $\xi(0,0) \in \mathbb{X}_0$ and the *stable* and *unstable* mode descriptions

$$(t,j) \in (W_k \times \mathbb{N}) \cap \text{dom } \xi \Rightarrow m(t,j) = 0,$$
$$(t,j) \in (Z_k \times \mathbb{N}) \cap \text{dom } \xi \Rightarrow (m(t,j) = 0 \text{ or } m(t,j) = 1).$$

Based on these implications, (41), (46) and (47), we have that for all $(t,j) \in (W_k \times \mathbb{N}) \cap \text{dom } \xi$, $k \in \mathbb{N} \cup \{-1\}$

$$U(\xi(t,j)) \leqslant e^{-\omega_1(t-\zeta_k-v_k)} U(\xi(\zeta_k + v_k, j)) + \theta^2 \int_{(\zeta_k+v_k)}^{t} e^{-\omega_1(t-s)} |w(s)|^2 ds \quad (55)$$

and for all $(t,j) \in (Z_k \times \mathbb{N}) \cap \text{dom } \xi$, $k \in \mathbb{N}$

$$U(\xi(t,j)) \leqslant e^{\omega_2(t-\zeta_m)} U(\xi(\zeta_k, j)) + \theta^2 \int_{\zeta_k}^{t} e^{\omega_2(t-s)} |w(s)|^2 ds. \quad (56)$$

In essence, the right-hand sides of (55) and (56) reflect bounds on the Lyapunov/storage function U over (hybrid) time for the stable and unstable modes, respectively. In order to asses the performance of a system $\mathcal{H}_\mathcal{T} \in \mathcal{H}(\nu, \tau_D, \varsigma, T)$, we require an upper-bound that holds for all $(t,j) \in \text{dom } \xi$. For this reason, consider the following statement.

Lemma 4. *For all $(t,j) \in$ dom ξ, it holds that*

$$U(\xi(t,j)) \leqslant \Upsilon(0,t) U(\xi(0,0)) + \theta^2 \int_0^t \Upsilon(s,t) |w(s)|^2 ds \quad (57)$$

with $\Upsilon(s,t) := e^{-\omega_1 |\bar{\Theta}_\xi(s,t)|} e^{\omega_2 |\bar{\Xi}_\xi(s,t)|}$.

Proof of Lemma 4: We will prove Lemma 4 by induction. First, we need to prove that (57) holds for all $(t,j) \in [0,\zeta_0) \times \mathbb{N} \cap \text{dom } \xi$. To do so, observe that for all $(t,j) \in W_{-1} \times \mathbb{N} \cap \text{dom } \xi$ it holds that $|\bar{\Theta}_\xi(0,t)| = t$ and $|\bar{\Xi}_\xi(0,t)| = 0$. By substituting the latter in (57), we can conclude that for all $(t,j) \in W_{-1} \times \mathbb{N} \cap \text{dom } \xi$, the inequality given in (57) coincides with (55). As such, (57) holds for all $(t,j) \in W_{-1} \times \mathbb{N} \cap \text{dom } \xi$ and thus for all $(t,j) \in [0,\zeta_0) \times \mathbb{N} \cap \text{dom } \xi$. Now assume (57) holds for all $(t,j) \in [0,\zeta_p) \times \mathbb{N} \cap \text{dom } \xi$, where $p \in \mathbb{N}$. By means of this hypothesis and the inequality in (56),

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2613445, IEEE Transactions on Control of Network Systems

we find that for all $(t,j) \in (Z_p \times \mathbb{N}) \cap \operatorname{dom} \xi$,

$$U(\xi(t,j)) \leqslant e^{\omega_2(t-\zeta_p)}\Upsilon(0,\zeta_p)U(\xi(0,0)) + \theta^2 e^{\omega_2(t-\zeta_p)} \int_0^{\zeta_p} \Upsilon(s,\zeta_p)|w(s)|^2 ds + \theta^2 \int_{\zeta_p}^{t} e^{\omega_2(t-s)}|w(s)|^2 ds. \quad (58)$$

