Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Towards the Coarsest Quantized Controller under Denial-of-Service Attacks

Dorus van Dinther * **Shuai Feng** ** **Hideaki Ishii** **
W. P. M. H. (Maurice) Heemels *

* *Control Systems Technology group, Dept. of Mechanical Eng., Eindhoven University of Technology, Eindhoven 5600 MB, The Netherlands.* {d.v.dinther@student., m.heemels@}tue.nl.
** *Dept. of Computer Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan.* {feng@sc.dis, ishii@c}.titech.ac.jp.

Abstract: In this paper, we consider networked control systems under Denial-of-Service (DoS) attacks. The control objective is to synthesize a quantized controller in which the quantizer is as coarse as possible for a networked control system subject to DoS attacks, while still guaranteeing (quadratic) stability. Our main result will explicitly show the trade-offs between system robustness against DoS and quantizer coarseness. A simulation example will demonstrate the strengths of the new method.

Keywords: Denial-of-Service attacks, secure networked control systems, control and estimation with data loss, control under communication constraints

1. INTRODUCTION

In recent years, there is an increasing number of reports regarding the malfunctions of networked control systems (Cárdenas et al. (2008); Sandberg et al. (2015); Cheng et al. (2017)), thereby spurring the interest of designing secure control systems that are resilient to attacks. In particular, a large number of security issues are caused by cyber attacks. The attacks mostly affect the exchange of data by corrupting their confidentiality, authenticity, and availability.

This paper is particularly interested in Denial-of-Service (DoS) attacks, which affect the availability of data, in combination with quantization over the input channel of the plant, see Fig. 1. These attacks jam the communication channels, causing packets to be dropped and hence a (temporal) loss of communication, see, e.g., De Persis and Tesi (2015); Dolk et al. (2017), which considered the stabilizing control problems under unlimited data-rate networks subject to DoS attacks. Motivated by bit-rate limitations of the communication channels, other studies have been conducted regarding the permissible coarseness of quantized signals for stabilization, such as Brockett and Liberzon (2000); Elia and Mitter (2001); Liberzon (2003); Fu and Xie (2005).

However, relatively little work is done on quantized control under DoS attacks. In Wakaiki et al. (2018), the case of quantized control under DoS attacks over the output channel of the plant is investigated, whereas in Feng et al. (2020) the minimum data rate is derived following the line of research of, e.g., Nair et al. (2007). To the best of the authors' knowledge, there have not been any studies into the problem tackled in this paper, consisting of the design of coarse stabilizing quantized control under DoS attacks over the input channel of the plant. In particular, we are interested in the system setting depicted in Fig. 1, of which more details follow in the next section.

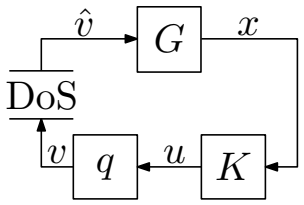

Fig. 1. Control architecture.

Note that quantized control under random packet losses was addressed in Tsumura et al. (2009). Non-quantized networked control systems that experience random packet losses are discussed extensively in Hespanha et al. (2007); Schenato et al. (2007); Zhang et al. (2013). However, DoS attacks can be sophistically organized and launched intelligently, in the sense that attackers would try to maximize the influence of attacks. Therefore describing an adversary's behaviour using stochastic processes such as random packet losses is hardly justified. This motivates the development of a new theoretical analysis for quantized networked control systems under DoS since the classical probability and expectation type analyses are not applicable in the context of DoS attacks launched by a malicious adversary.

Our contributions in this paper form a step towards solving the problem of finding the coarsest possible quantizer that stabilizes the system, when the maximum duration of the DoS attack is known. In fact, we consider a more

⋆ This work was supported in the part by the JST CREST Grant No. JPMJCR15K3 and by JSPS under Grant-in-Aid for Scientific Research Grant No. 18H01460.

conservative problem, by only looking at solutions using a common quadratic Lyapunov function in order to find solutions. As our main result, we present a finite-level time-varying quantizer, which ensures quadratic stability of the closed-loop system. We illustrate the main results through a numerical example.

The remainder of this paper is organized as follows. In Section 2, we present the problem setting of this paper, where the process, the class of quantizers and DoS attacks are introduced. Section 3 presents a result concerning static quantized control under DoS, where the number of quantization levels are infinite. In Section 4, we present the main result of this paper. We first propose the design of a dynamic quantized controller with finite quantization levels, and then characterize the system robustness against DoS. A numerical example is given in Section 5, and Section 6 concludes the paper with possible future research directions. Due to space reasons, we do not present the proofs.

