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

Dynamic Quantized Consensus of General Linear Multi-agent Systems under Denial-of-Service Attacks

Shuai Feng * **Hideaki Ishii** *

* *Department of Computer Science, Tokyo Institute of Technology, Yokohama 226-8542, Japan (e-mail: feng@sc.dis.titech.ac.jp, ishii@c.titech.ac.jp).*

Abstract: In this paper, we study a multi-agent consensus problem under Denial-of-Service (DoS) attacks with data rate constraints. We consider leaderless consensus under an undirected communication graph and assume that the graph is connected in the absence of DoS. The dynamics of the agents take general forms modeled as homogeneous linear time-invariant systems. In our analysis, we derive specific bounds on the data rate for the multi-agent system to achieve consensus even in the presence of DoS attacks. The main contribution of the paper is the characterization of the trade-off between the tolerable DoS attack level and the required data rates for the communication among the agents. To avoid quantizer saturation under DoS attacks, we employ dynamic quantization with zoom-in and zoom-out capabilities.

Keywords: Multi-agent systems; Denial-of-Service; Control under quantization; Cyber-physical systems.

1. INTRODUCTION

In the last two decades, the control of multi-agent systems has attracted substantial attention due to the progress of technologies in communication and computation areas, and some of the key applications can be found in formation control, control of large-scale systems and distributed sensor networks (Bullo, 2019). In particular, nowadays a closed-loop control system integrates sensors, computers and communication devices, which complies with the concept of cyber-physical systems (CPSs). While the industry notably benefits from the technology bloom in CPSs, a challenging situation also emerges along with the benefits, malicious cyber attacks on CPSs such as deceptive attacks and Denial-of-Service (DoS) (Cheng et al., 2017; Teixeira et al., 2015).

This paper deals with DoS attacks, which induce packet drops maliciously and hence corrupt the availability of data. The communication failures induced by DoS can exhibit a temporal profile quite different from the one induced by genuine packet losses; particularly packet dropouts induced by DoS need not follow a given class of probability distributions (Amin et al., 2009), and therefore the analysis techniques relying on probability may not be applicable. This poses new challenges in theoretical analysis and controller design.

In this paper, our focus is on the effects of DoS attacks on multi-agent systems. Recently, systems under DoS attacks have been studied from a control-theoretic viewpoint (Cetinkaya et al., 2019, 2017; De Persis and Tesi, 2015; Feng et al., 2020; Feng and Tesi, 2017; Feng and Hu, 2019; Li et al., 2017; Nugraha et al., 2019; Qin et al., 2017; Senejohnny et al., 2017; Xu et al., 2019). In (De Persis and Tesi, 2015), a framework is introduced where DoS attacks are characterized by their levels of *frequency* and *duration*. There, they derived an explicit characterization of DoS frequency and duration under which stability can be preserved through state-feedback control. For multi-agent systems under DoS, there are some recent results for consensus problems with infinite data-rate networks Feng and Hu (2019); Xu et al. (2019). For example, the paper (Feng and Hu, 2019) presents theoretical as well as comprehensive simulation studies for continuous-time system consensus under DoS attacks with the utilization of event-triggered control, where both leaderless and leader-follower consensus are considered.

Even without attacks, the real-time data exchanged within networked control systems may suffer from communication constraints. In particular, we address issues arising from constraints on data rate that can occur in multi-agent systems. Such a constraint can be modeled as introducing quantization with finite number of discrete outputs. Centralized systems under quantization have been extensively studied in the last two decades, for example by the seminal papers (Liberzon, 2003; Nair and Evans, 2004; Tatikonda and Mitter, 2004). The results in the papers show that insufficient bit rate in communication channel influences the stability of a networked control system. The work (Feng et al., 2020) extended these results to the case with DoS attacks. In the last decade, the quantized consensus problems of multi-agent systems have been broadly studied (Cai and Ishii, 2011; Carli et al., 2010; Kashyap et al., 2007; Li et al., 2010; Ma et al., 2018; Qiu et al., 2015; You and Xie, 2011) and some of them take data rate constraints into considerations. Also, the related problem of resilient consensus is studied in (Dibaji et al., 2017; Wang and Ishii, 2019) where some agents are malicious and may prevent consensus to take place.Our paper is particularly inspired by the quantized control of multi-agent systems in the work (You and Xie, 2011).

More specifically in this paper, we address two issues related to the joint effects of DoS attacks and data rate constraints. (i) For

[1] 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.

the dynamic quantization, when the global information of agent states is not available, a critical issue is to keep the states of each agent within the quantization range so as to avoid any quantizer saturation. Especially, when data may be missing due to DoS, we must keep track of the states by zooming out and scaling up the quantization range even if the quantization becomes coarse. (ii) After constructing the quantization of the states properly, the next issue is to find the tolerable bound of DoS attacks for achieving consensus. Especially, if the agent dynamics is unstable, sufficient data must be exchanged within the systems to realize the global objective of consensus. We will explicitly demonstrate how the resilience against DoS is affected by the available data rate in communication. Furthermore, it will be shown that in the absence of DoS attacks, our result is consistent with the one in (You and Xie, 2011).

