Cloud control for cyber-physical systems in the presence of DoS attacks

Priscila F. S. Guedes[1], Pedro H. S. Coutinho[2], Mohamed Chahine Ghanem[3], Márcio J. Lacerda[3]

***Abstract*— This paper investigates the impact of Denial-of-Service (DoS) attacks on sampled-data control systems with non-uniform sampling and extends the analysis to cloud-based control architectures subject to random delays and packet losses. A Lyapunov-based framework is developed to ensure exponential stability of linear time-invariant (LTI) systems under DoS conditions, with sufficient conditions derived via linear matrix inequalities (LMIs). Numerical simulations illustrate the performance of both local and cloud-based controllers, revealing that while both architectures achieve stability, the cloud-based implementation suffers from degraded transient performance due to communication uncertainties. The results highlight the trade-offs between resilience and performance in modern networked control systems.**

I. INTRODUCTION

The increasing reliance on communication networks to close control loops in cyber-physical systems (CPSs) has paved the way for the development of Networked Control Systems (NCSs) [1], [2], [3]. These architectures offer flexibility and reduced wiring costs, enabling distributed control in applications such as autonomous vehicles, smart grids, and industrial automation. However, this interconnectivity also introduces vulnerabilities, particularly when the communication network is subject to imperfections such as packet dropouts, time-varying delays, and limited bandwidth [4], [5], [6]. A critical concern in this context is the threat of Denial-of-Service (DoS) attacks, where malicious agents block or delay transmissions, effectively disrupting the availability of sensor or control data [7], [8], [9], [10], [11].

Recent studies have shown that cyberattacks, including DoS and false data injection threats, are increasingly concerning in practical networked systems. For instance, detection and mitigation of Distributed Denial-of-Service (DDoS) attacks have been investigated in 5G-enabled vehicular networks using xApp orchestration strategies [12]. Additionally, the vulnerability of Industrial Internet of Things (IIoT) devices to false data injection via communication protocols such as MQTT has also been demonstrated, highlighting risks beyond mere unavailability [13].

To address communication constraints and improve resource efficiency, sampled-data control strategies with non-uniform sampling intervals have been proposed. Unlike periodic schemes, these approaches update the control input only at irregularly spaced time instants, either through event-triggered mechanisms or randomized sampling [14], [15], [16]. Non-uniform sampling not only reduces bandwidth usage but also increases the unpredictability of transmission events, which can enhance resilience to cyberattacks. Furthermore, it allows for a more realistic representation of systems where sensors and controllers operate asynchronously due to hardware or network variability [17].

In the presence of DoS attacks, missing updates during their occurrence can significantly degrade performance. However, by employing sampled-data control strategies with aperiodic sampling, the irregularity of control updates reduces predictability and increases the resilience to DoS attacks in comparison to standard periodic sampling. To properly model the effect of DoS attacks in control systems, previous work has considered deterministic or stochastic frameworks, often assuming constraints on their frequency and duration [18]. Additionally, resilient strategies have been proposed for LPV systems subject to hybrid cyberattacks, combining Denial-of-Service and deception mechanisms. In [19], an event-triggered control approach is developed using LMI-based co-design techniques to handle both control update reduction and attack resilience, ensuring exponential stability even under adverse network conditions.

In this paper, we investigate the sampled-data control of linear time-invariant (LTI) systems in the presence of deterministic DoS attacks. The sampling instants are generated with random sampling times, reflecting realistic variability in sensing or communication delays. The DoS attacks are defined by intervals of activity during which control signals are completely blocked. To increase the resilience of the closed-loop system, the zero-input strategy is employed such that the input is set to zero when unsuccessful communication occurs due to DoS attacks. The stability analysis is studied using a looped-functional approach.

As an additional contribution, we also consider a cloud-based control configuration that introduces additional uncertainties such as random delays in state transmission and probabilistic packet loss, motivated by the growing deployment of Control-as-a-Service (CaaS) frameworks [20]. In this setting, the controller operates remotely and receives state measurements through a network prone to random failures. When a packet is successfully received, the control input is computed using a delayed state due to network latency. When lost, the system relies on the last valid control input. This architecture models realistic cloud scenarios where computational resources are offloaded to remote servers and

[1]Priscila F. S. Guedes is with Department of Electrical Engineering, Federal University of São João Del Rei – UFSJ, São João Del Rei, MG, Brazil pri12_guedes@hotmail.com

[2] Pedro H. S. Coutinho is with the Department of Electronics and Telecommunication Engineering, State University of Rio de Janeiro, Rio de Janeiro, Brazil. phcoutinho@eng.uerj.br

[3] Marcio J. Lacerda and Mohamed Chahine Ghanem are with the Cyber Security Research Centre, London Metropolitan University, London, UK. m.ghanem@londonmet.ac.uk, m.lacerda@londonmet.ac.uk

control decisions are applied asynchronously.