Notation: The sets of reals and integers are denoted by $\mathbb{R}$ and $\mathbb{Z}$, respectively. Let $\mathbb{Z}^+ := \{0, 1, 2, \ldots\}$ denote the set of nonnegative integers. Given a vector v, $\|v\|$ denotes the Euclidean norm of the vector v. The notations $\lambda_{\min}(M)$ and $\lambda_{\max}(M)$ denote the minimum and maximum eigenvalues of matrix M, respectively.

2. FRAMEWORK

In this section, we will first describe the overall problem setting. Then, we introduce the class of quantizers considered and their coarseness, as well as an assumption on the DoS model. The combination of these notions is then used to formulate the problem studied in this paper.

2.1 General problem setup

Consider the discrete-time networked control system depicted in Fig. 1. Here, the process $\mathcal{G}$ is represented by the state space equation given by

$$\mathcal{G}: \quad x_{k+1} = Ax_k + B\hat{v}_k, \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the process state and $\hat{v}_k \in \mathbb{R}$ is the control input at time $k \in \mathbb{Z}^+$. Assume that the matrix pair (A, B) is controllable. Moreover, to avoid trivial situations, we assume the system to be unstable, that is, the system matrix A has at least one eigenvalue with magnitude greater or equal to one.

The control input is sent from the sensor side, where the state feedback controller is located, to the actuator side. This communication is constrained due to the limited data rate available in the channel as well as the uncertainties caused by the DoS attacks. First, the control input u_k is generated by using the state feedback gain K as

$$u_k = Kx_k. \tag{2}$$

Before transmitted over the channel, this input u_k is quantized so that it takes a discrete value. Specifically, let $\mathcal{Q}$ be a countable set in $\mathbb{R}$ and let $q : \mathbb{R} \to \mathcal{Q}$ be the quantizer. Then,

$$v_k = q(u_k). \tag{3}$$

Finally, in the presence of DoS attacks, the input v_k sent over the network may be dropped and not reach the actuator side. This is expressed by

$$\hat{v}_k = \sigma_k v_k, \tag{4}$$

where σ_k is the indicator of the DoS at time k. If the transmission fails due to DoS, then $\sigma_k = 0$, and otherwise $\sigma_k = 1$. Note that we assume that when there is no input in case of DoS, the input is zero.

In this paper, we would like to synthesize both the feedback gain K and the quantizer q such that the quantizer is as coarse as possible, as defined in the next section, while still guaranteeing quadratic stability of the overall closed-loop system under a DoS attack model in line with those in De Persis and Tesi (2015); Dolk et al. (2017).

2.2 Quantizer class and coarseness

Our study is motivated by the research on logarithmic quantizers initiated by Elia and Mitter (2001). We introduce the class of memoryless quantizers accompanied with a one-bit memory. The memory is necessary to deal with the packet losses due to the DoS attacks, storing the information that whether or not the system (1) experienced DoS in the previous time-step.

As we will see later, the first quantizer presented in Section 3 is a static but infinite one. That is, the quantizer mapping is time-invariant and its output set $\mathcal{Q}$ is countable, containing an infinite number of quantization levels, i.e., its cardinality is $\text{card}(\mathcal{Q}) = \infty$. The coarseness of such an infinite quantizer q scales inversely with its quantization density, defined in the following:

***Definition* 1.** [Elia and Mitter (2001)] Given a quantizer $q : \mathbb{R} \to \mathcal{Q}$, its density is given by

$$d = \limsup_{\varepsilon \to 0} \frac{\text{card}(q([\varepsilon, 1/\varepsilon]))}{-\ln \varepsilon},$$

where $\text{card}(q([\varepsilon, 1/\varepsilon]))$ denotes the number of quantization levels in $\mathcal{Q}$ of the quantizer $q(\cdot)$ in the interval $[\varepsilon, 1/\varepsilon]$.

Hence, the coarsest quantizer q would have the lowest quantization density d.

The main result in Section 4 presents a dynamic finite-level quantizer, where the coarseness is based on its underlying infinite-level version. That is, the dynamic quantizer mapping is time-dependent and $\text{card}(\mathcal{Q}) < \infty$. Throughout this paper, we assume that the quantizer is symmetric, i.e., $q(u) = -q(-u)$ for all $u \in \mathbb{R}$.

2.3 The model of DoS attacks

Clearly, if the attacker can generate DoS all the time, feedback control would not be possible. Hence, we impose a constraint on the duration of the DoS attacks.

