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

DoS-Aware Quantized Control of Nonlinear Systems via Linearization ⋆

Rui Kato * **Ahmet Cetinkaya** ** **Hideaki Ishii** *

* *Department of Computer Science, Tokyo Institute of Technology, Yokohama, 226-8502, Japan (e-mail: kato@sc.dis.titech.ac.jp, ishii@c.titech.ac.jp).*
** *Information Systems Architecture Science Research Division, National Institute of Informatics, Tokyo, 101-8430, Japan (e-mail: cetinkaya@nii.ac.jp).*

Abstract: This paper deals with a quantized feedback stabilization problem of nonlinear networked control systems via linearization. In particular, we study circumstances where the communication channel is interrupted by Denial-of-Service (DoS) attacks and its data rate is limited. We employ a deterministic DoS attack model which constraints the amount of attacks only by their frequency and duration, allowing us to capture a large class of potential attacks. To achieve asymptotic stabilization, we propose a resilient dynamic quantizer in the sense that it does not saturate in the presence of packet losses caused by DoS attacks. A sufficient condition for stability is derived by restricting the average frequency and duration of attacks. Since our result only guarantees local stability, we explicitly investigate an estimate of the region of attraction, which may be reduced by attacks. A simulation example is presented for demonstration of our results.

Keywords: DoS attacks, quantized control, nonlinear systems, stability analysis, linearization.

1. INTRODUCTION

Networked control systems have been widely studied over the past several decades (Ishii and Francis (2002) and Bemporad et al. (2010)). When a communication channel is used in control systems, measurement and control input information exchanged over the channel need to be quantized. Moreover, it becomes necessary to investigate how the control system may be affected by data rate limitations of the channel. Many researchers thus tackled such data rate limited control problems from various perspectives (see, e.g., Nair et al. (2007) and the references therein).

On the other hand, in recent years, the viewpoint of cyber security has become important for networked control systems as such systems have been found to be vulnerable to attacks (see, e.g., Cárdenas et al. (2008) and Pasqualetti et al. (2015) for an overview). It has become clear that both cyber and physical attacks to control systems may induce critical incidents in the real world, resulting in, e.g., large financial losses. According to Amin et al. (2009), cyber attacks on control systems are classified to *deception attacks*, which are conducted by changing the contents of packet data, and *Denial-of-Service (DoS) attacks*, which refer to communication interruptions including jamming attacks. DoS attacks are particularly critical as it is easy to launch such attacks as mentioned in Teixeira et al. (2015). For this reason, we examine the effects of DoS attacks throughout the paper.

⋆ This work was supported in part by the JST CREST Grant No. JPMJCRl5K3, by JSPS under Grant-in-Aid for Scientific Research Grant No. 18H01460, and by JST ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603).

In this paper, we study stabilization of nonlinear control systems over data rate limited channels in the presence of DoS attacks. We follow a sampled-data control approach based on linearization. Though linearization-based control design is a typical method in practice, only few works deal with this approach in the literature. It is of particular interest in the context of DoS attacks, since they may bring critical issues when communication may be interrupted by adversaries. Kato et al. (2019) considered cases where a nonlinear system is locally controlled under DoS attacks. There, it is mentioned that if the state leaves the region of attraction due to DoS attacks, then it will not converge to the equilibrium even after the communication is restored. This paper extends the framework presented in Kato et al. (2019) to take quantization into account. Also, we follow the works by Hou et al. (1997) and Hu et al. (1999) in linearization analysis. We then derive a sufficient condition that the state trajectory remains within a certain stable region even under DoS attacks.

Similarly to De Persis and Tesi (2015), we treat DoS attacks in a deterministic manner rather than a stochastic one (see Cetinkaya et al. (2019b) for more detailed discussion on various DoS attack models). In the work of De Persis and Tesi (2015), DoS attacks were characterized in terms of average frequency and duration. There, input-to-state stability of linear systems is investigated under DoS attacks and conditions on allowable attack frequency and duration were obtained. These conditions were made less conservative in Feng and Tesi (2017) by using a predictor that estimates interrupted measurements. For nonlinear systems under DoS attacks, De Persis and Tesi (2016) investigated a global stabilization problem with certain

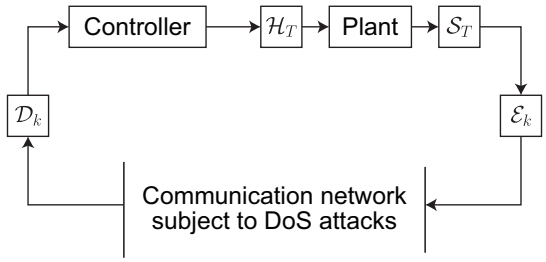

Fig. 1. Networked control system under DoS attacks

assumptions. Cetinkaya et al. (2017) and Cetinkaya et al. (2019a) provided a comprehensive treatment of both malicious and non-malicious packet losses. On the other hand, quantized control problems of linear systems under DoS attacks were considered in Wakaiki et al. (2019) with observer-based output feedback control and in Feng et al. (2019) to reveal the trade-off between the minimum data rate for stabilization and the tolerable level of DoS attacks.

