Quantized Output Feedback Stabilization under DoS Attacks

Masashi Wakaiki\(^1\), Ahmet Cetinkaya\(^2\), and Hideaki Ishii\(^2\)

Abstract—This paper addresses the stabilization of quantized linear systems under Denial-of-Service (DoS) attacks. Using a state transformation that satisfies a certain norm condition, we first propose an output encoding method that achieves the stabilization of systems with finite-data rates only under an assumption on the duration of DoS attacks. Next we add a condition on the frequency of DoS attacks and develop an output encoding method with an arbitrary state transformation. Finally we illustrate the obtained results with numerical simulations.

I. INTRODUCTION

Recent advances in computer and network technology make cyber-physical systems (CPSs) prevalent. Malicious attacks to CPSs can impact physical components through the cyber realm and can cause serious infrastructure damage and financial losses. One particular line of research aims at studying control problems under the manipulation of packets transmitted through communication channels; see, e.g., [1]–[3]. On the other hand, Denial-of-Service (DoS) attacks induce packet losses. Since DoS attacks do not require the detailed knowledge on the structure of targeted systems, attackers can launch these attacks in a relatively easy way.

This paper addresses the situation where channels for the transmission of plant measurements are networked and suffer from DoS attacks. Therefore, in the closed-loop system, the packets of the measurements may not be received by controllers. Although networked control with probabilistic packet losses was extensively investigated as surveyed in [4], [5], communication failures due to DoS attacks do not have particular probabilistic models. This motivates system designers to reconsider the control problem with packet losses from the viewpoint of cyber security. In recent studies [6]–[15], control problems under DoS attacks were widely investigated by both control-theoretic and game-theoretic approaches. Particularly, in [10]–[15], only assumptions on duration and frequency were placed for DoS attacks.

In addition to failing to data transmission induced by DoS attacks, signals in networked control systems should be quantized for transmission through digital channels. As surveyed in [16], [17], data-rate limitations for stabilization were obtained through the combination of control and information theory. The so-called zooming-in and zooming-out encoding method was developed in [18] for asymptotic stabilization with finite-data rates, and due to its simple structure, this method was extended to various systems, such as nonlinear systems [19], [20] and switched systems [21], [22]. However, relatively little work has been done on quantized control under DoS attacks.

In this paper, we propose output encoding methods for the stabilization of systems with finite-data rates in the presence of DoS attacks. If the closed-loop system does not suffer from DoS attacks, then coders can decrease their quantization ranges at every time-step, by using the measurement information. However, under DoS attacks, the decoder in the controller side cannot receive the measurement. Due to this lack of information, the error of output estimation used by the controller side cannot receive the measurement. Hence, we decrease the quantization ranges in the absence of DoS attacks like the zooming-in method but increase the quantization ranges in the presence of DoS attacks so that the encoder in the plant side can capture the measurement in its quantization region. Moreover, to ensure the closed-loop stability under a wide class of DoS attacks, we only assume that the duration and frequency of DoS attacks are averagely bounded, as in [10]–[15]. We can regard the proposed encoding strategy as a natural extension of the zooming-in method developed in [23], [24] to the case under DoS attacks.

We first design an output encoding method only under an assumption on the duration of DoS attacks, employing a state transformation that satisfies a certain norm condition. Next we place assumptions on the frequency as well as duration of DoS attacks and develop an encoding method with an arbitrary state transformation. If we know the frequency bound of DoS attacks, then we can exploit it to allow longer DoS durations by using the second encoding method. Both of the derived sufficient conditions on the DoS duration and frequency are characterized only by the growth and decay rates of the quantization ranges in the presence and absence of DoS attacks.

The remainder of this paper is organized as follows. In Section II, we introduce the plant, the controller, and the basic encoding method together with an assumption on the average duration of DoS attacks. In Section III, we provide the main result, i.e., a sufficient condition on the attack duration for closed-loop stability, which can be obtained under a suitable state transformation. Section IV is devoted to a proof of the main result. In Section V, we discuss an output encoding method with an arbitrary state transformation under assumptions on both of the duration and frequency of DoS attacks.

This work was supported in part by JSPS KAKENHI Grant Number JP17K14699 and by the JST CREST Grant No. JPMJCR15K3.

\(^1\)Masashi Wakaiki is with the Graduate School of System Informatics, Kobe University, Kobe, 657-8501, Japan (email: wakaiki@ruby.kobe-u.ac.jp).

\(^2\)Ahmet Cetinkaya and Hideaki Ishii are with the Department of Computer Science, Tokyo Institute of Technology, Yokohama, 226-8502, Japan (email: ahmet@dsl.mei.titech.ac.jp; ishii@c.titech.ac.jp).
attacks. A numerical example is presented in Section VI.

Notation: The set of non-negative integers is denoted by \( \mathbb{Z}_+ \). We denote by \( \rho(P) \) the spectral radius of \( P \in \mathbb{C}^{n \times n} \).

Let us denote by \( A^* \) the complex conjugate transpose of \( A \in \mathbb{C}^{m \times n} \). The Euclidean norm of \( v \in \mathbb{C}^n \) is denoted by \( |v| = (v^*v)^{1/2} \). The Euclidean induced norm of \( A \in \mathbb{C}^{m \times n} \) is defined by \( |A| = \sup \{|Av| : v \in \mathbb{C}^n, |v| = 1 \} \).

For \( v = [v_1 \cdots v_n]^* \in \mathbb{C}^n \), its maximum norm is \( |v|_\infty = \max \{|v_1|, \ldots, |v_n|\} \), and the corresponding induced norm of \( A \in \mathbb{C}^{m \times n} \) is given by \( |A|_\infty = \sup \{|Av|_\infty : v \in \mathbb{C}^n, |v|_\infty = 1 \} \). A square matrix in \( \mathbb{C}^{n \times n} \) is said to be Schur stable if all its eigenvalues lie in the unit disc.