***Assumption* 1.** [De Persis and Tesi (2015)] There exist $\Pi_d \geq 0$ and $\nu_d \in [0, 1]$ such that for $k \in \mathbb{Z}^+$, the duration of DoS attacks satisfies

$$\Phi_d(k) \leq \Pi_d + \nu_d k, \tag{5}$$

where $\Phi_d(k) = \sum_{p=0}^{k}(1 - \sigma_p)$ denotes the DoS duration in the number of samples on $[0, k]$ that experience DoS. Here Π_d does not scale with k and therefore provides the attacker with an initial budget, whereas the second term $\nu_d k$ does scale with the amount of samples k, which limits the percentage of samples that DoS is allowed. Note that

(5) does not have to satisfy any probability distribution as in the random packet-loss case.

***Remark* 1.** The works by De Persis and Tesi (2015); Dolk et al. (2017) have studied networked control under DoS in the continuous-time domain. There, to describe DoS attacks, an additional assumption on the frequency of them is required. This is needed in the continuous-time problem setting, where there is a possibility that the duration of a DoS attack is small, but the attackers emit considerably many pulse-like DoS attacks, which could still corrupt *all* communication attempts. In this paper, the DoS model is considered in the discrete-time setting and therefore the above situation is not present.

2.4 The coarsest quantizer without DoS attacks

The notion of density of static quantizers has gained much attention since the work by Elia and Mitter (2001) that derived the infimum density value analytically while still guaranteeing quadratic stability. The bound is expressed by the unstable eigenvalues of the process to be stabilized, explicitly showing that more unstable systems require more dense quantization and thus more communication. We briefly outline their result in the following since it will serve as the starting point for our study.

Consider the process in (1) under the quantized control input v_k when no DoS attack is present. That is, we assume $\sigma_k = 1$ for all $k \in \mathbb{Z}^+$ so that the control input becomes $\hat{v}_k = u_k = q(Kx_k)$. For this system $x_{k+1} = Ax_k + Bq(Kx_k)$, we say that it is quadratically stable if there exists a quadratic Lyapunov function $V(x) = x^T P x$ with a positive-definite matrix P such that $V(Ax + Bq(Kx)) - V(x) < 0$ for each $x \in \mathbb{R}^n \setminus \{0\}$.

The paper by Elia and Mitter (2001) showed that the coarsest quantizer for the quadratic stabilization, i.e., where there exists K such that $x_{k+1} = Ax_k + Bq(Kx_k)$ is quadratically stable, in this case has two characteristics: One is that the quantizer belongs to a logarithmic type of the form

$$q(u) = \begin{cases} v_i & \text{if } u \in \left(\dfrac{\rho+1}{2\rho} v_i, \dfrac{\rho+1}{2} v_i \right], \\ -v_i & \text{if } u \in \left[-\dfrac{\rho+1}{2} v_i, -\dfrac{\rho+1}{2\rho} v_i \right), \\ 0 & \text{if } u = 0, \end{cases} \tag{6}$$

where $\rho > 1$ is the expansion ratio and the discrete-valued outputs are given by $v_i = \rho^i v_0$ for $i \in \mathbb{Z}$ with $v_0 > 0$. Moreover, the largest, or the coarsest, expansion ratio $\rho^*_{\sup} > 1$ under which quadratic stabilization is possible (which is formally defined later) is expressed as

$$\rho^*_{\sup} = \frac{\prod_i |\lambda^u_i| + 1}{\prod_i |\lambda^u_i| - 1}, \tag{7}$$

where λ^u_i denote the unstable eigenvalues of A.

Note that the output set of the quantizer in (6) is given by $\mathcal{Q} = \{\pm v_i \mid i \in \mathbb{Z}\} \cup \{0\}$.

2.5 Problem formulation

When DoS attacks are successful in inducing packet losses, clearly the problem setting and the conditions for quadratic stabilization as given in Section 2.4 change and the largest expansion ratio $\rho^*_{\sup}$ in (7) may not be sufficient.

Hence, in this paper, the first question of interest is whether the networked control system in Fig. 1 with quantized control (3) and DoS attacks (4) under Assumption 1 can be quadratically stabilized by a suitable K. In particular, given the DoS attack parameters $\Pi_d \geq 0$ and $\nu_d \in [0, 1]$, we would like to find the largest expansion ratio $\rho_{\sup}(\Pi_d, \nu_d) \leq \rho^*_{\sup}$ for the quantization, such that quadratic stabilization is still possible.

This problem however turns out to be difficult to address. In this paper, we solve a slightly weaker version of this problem and find whether stabilization is possible for a given expansion ratio $\rho \in (1, \rho^*_{\sup}]$. This will be conducted in a manner consistent with the framework of Elia and Mitter (2001): If the level of DoS attacks goes down as $\Pi_d, \nu_d \to 0$, then the expansion ratio $\rho_{\sup}(\Pi_d, \nu_d)$ approaches $\rho^*_{\sup}$, that is, $\rho_{\sup}(0, 0) = \rho^*_{\sup}$. In this respect, our result to be presented in the next section can be seen as a generalization of the conventional result in Elia and Mitter (2001).

