University of Groningen

A comparison among deterministic packet-dropouts models in networked control systems

De Persis, Claudio; Tesi, Pietro

Published in:
IEEE Control Systems Letters

DOI:
[10.1109/LCSYS.2017.2759423](https://doi.org/10.1109/LCSYS.2017.2759423)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2017

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

De Persis, C., & Tesi, P. (2017). A comparison among deterministic packet-dropouts models in networked control systems. *IEEE Control Systems Letters*, 2(1), 109-114.
<https://doi.org/10.1109/LCSYS.2017.2759423>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

A Comparison Among Deterministic Packet-Dropouts Models in Networked Control Systems

Claudio De Persis¹ and Pietro Tesi²

Abstract—Several papers have studied networked control systems in the presence of packet dropouts. One can distinguish between deterministic and stochastic packet-dropout models, the former being particularly suited when packet dropouts are of a malicious nature. This letter aims at linking and comparing a number of deterministic packet-dropout models.

Index Terms—Networked control systems, nonlinear control systems, packet loss.

I. INTRODUCTION

SEVERAL papers have studied networked control systems in the presence of packet dropouts. One can distinguish between deterministic and stochastic packet dropouts models. While the latter has been thoroughly investigated in the realm of networked control systems, the former is gaining attention especially in connection with security issues. In fact, it is recognized that communication failures induced by malicious attacks can have a temporal profile quite different from the one exhibited by genuine packet losses, as assumed in the majority of studies on networked control. In particular, communication failures induced by malicious attacks need not follow a given class of probability distributions [1].

The aim of this letter is to link and compare a number of deterministic packet-dropout models. We will also discuss implications of the results and connect the results with the framework of asynchronous dynamical systems [2].

Notation: We denote by $\mathbb{R}$ the set of reals. Given $\alpha \in \mathbb{R}$, we let $\mathbb{R}_{>\alpha}$ ($\mathbb{R}_{\geq\alpha}$) denote the set of reals greater than (greater than or equal to) α . We let $\mathbb{N} := \{0, 1, 2, \dots\}$ denote the set of natural numbers. Given $\alpha \in \mathbb{N}$, $\mathbb{N}_{>\alpha}$ ($\mathbb{N}_{\geq\alpha}$) denotes the set of integers greater than (greater than or equal to) α . Given an interval $\mathcal{I}$, $|\mathcal{I}|$ denotes its length, and given a set $S = \cup_k \mathcal{I}_k$ consisting of a countable union of intervals $\mathcal{I}_k$, $|S|$ denotes its Lebesgue measure.

Manuscript received June 20, 2017; revised September 1, 2017; accepted September 25, 2017. Date of publication October 4, 2017; date of current version October 17, 2017. Recommended by Senior Editor C. Seatzu. (Corresponding author: Pietro Tesi.)

C. De Persis is with the ENTEG, University of Groningen, 9747 Groningen, The Netherlands (e-mail: c.de.persis@rug.nl).

P. Tesi is with the ENTEG, University of Groningen, 9747 Groningen, The Netherlands, and also with the DINFO, Università di Firenze, 50139 Firenze, Italy (e-mail: pietro.tesi@unifi.it).

Digital Object Identifier 10.1109/LCSYS.2017.2759423

II. DETERMINISTIC PACKET-DROPOUTS MODELS

We consider a networked system in which two units exchange data through a digital communication medium. This scenario can be representative of a centralized setting in which a process and a controller communicate via digital sensing and/or control channels, or a distributed setting where network units cooperate to achieve a common task, as occurs, for instance, in sensor fusion. We will assume that transmissions occur at a fixed rate. Let $\{t_k\}_{k \in \mathbb{N}}$, $t_0 := 0$, be the sequence of transmission attempts. Then,

$$t_{k+1} - t_k = \Delta \quad (1)$$

for every $k \in \mathbb{N}$, where $\Delta \in \mathbb{R}_{>0}$. Given Δ , the sequence of unsuccessful transmissions is also referred to as *pattern* of packet dropouts.

A classic deterministic model defines worst-case bounds on the maximum number of consecutive dropouts [3]–[7].

Model 1: The number of consecutive packet dropouts does not exceed N for some constant $N \in \mathbb{N}$.

Next, we consider a model which is related to the framework of asynchronous dynamical system [2]. We will discuss such connections later in Section V.

Model 2: For every $k \in \mathbb{N}$, let $\theta_k = 0$ when there is a packet dropout at time t_k and $\theta_k = 1$ otherwise. There exist constants $c \in \mathbb{R}_{\geq 0}$ and $\lambda \in \mathbb{R}_{>1}$ such that

$$\sum_{k=k_0}^{k_1} (1 - \theta_k) \leq c + \frac{k_1 - k_0}{\lambda} \quad (2)$$

for every $k_0, k_1 \in \mathbb{N}$ with $k_1 \geq k_0$.

Recently in [8], a different modelling framework has been considered, still of a deterministic type. Instead of looking at the behavior of dropouts, this approach aims at modelling the “source” of dropouts, for example a jamming signal that destroys the network availability [9], [10]. In the sequel, we will use the general term Denial-of-Service (DoS) signal to indicate the source of dropouts.