II. PROBLEM STATEMENT

The objective of this section is to introduce the closed-loop dynamics including a basic encoding scheme and an assumption on the duration of DoS attacks.

A. Plant

Consider a linear time-invariant system:

\[
\Sigma_P : \begin{cases} 
  x_{k+1} = Ax_k + Bu_k \\
  y_k = Cx_k 
\end{cases}
\]  

(1)

where \( x_k \in \mathbb{R}^n \), \( u_k \in \mathbb{R}^m \), and \( y_k \in \mathbb{R}^p \) are the state, the input, and the output of the plant, respectively. As illustrated in Fig. 1, the plant is connected with a controller through a communication network subject to DoS, which will be described soon.

We here assume that the system matrix \( A \) is not Schur stable. This is because if \( A \) is Schur stable, then the zero control input \( u_k = 0 \) \((k \in \mathbb{Z}_+)\) achieves the closed-loop stability for arbitrary DoS attacks, and hence the stabilization problem we consider is trivial. Throughout this paper, we place the following assumptions:

Assumption 2.1 (Initial state bound): A constant \( E_0 > 0 \) satisfying

\[ |x_0|_\infty \leq E_0 \]

is known.

Assumption 2.2 (Feedback and observer gains): The matrices \( K \in \mathbb{R}^{m \times n} \) and \( L \in \mathbb{R}^{n \times p} \) are chosen so that \( A - BK \) and \( A - LC \) are Schur stable.

Remark 2.3: We can obtain an initial state bound \( E_0 \) by the “zooming-out” procedure in [23].

B. Observer-based controller and DoS attack

For the case without DoS attacks, we construct the following observer-based controller:

\[
\Sigma_C : \begin{cases} 
  ˙{\hat{x}}_{k+1} = A\hat{x}_k + Bu_k + L(q_k - y_k) \\
  u_k = -K\hat{x}_k \\
  \hat{y}_k = C\hat{x}_k,
\end{cases}
\]  

(2)

where \( \hat{x}_k \in \mathbb{R}^n \), \( \hat{y}_k \in \mathbb{R}^p \), and \( q_k \in \mathbb{R}^p \) are the state estimate, the output estimate, and the quantized value generated from \( y_k \), respectively. We will provide the details of how to generate the quantized output \( q_k \) in the next subsection. We set an initial state estimate \( \hat{x}_0 \) to be \( \hat{x}_0 = 0 \).

When DoS attacks at time \( k \) occur, the controller cannot receive the quantized output \( q_k \). Therefore, for the case with DoS attacks, we use an open-loop controller:

\[
\Sigma_C : \begin{cases} 
  ˙{\hat{x}}_{k+1} = A\hat{x}_k + Bu_k \\
  u_k = -K\hat{x}_k \\
  \hat{y}_k = C\hat{x}_k,
\end{cases}
\]  

(3)

Let us denote by \( \Phi_d(k) \) the number of time-steps when DoS attacks are launched on the interval \([0,k]\), namely, when the dynamics of the controller is given by \( \Sigma_C^d \) on \([0,k]\). As in [10]–[15], we assume that the duration of DoS attacks is averagely bounded:

Assumption 2.4 (Duration of DoS attacks): There exist \( \Pi_d \geq 0 \) and \( \nu_d \in (0,1) \) such that for every \( k \geq 0 \), the DoS duration \( \Phi_d(k) \) satisfies

\[ \Phi_d(k) \leq \Pi_d + \nu_d k. \]  

(4)

We call \( \nu_d \) a DoS duration bound.

Remark 2.5: The authors of [10]–[12], [15] considered systems with disturbances and noise, and hence place the following DoS duration condition instead of (4):

\[ \Phi_d(k_1,k_2) \leq \Pi_d + \nu_d (k_2 - k_1) \quad \forall k_1, k_2 \in \mathbb{Z}_+ \text{ with } k_2 \geq k_1, \]  

(5)

where \( \Phi_d(k_1,k_2) \) is the length of the period when DoS attacks are launched on the interval \([k_1,k_2]\). Although our closed-loop system also has the quantization noise \( y_k - q_k \), the noise exponentially decreases to zero under a certain DoS duration condition (4). Therefore, we use the weaker condition (4) instead of (5).

Remark 2.6: The condition (4) implies that at most \( \Pi_d + \nu_d k \) packets are affected by DoS attacks on the interval \([0,k]\).

Since the system matrix \( A \) is not Schur stable, the targeted system can be regarded as a switched system with a stable mode (in the absence of attacks) and an unstable mode (in the presence of attacks), and the operation time of its unstable mode is not larger than \( \Pi_u + \nu_u k \). We have a similar situation for sampled-data switched systems with the average-dwell time assumption:

\[ \sigma(kh) \leq \Pi_0 + \nu_0 kh, \]  

(6)

where \( h > 0 \) is a sampling period, \( \sigma(kh) \) is the number of switches on the interval \([0, kh]\), and \( 1/\nu_0 \) is called an
average-dwell time. To see this, assume that mode mismatches between the plant and the controller due to intersample switching leads to the instability of the closed-loop system. If a switch occurs at $kh + \epsilon$ ($0 < \epsilon < h$), then the closed-loop system is unstable on the interval $[kh + \epsilon, (k + 1)h]$; otherwise, the system is stable. Therefore, the system behavior at sampling times is unstable in the switched case if $\epsilon > 0$ is sufficiently small. Moreover, from (6), the number of time-steps of such unstable behaviors on the interval $[0, kh]$ does not exceed $\Pi_0 + \nu_0 kh$ (see, e.g., [21], [22] for the details of sampled-data switched systems with quantization). In this sense, the average-dwell time assumption (6) for sampled-data switched systems is similar to the condition (4) on the average duration of DoS attacks. However, whereas the unstable behavior in the switched case varies in dependence upon switching times, the unstable behavior induced by DoS attacks is static. We can therefore obtain an encoding method for stabilization under DoS attacks in a much simpler way.