This paper is organized as follows. Preliminary results and problem formulation are presented in Section II, Section III details the main contributions of the paper. The effectiveness of the proposed method is illustrated via numerical experiments in Section IV, while Section V concludes the paper.

Notation: $X \in \mathbb{R}^{m\times n}$ represents a matrix with real entries of m rows and n columns. The transpose of a matrix X is denoted by $X^\top$. $P > 0$ ($P < 0$) represents a positive definite (negative definite) symmetric matrix. The identity and zero matrices of appropriate dimensions are denoted by I and 0, respectively. $diag(A, B)$ is the block diagonal matrix whose elements are A, B. For a given matrix X, $He(X) \triangleq X+X^T$.

II. PRELIMINARIES

Consider the following continuous-time plant,

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state and $u(t) \in \mathbb{R}^{n_u}$ is the control input at time $t > 0$, $\forall t \in \mathbb{R}$.

When no DoS attacks occur, the measured state $x(t)$ is sampled and transmitted at the instants t_k, $k \in \mathbb{N}_0$, with the signal $\hat{x}(t) = x(t_k)$ remaining constant over the interval $[t_k, t_{k+1})$ due to the zero-order hold (ZOH) mechanism. The sampling instants $t_k \in \mathbb{R}_{\geq 0}$ satisfy $t_0 = 0$, $t_{k+1} - t_k > 0$, $\lim_{k\to\infty} t_k = \infty$. However, during a DoS attack, the transmission attempt is blocked, preventing the update of $\hat{x}(t)$. Consequently, $\hat{x}(t)$ can be defined as follows:

$$\hat{x}(t) = \begin{cases} x(t_k), & \text{if a transmission is successful at } t = t_k, \\ \hat{x}(t^-), & \text{otherwise.} \end{cases} \tag{2}$$

Using a zero-input strategy [9], the control signal effectively applied to the plant is

$$u(t) = \sigma(t)Kx(t_k), \tag{3}$$

for all $t \in [t_k, t_{k+1})$, $K \in \mathbb{R}^{n_u\times n}$ is the control gain and

$$\sigma(t) = \begin{cases} 0, & \text{if a DoS is active at } t_k, \\ 1, & \text{otherwise.} \end{cases} \tag{4}$$

The auxiliary variable $\sigma(t)$ indicates whether the latest transmission attempt at t_k was unsuccessful ($\sigma(t) = 0$) or not ($\sigma(t) = 1$) due to the presence of DoS attacks.

Therefore, the closed-loop system is described as

$$\dot{x}(t) = Ax(t) + \sigma(t)BKx(t_k). \tag{5}$$

A. Exponential stability analysis under DoS attacks

Assumption 1 *Let the sequence of DoS attacks $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ and let $n(T_1, T_2)$ be the number of DoS on/off transitions occurring in the interval $[T_1, T_2)$, that is,*

$$n(T_1, T_2) = card\{n \in \mathbb{N} \mid h_n + \tau_n \in [T_1, T_2)\},$$

where card denotes the cardinality of the set. For given $\tau_D \in \mathbb{R}_{>0}$ and $\eta \in \mathbb{R}_{\geq 0}$, the sequence of DoS attacks $\{H_n\}_{n\in\mathbb{N}}$ satisfies the DoS frequency constraint:

$$n(T_1, T_2) \leq \eta + \frac{T_2 - T_1}{\tau_D}, \quad \forall T_1, T_2 \in \mathbb{R}_{\geq 0} \text{ with } T_2 \geq T_1.$$

Assumption 2 *For given $T \in \mathbb{R}_{>1}$ and $\kappa \in \mathbb{R}_{\geq 0}$, the sequence of DoS attacks $\{H_n\}_{n\in\mathbb{N}} \in \mathcal{I}_{DoS}$ satisfies the DoS duration constraint:*

$$|\Xi(T_1, T_2)| \leq \kappa + \frac{T_2 - T_1}{T}, \quad \forall T_1, T_2 \in \mathbb{R}_{\geq 0} \text{ with } T_2 \geq T_1.$$

The problem addressed in this work is stated as follows.

Problem: Consider the system (1) and the control law given by (3), under DoS attacks satisfying Assumptions 1, and 2, and a bounded set $\mathcal{T} = [T_{min}, T_{max}]$, with $T_{max} > T_{min} > 0$. Suppose that the feedback gain K is chosen such that the matrix $A + BK$ is Hurwitz, i.e., all its eigenvalues lie in the open left-half of the complex plane. Determine a looped functional that certifies that the origin of the closed-loop system (5) is exponentially stable for any arbitrary time-varying sampling interval $T_k = t_{k+1} - t_k$ with values in $\mathcal{T}$.

The stability analysis regarding the stated problem is stated in the following Proposition.