This paper is organized as follows. In Section 2, we introduce the framework consisting of multi-agent systems of general dynamics, the class of DoS attacks and the control objective studied here. Section 3 presents the controller architecture with the zoom-in and zoom-out dynamic quantization mechanism. Section 4 presents the main result of this paper, showing sufficient conditions for data rate without overflow and DoS bound under which consensus can be achieved. A numerical example is presented in Section 5, and finally Section 6 ends the paper with conclusions and possible future research directions.

Due to space limitation, we omit all the proofs in this paper and refer the readers to (Feng and Ishii, 2020) for more details.

Notation. We denote by $\mathbb{R}$ the set of reals. Given $b \in \mathbb{R}$, $\mathbb{R}_{\geq b}$ and $\mathbb{R}_{>b}$ denote the sets of reals no smaller than b and reals greater than b, respectively; $\mathbb{R}_{\leq b}$ and $\mathbb{R}_{<b}$ represent the sets of reals no larger than b and reals smaller than b, respectively; $\mathbb{Z}$ denotes the set of integers. For any $c \in \mathbb{Z}$, we denote $\mathbb{Z}_{\geq c} := \{c, c+1, \cdots\}$. Let $\lfloor v \rfloor$ be the floor function such that $\lfloor v \rfloor = \max\{o \in \mathbb{Z} | o \leq v\}$. Given a vector y and a matrix Γ, let $\|y\|$ and $\|y\|_\infty$ denote the ℓ_2 and ℓ_∞ norms of vector y, respectively, and $\|\Gamma\|$ and $\|\Gamma\|_\infty$ represent the corresponding induced norms of matrix Γ. $\rho(\Gamma)$ denotes the spectral radius of Γ. Given an interval $\mathcal{I}$, $|\mathcal{I}|$ denotes its length. The Kronecker product is denoted by $\otimes$. Let $\mathbf{0}$ and $\mathbf{1}$ denote column vectors with compatible dimensions, having all 0 and 1 elements, respectively.

2. FRAMEWORK: MULTI-AGENT SYSTEMS AND DOS

2.1 Communication graph

We let graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ denote the communication topology between agents, where $\mathcal{V} = \{1, 2, \cdots, N\}$ denotes the set of agents and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of edges. Let $\mathcal{N}_i$ denote the set of the neighbors of agent i, where $i = 1, 2, \cdots, N$. In this paper, we assume that the graph $\mathcal{G}$ is undirected and connected, *i.e.* if $j \in \mathcal{N}_i$, then $i \in \mathcal{N}_j$. Let $A_\mathcal{G} = [a_{ij}] \in \mathbb{R}^{N \times N}$ denote the adjacency matrix of the graph $\mathcal{G}$, where $a_{ij} > 0$ if and only if $j \in \mathcal{N}_i$ and $a_{ii} = 0$. Define the Laplacian matrix $L_\mathcal{G} = [l_{ij}] \in \mathbb{R}^{N \times N}$, in which $l_{ii} = \sum_{j=1}^N a_{ij}$ and $l_{ij} = -a_{ij}$ if $i \neq j$. Let λ_i $(i = 1, 2, \cdots, N)$ denote the eigenvalues of $L_\mathcal{G}$ and in particular we have $\lambda_1 = 0$ due to the graph being connected.

2.2 System description

The agents interacting over the network $\mathcal{G}$ are expressed as homogeneous linear time-invariant systems. For each $i = 1, 2, \cdots, N$, agent i is given as a sampled-data system with sampling period $\Delta \in \mathbb{R}_{>0}$ in the form of

$$x_i(k\Delta) = Ax_i((k-1)\Delta) + Bu_i((k-1)\Delta) \tag{1}$$

where $k \in \mathbb{Z}_{\geq 1}$, $A \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{n \times w}$. It is assumed that (A, B) is stabilizable. $x_i(k\Delta) \in \mathbb{R}^n$ denotes the state of agent i with $x_i(0) \in \mathbb{R}^n$ as the initial condition. We assume that an upper bound is known, *i.e.* $\|x_i(0)\|_\infty \leq C_{x_0} \in \mathbb{R}_{>0}$. Let $u_i((k-1)\Delta) \in \mathbb{R}^w$ denote its control input, whose computation will be given later.

We assume that the communication channel among the agents is bandwidth limited and subject to DoS, where transmission attempts take place periodically at $k\Delta$ with $k \in \mathbb{Z}_{\geq 1}$. Moreover, we assume that the transmission is acknowledgment based and free of delay. This implies that the decoders send acknowledgments to the encoders immediately when they receive encoded signals successfully. If some acknowledgments are not received by the encoders, it implies that due to the presence of DoS, the decoders do not receive any data at all, and hence they do not send acknowledgments.

Agent $i = 1, 2, \cdots, N$ can only exchange information with its neighbor agents $j \in \mathcal{N}_i$. Due to the constraints of network bandwidth, signals are encoded with a limited number of bits at transmission attempts. In the presence of DoS, some of the transmission attempts may fail. For the ease of illustration, we let s_r represent the instants of successful transmissions. Note that $s_0 \in \mathbb{R}_{\geq \Delta}$ represents the instant when the first successful transmission occurs. Also, we let s_{-1} denote the time instant 0.

