Networked Control Under DoS Attacks

Feng, Shuai; Cetinkaya, Ahmet; Ishii, Hideaki; Tesi, Pietro; Persis, Claudio De

Published in:
IEEE-Transactions on Automatic Control

DOI:
10.1109/TAC.2020.2981083

Publication date:
2021

Networked Control Under DoS Attacks: Tradeoffs Between Resilience and Data Rate

Shuai Feng, Ahmet Cetinkaya, Hideaki Ishii, Pietro Tesi, and Claudio De Persis

***Abstract*—In this article, we study communication-constrained networked control problems for linear time-invariant systems in the presence of Denial-of-Service (DoS) attacks, namely attacks that prevent transmissions over the communication network. Our article aims at exploring the tradeoffs between system resilience and network bandwidth capacity. Given a class of DoS attacks, we characterize the bit-rate conditions that are dependent on the unstable eigenvalues of the dynamic matrix of the plant and the parameters of DoS attacks, under which exponential stability of the closed-loop system can be guaranteed. Our characterization clearly shows the tradeoffs between the communication bandwidth and resilience against DoS. An example is given to illustrate the proposed approach.**

***Index Terms*—Cyber-physical systems, Denial-of-Service (DoS) attacks, networked control systems, quantized control.**

I. Introduction

Cyber-physical systems (CPSs) have attracted much attention due to the advances in automation. Integrating communication and computation technologies, CPSs have a broad spectrum of applications ranging from small local control systems to large-scale systems, some of which are safety-critical. Thus, the malfunction of the safety-critical CPSs would induce destructive consequences to the physical world. Among the variety of aspects in reliability problems, the security of CPSs becomes a challenge from both practical and theoretical points of view. The security of CPSs mostly concerns the resilience against or protection from malicious attacks, e.g., deceptive attacks and Denial-of-Service (DoS) [2], [3].

This article deals with DoS attacks. The intention of DoS attackers is to induce instability by maliciously jamming the bandwidth-limited channel. It is well known that an insufficient bit rate in the communication channel influences the stability of a networked control system [4], not to mention networked control with packet drops [5]. Hence, the topic of networked control under data rate constraints and random packet dropouts has been investigated by many researchers. However, those results may not be applicable in the context of DoS since the communication failures induced by DoS can exhibit a temporal profile quite different from the one induced by genuine packet losses; particularly packet dropouts induced by DoS need not follow a given class of probability distributions [6]. This poses new challenges in theoretical analysis and controller design.

The literature on networked control with bit-rate limitation is large and diverse [7]–[11] and the problem when quantization and genuine packet losses coexist has been well studied (see e.g. [12]–[16]). In [8], the authors obtain necessary and sufficient conditions concerning the observability and stabilization for the networked control of a linear time-invariant system under communication constraints. These conditions are independent of information patterns and only reliant on the inherent property of the considered plant, i.e., the unstable eigenvalues of the dynamic matrix of the plant. The articles [12] and [16] investigate data rate problems for mean square stability under Markovian packet losses. Necessary and sufficient conditions for stabilization are obtained for both scalar and vector systems. Some research approach the control problem with data rate constraints more from information theoretic viewpoints [17].

Recently, systems under DoS attacks have been studied from the control-theoretic viewpoint [18]–[30]. In [18], a framework is introduced where DoS attacks are characterized by *frequency* and *duration*. The contribution is an explicit characterization of DoS frequency and duration under which stability can be preserved through state-feedback control. Extensions have been considered dealing with self-triggered networks [19] and nonlinear systems [20]. In [21], the authors generalize this model and consider a scenario where malicious jamming attacks and genuine packet losses coexist, in which the effects of malicious attacks and random packet losses are merged and characterized by an overall packet drop ratio. In [22], the authors investigate launching DoS attacks optimally to a network with genuine packet losses. Specifically, the attacker aims at maximizing the estimation error with constrained energy. In [23], the authors formulate a two-player zero-sum stochastic game framework to consider a remote secure estimation problem, where the signals are transmitted over a multi-channel network under DoS attacks. A game-theory-based model where transmitters and jammers have multiple choices of sending and interfering power is considered in [24]. The recent article [25] investigates the stabilization problem of a discrete-time output feedback system under quantization and DoS attacks. With the satisfaction of a certain norm condition, a lower bound of quantization level and an upper bound of DoS duration are obtained together guaranteeing stability.

In this article, we consider the tradeoffs between system resilience and data rate and explore how they interactively affect the stability of a linear time-invariant continuous-time process, possibly open-loop unstable and with complex eigenvalues. Specifically, the communication between sensor and controller takes place over a bit-rate limited channel subject to DoS attacks. Here, we assume that the channel is free of random dropouts and errors, e.g., single bit errors and burst errors. Previously, we have shown that a controller with prediction capability significantly promotes the resilience of a networked control system against DoS in the sense that the missing signals induced by

Manuscript received May 10, 2019; revised December 18, 2019; accepted March 5, 2020. Date of publication March 16, 2020; date of current version December 24, 2020. This work was supported in part by the JST CREST under Grant JPMJCRI5K3 and in part by JST ERATO HASUO Metamathematics for Systems Design Project under Grant JPMJER1603. This paper was presented in part at the American Control Conference, Philadelphia, PA, USA, July 10–12, 2019 [1]. Recommended by Associate Editor W. X. Zheng. *(Corresponding author: Shuai Feng.)*

Shuai Feng and Hideaki Ishii are with the Department of Computer Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan (e-mail: feng@sc.dis.titech.ac.jp; ishii@c.titech.ac.jp).

Ahmet Cetinkaya is with the Information Systems Architecture Science Research Division, National Institute of Informatics, Tokyo 101-8430, Japan (e-mail: cetinkaya@nii.ac.jp).

Pietro Tesi is with the DINFO, University of Florence, 50139 Firenze, Italy, and also with the ENTEG, Faculty of Science and Engineering, University of Groningen, 9747AG Groningen, The Netherlands (e-mail: pietro.tesi@unifi.it, p.tesi@rug.nl).

Claudio De Persis is with the ENTEG, Faculty of Science and Engineering, University of Groningen, 9747AG Groningen, The Netherlands (e-mail: c.de.persis@rug.nl).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2020.2981083

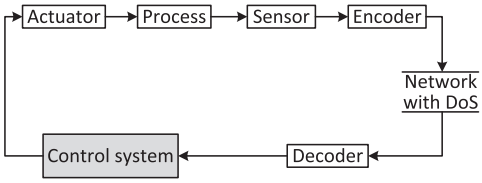

Fig. 1. Controller and actuator co-location architecture.

DoS attacks can be reconstructed and then applied for computing the control input [26], [27], [30]. Under proper design, the system can achieve ISS-like robust stability or asymptotic stability in the presence or absence of disturbance and noise, respectively. However, when the network has limited bandwidth, the existing results obtained are not applicable any longer because signal deviation induced by quantization cannot be simply treated as bounded noise under the control architecture in [27], and such signal deviation influences the accuracy of estimation/prediction and hence the resilience of the closed-loop control system.

Therefore, there are tradeoffs between communication bandwidth and system resilience. An interesting question is to find how large the data rate should be in order to guarantee the stability of a system under DoS attacks and also to ensure that the data rate is minimum if one does not consider DoS. We may state this question in another way as how much the limited bit rate degrades the robustness of a networked control system in terms of stabilization. We follow the approach aligned with that for the minimum data rate control problems discussed above. In particular, we recover those results in the case without any DoS. By applying the system transformation, we associate the bit rates with the eigenvalues of the dynamic matrix of the process and DoS parameters, and explicitly characterize the relationship between system resilience and bit rates. Specifically, we compute a bit-rate bound element-wise, larger than which the closed-loop system is exponentially stable. This on the other hand reveals the "robustness degradation" induced by quantization. Moreover, we also present a stability condition over the average data rate.

This article is organized as follows. In Section II, we introduce the framework that includes system description and transformation, a class of DoS attacks and the main contribution of this article. Section III presents a uniform quantizer and controller design. In Section IV, we present the main result, which includes the analysis of quantization range, prediction error, and stabilization. A numerical example is presented in Section V, and finally, Section VI concludes this article and introduces possible future research directions.

