Dynamic Quantized Consensus of General Linear Multiagent Systems Under Denial-of-Service Attacks

Feng, Shuai; Ishii, Hideaki

Published in:
IEEE Transactions on Control of Network Systems

DOI:
10.1109/TCNS.2022.3140684

Dynamic Quantized Consensus of General Linear Multiagent Systems Under Denial-of-Service Attacks

Shuai Feng and Hideaki Ishii, *Fellow, IEEE*

***Abstract*—In this article, we study multiagent consensus problems under Denial-of-Service (DoS) attacks with data rate constraints. We first consider the leaderless consensus problem and after that we briefly present the analysis of leader–follower consensus. The dynamics of the agents take general forms modeled as homogeneous linear time-invariant systems. In our analysis, we derive lower bounds on the data rate for the multiagent systems to achieve leaderless and leader–follower consensus in the presence of DoS attacks, under which the issue of overflow of quantizer is prevented. The main contribution of the article is the characterization of the tradeoff between the tolerable DoS attack levels for leaderless and leader–follower consensus and the required data rates for the quantizers during the communication attempts among the agents. To mitigate the influence of DoS attacks, we employ dynamic quantization with zooming-in and zooming-out capabilities for avoiding quantizer saturation.**

***Index Terms*—Consensus, Denial-of-Service, multiagent systems, packet losses, quantized control.**

I. Introduction

IN THE last two decades, the control of multiagent systems has attracted substantial attention due to the progress of technologies in communication and computation areas. Some of the key applications can be found in formation control, control of large-scale systems, and distributed sensor networks [1]. In particular, these days, 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 due to malicious cyber attacks on CPSs [2]–[5], in the form of, e.g., deceptive attacks and Denial-of-Service (DoS).

Manuscript received January 7, 2021; revised June 1, 2021 and June 2, 2021; accepted November 7, 2021. Date of publication January 5, 2022; date of current version June 20, 2022. This work was supported in the part by the JST CREST under Grant JPMJCR15K3 and in part by JSPS under Grant-in-Aid for Scientific Research Grant 18H01460. Recommended by Associate Editor Iman Shames. *(Corresponding author: Shuai Feng.)*

Shuai Feng is with ENTEG, Faculty of Science and Engineering, University of Groningen, 9747AG Groningen, The Netherlands (e-mail: s.feng.ac@gmail.com).

Hideaki Ishii is with the Department of Computer Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan (e-mail: ishii@c.titech.ac.jp).

Digital Object Identifier 10.1109/TCNS.2022.3140684

This article specifically 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 those caused by genuine packet losses due to network congestion; particularly, packet dropouts resulting from malicious DoS need not follow a given class of probability distributions [6] and, therefore, the analysis techniques relying on probabilistic arguments may not be applicable. This poses new challenges in theoretical analysis and controller design.

In this article, our focus is on the effects of DoS attacks on multiagent systems. Recently, systems under such attacks have been studied from a control-theoretic viewpoint [7]–[16]. In [7], 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 multiagent systems under DoS, there are some recent results for consensus problems with infinite data-rate communication. For example, [13] presents theoretical as well as comprehensive simulation studies for continuous-time system consensus under DoS attacks with the utilization of event-triggered control.

Wireless communication appeals to industry due to its advantages, such as transmission over long distances and lower costs for large-scale implementation. However, the transmitted signals are subject to analog-digital conversion and hence quantization. Real-time data exchanged within networked control systems may suffer from data rate constraints and hence the quantization effects on signals need to be taken into account at the design stage.

Static and dynamic quantizations have been proposed for various control problems. Centralized control systems under quantized communication have been extensively studied in the last two decades, for example, by the seminal articles [17], [18]. The results in such works show that an insufficient bit rate in the communication channel influences the stability of a networked control system. Reference [9] extended these results to the case with DoS attacks by utilizing zooming-in and out dynamic quantization for centralized systems. In this article, we address issues arising from constraints on the data rate that can occur in multiagent systems.

In addition to centralized systems, quantized consensus problems of multiagent systems have been broadly studied in the last decade [19]–[22] and some of them take data rate constraints

into consideration. Indeed, the issue of data rate in networked control of multiagent systems will become relevant especially if the agents try to reach consensus on multiple variables and the volume of data communicated among agents is large. Reducing the data size for each variable is one way to make the system robust to changes in the available data rate, e.g., in wireless communication. In [21], the authors consider the zooming-in only quantized controller with a finite data rate. However, such a controller may not be feasible in the context of DoS since the quantizer would have overflow problems under DoS, due to state divergence. This is one of the central problems caused by considering data rate/quantization when investigating a resilient control problem. In order to mitigate the influence of DoS attacks and to ensure that a channel with a finite data rate is still feasible, in this article, we design a quantized controller with both *zooming-in* and *zooming-out* capabilities. We will show that in the absence of DoS attacks, our result in the part of leaderless consensus is consistent with the one in [21].

In light of the existing literature mentioned above and the comparisons, we summarize the contributions of this article. Our work addresses the joint effects of DoS attacks and data rate constraints for both the leaderless and leader–follower consensus problems as follows.

1) We explicitly demonstrate the tradeoffs between *the resilience against DoS* and *the necessary data rate in communication*. That is, we find a data-rate dependent bound of DoS *frequency* and *duration* under which consensus can be achieved. Such tradeoffs can provide useful information for the allocation of communication resources, e.g., to ensure that the multiagent systems can realize the global objective of consensus under DoS, how much data rate must be allocated to the channel; and to improve the resilience, how much additional data rate must be ensured and so on.
2) We develop the zooming-in and zooming-out dynamic quantization for the case of multiagent systems. Specifically, we provide the sufficient number of quantization levels and the resulting bit rate, and particularly introduce the computation of zooming-out factor counteracting packet dropouts. They together ensure that the encoding–decoding systems are free of overflow under DoS-induced packet losses.