2.3 Time-constrained DoS

In this paper, we refer to DoS as the event for which all the encoded signals cannot be received by the decoders and it affects all the agents. We consider a general DoS model that describes the attacker's action by the frequency of DoS attacks and their duration. Let $\{h_q\}_{q \in \mathbb{Z}_0}$ with $h_0 \geq \Delta$ denote the sequence of DoS *off/on* transitions, that is, the time instants at which DoS exhibits a transition from zero (transmissions are successful) to one (transmissions are not successful). Hence, $H_q := \{h_q\} \cup [h_q, h_q + \tau_q[$ represents the q-th DoS time-interval, of a length $\tau_q \in \mathbb{R}_{\geq 0}$, over which the network is in DoS status. If $\tau_q = 0$, then H_q takes the form of a single pulse at h_q. Given $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$, let $n(\tau, t)$ denote the number of DoS *off/on* transitions over $[\tau, t]$, and let $\Xi(\tau, t) := \bigcup_{q \in \mathbb{Z}_0} H_q \bigcap [\tau, t]$ be the subset of $[\tau, t]$ where the network is in DoS status.

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

$$n(\tau, t) \leq \eta + \frac{t - \tau}{\tau_D} \tag{2}$$

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

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

$$|\Xi(\tau, t)| \leq \kappa + \frac{t - \tau}{T} \tag{3}$$

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

Remark 1. Assumptions 1 and 2 do only constrain a given DoS signal in terms of its *average* frequency and duration. Following

(Hespanha and Morse, 1999), τ_D can be defined as the average dwell-time between consecutive DoS off/on transitions, while η is the chattering bound. Assumption 2 expresses a similar requirement with respect to the duration of DoS. It expresses the property that, on the average, the total duration over which communication is interrupted does not exceed a certain *fraction* of time, as specified by $1/T$. Like η, the constant κ plays the role of a regularization term. It is needed because during a DoS interval, one has $|\Xi(h_q, h_q + \tau_q)| = \tau_q > \tau_q/T$. Thus κ serves to make (3) consistent. Conditions $\tau_D > 0$ and $T > 1$ imply that DoS cannot occur at an infinitely fast rate or be always active. ■

The next lemmas relate DoS parameters and the number of unsuccessful and successful transmissions, respectively.

Lemma 1. Consider a periodic transmission with sampling interval Δ along with DoS attacks in Assumptions 1 and 2. If $1/T + \Delta/\tau_D < 1$, then m, representing the number of unsuccessful transmissions between s_{r-1} and s_r with $r = 0, 1, \cdots$, satisfies

$$\begin{aligned} m =& \ (s_r - s_{r-1})/\Delta - 1 \\ \leq M =& \left\lfloor (\kappa + \eta\Delta)\left(1 - 1/T - \Delta/\tau_D\right)^{-1}/\Delta \right\rfloor \in \mathbb{Z}_{\geq 0}. \end{aligned} \tag{4}$$

■

Lemma 2. Consider the DoS attacks characterized by Assumptions 1 and 2 and the network sampling period Δ. If $1/T + \Delta/\tau_D < 1$, then $T_S(\Delta, k\Delta)$, denoting the number of successful transmissions within the interval $[\Delta, k\Delta]$, satisfies

$$T_S(\Delta, k\Delta) \geq \left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D}\right) k - \frac{\kappa + \eta\Delta}{\Delta}. \tag{5}$$

■

Remark 2. If the network is free of DoS attacks ($T = \tau_D = \infty$ and $\kappa = \eta = 0$), then $m = Q = 0$ and $T_S(\Delta, k\Delta) = k$, *i.e.* there is no failed transmissions between s_{r-1} and s_r for every r, and every transmission attempt will be successful, respectively. Therefore, they are reduced to nominal standard periodic transmissions. ■

2.4 Control objective

The objective of this paper is to design a quantized controller, possibly dynamic, in such a way that a finite-level quantizer is not overflowed and the multi-agent systems (1) can tolerate as many DoS attacks as possible for reaching consensus. Specifically, we introduce the average of the states

$$\bar{x}(k\Delta) = (\sum_{i=1}^{N} x_i(k\Delta))/N \in \mathbb{R}^n \tag{6}$$

and consensus among the agents is defined by

$$\lim_{k\to\infty} \|x_i(k\Delta) - \bar{x}(k\Delta)\|_\infty = 0, \ \ i = 1, 2, \cdots, N. \tag{7}$$

3. DYNAMIC QUANTIZED CONTROL UNDER DOS

For the ease of illustration, in the remainder of the paper we simply let k represent $k\Delta$, *e.g.* $x_i(k)$ represents $x_i(k\Delta)$.