For considering the required data rate for networked control, we aim to design dynamic quantizers which are resilient to packet losses in the communication channel. To this end, we employ time-varying quantizers with the zooming-in and zooming-out capabilities explored by Liberzon and Hespanha (2005) for nonlinear systems. However, there are few works dealing with both the quantization effects and packet losses. If there are packet losses, these dynamic quantizers may saturate. The saturation phenomenon of a dynamic quantizer was investigated by Liberzon and Nešić (2007), where the system is subject to large disturbances. As noted in that paper, saturation of a dynamic quantizer can introduce performance degradation, and hence, we should avoid such situations. For linear systems under probabilistic packet losses, the minimum data rate problem has been addressed in You and Xie (2011) and Minero et al. (2013).

The subsequent sections are organized as follows. In Section 2, we describe the problem setting and the DoS attack model used in this paper. The encoding/decoding scheme and the proposed resilient dynamic quantizer are introduced in Section 3. The main results of this paper are presented in Section 4, where a sufficient condition for stability and an initial condition to guarantee the convergence of state trajectories are derived. In Section 5, we present a simulation example. Finally, we conclude the paper in Section 6.

Throughout this paper, we employ the following notation. The sets of nonnegative reals and nonnegative integers are denoted by $\mathbb{R}_+$ and $\mathbb{Z}_+$, respectively. Given a vector v and a matrix M, $\|v\|_\infty$ and $\|M\|_\infty$ respectively denote the ∞-norm and the induced ∞-norm. The length of an interval $\mathcal{I}$ is denoted by $|\mathcal{I}|$.

2. PROBLEM FORMULATION

Consider the nonlinear networked control system depicted in Fig. 1, where a communication channel is inserted between the sensor and the controller. In this section, we describe the problem setting of networked control and the DoS attack model characterized by their frequency and duration.

2.1 Nonlinear networked control system

In Fig. 1, the plant to be controlled is described by

$$\dot{x}(t) = f(x(t), u(t)), \quad t \geq 0, \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state and $u(t) \in \mathbb{R}^m$ is the control input at time t. The initial state is given by $x(0) = x_0 \in \mathbb{R}^n$. Assume that $f\colon \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is continuously differentiable and that the system (1) has an equilibrium point at the origin, i.e., $f(0,0) = 0$. Then, we impose the following assumption.

Assumption 1. The function f in (1) is Lipschitz in a certain region $\mathcal{D} := \{x \in \mathbb{R}^n : \|x\|_\infty < \varrho\}$ for any input $u \in \mathbb{R}^m$, where $\varrho > 0$ is some positive number. That is, there exists $L \geq 0$ satisfying $\|f(y,u) - f(z,u)\|_\infty \leq L\|y - z\|_\infty$ for all $y, z \in \mathcal{D}$ and $u \in \mathbb{R}^m$.

Letting $T > 0$ be a fixed sampling period, we denote by $t_k := kT$, $k \in \mathbb{Z}_+$, the sampling instants. The ideal sampler $\mathcal{S}_T$ measures the state at each sampling time. The sampled state is then transformed by the encoder $\mathcal{E}_k$ into a certain symbol to be sent through the channel. At the controller side, the decoder $\mathcal{D}_k$ produces the quantized state after receiving the packet as explained in the next section. During the sampling/transmission intervals, the input is kept constant by the zeroth-order hold $\mathcal{H}_T$.

For given constants $\bar{x} \in \mathbb{R}^n$ and $\bar{u} \in \mathbb{R}^m$, let $\phi(t, \bar{x}, \bar{u})$ be the solution to (1) for $t \in [0, T]$ with the initial state $x_0 = \bar{x}$ and the constant input $u(t) \equiv \bar{u}$. Then, we define $\phi_T(\bar{x}, \bar{u}) := \phi(T, \bar{x}, \bar{u})$. Furthermore, for ease of presentation, we write the sampled value $x(t_k)$ as x_k for each $k \in \mathbb{Z}_+$, and the same notation is used for other variables as well.