3. STATIC QUANTIZER DESIGN

In this section, we provide the solution to the problem of designing the static quantized control scheme for quadratic stabilization under DoS attacks, when $\rho \in (1, \rho^*_{\sup}]$ is fixed.

Given the DoS attack parameters $\Pi_d \geq 0$ and $\nu_d \in [0, 1]$, for the logarithmic quantizer (6), take the quantization expansion ratio satisfying $\rho \in (1, \rho^*_{\sup}]$. Then, we let

$$\gamma = \frac{\rho + 1}{\rho - 1}, \quad \beta = \left(\frac{\prod_i |\lambda^u_i|}{\gamma} \right)^{2/m}, \tag{8}$$

where λ^u_i with $i = 1, \ldots, m$ are the unstable eigenvalues of A. Moreover, take $A_\beta = A/\sqrt{\beta}$. Then, there exists a positive-definite matrix P satisfying the matrix inequality

$$A^T_\beta P A_\beta - P - \left(1 - \frac{1}{\gamma^2} \right) \frac{A^T_\beta P B B^T P A_\beta}{B^T P B} < 0. \tag{9}$$

The existence of such P can be shown since by the choice of ρ, it holds $\gamma > \prod_i^m |\lambda^u_i / \sqrt{\beta}|$ (see, e.g., Ishii (2006)). Now, for the control input u in (2), we use the feedback gain given by $K = -B^T P A / (B^T P B)$. This is known as the controller that makes the Lyapunov function $V(x) = x^T P x$ decrease the most when no quantization and no DoS are introduced in the control.

Next, with this matrix P, we define the parameter α by

$$\alpha := \lambda_{\max}(P^{-\frac{1}{2}} A^\top P A P^{-\frac{1}{2}}). \tag{10}$$

Here is the main result of this section for the design of the static quantizer.

***Theorem* 1.** Consider the process (1) under the quantized control and DoS in (2)–(4) with the logarithmic type quantizer in (6) with expansion ratio $\rho \in (1, \rho^*_{\sup}]$. Suppose that Assumption 1 holds. If $K = -B^T P A / (B^T P B)$ and the DoS parameter ν_d satisfies

$$\nu_d < \frac{-\ln \beta}{\ln \alpha - \ln \beta} =: \bar{\nu}_d, \tag{11}$$

then the system (1) is quadratically stable.

***Remark* 2.** We note that the results in Theorems 1 and 2 (the latter follows in the next section) do not present the coarsest possible quantizer under a given duration of the DoS attacks, as the solution to P in (9) is not unique. Hence, a different P satisfying (9) results in a different α in (10), leading to a different bound $\bar{\nu}_d$ in (11).

To establish the theorem, we will exploit the quadratic Lyapunov function $V(x) = x^T P x$ using the solution to the matrix inequality in (9). This function will decrease while there is no attack, while it may increase when DoS attacks are launched. In particular, with the parameters α in (10) and β in (8), we can show that the following inequalities hold:

$$\begin{cases} \text{DoS present:} & V(Ax_k) \le \alpha V(x_k) \\ \text{DoS absent:} & V(Ax_k + Bq(Kx_k)) \le \beta V(x_k). \end{cases} \tag{12}$$

We now present three lemmas that relate the change in the Lyapunov function depending on the DoS modes in (12). First, the divergence rate of $V(x)$ during attacks can be characterized as follows.

***Lemma* 1.** Given a Lyapunov function $V(x) = x^\top P x$, with positive-definite P, the smallest α satisfying the inequality $V(Ax) \le \alpha V(x)$ for all $x \in \mathbb{R}^n$ is given by

$$\alpha = \lambda_{\max}(P^{-\frac{1}{2}} A^\top P A P^{-\frac{1}{2}}).$$

We next consider the case when there is no DoS attack. The next lemma is a corollary of the result characterizing the coarsest quantizer discussed earlier and is derived in Elia and Mitter (2001). It shows the coarsest quantizer having the largest expansion ratio for achieving quadratic stability with guaranteed decay rate of β.