3.1 Uniform quantizer

The limitation of bandwidth implies that transmitted signals are subject to quantization. Let $\chi \in \mathbb{R}$ be the original scalar signal before quantization and $q_R(\cdot)$ be the quantization function for scalar input values as

$$q_R(\chi) = \begin{cases} 0 & -\sigma < \chi < \sigma \\ 2z\sigma & (2z-1)\sigma \leq \chi < (2z+1)\sigma \\ 2R\sigma & \chi \geq (2R+1)\sigma \\ -q_R(-\chi) & \chi \leq -\sigma \end{cases} \tag{8}$$

where $R \in \mathbb{Z}_{>0}$ is to be designed and $z = 1, 2, ..., R$, and $\sigma \in \mathbb{R}_{>0}$. If the quantizer is unsaturated, then the error induced by quantization satisfies

$$|\chi - q_R(\chi)| \leq \sigma, \text{ if } |\chi| \leq (2R+1)\sigma \tag{9}$$

Observe that the quantizer has $2R + 1$ levels and is determined by two parameters σ and R, which determine the density and quantization range of the quantizer, respectively. Moreover, we define the vector version of the quantization function as $Q_R(\beta) = [\, q_R(\beta_1) \ q_R(\beta_2) \ \cdots \ q_R(\beta_f)\,]^T \in \mathbb{R}^f$, where $\beta = [\beta_1 \ \beta_2 \ \cdots \beta_f]^T \in \mathbb{R}^f$ with $f \in \mathbb{Z}_{\geq 1}$.

3.2 Control architecture

For each agent i, the control input $u_i(k)$ is expressed as a function of the relative states available locally at time k. Specifically, it is given by

$$u_i(k) = K \sum_{j=1}^{N} a_{ij}(\hat{x}_j^i(k) - \hat{x}_i^i(k)), k = 0, 1, \cdots \tag{10}$$

where $\hat{x}_j^i \in \mathbb{R}^n$ denotes the estimation of the state of agent j by agent i. Here we assume that there exists a feedback gain $K \in \mathbb{R}^{w\times n}$ such that the spectral radius of

$$J(1) = \text{diag}(A - \lambda_2 BK, \cdots, A - \lambda_N BK) \tag{11}$$

satisfies $\rho(J(1)) < 1$. This is a necessary and sufficient condition for the agents to reach consensus when no DoS is present and infinite bandwidth is available for communication (Li et al., 2009).

In (10), the estimate of the state of agent j by agent i equals to the one estimated by agent ϵ such that $\hat{x}_j^i(k) = \hat{x}_j^\epsilon(k) = \hat{x}_j^j(k)$ with $i, \epsilon \in \mathcal{N}_j$, then we omit the superscripts there and let

$$u_i(k) = K \sum_{j=1}^{N} a_{ij}(\hat{x}_j(k) - \hat{x}_i(k)), k = 0, 1, \cdots. \tag{12}$$

Agent i estimates the states of its neighbors based on the information available from communication. Also, to stay consistent with the neighbors, it will compute the estimate of its own. These estimated states will be computed at each time $k = 1, 2, \cdots$ as

$$\hat{x}_j(k) = \begin{cases} A\hat{x}_j(k-1) + \theta(k-1)\hat{Q}_j(k) & \text{if } k \notin H_q \\ A\hat{x}_j(k-1) & \text{if } k \in H_q \end{cases} \tag{13}$$

where $j \in \{i\} \cup \mathcal{N}_i$ and the initial estimates will be set as $\hat{x}_j(0) = \mathbf{0}$. Here, $\hat{Q}_j(k) \in \mathbb{R}^n$ contains the information of $x_j(k)$ and is defined as

$$\hat{Q}_j(k) = Q_R\left(\frac{x_j(k) - A\hat{x}_j(k-1)}{\theta(k-1)}\right), \ k = 1, 2, \cdots. \tag{14}$$

An important parameter in the quantization in (14) is the scaling parameter $\theta(k-1)$. By adjusting its size dynamically, the state will be kept within the bounded quantization range and quantized without saturation. The scaling parameter $\theta(k) \in \mathbb{R}_{>0}$ can be updated as

$$\theta(k) = \begin{cases} \gamma_1\theta(k-1) & \text{if } k \notin H_q \\ \gamma_2\theta(k-1) & \text{if } k \in H_q \end{cases}, \ \ k = 1, 2, \cdots \tag{15}$$

with $\theta(0) = \theta_0 \in \mathbb{R}_{>0}$, where $0 < \gamma_1 < 1$ and $\gamma_2 > 0$. The design of γ_1, γ_2 and θ_0 will be specified later. Observe that the scaling parameter is updated locally at each agent by checking the presence of DoS attacks over time.

Due to the constraints of channel bandwidth, the information about the state $x_j(k)$ is quantized into $\hat{Q}_j(k)$ as in (14). If the transmission attempts succeed, the decoders estimate $x_j(k)$ by the first equation in (13) and the scaling parameter θ in the encoders and decoders is updated as in the first equation in (15). If the transmission attempt fails, then the information of $x_j(k)$ cannot be acquired by the decoders since $\hat{Q}_j(k)$ is corrupted by DoS. Then, the decoders estimate $x_j(k)$ by the second equation in (13) and the scaling parameter θ in the encoders and decoders updates as in the second equation in (15).

Note that in the control input computation (12), we use $\hat{x}_i(k)$ to compute $u_i(k)$ instead of $x_i(k)$. Due to space limitation, we omit the details of the rationales and refer the readers to the discussion regarding (52) in You and Xie (2011) and the references therein.