C. Basic encoding scheme

Define the error $e \in \mathbb{R}^n$ of the state estimation by

$$e_k := x_k - \hat{x}_k.$$  

Using an invertible matrix $R \in \mathbb{C}^{n \times n}$, we also define the error $e_{R,k} \in \mathbb{C}^n$ by

$$e_{R,k} := Re_k.$$  

Suppose that we obtain an error bound $E_{R,k}$ such that

$$|e_{R,k}|_{\infty} \leq E_{R,k}. \quad (7)$$

Since $\hat{x}_k = 0$, it follows from Assumption 2.1 that

$$|e_{R,0}|_{\infty} = |R \hat{x}_0|_{\infty} \leq \|R\| \|E_0\|_{\infty} =: E_{R,0}.$$  

The subsequent sections are devoted to the computation of a bound sequence $\{E_{R,k}\}$ for stabilization, based on the zooming-in encoding method developed in [18], [23].

Since $y_k - \hat{y}_k = Ce_k = CR^{-1}e_{R,k}$, $\forall k \geq Z_+$, it follows that if the error bound $E_{R,k}$ satisfies (7), then

$$|y_k - \hat{y}_k|_{\infty} \leq \|CR^{-1}\|_{\infty} E_{R,k}. \quad (8)$$

We divide the hypercube

$$\{y \in \mathbb{R}^p : |y - \hat{y}_k|_{\infty} \leq \|CR^{-1}\|_{\infty} E_{R,k}\} \quad (8)$$

into $N^p$ equal boxes and assign an index in $\{1, \ldots, N^p\}$ to each divided box by a certain one-to-one mapping for all $k \in Z_+$. The encoder sends to the decoder the index $q_k$ of the divided box containing $y_k$, and then the decoder generates $\hat{y}_k$ equal to the center of the box with the index $q_k$. If $y_k$ lies on the boundary of several boxes, then we can choose any one of them. The quantization error $|y_k - q_k|_{\infty}$ of this encoding method satisfies

$$|y_k - q_k|_{\infty} \leq \frac{\|CR^{-1}\|_{\infty}}{N} E_{R,k}. \quad (9)$$

Remark 2.7: This encoding method requires that the encoder in the plant side also has the same type of observers that is synchronized with the one in the controller side. For this reason, the encoder sends acknowledgments to the plant side at each time, which allows the encoder to detect the DoS attacks. This setting is similar to that of [12], but has been commonly employed in networked control under non-malicious packet losses; see, e.g., the survey [4].

III. MAIN RESULT

In this section, we provide the main result on quantized control under DoS attacks. Before stating the main result, we provide a basic fact of the maximum norm.

**Proposition 3.1:** Assume that $A \in \mathbb{C}^{n \times n}$ is Schur stable. Take a constant $c \in \mathbb{R}$ and an invertible matrix $R_e \in \mathbb{C}^{n \times n}$ satisfying

$$c > \frac{1}{1 - \rho(A)} \quad (10)$$

and

$$R_e(cA)R_e^{-1} = J_c, \quad (11)$$

where $J_c$ is the Jordan canonical form of $cA$. Then the matrix $R_e$ satisfies

$$\|R_eAR_e^{-1}\|_{\infty} \leq \frac{1}{c} + \rho(A) < 1. \quad (12)$$

Proof: Let us denote the eigenvalues of $A$ by $\lambda_1, \ldots, \lambda_r$. Then the diagonal part of the Jordan canonical form $J_c$ consists of $c\lambda_1, \ldots, c\lambda_r$. Moreover, for every matrix $V \in \mathbb{C}^{n \times n}$ whose $(i, j)$th element is denoted by $v_{ij}$, we have

$$\|V\|_{\infty} = \max_{i=1,\ldots,r} \sum_{j=1}^n |v_{ij}|.$$  

Therefore, it follows from (10) that

$$\left|\frac{1}{c} J_c\right|_{\infty} \leq \frac{1}{c} + \max_{i=1,\ldots,r} |\lambda_i| = \frac{1}{c} + \rho(A) < 1. \quad (13)$$

Combining (11) and (13), we obtain the desired conclusion (12).

Let an invertible matrix $R \in \mathbb{C}^{n \times n}$ satisfy

$$\|R(A - LC)R^{-1}\|_{\infty} < 1. \quad (14)$$

Note that such a matrix $R$ always exists under Assumption 2.2 by Proposition 3.1. We set the error bound $\{E_{R,k}\}$ to be

$$E_{R,k+1} := \begin{cases} \vartheta_e E_{R,k} & \text{if there is an attack at time } k \\ \partial E_{R,k} & \text{otherwise,} \end{cases} \quad (15)$$

where

$$\vartheta_e := \|RAR^{-1}\|_{\infty} \quad (16)$$

and

$$\vartheta := \|R(A - LC)R^{-1}\|_{\infty} + \frac{\|RL\|_{\infty} \cdot \|CR^{-1}\|_{\infty}}{N}. \quad (17)$$

The encoding method with this error bound $\{E_{R,k}\}$ achieves the asymptotic convergence of the state and its estimate.
Theorem 3.2: Let Assumptions 2.1, 2.2, and 2.4 hold. If the number of quantization steps $N$ and the DoS duration bound $\nu_d$ satisfy
\begin{align}
N &> \frac{\|RL\|_\infty \cdot \|CR^{-1}\|_\infty}{1 - \|R(A - LC)R^{-1}\|_\infty} \quad (18) \\
\nu_d &< \frac{\log(1/\delta)}{\log(\theta_a/\delta)} \quad (19)
\end{align}
Then the encoding method with the error bound $\{E_{R,k}\}$ constructed by the update rule (15) achieves the state convergence:
\begin{align}
\lim_{k \to \infty} x_k = 0, \quad \lim_{k \to \infty} \hat{x}_k = 0. \quad (20)
\end{align}

We provide a proof of Theorem 3.2 in Section IV.