Let $\{h_n\}_{n \in \mathbb{N}}$ with $h_0 \in \mathbb{R}_{\geq 0}$ denote the sequence of DoS *off/on* transitions, that is the times at which the DoS signal changes from zero (transmissions are allowed) to one (transmissions are denied). Thus $H_n := \{h_n\} \cup [h_n, h_n + \tau_n[$ represents the n -th DoS time-interval of a length $\tau_n \in \mathbb{R}_{\geq 0}$, where $h_n + \tau_n$ is the n -th *on/off* transition of the DoS signal. Given $\tau, t \in \mathbb{R}_{\geq 0}$

with $t \geq \tau$, let $n(\tau, t)$ be the number of DoS *off/on* transitions over $[\tau, t]$, and let

$$\Xi(\tau, t) := \bigcup_{n \in \mathbb{N}} H_n \cap [\tau, t] \quad (3)$$

be the subset of $[\tau, t]$ where transmissions are denied.

The following model of DoS signals is introduced.

Model 3: There exist constants $\eta \in \mathbb{R}_{\geq 0}$, $\kappa \in \mathbb{R}_{\geq 0}$, $\tau_f \in \mathbb{R}_{>0}$ and $\tau_d \in \mathbb{R}_{>1}$ such that

$$n(\tau, t) \leq \eta + \frac{t - \tau}{\tau_f} \quad (4)$$

and

$$|\Xi(\tau, t)| \leq \kappa + \frac{t - \tau}{\tau_d} \quad (5)$$

for all $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$.

Thus, given a DoS signal $\mathcal{S}$ and a sampling time Δ , the *pattern* of dropouts resulting from $\mathcal{S}$ and Δ is the sequence of transmission attempts that belong to some interval of $\mathcal{S}$.

Both Models 2 and 3 constrain the number of dropouts in an “average” sense. Following [11], the parameter λ in Model 2 can be defined as the average dwell-time between consecutive packet dropouts, while c is the chattering bound. Condition $\lambda \in \mathbb{R}_{>1}$ guarantees that successful transmissions exist. Similarly, Model 3 constrains a DoS signal in terms of its average frequency and duration. The parameter τ_f represents the average dwell-time between consecutive DoS *off/on* transitions, while η is the chattering bound. Condition (5) expresses a similar requirement with respect to the duration of a DoS signal. Conditions $\tau_f \in \mathbb{R}_{>0}$ and $\tau_d \in \mathbb{R}_{>1}$ imply that a DoS signal cannot occur at an infinitely fast rate or be always active.

III. A COMPARISON AMONG DETERMINISTIC PACKET-DROPOUTS MODELS

A. A Comparison Between Models 1 and 2

Theorem 1: Consider a transmission policy as in (1). A packet-dropout pattern satisfying Model 2 satisfies Model 1 with $N = W$, where

$$W := \left\lceil \left(c - \frac{1}{\lambda} \right) \frac{\lambda}{\lambda - 1} \right\rceil. \quad (6)$$

Proof: The worst-case number $w(k_0, k_1)$ of dropouts that can occur on $[t_{k_0}, t_{k_1}]$ is $k_1 - k_0 + 1$. By Model 2, we then have $k_1 - k_0 + 1 \leq c + (k_1 - k_0)/\lambda$, which implies

$$\begin{aligned} w(k_0, k_1) &= k_1 - k_0 + 1 \\ &\leq \left\lceil \left(c - \frac{1}{\lambda} \right) \frac{\lambda}{\lambda - 1} \right\rceil \end{aligned} \quad (7)$$

where the inequality follows because $w(k_0, k_1)$ is an integer. This yields the result since t_{k_0} and t_{k_1} are arbitrary. ■

Remark 1: Notice that $W \geq 1$ if and only if $c \geq 1$. In fact, it is easy to see that in Model 2 there are no packet dropouts if $c < 1$.

Theorem 2: Consider a transmission policy as in (1). A packet-dropout pattern satisfying Model 1 satisfies Model 2 with

$$(c, \lambda) = \left(\frac{2N}{N+1}, \frac{N+1}{N} \right). \quad (8)$$

Proof: By Model 1, at most N transmissions can fail every $N+1$ consecutive transmission attempts. Thus, every $k \in \mathbb{N}$ transmission attempts there are not more than $k - \left\lfloor \frac{k}{N+1} \right\rfloor$ packet dropouts. Since

$$\left\lfloor \frac{k}{N+1} \right\rfloor \geq \frac{k}{N+1} - \frac{N}{N+1} \quad (9)$$

then

$$\begin{aligned} \sum_{k=k_0}^{k_1} (1 - \theta_k) &\leq k_1 - k_0 + 1 - \left(\frac{k_1 - k_0 + 1}{N+1} - \frac{N}{N+1} \right) \\ &= (k_1 - k_0) \frac{N}{N+1} + \frac{2N}{N+1} \end{aligned} \quad (10)$$

which is the thesis. ■

Remark 2: A model very similar to Model 1 is considered in [12]. There, one assumes that on every interval containing P communication attempts at most $R < P$ attempts can fail. Clearly this model satisfies Model 1 with $N = R$. Conversely, a packet-dropout pattern satisfying Model 1 does also satisfy this model with $R = N$ and $P = N+1$.