Proposition 3 *Let $V : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function that satisfies*

$$c_1||x||^2 \leq V(x) \leq c_2||x||^2, \tag{6}$$

for scalars $c_1, c_2 > 0$. Let $\chi_k \in \mathcal{C}([-T_k, 0], \mathbb{R}^n)$ be a lifted function defined as

$$\chi_k(\tau) = x(t_k + \tau), \tag{7}$$

for any transmission attempt instant t_k. And let $\mathcal{V}_0 : [0, T_k] \times \mathcal{C}([0, T_k], \mathbb{R}^n) \to \mathbb{R}$ be a functional that satisfies the looping condition

$$\mathcal{V}_0(0, \chi_k) = e^{\omega_1 T_k}\mathcal{V}_0(T_k, \chi_k), \tag{8}$$

with

$$\mathcal{V}_0(0, \chi_k) \leq \delta V(\chi_k(0)), \tag{9}$$

$$-\delta V(\chi_k(0)) \leq e^{\omega_1 \tau}\mathcal{V}_0(\tau, \chi_k), \tag{10}$$

for some $\delta \geq 0$ and $\tau \in [0, T_k]$.

If the following conditions hold:

1) *When t_k belongs to a DoS interval, then*

$$\dot{V}(x(t)) \leq \omega_2 V(x(t)), \tag{11}$$

for all $t \in [t_k, t_{k+1})$.

2) *When t_k does not belong to a DoS interval, then*

$$\frac{d}{d\tau}U(\tau, \chi_k) \leq 0, \tag{12}$$

for all $\tau \in [0, T_k)$, where

$$U(\tau, \chi_k) = e^{\omega_1 \tau}(V(\chi_k(\tau)) + \mathcal{V}_0(\tau, \chi_k)), \tag{13}$$

3) *The frequency and duration of the DoS sequence satisfy*

$$\frac{1}{T} + \frac{T_{max}}{\tau_D} < \frac{\omega_1}{\omega_1 + \omega_2}. \tag{14}$$

Then, the closed-loop system (5) *is exponentially stable.*

Proof: The proof can be found in [9]. ■

III. MAIN RESULTS

A. Stability analysis in the presence of DoS attacks

Proposition 4 *Consider the system given by the interconnection of* (1) *and* (3) *in the presence of DoS attacks. Let K be a gain selected such that the matrix $A+BK$ is Hurwitz. Given positive scalars ω_1, ω_2 and h, if there exist matrices $P>0$, $R>0$, $S_1=S_1^T$, S_2, $X\geq 0$ all belonging to $\mathbb{R}^{n\times n}$, $\mathcal{X}\in\mathbb{R}^{4n\times n}$ and $Y\in\mathbb{R}^{2n\times 4n}$ such that the following inequalities are satisfied:*

$$A^TP+PA-\omega_2 P\leq 0. \tag{15}$$

$$\phi_1+h_2(0)\phi_2+h_4(0)\phi_4<0, \tag{16}$$

$$\begin{bmatrix}\Phi_1 & h_3(T_{min})Y^T\\ \star & -h_3(T_{min})\mathcal{R}\end{bmatrix}<0, \tag{17}$$

where $\Phi_1=h_1(T_{min})\phi_1+h_2(T_{min})\phi_2+h_4(T_{min})\phi_4$,

$$\begin{bmatrix}\Phi_2 & h_3(T_{max})Y^T\\ \star & -h_3(T_{max})\mathcal{R}\end{bmatrix}<0, \tag{18}$$

where $\Phi_2=h_1(T_{max})\phi_1+h_2(T_{max})\phi_2+h_4(T_{max})\phi_4$, *and*

$$\begin{aligned}h_1(\tau)&=e^{\omega_1\tau},\\ h_2(\tau,T_k)&=\frac{1}{\omega_1}(e^{\omega_1 T_k}-e^{\omega_1\tau}),\\ h_3(\tau,T_k)&=\frac{e^{\omega_1 T_k}}{\omega_1}(e^{\omega_1\tau}-1),\\ h_4(\tau,T_k)&=2e^{\omega_1 T_k}+((e^2-4)e^{\frac{\omega_1}{2}T_k}+1)e^{\omega_1\tau}.\end{aligned} \tag{19}$$

and

$$\begin{aligned}\phi_1 &= He(M_1^TPM_4)+\omega_1 M_1^TPM_1+He(\mathcal{X}\mathcal{B})\\ &\quad -M_{12}^TS_1M_{12}-He(M_{12}^TS_2M_2)-He(Y^TW),\\ \phi_2 &= M_4^TRM_4+He(M_4^TS_1M_{12})+He(M_4^TS_2M_2),\\ \phi_4 &= M_2^TXM_2,\\ \mathcal{B} &= \begin{bmatrix}A & BK & 0 & -I\end{bmatrix},\\ \mathcal{R} &= diag(R,3R),\end{aligned}$$