Remark 3.3: The sufficient condition (19) on the DoS duration bounds $\nu_d$ is characterized only by the growth and decay rates $\theta_a, \theta$ of the error bound $E_{R,k}$. The worst-case growth rate of the error $|e_{R,k}|$ under DoS attacks leads to $\theta_a$. The decay rate $\theta$ satisfies $\theta < 1$ under the condition (18) on $N$ and converges to $\|R(A - LC)R^{-1}\|_\infty$, which is (almost) equal to $\rho(A - LC)$ under a suitable transformation $R$, as $N$ increases.

Remark 3.4: The major difference between the proposed output encoding method and the existing ones in [23], [24] is that in the proposed method, the quantization range $\|CR^{-1}\|_\infty E_{R,k}$ decreases at every time $k$ due to the use of the linear transformation $e_{R,k} = R e_k$. This fact allows us to analyze the closed-loop stability in a less conservative way. This point becomes clearer in Section V, where we include an additional condition on the frequency of DoS attacks.

Remark 3.5: If the system is observable and if $L$ is a deadbeat gain, then all of the eigenvalues of $A - LC$ are zero. From Proposition 3.1, for every $\varepsilon > 0$, there exists an invertible matrix $R \in \mathbb{C}^{n \times n}$ such that
\begin{align}
\|R(A - LC)R^{-1}\|_\infty < \varepsilon.
\end{align}
In this case, since $\theta$ in (17) satisfies $\limsup_{N \to \infty} \theta \leq \varepsilon$, it follows from Theorem 3.2 that, for an arbitrary DoS duration bound $\nu_d \in (0, 1)$, there exists a partition number $N$ such that the state convergence (20) is satisfied, which is consistent with Theorem 2 of [12].

IV. PROOF OF THEOREM 3.2

In this section, we show that the error bound $\{E_{R,k}\}$ defined by (15) satisfies $|e_{R,k}|_\infty \leq E_{R,k}$ for every $k \in \mathbb{Z}_+$. If this inequality holds, then the quantization error $|y_k - q_k|_\infty$ satisfies (9), which leads to the state convergence (20).

A. Design of error bound

We first study an encoding method in the absence of DoS attacks.

Lemma 4.1: Consider the system combined with $\Sigma_P$ in (1) and $\Sigma_C$ in (2). Assume that $|e_{R,k}|_\infty \leq E_{R,k}$, and set
\begin{align}
E_{R,k+1} = \theta E_{R,k} \quad (21)
\end{align}
where $\theta$ is defined by (17). Then we have $|e_{R,k+1}|_\infty \leq E_{R,k+1}$.

Proof: We see from (1) and (2) that the state estimation error $e_k$ satisfies
\begin{align}
e_{k+1} = (A - LC)e_k + L(y_k - q_k).
\end{align}
Since $e_{R,k} = R e_k$, it follows that
\begin{align}
e_{R,k+1} = R(A - LC)R^{-1}e_{R,k} + RL(y_k - q_k). \quad (22)
\end{align}
Therefore, we have from (9) that
\begin{align}
|e_{R,k+1}|_\infty \\
\leq \|R(A - LC)R^{-1}\|_\infty \cdot |e_{R,k}|_\infty + \|RL\|_\infty \cdot |y_k - q_k|_\infty \\
\leq \left( \|R(A - LC)R^{-1}\|_\infty + \frac{\|RL\|_\infty \cdot \|CR^{-1}\|_\infty}{N} \right) E_{R,k}.
\end{align}
Thus, $E_{R,k+1}$ defined by (21) satisfies $|e_{R,k+1}|_\infty \leq E_{R,k+1}$.

Next we investigate the error bound $E_{R,k+1}$ if a DoS attack occurs at time $k$.

Lemma 4.2: Consider the system combined with $\Sigma_P$ in (1) and $\Sigma_C$ in (3). Assume that $|e_{R,k}|_\infty \leq E_{R,k}$, and set
\begin{align}
E_{R,k+1} = \theta_a E_{R,k} \quad (23)
\end{align}
where $\theta_a$ is defined as in (16). Then we have $|e_{R,k+1}|_\infty \leq E_{R,k+1}$.

Proof: From (1) and (3), the estimation error $e_k$ satisfies
\begin{align}
e_{k+1} = Ae_k + \Omega (e_{R,k} + \varepsilon_{R,k+1}).
\end{align}
Thus, $e_{k+1}$ satisfies the inequality $|e_{R,k+1}|_\infty \leq E_{R,k+1}$.

B. State convergence

We show that the error bound $\{E_{R,k}\}$ in (15) converges to zero without saturating the quantizer if the DoS duration bound $\nu_d$ satisfies (19).

Lemma 4.3: Under the same hypotheses of Theorem 3.2, the error bound $\{E_{R,k}\}$ satisfies
\begin{align}
|e_{R,k}|_\infty \leq E_{R,k} \quad \forall k \geq 0 \quad (24)
\end{align}
and exponentially converges to zero: There exist $\Omega \geq E_{R,0}$ and $\gamma \in (0, 1)$ such that
\begin{align}
E_{R,k} \leq \Omega \gamma^k \quad \forall k \geq 0. \quad (25)
\end{align}

Proof: From Lemmas 4.1 and 4.2, we directly obtain the first conclusion (24), and it is enough to prove the second conclusion (25) under the condition (19).

Using the length $\Phi_a(k)$ of the time-period when DoS attacks are launched on the interval $[0, k]$, we can write $E_{R,k}$ as
\begin{align}
E_{R,k} = \Phi_a(k) \cdot \Phi_a(k) \cdot E_{R,0}.
\end{align}
Therefore, we have under Assumption 2.4 that
\begin{align}
E_{R,k} \leq \Phi_a(k)^\mu a(k)^k \cdot E_{R,0}.
\end{align}
Since the inequality (19) is equivalent to \( \theta_1 - \nu_d \cdot \hat{\theta}_0 \leq 1 \), it follows that the exponential convergence of the error bound (25) is achieved.