Since for all $t \in Z_p$ and all $s \in [0,t]$, $|\bar{\Theta}_\xi(s,\zeta_p)| = |\bar{\Theta}_\xi(s,t)|$ and $t-\zeta_p+|\bar{\Xi}_\xi(s,\zeta_p)| = |\bar{\Xi}_\xi(s,t)|$, we have that $e^{\omega_2(t-\zeta_p)}\Upsilon(s,\zeta_p) = \Upsilon(s,t)$ for all $t \in Z_p$ and all $s \in [0,t]$. Substitution of the latter in (58) yields that for all $(t,j) \in (Z_p \times \mathbb{N}) \cap \operatorname{dom} \xi$,

$$U(\xi(t,j)) \leqslant \Upsilon(0,t)U(\xi(0,0)) + \theta^2 \int_0^{\zeta_p} \Upsilon(s,t)|w(s)|^2 ds + \theta^2 \int_{\zeta_p}^{t} e^{\omega_2(t-s)}|w(s)|^2 ds. \quad (59)$$

Note that for all $t \in Z_p$ and $s \in [\zeta_p, t]$, $t-s = |\bar{\Xi}_\xi(s,t)|$ and in accordance with (51), $|\bar{\Theta}_\xi(s,t)| = 0$ and thus $e^{\omega_2(t-s)} = \Upsilon(s,t)$ for all $t \in Z_p$ and $s \in [\zeta_p, t]$. By combining the latter with (59), we can see that (57) holds for all $(t,j) \in ([0,\zeta_p + v_p) \times \mathbb{N}) \cap \operatorname{dom} \xi$, $p \in \mathbb{N}$.

Now we consider the interval W_p. Using (55), we have that for all $(t,j) \in (W_p \times \mathbb{N}) \cap \operatorname{dom} \xi$,

$$U(\xi(t,j)) \leqslant e^{-\omega_1(t-\zeta_p-v_p)}\Upsilon(0,\zeta_p+v_p)U(\xi(0,0)) + \theta^2 e^{-\omega_1(t-\zeta_p-v_p)} \int_0^{\zeta_p+v_p} \Upsilon(s,\zeta_p+v_p)|w(s)|^2 ds + \theta^2 \int_{\zeta_p+v_p}^{t} e^{-\omega_1(t-s)}|w(s)|^2 ds. \quad (60)$$

Since $t-\zeta_p-v_p+|\bar{\Theta}_\xi(s,\zeta_p+v_p)| = |\bar{\Theta}_\xi(s,t)|$ and $|\bar{\Xi}_\xi(s,\zeta_p+v_p)| = |\bar{\Xi}_\xi(s,t)|$ for all $t \in W_p$ and all $s \in [0,t]$, we obtain

$$e^{-\omega_1(t-\zeta_p)}\Upsilon(s,\zeta_p) = \Upsilon(s,t) \quad (61)$$

for all $t \in W_p$ and all $s \in [0,t]$. Substitution of (61) in (60) yields that for all $(t,j) \in (W_p \times \mathbb{N}) \cap \operatorname{dom} \xi$,

$$U(\xi(t,j)) \leqslant \Upsilon(0,t)U(\xi(0,0)) + \theta^p \int_0^{\zeta_p} \Upsilon(s,t)|w(s)|^2 ds + \theta^p \int_{\zeta_p}^{t} e^{-\omega_1(t-s)}|w(s)|^2 ds. \quad (62)$$

Combining (61) with the fact that for all $t \in W_p$ and $s \in [\zeta_p + v_p, t]$, $t-s = |\bar{\Theta}_\xi(s,t)|$ and in accordance with (50), $|\bar{\Xi}_\xi(s,t)| = 0$, we can see that $e^{-\omega_1(t-s)} = \Upsilon(s,t)$ for all $t \in W_p$ and $s \in [\zeta_p + v_p, t]$. By means of the latter, we can conclude that (57) coincides with (62) and thus (57) holds for all $(t,j) \in ([0,\zeta_{p+1}) \times \mathbb{N}) \cap \operatorname{dom} \xi$, which concludes the proof of Lemma 4. □