with

$$\begin{aligned}M_1 &= \begin{bmatrix}I & 0 & 0 & 0\end{bmatrix},\quad M_2=\begin{bmatrix}0 & I & 0 & 0\end{bmatrix},\\ M_3 &= \begin{bmatrix}0 & 0 & I & 0\end{bmatrix},\quad M_4=\begin{bmatrix}0 & 0 & 0 & I\end{bmatrix},\\ M_{12} &= \begin{bmatrix}I & -I & 0 & 0\end{bmatrix},\quad W=\begin{bmatrix}M_{12}\\ M_1+M_2-2M_3\end{bmatrix},\end{aligned}$$

then the conditions (11) *and* (12) *hold with*

$$V(x)=x^TPx \tag{20}$$

and

$$\begin{aligned}\mathcal{V}_0(\tau,\chi_k)=&f_1(\tau,T_k)\zeta_k^T(\tau)(S_1\zeta_k(\tau)+2S_2\chi_k(0))\\ &+f_1(\tau,T_k)\int_0^\tau \dot\chi_k^T(s)R\dot\chi_k(s)ds\\ &+f_2(\tau,T_k)\chi_k^T(0)X\chi_k(0)+\gamma e^{-\omega_1\tau}||\chi_k(0)||^2,\end{aligned} \tag{21}$$

where $\zeta_k(\tau)=\chi_k(\tau)-\chi_k(0)$, $\gamma>0$, *and*

$$\begin{aligned}f_1(\tau,T_k)&=\frac{1}{\omega_1}(e^{\omega_1(T_k-\tau)}-1),\\ f_2(\tau,T_k)&=\frac{e^{-\omega_1\tau}}{\omega_1}[(e^{\omega_1 T_k}-1)(e^{\omega_1\tau}-1)-(e^{\omega_1\tau}-1)^2].\end{aligned}$$

If the frequency and duration of the DoS sequence satisfy (14)*, then the origin of the closed-loop system* (5) *is exponentially stable.*

Proof: The proof is now conducted by analyzing the two distinct operational modes of the closed-loop system, corresponding to transmission events occurring either with or without DoS attacks. First, consider a scenario where a transmission attempt takes place during a DoS attack. In this case, the system operates in an unforced mode, and its dynamics are given by:

$$\dot x(t)=Ax(t). \tag{22}$$

Thus, if the inequality (15) is satisfied, it follows that (11) holds with $V(x)$ given in (20).

When a transmission is attempted in the absence of attacks, the analysis is carried out considering the time interval $t\in[t_k,t_k+T_k)$, or $\tau\in[0,T_k)$, such that the closed-loop system, in the absence of DoS attacks, can be written as

$$\dot x(t)=Ax(t)+BKx(t_k).$$

As $\chi_k(\tau)=x(t_k+\tau)$, then

$$\dot x(t_k+\tau)=Ax(t_k+\tau)+BKx(t_k),$$

which can be rewritten as

$$\dot\chi_k(\tau)=A\chi_k(\tau)+BK\chi_k(0).$$

In this case, the derivative of (13) w.r.t. τ is

$$\begin{aligned}\dot U(\tau,\chi_k)=&h_1(\tau)(2\dot\chi_k^T(\tau)P\chi_k^T(\tau)+\omega_1\chi_k^T(\tau)P\chi_k^T(\tau))\\ &-h_1(\tau)\zeta_k^T(\tau)[S_1\zeta_k^T(\tau)+2S_2\chi_k(0)]\\ &-h_1(\tau)\int_0^\tau\dot\chi_k^T(s)R\dot\chi_k(s)ds\\ &+h_2(\tau,T_k)\dot\chi_k^T(\tau)[R\dot\chi_k^T(\tau)+2S_1\zeta_k(\tau)+2S_2\chi_k(0)]\\ &+((e^{\omega_1 T_k}+1)e^{\omega_1\tau}-2e^{2\omega_1\tau})\chi_k^T(0)X\chi_k^T(0).\end{aligned} \tag{23}$$

By applying the Wirtinger-based integral inequality [21], the integral term in (23) can be upper-bounded by

$$-\int_0^\tau\dot\chi_k^T(s)R\dot\chi_k(s)ds\leq-\frac{1}{\tau}\xi_k^T(\tau)W^T\mathcal{R}W\xi_k(\tau) \tag{24}$$

where $\xi_k(\tau)=(\chi_k(\tau),\chi_k(0),\upsilon_k(\tau),\dot\chi_k(\tau))$, with $\upsilon_k(\tau)=\frac{1}{\tau}\int_0^\tau\chi_k(s)ds$. Since $R>0$, the inverse of $\mathcal{R}$ exists and $(\mathcal{R}W-\tau Y)^T\mathcal{R}^{-1}(\mathcal{R}W-\tau Y)\geq 0$, implying that

$$-\frac{1}{\tau}W^T\mathcal{R}W\leq-He(Y^TW)+\tau Y^T\mathcal{R}^{-1}Y. \tag{25}$$