Notation: Let $\mathbb{R}$ denote the set of reals. Given $b \in \mathbb{R}$, $\mathbb{R}_{\geq b}$ and $\mathbb{R}_{>b}$ denote the sets of reals no smaller than b and reals greater than b, respectively; $\mathbb{R}_{\leq b}$ and $\mathbb{R}_{<b}$ represent the sets of reals no larger than b and reals smaller than b, respectively; $\mathbb{Z}$ denotes the set of integers. For any $c \in \mathbb{Z}$, we denote $\mathbb{Z}_c := \{c, c+1, \cdots\}$. Let $\lfloor v \rfloor$ be the floor function such that $\lfloor v \rfloor = \max\{w \in \mathbb{Z} | w \leq v\}$. Given a vector y, $\|y\|$ is its Euclidean norm. Given a matrix Γ, $\|\Gamma\|$ represents its spectral norm and Γ^{T} is its transpose. Given an interval $\mathcal{I}$, $|\mathcal{I}|$ denotes its length. The Kronecker product is denoted by $\otimes$. Finally, given a signal $\mathcal{F}$, $\mathcal{F}(t^-)$ denotes the limit from below at t.

II. Framework

A. System Description

Consider the networked control system in Fig. 1, which has been widely studied in the previous works such as [7], [9], [10], and [16]. The process is a linear time-invariant continuous-time system given by

$$\dot{x}(t) = Ax(t) + Bu(t), \quad t \in \mathbb{R}_{\geq 0} \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$ is the state with $x(0)$ arbitrary, $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_u}$, $u(t) \in \mathbb{R}^{n_u}$ is the control input and (A, B) is stabilizable. Let $K \in \mathbb{R}^{n_u \times n_x}$ be a matrix such that the real part of each eigenvalue of $A + BK$ is strictly negative. Let $\lambda_r = c_r \pm d_r i$ be the eigenvalues of A with $c_r, d_r \in \mathbb{R}$, where i represents the imaginary number. We assume that the state is measurable by sensors.

The measurement channel has limited bandwidth and is moreover subject to DoS (see Fig. 1). The transmission attempts between the encoder and decoder are carried out periodically, i.e.,

$$t_{k+1} - t_k = \Delta, \quad k \in \mathbb{Z}_0 \tag{2}$$

where $\{t_k\} = \{t_0, t_1, \dots\}$ denotes the sequence of the instants of transmission attempts and Δ denotes the sampling interval. By convention, we let $t_0 = 0$. Moreover, we assume that the network communication protocol is acknowledgment-based (like the TCP protocol) without any delay in terms of both encoded signal and acknowledgment transmissions.[1]

Since we consider a controller-actuator co-location architecture as in Fig. 1, only the measurement channel is subject to DoS, and the control channel is free from DoS disruptions and always available. Due to DoS attacks, not all the transmission attempts succeed. Hence, we denote by $\{z_m\}_{m \in \mathbb{Z}_0} = \{z_0, z_1, \dots\} \subseteq \{t_k\}_{k \in \mathbb{Z}_0}$ the sequence of the time instants at which successful transmissions occur.

B. System Transformation

In order to facilitate the analysis in Sections III and IV, we carry out the transformation as follows.

Lemma 1: There exists a transformation $\bar{x}(t) = E(t)Sx(t)$, possibly time-varying, which transforms (1) into

$$\dot{\bar{x}}(t) = \bar{A}\bar{x}(t) + \bar{B}(t)u(t) \tag{3}$$

where $\bar{A} \in \mathbb{R}^{n_x \times n_x}$ is a block diagonal matrix such that

$$\begin{aligned} \bar{A} &= E(t)SAS^{-1}E(t)^{-1} + \dot{E}(t)E(t)^{-1} \\ &= \mathrm{diag}\left(\bar{A}_1, \bar{A}_2, \dots, \bar{A}_p\right) \end{aligned} \tag{4}$$

where S and $E(t)$ are given in the Appendix. Let $r = 1, 2, \dots, p$, where $p \in \mathbb{Z}_1$ denotes the number of submatrices on the diagonal of $\bar{A}$. Therefore, one has

$$\bar{A}_r = \begin{bmatrix} c_r & 1 & & \\ & c_r & 1 & \\ & & \ddots & 1 \\ & & & c_r \end{bmatrix} \in \mathbb{R}^{n_r \times n_r} \tag{5}$$

corresponding to the real eigenvalue $\lambda_r = c_r$, and

$$\bar{A}_r = \begin{bmatrix} c_r & 1 & & \\ & c_r & 1 & \\ & & \ddots & 1 \\ & & & c_r \end{bmatrix} \otimes I \in \mathbb{R}^{2n_r \times 2n_r}, \; I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{6}$$

corresponding to the complex eigenvalues $\lambda_r = c_r \pm d_r i$ with $d_r \neq 0$. Besides, $\bar{B}(t) = E(t)SB$. ■

This lemma is essential for achieving a tight result and the minimum data rate in the absence of DoS attacks. Notice that in the context of discrete-time systems with random packet dropouts, time-varying transformation may not be a necessary step [12]. If A has no complex

[1]The decoder sends an acknowledgment to the encoder immediately when it successfully receives an encoded signal. If the acknowledgment is not received by the encoder at a sampling instant, it implies that due to the presence of DoS the decoder did not receive the transmission at all, and hence the decoder did not send the acknowledgment.

eigenvalues, then the transformation reduces to a time-invariant one, under which $\bar{A}$ becomes the Jordan form of A, and $\bar{B}(t)$ reduces to a time-invariant matrix.

C. Time-Constrained DoS

We refer to DoS as the phenomenon for which some transmission attempts may fail. We consider a general DoS model that constrains the attacker action in time by only posing limitations on the frequency of DoS attacks and their duration. Let $\{h_n\}_{n\in\mathbb{Z}_0}$ with $h_0 \geq 0$ denote the sequence of DoS *off/on* transitions, that is, the time instants at which DoS exhibits a transition from zero (transmissions are possible) to one (transmissions are not possible). Hence, $H_n := \{h_n\} \cup [h_n, h_n + \tau_n[$ represents the nth DoS time-interval, of a length $\tau_n \in \mathbb{R}_{\geq 0}$, over which the network is in DoS status. If $\tau_n = 0$, then H_n takes the form of a single pulse at h_n. Given $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$, let $n(\tau, t)$ denote the number of DoS *off/on* transitions over $[\tau, t]$, and let $\Xi(\tau, t) := \bigcup_{n\in\mathbb{Z}_0} H_n \bigcap [\tau, t]$ be the subset of $[\tau, t]$ where the network is in DoS status.

Assumption 1: (*DoS frequency*). There exist constants $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{>0}$ such that

$$n(\tau, t) \leq \eta + \frac{t-\tau}{\tau_D} \tag{7}$$

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

Assumption 2: (*DoS duration*). There exist constants $\kappa \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ such that

$$|\Xi(\tau, t)| \leq \kappa + \frac{t-\tau}{T} \tag{8}$$

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

Remark 1: Assumptions 1 and 2 do only constrain a given DoS signal in terms of its *average* frequency and duration. Following [31], τ_D can be considered as the average dwell-time between consecutive DoS *off/on* transitions, while η is the chattering bound. Assumption 2 expresses a similar requirement with respect to the duration of DoS. It expresses the property that, on average, the total duration over which communication is interrupted does not exceed a certain *fraction* of time, as specified by $1/T$. Like η, the constant κ plays the role of a regularization term. It is needed because during a DoS interval, one has $|\Xi(h_n, h_n + \tau_n)| = \tau_n > \tau_n/T$. Thus, κ serves to make (8) consistent. Conditions $\tau_D > 0$ and $T > 1$ imply that DoS cannot occur at an infinitely fast rate and be always active. ■

The next lemma from [30] relates DoS parameters and the time elapsing between successful transmissions.

Lemma 2: (see [30, Lemma 1]) Consider the periodic transmission as in (2) along with DoS attacks in Assumptions 1 and 2. If $1/T + \Delta/\tau_D < 1$, then the sequence of successful transmissions satisfies $z_0 \leq Q$ and $z_{m+1} - z_m \leq Q + \Delta$ for all $m \in \mathbb{Z}_0$, where $Q := (\kappa + \eta\Delta)(1 - 1/T - \Delta/\tau_D)^{-1}$. ■

We let $T_S(z_0, t)$ denote the number of successful transmissions within the interval $[z_0, t[$ $(t \geq z_0)$. The following lemma presents the relationship between DoS attacks, the time interval $[z_0, t[$ and $T_S(z_0, t)$.