We now make more specific comparisons with existing works. As mentioned above, [13] considers consensus under DoS attacks with infinite data rates for communication. There, the sufficient condition on DoS attacks for reaching consensus mainly depends on the properties of the multiagent systems (e.g., the system matrix A and consensus rate during DoS-free periods). In contrast, our article incorporates the constraints on data rate and develops encoding and decoding systems functioning even in the presence of DoS. In this case, the system resilience also depends on data rate.

The computation of zooming-out factor for multiagent systems is one of the key technical challenges in this article. This issue arises due to the lack of "global state information" to the agents (when the network forms a noncomplete graph). For the centralized system case in [9], such information is in fact useful in the zooming-in and out dynamic quantization applied there. In the case of multiagent systems, the encoding–decoding system of a single agent cannot have the information about its neighbors' states and also control inputs under DoS (since control inputs of its neighbors also depend on their own neighbors). This lack of information induces considerable technical difficulties for tracking the states of neighbors and, hence, for the design of the zooming-out factor.

The rest of this article is organized as follows. In Section II, we introduce the framework consisting of multiagent systems and the class of DoS attacks. Section III presents the results of leaderless consensus, which includes the controller architecture with the zooming-in and zooming-out dynamic quantization mechanism, sufficient conditions for data rates, and DoS bounds under which consensus can be achieved. Section IV briefly presents an extension of the results to the leader–follower consensus problem. A numerical example is presented in Section V. Finally, Section VI concludes this article.

This article mainly focuses on the case of leaderless consensus, which provides the theoretical foundations for the part of leader–follower consensus. Preliminary results for quantized leaderless and leader–follower consensus under DoS can be found in our conference articles in [23] and [24], respectively. Compared with them, this article provides full proofs of the results, more discussions, and comparisons.

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 2- and ∞- 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 the column vectors with compatible dimensions, having all 0 and 1 elements, respectively.

II. Framework: Multiagent Systems and DoS

A. Communication Graph

We let graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ denote the communication topology between agents, where $\mathcal{V} = \{1, 2, \ldots, N\}$ 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 $i = 1, \ldots, N$. In this article, 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 $(i = 1, \ldots, N)$ denote the eigenvalues of $L_\mathcal{G}$ and, in particular, we have $\lambda_1 = 0$ due to the graph being connected.

B. System Description

The agents with interacting over the network $\mathcal{G}$ are expressed as homogeneous general linear multiagent systems. For each $i = 1, 2, \ldots, N$, 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., $\|x_i(0)\|_\infty \leq C_{x_0} \in \mathbb{R}_{>0}$. Note that C_{x_0} can be an arbitrarily large real as long as it satisfies this bound. This is for preventing the overflow of state quantization for the initial condition. 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 time $k\Delta$ 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 did not receive any data and hence they do not send acknowledgments.

Agent $i = 1, 2, \ldots, N$ 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. In the presence of DoS, transmission attempts may fail. For the ease of notation, we let s_r represent the instants of successful transmissions. Note that $s_0 \in \mathbb{R}_{\geq\Delta}$ is the instant when the first successful transmission occurs. Also, we let s_{-1} denote the time instant 0.

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

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

where $R \in \mathbb{Z}_{>0}$ is to be designed and $z = 1, 2, \ldots, R$, and $\sigma \in \mathbb{R}_{>0}$. If the quantizer is unsaturated such that $|\chi| \leq (2R+1)\sigma$, then the error induced by quantization satisfies

$$|\chi - q_R(\chi)| \leq \sigma, \text{ if } |\chi| \leq (2R+1)\sigma. \tag{3}$$

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 $f \in \mathbb{Z}_{\geq 1}$.

To design safe control systems, we must make assumptions regarding the DoS attacks that we expect the systems with sufficient safety margins. If the attackers are more capable than the assumed attack level, it would clearly be hard to guarantee consensus. This will, however, be true for any model. In the next section, we introduce a deterministic model characterizing DoS attacks. This allows us to consider the worst-case attacks, without assuming any probability distributions for launching attacks as in the random packet loss model commonly studied in the networked control literature.

C. Time-Constrained DoS

In this article, 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 qth 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 $\Xi(\tau, t) := \bigcup_{q\in\mathbb{Z}_0} H_q \cap [\tau, t]$ 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

$$n(\tau, t) \leq \eta + \frac{t-\tau}{\tau_D} \tag{4}$$

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

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

$$|\Xi(\tau, t)| \leq \kappa + \frac{t-\tau}{T} \tag{5}$$

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

Remark 1: Assumptions 1 and 2 do only constrain a given DoS signal in terms of its *average* frequency and duration. Following [25], 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 (5) 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 under Assumptions 1 and 2. If $1/T + \Delta/\tau_D < 1$, then, $m_r \in \mathbb{Z}_{\geq 0}$, representing the number of unsuccessful transmissions between s_{r-1} and s_r with $r = 0, 1, \cdots$, satisfies

$$m_r = (s_r - s_{r-1})/\Delta - 1$$

$$\leq M = \left\lfloor \frac{(\kappa + \eta\Delta)\left(1 - 1/T - \Delta/\tau_D\right)^{-1}}{\Delta} \right\rfloor. \quad (6)$$

Proof. This lemma can be easily derived from Lemma 1 in [11] and we refer the readers to the full proof there. ■

For the ease of notation, we let m represent m_r in the subsequent sections.

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

$$T_S(\Delta, k\Delta) \geq (1 - 1/T - \Delta/\tau_D)\, k - (\kappa + \eta\Delta)/\Delta. \quad (7)$$

Proof. This lemma can be easily derived from Lemma 3 in [9] and we refer the readers to that article. ■

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

III. Leaderless Quantized Consensus Under DoS

The objective of this section is to design a quantized controller, possibly dynamic, in such a way that a finite-level quantizer is not overflowed and the multiagent system (1) can tolerate as many DoS attacks as possible for reaching consensus. Specifically, we introduce the average of the states $\overline{x}(k\Delta) = \frac{1}{N}\sum_{i=1}^{N} x_i(k\Delta) \in \mathbb{R}^n$ and consensus among the agents is defined by

$$\lim_{k\to\infty} \|x_i(k\Delta) - \overline{x}(k\Delta)\|_\infty = 0, \quad i = 1, 2, \ldots, N. \quad (8)$$

For the ease of illustration, in the rest of the article we simply let k represent $k\Delta$, e.g., $x_i(k)$ represents $x_i(k\Delta)$. We are interested in some A having at least one eigenvalue on or outside the unit circle. Otherwise, the multiagent system in (1) can achieve state consensus by setting $u_i(k) = 0$ for all k.