Using Lemma 4.3, we can prove Theorem 3.2 by the standard approach.

**Proof of Theorem 3.2:** The state \( x_k \) satisfies

\[
x_{k+1} = Ax_k - BKu_k
= (A - BK)x_k + BKR^{-1}e_k
= (A - BK)^{k+1}x_0 + \sum_{\ell=0}^{k} (A - BK)^{k-\ell} BKR^{-1} e_{R,\ell}.
\]

Therefore,

\[
|x_{k+1}|_\infty \leq \| (A - BK)^{k+1} \|_\infty \cdot |x_0|_\infty
+ \sum_{\ell=0}^{k} \| (A - BK)^{k-\ell} \|_\infty \cdot \| BKR^{-1} \|_\infty \cdot |e_{R,\ell}|_\infty.
\]

(26)

From Lemma 4.3, there exist \( \Omega \geq E_{R,0} \) and \( \gamma \in (0, 1) \) such that

\[
|e_{R,\ell}|_\infty \leq \Omega^\gamma \ell \quad \forall \ell \geq 0.
\]

(27)

Moreover, since \( A - BK \) is Schur stable by Assumption 2.2, there exist \( \Omega_K \geq 1 \) and \( \bar{\gamma} \in (\gamma, 1) \) such that

\[
\| (A - BK)^t \|_\infty \leq \Omega_K \bar{\gamma}^t \quad \forall t \geq 0.
\]

(28)

Substituting (27) and (28) into (26), we obtain

\[
|x_{k+1}|_\infty \leq \Omega_K \bar{\gamma}^{k+1} |x_0|_\infty + \Omega_K \| BKR^{-1} \|_\infty (k + 1) \bar{\gamma}^k.
\]

(29)

Since for every \( \epsilon > 0 \), there exists a constant \( \alpha \geq 1 \) such that \( k \bar{\gamma}^k \leq \alpha (\gamma + \epsilon)^k \) for all \( k \in \mathbb{Z}_+ \), it follows from (29) that \( |x_k|_\infty \) exponentially converges to zero. Additionally, since \( \bar{x}_k = x_k - R^{-1} e_{R,k} \), it follows that

\[
|\bar{x}|_\infty \leq |x_k|_\infty + \| R^{-1} \|_\infty E_{R,k},
\]

and hence \( |\bar{x}|_\infty \) also exponentially converges. This completes the proof.

\[\blacksquare\]

**V. ENCODING METHOD UNDER DoS FREQUENCY ASSUMPTION**

In Theorem 3.2, we obtained a sufficient condition on a DoS duration bound \( \nu_d \) for stabilization, using the linear transformation \( e_{R,k} = R e_k \) with the norm condition (14). On the other hand, the parameter \( R \) can be tuned for other purposes. For example, to allow longer DoS duration, we should choose the matrix \( R \) minimizing the growth rate \( \theta_0 = \| RAR^{-1} \|_\infty \) of the error bound. However, it is generally difficult to find an invertible matrix \( R \) satisfying these norm conditions simultaneously. In this section, we therefore generalize the encoding method to the case where the matrix \( R \) does not satisfy the norm condition (14), by placing an additional assumption on the frequency of DoS attacks.

Let us denote by \( \Phi_f \) the number of consecutive DoS attacks until time \( k \), namely, how many times the controller switches from \( \Sigma_C \) to \( \Sigma_C^c \) on \([0, k]\).

**Assumption 5.1 (Frequency of DoS attacks):** There exist \( \Pi_f \geq 0 \) and \( \nu_f \in (0, 1/2] \) such that for every \( k \geq 0 \), the DoS frequency \( \Phi_f(k) \) satisfies

\[
\Phi_f(k) \leq \Pi_f + \nu_f k.
\]

(30)

We call \( \nu_f \) a DoS frequency bound.

Let \( M_0 \geq 1, M \geq \| L \|_\infty \) and \( \rho \in (0, 1) \) satisfy

\[
\| R(A - LC)^t R^{-1} \|_\infty \leq M_0 \rho^t \quad \forall t \geq 0
\]

(31)

\[
\| R(A - LC)^t L \|_\infty \leq M \rho^t \quad \forall t \geq 0.
\]

(32)

Define constants \( \theta_a, \theta_c, \theta > 0 \) by

\[
\theta_a := \theta_a = \| RAR^{-1} \|_\infty
\]

(33)

\[
\theta_0 := M_0 \rho + \frac{M\| CR^{-1} \|_\infty}{N}
\]

(34)

\[
\theta := \rho + \frac{M\| CR^{-1} \|_\infty}{N}.
\]

(35)

Using these constants, we set the error bound \( \{ E_{R,k} \} \) to be

\[
E_{R,k+1} := \begin{cases} \theta a E_{R,k} & \text{if there is an attack at time } k \\ \theta_0 E_{R,k} & \text{elseif } k = 0 \text{ or there is an attack at time } k - 1 \\ \theta E_{R,k} & \text{otherwise.} \end{cases}
\]

(36)

Exploiting the assumption on the frequency of DoS attacks, we show that the encoding method with the above error bound \( \{ E_{R,k} \} \) leads to the closed-loop stability.

**Theorem 5.2:** Let Assumptions 2.1, 2.2, 2.4, and 5.1 hold. If the number of quantization steps \( N \), the DoS duration bound \( \nu_d \), and the DoS frequency bound \( \nu_f \) satisfy

\[
N > \frac{M\| CR^{-1} \|_\infty}{1 - \rho}
\]

(37)

\[
\nu_d < \frac{\log(1/\theta)}{\log(\theta_0/\theta)} - \frac{\log(\theta_0/\theta)}{\log(\theta_0/\theta)} \nu_f,
\]

(38)

then the encoding method with the error bound \( \{ E_{R,k} \} \) constructed by the update rule (36) achieves the state convergence (20).