Lemma 3: Consider the DoS attacks characterized by Assumptions 1 and 2 and the periodic transmission in (2). If $1/T + \Delta/\tau_D < 1$, then $T_S(z_0, t)$ satisfies

$$T_S(z_0, t) \geq \frac{1 - \frac{1}{T} - \frac{\Delta}{\tau_D}}{\Delta}(t - z_0) - \frac{\kappa + \eta\Delta}{\Delta}. \tag{9}$$

Proof: Notice that Assumptions 1 and 2 specify the DoS frequency and duration for the interval $[\tau, t]$. Recall that $n(\tau, t)$ denotes the number of DoS *off/on* transitions over $[\tau, t]$ and satisfies Assumption 1. Let $\underline{n}(\tau, t)$ be the number of DoS *off/on* transitions over $[\tau, t[$. One can verify that $\underline{n}(\tau, t) \leq n(\tau, t) \leq \eta + (t - \tau)/\tau_D$ for $t \geq \tau$. Likewise, we obtain that the duration of DoS attacks $|\underline{\Xi}(\tau, t)|$ for $[\tau, t[$ satisfies $|\underline{\Xi}(\tau, t)| \leq |\Xi(\tau, t)| \leq \kappa + (t - \tau)/T$.

Consider an interval $[z_0, t[$. Let H_n represent the nth DoS time-interval with $h_n \in [z_0, t[$. One can verify that the number of unsuccessful transmissions during H_n is no larger than $\tau_n/\Delta + 1$. Hence, the number of unsuccessful transmissions in $[z_0, t[$ satisfies $T_U(z_0, t) \leq \sum_{k=0}^{\underline{n}(z_0,t)-1}(\tau_k/\Delta + 1) \leq |\underline{\Xi}(z_0, t)|/\Delta + \underline{n}(z_0, t)$. Let $T_A(z_0, t)$ denote the number of total transmission attempts in $[z_0, t[$ and one has that $T_A(z_0, t) \geq (t - z_0)/\Delta$. On the other hand, one also has $T_S(z_0, t) = T_A(z_0, t) - T_U(z_0, t)$, with which the inequality (9) can be obtained. ■

Remark 2: In the scenario of a reliable network ($T = \tau_D = \infty$ and $\kappa = \eta = 0$), Q in Lemma 2 becomes zero, and $T_U(z_0, t) = 0$ implies $T_S(z_0, t) = T_A(z_0, t)$. This means that every transmission attempt ends up with a successful transmission. Thus, Lemmas 2 and 3 describe a standard periodic transmission policy. ■

D. Literature Review and Paper Contribution

We first introduce one of our previous results for the ease of comparison and then present the contribution of this article. The robustness problem of the structure as in Fig. 1 has been investigated in [26] and [27], where it is assumed that the network has infinite bandwidth. We briefly recall the controller and the result in [27]. Let $\xi(t)$ denote the estimation of $x(t)$ and $n(t)$ represents bounded noise, then the control system in [27] is

$$\begin{cases} u(t) = K\xi(t) \\ \begin{cases} \dot{\xi}(t) = A\xi(t) + Bu(t), & \text{if } t \neq z_m \\ \xi(t) = x(t) + n(t), & \text{if } t = z_m. \end{cases} \end{cases} \tag{10}$$

Theorem 1: (see [27]) Consider the dynamical system as in (1) under a co-located control system as in (10). The closed-loop system is stable for any DoS sequence satisfying Assumptions 1 and 2 with arbitrary η and κ, and with τ_D and T such that

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < 1. \tag{11}$$

In case $\|n(t)\| = 0$, the result above still holds. ■

Article Main Contribution: Exploiting the controller in (10) and the architecture in Fig. 1, we first design the encoder and decoder such that they are free of overflow of quantization range even in the presence of DoS attacks. Afterwards, we obtain that the closed-loop system is exponentially stable if the bit rate R_r satisfies

$$R_r \begin{cases} > c_r \Delta \log_2 e \left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D}\right)^{-1}, & \text{if } c_r \geq 0 \\ \geq 0, & \text{if } c_r < 0 \end{cases} \tag{12}$$

where R_r represents the number of bits applied to the signals corresponding to the blocks in $\bar{A}$. The condition (12) is general enough in the sense that in the absence of DoS attacks, the result of minimum data rate control is recovered (see Remark 4). On the other hand, we characterize the resilience of the system, namely the DoS attack boundary shaped by data rate. One can preserve closed-loop stability if the frequency and duration of DoS attacks satisfy

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < 1 - \frac{c_r \Delta \log_2 e}{R_r}, \ \forall c_r \geq 0 \tag{13}$$

where $R_r > 0$. Clearly, the signal inaccuracy due to quantization cannot be simply treated as the one caused by measurement noise in the sense that the noise does not enter the right-hand side of (11), whereas the quantization degrades system robustness by introducing $-c_r \Delta \log_2 e / R_r$ to the right-hand side of (13). One can get close to the result in (11) by increasing the data rate R_r.

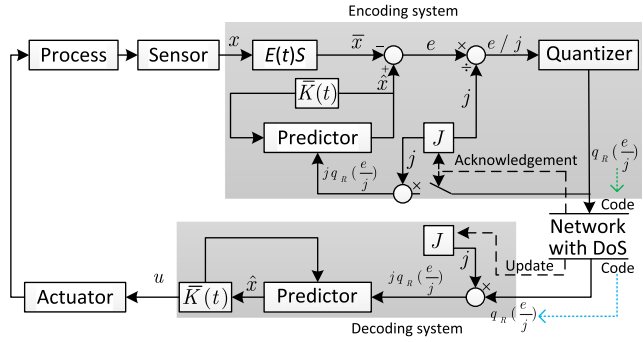

Fig. 2. Control architecture with encoding and decoding systems. The black solid lines and dashed lines represent paths of signals computed by embedded blocks and triggering signals generated by communication protocol, respectively. The green-dashed line represents the process that converts signals into code and the blue one represents the reversed process.

III. Control Architecture

A. Uniform Quantizer

The limitation of bandwidth implies that transmitted signals are subject to quantization. Let

$$\chi_l := e_l/j_l \tag{14}$$

be the original lth signal before quantization and $q_{\mathcal{R}_l}(\chi_l)$ represents the quantized signal of χ_l encoded by $\mathcal{R}_l$ bits, where $l = 1, 2, 3, \ldots, n_x$. The choices of $\mathcal{R}_l$, $e_l \in \mathbb{R}$ and $j_l \in \mathbb{R}_{>0}$ will be specified later. We implement a uniform quantizer such that

$$q_{\mathcal{R}_l}(\chi_l) := \begin{cases} \frac{\lfloor 2^{\mathcal{R}_l-1}\chi_l \rfloor + 0.5}{2^{\mathcal{R}_l-1}}, & \text{if } -1 \le \chi_l < 1 \\ 1 - \frac{0.5}{2^{\mathcal{R}_l-1}}, & \text{if } \chi_l = 1 \end{cases} \tag{15}$$

if $\mathcal{R}_l \in \mathbb{Z}_1$ and

$$q_{\mathcal{R}_l}(\chi_l) = 0 \tag{16}$$

if $\mathcal{R}_l = 0$. Note that for any $j_l \in \mathbb{R}_{>0}$ the following holds:

$$\left| e_l - j_l q_{\mathcal{R}_l}\left(e_l/j_l\right) \right| \le j_l/2^{\mathcal{R}_l}, \quad \text{if } |e_l|/j_l \le 1 \tag{17}$$

for both cases, namely $\mathcal{R}_l \in \mathbb{Z}_0$ [12], [14].

B. Controller Design

The basic idea of the control system design is that we equip the encoding and decoding systems with prediction capability to properly quantize data and more importantly predict the missing signals that are interrupted by DoS. The encoding system outputs quantized signals and transmits them to the decoding system through a DoS-corrupted network. The decoding system attempts to predict future signals based on the received quantized signals.