***Lemma* 2.** The coarsest quantizer q, which can achieve quadratic stability with decay rate $\beta \in (0,1)$, i.e., $V(Ax + Bq(Kx)) \le \beta V(x)$ for all $x \in \mathbb{R}^n$ and for some $V(x) = x^\top P x$ with $P > 0$ and some feedback gain K in the case when there are no DoS attacks, is of the form of (6) and characterized by the expansion ratio $\rho_{\sup}$ given by

$$\rho_{\sup} = \frac{\gamma_{\inf} + 1}{\gamma_{\inf} - 1}, \quad \gamma_{\inf} = \prod_i \left| \frac{\lambda_i^u}{\sqrt{\beta}} \right|. \tag{13}$$

More specifically, for any $\rho \in (1, \rho_{\sup})$, the solution $P > 0$ to the matrix inequality in (9) exists, with which it holds that $V(Ax + Bq(Kx)) \le \beta V(x)$ with the feedback gain $K = -B^T P A / (B^T P B)$.

Note that the definitions in (13) are obtained by reversing (8). By setting $\beta = 1$ in this result, the largest expansion ratio $\rho^*_{\sup}$ for achieving quadratic stabilization given in (7) can be obtained.

Finally, in view of the bounds on the changes in the Lyapunov function $V(x_k)$ in the presence/absence of DoS attacks in (12), we can relate them to the DoS duration bound as follows.

***Lemma* 3.** Suppose that the duration of the DoS attacks are bounded as in Assumption 1. Then, the Lyapunov function $V(x_k)$ satisfying the bounds in (12) characterized by $\alpha > 1$ and $\beta \in (0,1)$ exponentially decreases if the DoS parameter ν_d satisfies (11).

The proof of Theorem 1 now follows by combining the three lemmas above.

4. FINITE-LEVEL TIME-VARYING QUANTIZER

In this section, we focus on an implementable finite-level quantizer. It has a dynamic structure and uses the same coarseness as the static one in the previous section. The coarsest quantizer defined in Section 3 has an infinite number of quantization levels. This is mostly because the quantization steps become infinitesimally small as $u \to 0$. Moreover, no upper bound on the quantizer output is defined. Both of these issues should be resolved for the coarse quantizers to be implemented in a real system.

Here, we introduce a time-varying variant of the logarithmic quantizer having finite levels and develop a quantized control scheme for quadratically stabilizing the process $\mathcal{G}$ in (1). The finite-level logarithmic quantizer is expressed as follows. First, it has two parameters: A positive integer $N \in \mathbb{Z}^+$ and the initial quantized output $v_0 > 0$. Its output set is given by $\mathcal{Q}_N = \{\pm v_i \mid i = 0, 1, \dots, N-1\} \cup \{0\}$. Then, let the finite-level quantizer $q_{v_0} : [-(\rho+1)\rho^{N-1} v_0/2, (\rho+1)\rho^{N-1} v_0/2] \to \mathcal{Q}_N$ be given by

$$q_{v_0}(u) = \begin{cases} v_i, & u \in \left(\dfrac{\rho+1}{2\rho} v_i, \dfrac{\rho+1}{2} v_i \right], \\ -v_i, & u \in \left[-\dfrac{\rho+1}{2} v_i, -\dfrac{\rho+1}{2\rho} v_i \right), \\ 0, & u \in [-\epsilon, \epsilon], \end{cases} \tag{14}$$

where $v_i = \rho^i v_0$, $i = 0, 1, \dots, N-1$, $\epsilon = v_0(\rho+1)/(2\rho)$. Note that this quantizer has the same structure as the infinite-level logarithmic one in (6), but has a truncated output set $\mathcal{Q}_N$. In particular, the outputs are bounded from above and from below (larger than 0 in magnitude). Moreover, for small inputs $u \in [-\epsilon, \epsilon]$, the output will be approximated to zero.

In what follows, we will adopt the same level of coarseness for this quantizer as that in the previous section. Hence, by following the design procedure there and by Theorem 1, we take the expansion ratio ρ from the interval $(1, \rho^*_{\sup}]$.

To make this quantizer dynamic, we can use a time-varying parameter $v_0(k)$. In such a case, the control input v_k is given by $v_k = q_{v_0(k)}(Kx_k)$. The parameter $v_0(k)$ changes the domain and step widths of the quantization dynamically. This quantizer takes only a finite number $2N+1$ of quantization levels at each time. Moreover, the bit-rate necessary for updating $v_0(k)$ is finite, which is relevant because we are looking for minimal and implementable use of a communication network. Therefore, the proposed quantization method can be realized using finite capacity (Tsumura et al., 2009). This type of "zooming in/zooming out" quantization was first introduced in Brockett and Liberzon (2000).