B. A Comparison Between Models 2 and 3

In order to link Models 2 and 3, we will avail ourselves of a technical lemma, which establishes a suitable notion of equivalence between DoS signals.

Definition 1: Given a sampling time Δ , two DoS signals are said to be “packet-dropout equivalent” (PE) if they generate exactly the same pattern of packet dropouts.

Lemma 1: Consider a transmission policy as in (1), along with a DoS signal $\mathcal{S}$ satisfying Model 3 with parameters $(\kappa, \tau_d, \eta, \tau_f)$. Then, there exists a DoS signal $\bar{\mathcal{S}}$ satisfying Model 3 and such that $\mathcal{S}$ and $\bar{\mathcal{S}}$ are PE. In particular, $\bar{\mathcal{S}}$ has parameters

$$(\bar{\kappa}, \bar{\tau}_d, \bar{\eta}, \bar{\tau}_f) = \left(0, \infty, \frac{\kappa}{\Delta} + \eta + T, \frac{\Delta}{T} \right) \quad (11)$$

where

$$T := \frac{1}{\tau_d} + \frac{\Delta}{\tau_f} \quad (12)$$

Proof: See the Appendix. ■

Building on $\bar{\mathcal{S}}$, one can actually construct infinitely many PE signals by adding to $\bar{\mathcal{S}}$ DoS intervals which do not interfere at all with the transmissions. The form of $\bar{\mathcal{S}}$ is particularly useful since $\bar{\mathcal{S}}$ takes the form of a train of pulses due to $(\bar{\kappa}, \bar{\tau}_d) = (0, \infty)$. In this way, one eliminates the portions of DoS that do not interfere with the transmissions and one can bound the frequency of dropouts directly in terms of the DoS frequency.

Using Lemma 1, we prove a first implication.

Theorem 3: Consider a transmission policy as in (1), along with a DoS signal that satisfies Model 3 with $T < 1$. Then, the resulting packet-dropouts pattern satisfies Model 2 with

$$(c, \lambda) = \left(\frac{\kappa}{\Delta} + \eta + T, \frac{1}{T} \right) \quad (13)$$

Proof: Consider a DoS signal $\mathcal{S}$ satisfying Model 3 with parameters $(\kappa, \tau_d, \eta, \tau_f)$. In view of Lemma 1, a PE signal $\bar{\mathcal{S}}$

has parameters as in (11). Let $\bar{n}(\tau, t)$ denote the number of *off/on* transitions of $\mathcal{S}$ over $[\tau, t]$. Hence,

$$\begin{aligned} \sum_{k=k_0}^{k_1} (1 - \theta_k) &= \bar{n}(t_{k_0}, t_{k_1}) \\ &\leq \frac{\kappa}{\Delta} + \eta + T + \frac{T}{\Delta} (t_{k_1} - t_{k_0}) \end{aligned} \quad (14)$$

The thesis follows since $t_{k_1} - t_{k_0} = (k_1 - k_0)\Delta$. ■

We now focus on the converse implication.

Theorem 4: Consider a transmission policy as in (1), along with a packet-dropout pattern $\mathcal{P}$ satisfying Model 2. Then, there exist infinitely many PE DoS signals satisfying Model 3 with $T < 1$, which generate the pattern $\mathcal{P}$. One of them has parameters

$$(\kappa, \tau_d, \eta, \tau_f) = (0, \infty, c, \lambda\Delta) \quad (15)$$

Proof: Consider a packet-dropout pattern $\mathcal{P}$, and let $\{\ell_n\}_{n \in \mathbb{N}}$ denote the corresponding sequence of unsuccessful transmissions. One can model $\mathcal{P}$ as the result of a DoS signal with $(h_n, \tau_n) := (\ell_n, 0)$. Thus (5) holds with $\kappa = 0$ and $\tau_d = \infty$. As for $n(\tau, t)$ notice that, by construction, $n(\tau, t)$ equals the number of dropouts occurring on $[\tau, t]$. In particular, $n(\tau, t) = 0$ whenever $[\tau, t]$ does not contain any dropout, while $n(\tau, t) = n(t_{k_0}, t_{k_1})$ where $k_0 := \min\{k : t_k \geq \tau\}$ and $k_1 := \max\{k : t_k \leq t\}$ otherwise. Hence,

$$n(\tau, t) = \sum_{k=k_0}^{k_1} (1 - \theta_k) \quad (16)$$

In view Model 2 we have

$$n(\tau, t) \leq c + \frac{k_1 - k_0}{\lambda} \quad (17)$$

Since $k_1 - k_0 = (t_{k_1} - t_{k_0})/\Delta \leq (t - \tau)/\Delta$ then (4) holds true with $\eta = c$ and $\tau_f = \lambda\Delta$. Building on $\mathcal{S}$, infinitely many PE signals can be constructed by adding to $\mathcal{S}$ DoS intervals which do not interfere with the transmission instants. ■

Remark 3: As discussed in Remark 1, there are no packet dropouts when $c < 1$. In this case, we have $\eta < 1$. It is immediate to see that this condition indeed implies no packet dropouts in Model 3 since the existence of a packet dropout requires the existence of a DoS *off/on* transition at a certain time t which implies $n(t, t) = 1 \leq \eta$.