Moreover, the closed-loop equation in (III-A) allows to define the following null-term

$$2h_1(\tau)\xi_k^T(\tau)\mathcal{X}\mathcal{B}\xi_k(\tau)=0. \tag{26}$$

It follows from (23), (25) and (26) that

$$\begin{aligned}\dot{U}(\tau,\chi_k) \leq & h_1(\tau)(2\dot{\chi}_k^T(\tau)P\chi_k^T(\tau)+\omega_1\chi_k^T(\tau)P\chi_k^T(\tau))\\ & -h_1(\tau)\zeta_k^T(\tau)[S_1\zeta_k^T(\tau)+2S_2\chi_k(0)]\\ & -h_1(\tau)\xi_k^T(\tau)(He(Y^TW)-\tau Y^T\mathcal{R}^{-1}Y)\xi_k(\tau)\\ & +h_2(\tau,T_k)\dot{\chi}_k^T(\tau)[R\dot{\chi}_k^T(\tau)+2S_1\zeta_k(\tau)+2S_2\chi_k(0)]\\ & +((e^{\omega_1 T_k}+1)e^{\omega_1\tau}-2e^{2\omega_1\tau})\chi_k^T(0)X\chi_k^T(0)\\ & +2h_1(\tau)\xi_k^T(\tau)\mathcal{X}\mathcal{B}\xi_k(\tau). \end{aligned} \tag{27}$$

Since $\tau h_1(\tau) \leq h_3(\tau,T_k)$ and $((e^{\omega_1 T_k}+1)e^{\omega_1\tau}-2e^{2\omega_1\tau}) \leq h_4(\tau,T_k)$, $\forall\tau\in[0,T_k]$, it is possible to write

$$\dot{U}(\tau,\chi_k) \leq \xi_k^T(\tau)\phi(\tau)\xi_k(\tau), \tag{28}$$

where $\phi(\tau) = h_1(\tau)\phi_1 + \sum_{i=1}^{3} h_i(\tau,T_k)\phi_i$, with $\phi_3 = Y^T\mathcal{R}^{-1}Y$. A sufficient condition to ensure (12) holds is

$$\phi(\tau) < 0. \tag{29}$$

With $\tau\in[0,T_k]$ and $T_k\in[T_{min},T_{max}]$. First we evaluated $\phi(\tau)$ at $\tau=0$, and we get (16). Evaluating $\phi(\tau)$ at $\tau=T_{min}$, we have

$$h_1(T_{min})\phi_1 + h_2(T_{min})\phi_2 + h_3(T_{min})\phi_3 + h_4(T_{min})\phi_4 < 0,$$

applying Schur complement yields (17). Finally, evaluating $\phi(\tau)$ at $\tau=T_{max}$, and applying the Schur complement, one has (18). These conditions are sufficient to ensure that (29) holds, concluding the proof.

■

B. Cloud Control

The cloud-based controller accounts for packet losses and random delays, inspired by the modeling framework of cloud control systems under uncertainties proposed by [22]. Specifically, the control law is updated based on successful packet delivery, as indicated by $\beta(t)$, and delayed states due to network latency are taken into account.

Consider the continuous-time linear system (1). A cloud-based controller generates the control signal and is subject to DoS attacks, packet losses, and random delays. Thus, the actual control input applied to the system is given by:

$$\tilde{u}(t) = \sigma(t)\tilde{u}(t_k), \quad \text{for } t\in[t_k,t_{k+1}), \tag{30}$$

where $\sigma(t)\in\{0,1\}$ is a switching signal that indicates the presence of a DoS attack, as defined in (4). Moreover, the signal $\tilde{u}(t)$ is computed at sampling instants t_k, and held constant between samples using ZOH.

To consider the presence of random delays, let $\beta(t)$ be a binary variable indicating whether the control packet at time t_k was successfully transmitted:

$$\tilde{u}(t_k) = \beta(t)Kx(t_{k-d_k}) + (1-\beta(t))\tilde{u}(t_{k^-}), \tag{31}$$

where $\beta(t)=1$ if the packet is received (with delay $d_k\in[0,T_k]$) and $\beta(t)=0$ if the packet is lost and the previous valid control is reused. Moreover, $x(t_{k-d_k})$ is the delayed state due to communication latency, and $\tilde{u}(t_{k^-})$ is the last valid control.

It is important to note that the conditions presented in Section III-A do not account for the presence of packet losses or random delays. However, if the packet losses exhibit the same duration and frequency characteristics as the DoS attacks, the proposed conditions can still guarantee stability. In the numerical experiments, we will evaluate the robustness of these conditions in the presence of random delays.

IV. NUMERICAL EXPERIMENTS

To illustrate the efficacy of the proposed method, numerical experiments are considered[1]. Consider the following system borrowed from [9], [18], [25]:

$$\dot{x} = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}x(t) + u(t), \tag{32}$$

which is open-loop unstable. Consider the following gain

$$K = \begin{bmatrix}-4.5 & -1\\ 0 & -6\end{bmatrix}, \tag{33}$$

that ensures that the matrix $(A+BK)$ is Hurwitz stable.