Let $\hat{x}(k) = [\hat{x}_1^T(k)\ \hat{x}_2^T(k) \cdots \hat{x}_N^T(k)]^T \in \mathbb{R}^{nN}$ and $Q(k) = [\hat{Q}_1^T(k)\ \hat{Q}_2^T(k) \cdots \hat{Q}_N^T(k)]^T \in \mathbb{R}^{nN}$. One can obtain the compact form of (13) as

$$\hat{x}(k) = \begin{cases} (I_N \otimes A)\hat{x}(k-1) + \theta(k-1)Q(k) & \text{if } k \notin H_q \\ (I_N \otimes A)\hat{x}(k-1) & \text{if } k \in H_q \end{cases} \tag{16}$$

for $k = 1, 2, \cdots$. Let $e_i(k) = x_i(k) - \hat{x}_i(k) \in \mathbb{R}^n$ denote the estimation error and let $e(k) = [e_1^T(k)\ e_2^T(k)\ \cdots\ e_N^T(k)]^T \in \mathbb{R}^{nN}$ and $x(k) = [x_1^T(k)\ x_2^T(k) \cdots x_N^T(k)]^T \in \mathbb{R}^{nN}$. Then one obtains the compact form of the dynamics of the agents as

$$x(k) = Gx(k-1) + Le(k-1) \tag{17}$$

where

$$G = I_N \otimes A - L_{\mathcal{G}} \otimes BK, \ \ L = L_{\mathcal{G}} \otimes BK. \tag{18}$$

Recall the $\bar{x}(k)$ in (6), then the discrepancy between the state of agent i and $\bar{x}$ is denoted by $\delta_i(k) = x_i(k) - \bar{x}(k) \in \mathbb{R}^n$. By defining $\delta(k) = [\delta_1^T(k)\ \delta_2^T(k)\ \cdots\ \delta_N^T(k)]^T \in \mathbb{R}^{nN}$, one has $x(k) = \delta(k) + I_N \otimes \bar{x}(k)$. By applying it into (17), one obtains

$$\delta(k) = G\delta(k-1) + Le(k-1). \tag{19}$$

It is now clear that if $\|\delta(k)\|_\infty \to 0$ as $k \to \infty$, the consensus of the multi-agent systems (1) is achieved as in (7). Under DoS attacks, $e(k)$ may diverge and then the consensus of the multi-agent systems may not be achieved.

4. MAIN RESULT

This section first presents the dynamics of the multi-agent systems under quantization in the absence and presence of DoS attacks. Then we will present the main result.

4.1 Dynamics of the multi-agent systems

In this subsection, we formulate the dynamics of the multi-agent systems in the absence and presence of DoS. First, we present the dynamics of $e(k)$ with $e(k-1)$ and $\delta(k-1)$.

If the transmission succeeds such that $k \notin H_q$ for $k = 1, 2, \cdots$, then according to (16), one has

$$\begin{aligned} e(k) &= x(k) - \hat{x}(k) \\ &= x(k) - (I_N \otimes A)\hat{x}(k-1) - \theta(k-1)Q(k) \\ &= x(k) - (I_N \otimes A)\hat{x}(k-1) \\ &\quad - \theta(k-1)Q_R\left(\frac{x(k) - (I_N \otimes A)\hat{x}(k-1)}{\theta(k-1)}\right). \end{aligned} \tag{20}$$

Note that $x(k) - (I_N \otimes A)\hat{x}(k-1) = He(k-1) - L\delta(k-1)$, where

$$H = I_N \otimes A + L_{\mathcal{G}} \otimes BK. \tag{21}$$

Then (20) can be rewritten as

$$\begin{aligned} e(k) &= He(k-1) - L\delta(k-1) \\ &\quad - \theta(k-1)Q_R\left(\frac{He(k-1) - L\delta(k-1)}{\theta(k-1)}\right). \end{aligned} \tag{22}$$

If the transmission fails such that $k \in H_q$ for $k = 1, 2, \cdots$, then in view of (16), one has

$$\begin{aligned} e(k) &= x(k) - (I_N \otimes A)\hat{x}(k-1) \\ &= He(k-1) - L\delta(k-1). \end{aligned} \tag{23}$$

In the analysis above, we have presented the system dynamics with e and δ. To facilitate the analysis, we let $\alpha(k) =: \delta(k)/\theta(k)$ and $\xi(k) =: e(k)/\theta(k)$, where $\theta(k)$ is given in (15). Then we formulate the system dynamics in terms of α and ξ.

If the transmission succeeds such that $k \notin H_q$, in view of the first of (15), (19) and (22), one has

$$\alpha(k) = \frac{G}{\gamma_1}\alpha(k-1) + \frac{L}{\gamma_1}\xi(k-1) \tag{24}$$

$$\begin{aligned} \xi(k) &= \frac{H\xi(k-1) - L\alpha(k-1)}{\gamma_1} \\ &\quad - \frac{Q_R\left(H\xi(k-1) - L\alpha(k-1)\right)}{\gamma_1} \end{aligned} \tag{25}$$

It is easy to infer that if $\|H\xi(k-1) - L\alpha(k-1)\|_\infty \le (2R+1)\sigma$, then by (9) one has $\|\xi(k)\|_\infty \le \sigma/\gamma_1$.