Theorems 3 and 4 rely on condition $T < 1$. In this respect, note that in Model 2 condition $\lambda > 1$ is needed to ensure that successful transmissions exist. As next lemma shows, condition $T < 1$ plays exactly the same role with respect to Model 3.

Lemma 2: Consider a transmission policy as in (1), and let $\mathcal{D}(\tau_f, \tau_d)$ denote the class of all the DoS signals satisfying Model 3 with $T \geq 1$. Then, $\mathcal{D}(\tau_f, \tau_d)$ contains infinitely many signals that destroy every transmission.

Proof: Let $\tau_d = p/q$ where $p, q \in \mathbb{N}$ with $p > q$, and let $\tau_f = (p\Delta)/(p - q)$. Clearly $T = 1$. Decompose $\mathbb{R}_{\geq 0}$ as

$$\mathbb{R}_{\geq 0} = \bigcup_{k \in \mathbb{N}} [kp\Delta, (k+1)p\Delta[\quad (18)$$

and consider a DoS signal which for each $k \in \mathbb{N}$ behaves as follows: (i) it remains active over $[kp\Delta, kp\Delta + q\Delta]$; and (ii) it remains idle till $(k+1)p\Delta$ except for $p - q - 1$ pulses at times $kp\Delta + (q+1)\Delta, kp\Delta + (q+2)\Delta, \dots, kp\Delta + (p-1)\Delta$. By construction, this signal disrupts every transmission. Such signals are infinitely many as p and q are arbitrary. It is an easy matter to see that the considered DoS signal does indeed satisfy Model 3 with the given (τ_f, τ_d) and with $\eta = p - q$ and $\kappa = q\Delta$. ■

As shown next, condition $T < 1$ also suffices to ensure that the maximum number of consecutive packet dropouts is uniformly bounded.

C. A Comparison Between Models 1 and 3

Theorem 5: Consider a transmission policy as in (1), along with a DoS signal satisfying Model 3. If $T < 1$ then the resulting packet-dropouts pattern satisfies Model 1 with $N = S$, where

$$S := \left\lfloor \left(\frac{\kappa}{\Delta} + \eta \right) \frac{1}{1 - T} \right\rfloor \quad (19)$$

Proof: By Theorem 3, the resulting packet-dropout pattern satisfies Model 2 with $c = \kappa/\Delta + \eta + T$ and $\lambda = 1/T$. Hence, the thesis follows from Theorem 1. ■

Theorem 6: Consider a transmission policy as in (1), along with a packet-dropouts pattern $\mathcal{P}$ satisfying Model 1. Then, there exist infinitely many PE DoS signals satisfying Model 3 with $T < 1$, which generate the pattern $\mathcal{P}$. One of them has parameters

$$(\kappa, \tau_d, \eta, \tau_f) = \left(0, \infty, \frac{2N}{N+1}, \frac{\Delta(N+1)}{N} \right) \quad (20)$$

Proof: By Theorem 2, the packet-dropout pattern satisfies Model 2 with $c = 2N/(N+1)$ and $\lambda = (N+1)/N$. Hence, the thesis follows from Theorem 4. ■

IV. APPLICATIONS TO NETWORKED CONTROL

One of the main implications of the foregoing analysis is the possibility to reformulate stability properties for a given packet-dropout model in terms of the other models.

A. Stability of Networked Control Systems

Consider a dynamical system of the form

$$\dot{x} = f(x, u), \quad y = h(x, u) \quad (21)$$

where $x \in \mathbb{R}^n$ is the state with initial condition $x(t_0) = x_0$; $u \in \mathbb{R}^m$ is the process input, and $y \in \mathbb{R}^p$ is the process output. The process-controller communication is networked which means that the control system can only receive process data and send control updates at discrete-times t_k with $t_{k+1} = t_k + \Delta$ for every $k \in \mathbb{N}$ where $\Delta \in \mathbb{R}_{>0}$. The control action is implemented in a classic *sample-and-hold* fashion. Let $\{z_m\}_{m \in \mathbb{N}}$ denote the sequence of successful transmissions. The controller has dynamics

$$\dot{\xi} = g(\xi, \bar{y}), \quad u = l(\xi, \bar{y}) \quad (22)$$

where, given a signal s ,

$$\bar{s}(t) = \begin{cases} 0, & t < z_0 \\ s(z_m), & t \in [z_m, z_{m+1}) \end{cases} \quad (23)$$

Here, $\xi \in \mathbb{R}^q$ is the state with initial condition $\xi(t_0) = \xi_0$; $\bar{y} \in \mathbb{R}^p$ is the controller input, and $u \in \mathbb{R}^m$ is the controller output. In words, in the nominal situation in which there are no dropouts, the control signal u is given by $l(\xi(z_m), y(z_m))$ for all $t \in [z_m, z_{m+1})$. When a transmission failure occurs the actuator keeps the last received control value.

Hereafter, stability is meant in a Lyapunov sense.

Theorem 7: Consider a control system as in (21) and (22). Assume that (x_0, ξ_0, Δ) are such that an equilibrium of the control system is (asymptotically) stable for every packet-dropout pattern that satisfies Model 1 with $N \leq N_* \in \mathbb{N}$. Then, the equilibrium remains (asymptotically) stable for every packet-dropout pattern that satisfies Model 2 with (c, λ) such that $W \leq N_*$ where W is as in (6), and every DoS signal satisfying Model 3 with $(\kappa, \tau_d, \eta, \tau_f)$ such that $T < 1$ and $S \leq N_*$ where S is as in (19).