We can prove Theorem 5.2 in a way similar to Theorem 3.2. However, we first have to modify the encoding method used in the absence of DoS attacks. Although this result is an easy extension of Theorem 4 in [24], we sketch a proof.

**Lemma 5.3:** Consider the system combined with \( \Sigma_P \) in (1) and \( \Sigma_C \) in (2). Assume that \( |e_{R,k}|_\infty \leq E_{R,k} \), and set

\[
E_{R,k+\ell+1} = \begin{cases} \theta_0 E_{R,k} & \text{if } \ell = 0 \\ \theta E_{R,k+\ell} & \text{otherwise,} \end{cases}
\]

(39)

where \( \theta_0 \) and \( \theta \) are defined by (34) and (35). Then we have \( |e_{R,k+\ell}|_\infty \leq E_{R,k+\ell} \) for all \( \ell \geq 1 \).

**Proof:** From the dynamics of the state estimation error \( e_{R,k} \) in (22), we obtain

\[
e_{R,k+\ell} = R(A - LC)^{\ell} R^{-1} e_{R,k}
+ \sum_{i=0}^{\ell-1} R(A - LC)^{\ell-i-1} L(y_{k+i} - q_{k+i}).
\]
It follows from (9) that
\[ |e_{R,k+i}| \leq \|R(A - LC)^{s}R^{-1}\|_{\infty} E_{R,k} \]
\[ + \sum_{i=0}^{\ell-1} \|R(A - LC)^{s-i-1}L\|_{\infty} \frac{\|CR^{-1}\|_{\infty}}{N} E_{R,k+i}. \]
Using the norm conditions (31) and (32), we further have
\[ |e_{R,k+i}| \leq M_0 \rho^s E_{R,k} + \frac{M_1 \|CR^{-1}\|_{\infty}}{N} \sum_{i=0}^{\ell-1} \rho^{s-i-1} E_{R,k+i}. \]
A simple calculation shows that \( E_{R,k} \) constructed by the update rule (39) satisfies
\[ E_{R,k+\ell} = M_0 \rho^s E_{R,k} + \frac{M_1 \|CR^{-1}\|_{\infty}}{N} \sum_{i=0}^{\ell-1} \rho^{s-i-1} E_{R,k+i} \]
for every \( \ell \geq 1 \). Combining (40) and (41), we obtain
\[ |e_{R,k+\ell}| \leq E_{R,k+\ell} \text{ for all } \ell \geq 1. \] This completes the proof.

**Proof of Theorem 5.2:** If the error bound \( E_{R,k} \) satisfies (24) and (25), then the same argument as that in the proof of Theorem 3.2 shows that the state convergence (20) is achieved. Lemmas 4.2 and 5.3 lead to (24), and (25) can be obtained as follows.

Assume that until the time \( k = T \), DoS attacks are launched at
\[ k = k_1, \ldots, k_i + d_i - 1 \quad \forall i = 1, \ldots, p \]
where \( k_1 \geq 0, k_p + d_p \leq T, d_i \geq 0 \quad (i = 1, \ldots, p) \), and
\[ k_i + d_i < k_{i+1} \quad \forall i = 1, \ldots, p - 1. \]
Note that \( p \) and \( \sum_{i=1}^{p} d_i \) are the total number and duration of DoS attacks on \([0, T]\), respectively.

In what follows, we assume that \( k_1 > 0 \) and \( k_p + d_p - 1 < T \), but in the case where \( k_1 = 0 \) or \( k_p + d_p - 1 = T \), one can prove the convergence of the error bound (25) in a similar way.

Define
\[ r_1 := k_1 - 1 \]
\[ r_i := k_i - k_{i-1} - d_{i-1} - 1 \quad \forall i = 2, \ldots, p \]
\[ r_{p+1} := T - k_p - d_p - 1. \]
Then \( r_i \geq 0 \) for every \( i = 1, \ldots, p+1 \). Since DoS attacks are not launched on the interval \([0, k_1]\), it follows from Lemma 5.3 that
\[ E_{R,k_1} = \theta^{r_1} \theta_0 E_{R,0}. \]
On the other hand, since DoS occurs on the interval \([k_1, \ldots, k_1 + d_1]\), we have from Lemma 4.2 that
\[ E_{R,k_1 + d_1} = \theta^{d_1} \theta_0 E_{R,k_1} = \theta^{d_1} \theta^{r_1} \theta_0 E_{R,0}. \]
Continuing in this way, we see that the error bound \( E_{R,T} \) at the time \( k = T \) satisfies
\[ E_{R,T} = \theta^{r_{p+1}} \theta_0 E_{R,k_p + d_p} \]
\[ = \theta \sum_{i=1}^{p+1} r_i \cdot \theta_0 ^{p+1} \cdot \theta_0 ^{r_{p+1}} \cdot \theta_0 E_{R,0}. \] By definition,
\[ \sum_{i=1}^{p} r_i = T - (p + 1) - \sum_{i=1}^{p} d_i. \]
Moreover, it follows from Assumptions 2.4 and 5.1 that
\[ \sum_{i=1}^{p} d_i = \Phi_d(T) \leq \Pi_d + \nu_d T \]
\[ p = \Phi_f(T) \leq \Pi_f + \nu_f T. \]
Therefore, we have from (42) that
\[ E_{R,T} = \left( \theta^T \cdot \theta^{(p+1)} \cdot \theta^{-\sum_{i=1}^{p} d_i} \right) \cdot \theta_0 ^{p+1} \cdot \theta_0 ^{\sum_{i=1}^{p} d_i} E_{R,0} \]
\[ = \theta^T \cdot \left( \frac{\theta_0}{\theta} \right) ^{p+1} \cdot \left( \frac{\theta_0}{\theta} \right) ^{\sum_{i=1}^{p} d_i} E_{R,0} \]
\[ \leq \theta^T \cdot \left( \frac{\theta_0}{\theta} \right) ^{\Pi_f + \nu_f T + 1} \cdot \left( \frac{\theta_0}{\theta} \right) ^{\Pi_d + \nu_d T} E_{R,0} \]
\[ = \theta_0 ^{\Pi_f + 1} \cdot \theta_0 ^{\Pi_d} \cdot \theta \cdot \left( \frac{\theta_0}{\theta} \right) ^{\nu_f} \cdot \theta \cdot \left( \frac{\theta_0}{\theta} \right) ^{\nu_d} \cdot \left( \frac{\theta_0}{\theta} \right) ^{T} E_{R,0}. \]
Since the inequality (38) is equivalent to
\[ \theta \cdot \left( \frac{\theta_0}{\theta} \right) ^{\nu} \cdot \left( \frac{\theta_0}{\theta} \right) ^{\nu} < 1, \]
it follows that the exponential convergence of the error bound (25) is achieved.