If the transmission fails such that $k \in H_q$, then according to the second of (15), (19) and (23), one has

$$\alpha(k) = \frac{G}{\gamma_2}\alpha(k-1) + \frac{L}{\gamma_2}\xi(k-1) \tag{26}$$

$$\xi(k) = \frac{H}{\gamma_2}\xi(k-1) - \frac{L}{\gamma_2}\alpha(k-1) \tag{27}$$

Compared with (25), $\xi(k)$ induced by (27) may not satisfy $\|\xi(k)\|_\infty \le \sigma/\gamma_1$. In the event that $\|\xi(k)\|_\infty > \sigma/\gamma_1$, there is a possibility that $\|H\xi(k) - L\alpha(k)\|_\infty > (2R+1)\sigma$, which demonstrates that quantizer overflow occurs. In the following, with the control scheme introduced in (12) to (15), we will show that quantizer overflow will not occur by properly designing the scaling parameter $\theta(k)$ in (15), and then discuss the trade-offs between resilience and data rate.

4.2 Overflow-free quantizer and consensus

In this subsection, we will present the main result of this paper, showing the number of quantizer levels such that it is not overflowed, and a sufficient condition for consensus. Before presenting the main result, we first introduce some preliminaries that will be used in the theorem.

In view of the matrices G, L and H in (18) and (21), respectively, we define the matrices

$$\bar{A} = \begin{bmatrix} G & L \\ -L & H \end{bmatrix}, \ \bar{A}(m) = \bar{A}^m = \begin{bmatrix} \bar{A}_{11}(m) & \bar{A}_{12}(m) \\ \bar{A}_{21}(m) & \bar{A}_{22}(m) \end{bmatrix} \quad (28)$$

where $\bar{A}_{11}(m), \bar{A}_{12}(m), \bar{A}_{21}(m)$ and $\bar{A}_{22}(m)$ are compatible submatrices with dimensions nN in $\bar{A}(m)$ and the integer m satisfies $0 \leq m \leq M$ as in Lemma 1. Then, we define $G(m+1)$ and $\bar{G}(m+1)$ as

$$G(m+1) = (G\bar{A}_{11}(m) + L\bar{A}_{21}(m))/\gamma_2^m \quad (29)$$

$$\bar{G}(m+1) = (\Phi \otimes I_n)^T G(m+1)(\Phi \otimes I_n) \quad (30)$$

in which the unitary matrix Φ takes $\Phi = [\mathbf{1}/\sqrt{N} \ \phi_2 \ \cdots \ \phi_N] \in \mathbb{R}^{N\times N}$ where $\phi \in \mathbb{R}^N$ with $i = 2, 3, \cdots, N$ satisfies $\phi_i^T L_{\mathcal{G}} = \lambda_i \phi_i^T$. Let the matrix $J(m+1) \in \mathbb{R}^{n(N-1)\times n(N-1)}$ denote the remaining parts of $\bar{G}(m+1)$ in (30) after deleting the first n rows and columns. Then we define the set $\mathcal{J}$ as

$$\mathcal{J} := \{J(1), \cdots, J(m+1), \cdots, J(M+1)\}. \quad (31)$$

Note that $J(m+1)$ is reduced to $J(1)$ in (11) when $m = 0$, which is independent of γ_2. If $1 \leq m \leq M$, then $J(m+1)$ is dependent on γ_2. With the $\bar{A}_{12}(m)$ and $\bar{A}_{22}(m)$ in (28), and the G and L in (18) , we let $L(m+1) = (G\bar{A}_{12}(m) + L\bar{A}_{22}(m))/\gamma_2^m$ and compute $C_0 = \max_{m=0,1,\cdots,M} \|L(m+1)\|$. With such C_2, we further compute

$$C_1 = \max\left\{2C_2\sqrt{Nn}, \frac{C_0 C_2 \sqrt{Nn}\sigma}{(1-d)\gamma_1}\right\} \quad (32)$$

where the parameters satisfy $C_2 > 0$, and $\rho(J(1)) < d < 1$ depends on the choices of γ_1 and γ_2 and they satisfy $\| \left(J(m+1)/\gamma_1\right)^k \| \leq C_2 d^k$ for $m = 1, 2, \cdots, M$.

To facilitate the analysis of the main result, we first introduce the lemma below.

Lemma 3. Take γ_1 and γ_2 such that

$$\max_{m=1,2,\cdots,M} \rho(J(m+1)) \leq \rho(J(1)) < \gamma_1 < 1 \quad (33)$$

and let $\theta_0 \geq C_{x_0}\gamma_1\sigma$. If $\|\xi(s_p)\|_\infty \leq \sigma/\gamma_1$ for $p = 0, 1, \cdots, r$, then $\|[\alpha^T(s_r) \ \ \xi^T(s_r)]^T\|$ is upper-bounded such that

$$\|[\alpha^T(s_r) \ \ \xi^T(s_r)]^T\| \leq \sigma\sqrt{C_1^2 + Nn}/\gamma_1 \quad (34)$$

with C_1 in (32).