The following preliminary result is presented. At first, take N large enough such that

$$N \ge \log_\rho \left(F_0 / \sqrt{\beta} \right),$$

where

$$F_0 := \frac{\sqrt{b_{\inf}}(\rho+1)|\mu_+|}{2\sqrt{\lambda_{\min}(P)}\|\tilde{Q}^{-1} A^\top P B\|}$$

and $b = b_{\inf}$ as in (Elia and Mitter, 2001, pp.1395–1397), i.e., the minimum positive solution to the LMI problem

$$\exists \tau > 0 : \; b\Gamma - \bar{A}^\top \bar{P} \bar{A} - \tau \Sigma \geq 0,$$

where $\Gamma = \mathrm{diag}(0, 0, \ldots, 0, 1) \in \mathbb{R}^{n \times n}$, $\bar{A} = T^{-1} A T$, $\bar{P} = T^\top P T$, and $\Sigma = \bar{A}^\top \bar{P} \bar{A} - \bar{P}$. Moreover

$$T = \begin{bmatrix} W & \dfrac{K^\top}{\|K\|^2} \end{bmatrix},$$

such that the columns of W span the orthonormal null-space of K.

Define the level set $L_V(c) = \{x \in \mathbb{R}^n | V(x) \leq c\}$ of the Lyapunov function $V(x)$ and let

$$c_1(v_0(k)) := \left(\frac{\rho + 1}{2\rho} v_0(k) \right)^2 b_{\inf}, \tag{15}$$

$$c_2(v_0(k)) := \lambda_{\min}(P) \left(\frac{\|\tilde{Q}^{-1} A^\top P B\| v_{N-1}}{|\mu_+|} \right)^2, \tag{16}$$

where $\delta > 0$ is a small scalar and

$$\tilde{Q} := Q + \delta I = \frac{A^\top P B B^\top P A}{B^\top P B} \frac{1}{\hat{\gamma}^2} + \delta I,$$

$$\mu_\pm := -\frac{B^\top P A \tilde{Q}^{-1} A^\top P B}{B^\top P B} \pm \sqrt{\frac{B^\top P A \tilde{Q}^{-1} Q \tilde{Q}^{-1} A^\top P B}{B^\top P B}}.$$

Here, because P and $\tilde{Q}$ are positive definite and Q non-negative definite, the following lemma holds.

***Lemma* 4.** For the given Q and $\tilde{Q}$, $\mu_\pm$ is real and $|\mu_+| \leq |\mu_-|$.

Recall that we are looking for a finite-level quantizer, which is the coarsest possible quantizer such that the system is quadratically stable under a DoS attack. To this end, two areas are defined. The first area is the dead-zone area, whereas the second area represents the area in which *all* states – which includes those outside of the dead-zone – should lie. The next lemma introduces bounds on the Lyapunov function both inside and outside the dead-zone as a step towards a finite-level quantizer.

***Lemma* 5.** There exists an updating sequence $v_0(k)$ with initial condition $v_0(0)$ under the control law $v(k) = q_{v_0(k)}(K_{\mathrm{GD}} x_k)$ such that the following holds:

$$\begin{aligned} V(x_{k+1}) &\leq c_1(v_0(k+1)), \quad \forall x_k \in L_V(c_1(v_0(k))), \\ V(x_{k+1}) &\leq c_2(v_0(k+1)), \quad \forall x_k \in L_V(c_2(v_0(k))) \setminus \\ &\qquad\qquad L_V(c_1(v_0(k))), \end{aligned}$$

where $L_V(c_2(v_0(k))) \setminus L_V(c_1(v_0(k)))$ is non-empty and $c_1(\cdot)$, $c_2(\cdot)$ as in (15), (16), respectively.

With the above lemma, the bounds for inside and outside the dead-zone are defined. A sequence for $v_0(k)$ is needed for achieving $V(x_k) \to 0$ when $k \to \infty$, for which the dynamics remain within the bounds $c_1(v_0)$, $c_2(v_0)$. Note that these bounds are time-varying depending on the states of DoS attacks. Specifically, both should grow in the "DoS present" mode and decrease otherwise.

Given a positive scalar $R_0 > 0$, suppose the initial state satisfies $\|x_0\| \leq R_0$. Let the initial value of v_0 be

$$v_0(0) = \sqrt{\frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}} \frac{|\mu_+| R_0}{\|\tilde{Q}^{-1} A^\top P B\| \rho^{N-1}}$$

and let $v_0(k)$ update as

$$v_0(k+1) = \begin{cases} F_0 \rho^{-N} v_0(k), & \text{if } (\sigma_k, w_k) = (1,1), \\ \sqrt{\beta} v_0(k), & \text{if } (\sigma_k, w_k) = (1,0), \\ \sqrt{\alpha} v_0(k), & \text{if } \sigma_k = 0, \end{cases} \tag{17}$$

where $\sigma_k \in \{0, 1\}$ indicates whether the system experiences DoS at time k and

$$w_k := \begin{cases} 1, & \text{if } x_k \in L_V(c_1(v_0(k))), \\ 0, & \text{if } x_k \in L_V(c_2(v_0(k))) \setminus L_V(c_1(v_0(k))). \end{cases}$$

Note that the update for v_0 requires the knowledge of σ_k at time $k+1$, which can be realized by the utilization of an acknowledgment-based protocol (e.g., TCP protocol). At each time k the index of the quantized signal $v(k)$ as well as the binary signal w_k need to be transmitted between the encoder and decoder. In both the encoder and decoder, $v_0(k)$ can be constructed because of the acknowledgments.