A. Control Architecture for Leaderless Consensus

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

$$u_i(k) = K \sum_{j=1}^{N} a_{ij}(\hat{x}_j^i(k) - \hat{x}_i^i(k)), \; k = 0, 1, \ldots \quad (9)$$

where $\hat{x}_j^i(k) \in \mathbb{R}^n$ denotes the estimation of the state of agent j by agent i, whose computation will be given later. We assume that there exists a feedback gain $K \in \mathbb{R}^{w\times n}$ such that the spectral radius of

$$J(1) = \mathrm{diag}(A - \lambda_2 BK, \ldots, A - \lambda_N BK) \quad (10)$$

satisfies $\rho(J(1)) < 1$. This is a standard condition for consensus when no DoS is present [21], [26].

In (9), the estimate of the state of agent j by agent i equals the one estimated by agent l such that $\hat{x}_j^i(k) = \hat{x}_j^l(k) = \hat{x}_j^j(k)$ with $i, l \in \mathcal{N}_j$. Thus, we omit the superscripts and let

$$u_i(k) = K \sum_{j=1}^{N} a_{ij}(\hat{x}_j(k) - \hat{x}_i(k)), k = 0, 1, \ldots. \quad (11)$$

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 $k = 1, 2, \ldots$ as

$$\hat{x}_j(k) = \begin{cases} A\hat{x}_j(k-1) + \theta(k-1)\hat{Q}_j(k) & \text{if } k \notin H_q \\ A\hat{x}_j(k-1) & \text{if } k \in H_q \end{cases} \quad (12)$$

where $j \in \{i\} \cup \mathcal{N}_i$ and the initial estimates will be set as $\hat{x}_j(0) = \mathbf{0}$. The scaling parameter $\theta(k) \in \mathbb{R}_{>0}$ in (12) is updated as

$$\theta(k) = \begin{cases} \gamma_1\theta(k-1) & \text{if } k \notin H_q \\ \gamma_2\theta(k-1) & \text{if } k \in H_q \end{cases} \quad k = 1, 2, \ldots \quad (13)$$

with $\theta(0) = \theta_0 \in \mathbb{R}_{>0}$, where $0 < \gamma_1 < 1$ and $\gamma_2 > 0$. The scaling parameter $\theta(k)$ mentioned above is used in the quantization $\hat{Q}_j(k)$ given by

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

for preventing quantizer overflow. By adjusting the size of $\theta(k)$ dynamically, the state will be kept within the bounded quantization range without saturation, i.e., $\dfrac{x_j(k) - A\hat{x}_j(k-1)}{\theta(k-1)}$ in $Q_R(\cdot)$ is upper bounded by some certain values. The parameters γ_1 and γ_2 in (13) are for zooming in and out such that the quantization scaling parameter $\theta(k)$ changes dynamically to mitigate the influence of DoS. Under DoS attacks, the discrepancies between the states of the multiagent systems may diverge. Therefore, the quantizers must zoom out and increase their ranges so that the states can be measured properly. If the transmissions succeed, the quantizers zoom in and $\theta(k)$ decreases by using γ_1. The design of γ_1, γ_2, and θ_0 will be specified later.

Observe that the controller state is updated locally at each agent by checking the presence of DoS attacks over time. It is clear that each agent has access to the knowledge of DoS attacks in real time from not receiving data from the neighbors at the scheduled periodic transmission instants. One sees that the estimator (12) switches the estimation strategy adaptively to the information if $\hat{Q}_j(k)$ is available to the controller ($k \notin H_q$) or not ($k \in H_q$). In particular, if $\hat{Q}_j(k)$ is lost, then set $\hat{Q}_j(k) = 0$. The "to zero" strategy is commonly used in networked control problems with information loss. Note that the calculation of $\hat{Q}_j(k)$ (at the encoder) is dependent on $\theta(k-1)$ that needs the past information of $k-1 \notin H_q$ or $k-1 \in H_q$, instead of the corresponding information for k.

The overall estimation and update processes are summarized as follows. The state $x_j(k)$ is quantized into $\hat{Q}_j(k)$ as in (14) by the encoder and agent j attempts to send it to the decoders of its neighbors. If the transmission attempt succeeds and $\hat{Q}_j(k)$ is received, the decoders estimate $x_j(k)$ by the first equation in (12) and the scaling parameter $\theta(k)$ in the encoders and decoders

zooms in by the first equation in (13). If the transmission attempt fails, 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 (12) and the scaling parameter $\theta(k)$ in the encoders and decoders zooms out as in the second equation in (13).

Note that in the control input (11), 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 [21] and the references therein.

Let $\hat{x}(k) = [\hat{x}_1^T(k)\ \hat{x}_2^T(k) \dots \hat{x}_N^T(k)]^T \in \mathbb{R}^{nN}$ 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 (12) as

$$\hat{x}(k) = \begin{cases} (I_N \otimes A)\hat{x}(k-1) + \theta(k-1)Q(k) & \text{if } k \notin H_q \\ (I_N \otimes A)\hat{x}(k-1) & \text{if } k \in H_q \end{cases} \tag{15}$$

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

$$x(k) = Gx(k-1) + Le(k-1) \tag{16}$$

where

$$G = I_N \otimes A - L_{\mathcal{G}} \otimes BK, \quad L = L_{\mathcal{G}} \otimes BK. \tag{17}$$

Recall the average of the states $\overline{x}(k)$ before (8). The discrepancy between the state of agent i and $\overline{x}$ is denoted by $\delta_i(k) = x_i(k) - \overline{x}(k) \in \mathbb{R}^n$. By defining $\delta(k) = [\delta_1^T(k)\ \delta_2^T(k)\ \dots\ \delta_N^T(k)]^T \in \mathbb{R}^{nN}$, one has $x(k) = \delta(k) + I_N \otimes \overline{x}(k)$. By applying it to (16), one obtains

$$\delta(k) = G\delta(k-1) + Le(k-1). \tag{18}$$

It is clear that if $\|\delta(k)\|_\infty \to 0$ as $k \to \infty$, consensus of the multiagent system (1) is achieved as in (8). If $\|e(k)\| = 0$ or is upper bounded by a certain value [21] for all k, it is obvious that consensus can be achieved. Under DoS attacks, however, $e(k)$ may diverge and consequently consensus among the agents may not be achieved.