Now we are ready to present the main result.

Theorem 1. Consider the multi-agent system (1) with control action (12) to (15), where they exchange information via the undirected graph $\mathcal{G}$. The communication attempts are periodic with sampling interval Δ. Suppose that the DoS attacks characterized in Assumptions 1 and 2 satisfy $1/T + \Delta/\tau_D < 1$. Let γ_1 and γ_2 be chosen such that $\max_{m=1,2,\cdots,M} \rho(J(m+1)) \leq \rho(J(1)) < \gamma_1 < 1$, where $J(1)$ and $J(m+1)$ are in (11) and (31), respectively, and let $\theta_0 \geq C_{x_0}\gamma_1/\sigma$. Then, the quantizer (8) is not overflowed, if R satisfies

$$2R + 1 \geq \|[-L \ H]\|_\infty \zeta \sqrt{C_1^2 + Nn}/\gamma_1 \quad (35)$$

with $C_1 \in \mathbb{R}_{>0}$ in (32), $\zeta = \max\{1, \|(\bar{A}/\gamma_2)^M\|\}$, $\bar{A}$ in (28) and M in Lemma 1. Moreover, when (35) holds and DoS attacks satisfy

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < \frac{-\ln\gamma_1}{\ln\gamma_2 - \ln\gamma_1} \quad (36)$$

then consensus of $x_i(k\Delta)$ is achieved.

Remark 3. In view of the right-hand side of (36), it is good to have small γ_1 and γ_2 for improving the robustness, though a small γ_1 will result in large data rate. It is clear that γ_1 can affect $2R+1$ directly. More importantly, γ_1 can also affect C_1 in the sense that if one lets $\gamma_1 \to \rho(J(1))$, then $C_1 \to \infty$. It is trivial that if there are no DoS attacks in the network, then $\gamma = \gamma_1$ and the problem in this paper is reduced to the one in (You and Xie, 2011). The principle of selecting γ_2 is to make $\rho(J(m+1)) \leq \rho(J(1))$ hold, where $m \neq 0$. Then, γ_2 essentially depends on the systems to be controlled, the communication topology and M that depends on DoS (in Lemma 1). ■

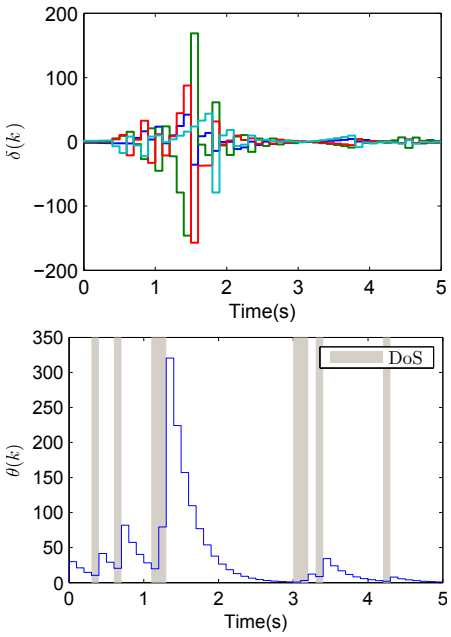

Fig. 1. Time responses of $\delta(k)$ (top) and $\theta(k)$ (bottom).

5. NUMERICAL EXAMPLE

In this section, we consider the system setting as that in the numerical example in (You and Xie, 2011). Take $A = 1.1$, $B = 1$ and $N = 4$. The Laplacian matrix of the undirected and connected communication graph is

$$L_{\mathcal{G}} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{bmatrix}. \quad (37)$$

We select the state-feedback gain to be $K = 0.44$.

Let the network transmission interval be $\Delta = 0.1$s. We consider a sustained DoS attack with variable period and duty cycle, generated randomly. Over a simulation horizon of 5s, the DoS signal yields $|\Xi(0,5)| = 0.8$s and $n(0,5) = 6$. This corresponds to values (averaged over 5s) of $\tau_D \approx 0.96$ and $T \approx 1.29$, and the DoS attacks in this example yield $\Delta/\tau_D + 1/T \approx 0.28$.

With the selected K, one has $\rho(J(1)) = 0.66$. According to Theorem 1, we choose $\gamma_1 = 0.7$ and $\gamma_2 = 4.0333$. By such selected parameters, the number of quantization levels yields $2R + 1 \geq 6809$, which can be encoded by 13 bits, and the sufficient DoS-bound condition for consensus is $1/T + \Delta/\tau_D < 0.2037$. This gap regarding the bound of $\Delta/\tau_D + 1/T$ shows that our result is a sufficient condition, and there is conservativeness in the analysis. The time responses of $\delta(k)$ and scaling parameter $\theta(k)$ are given in Figure 1. One can observe that consensus is successfully achieved.