**Remark 5.4:** In the previous studies [10]–[12], [15], the assumption on the frequency of DoS attacks are used because, to achieve stability in the continuous-time domain, the frequency at which DoS are launched must be small compared with the sampling rate. Therefore, as in [14], the assumption on the DoS frequency bound is not needed for the discrete-time case. However, the output encoding method in Theorem 5.2 increases the error bound, \( E_{R,k+1} = \theta_0 E_{R,k} \), at the first time-step after DoS attacks occur, and therefore we here employ this frequency assumption to obtain a less conservative sufficient condition.

**Remark 5.5:** It follows from Proposition 3.1 that for every \( \epsilon > 0 \), we can obtain an invertible matrix \( R \in \mathbb{C}^{n \times n} \) satisfying
\[ \rho(A) \leq \rho_0 = \|R2A^{-1}\|_{\infty} \leq \rho(A) + \epsilon. \]
As seen in the numerical example of the next section, such a matrix \( R \) can often lead to the update rule (36) that allows longer DoS duration than the update rule (15) under sufficiently small DoS frequency.

**Remark 5.6:** If an invertible matrix \( R \in \mathbb{C}^{n \times n} \) satisfies (14), then we can recover Theorem 3.2 from Theorem 5.2. In fact, we can set the constants \( \rho, M_0, M \) in (31) and (32) to be
\[ \rho = \|R(A - LC)^{s}R^{-1}\|_{\infty}, \quad M_0 = 1, \quad M = \|RL\|_{\infty}. \]
Then \( \theta_0 \) and \( \theta \) defined in (34), (35) are equal to \( \theta \) in (17). Moreover, since \( \log(\theta_0/\theta) = 0 \), the conditions on \( N \) and \( \nu_d \) in Theorem 5.2 are the same as those in Theorem 3.2.
VI. NUMERICAL EXAMPLES

A linearized model of an unstable batch reactor studied in [25] is given by $\dot{x} = Ax + Bu, y =Cx$, where

$$
A := \begin{bmatrix}
1.38 & -0.2077 & 6.715 & -5.676 \\
-0.5814 & -4.29 & 0 & 0.675 \\
1.067 & 4.273 & -6.654 & 5.893 \\
0.48 & 4.273 & -1.343 & -2.104 \\
\end{bmatrix},
B := \begin{bmatrix}
0 & 0 \\
5.679 & 0 \\
1.136 & -3.146 \\
1.136 & 0 \\
\end{bmatrix},
C := \begin{bmatrix}
1 & 0 & 1 & -1 \\
0 & 1 & 0 & 0 \\
\end{bmatrix}.
$$

This model is widely used as a benchmark example, and we here discretize this plant with the sampling period $h = 0.3$. We set the partition number $N$ of the output quantization to be $N = 111$. We use the feedback gain $K$ that is the linear quadratic regulator whose state weighting matrix and input weighting matrix are the identity matrices $I_4$ and $I_2$. We also set the observer gain $L$ that is the steady-state Kalman filter whose covariances of the process noise and measurement noise are $I_4$ and $0.1 \times I_2$.

The closed-loop system with the encoding method of Theorem 3.2 is asymptotically stable under the DoS duration

$$
\nu_d < 0.107,
$$

where we construct the transformation matrix $R$ so that $\| R(A - LC)R^{-1} \|_{\infty} = \rho(A - LC)$. On the other hand, the encoding method of Theorem 5.2 achieves the closed-loop stability if the DoS duration and frequency bounds $\nu_d$ and $\nu_f$ satisfy

$$
\nu_d < 0.2796 - 1.614\nu_f,
$$

where $R$ is chosen so that $\| RAR^{-1} \|_{\infty} = \rho(A)$. Therefore, if the frequency of DoS attacks is sufficiently small, then the encoding method of Theorem 5.2 allows longer duration of DoS attacks without compromising the closed-loop stability in this example. On the other hand, if we can ensure (46), then we do not need to know the attack frequency and the encoding method of Theorem 5.2 can tolerate DoS attacks with large frequency.

Let us denote the state $x$ and its estimate $\hat{x}$ by $x = [x^1 \ x^2 \ x^3 \ x^4]^T$ and $\hat{x} = [\hat{x}^1 \ \hat{x}^2 \ \hat{x}^3 \ \hat{x}^4]^T$, respectively. For the computation of time responses, we set the initial state $x_0$ and its bound $E_0$ to be $x_0 = [1 \ -0.5 \ 0 \ 1]^T$ and $E_0 = 1.1$. We first show time responses under the encoding method of Theorem 3.2 without assuming any frequency conditions of DoS attacks. Fig. 2 depicts the stable case where DoS attacks satisfy the duration condition (4) with $(\Pi_d, \nu_d) = (1, 0.10)$. DoS attacks are launched on the intervals that are colored in gray. Fig. 2a illustrates the trajectories of $x^1$ and $\hat{x}^1$, which oscillate after DoS attacks unlike the case without quantization. This oscillation is caused by a large error bound $E_R$ due to the DoS attack, as shown in Fig. 2b. Therefore, even after the DoS attack, the quantized output $q$ is zero until the error bound becomes small, and the Luenberger observer does not estimate the plant state correctly. However, since the DoS duration $\nu_d = 0.10$ satisfies (46), the error bound $E_R$ converges to zero, which leads to the closed-loop stability.