As shown in Fig. 2, on the sensor side the encoding system is embedded with a predictor for predicting $\bar{x}(t)$. Let $\hat{x}(t) = [\hat{x}_1(t)\ \hat{x}_2(t)\ \cdots\ \hat{x}_{n_x}(t)]^{\mathrm{T}}$ denote the prediction of $\bar{x}(t) = [\bar{x}_1(t)\ \bar{x}_2(t)\ \cdots\ \bar{x}_{n_x}(t)]^{\mathrm{T}}$. The error $e(t) = [e_1(t)\ e_2(t)\ \cdots\ e_{n_x}(t)]^{\mathrm{T}}$ describes the discrepancy between $\bar{x}(t)$ and $\hat{x}(t)$, where

$$e_l(t) := \hat{x}_l(t) - \bar{x}_l(t), \ \ l = 1, 2, \ldots, n_x. \tag{18}$$

Furthermore, we will design a dynamic system in (20), in which the state $J(t) = [j_1(t)\ j_2(t)\ \cdots\ j_{n_x}(t)]^{\mathrm{T}}$ is positive for $t \in \mathbb{R}_{\ge 0}$, where $j_l(t)$ represents the quantization range that bounds the error, i.e., $j_l(t) \ge |e_l(t)|$ for $t \in \mathbb{R}_{\ge 0}$ as it will be shown later.

On the actuator side, the decoding system is a copy of the encoding system. Once there is a successful transmission containing the encoded state at z_m, it recovers $q_{\mathcal{R}_l}(\chi_l(z_m))$ based on the received code and updates the predictor, and sends an acknowledgment back to the encoding system. We assume that the encoding and decoding systems have the same initial conditions. Therefore, identical structures and initial conditions, and acknowledgments guarantee synchronization of all the signals in the encoding and decoding systems.

The predictor in both the encoding and decoding systems predicting $\bar{x}(t)$ is given by

$$\begin{cases} \begin{cases} \dot{\hat{x}}(t) = \bar{A}\hat{x}(t) + \bar{B}(t)u(t), & t \ne z_m \\ \hat{x}(t) = \hat{x}(t^-) - \Phi(t^-), & t = z_m \end{cases} \\ u(t) = \bar{K}(t)\hat{x}(t) \end{cases} \tag{19}$$

where $\bar{K}(t) = KS^{-1}E(t)^{-1} \in \mathbb{R}^{n_u \times n_x}$. The vector $\Phi(t)$ in (19) is given by $\Phi(t) = [\phi_1(t)\ \phi_2(t)\ \cdots\ \phi_{n_x}(t)]^{\mathrm{T}}$, where $\phi_l(t) = j_l(t)q_{\mathcal{R}_l}(\chi_l(t))$. Recall that $\chi_l(t) = e_l(t)/j_l(t)$, in which $j_l(t)$ is the lth entry in the vector $J(t) = [j_1(t)\ j_2(t)\ \cdots\ j_{n_x}(t)]^{\mathrm{T}}$. The impulsive system computing $J(t)$ is given as follows:

$$\begin{cases} \begin{cases} \dot{J}(t) = \bar{A}J(t), & t \ne z_m \\ J(t) = HJ(t^-), & t = z_m \end{cases} \\ H = \mathrm{diag}(2^{-R_1}I_1, 2^{-R_2}I_2, \ldots, 2^{-R_p}I_p) \end{cases} \tag{20}$$

where $H \in \mathbb{R}^{n_x \times n_x}$ and $I_r \in \mathbb{R}^{n_r \times n_r}$ or $I_r \in \mathbb{R}^{2n_r \times 2n_r}$ represents the identity matrix with dimension matching that of $\bar{A}_r$ in (5) or (6), respectively. At the moment of a successful transmission, $J(t)$ in both the encoding and decoding systems is updated according to the second equation in (20). At last, the initial conditions of $\hat{x}$ and J in the encoding and decoding systems are identical and satisfy

$$\hat{x}_l(0^-) = 0, \ j_l(0^-) > |\bar{x}_l(0^-)|, \ l = 1, 2, \ldots, n_x. \tag{21}$$

It is worth mentioning that $\mathcal{R}_l$ represents the number of bits applied to the lth quantized signal, which is element-wise. Since the lth quantized signal must be associated with one block $\bar{A}_r$ ($r = 1, 2, \ldots, p$), hence in this article the data rate analysis is based on the index of $\bar{A}_r$, and all the elements corresponding to $\bar{A}_r$ apply R_r bits. For example, if the lth signal is associated with $\bar{A}_r$, then $\mathcal{R}_l = R_r$. In the results of this article, we will obtain the bounds of $\{R_r\}_{r=1,2,\ldots,p}$, so that $\{\mathcal{R}_l\}_{l=1,2,\ldots,n_x}$ can be determined.

IV. Main Result

We will first show that the uniform quantizer (15) is free of overflow and then conduct the analysis concerning stability.

A. Overflow-Free Quantization Under DoS

In this subsection, our intention is to show that $j_l(t) \ge |e_l(t)|$ for $t \in \mathbb{R}_{\ge 0}$ with $l = 1, 2, \ldots, n_x$, which implies the uniform quantizer (15) does not saturate. Exploiting (18) and the continuity of $\bar{x}(t)$ such that $\bar{x}(t) = \bar{x}(t^-)$, we have

$$\begin{aligned} e_l(t) &= \hat{x}_l(t) - \bar{x}_l(t) \\ &= \hat{x}_l(t^-) - \bar{x}_l(t^-) - j_l(t^-)q_{\mathcal{R}_l}\left(e_l(t^-)/j_l(t^-)\right) \\ &= e_l(t^-) - j_l(t^-)q_{\mathcal{R}_l}\left(e_l(t^-)/j_l(t^-)\right), \ \ t = z_m \end{aligned} \tag{22}$$

where $l = 1, 2, \ldots, n_x$. Hence, the dynamics of $e(t)$ obeys

$$\begin{cases} \dot{e}(t) = \bar{A}e(t), & t \ne z_m \\ e(t) = e(t^-) - \Phi(t^-), & t = z_m. \end{cases} \tag{23}$$

Moreover, observing (23) and (20), one has $\dot{e}(t) = \bar{A}e(t)$ and $\dot{J}(t) = \bar{A}J(t)$, respectively, for $t \ne z_m$. Their solutions are $e(t) = e^{\bar{A}t}e(0)$ and $J(t) = e^{\bar{A}t}J(0)$, respectively, for $0 \le t < z_0$ (if $z_0 \ne 0$) or $0 \le t < z_1$ (if $z_0 = 0$). Here, by (4)–(6), we can obtain $e^{\bar{A}t} = \mathrm{diag}(U_1(t), U_2(t), \ldots, U_p(t))$ with

$$U_r(t) = e^{c_r t}V_r(t) \otimes W, \quad r = 1, 2, \ldots, p \tag{24}$$

where

$$V_r(t)=\begin{bmatrix} 1 & t & \cdots & \cdots & \frac{t^{n_r-1}}{(n_r-1)!} \\ & 1 & t & \cdots & \frac{t^{n_r-2}}{(n_r-2)!} \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & t \\ & & & & 1 \end{bmatrix}, W=\begin{cases} 1, & \text{if } d_r=0 \\ I, & \text{if } d_r\neq 0 \end{cases} \quad (25)$$

in which $I\in\mathbb{R}^{2\times 2}$ is the identity matrix.

By $e(t)=e^{\bar{A}t}e(0)$, one can obtain that $|e(t)|\leq e^{\bar{A}t}|e(0)|$ holds element-wise, where $|\cdot|$ denotes a function that computes the absolute value of each element in a vector, i.e., $|e(t)|=[|e_1(t)|\ |e_2(t)|\ \cdots\ |e_{n_x}(t)|]^{\mathrm{T}}$. Define the vector $\varepsilon(t):=J(t)-|e(t)|=[\varepsilon_1(t)\ \varepsilon_2(t)\ \cdots\ \varepsilon_{n_x}(t)]^{\mathrm{T}}$. If $z_0\neq 0$, one has $\varepsilon(t)=J(t)-|e(t)|\geq e^{\bar{A}t}J(0)-e^{\bar{A}t}|e(0)|=e^{\bar{A}t}\varepsilon(0)$ for $0\leq t<z_0$. By (21), one knows that $\varepsilon(0)=J(0)-|e(0)|=J(0)-|\hat{x}(0)-\bar{x}(0)|=J(0^-)-|\hat{x}(0^-)-\bar{x}(0^-)|=J(0^-)-|\bar{x}(0^-)|>0$ and thus every element in the vector $\varepsilon(0)$ is positive, which implies that every element in the vector $\varepsilon(t)$ is positive for $0\leq t<z_0$. Thus, one can infer that $j_l(z_0^-)-|e_l(z_0^-)|>0$, and hence $j_l(z_0^-)-|e_l(z_0^-)|\geq 0$. In view of (22), one has