To observe the behavior of the system (32), the fourth-order Runge-Kutta method with $\Delta t = 10^{-2}$, initial conditions $x_0 = \begin{bmatrix}1 & -1\end{bmatrix}$, non periodic sampling with transmission rate $T_k\in\mathcal{T} = [0.03, 0.15]$ s, $\omega_1 = 6.6250$, $\omega_2 = 2.1799$, $n=15$, $\Xi = 6.28$ s, $\eta=0$, $\tau_D = 0.7143$, $\kappa=1$ and $T=1.5921$ were employed. Considering these parameters, the following matrix P is obtained from Proposition 4:

$$P = \begin{bmatrix}0.0460 & -0.0020\\ -0.0020 & 1.4926\end{bmatrix}.$$

By incorporating delays and losses as part of the communication channel, it is possible to assess the resilience of the system against multiple sources of degradation, highlighting the combined impact of cyber threats and communication failures.

Figure 1 (a) compares the performance of two scenarios

- a local controller with blocked updates during DoS, and
- a remote (cloud-based) controller subject to random delays and packet losses.

The same DoS parameters were used, considering a packet loss probability of 10% and a random delay in the interval $[0.03, 0.15]$ s.

It is observed that although both systems achieve asymptotic stability, the cloud-based controller exhibits degraded transient performance, as evidenced by larger oscillations in the state trajectories $x(t)$. These differences arise primarily due to two factors: random communication delays, which cause the controller to act on outdated state information, and packet losses, which result in the reuse of obsolete control inputs when updates are not received.

Despite these limitations, the cloud-based control system demonstrated robust behavior, with convergence observed even in the presence of DoS attacks and communication

[1]The numerical experiments were performed using MATLAB (R2020a) 64 bits for Windows 11, in a machine with Intel Core i5-8265U (1.8 GHz) processor and 8 GB RAM. The codes were implemented by using the packages YALMIP [23], and the solver Mosek [24].

uncertainties. This reinforces the viability of cloud-based control in distributed or remote applications, particularly when some degree of performance degradation is acceptable in exchange for improved scalability and flexibility.

Figure 1 (b) illustrates the packet success indicator $\beta(t)$ at each sampling instant. The gray vertical bands represent time intervals during which DoS attacks occur. When $\beta(t) = 1$, the control packet from the cloud is successfully received (i.e., no packet loss occurred). When $\beta(t) = 0$, the control packet was lost, which may happen even outside of DoS periods due to probabilistic communication failures.

Importantly, even if $\beta(t) = 1$, the control signal is not applied to the plant during a DoS attack, as the system enforces $u = 0$ in those intervals. Thus, a successful transmission from the cloud does not guarantee the actuation of control when a DoS attack is active. This explains occurrences where $\beta(t) = 1$ within DoS intervals, yet the effective control remains null.

Figure 2 presents successful and unsuccessful transmission attempts under both DoS-only and DoS combined with cloud-based control scenarios. As expected, the number of successful transmissions is lower in the DoS and Cloud setups. This is due to the presence of random packet losses and additional delays introduced by the cloud communication layer, which are captured by the transmission indicator $\beta(t)$. Even though both systems operate under the same sampling instants, cloud-induced losses and delays reduce the effective number of successful updates, which is reflected in the transmission statistics.

Remark 1 *Successful control updates in the cloud-based system occur only when three conditions are simultaneously satisfied: (i) the sampling instant t_k aligns closely with the simulation time grid, (ii) no DoS attack is active during the update, and (iii) the transmission is successful, i.e., $\beta(t) = 1$. However, since the sampling instants t_k are randomly generated and do not exactly match the simulation times t, some successful transmissions may not result in actual control updates. This explains the absence of blue segments (i.e., successful updates) in certain time intervals without DoS and with $\beta(t) = 1$, such as between $t = 3$ and $t = 4$. Additionally, random communication delays may shift the applied control further in time, contributing to the lack of updates despite successful transmission.*

V. CONCLUSION

This work studied linear control systems subject to DoS attacks that can maintain exponential stability when equipped with a suitable sampled-data feedback law, even under irregular sampling schedules. By extending the analysis to cloud-based control configurations, we incorporated realistic communication challenges such as random delays and packet losses. Simulation results confirmed that although cloud-based control introduces transient degradation, it preserves the system's stability under DoS conditions. These findings emphasize the viability of resilient remote control strategies for cyber-physical systems. A direction for future work is to propose stability certificates that take into account DoS attacks, packet losses, and random delays at the same time.

REFERENCES

[1] W. Zhang, M. S. Branicky, and S. M. Phillips, "Stability of networked control systems," *IEEE Control Systems Magazine*, vol. 21, no. 1, pp. 84–99, 2001.