B. Dynamics of the Multiagent Systems

In this section, we present the dynamics of the multiagent system under quantization, in terms of $e(k)$ with $e(k-1)$ and $\delta(k-1)$ for the two cases, i.e., in the absence and presence of DoS attacks.

If the transmission succeeds such that $k \notin H_q$ for $k = 1, 2, \dots$, then according to (15), one has

$$\begin{aligned} e(k) &= x(k) - \hat{x}(k) \\ &= x(k) - (I_N \otimes A)\hat{x}(k-1) - \theta(k-1)Q(k) \\ &= x(k) - (I_N \otimes A)\hat{x}(k-1) \\ &\quad - \theta(k-1)Q_R\left(\frac{x(k) - (I_N \otimes A)\hat{x}(k-1)}{\theta(k-1)}\right). \end{aligned} \tag{19}$$

Note that

$$x(k) - (I_N \otimes A)\hat{x}(k-1) = He(k-1) - L\delta(k-1) \tag{20}$$

where

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

Then (19) can be rewritten as

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

If the transmission fails such that $k \in H_q$ for $k = 1, 2, \dots$, then in view of (15), one has

$$e(k) = x(k) - \hat{x}(k) = x(k) - (I_N \otimes A)\hat{x}(k-1). \tag{23}$$

Then, apply (20) to (23).

In the abovementioned case, we have presented the system dynamics using $e(k)$ and $\delta(k)$. To facilitate the analysis, we let

$$\alpha(k) = \delta(k)/\theta(k) \qquad \xi(k) = e(k)/\theta(k) \tag{24}$$

where $\theta(k)$ is given in (13). Then, we formulate the system dynamics in terms of $\alpha(k)$ and $\xi(k)$.

If the transmission succeeds such that $k \notin H_q$, in view of the first case in (13), (18), and (22), one has

$$\alpha(k) = \frac{G}{\gamma_1}\alpha(k-1) + \frac{L}{\gamma_1}\xi(k-1) \tag{25}$$

$$\begin{aligned} \xi(k) = &\ \frac{H\xi(k-1) - L\alpha(k-1)}{\gamma_1} \\ &- \frac{Q_R\left(H\xi(k-1) - L\alpha(k-1)\right)}{\gamma_1}. \end{aligned} \tag{26}$$

It is easy to infer that if $\|H\xi(k-1) - L\alpha(k-1)\|_\infty \le (2R+1)\sigma$, then by (3) one has $\|\xi(k)\|_\infty \le \sigma/\gamma_1$.

If the transmission fails such that $k \in H_q$, then according to the second case in (13), (18), and (23), one has

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

$$\xi(k) = \frac{H}{\gamma_2}\xi(k-1) - \frac{L}{\gamma_2}\alpha(k-1). \tag{28}$$

Compared with (26), $\xi(k)$ induced by (28) 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.

We explain the intuition of the zooming-in and zooming-out mechanism in the context of quantized control of multiagent systems under transmission losses. In the dynamics of $\alpha(k)$ and $\xi(k)$ in (25) and (26) under successful transmissions, one can see that γ_1 appears in the denominators on the right-hand sides. Similarly, in (27) and (28), γ_2 appears in the case of transmission failures. When DoS attacks occur, the systems are in the open-loop status and thus $\alpha(k)$ and $\xi(k)$ grow in general. The parameter γ_2 can be considered as a factor to compensate the growth rate. To keep the growth of $H\xi(k) - L\alpha(k)$ small, we must find a sufficiently large γ_2 since $\alpha(k)$ and $\xi(k)$ are divided

by γ_2 during DoS (see the right-hand sides of (27) and (28)). As a result, it is possible to keep $\|H\xi(k) - L\alpha(k)\|_\infty \leq (2R+1)\sigma$ during DoS, which implies that quantizer overflow will not occur.

While the idea of zooming-in and zooming-out is intuitive, the computation of the parameters γ_1 and γ_2 is not straightforward in the context of quantized control of multiagent systems. Compared with quantized control of centralized systems, e.g., in [9] and[27], one of the challenges in this article arises from the constraint of distributed systems, where each agent knows only a fraction of the global information. Due to this, the "decedent" state estimation/prediction scheme as in the articles [9] and[27] is very difficult to implement here and more importantly the estimation error is also coupled with the state, e.g., $\xi(k)$ depends on $\alpha(k)$ in (28). By contrast, in quantized control of centralized systems, this coupling problem between estimation error and state does not arise.

In the following, with the control scheme introduced in (11)–(13), we will show that quantizer overflow will not occur by properly designing the scaling parameter $\theta(k)$ in (13) with γ_1 and γ_2, and then discuss the tradeoffs between resilience and data rate.

C. Overflow-Free Quantizer and Leaderless Consensus

In this section, we will present the results for quantized leaderless consensus under DoS, showing the number of quantizer levels such that it is not overflowed, and a sufficient condition for consensus. Before presenting the results, we introduce some preliminaries that will be used in the theorem.