Step IV. *Stability and performance analysis.* In the last step of the proof, we show that under $(\nu, \tau_D, \varsigma, T)$-DoS sequences with τ_D and T satisfying (31), the system $\mathcal{H}_\mathcal{T}$ is UGES, and has a finite *induced* $\mathcal{L}_\infty$*-gain*. By means of (54) and the fact that $|\bar{\Theta}_\xi(T_1,T_2)| = T_2 - T_1 - |\bar{\Xi}_\xi(T_1,T_2)|$, we obtain that

$$\Upsilon(T_1,T_2) \leqslant \kappa e^{-\beta_*(T_2-T_1)}, \quad (63)$$

for all $T_2 \in \mathbb{R}_{\geqslant 0}$ and all $T_1 \in \left[\left(\bigcup_{k\in\mathbb{N}} W_{k-1}\right) \cup \{0\}\right] \cap [0,T_2]$, where $\kappa := e^{\varsigma_*(\omega_1+\omega_2)}$ and where $\beta_* := \omega_1 - (\omega_1+\omega_2)/T_*$. Important to note is that condition (31) assures that $\beta_* > 0$.

The inequality given in (63) does not only hold for $T_1 \in \left[\left(\bigcup_{k\in\mathbb{N}} W_{k-1}\right) \cup \{0\}\right] \cap [0,T_2]$. In fact, the inequality holds for all $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_1 \leqslant T_2$ due to the following. Let $0 \leqslant T_1 \leqslant T_2$ be arbitrary and consider $T_1^* = \sup\left\{\tilde{T} \leqslant T_1 \mid \tilde{T} \in \left(\bigcup_{k\in\mathbb{N}} W_k\right) \cup \{0\}\right\}$. Since $|\Theta(T_1^*, T_1)| = 0$, we can write $\Upsilon(T_1^*, T_2) = \Upsilon(T_1,T_2)e^{\omega_2(T_1-T_1^*)}$ for all $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_1 \leqslant T_2$. Hence, we have that $\Upsilon(T_1,T_2) \leqslant \Upsilon(T_1^*,T_2)$. Due to (63) and the facts that $\beta^* > 0$ and $T_1^* \in \left[\left(\bigcup_{k\in\mathbb{N}} W_k\right) \cup \{0\}\right] \cap [0,T_2]$, we have that $\Upsilon(T_1^*,T_2) \leqslant \kappa e^{-\beta_*(T_2-T_1^*)} \leqslant \kappa e^{-\beta_*(T_2-T_1)}$. for all $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_1 \leqslant T_2$. Hence, (63) holds for all $T_1, T_2 \in \mathbb{R}_{\geqslant 0}$ with $T_1 \leqslant T_2$.

1) Stability analysis for the case $w = 0$. By combining (63) and (57) for the case $w = 0$, we find that for all $(t,j) \in \operatorname{dom} \xi$

$$U(\xi(t,j)) \leqslant \kappa e^{-\beta_* t}U(\xi(0,0)).$$

Using (23), (25), (40) and the fact that $\eta(0,0) = 0$, we obtain

$$|\xi(t,j)|_\mathcal{A} \leqslant \sqrt{\frac{\kappa \max(\bar{c}_V, \tilde{c}_W)}{\underline{c}_U}} e^{-(\beta_*/2)t}|\xi(0,0)|_\mathcal{A},$$

where $\tilde{c}_W := \gamma\phi_{miet}\bar{c}_W^2$. Given the fact that due to (31) $\beta_* > 0$, we can conclude that $\mathcal{H}_\mathcal{T}$ is UGES under $(\nu, \tau_D, \varsigma, T)$-DoS sequences.