If a DoS attack is active at a sampling time, then the packet transmission at that instant fails. In this case, the control input is set to zero until the next packet reaches the controller side. Let $\theta_k \in \{0, 1\}$ be the indicator that stands for the absence or presence of packet losses. If a packet loss occurs at time t_k, we set $\theta_k = 1$, and otherwise $\theta_k = 0$. Then, the control input applied to the plant (1) is given as follows:

$$u(t) = (1 - \theta_k) K q_k, \quad t \in [t_k, t_{k+1}), \quad k \in \mathbb{Z}_+, \tag{2}$$

where $K \in \mathbb{R}^{m \times n}$ is a feedback gain matrix, the choice of which is given later. Moreover, $q_k \in \mathbb{R}^n$ denotes the quantized value of the sampled state x_k.

2.2 Data rate limitation

Since we consider a communication channel whose data rate is limited, the information that the packet can contain is taken from a finite set. Let $\mathcal{M} := \{0, 1, \ldots, M^n - 1\}$ be the set of integers that can be sent by communication at once, where M is a positive integer expressing the number of the quantization levels in one coordinate of $\mathbb{R}^n$. In this case, the data rate of the channel is denoted by $R := n \log_2(M)/T$ bits per unit of time. Defining $\Lambda := \mathrm{e}^{LT}$, we make the following assumption, which can be found in Liberzon and Hespanha (2005).

Assumption 2. The number of the quantization levels M satisfies $M > \Lambda$.

2.3 Averagely constrained DoS attacks

Here, we introduce a deterministic class of DoS attacks. For $i \in \mathbb{Z}_+$, let $a_i \geq 0$ and $\tau_i \geq 0$ denote the launching time and the length of the ith DoS attack, respectively. Notice that when $\tau_i = 0$, the attack is impulsive, and thus, it has no length. We then define the collection of DoS attack intervals by $\mathcal{A}(t) := \bigcup_{i\in\mathbb{Z}_+}[a_i, a_i+\tau_i]\cap[0,t]$. Furthermore, we denote by $N(t)$ the number of DoS attacks for which the starting time is inside the interval $[0,t]$. Following the work of De Persis and Tesi (2015), we consider the assumptions below on the frequency and duration of DoS attacks.

Assumption 3. (DoS frequency). There exist $\kappa_F \geq 0$ and $\rho_F \in [0,\infty)$ such that $N(t) \leq \kappa_F + \rho_F t$ for all $t \geq 0$.

Assumption 4. (DoS duration). There exist $\kappa_D \geq 0$ and $\rho_D \in [0,1)$ such that $|\mathcal{A}(t)| \leq \kappa_D + \rho_D t$ for all $t \geq 0$.

Remark 1. In contrast with the assumptions used in Feng and Tesi (2017) and Feng et al. (2020), by using Assumptions 3 and 4, one can treat a wider class of DoS attacks. In particular, under Assumptions 3 and 4, the maximum period of unsuccessful packet transmissions needs not be bounded. The constants ρ_F and ρ_D represent the allowable average frequencies and durations of DoS attacks, whereas κ_F and κ_D indicate the initial energy to launch attacks. We note that, in this framework, an attacker does not need to follow certain attack strategies (e.g., periodic one). If an attacker can launch long and/or frequent DoS attacks, then all the packet transmissions may fail. Such situations may occur when frequent attacks with $\rho_F \geq 1/T$ are allowed.

3. QUANTIZED CONTROL VIA LINEARIZATION

In this section, we consider the stabilization problem with quantized state feedback. First, we explore linearization analysis of the continuous-time nonlinear system (1). Then, the encoding/decoding procedure and the resilient design of a dynamic quantizer are introduced.

3.1 Linearization analysis

Linearization of (1) around the origin yields

$$\dot{x}(t) = Ax(t) + Bu(t) + g(x(t), u(t)), \tag{3}$$

where

$$A := \left.\frac{\partial f(x,u)}{\partial x}\right|_{x=0,u=0}, \quad B := \left.\frac{\partial f(x,u)}{\partial u}\right|_{x=0,u=0},$$

and $g(x,u) := f(x,u) - Ax - Bu$ is the remainder term of the linear approximation. It is assumed that A is unstable and that the pair (A,B) is stabilizable.

Discretizing the system (3) with the period T, we obtain

$$x_{k+1} = \widetilde{A}x_k + \widetilde{B}u_k + \widetilde{g}(x_k, u_k), \tag{4}$$

where $\widetilde{A} := \mathrm{e}^{AT}$, $\widetilde{B} := \int_0^T \mathrm{e}^{As}\,\mathrm{d}sB$, and

$$\widetilde{g}(x_k,u_k) := \int_0^T \mathrm{e}^{A(T-s)}\, g(\phi(s,x_k,u_k),u_k)\,\mathrm{d}s.$$

Suppose that stabilizability of (A,B) is preserved through sampling. Also, suppose that the controller gain K in (2) is designed such that $\widetilde{A}+\widetilde{B}K$ is Schur stable. In this case, the origin of (1) is locally asymptotically stable, but global stability is not guaranteed.