Using the matrices G, L, and H in (17) and (21), respectively, we define the matrices

$$\overline{A} = \begin{bmatrix} G & L \\ -L & H \end{bmatrix}, \ \overline{A}(m) = \overline{A}^m = \begin{bmatrix} \overline{A}_{11}(m) & \overline{A}_{12}(m) \\ \overline{A}_{21}(m) & \overline{A}_{22}(m) \end{bmatrix} \tag{29}$$

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

$$G(m+1) = (G\overline{A}_{11}(m) + L\overline{A}_{21}(m))/\gamma_2^m \tag{30}$$

$$\overline{G}(m+1) = (U \otimes I_n)^T G(m+1)(U \otimes I_n) \tag{31}$$

in which the unitary matrix U is given by

$$U = [\mathbf{1}/\sqrt{N} \ \phi_2 \ \ldots \ \phi_N] \in \mathbb{R}^{N\times N} \tag{32}$$

where $\phi_i \in \mathbb{R}^N$ with $i = 2, 3, \ldots, N$ 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 $\overline{G}(m+1)$ in (31) after deleting the top n rows and the left n columns from $\overline{G}(m+1)$. Then, we define the set $\mathcal{J}$ as

$$\mathcal{J} = \{J(1), \ldots, J(m+1), \ldots, J(M+1)\}. \tag{33}$$

Note that $J(m+1)$ is reduced to $J(1)$ in (10) 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 matrices $\overline{A}_{12}(m)$ and $\overline{A}_{22}(m)$ in (29), and G and L in (17), we let

$$L(m+1) = (G\overline{A}_{12}(m) + L\overline{A}_{22}(m))/\gamma_2^m \tag{34}$$

and then compute

$$C_0 = \max_{m=0,1,\ldots,M} \|L(m+1)\|. \tag{35}$$

With such C_0, we further compute

$$C_1 = \max\left\{2C_2\sqrt{Nn}, \frac{C_0 C_2 \sqrt{Nn}\sigma}{(1-d)\gamma_1}\right\} \in \mathbb{R}_{>0} \tag{36}$$

where $d = d_0/\gamma_1$. Here, the parameters $\rho(J(1)) < d_0 < 1$ and $C_2 \geq 1$ in (36) exist and satisfy $\|J(1)^p\| \leq C_2 d_0^p$ with $p \in \mathbb{Z}_{\geq 1}$ [28]. The choices and discussions concerning γ_1 and also γ_2 will be given in Lemma 3 and thereafter.

To facilitate the proof of Theorem 1, we introduce the lemma below, whose proof is provided in the Appendix.

Lemma 3: Take γ_1 and γ_2 such that

$$d_0 < \gamma_1 < 1, \ \max_{m=1,\ldots,M} \|J(m+1)\| \leq \rho(J(1))/C_2 \tag{37}$$

in which M from Lemma 1 and $C_2 \in \mathbb{R}_{\geq 1}$ satisfies $\|J(1)^p\| \leq C_2 d_0^p$ with $\rho(J(1)) < d_0 < 1$. Let $\theta_0 \geq C_{x_0}\gamma_1/\sigma$. If $\|\xi(s_p)\|_\infty \leq \sigma/\gamma_1$ for $p = 0, 1, \ldots, r$, then $\|[\alpha^T(s_r) \ \ \xi^T(s_r)]^T\|$ is upper-bounded as

$$\|[\alpha^T(s_r) \ \ \xi^T(s_r)]^T\| \leq \sigma\sqrt{C_1^2 + Nn}/\gamma_1 \tag{38}$$

where C_1 is given in (36). ■

After finding C_2 and d_0 for $\|J(1)^p\| \leq C_2 d_0^p$, one must first choose a γ_1 such that $d_0 < \gamma_1 < 1$. Recall that γ_2 appears in the denominators of $J(2), \ldots, J(M+1)$ by (30). Then, one selects a sufficiently large γ_2 such that the second inequality in (37) holds. Note that as long as C_2 and d_0 are determined, the choices of γ_1 and γ_2 can be made independently.

Now, we are ready to present the results for quantized leaderless consensus under DoS attacks.

Theorem 1: Consider the multiagent system (1) with control inputs (11)–(13), where the agents 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 $1/T + \Delta/\tau_D < 1$. The parameters γ_1, γ_2, and θ_0 are chosen in accordance to Lemma 3. If R satisfies

$$2R + 1 \geq \|[-L \ H]\|_\infty \zeta \frac{\sqrt{C_1^2 + Nn}}{\gamma_1} \tag{39}$$

with C_1 in (36), $\zeta = \max_{m=0,1,\ldots,M} \|(\overline{A}/\gamma_2)^m\|$, $\overline{A}$ in (29) and M in Lemma 1, then, the following hold:

1) the quantizer (2) is not overflowed, and
2) if in addition the DoS attacks satisfy

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < \frac{-\ln\gamma_1}{\ln\gamma_2 - \ln\gamma_1} \tag{40}$$

then, consensus of $x_i(k\Delta)$ is achieved as in (8).

Proof. Recall that s_r represents a successful transmission instant.

1) The unsaturation of the quantizer is proved by induction. More specifically we show that if the quantizer is not overflowed such that $\|\xi(s_p)\|_\infty \le \sigma/\gamma_1$ for $p = -1, 0, \ldots, r$, then, the quantizer will not saturate at the transmission attempts within the interval $]s_r, s_{r+1}]$ and hence $\|\xi(s_{r+1})\|_\infty \le \sigma/\gamma_1$.

a) If $s_{r+1} = s_r + \Delta$, in view of (26), it is easy to verify that the quantizer $Q(s_{r+1}) = Q_R(H\xi(s_r) - L\alpha(s_r))$ is not overflowed in the sense that

$$\left\|[-L \quad H]\left[\alpha^T(s_r)\ \xi^T(s_r)\right]^T\right\|_\infty \le (2R+1)\sigma \tag{41}$$

where the norm of $[\alpha^T(s_r)\ \xi^T(s_r)]^T$ is given in Lemma 3. This implies $\|\xi(s_{r+1})\|_\infty \le \sigma/\gamma_1$.

b) If $s_{r+1} > s_r + \Delta$, it means that the transmissions before s_{r+1} at the instants $s_r + \Delta, s_r + 2\Delta, \ldots, s_r + m\Delta$ fail, where $m \le M$. We verify that the quantizer is also free of overflow at the instants $s_r + \Delta, s_r + 2\Delta, \ldots, s_r + m\Delta$ and s_{r+1} since

$$\begin{aligned}&\left\|[-L \ \ H]\left[\alpha^T(s_r + m\Delta)\ \xi^T(s_r + m\Delta)\right]^T\right\|_\infty \\ &\le \|[-L \ \ H]\|_\infty \left\|\overline{A}(m)/\gamma_2^m\right\| \left\|\left[\alpha^T(s_r)\ \xi^T(s_r)\right]^T\right\| \\ &\le (2R+1)\sigma, \ \ 0 \le m \le M.\end{aligned} \tag{42}$$

This implies $\|\xi(s_{r+1})\|_\infty \le \sigma/\gamma_1$. In view of *a)* and *b)*, by induction, we conclude that the quantizer satisfying (39) is not overflowed for all the transmissions in the interval $]s_r, s_{r+1}]$ $(r = -1, 0, \cdots)$ and hence for all the transmissions.