2) Performance analysis for the case $w \neq 0$ in terms of induced $\mathcal{L}_\infty$-gain. Substitution of (63) in (57) yields

$$U(\xi(t,j)) \leqslant \kappa U(\xi(0,0)) + \kappa\theta^2 \int_0^t e^{-\beta_*(t-s)} ds \|w\|_{\mathcal{L}_\infty}^2.$$

The facts that $U(\xi(t,j)) \geqslant V(x(t,j)) \geqslant c_z|z(t,j)|^2$ and $U(\xi(0,0)) \leqslant \max(\bar{c}_V, \tilde{c}_W)\,|\xi(0,0)|_\mathcal{A}^2$, we now obtain that for all $(t,j) \in \operatorname{dom} \xi$

$$\|z\|_{\mathcal{L}_\infty} \leqslant \sqrt{\frac{\kappa}{c_z}\max(\bar{c}_V, \tilde{c}_W)}|\xi(0,0)|_\mathcal{A} + \theta\sqrt{\frac{\kappa}{c_z\beta^*}}\|w\|_{\mathcal{L}_\infty}.$$

Hence, (22) is satisfied with $\beta(r) = \sqrt{\frac{\kappa}{c_z}\max(\bar{c}_V, \tilde{c}_W)}r$ and $\vartheta = \theta\sqrt{\frac{\kappa}{c_z\beta^*}}$ for $p = \infty$ which completes the proof. □

REFERENCES

[1] V. S. Dolk, P. Tesi, C. D. Persis, and W. P. M. H. Heemels, "Output-based event-triggered control systems under denial-of-service attacks," in *2015 54th IEEE Conf. on Decision and Control (CDC)*, Dec 2015, pp. 4824–4829.

[2] H. Sandberg, S. Amin, and K. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, Feb 2015.

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

[4] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

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

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

[7] H. S. Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated DoS jamming attacks," *SIAM Journal on Control and Optimization*, 2013, submitted, Revised 2016.

[8] 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*, July 2011, pp. 1–6.

[9] D. Borgers and W. Heemels, "Event-separation properties of event-triggered control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 10, pp. 2644–2656, Oct 2014.

[10] M. Donkers and W. Heemels, "Output-based event-triggered control with guaranteed $\mathcal{L}_\infty$-gain and improved and decentralized event-triggering," *IEEE Trans. Autom. Control*, vol. 57, no. 6, pp. 1362–1376, June 2012.

[11] J. Hespanha and A. Morse, "Stability of switched systems with average dwell-time," in *Proc. 38th IEEE Conf. Decision and Control*, vol. 3, 1999, pp. 2655–2660 vol.3.

[12] V. Dolk, D. Borgers, and W. Heemels, "Dynamic event-triggered control: Tradeoffs between transmission intervals and performance," in *Proc. 53rd IEEE Conf. Decision and Control (CDC)*, Dec 2014, pp. 2764–2769.

[13] V. S. Dolk, D. P. Borgers, and W. P. M. H. Heemels, "Output-based and decentralized dynamic event-triggered control with guaranteed lp-gain performance and zeno-freeness," *IEEE Transactions on Automatic Control*, 2016, accepted for publication, DOI: 10.1109/TAC.2016.2536707.

[14] D. Borgers and W. Heemels, "Stability analysis of large-scale networked control systems with local networks: A hybrid small-gain approach," in *Hybrid Systems: Computation and Control (HSCC) 2014, Berlin, Germany*, April 2014.

[15] K. Åström and B. Bernhardsson, "Comparison of periodic and event based sampling for first-order stochastic systems," vol. 11, 1999, pp. 301–306.

[16] K.-E. Årzén, "A simple event-based PID controller," in *Proceedings of the 14th IFAC World congress*, Beijing, P.R. China, Jan. 1999.

[17] T. Henningsson, E. Johannesson, and A. Cervin, "Sporadic event-based control of first-order linear stochastic systems," *Automatica*, vol. 44, no. 11, pp. 2890 – 2895, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0005109808002550

[18] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1680–1685, September 2007.

[19] W. Heemels, K. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proc. 51th IEEE Conf. Decision and Control*, Dec 2012, pp. 3270–3285.

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

[21] 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.