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

***Theorem* 2.** Given the process (1) with controller $u_k = K x_k$, with state feedback gain $K = -(B^\top P A)/(B^\top P B)$. Given a value $\rho_{\sup} > 0$, if there exists a $P > 0$ satisfying (9) and the DoS attack satisfies (11), then the process (1) is quadratically stable under the design of the quantizer $q_{v_0(k)}(u)$ in (14) with $v_0(k)$ in (17).

It is worth mentioning that the level of tolerable DoS attacks under dynamic quantized control in Theorem 2 is the same as the one for the static quantized controller in Section 3.

5. NUMERICAL RESULTS

We examine the same second-order unstable system as in Tsumura et al. (2009), given by

$$x(k+1) = \begin{bmatrix} 0 & 1 \\ 1.8 & -0.3 \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \hat{v}(k).$$

The eigenvalues are $1.2, -1.5$. We run a numerical simulation in Matlab to test the finite-level, time-varying quantizer q_{v_0} from (14) for this system.

The worst-case DoS attack would be *an attack launched with its full budget at* $k = 0$, i.e., the start of simulation. Let $\Theta := \lfloor k \bar{\nu}_d \rfloor$ be the total amount of allowed DoS samples on an interval $[0, k]$ for a given β. With this attack, there is no absolute decrease in the state before the attack is launched, such that the Lyapunov function will reach its peak at $V(x(\Theta)) = \alpha^\Theta V(x(0))$. Consequently, compensating this maximum value takes the most amount of time-steps where control is applied, before it converges to the origin.

The simulation is run for a fixed value of the convergence parameter $\beta = 0.49$ (recall that β should lie in $(0, 1)$ and that the corresponding coarseness parameter ρ can be obtained from β) for $k = 150$ samples with initial condition $x_0 = [-10 \; 2]^\top$. In the simulation, we take $\Pi_d = 0$ as this does not affect overall stability for $k \to \infty$. The resulting DoS bound is $\bar{\nu}_d \simeq 0.2632$, such that $\Theta = 39$. The expansion ratio $\rho_{\sup}$ follows from inserting this value

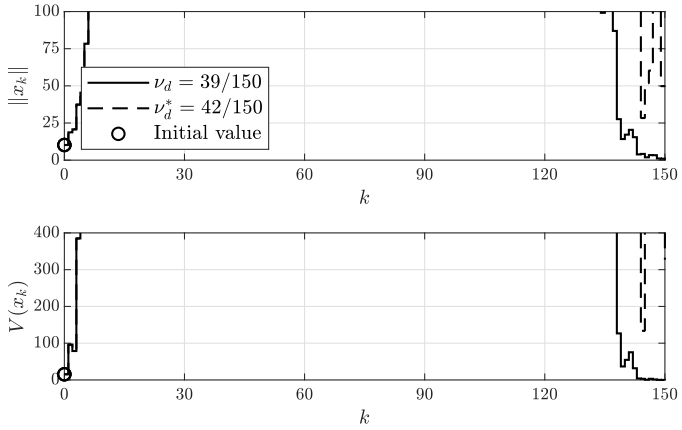

Fig. 2. Simulation of the system with time-varying quantizer under DoS, showing the resulting norm of x_k and the Lyapunov function $V(x_k)$, for a stable and unstable amount of DoS samples.

for β in (13). Moreover, all parameters are chosen in a coarsest or worst-case scenario, i.e., $\rho = \rho_{\text{sup}} \simeq 1.7481$, $R_0 = \|x_0\|^2$, $N = \lceil \log_\rho(F_0/\sqrt{\beta}) \rceil = 3$, and so on. The DoS budget is maximized as well. Hence this simulation is a 'worst-case' simulation of the theory if the attack is launched at the start of the simulation. Additionally, a P satisfying (9) is given by

$$P = \begin{bmatrix} 0.2231 & -0.0511 \\ -0.0511 & 0.4553 \end{bmatrix}.$$

To numerically demonstrate the tightness of the quadratic stability condition (11), we simulate for $\nu_d = \Theta/k = 39/150 < \bar{\nu}_d$ and $\nu_d^* = 42/150 > \bar{\nu}_d$, such that $\sigma_k = 0$ when $0 \leq k \leq 39$ and $0 \leq k \leq 42$, respectively. Moreover, $\sigma_k = 1$ when $40 \leq k \leq 150$ and $43 \leq k \leq 150$, respectively.