2) Now we show leaderless consensus in the states. If the quantizer is not saturated, then one has

$$\begin{aligned}\|\alpha(s_r + m\Delta)\|_\infty &\le \|[\alpha^T(s_r + m\Delta)\ \ \xi^T(s_r + m\Delta)]^T\| \\ &\le \left\|\overline{A}(m)/\gamma_2^m\right\| \left\|[\alpha^T(s_r) \quad \xi^T(s_r)]^T\right\| \\ &\le \sigma \left\|\overline{A}(m)/\gamma_2^m\right\| \sqrt{C_1^2 + Nn}/\gamma_1\end{aligned} \tag{43}$$

for $1 \le m \le M$, where the third inequality is obtained from (38). Incorporating the scenario of $m = 0$, we have $\|\alpha(k)\|_\infty \le \sigma\zeta\sqrt{C_1^2 + Nn}/\gamma_1$ where $\zeta = \max_{m=0,1,\ldots,M} \|(\overline{A}/\gamma_2)^m\|$. Recall the definition of $T_S(\Delta, k\Delta)$ in Lemma 2 and let $T_U(\Delta, k\Delta)$ denote the number of unsuccessful transmissions in the interval $[\Delta, k\Delta]$. In view of $\delta(k) = \theta(k)\alpha(k) = \gamma_1^{T_S(\Delta,k\Delta)}\gamma_2^{T_U(\Delta,k\Delta)}\theta_0\alpha(k)$, one has

$$\|\delta(k)\|_\infty \le C_3\gamma^k\theta_0\|\alpha(k)\|_\infty \le C_3\gamma^k\theta_0\zeta\sqrt{C_1^2 + Nn}\sigma/\gamma_1$$

where $C_3 = (\gamma_2/\gamma_1)^{(\kappa+\eta\Delta)/\Delta}$ and

$$\gamma = \gamma_1^{1-\frac{1}{T}-\frac{\Delta}{\tau_D}}\gamma_2^{\frac{1}{T}+\frac{\Delta}{\tau_D}} < 1 \tag{44}$$

by (40). Thus, we have $\|\delta(k)\|_\infty \to 0$ when $k \to \infty$, which implies that leaderless consensus is achieved. ■

Remark 3: As mentioned earlier, the theorem characterizes the tradeoff between resilience of the agent system to DoS attacks and the necessary data rate in communication. This can be seen from the roles that the parameters γ_1 and γ_2 play in our design. They determine the update of the scaling parameter $\theta(k)$ depending on the presence of DoS attacks. For improving the robustness, it helps to use small γ_1 and γ_2 in (37), which will enlarge the class of tolerable DoS attacks as seen in (40). On the other hand, a small γ_1 ($\gamma_1 \to d_0$) will result in large data rate. We can confirm this in the lower bound for $2R + 1$ in (39) and also the definition of C_1 in (36). Intuitively, this tradeoff has a clear implication: higher resilience needs more data rate. ■

Remark 4: Another aspect of γ_1 and γ_2 is that keeping them small helps the convergence rate for arriving at consensus. This can be checked as follows: small γ_1 and γ_2 help the convergence rate of $\theta(k)$. Then, from (24), this can result in a fast convergence rate of $\delta(k)$ and hence the state consensus. Though the analysis methods in our article and [13] are different, they have some common points. For example, it is good to have fast consensus rate by controller design during DoS-free periods. In our article, this can be realized by tuning K and enlarging data rates. In [13], this can be realized by tuning the solution to algebraic Riccati equation. ■

Note that from the iteration (25) and the discussion after (18), when DoS is absent, the iteration of $\alpha(k)$ depends on $J(1)/\gamma_1$, which is similar to the result achieved in [21]. In this article, we extend this to the case when $0 \le m \le M$ consecutive packet dropouts can occur, where the condition is written in terms of $J(m+1)/\gamma_1$ with $J(m+1)$ in (37). The data rate result given by (39) can be conservative than the corresponding one in [21]. This is due to the worst-case type of analysis when considering uncertain DoS attacks, e.g., the use of $\max$ in C_0 in (35) and ζ in (39). At last, the parameter C_2 in (37) can also make γ_2 conservative. The purpose of letting C_2 be in the denominator in (37) is for compensating the "jumps" in the switched system from one mode to the others (DoS modes and non-DoS mode).

It is clear from our results that a control designer may not need the exact knowledge of the real-time DoS parameters. He/she only needs to assume that DoS attacks satisfy the condition $1/T + \Delta/\tau_D < 1$, under which Lemmas 1 and 2 hold. At or above the threshold 1 (i.e., $1/T + \Delta/\tau_D \ge 1$), τ_D and T can give rise to DoS signals that destroy consensus, no matter what the controller is, e.g., $T = 1$ (DoS attacks are present for 100% of total time) and/or $\tau_D = \Delta$ (DoS attacks can coincide with all transmission instants). Furthermore, a designer may estimate the DoS parameters (η, τ_D, κ, and T) from past experience and may also add safety margins to the parameters to ensure more robustness in the design.