Proof: Consider Model 2 and suppose that the claim is not true. Then, there exists a packet-dropout pattern that causes instability with (c, λ) such that $W \leq N_*$. However, in view of Theorem 1 this pattern can generate at most $N = W$ consecutive dropouts, which leads to a contradiction since the system is (asymptotically) stable for every $N \leq N_*$. As for Model 3, the result can be shown in an analogous way using Theorem 5. ■

Theorem 8: Consider a control system as in (21) and (22). Assume that (x_0, ξ_0, Δ) are such that an equilibrium of the control system is (asymptotically) stable for every packet-dropout pattern that satisfies Model 2 with $\lambda \geq \lambda_* \in \mathbb{R}_{>1}$ and $c \leq c_* \in \mathbb{R}_{\geq 0}$. Then, the equilibrium of the control system remains (asymptotically) stable for every packet-dropout pattern that satisfies Model 1 with N such that

$$\begin{cases} \frac{2N}{N+1} \leq c_* \\ N \leq \left\lfloor \frac{1}{\lambda_* - 1} \right\rfloor \end{cases} \quad (24)$$

and every DoS signal satisfying Model 3 with $(\kappa, \tau_d, \eta, \tau_f)$ such that $k/\Delta + \eta + T \leq c_*$ and $T \leq 1/\lambda_*$.

Proof: Consider Model 1 and suppose that the claim is not true. Then, there exists a packet-dropout pattern that causes instability with N satisfying (24). However, by Theorem 2 this pattern satisfies Model 2 with $c = 2N/(N+1)$ and $\lambda = (N+1)/N$. Since the system is (asymptotically) stable whenever $\lambda \geq \lambda_*$ and $c \leq c_*$ we must have either $2N/(N+1) > c_*$ or $N > 1/(\lambda_* - 1)$, which contradicts (24). This leads to a contradiction. As for Model 3, the result can be shown in an analogous way using Theorem 3. ■

Theorem 9: Consider a control system as in (21) and (22). Assume that (x_0, ξ_0, Δ) are such that an equilibrium of the control system is (asymptotically) stable for every DoS signal that satisfies Model 3 with $(\kappa, \tau_d, \eta, \tau_f)$ such that $T \leq T_* \in \mathbb{R}_{\geq 0}$ with $T_* < 1$ and $(\kappa, \eta) \leq (\kappa_*, \eta_*)$, where $\kappa_*, \eta_* \in \mathbb{R}_{\geq 0}$. Then, the equilibrium of the control system remains (asymptotically) stable for every packet-dropout pattern

satisfying Model 1 with

$$\begin{cases} \frac{2N}{N+1} \leq \eta_* \\ N \leq \left\lfloor \frac{T_*}{1-T_*} \right\rfloor \end{cases} \quad (25)$$

and every packet-dropout pattern satisfying Model 2 with (c, λ) such that $c \leq \eta_*$ and $\lambda \geq 1/T_*$.

Proof: Consider Model 1, and suppose that the claim is not true. Then, there exists a pattern $\mathcal{P}$ which induces instability with N satisfying (25). By Theorem 6, $\mathcal{P}$ can be thought of as generated by a DoS signal with parameters $\kappa = 0$, $\tau_d = \infty$, $\eta = 2N/(N+1)$ and $\tau_f = \Delta(N+1)/N$. Since condition $\kappa \leq \kappa_*$ trivially holds, we must have either $\eta = 2N/(N+1) > \eta_*$ or $T = N/(N+1) > T_*$. This leads to a contradiction. As for Model 2, the result can be shown in an analogous way using Theorem 4. ■

Remark 4: In Theorem 9, the constraints for Models 1 and 2 do not depend on κ_* . This comes from modeling a DoS signal via a PE signal consisting in a train of pulses, as done in Theorems 4 and 6.

It is interesting to observe that the first constraint in (24) and (25) becomes inactive when $c_* \geq 2$ and $\eta_* \geq 2$. This situation happens whenever stability is not compromised by long but sporadic sequences of dropouts. In this case, proving (asymptotic) stability for Models 2 and/or 3 clearly yields results that are less conservative than Model 1, which never allows a sequence of packet dropouts to exceed a prescribed bound N .

We exemplify this point for the case of linear dynamics.

Theorem 10: Consider a dynamical system of the form $\dot{x} = Ax + Bu$ along with the control action $u = K\bar{x}$, where $\bar{x}$ is defined as in (23) and K is a suitable state-feedback matrix such that all the eigenvalues of $\Phi = A + BK$ have negative real part. Given any positive symmetric definite matrix Q , let P be the solution of the Lyapunov equation $\Phi^\top P + P\Phi + Q = 0$. Let α_1 and α_2 be equal to the smallest and largest eigenvalue of P , respectively, γ_1 equal to the smallest eigenvalue of Q , $\gamma_2 := \|2PBK\|$ and $\gamma_3 := \|2P\|$. Let $\sigma \in \mathbb{R}_{>0}$ be such that $\gamma_1 - \sigma\gamma_2 > 0$. Let the sampling rate $\Delta \leq \Delta_*$ where

$$\Delta_* := \left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \quad (26)$$

when $\mu_A \leq 0$ and

$$\Delta_* := \frac{1}{\mu_A} \log \left[\left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \mu_A + 1 \right] \quad (27)$$

when $\mu_A > 0$, where μ_A is the logarithmic norm of A . Let $\omega_1 := (\gamma_1 - \gamma_2\sigma)/2\alpha_2$ and $\omega_2 := 2\gamma_2/\alpha_1$. Then, the closed-loop system is asymptotically stable (depending on the modelling tool of choice):