$$\begin{aligned} |e_l(z_0)| &= \left|e_l(z_0^-)-j_l(z_0^-)q_{\mathcal{R}_l}\left(e_l(z_0^-)/j_l(z_0^-)\right)\right| \\ &\leq j_l(z_0^-)/2^{\mathcal{R}_l}=j_l(z_0) \end{aligned} \quad (26)$$

where the inequality is implied by (17) and the second equality is implied by (20), from which one obtains that $|e_l(z_0)|\leq j_l(z_0)$ and furthermore $\varepsilon(z_0)\geq 0$. Following the analysis of $\varepsilon(t)$ for $0\leq t<z_0$, one could obtain that $\varepsilon(t)\geq e^{\bar{A}(t-z_0)}\varepsilon(z_0)$ with $z_0\leq t<z_1$. This implies that every element in $\varepsilon(t)$ is nonnegative and $|e_l(t)|\leq j_l(t)$ for $z_0\leq t<z_1$. By simple induction, we can verify that $|e_l(t)|\leq j_l(t)$ for $t\in\mathbb{R}_{\geq 0}$ if $z_0\neq 0$.

If $z_0=0$, we know that $|e_l(z_0^-)|=|e_l(0^-)|=|\bar{x}_l(0^-)|<j_l(0^-)=j_l(z_0^-)$, and hence $j_l(z_0^-)-|e_l(z_0^-)|\geq 0$. Following (26), one gets $|e_l(z_0)|\leq j_l(z_0)$. The remaining part follows the same analysis in the last scenario to obtain $|e_l(t)|\leq j_l(t)$ for $t\in\mathbb{R}_{\geq 0}$ if $z_0=0$. Therefore, we conclude that

$$|e_l(t)|\leq j_l(t),\ \ l=1,2,\ldots,n_x,\quad t\in\mathbb{R}_{\geq 0} \quad (27)$$

and thus the quantizer (15) is not overflowed, and (17) always holds. Notice that (27) holds for $t\in\mathbb{R}_{\geq 0}$, which implies $|e_l(t)|$ is always bounded by $j_l(t)$ in the absence and presence of DoS attacks. Without losing generality, we focus the attention from z_0 onwards.

B. Dynamics of the Encoding and Decoding Systems

Since the evolutions of the signals in the encoding and decoding systems are identical, we avoid their distinction in this part.

Considering (20) and simple iteration, we obtain that $J(z_m)=P(z_{m-1},\ z_m)J(z_{m-1})=\prod_{k=1}^{m}P(z_{k-1},\ z_k)J(z_0)=P(z_0,\ z_m)J(z_0)$, in which $P(z_{m-1},z_m)=He^{\bar{A}(z_m-z_{m-1})}$ is a block diagonal matrix in view of H in (20) and $e^{\bar{A}t}=\mathrm{diag}(U_1(t),U_2(t),\cdots,U_p(t))$ before (24). Let $P_r(z_{m-1},z_m)$ denote the matrices on the diagonal of $P(z_{m-1},z_m)$ and it is easy to verify that $P_r(z_{m-1},z_m)=2^{-R_r}U_r(\Delta_m)$ with $\Delta_m:=z_m-z_{m-1}$. By iteration, one has

$$P_r(z_0,z_m)=\prod_{k=1}^{m}P_r(z_{k-1},z_k)=\prod_{k=1}^{m}(2^{-R_r}U_r(\Delta_k)). \quad (28)$$

Recall that $\{z_m\}_{m\in\mathbb{Z}_0}$ denotes the sequence of time instants of the successful transmissions. Now we introduce a lemma concerning the convergence of $J(z_m)$.

Lemma 4: Consider the dynamics of $J(t)$ in (20) and the DoS attacks in Assumptions 1 and 2 satisfying $1/T+\Delta/\tau_D<1$ with network sampling interval Δ as in (2). All the elements in the vector $J(z_m)$ converge to zero as $z_m\to\infty$ if R_r satisfies

$$R_r\begin{cases} >\left(1-\frac{1}{T}-\frac{\Delta}{\tau_D}\right)^{-1}c_r\Delta\log_2 e, & \text{if } c_r\geq 0 \\ \geq 0, & \text{if } c_r<0 \end{cases} \quad (29)$$

where c_r is the real part of λ_r and $r=1,2,\ldots,p$.

Proof: In this proof, we mainly show that $\|P(z_0,z_m)\|$ converges to zero as $z_m\to\infty$ when $1/T+\Delta/\tau_D<1$ and (29) holds, which implies the convergence of $J(z_m)$.

According to (24), (28) and exploiting that $m=T_S(z_0,z_m)$ in Lemma 3, we have

$$\begin{aligned} P_r(z_0,z_m) &= (2^{-R_r})^m U_r\Big(\sum_{k=1}^{m}\Delta_k\Big) \\ &= \left(e^{c_r(z_m-z_0)}/(2^{R_r})^m\right)V_r(z_m-z_0)\otimes W \\ &\leq \theta_r(\alpha_r)^{z_m-z_0}V_r(z_m-z_0)\otimes W \end{aligned} \quad (30)$$

where $\theta_r:=2^{\frac{R_r(\kappa+\eta\Delta)}{\Delta}}$. When $1/T+\Delta/\tau_D<1$ and (29) holds, the α_r in (30) satisfies

$$\alpha_r:=e^{c_r}/2^{R_r\frac{1-\frac{1}{T}-\frac{\Delta}{\tau_D}}{\Delta}}<1. \quad (31)$$

In view of $(\alpha_r)^tV_r(t)$ with $\alpha_r<1$ in (30), it is implied that there exist finite numbers C_0^r, C_1^r, and $\mu_r<0$ such that $P_r(z_0,z_m)\leq C_0^re^{\mu_r(z_m-z_0)}V_r(C_1^r)\otimes W$, and hence, we obtain that there exists finite C_2 and $\mu<0$ such that

$$\|J(z_m)\|\leq C_2e^{\mu(z_m-z_0)}\|J(z_0)\|. \quad (32)$$

Finally, we obtain the convergence of $J(z_m)$ when $z_m\to\infty$. ■

After proving the convergence of $J(z_m)$, now we introduce another lemma concerning the convergence of $J(t)$ and $e(t)$.

Lemma 5: Consider $J(t)$ and $e(t)$ whose dynamics are given by (20) and (23), respectively. Suppose that the DoS attacks in Assumptions 1 and 2 satisfy $1/T+\Delta/\tau_D<1$. If the bit rate R_r satisfies (29), then $J(t)$ and $e(t)$ converge exponentially to the origin.

Proof: According to (20), (32) and Lemma 2, for $z_m\leq t<z_{m+1}$, we have

$$\begin{aligned} \|J(t)\| &\leq e^{\bar{v}(t-z_m)}\|J(z_m)\|\leq e^{v(z_{m+1}-z_m)}\|J(z_m)\| \\ &= C_2e^{v(z_{m+1}-z_m)}e^{-\mu(z_{m+1}-z_m)}e^{\mu(z_{m+1}-z_0)}\|J(z_0)\| \\ &\leq C_2e^{v(Q+\Delta)}e^{-\mu(Q+\Delta)}e^{\mu(z_{m+1}-z_0)}\|J(z_0)\| \\ &\leq \gamma_0e^{\mu(t-z_0)}\|J(z_0)\| \end{aligned} \quad (33)$$

where $v=\max\{0,\bar{v}\}$ with $\bar{v}=\lambda_{\max}(\frac{\bar{A}+\bar{A}^{\mathrm{T}}}{2})$ denoting the logarithmic norm of $\bar{A}$ and $\gamma_0:=C_2e^{v(Q+\Delta)}e^{-\mu(Q+\Delta)}$. Since γ_0 is finite and $\mu<0$, we conclude that $J(t)$ exponentially converges to the origin when $t\to\infty$. In light of (27), one could also obtain

$$\|e(t)\|\leq\|J(t)\|\leq\gamma_0e^{\mu(t-z_0)}\|J(z_0)\| \quad (34)$$

which implies the convergence of $e(t)$. ■

C. Main Result

Now we are ready to present the main result of this article.