IV. Leader–Follower Consensus Under DoS

In this section, we will discuss leader–follower consensus under DoS attacks. The dynamics of the followers is taken as (1). Let 0 be the index for the leader. The dynamics of the leader is given as an autonomous system such that

$$x_0(k\Delta) = Ax_0((k-1)\Delta), \ k \in \mathbb{Z}_{\ge 1} \tag{45}$$

where $x_0(k) \in \mathbb{R}^n$ is the state of the leader, and A and Δ are the same as in (1). Similarly to the scenario of leaderless consensus, we assume that an upper bound on the initial state of the leader is known as $\|x_0(0)\|_\infty \le \widetilde{C}_{x_0}$. For the ease of analysis, we assume that $\widetilde{C}_{x_0} \le C_{x_0}$. We say that the leader–follower consensus is

achieved if

$$\lim_{k\to\infty} \|x_i(k\Delta) - x_0(k\Delta)\|_\infty = 0, \quad i = 1, 2, \ldots, N. \tag{46}$$

Communication topology: In this section, the communication topology among the followers is represented by an undirected and connected graph $\mathcal{G}$ as in Section II-A, whose Laplacian matrix is denoted by $L_\mathcal{G}$. We also assume that only a fraction of the followers can receive the information from the leader. Let a_{i0} represent the leader–follower interaction, i.e., if agent i can directly receive the information from the leader, then $a_{i0} > 0$, and otherwise $a_{i0} = 0$. Moreover, we let the diagonal matrix be $D = \mathrm{diag}(a_{10}, a_{20}, \ldots, a_{N0}) \in \mathbb{R}^{N\times N}$. For simplicity, we let k represent $k\Delta$ in the following analysis.

A. Framework of Leader–Follower Control

For achieving the leader–follower consensus as in (46), we let the control input to the follower agent $i \in \mathcal{V}$ in (1) as

$$u_i(k) = K\sum_{j=1}^{N} a_{ij}(\hat{x}_j(k) - \hat{x}_i(k)) + Ka_{i0}(\hat{x}_0(k) - \hat{x}_i(k)) \tag{47}$$

where $\hat{x}_j(k)$ denotes the estimate of $x_j(k)$ obtained by (12) and (14) for $j \in \{i\} \cup \mathcal{N}_i$. Besides, $\hat{x}_0(k)$ denotes the estimation of $x_0(k)$ and is also estimated as in (12) and (14). The zooming-in and zooming-out quantization mechanism is still valid for leader–follower consensus control. The scaling parameter $\theta(k)$ is in the form as in (13). The zooming-in and zooming-out parameters γ_1 and γ_2 for leader–follower consensus will be given later in this section. Here, we assume that there exists a feedback gain $K \in \mathbb{R}^{w\times n}$ for leader–follower consensus such that the spectral radius of $A - \widetilde{\lambda}_i BK$ $(i = 1, 2, \ldots, N)$ are smaller than 1, where $\widetilde{\lambda}_i$ denote the eigenvalues of $L_\mathcal{G} + D$. We let $\widetilde{\delta}_i(k) = x_i(k) - x_0(k)$ and $e_i(k) = x_i(k) - \hat{x}_i(k)$. Moreover, let $e_0(k) = x_0(k) - \hat{x}_0(k)$. Let the vectors be $\widetilde{\delta}(k) = [\widetilde{\delta}_1^T(k)\ \widetilde{\delta}_2^T(k)\ \ldots \widetilde{\delta}_N^T(k)]^T$ and $e(k) = [e_1^T(k)\ e_2^T(k)\ \ldots e_N^T(k)]^T$. Then, we obtain the compact form

$$\widetilde{\delta}(k) = \Pi\widetilde{\delta}(k-1) + \Sigma e(k-1) - \Phi(1_N \otimes e_0(k-1)) \tag{48}$$

where the matrices are given by $\Pi = I_N \otimes A - (L_\mathcal{G} + D) \otimes BK$, $\Sigma = (L_\mathcal{G} + D) \otimes BK$, and $\Phi = D \otimes BK$. Note that the eigenvalues of Π equal to those of $A - \widetilde{\lambda}_i BK$ with spectral radius $\rho(A - \widetilde{\lambda}_i BK) < 1$ $(i = 1, 2, \ldots, N)$. If the dynamics of $\widetilde{\delta}(k)$ is stable as $\|\widetilde{\delta}(k)\|_\infty \to 0$ $(k \to \infty)$, then, the leader–follower consensus is achieved as in (46).

B. System Dynamics of Leader–Follower Consensus Under DoS

In light of (48), one sees that the convergence of $\widetilde{\delta}(k)$ depends on $e(k)$ and $e_0(k)$. We first analyze $e_0(k)$, whose dynamics follows

$$e_0(k) = \begin{cases} Ae_0(k-1) - \theta(k-1)Q_R\left(\frac{Ae_0(k-1)}{\theta(k-1)}\right) & k \notin H_q \\ Ae_0(k-1) & k \in H_q. \end{cases} \tag{49}$$

It is clear that the dynamics of $e_0(k)$ depends on only $e_0(k-1)$, which is different from that in leaderless consensus, where the dynamics of $e_i(k)$ depends on $e_i(k-1)$, $e_j(k-1)$, $\delta_i(k-1)$, and $\delta_j(k-1)$ $(j \in \mathcal{N}_i)$. This is because the leader agent does not receive information from its neighbors and hence its state is decoupled from those of the followers. On the other hand, the phenomenon that the estimation errors of followers' states are still coupled as occurred in the leaderless consensus problem. As we will see later, the estimation errors of followers' states are also coupled with $e_0(k)$.