The simulation results are shown in Fig. 2. The plots first show an exponential increase due to the DoS attack, which is launched with the complete budget at the start of simulation, followed by convergence after no more DoS is allowed by the DoS bound ν_d. As can be seen, the states converge for ν_d, but they do not converge for ν_d^* whose simulation results diverge. Increasing the number of samples k over which the simulation is run would only further increase the divergence in the case of ν_d^*, while still guaranteeing convergence for ν_d. This shows the tightness of the quadratic stability condition in Lemma 3.

Note that the solution for P that satisfies (9) has not been optimized, such that it would result in the lowest value of α in (10). Therefore, the bound $\bar{\nu}_d$ in this numerical example is likely not the largest value and it is possible that the most amount of DoS allowed for $\beta = 0.49$ is larger than 39 to still achieve quadratic stability. However, this example does show that it will be smaller than 42 samples of DoS, as this would not result in quadratic stability as depicted in Fig. 2.

6. CONCLUSION

In this paper, we have proposed the design of the possible coarsest quantizers that can lead to closed-loop stability guaranteed by a quadratic Lyapunov function under the considered class of DoS attacks. In particular, we have presented the design of the finite-level dynamic quantizer, and it is shown that the system under dynamic quantized control has a comparable resilience as the one under infinite-level static quantized control.

REFERENCES

Brockett, R.W. and Liberzon, D. (2000). Quantized feedback stabilization of linear systems. *IEEE Trans. on Automatic Control*, 45(7), 1279–1289.

Cárdenas, A.A., Amin, S., and Sastry, S. (2008). Research challenges for the security of control systems. *Proc. of the 3rd Conf. on Hot Topics in Security*, 6.

Cheng, P., Shi, L., and Sinopoli, B. (2017). Guest editorial special issue on secure control of cyber-physical systems. *IEEE Trans. on Control of Network Systems*, 4(1), 1–3.

De Persis, C. and Tesi, P. (2015). Input-to-state stabilizing control under Denial-of-Service. *IEEE Trans. on Automatic Control*, 60(11), 2930–2944.

Dolk, V.S., Tesi, P., De Persis, C., and Heemels, W.P.M.H. (2017). Event-triggered control systems under Denial-of-Service attacks. *IEEE Trans. on Control of Network Systems*, 4(1), 93–105.

Elia, N. and Mitter, S.K. (2001). Stabilization of linear systems with limited information. *IEEE Trans. on Automatic Control*, 46(9), 1384–1400.

Feng, S., Cetinkaya, A., Ishii, H., Tesi, P., and Persi, C.D. (2020). Networked control under DoS attacks: Tradeoffs between resilience and data rate. *IEEE Trans. on Automatic Control*, to appear.

Fu, M. and Xie, L. (2005). The sector bound approach to quantized feedback control. *IEEE Trans. on Automatic Control*, 50(11), 1698–1711.

Hespanha, J.P., Naghshtabrizi, P., and Xu, Y. (2007). A survey of recent results in networked control systems. *Proc. of the IEEE*, 95(1), 138–162.

Ishii, H. (2006). Stabilization under shared communication with message losses and its limitations. In *Proc. of the 45th IEEE CDC*, 4974–4979.

Liberzon, D. (2003). On stabilization of linear systems with limited information. *IEEE Trans. on Automatic Control*, 48(2), 304–307.

Nair, G.N., Fagnani, F., Zampieri, S., and Evans, R.J. (2007). Feedback control under data rate constraints: An overview. *Proc. of the IEEE*, 95(1), 108–137. doi: 10.1109/JPROC.2006.887294.

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

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., and Sastry, S.S. (2007). Foundations of control and estimation over lossy networks. *Proc. of the IEEE*, 95(1), 163–187.

Tsumura, K., Ishii, H., and Hoshina, H. (2009). Tradeoffs between quantization and packet loss in networked control of linear systems. *Automatica*, 45(12), 2963–2970.

Wakaiki, M., Cetinkaya, A., and Ishii, H. (2018). Quantized output feedback stabilization under DoS attacks. *Proc. of the ACC*, 2018-June, 6487–6492.

Zhang, L., Gao, H., and Kaynak, O. (2013). Network-induced constraints in networked control systems – A survey. *IEEE Trans. on Industrial Informatics*, 9(1), 403–416.