Theorem 2: Consider the linear time-invariant process (1) and its transformed system (3) with control action (19)–(21) under the transmission policy in (2). The transmitted signals are quantized by the uniform quantizer (15) and (16). Suppose that the DoS attacks characterized in Assumptions 1 and 2 satisfy $1/T+\Delta/\tau_D<1$. If the bit rate R_r with $r=1,2,\ldots,p$ satisfies (29) then the state of the closed-loop system exponentially converges to the origin.

Proof: Recall the control input $u(t) = \bar{K}(t)\hat{x}(t) = KS^{-1}E(t)^{-1}\hat{x}(t) = K\widetilde{x}(t)$, where $\widetilde{x}(t) = S^{-1}E(t)^{-1}\hat{x}(t)$ can be interpreted as the estimation of the original process state $x(t)$ in (1). Then, one has the discrepancy between $\widetilde{x}(t)$ and $x(t)$ such that $\widetilde{e}(t) := \widetilde{x}(t) - x(t)$. Thus, (1) can be rewritten as $\dot{x}(t) = (A + BK)x(t) + BK\widetilde{e}(t)$, whose solution is

$$x(t) = e^{(A+BK)(t-z_0)}x(z_0) + \int_{z_0}^{t} e^{(A+BK)(t-\tau)}BK\widetilde{e}(\tau)d\tau \quad (35)$$

where $t \in \mathbb{R}_{\geq z_0}$. From the equation above, one can see that the stability of $x(t)$ depends on $\widetilde{e}(t)$. Thus, we analyze $\widetilde{e}(t)$ such that $\widetilde{e}(t) = \widetilde{x}(t) - x(t) = S^{-1}E(t)^{-1}\hat{x}(t) - S^{-1}E(t)^{-1}\bar{x}(t) = S^{-1}E(t)^{-1}(\hat{x}(t) - \bar{x}(t)) = S^{-1}E(t)^{-1}e(t)$. Since $1/T + \Delta/\tau_D < 1$ and R_r satisfies (29), then the inequalities in (34) hold. Therefore, one has $\|\widetilde{e}(t)\| \leq \|S^{-1}E(t)^{-1}\|\|e(t)\| \leq \|S^{-1}E(t)^{-1}\|\gamma_0 e^{\mu(t-z_0)}\|J(z_0)\| \leq \gamma_1 e^{\mu(t-z_0)}\|J(z_0)\|$, where $\gamma_1 > 0$. Note that such γ_1 exists and is finite since $\|S^{-1}E(t)^{-1}\|$ is bounded. Since $A + BK$ is Hurwitz, there exist finite reals $\beta \geq 1$ and $\sigma < 0$ such that $\|e^{(A+BK)t}\| \leq \beta e^{\sigma t}$ for $t \geq 0$. Using this inequality together with (35) and $\|\widetilde{e}(t)\| \leq \gamma_1 e^{\mu(t-z_0)}\|J(z_0)\|$, we obtain

$$\begin{aligned}
\|x(t)\| \leq\ & \beta e^{\sigma(t-z_0)}\|x(z_0)\| \\
& + \int_{z_0}^{t} \beta e^{\sigma(t-\tau)}\|BK\|\gamma_1 e^{\mu(\tau-z_0)}\|J(z_0)\|d\tau \\
\leq\ & \beta e^{\bar{\xi}(t-z_0)}\|x(z_0)\| \\
& + \int_{z_0}^{t} \beta e^{\bar{\xi}(t-\tau)}\|BK\|\gamma_1 e^{\bar{\xi}(\tau-z_0)}\|J(z_0)\|d\tau \\
\leq\ & \beta e^{\bar{\xi}(t-z_0)}\|x(z_0)\| \\
& + \beta(t-z_0)e^{\bar{\xi}(t-z_0)}\gamma_1\|BK\|\|J(z_0)\| \qquad (36)
\end{aligned}$$

where $\bar{\xi} := \max\{\mu, \sigma\} \in \mathbb{R}_{<0}$. Since $\bar{\xi} < 0$, there exist two finite reals δ satisfying $\bar{\xi} < \delta < 0$ and C_3 such that $(t - z_0)e^{\bar{\xi}(t-z_0)} \leq C_3 e^{\delta(t-z_0)}$. Then, we have

$$\|x(t)\| \leq e^{\delta(t-z_0)}(\beta\|x(z_0)\| + C_3\beta\gamma_1\|BK\|\|J(z_0)\|). \quad (37)$$

It is immediate to see that $x(t)$ exponentially converges to the origin as $t \to \infty$.

Moreover, in view of (33) and (34), and the fact that $\bar{x}(t) = E(t)Sx(t)$ and $\|\hat{x}(t)\| \leq \|e(t)\| + \|\bar{x}(t)\|$, we conclude that $J(t)$, $e(t)$, $\bar{x}(t)$, $\hat{x}(t)$, and $x(t)$ exponentially converge to the origin as $t \to \infty$. ■

Remark 3: We emphasize that this theorem characterizes how the bit rate influences the system's resilience. Condition (29) can be rewritten as

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < 1 - \frac{c_r \Delta \log_2 e}{R_r}, \quad \forall c_r \geq 0 \quad (38)$$

where $R_r > 0$. The inequality above explicitly quantifies how the data rate affects the robustness, e.g., the larger R_r, the smaller T, and τ_D can be, which implies that the system can tolerate more DoS attacks in terms of duration and frequency, and still preserve stability. Fig. 3 exemplifies this characterization. ■

Remark 4: In view of Theorem 2, if the network is reliable ($T = \tau_D = \infty$ and $\kappa = \eta = 0$), one obtains that the closed-loop system is exponentially stable if R_r satisfies

$$R_r \begin{cases} > c_r \Delta \log_2 e, & \text{if } c_r \geq 0 \\ \geq 0, & \text{if } c_r < 0 \end{cases} \quad r = 1, 2, \ldots, p. \quad (39)$$

To this end, we almost recover the results of minimum data rate obtained in [7], [8], and [10]. By "almost", we mean that if one omits disturbance and noise in [7], or convert our results into discrete-time form as in [8] and [10], then the data rates obtained in this article in the absence of DoS

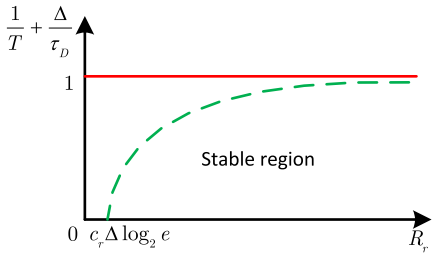

Fig. 3. Characterization of system resilience and data rate. The green-dashed curve is the function $1/T + \Delta/\tau_D = 1 - c_r \Delta \log_2 e / R_r$ with $c_r > 0$. If the pair $(R_r, 1/T + \Delta/\tau_D)$ is in the stable region (strictly under the green-dashed curve), then the system is stable. If $c_r = 0$, the stable region is in rectangular shape.

and the ones in the articles above are equivalent. This is the advantage of the result obtained in this article as we can recover the minimum data rate. By contrast, the article [25] considering data rates for the output-feedback scenario under DoS attacks cannot achieve this. ■

The parameters in Assumptions 1 and 2 can also be regarded as design parameters before the design of the encoding and decoding systems, and those parameters only specify the boundary within which an attacker behaves. Thus, if the attacks comply with the predefined boundary, the system with the data rate in (29) can achieve stability, even without the knowledge of the parameters of the attacks in real time.

Under Theorem 2, the average data rate associated with the successfully received packets is

$$\begin{aligned}
D_d &:= \lim_{z_m \to \infty} (z_m - z_0)^{-1} \sum_{l=1}^{n_x} \mathcal{R}_l T_S(z_0, z_m) \\
&> \sum_{k \in \{l | c_l \geq 0\}} c_k \log_2 e \qquad (40)
\end{aligned}$$

which essentially depends on the real parts of the unstable eigenvalues of the dynamic matrix of the process. The average data rate associated with the transmission attempts is

$$D_e := \sum_{l=1}^{n_x} \mathcal{R}_l/\Delta > \left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D}\right)^{-1} \sum_{k \in \{l | c_l \geq 0\}} c_k \log_2 e \quad (41)$$

which is the corresponding result under DoS attacks comparing with the achieved result in [32] where genuine packet dropout is considered. Moreover, under a 100% reliable network, one should have $D_e = D_d$. Due to DoS attacks, one may have $D_e > D_d$, and the lower bound of D_e is scaled by $(1 - 1/T - \Delta/\tau_D)^{-1} \in \mathbb{R}_{\geq 1}$. This reflects the need of redundant communication resources to compensate for the side effect of DoS attacks.