Although Wakaiki et al. (2019) considers the discrete-time system, we employ the sampled-data setting as bounds on the inter-sample behavior are required to analyze the nonlinearity of (4).

We first give a result involving the inter-sample behavior of the continuous-time system (1). We define $c_0 := [1 + T(\|BK\|_\infty + \|K\|_\infty)]\,\mathrm{e}^{T(\|A\|_\infty+1)}$ and $c_1 := \mathrm{e}^{T(\|A\|_\infty+1)}$ to obtain the following lemma.

Lemma 1. For any $\bar{x} \in \mathbb{R}^n$, consider the solution $\phi(t,\bar{x},\bar{u})$ to (1) with $\bar{u} = (1-\theta)K\bar{x}$, where $\theta \in \{0,1\}$. Then, there exists a constant $d > 0$ such that $\|\bar{x}\|_\infty < d$ implies

$$\|\phi(t,\bar{x},\bar{u})\|_\infty \leq \begin{cases} c_0\|\bar{x}\|_\infty & \text{if } \theta = 0, \\ c_1\|\bar{x}\|_\infty & \text{if } \theta = 1, \end{cases}$$

for all $t \in [0,T)$.

To show local stability of the origin, we need to obtain bounds on the nonlinear term $\widetilde{g}(x_k,u_k)$ in (4). The following lemma characterizes the region, inside which the norm of the nonlinear term can be upper-bounded by a linear function of the state norm.

Lemma 2. For any $\bar{x} \in \mathbb{R}^n$, consider the nonlinear function $\widetilde{g}(\bar{x},\bar{u})$ in (4) with $\bar{u} = (1-\theta)K\bar{x}$, where $\theta \in \{0,1\}$. Given $\gamma > 0$, we define $\gamma_0 := (c_0 + \|K\|_\infty)\gamma T\,\mathrm{e}^{T\|A\|_\infty}$ and $\gamma_1 := c_1\gamma T\,\mathrm{e}^{T\|A\|_\infty}$. Then, there exists a constant $\delta \in (0,d]$ such that $\|\bar{x}\|_\infty < \delta$ implies

$$\|\widetilde{g}(\bar{x},\bar{u})\|_\infty \leq \begin{cases} \gamma_0\|\bar{x}\|_\infty & \text{if } \theta = 0, \\ \gamma_1\|\bar{x}\|_\infty & \text{if } \theta = 1, \end{cases}$$

where d is as in Lemma 1.

3.2 Encoding/decoding procedure

Here, we state the encoding/decoding procedure of the dynamic quantizer following Liberzon and Hespanha (2005). For $\xi \in \mathbb{R}^n$ and $E \geq 0$, let

$$\mathcal{Q}(\xi,E) := \{x \in \mathbb{R}^n : \|x-\xi\|_\infty \leq E\}.$$

In our dynamic quantizer, the quantization region at time t_k is given by $\mathcal{Q}(\xi_k,E_k)$. This is a hypercube which has the edges of length $2E_k \geq 0$ and is centered at $\xi_k \in \mathbb{R}^n$. Since the initial state is not known exactly in general, we set $\xi_0 = 0$. We impose the following assumption on the initial state for given E_0.

Assumption 5. For given $E_0 \geq 0$, the initial state x_0 of (1) satisfies $\|x_0\|_\infty \leq E_0$.

The variables ξ_k and E_k are adjusted based on the reachable set of the state to avoid saturation of the quantizer. In the present paper, we assume that an acknowledgement signal or the value of θ_k is exchanged between the encoder and decoder and that this signal is not subject to DoS attacks similarly to Wakaiki et al. (2019) and Feng et al. (2020). At each sampling time t_k, the state x_k is quantized as follows:

1. The encoder partitions $\mathcal{Q}(\xi_k,E_k)$ into the M^n equal boxes with the same dimension, each of which is indexed by an integer in $\mathcal{M}$.
2. If the sampled state x_k lies in the box indexed by $i \in \mathcal{M}$, then the symbol $s_k = i$ is transmitted through the communication channel.

3. If the packet containing the symbol $s_k = i$ reaches the controller side, the quantized state q_k is produced as the center of the box of index i.
4. The encoder and decoder update their own variables ξ_k and E_k based on the value of the acknowledgement signal θ_k.

If we know which partitioned box the state lies in, then the reachable set at the next sampling instant can be estimated, which is smaller than the current quantization region, resulting in the zooming-in process. However, if the packet loss occurs at time t_k, we know only that the state x_k is inside $\mathcal{Q}(\xi_k, E_k)$. Then, one needs to expand the quantization region to capture the state x_{k+1} at the next sampling time t_{k+1}, leading to the zooming-out process. In the next subsection, we explain how the quantizer is updated depending on the value of θ_k while the effects of DoS attacks are taken into account.