[2] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

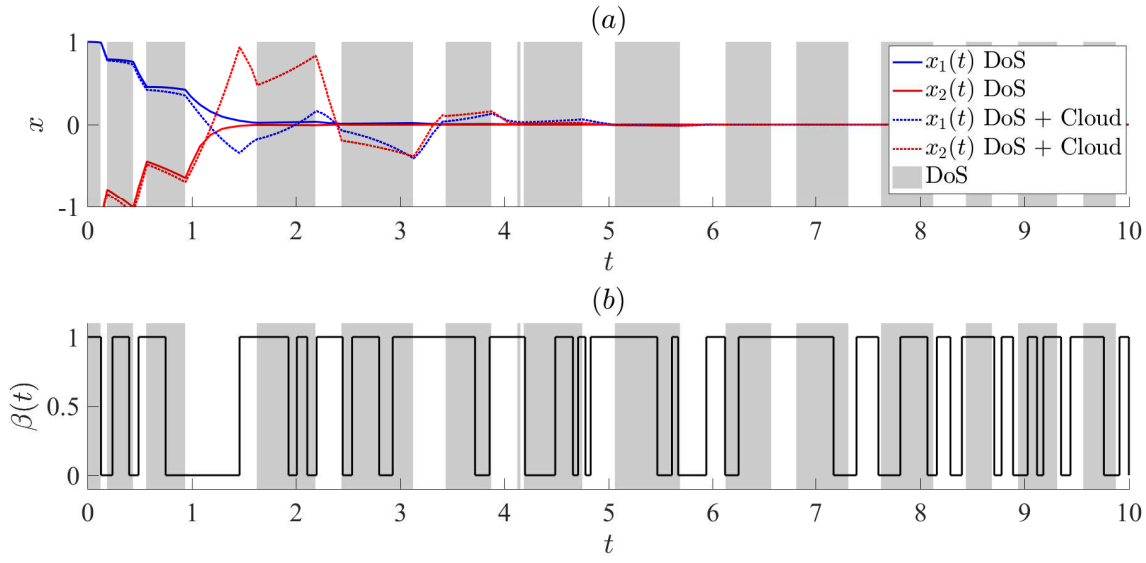

Fig. 1: a) Simulation results of the closed-loop system with the controller (3) with K in (33). (b) Binary indicator that represents whether the control was effectively updated or not at a given sampling instant in accordance with (31). The vertical gray stripes represent the time intervals in which the DoS attack is active.

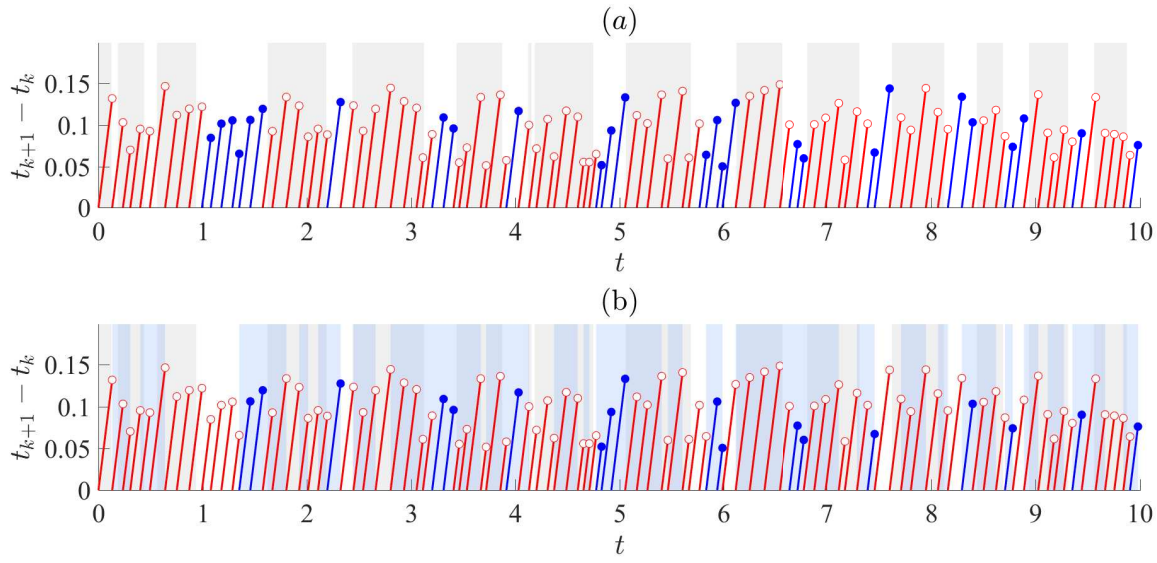

Fig. 2: Sampling intervals $t_{k+1} - t_k$ over time. Each line segment corresponds to a transmission attempt between two consecutive sampling instants. Red segments indicate unsuccessful transmissions, while blue ones indicate successful transmissions. Shaded gray regions represent periods affected by Denial-of-Service (DoS) attacks and shaded blue regions represent $\beta(t) = 1$. (a) System affected by DoS attacks only. (b) System under DoS attacks with cloud-based control.