- For every packet-dropout pattern satisfying Model 1 with $N \leq N_*$, where N_* is any positive integer such that $N_* < \lfloor \omega_1/\omega_2 \rfloor$.
- For every packet-dropout pattern satisfying Model 2 with arbitrary c , and $\lambda \geq \lambda_*$ where λ_* is any positive real such that $\lambda_* > (\omega_1 + \omega_2)/\omega_1$.
- For every DoS signal satisfying Model 3 with arbitrary (κ, η) , and (τ_d, τ_f) such that $T \leq T_*$, where T is as

in (12) and T_* is any positive real number such that $T_* < \omega_1/(\omega_1 + \omega_2)$.

Proof: The proof of (c) can be found in [8]. Then also (a) and (b) hold true in view of Theorem 9. ■

As discussed in [8], ω_1 (respectively ω_2) represents the converging (diverging) rate of the closed-loop system in the absence (presence) of packet dropouts. One sees that in this case Models 2 and 3 provide less conservative results. For instance, when $\omega_1 = \omega_2 = \bar{\omega}$ conditions (b) and (c) amounts to requiring that, on the average, the number of successful transmissions is larger than half of the transmission attempts. Instead, condition (a) indicates that the maximum number of consecutive packet dropouts is zero in the worst case. This result is correct because a sequence $\{z_m\}_{m \in \mathbb{N}}$ of successful transmissions given by $z_m = 2\Delta m$ (successful transmissions and dropouts following one another) destroys asymptotic stability. However, condition (a) fails to capture that long but sporadic sequences of dropouts need not destroy stability. Stability results with respect to Models 2 and 3 have been considered also in nonlinear [13] and distributed [14], [15] settings.

B. Intrusion Detection and Stealthiness

As discussed in [16], *packet reception rate* (PRR) provides an effective means for intrusion detection systems. PRR is the rate of packets successfully transmitted compared to the number of transmissions. In a framework with genuine random packet dropouts, a threshold of d consecutive drops may be used to trigger an alarm. Specifically, consider an arbitrary observation window $\tau \in \mathbb{N}_1$, and let $\theta_k = 0$ when there is a packet dropout at time t_k and $\theta_k = 1$ otherwise. An alarm is triggered when

$$\sum_{k=i}^{i+\tau-1} (1 - \theta_k) \leq d \quad (28)$$

where $i \in \mathbb{N}$, and is not triggered otherwise.

Model 1 then provides a natural framework to account for intrusion detection issues. In this respect, Theorem 5 can be used to tune the parameters τ and d to guarantee that DoS signals with prescribed $(\kappa, \tau_d, \eta, \tau_f)$ can be detected. On the other hand, given τ and d , Theorem 5 also characterizes classes of DoS signals that can remain undetected.

V. ASYNCHRONOUS DYNAMICAL SYSTEMS

In [2], a framework is introduced to model dynamical systems driven by events that occur asynchronously. This framework has been exploited to model networked systems subject to dropouts defined in terms of *rate* of data loss [17], [18]. Hereafter, we consider a version of asynchronous dynamical systems that fits the purpose of our discussion.

Consider a dynamical system governed by

$$\dot{x} = f_s(x) \quad (29)$$

where $x \in \mathbb{R}^n$, $s \in \mathcal{I} := \{1, 2\}$, and $\mathcal{I}$ represents the set of discrete states with corresponding set of rates $\{1 - r, r\}$, where $r \in [0, 1]$. The function f_1 describes the system dynamics

in nominal conditions while f_2 describes the system dynamics when dropouts occur. Let us introduce one more dropout model.

Model 4: For any $k \in \mathbb{N}$, let $\theta_k = 0$ when there is a packet dropout at time t_k and $\theta_k = 1$ otherwise. For any $k_0 \in \mathbb{N}$, the *packet dropout rate* r is defined as

$$r := \limsup_{m \rightarrow +\infty} \frac{1}{m} \sum_{k=k_0}^{k_0+m-1} (1 - \theta_k) \quad (30)$$

In contrast with the definition of *rate of events* in [2], the definition of packet dropout rate above uses the limit superior rather than the limit. The quantity r is also termed *data missing rate* in [19] and *jamming rate* [20] in communication networks.

Assume there exist a class $\mathcal{C}^1$ function $V : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ such that $v_1(\|x\|) \leq V(x) \leq v_2(\|x\|)$ for some class $\mathcal{K}_\infty$ functions v_1, v_2 . Hassibi *et al.* [2] show that the system is asymptotically stable if there exist two constants c_1 and c_2 such that

$$(1 - r)c_1 + rc_2 > 0 \quad (31)$$

and

$$\frac{\partial V}{\partial x} f_i(x) \leq -c_i V(x) \quad (32)$$

for $i = 1, 2$. Assuming $c_1 > 0$ (stable behavior in nominal conditions) and $c_2 < 0$ (unstable behavior in the presence of packet dropouts), (31) can be rearranged as

$$r < \frac{c_1}{c_1 - c_2} \quad (33)$$

which has exactly the same form as the constraint on λ and T in Theorem 10 upon letting $\omega_1 := c_1$ and $\omega_2 := -c_2$. This model is indeed connected with Models 2 and 3.