3.3 Resilient dynamic quantizer design

As long as the state x_k lies in the quantization region $\mathcal{Q}(\xi_k, E_k)$, the quantization error satisfies

$$\|x_k - q_k\|_\infty \leq \frac{1}{M} E_k. \tag{5}$$

To avoid saturation of the quantizer, i.e., to ensure that the state never goes outside the quantization region, both the encoder and decoder need to calculate ξ_{k+1} and E_{k+1} so that

$$\|x_{k+1} - \xi_{k+1}\|_\infty \leq E_{k+1}, \tag{6}$$

which is equivalent to $x_{k+1} \in \mathcal{Q}(\xi_{k+1}, E_{k+1})$.

To do this, we propose the following dynamic quantizer. The encoder and decoder generate ξ_{k+1} and E_{k+1} by the following update rules:

$$\xi_{k+1} := \begin{cases} \phi_T(q_k, Kq_k) & \text{if } \theta_k = 0, \\ \phi_T(\xi_k, 0) & \text{if } \theta_k = 1, \end{cases} \tag{7}$$

$$E_{k+1} := \begin{cases} \dfrac{\Lambda}{M} E_k & \text{if } \theta_k = 0, \\ \Lambda E_k & \text{if } \theta_k = 1. \end{cases} \tag{8}$$

The quantizer needs to be capable to expand its quantization region when packet losses occur. Here, we note that the coordinate transformations to update the quantization region considered in Wakaiki et al. (2019) and Feng et al. (2020) are applicable only to linear systems. In the current case, we cover the nonlinearity by simulating the evolution of the state trajectory by (7) at each sampling time, which can be computationally expensive. However, our main focus is linearization in the stabilization problem, and we do not aim to reduce such computational complexities. Thus, it is assumed that calculating (7) can be performed.

In what follows, we show that the dynamic quantizer (7) and (8) locally satisfies the condition (6) at times when both zooming-in and zooming-out occur.

Zooming-in process. We first consider the case where the packet transmission at time t_k is successful, that is, $\theta_k = 0$. In this case, both the encoder and the decoder know the value of the quantized state q_k. If $x_k, q_k \in \mathcal{D}$, where $\mathcal{D}$ is given in Assumption 1, then we can see from (7) that

$$\|x_{k+1} - \xi_{k+1}\|_\infty \leq \Lambda \|x_k - q_k\|_\infty \leq \frac{\Lambda}{M} E_k,$$

where the last inequality follows from the boundary condition (5). From (8), we can guarantee the condition (6).

Zooming-out process. We then consider the case where the communication fails due to DoS attacks, that is, $\theta_k = 1$. In this case, the decoder does not know the value of q_k but knows that of ξ_k, and thus, the update rule (7) can be performed. Whenever $x_k, q_k \in \mathcal{D}$, we have

$$\|x_{k+1} - \xi_{k+1}\|_\infty \leq \Lambda \|x_k - \xi_k\|_\infty \leq \Lambda E_k.$$

Hence, we can use (7) and (8) to ensure that (6) holds for all $k \in \mathbb{Z}_+$.

4. MAIN RESULTS

In this section, we consider stability analysis of the nonlinear system (1) with the control input (2).

4.1 Stability condition under DoS attacks

Various ways to analyze asymptotic stability of switched systems have been proposed such as a switched Lyapunov function approach (Liberzon (2014)) and a common Lyapunov function approach (Wakaiki and Yamamoto (2017)). In this paper, we employ a switched Lyapunov-like function to handle the unstable dynamics stimulated by DoS attacks.

Let $\varphi_0 \in (0, 1)$ and $\varphi_1 \in (1, \infty)$ be scalars satisfying that $\varphi_0^{-1/2}(\widetilde{A} + \widetilde{B}K)$ and $\varphi_1^{-1/2}\widetilde{A}$ are Schur stable, respectively. Then, there exist positive-definite matrices $P_0, P_1 \in \mathbb{R}^{n \times n}$ such that

$$(\widetilde{A} + \widetilde{B}K)^\top P_0 (\widetilde{A} + \widetilde{B}K) - \varphi_0 P_0 \prec 0, \tag{9}$$

$$\widetilde{A}^\top P_1 \widetilde{A} - \varphi_1 P_1 \prec 0. \tag{10}$$

Following the work of Liberzon (2014), we define for $p \in \{0, 1\}$ a positive definite function $W_p \colon \mathbb{R}^n \times \mathbb{R}_+ \to \mathbb{R}_+$ as follows:

$$W_p(\xi, E) := \xi^\top P_p \xi + \eta_p E^2, \quad \xi \in \mathbb{R}^n, \quad E \geq 0, \tag{11}$$

where $\eta_0, \eta_1 > 0$ are sufficiently large numbers. These functions satisfy the following two properties, both of which are not difficult to verify. First, there exist $\alpha, \beta > 0$ such that for every $p \in \{0, 1\}$,

$$\alpha(\|\xi\|_\infty + E)^2 \leq W_p(\xi, E) \leq \beta(\|\xi\|_\infty + E)^2. \tag{12}$$