6. CONCLUSIONS

In this paper, we have presented results for the consensus problem of linear multi-agent systems with general dynamics under network data rate limitation and malicious DoS attacks. The design of quantized controller and the characterization of DoS attacks for consensus have been given. In particular, we have provided a feasible way of designing dynamic quantized control with zoom-in and zoom-out capabilities for the multi-agent systems with general dynamics, and such dynamic quantization makes finite data rate control possible without quantizer overflow under malicious DoS attacks. We have then characterized the bound of DoS attacks under which consensus of the multi-agent systems can be guaranteed, and have further discussed the trade-offs between bit rates and robustness against DoS.

The results in this paper can be extended in various directions. One possible direction is to implement event-triggered control to save communication resources in the number of transmissions (Ma et al., 2018). It is also interesting to study the scenario when the multi-agent systems are subject to local DoS attacks.

REFERENCES

Amin, S., Càrdenas, A., and Sastry, S. (2009). Safe and secure networked control systems under Denial-of-Service attacks. *Hybrid Systems: Computation and Control*, 31–45.

Bullo, F. (2019). *Lectures on Network Systems*. Kindle Direct Publishing.

Cai, K. and Ishii, H. (2011). Quantized consensus and averaging on gossip digraphs. *IEEE Transactions on Automatic Control*, 56(9), 2087–2100.

Carli, R., Fagnani, F., Frasca, P., and Zampieri, S. (2010). Gossip consensus algorithms via quantized communication. *Automatica*, 46(1), 70–80.

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

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

Cheng, P., Shi, L., and Sinopoli, B. (2017). Guest editorial: Special issue on secure control of cyber-physical systems. *IEEE Transactions 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 Transactions on Automatic Control*, 60(11), 2930–2944.

Dibaji, S.M., Ishii, H., and Tempo, R. (2017). Resilient randomized quantized consensus. *IEEE Transactions on Automatic Control*, 63(8), 2508–2522.

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 Transactions on Automatic Control*. doi:10.1109/TAC.2020.2981083.

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

Feng, S. and Ishii, H. (2020). Dynamic quantized consensus of general linear multi-agent systems under Denial-of-Service attacks. *arXiv preprint arXiv:2004.13815*, 1–12.

Feng, Z. and Hu, G. (2019). Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. *IEEE Transactions on Control Systems Technology*, 28(3), 741–752.

Hespanha, J.P. and Morse, A.S. (1999). Stability of switched systems with average dwell-time. In *Proceedings of IEEE Conference on Decision and Control*, 2655–2660.

Kashyap, A., Başar, T., and Srikant, R. (2007). Quantized consensus. *Automatica*, 43(7), 1192–1203.

Li, T., Fu, M., Xie, L., and Zhang, J.F. (2010). Distributed consensus with limited communication data rate. *IEEE Transactions on Automatic Control*, 56(2), 279–292.

Li, Y., Quevedo, D.E., Dey, S., and Shi, L. (2017). SINR-based DoS attack on remote state estimation: A game-theoretic approach. *IEEE Transactions on Control of Network Systems*, 4(3), 632–642.

Li, Z., Duan, Z., Chen, G., and Huang, L. (2009). Consensus of multiagent systems and synchronization of complex networks: A unified viewpoint. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 57(1), 213–224.

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

Ma, J., Ji, H., Sun, D., and Feng, G. (2018). An approach to quantized consensus of continuous-time linear multi-agent systems. *Automatica*, 91, 98–104.

Nair, G.N. and Evans, R.J. (2004). Stabilizability of stochastic linear systems with finite feedback data rates. *SIAM Journal on Control and Optimization*, 43(2), 413–436.

Nugraha, Y., Hayakawa, T., Cetinkaya, A., Ishii, H., and Zhu, Q. (2019). Subgame perfect equilibrium analysis for jamming attacks on resilient graphs. In *Proceedings of American Control Conference*, 2060–2065.

Qin, J., Li, M., Shi, L., and Yu, X. (2017). Optimal Denial-of-Service attack scheduling with energy constraint over packet-dropping networks. *IEEE Transactions on Automatic Control*, 63(6), 1648–1663.

Qiu, Z., Xie, L., and Hong, Y. (2015). Quantized leaderless and leader-following consensus of high-order multi-agent systems with limited data rate. *IEEE Transactions on Automatic Control*, 61(9), 2432–2447.

Senejohnny, D., Tesi, P., and De Persis, C. (2017). A jamming-resilient algorithm for self-triggered network coordination. *IEEE Transactions on Control of Network Systems*, 5(3), 981–990.

Tatikonda, S. and Mitter, S. (2004). Control under communication constraints. *IEEE Transactions on Automatic Control*, 49(7), 1056–1068.

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

Wang, Y. and Ishii, H. (2019). An event-triggered approach to quantized resilient consensus. In *Proceedings of European Control Conference*, 2719–2724. To appear, *Int. J. Nonlinear and Robust Control*, 2020.

Xu, W., Ho, D.W.C., Zhong, J., and Chen, B. (2019). Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. *IEEE Transactions on Neural Networks and Learning Systems*, 30(10), 3137–3149.

You, K. and Xie, L. (2011). Network topology and communication data rate for consensusability of discrete-time multi-agent systems. *IEEE Transactions on Automatic Control*, 56(10), 2262–2275.