Theorem 11: Consider a packet-dropout pattern that satisfies Model 2 and the limit superior ρ of the series on the right hand side of (2) normalized by the number of elements of the series is convergent, namely

$$\limsup_{k_1 - k_0 \rightarrow +\infty} \frac{1}{k_1 - k_0 + 1} \sum_{k=k_0}^{k_0 + (k_1 - k_0)} (1 - \theta_k) =: \rho \quad (34)$$

Then the packet dropout pattern also satisfies Model 4 with packet dropout rate r satisfying

$$r = \rho \leq \frac{1}{\lambda} \quad (35)$$

Proof: By (2), any packet-dropout pattern generated according to Model 2 must satisfy

$$\frac{1}{k_1 - k_0 + 1} \sum_{k=k_0}^{k_1} (1 - \theta_k) \leq \frac{c}{k_1 - k_0 + 1} + \frac{k_1 - k_0}{\lambda(k_1 - k_0 + 1)} \quad (36)$$

The sequence on the left side satisfies $\sup_{h \geq k_1 - k_0} \frac{1}{h+1} \sum_{k=k_0}^{k_0+h} (1 - \theta_k) \leq \frac{c}{k_1 - k_0 + 1} + \frac{1}{\lambda}$, for all $k_1 - k_0 \geq 0$. By the comparison theorem for series, taking the limit as $k_1 - k_0 \rightarrow +\infty$, we obtain the thesis. ■

From the relation between Models 2 and 3, it is an easy matter to see that (35) holds true with respect to Model 3 with $1/\lambda$ replaced by T .

Theorem 11 shows that Models 2 and 3 can be used to asymptotically bound a given *rate* of data loss. These models still present an advantage with respect to Model 4 since

they have parameters (c in Model 2 and (κ, η) in Model 3) which can be tuned to ensure bounds also on the transient. This is not possible for Model 4 which only specifies asymptotic properties.

VI. CONCLUSION

In this letter, we have compared a number of deterministic packet-dropout models, and discussed their relative merits within the context of networked control. The analysis, here, rests on the hypothesis that transmissions are carried out at a constant frequency. Extending the present analysis to aperiodic settings is certainly interesting for gaining a better understanding of event-based and self-triggered control [21] in the presence of packet dropouts.

APPENDIX PROOF OF LEMMA 1

Let $\{\ell_n\}_{n \in \mathbb{N}}$ be the sequence of dropouts induced by $\mathcal{S}$. We construct a DoS signal $\bar{\mathcal{S}}$ with the property that each instance of $\bar{\mathcal{S}}$ starts at $\bar{h}_n = \ell_n$ and has duration $\bar{\tau}_n = 0$, giving $\bar{H}_n := \{\bar{h}_n\} \cup [\bar{h}_n, \bar{h}_n + \bar{\tau}_n] = \{\bar{h}_n\}$. By construction, $\bar{\mathcal{S}}$ takes the form of a train of pulses superimposed to the dropouts induced by $\mathcal{S}$. Proceeding as in Section II, let $\bar{n}(\tau, t)$ denote the number of off/on transitions of $\bar{\mathcal{S}}$ over $[\tau, t]$, and let $\bar{\Xi}(\tau, t) := \bigcup_{n \in \mathbb{N}} \bar{H}_n \cap [\tau, t]$. The signal $\bar{\mathcal{S}}$ satisfies (5) with respect to $\bar{\Xi}$ with $\bar{\kappa} = 0$ and $\bar{\tau}_d = \infty$. As for condition (4), $\bar{n}(\tau, t) = 0$ whenever $[\tau, t]$ does not contain any dropout, while $\bar{n}(\tau, t) = \bar{n}(\ell_r, \ell_s)$ where $r := \min\{n : \ell_n \geq \tau\}$ and $s := \max\{n : \ell_n \leq t\}$ otherwise. In the former case, the thesis holds trivially. We then focus on the latter case. We claim that

$$\bar{n}(\ell_r, \ell_s) \Delta \leq |\bar{\Xi}(v_r, \ell_s)| + n(v_r, \ell_s) \Delta \quad (37)$$

where $v_r := \max\{0, \ell_r - \Delta\}$. To begin with, we prove the claim for $s = r$. If $\ell_r = 0$ then $v_r = \ell_s = 0$, and the claim follows from the fact that $n(0, 0)$ must be equal to 1 since $\mathcal{S}$ and $\bar{\mathcal{S}}$ are PE by construction. If instead $\ell_r \geq \Delta$ then $v_r = \ell_r - \Delta$. In this case, either $|\bar{\Xi}(\ell_r - \Delta, \ell_r)| = \Delta$ or $n(\ell_r - \Delta, \ell_r) \geq 1$. The former case means that there is a DoS interval blocking the transmission at $\ell_r - \Delta$ which persists up to ℓ_r , while the latter case means that a new DoS interval arises before ℓ_r . In either case we get

$$|\bar{\Xi}(\ell_r - \Delta, \ell_r)| + n(\ell_r - \Delta, \ell_r) \Delta = \Delta \quad (38)$$

This shows the claim for $s = r$.