Second, there exist $\mu_0, \mu_1 \geq 1$ such that

$$W_1(\xi, E) \leq \mu_0 W_0(\xi, E), \quad W_0(\xi, E) \leq \mu_1 W_1(\xi, E). \tag{13}$$

Remark 2. Here, we explain the difference from the analysis of our previous work (Kato et al. (2019)). The functions in (11) are composed of two parts: The first part corresponds to the classical quadratic Lyapunov function and the second part is related to the quantization error. If one employs the dynamic quantizer as explained in the previous section, then the quantization error is expected to converge to zero. Therefore, by just adding the error term, one can utilize (11) as a Lyapunov function.

The function $W_{\theta_k}(\xi_k, E_k)$ decreases under the nominal operation, whereas it increases under DoS attacks. The following lemma provides a local characterization of the switched Lyapunov-like function $W_{\theta_k}(\xi_k, E_k)$. Define $\nu_0 :=$

$\max\{\varphi_0, \Lambda^2/M^2\}$ and $\nu_1 := \max\{\varphi_1, \Lambda^2\}$. Then, the convergence rate and the divergence rate of this function corresponding to the occurrence of packet losses are given as follows.

Lemma 3. Consider the nonlinear system (1) with (2) as well as the dynamic quantizer (7) and (8). Suppose that Assumptions 1–5 hold. Choose $\gamma > 0$ sufficiently small to take a constant $\delta \in (0, \varrho]$ from Lemma 2. Then, there exist $\omega_0 \in [\nu_0, 1)$ and $\omega_1 \in [\nu_1, \infty)$ such that $\|\xi_k\|_\infty + E_k \leq \delta$ implies

$$W_{\theta_{k+1}}(\xi_{k+1}, E_{k+1}) \leq \begin{cases} \omega_{\theta_k} W_{\theta_k}(\xi_k, E_k) & \text{if } \theta_{k+1} = \theta_k, \\ \mu_{\theta_k} \omega_{\theta_k} W_{\theta_k}(\xi_k, E_k) & \text{if } \theta_{k+1} \neq \theta_k, \end{cases} \tag{14}$$

where μ_0 and μ_1 are as in (13).

Remark 3. The convergence and divergence rates ω_0 and ω_1 partly depend on the data rate for the communication channel. However, if the data rate is sufficiently large, then ω_0 and ω_1 converge to that of the infinite data rate case, which is determined only by the dynamics of the plant (1). In this case, we can recover our previous results presented in Kato et al. (2019).

Now, we are ready to state our main result. Let $\kappa_D^* := \kappa_D + \kappa_F T$ and $\rho_D^* := \rho_D + \rho_F T$. In the following theorem, we extend the result of Kato et al. (2019) to the case where quantization needs to be considered.

Theorem 4. Consider the nonlinear networked control system (1) with the control input (2). Suppose that Assumptions 1–5 hold. If

$$\rho_F T \ln \mu_0 \mu_1 + (1 - \rho_D^*) \ln \nu_0 + \rho_D^* \ln \nu_1 < 0, \tag{15}$$

then the origin is locally asymptotically stable.

Remark 4. We can observe that the stability is determined depending on the average amount of DoS attacks, which is characterized by ρ_F and ρ_D in Assumptions 3 and 4. The stability condition (15) is similar to that of De Persis and Tesi (2015) for cases without quantization (see also De Persis and Tesi (2016) for nonlinear systems). Since our focus is on a linearization approach, we can recover the global stability result for linear systems by ignoring the nonlinear parts of (3). However, as we discuss below, the local stability point of view is important when DoS attacks are addressed in stabilization problems.

Remark 5. The dynamic quantizer proposed in this paper is resilient in the sense that it does not saturate even under DoS attacks. The above theorem can also be seen as an extension of the work by Liberzon and Hespanha (2005), where the effects of packet losses are not considered. Asymptotic stabilization of switched systems by quantized state feedback is also considered in Liberzon (2014), where the switching condition for stability was derived. Here, in contrast, we further take into account the unstable dynamics induced by DoS attacks. The local stability condition derived above indicates the allowable average frequency and duration of such attacks.