Fig. 3 illustrates the trajectories of $x^1$, $\hat{x}^1$ and $E_R$ under DoS attacks with $(\Pi_d, \nu_d) = (1, 0.11)$. The DoS duration $\nu_d = 0.11$ does not satisfy (46), and we see from Fig. 3b that DoS attacks make the error bound $E_R$ diverge. As the error bound $E_R$ increases, the upper bound of the quantization error $y - q$ becomes large. This error leads to the instability of the closed-loop system as shown in Fig. 3a, although the difference between the bound $\nu_d < 0.107$ in (46) and $\nu_d = 0.11$ used in Fig. 3 is small. We see that the sufficient condition (38) is fairly tight in this example.

Finally, we compute a time response by using the encoding method of Theorem 5.2, and Fig. 3 illustrates it under DoS attacks satisfying the duration condition (4) with $(\Pi_d, \nu_d) = (1, 0.20)$ and the frequency condition (30) with $(\Pi_f, \nu_f) = (1, 0.04)$. Note that if we set the DoS frequency bound $\nu_f$ to be $\nu_f = 0.04$, then the DoS duration bound $\nu_d$ must satisfy $\nu_d < 0.215$ to achieve (47). The error bound $E_R$ rapidly increases during the period $[40, 60]$ due to the large frequency of DoS attacks, but the closed-loop system is stable despite the longer DoS duration. This is because the encoding method in Theorem 5.2 has a small growth rate $\theta_a = 1.817$ in the presence of DoS attacks, compared with the growth rate $\theta_a = 5.678$ of the encoding method in Theorem 3.2.

VII. CONCLUDING REMARKS

We studied the problem of quantized output feedback stabilization under DoS attacks. The proposed encoding methods decrease the quantization range in the absence of
DoS attacks but increase the range for avoiding the saturation of the quantizer if DoS attacks occur. We obtained sufficient conditions on the DoS duration and frequency bounds for stabilization with finite-data rates, which are characterized by the growth and decay rates of the quantization range in the presence and absence of DoS attacks. Future work involves addressing more general systems by incorporating disturbances, noise, and model uncertainty.

REFERENCES

[1] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Trans. Automat. Control, vol. 59, pp. 1454–1467, 2014.

[2] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in Proc. ACC’15, 2015.

[3] Y. Shoukry and P. Tabuada, “Event-triggered state observers for sparse sensor noise/attacks,” IEEE Trans. Automat. Control, vol. 61, pp. 2079–2091, 2016.

[4] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, “A survey of recent results in networked control systems,” Proc. IEEE, vol. 95, pp. 138–162, 2007.

[5] L. Zhang, H. Gao, and O. Kaynak, “Network-induced constraints in networked control systems—a survey,” IEEE Trans. Ind. Inform., vol. 9, pp. 406–416, 2013.

[6] S. Amin, A. A. Cárdenas, and S. S. Sastry, “Safe and secure networked control systems under denial-of-service attacks,” in Proc. 12th HSCC, 2009.

[7] S. Bhattacharya, A. Gupta, and T. Başar, “Jamming in mobile networks: A game-theoretic approach,” J. Numer. Algeb. Control Optim., vol. 3, pp. 1–30, 2013.

[8] S. Liu, P. X. Liu, and A. E. Saddik, “A stochastic game approach to the security issue of networked control systems under jamming attacks,” J. Frankl. Inst., vol. 351, pp. 4570–4583, 2014.

[9] 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.

[10] C. De Persis and P. Tesi, “Input-to-state stabilizing control under denial-of-service,” IEEE Trans. Automat. Control, vol. 60, pp. 2930–2944, 2015.

[11] ——, “Networked control of nonlinear systems under denial-of-service,” Systems & Control Letters, vol. 96, pp. 124–131, 2016.

[12] S. Feng and P. Tesi, “Resilient control under denial-of-service: Robust design,” Automatica, vol. 79, pp. 42–51, 2017.

[13] A. Cetinkaya, H. Ishii, and T. Hayakawa, “Enhanced stability analysis for networked control systems under random and malicious packet losses,” in Proc. 55th IEEE CDC, 2016.

[14] ——, “Networked control under random and malicious packet losses,” IEEE Trans. Automat. Control, vol. 62, pp. 2434–2449, 2017.

[15] D. Senjolyuny, P. Tesi, and C. De Persis, “A jamming-resilient algorithm for self-triggered network coordination,” 2017, to appear in IEEE Trans. Control Network Systems.

[16] G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans, “Feedback control under data rate constraints: An overview,” Proc. IEEE, vol. 95, pp. 108–137, 2007.

[17] H. Ishii and K. Tsumura, “Data rate limitations in feedback control signals,” Automatica, vol. 39, pp. 1543–1554, 2003.

[18] D. Liberon, “Stabilization of linear systems with limited information feedback,” IEEE Trans. Automat. Control, vol. 50, pp. 910–915, 2005.

[19] D. Liberon, “Finite data-rate feedback stabilization of switched and linear hybrid systems,” Automatica, vol. 52, pp. 409–420, 2014.

[20] M. Wakaiki and Y. Yamamoto, “Stabilization of switched systems with sampled and quantized output feedback,” IET Control Theory Appl., vol. 11, pp. 1913–1921, 2017.

[21] D. Liberon, “Stabilization of linear systems with limited information,” IEEE Trans. Automat. Control, vol. 48, pp. 304–307, 2003.

[22] M. Wakaiki, Y. Yamamoto, and M. Wakaiki, “Stabilization of switched systems by Luenberger observers,” in Proc. 20th IFAC WC, 2017, arXiv:1703.06567.

[23] H. H. Rosenbrock, Computer-Aided Control System Design. New York: Academic Press, 1974.