Assume now that the claim holds true for a certain $s \geq r$. By construction, it holds that $\bar{n}(\ell_r, \ell_{s+1}) = \bar{n}(\ell_r, \ell_s) + 1$. On the other hand, reasoning as before, either $|\bar{\Xi}(v_r, \ell_{s+1})| = |\bar{\Xi}(v_r, \ell_{s+1} - \Delta)| + \Delta$ or $n(v_r, \ell_{s+1}) \geq n(v_r, \ell_{s+1} - \Delta) + 1$. In either case we get

$$\begin{aligned} \bar{n}(\ell_r, \ell_{s+1}) \Delta &= \bar{n}(\ell_r, \ell_s) \Delta + \Delta \\ &\leq |\bar{\Xi}(v_r, \ell_s)| + n(v_r, \ell_s) \Delta + \Delta \\ &\leq |\bar{\Xi}(v_r, \ell_{s+1})| + n(v_r, \ell_{s+1}) \Delta \end{aligned} \quad (39)$$

This shows (37). The thesis follows applying Model 3 to the right-hand side of (37), which gives

$$\bar{n}(\ell_r, \ell_s) \Delta \leq \kappa + \eta \Delta + T(\ell_s - v_r) \quad (40)$$

and noting that $\ell_s - v_r \leq t - \tau + \Delta$.

REFERENCES

- [1] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control* (LNCS 5469), R. Majumdar and P. Tabuada, Eds. Berlin, Germany: Springer, 2009, pp. 31–45.
- [2] A. Hassibi, S. P. Boyd, and J. P. How, "Control of asynchronous dynamical systems with rate constraints on events," in *Proc. 38th IEEE Conf. Decis. Control*, Phoenix, AZ, USA, 1999, pp. 1345–1351.
- [3] D. Yue, Q.-L. Han, and C. Peng, "State feedback controller design of networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 11, pp. 640–644, Nov. 2004.
- [4] H. Lin and P. J. Antsaklis, "Stability and persistent disturbance attenuation properties for a class of networked control systems: Switched system approach," *Int. J. Control*, vol. 78, no. 18, pp. 1447–1458, 2005.
- [5] P. Naghshtabrizi and J. P. Hespanha, "Designing observer-based controller for network control system," in *Proc. 44th IEEE Conf. Decis. Control*, Seville, Spain, 2005, pp. 2876–2880.
- [6] W. P. M. H. Heemels and N. van de Wouw, "Stability and stabilization of networked control systems," in *Networked Control Systems* (Lecture Notes in Control and Information Sciences), vol. 406, A. Bemporad, M. Heemels, and M. Johansson, Eds. London, U.K.: Springer, 2010, pp. 203–253.
- [7] D. E. Quevedo and D. Nešić, "Input-to-state stability of packetized predictive control over unreliable networks affected by packet-dropouts," *IEEE Trans. Autom. Control*, vol. 56, no. 2, pp. 370–375, Feb. 2011.
- [8] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.
- [9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Urbana, IL, USA, 2005, pp. 46–57.
- [10] D. J. Thunte and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. 25th IEEE Commun. Soc. Mil. Commun. Conf. (MILCOM)*, Washington, DC, USA, 2006, pp. 1–7.
- [11] J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Proc. 38th IEEE Conf. Decis. Control*, Phoenix, AZ, USA, 1999, pp. 2655–2660.
- [12] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decis. Control*, Atlanta, GA, USA, 2010, pp. 1096–1101.
- [13] C. De Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," *Syst. Control Lett.*, vol. 96, pp. 124–131, Oct. 2016.
- [14] D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered coordination over a shared network under denial-of-service," in *Proc. 54th IEEE Conf. Decis. Control*, Osaka, Japan, 2015, pp. 3469–3474.
- [15] W. Zhang, Y. Tang, T. Huang, and J. Kurths, "Sampled-data consensus of linear multi-agent systems with packet losses," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published. [Online]. Available: <http://ieeexplore.ieee.org/document/7546899/>, doi: 10.1109/TNNLS.2016.2598243
- [16] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
- [17] W. Zhang, M. Branicky, and S. M. Phillips, "Stability of networked control systems," *IEEE Control Syst. Mag.*, vol. 21, no. 1, pp. 84–99, Feb. 2001.
- [18] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.
- [19] W.-A. Zhang and L. Yu, "Stabilization of sampled-data control systems with control inputs missing," *IEEE Trans. Autom. Control*, vol. 55, no. 2, pp. 447–452, Feb. 2010.
- [20] L. Anantharamu, B. S. Chlebus, D. R. Kowalski, and M. A. Rokicki, "Medium access control for adversarial channels with jamming," in *Proc. 18th Int. Colloquium Struct. Inf. Commun. Complexity (SIROCCO)*, Gdańsk, Poland, 2011, pp. 89–100.
- [21] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proc. 51st IEEE Conf. Decis. Control*, Maui, HI, USA, 2012, pp. 3270–3285.