4.2 Convergence condition on initial states

In the previous part of this section, we derived a local stability condition. Due to linearization, we need to keep the state within a small region around the equilibrium even in the presence of packet losses. Otherwise, the state cannot converge to the equilibrium point. Also, we need to set the initial condition so that the inequality (14) is guaranteed. The following result provides a condition on E_0 that guarantees the state trajectory to stay inside the stability region at all times and eventually converge to the origin.

Theorem 5. Consider the nonlinear networked control system (1) with the control input (2). Suppose that Assumptions 1–5 hold. Let ω_0, ω_1, and δ be taken from Lemma 3. Also, suppose that (15) holds. If we choose E_0 to satisfy

$$E_0 < (\mu_0 \mu_1)^{-\kappa_F/2} \left(\frac{\omega_0}{\omega_1}\right)^{\kappa_D^*/(2T)} \delta^*, \tag{16}$$

where $\delta^* := \delta\sqrt{\alpha/\beta}$, then the state trajectory $x(t)$ remains within the set $\{x \in \mathbb{R}^n : \|x\|_\infty < \delta\}$ for all $t \geq 0$ and satisfies $\lim_{t\to\infty} \|x(t)\|_\infty = 0$.

Remark 6. The result in Theorem 5 is important in the sense that the condition (16) may not hold while the stability condition (15) holds. Such a case occurs when the DoS parameters κ_F and κ_D are large. The above theorem provides a quantitative condition under which the state trajectory can remain within the nominal region of attraction arising due to linearization. Here, we emphasize that a certain level of DoS attacks makes the state go outside the region of attraction, possibly leading to an unstable behavior.

5. SIMULATION EXAMPLE

Here, we demonstrate our main results by showing a simulation example.

Consider the Liénard system

$$\ddot{z}(t) - (1 - 3az^2(t) - 5bz^4(t))\dot{z}(t) + z(t) = u(t),$$

where $a = 1/3$ and $b = 1/50$. Choosing state as $x(t) = [x_1(t)\ x_2(t)]^\top = [z(t)\ \dot{z}(t) - \int_0^{z(t)} (1 + 3aw^2 - 5bw^4)\,\mathrm{d}w]^\top$, we obtain the state equation

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} x_2(t) + x_1(t) + ax_1^3(t) - bx_1^5(t) \\ -x_1(t) + u(t) \end{bmatrix}.$$

The right-hand side of the above equation is locally Lipschitz with $L = 10$ satisfying Assumption 1. Also, we choose the sampling period as $T = 0.1$ and the number of quantization levels as $M = 6$. The uncontrolled system has an unstable equilibrium point at the origin and exhibits a stable limit cycle. To stabilize the origin, we consider our linearization-based framework. Specifically, we set the feedback gain to $K = [-1.81\ -1.90]^\top$, which is obtained by using the LQR method on the linearized system. With the setting mentioned above, the solution of this system exhibits a stable limit cycle if the uncontrolled time is sufficiently long. Once the state trajectory approaches the limit cycle, the state is unable to converge to the origin by the linearization-based control.

The simulation result is presented in Fig. 2, where the initial state is set to $x_0 = [0.1\ \ 0.1]^\top$. In the figure, the shaded parts represent the DoS attack intervals. The bottom figure shows the changes in the radius E_k of the quantizer. One can observe that saturation is avoided by expanding the quantization region when DoS is present. From the simulation result, we can see that the state $x(t)$ converges to the origin under DoS attacks.