[3] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527–2535, 2009.

[4] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Transactions on Automatic control*, vol. 52, no. 9, pp. 1680–1685, 2007.

[5] X. Wang and M. D. Lemmon, "Event-triggering in distributed networked control systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 3, pp. 586–601, 2010.

[6] M. S. Mahmoud, "Cloud-based control systems: Basics and beyond," in *Journal of Physics: Conference Series*, vol. 1334, no. 1. IOP Publishing, 2019, p. 012006.

[7] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proceedings of the 2010 American Control Conference*, 2010, pp. 3690–3696.

[8] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International workshop on hybrid systems: computation and control*, 2009, pp. 31–45.

[9] P. H. S. Coutinho, I. Bessa, P. S. Pessim, and R. M. Palhares, "A switching approach to event-triggered control systems under denial-of-service attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 50, p. 101383, 2023.

[10] P. S. P. Pessim and M. J. Lacerda, "State-feedback control for Cyber-physical LPV systems under DoS attacks," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 1043–1048, 2021.

[11] ——, "On the robustness of cyber-physical LPV systems under DoS attacks," *Journal of The Franklin Institute*, vol. 359, no. 2, pp. 677–696, January 2021.

[12] M. Awad, A. Ait Hamid, Y. Ranganathan, N. Choubik, R. Langar, and W. Jaafar, "XApps for DDoS attacks detection and mitigation in 5G-V2X O-RAN networks," in *2024 7th Conference on Cloud and Internet of Things (CIoT)*. IEEE, 2024, pp. 1–2.

[13] W. Alsabbagh, C. Kim, N. S. Patil, and P. Langendörfer, "Beyond the lens: false data injection attacks on IIoT-cameras through MQTT manipulation," in *2024 7th Conference on Cloud and Internet of Things (CIoT)*. IEEE, 2024, pp. 1–7.

[14] M. Miskowicz, "Send-on-delta concept: An event-based data reporting strategy," *Sensors*, vol. 6, no. 1, pp. 49–63, 2006.

[15] W. H. Heemels, M. Donkers, and A. R. Teel, "Periodic event-triggered control for linear systems," IEEE Transactions on automatic control, vol. 58, no. 4, pp. 847–861, 2012.

[16] M. Donkers and W. Heemels, "Output-based event-triggered control with guaranteed L$_\infty$-gain and improved event-triggering," in *49th IEEE Conference on Decision and Control (CDC)*, 2010, pp. 3246–3251.

[17] C. Nowzari, E. Garcia, and J. Cortés, "Event-triggered communication and control of networked systems for multi-agent consensus," *Automatica*, vol. 105, pp. 1–27, 2019.

[18] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[19] M. L. Peixoto, P. S. Pessim, P. H. Coutinho, I. Bessa, and R. M. Palhares, "Event-triggered control for lpv systems under hybrid cyberattacks," *Journal of Control, Automation and Electrical Systems*, vol. 35, no. 2, pp. 252–265, 2024.

[20] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[21] A. Seuret and F. Gouaisbaut, "Wirtinger-based integral inequality: Application to time-delay systems," *Automatica*, vol. 49, no. 9, pp. 2860–2866, 2013.

[22] S. Guan and S. Niu, "Stability-based controller design of cloud control system with uncertainties," *IEEE Access*, vol. 9, pp. 29 056–29 070, 2021.

[23] J. Lofberg, "Yalmip : a toolbox for modeling and optimization in matlab," in *2004 IEEE International Conference on Robotics and Automation*, 2004, pp. 284–289.

[24] E. D. Andersen and K. D. Andersen, "The MOSEK interior point optimizer for linear programming: An implementation of the homogeneous algorithm," in *High Performance Optimization*, ser. Applied Optimization, H. Frenk, K. Roos, T. Terlaky, and S. Zhang, Eds. Springer US, 2000, vol. 33, pp. 197–232.

[25] F. Forni, S. Galeani, D. Nešić, and L. Zaccarian, "Lazy sensors for the scheduling of measurement samples transmission in linear closed loops over networks," in *49th IEEE conference on decision and control (CDC)*. IEEE, 2010, pp. 6469–6474.

[26] M.C. Ghanem, 2023. Towards an efficient automation of network penetration testing using model-based reinforcement learning (Doctoral dissertation, City, University of London).

[27] A. S. Basnet, M. C. Ghanem, D. Dunsin, H. Kheddar, and W. Sowinski-Mydlarz, 2025. Advanced persistent threats (apt) attribution using deep reinforcement learning. Digital Threats: Research and Practice.

[28] M. Alshinwan, A.G. Memon, M. C. Ghanem, and M. Almaayah, 2025. Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. Jordanian Journal of Informatics and Computing, 2025(1), pp.27-36.

[29] M. Ghanem, A. Mouloudi, and M. Mourchid, 2015. Towards a scientific research based on semantic web. Procedia Computer Science, 73, pp.328-335.