D. Stability Condition Over the Average Data Rate

In Theorem 2, we have shown the data rate conditions, under which the closed-loop system is stable. The setting there is that the number of bits transmitted at z_m ($m = 0, 1, \cdots$) are identical and equivalent to R_r. In this section, we loose the sufficient condition above in the sense that the number of bits at each z_m does not have to be identical. In particular, we show that if the average value of them is greater than $(1 - 1/T - \Delta/\tau_D)^{-1} c_r \Delta \log_2 e$ with $c_r \geq 0$, then the closed-loop system is still stable.

Assume that the number of bits assigned to each transmission attempt can change over time, and let $R_r(t_k)$ denote the number of bits applied to each element corresponding to $\bar{A}_r$ at t_k. Here, we introduce two notions of average data rates. One is the average over all transmission attempts $\widetilde{R}_{r,k} := (R_r(t_0) + R_r(t_1) +$

$\cdots + R_r(t_{k-1}))/k$ with $k = 1, 2, \cdots$. The other is over all successful transmissions $\bar{R}_{r,m} := (R_r(z_0) + R_r(z_1) + \cdots + R_r(z_{m-1}))/m$ with $m = 1, 2, \cdots$. Clearly, both averages will be finite if the maximum number of bits that the network can transmit in one transmission is finite, namely $R_r(t_k) < \infty$ for $k \in \mathbb{Z}_0$. In the current case, we use time-varying $\mathcal{R}_l$ in (15) for quantization.

Recall the definitions of $\{t_k\}_{k\in\mathbb{Z}_0}$ and $\{z_m\}_{m\in\mathbb{Z}_0}$. The proposition below presents a sufficient condition for stability concerning the average data rate.

Proposition 1: Under the transmission policy in (2), consider the process (1) and its transformed system (3) with control action (19)–(21) and the uniform quantizer (15) and (16), where R_r becomes $R_r(t_k)$ that are finite and possibly time-varying. The DoS attacks are characterized as in Assumptions 1 and 2 and satisfy $1/T + \Delta/\tau_D < 1$. If the average value of bits along $\{z_{m-1}\}_{m=1,2,\ldots}$ satisfies

$$\bar{R}_{r,m} \begin{cases} > (1 - 1/T - \Delta/\tau_D)^{-1} c_r \Delta \log_2 e, & \text{if } c_r \geq 0 \\ \geq 0, & \text{if } c_r < 0 \end{cases} \tag{42}$$

for $r = 1, 2, \ldots, p$, then the closed-loop system is stable.

Proof. By observing (30) and exploiting that $m = T_S(z_0, z_m)$ in Lemma 3, we could obtain that $P_r(z_0, z_m)$ under the average data rate scenario is given by

$$\begin{aligned} P_r(z_0, z_m) &= U_r\Big(\sum_{k=1}^{m} \Delta_k\Big) \prod_{k=1}^{m} 2^{-R_r(z_{k-1})} \\ &= \frac{e^{c_r(z_m - z_0)}}{\prod_{k=1}^{m} 2^{R_r(z_{k-1})}} V_r(z_m - z_0) \otimes W \\ &= \frac{e^{c_r(z_m - z_0)}}{(2^{\bar{R}_{r,m}})^m} V_r(z_m - z_0) \otimes W \\ &\leq \bar{\theta}_{r,m} (\bar{\alpha}_{r,m})^{z_m - z_0} V_r(z_m - z_0) \otimes W \end{aligned} \tag{43}$$

where $\bar{\theta}_{r,m} := 2^{\frac{\bar{R}_{r,m}(\kappa + \eta\Delta)}{\Delta}}$ is finite. When (42) holds, one has

$$\bar{\alpha}_{r,m} := e^{c_r} / 2^{\bar{R}_{r,m} \frac{1 - \frac{1}{T} - \frac{\Delta}{\tau_D}}{\Delta}} < 1. \tag{44}$$

The rest of the proof can follow the analysis after (31), and we obtain the stability of the closed-loop system. ■

It is worth mentioning that Proposition 1 concerns the sequence of $\{R_r(z_m)\}$ instead of $\{R_r(t_k)\}$. This expresses that the average value of bits of all the *successful* transmissions, namely $\bar{R}_{r,m}$ for $m = 1, 2, \ldots$, should satisfy (42), instead of the average value of bits of all the transmissions attempts $\widetilde{R}_{r,k}$. In fact, even if $\widetilde{R}_{r,k} > (1 - 1/T - \Delta/\tau_D)^{-1} c_r \Delta \log_2 e$, it is still possible that $\bar{R}_{r,m} \leq (1 - 1/T - \Delta/\tau_D)^{-1} c_r \Delta \log_2 e$ and instability may occur.

In practice, one can use (42) to compute the number of bits online, so that stability can be guaranteed. For example, the coding systems can precompute the number of bits right before each transmission attempt such that if the transmission attempt succeeds then (42) holds. In this case, the number of bits at the decoding side needs to be adjusted according to the received data size.

V. Numerical Example

For simplicity, we consider a process that is in Jordan form and taken from [33] and show the simulation results. The system to be controlled is open-loop unstable and is characterized by the matrices

$$A = \bar{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \bar{B}(t) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{45}$$

The state-feedback matrix is given by

$$K = \bar{K}(t) = \begin{bmatrix} -2.1961 & -0.7545 \\ -0.7545 & -2.7146 \end{bmatrix}. \tag{46}$$

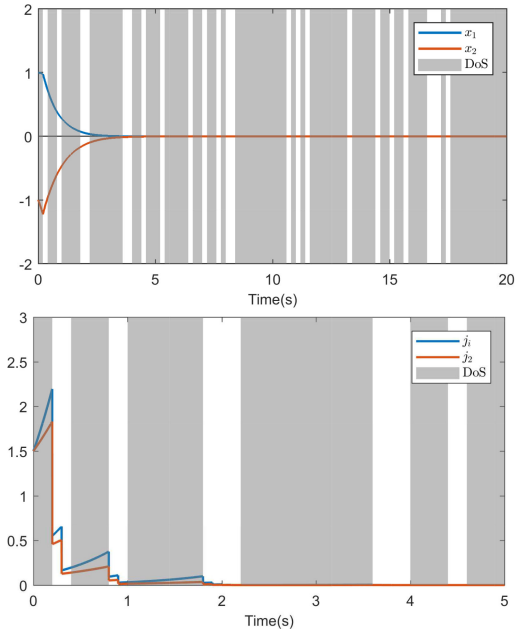

Fig. 4. Simulation plots of $x(t)$ (top) and $J(t)$ (bottom).

The network transmission interval is given by $\Delta = 0.1$ s. We consider a sustained DoS attack with variable period and duty cycle, generated randomly. Over a simulation horizon of 20 s, the DoS signal yields $|\Xi(0, 20)| = 15.52$ s and $n(0, 20) = 20$. This corresponds to values (averaged over 20 s) of $\tau_D \approx 0.96$ and $T \approx 1.29$, and $\sim 80\%$ of transmission failures. It is simple to verify that $\Delta/\tau_D + 1/T \approx 0.8793$.

According to Theorem 2, we obtain that

$$R_1 > (1 - 1/T - \Delta/\tau_D)^{-1} c_r \Delta \log_2 e = 1.1953. \tag{47}$$

Then, we select $R_1 = 2$. The simulation results of $x(t)$ and $J(t)$ (0–5 s) are shown in Fig. 4. It is clear that the closed-loop system is stable. From another viewpoint, if the data rate of the channel is preselected as $R_1 = 2$, the closed-loop system should be stable under the attacks in this example since the DoS parameters satisfy $1/T + \Delta/\tau_D \approx 0.8793 < 1 - c_1 \Delta \log_2 e / R_1 = 0.9279$.

In fact, the obtained value of bit rate is conservative. The stability can be still preserved at the lower rate with $R_1 = 1$ under the same pattern of DoS attacks. One factor contributing to the conservativeness is that the actual number of successful transmissions is much larger than the theoretical value computed in Lemma 3.