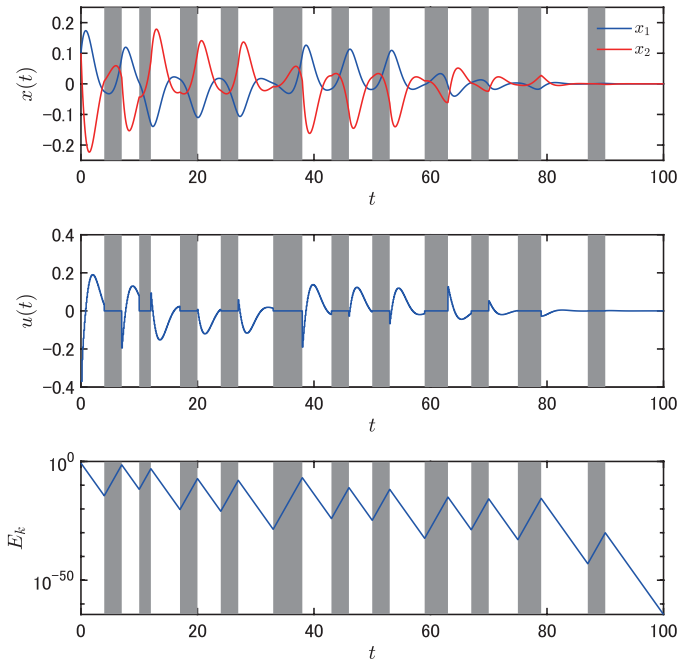

Fig. 2. Trajectories of system state, input, and size of the quantization range

6. CONCLUSION

In this paper, we have considered a quantized stabilization problem of nonlinear networked control systems under DoS attacks. Our proposed control strategy is based on the linearization framework used together with a resilient dynamic quantizer which does not saturate in the presence of packet losses. A sufficient condition for stability and an estimate of the region of attraction have been derived characterizing tolerable frequency and duration of DoS attacks. The simulation example demonstrates our results.

REFERENCES

Amin, S., Cárdenas, A.A., and Sastry, S.S. (2009). Safe and secure networked control systems under Denial-of-Service attacks. In *Proc. 12th Int. Conf. Hybrid Syst., Comput. Control*, 31–45.

Bemporad, A., Heemels, M., and Johansson, M. (2010). *Networked Control Systems*. Springer-Verlag.

Cárdenas, A.A., , Amin, S., and Sastry, S. (2008). Research challenges for the security of control systems. In *Proc. 3rd Conf. Hot Topics in Security*, 1–6.

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2017). Networked control under random and malicious packet losses. *IEEE Trans. Autom. Control*, 62(5), 2434–2449.

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2019a). Analysis of stochastic switched systems with application to networked control under jamming attacks. *IEEE Trans. Autom. Control*, 64(5), 2013–2028.

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2019b). An overview on Denial-of-Service attacks in control systems: Attack models and security analyses. *Entropy*, 21(2).

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

De Persis, C. and Tesi, P. (2016). Networked control of nonlinear systems under Denial-of-Service. *Syst. Control Lett.*, 96, 124–131.

Feng, S., Cetinkaya, A., Ishii, H., Tesi, P., and De Persis, C. (2020). Networked control under dos attacks: Trade-offs between resilience and data rate. *IEEE Trans. Autom. Control*. To appear.

Feng, S., Cetinkaya, A., Ishii, H., Tesi, P., and De Persis, C. (2019). Networked control under DoS attacks: Trade-off between resilience and data rate. In *Proc. American Control Conf.*, 378–383.

Feng, S. and Tesi, P. (2017). Resilient control under Denial-of-Service: Robust design. *Automatica*, 79, 42–51.

Hou, L., Michel, A.N., and Ye, H. (1997). Some qualitative properties of sampled-data control systems. *IEEE Trans. Autom. Control*, 42(12), 1721–1725.

Hu, B., Feng, Z., and Michel, A.N. (1999). Quantized sampled-data feedback stabilization for linear and nonlinear control systems. In *Proc. 38th IEEE Conf. Decision Control*, 4392–4397.

Ishii, H. and Francis, B.A. (2002). *Limited Data Rate in Control Systems with Networks*. Springer-Verlag.

Kato, R., Cetinkaya, A., and Ishii, H. (2019). Stabilization of nonlinear networked control systems under Denial-of-Service attacks: A linearization approach. In *Proc. American Control Conf.*, 1444–1449.

Liberzon, D. (2014). Finite data-rate feedback stabilization of switched and hybrid linear systems. *Automatica*, 50(2), 409–420.

Liberzon, D. and Hespanha, J.P. (2005). Stabilization of nonlinear systems with limited information feedback. *IEEE Trans. Autom. Control*, 50(6), 910–915.

Liberzon, D. and Nešić, D. (2007). Input-to-state stabilization of linear systems with quantized state measurements. *IEEE Trans. Autom. Control*, 52(5), 767–781.

Minero, P., Coviello, L., and Franceschetti, M. (2013). Stabilization over Markov feedback channels: The general case. *IEEE Trans. Autom. Control*, 58(2), 349–362.

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

Pasqualetti, F., Dörfler, F., and Bullo, F. (2015). Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. *IEEE Control Syst. Mag.*, 35(1), 110–127.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, 51, 135–148.

Wakaiki, M., Cetinkaya, A., and Ishii, H. (2019). Stabilization of networked control systems under DoS attacks and output quantization. *IEEE Trans. Autom. Control*. To appear.

Wakaiki, M. and Yamamoto, Y. (2017). Stabilization of switched linear systems with quantized output and switching delays. *IEEE Trans. Autom. Control*, 62(6), 2958–2964.

You, K. and Xie, L. (2011). Minimum data rate for mean square stabilizability of linear systems with Markovian packet losses. *IEEE Trans. Autom. Control*, 56(4), 772–785.