[22] 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.

[23] X. Wang and M. D. Lemmon, "Event design in event-triggered feedback control systems," in *Decision and Control, 2008. CDC 2008. 47th IEEE Conference on*, Dec 2008, pp. 2105–2110.

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

[25] D. Carnevale, A. Teel, and D. Nešić, "A Lyapunov proof of an improved maximum allowable transfer interval for networked control systems," *IEEE Trans. Autom. Control*, vol. 52, no. 5, pp. 892–897, May 2007.

[26] W. Heemels, A. 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*, pp. 1781–1796, 2010.

[27] J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Lp string stability of cascaded systems: Application to vehicle platooning," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 2, pp. 786–793, March 2014.

V.S. Dolk received the M.Sc. degree (cum laude) in mechanical engineering from the Eindhoven University of Technology (TU/e), Eindhoven, the Netherlands, in 2013 where he is currently pursuing the Ph.D. degree.

His research interests include hybrid dynamical systems, networked control systems, intelligent transport systems and event-triggered control.

P. Tesi received the Laurea degree and the Ph.D. degree in Computer & Control Engineering, both from the University of Florence, Italy, in 2005 and 2010, respectively. During his PhD he has been a visiting scholar at the University of California, Santa Barbara, CA, USA. Thereafter, he held a postdoctoral position at the University of Genoa, Italy. Dr. Tesi also worked in the automation industry on research and development of networked SCADA systems. He is currently an Assistant Professor at the Faculty of Mathematics and Natural Sciences, University of Groningen, The Netherlands, Since 2014, he is an Associate Editor of the IEEE Control Systems Society Conference Editorial Board. His main research interests include adaptive control, hybrid systems, networked control and adaptive optics.

C. De Persis received the Laurea degree (cum laude) in electrical engineering in 1996 and the Ph.D. degree in system engineering in 2000, both from Sapienza University of Rome, Rome, Italy. He is currently a Professor at the Engineering and Technology Institute, Faculty of Mathematics and Natural Sciences, University of Groningen, the Netherlands. He is also affiliated with the Jan Willems Center for Systems and Control. Previously he was with the Department of Mechanical Automation and Mechatronics, University of Twente and with the Department of Computer, Control, and Management Engineering, Sapienza University of Rome. He was a Research Associate at the Department of Systems Science and Mathematics, Washington University, St. Louis, MO, USA, in 2000-2001, and at the Department of Electrical Engineering, Yale University, New Haven, CT, USA, in 2001-2002. His main research interest is in control theory, and his recent research focuses on dynamical networks, cyberphysical systems, smart grids and resilient control. He was an Editor of the *International Journal of Robust and Nonlinear Control* (2006-2013), an Associate Editor of the *IEEE Control Systems Technology* (2010-2015) and of the *IEEE Transactions on Automatic Control* (2012-2015), and is currently an Associate Editor of Automatica (2013-present).

W.P.M.H. Heemels received the M.Sc. degree in mathematics and the Ph.D. degree in control theory (both summa cum laude) from the Eindhoven University of Technology (TU/e), the Netherlands, in 1995 and 1999, respectively. From 2000 to 2004, he was with the Electrical Engineering Department, TU/e and from 2004 to 2006 with the Embedded Systems Institute (ESI). Since 2006, he has been with the Department of Mechanical Engineering, TU/e, where he is currently a Full Professor. He held visiting professor positions at the Swiss Federal Institute of Technology (ETH), Switzerland (2001) and at the University of California at Santa Barbara (2008). In 2004, he worked also at the company Océ, the Netherlands. His current research interests include hybrid and cyber-physical systems, networked and event-triggered control systems and constrained systems including model predictive control. Dr. Heemels served/s on the editorial boards of *Automatica*, *Nonlinear Analysis: Hybrid Systems*, *Annual Reviews in Control*, and *IEEE Transactions on Automatic Control*. He was a recipient of a personal VICI grant awarded by STW (Dutch Technology Foundation). He is a Fellow of the IEEE.