VI. Conclusion

We investigated the tradeoff problem for stabilizing control of a networked control system under limited bandwidth and DoS attacks. It was shown that the sufficient condition of bit rate for stabilization depends on the unstable eigenvalues of the dynamic matrix of the process as well as DoS attacks. It is emphasized that the results of this article clearly indicate the tradeoffs between the amount of transmitted data and the robustness against DoS attacks. In particular, the approach is in accordance with the recent studies on the minimum data rate control problems.

In the future, disturbance, noise, transmission error, random dropouts, and output feedback might be taken into consideration. One could also consider the scenario of unreliable acknowledgment as in [34], under which signal desynchronization between encoder and decoder might happen. Moreover, transmission delays and system dynamics with uncertainties could be investigated by following the analysis in [13] and [35].

APPENDIX

The Appendix is for presenting the matrices S and $E(t)$ in (4). For the calculation of (4) to (6), we refer the readers to [8], [36] and [37], where time-varying transformations are applied.

The matrix $S \in \mathbb{R}^{n_x \times n_x}$ is a transformation matrix such that $\widetilde{A} = SAS^{-1} = \text{diag}(A_1, A_2, \ldots, A_p) \in \mathbb{R}^{n_x \times n_x}$ is the Jordan form of A [38]. If A_r in $\widetilde{A}$ is associated with the real eigenvalue $\lambda_r = c_r$, then A_r equals to the right-hand side of (5). If A_r in $\widetilde{A}$ is associated with the complex eigenvalues $\lambda_r = c_r \pm d_r i$ ($d_r \neq 0$), then one has

$$A_r = \begin{bmatrix} D_r & I & & \\ & D_r & I & \\ & & \ddots & I \\ & & & D_r \end{bmatrix} \in \mathbb{R}^{2n_r \times 2n_r}, D_r = \begin{bmatrix} c_r & -d_r \\ d_r & c_r \end{bmatrix}. \tag{48}$$

The matrix $E(t)$ is given by

$$E(t) = \text{diag}(E_1(t), E_2(t), \ldots, E_p(t)) \in \mathbb{R}^{n_x \times n_x} \tag{49}$$

where $E_r(t) = \text{diag}(1, 1, \ldots, 1) \in \mathbb{R}^{n_r \times n_r}$ corresponds to the real eigenvalue $\lambda_r = c_r$, or $E_r(t) = \text{diag}(\varpi_r(t), \varpi_r(t), \ldots, \varpi_r(t)) \in \mathbb{R}^{2n_r \times 2n_r}$ corresponds to the complex eigenvalues $\lambda_r = c_r \pm d_r i$ ($d_r \neq 0$) with

$$\varpi_r(t) = \begin{bmatrix} \cos(d_r t) & \sin(d_r t) \\ -\sin(d_r t) & \cos(d_r t) \end{bmatrix}. \tag{50}$$

■

REFERENCES

[1] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. De Persis, "Networked control under DoS attacks: Trade-off between resilience and data rate," in *Proc. Amer. Control Conf.*, 2019, pp. 378–383.

[2] P. Cheng, L. Shi, and B. Sinopoli, "Guest editorial: Special issue on secure control of cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 1–3, Mar. 2017.

[3] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[4] P. Antsaklis and J. Baillieul, "Guest editorial: Special issue on networked control systems," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1421–1423, Sep. 2004.

[5] 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, 2007.

[6] S. Amin, A. Càrdenas, and S. Sastry, "Safe and secure networked control systems under Denial-of-Service attacks," in *Int. Workshop Hybrid Syst.: Comput. Control*, 2009, pp. 31–45.

[7] J. Hespanha, A. Ortega, and L. Vasudevan, "Towards the control of linear systems with minimum bit-rate," in *Proc. Int. Symp. Math. Theory Netw. Syst*, 2002.

[8] S. Tatikonda and S. Mitter, "Control under communication constraints," *IEEE Trans. Autom. Control*, vol. 49, no. 7, pp. 1056–1068, Jul. 2004.

[9] D. Liberzon, "On stabilization of linear systems with limited information," *IEEE Trans. Autom. Control*, vol. 48, no. 2, pp. 304–307, Feb. 2003.

[10] G. N. Nair and R. J. Evans, "Stabilizability of stochastic linear systems with finite feedback data rates," *SIAM J. Control Optim.*, vol. 43, no. 2, pp. 413–436, 2004.

[11] P. Tallapragada and J. Cortés, "Event-triggered stabilization of linear systems under bounded bit rates," *IEEE Trans. Autom. Control*, vol. 61, no. 6, pp. 1575–1589, Jun. 2016.

[12] K. You and L. Xie, "Minimum data rate for mean square stabilizability of linear systems with Markovian packet losses," *IEEE Trans. Autom. Control*, vol. 56, no. 4, pp. 772–785, Apr. 2011.

[13] K. Okano and H. Ishii, "Stabilization of uncertain systems with finite data rates and Markovian packet losses," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 298–307, Dec. 2014.

[14] K. You and L. Xie, "Minimum data rate for mean square stabilization of discrete LTI systems over lossy channels," *IEEE Trans. Autom. Control*, vol. 55, no. 10, pp. 2373–2378, Oct. 2010.

[15] Q. Ling, "Bit-rate conditions to stabilize a continuous-time linear system with feedback dropouts," *IEEE Trans. Autom. Control*, vol. 63, no. 7, pp. 2176–2183, Jul. 2018.

[16] P. Minero, L. Coviello, and M. Franceschetti, "Stabilization over Markov feedback channels: The general case," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 349–362, Feb. 2013.

[17] S. Yuksel and T. Basar, "Minimum rate coding for LTI systems over noiseless channels," *IEEE Trans. Autom. Control*, vol. 51, no. 12, pp. 1878–1887, Dec. 2006.

[18] 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.

[19] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 981–990, Sep. 2018.

[20] C. De Persis and P. Tesi, "Networked control of nonlinear systems under Denial-of-Service," *Syst. Control Lett.*, vol. 96, pp. 124–131, 2016.

[21] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2434–2449, May 2017.

[22] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal Denial-of-Service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[23] K. Ding, Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A multi-channel transmission schedule for remote state estimation under DoS attacks," *Automatica*, vol. 78, pp. 194–201, 2017.

[24] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

[25] M. Wakaiki, A. Cetinkaya, and H. Ishii, "Quantized output feedback stabilization under DoS attacks," in *Proc. Amer. Control Conf.*, 2018, pp. 6487–6492.

[26] S. Feng and P. Tesi, "Resilient control under Denial-of-Service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[27] S. Feng and P. Tesi–, "Resilient control under Denial-of-Service: Robust design," in *Proc. Amer. Control Conf.*, 2016, pp. 4737–4742.

[28] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Analysis of stochastic switched systems with application to networked control under jamming attacks," *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 2013–2028, May 2019.

[29] A. Y. Lu and G. H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under Denial-of-Service," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1813–1820, Jun. 2018.

[30] S. Feng and P. Tesi, "Networked control systems under Denial-of-Service: Co-located vs. remote architectures," *Syst. Control Lett.*, vol. 108, pp. 40–47, 2017.

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

[32] S. Tatikonda and S. Mitter, "Control over noisy channels," *IEEE Trans. Autom. Control*, vol. 49, no. 7, pp. 1196–1201, Jul. 2004.

[33] 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 *Proc. IEEE Conf. Decis. Control*, 2010, pp. 6469–6474.

[34] H. Lin, H. Su, P. Shi, Z. Shu, R. Lu, and Z.-G. Wu, "Optimal estimation and control for lossy network: Stability, convergence, and performance," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4564–4579, Sep. 2017.

[35] K. Liu, E. Fridman, and K. H. Johansson, "Dynamic quantization of uncertain linear networked control systems," *Automatica*, vol. 59, pp. 248–255, 2015.

[36] F. Mazenc and O. Bernard, "Interval observers for linear time-invariant systems with disturbances," *Automatica*, vol. 47, no. 1, pp. 140–147, 2011.

[37] J. Pearson, J. P. Hespanha, and D. Liberzon, "Control with minimal cost-per-symbol encoding and quasi-optimality of event-based encoders," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2286–2301, May 2017.

[38] L. Perko, *Differential Equations and Dynamical Systems*. Berlin, Germany: Springer, 2013.