Now we discuss the evolution of $e(k)$. In the scenario of leader–follower consensus, (19) and (23) still hold. However, the item $x(k) - (I_N \otimes A)\hat{x}(k-1)$ is different from the one in (20), and now it is in the form of

$$\begin{aligned} &x(k) - (I_N \otimes A)\hat{x}(k-1) \\ &= \Omega e(k-1) - \Sigma\widetilde{\delta}(k-1) - \Phi(1_N \otimes e_0(k-1)) \end{aligned} \tag{50}$$

where $\Omega = I_N \otimes A + (L_\mathcal{G} + D) \otimes BK$. Substituting (50) into (19) and (23), respectively, one can obtain the dynamics of $e(k)$ in the absence and presence of DoS attacks in the scenario of leader–follower consensus. Due to space limitation, we omit presenting them. Define three vectors $\beta(k), \epsilon(k)$, and $\epsilon_0(k) \in \mathbb{R}^{nN}$

$$\beta(k) = \frac{\widetilde{\delta}(k)}{\theta(k)}, \ \epsilon(k) = \frac{e(k)}{\theta(k)}, \ \epsilon_0(k) = \frac{1_N \otimes e_0(k)}{\theta(k)}. \tag{51}$$

Then, we obtain the dynamics of these variables for the two cases, i.e., successful and failed transmissions.

If the transmission succeeds such that $k \notin H_q$, we have

$$\beta(k) = \frac{\Pi}{\gamma_1}\beta(k-1) + \frac{\Sigma}{\gamma_1}\epsilon(k-1) - \frac{\Phi}{\gamma_1}\epsilon_0(k-1) \tag{52}$$

$$\begin{aligned} \epsilon(k) = &\frac{\Omega}{\gamma_1}\epsilon(k-1) - \frac{\Sigma}{\gamma_1}\beta(k-1) - \frac{\Phi}{\gamma_1}\epsilon_0(k-1) \\ &- \frac{1}{\gamma_1}Q_R\left(\Omega\epsilon(k-1) - \Sigma\beta(k-1) - \Phi\epsilon_0(k-1)\right) \end{aligned} \tag{53}$$

$$\epsilon_0(k) = \frac{I_N \otimes A}{\gamma_1}\epsilon_0(k-1) - \frac{1}{\gamma_1}Q_R((I_N \otimes A)\epsilon_0(k-1)). \tag{54}$$

If the transmission fails such that $k \in H_q$, we have

$$\beta(k) = \frac{\Pi}{\gamma_2}\beta(k-1) + \frac{\Sigma}{\gamma_2}\epsilon(k-1) - \frac{\Phi}{\gamma_2}\epsilon_0(k-1) \tag{55}$$

$$\epsilon(k) = \frac{\Omega}{\gamma_2}\epsilon(k-1) - \frac{\Sigma}{\gamma_2}\beta(k-1) - \frac{\Phi}{\gamma_2}\epsilon_0(k-1) \tag{56}$$

$$\epsilon_0(k) = \frac{I_N \otimes A}{\gamma_2}\epsilon_0(k-1). \tag{57}$$

Comparing the expressions of $Q_R(\cdot)$ in (26) and (53), one sees that the dynamics of $\epsilon(k)$ (transformed estimation error of follower state) also depends on $\epsilon_0(k)$ (transformed estimation error of leader state). By contrast, in the leaderless consensus problem, this does not occur. Therefore, the leader state also needs to be properly quantized. This is

one of the major differences of leader–follower consensus from the leaderless one. By (53) and (54), it is easy to infer that if $\|\Omega\epsilon(k-1)-\Sigma\beta(k-1)-\Phi\epsilon_0(k-1)\|_\infty \le (2R+1)\sigma$ and $\|(I_N\otimes A)\epsilon_0(k-1)\|_\infty \le (2R+1)\sigma$, then by (3) one has $\|\epsilon(k)\|_\infty \le \sigma/\gamma_1$ and $\|\epsilon_0(k)\|_\infty \le \sigma/\gamma_1$, respectively. This means that if the transmissions succeed at k, $\epsilon(k)$ and $\epsilon_0(k)$ can be reset.

By (56), it is possible that $\|\epsilon(k)\|_\infty \le \sigma/\gamma_1$ does not hold during DoS, since $\epsilon(k)$ cannot be reset as in (53). Similar to the case in the leaderless consensus problem, here in the event that $\|\epsilon(k)\|_\infty > \sigma/\gamma_1$, there is also a possibility that $\|\Omega\epsilon(k)-\Sigma\beta(k)-\Phi\epsilon_0(k)\|_\infty > (2R+1)\sigma$, which demonstrates that the quantizer overflow for the follower state occurs. Moreover, in view of (54) and (57), the overflow problem can also happen to the quantization of leader state during DoS. In the following, with the control scheme introduced in (47), we will show that quantizer overflow for both leader and follower states will not occur if one properly designs the scaling parameter $\theta(k)$ in (13). Then, we will discuss the tradeoffs between resilience and data rate.

C. Result for Leader–Follower Consensus

To facilitate the subsequent analysis of leader–follower consensus, we introduce some preliminaries.

In view of the matrices Π, Σ, Φ, and Ω in (48) and (50), respectively, we define the matrices

$$\widetilde{A} = \begin{bmatrix} \Pi & \Sigma & -\Phi \\ -\Sigma & \Omega & -\Phi \\ \mathbf{0} & \mathbf{0} & I_N\otimes A \end{bmatrix} \quad \text{and} \tag{58}$$

$$\widetilde{A}(m) = \widetilde{A}^m = \begin{bmatrix} \widetilde{A}_{11}(m) & \widetilde{A}_{12}(m) & \widetilde{A}_{13}(m) \\ \widetilde{A}_{21}(m) & \widetilde{A}_{22}(m) & \widetilde{A}_{23}(m) \\ \mathbf{0} & \mathbf{0} & I_N\otimes A^m \end{bmatrix} \tag{59}$$

where $\widetilde{A}_{11}(m)$, $\widetilde{A}_{12}(m)$, $\widetilde{A}_{13}(m)$, $\widetilde{A}_{21}(m)$, $\widetilde{A}_{22}(m)$, and $\widetilde{A}_{23}(m)$ are compatible submatrices of $\widetilde{A}(m)$ and the integer m satisfies $0\le m\le M$ as in Lemma 1. Then, we define $P(m+1) = (\Pi\widetilde{A}_{11}(m)+\Sigma\widetilde{A}_{21}(m))/\gamma_2^m$, $S(m+1) = (\Pi\widetilde{A}_{12}(m)+\Sigma\widetilde{A}_{22}(m))/\gamma_2^m$ and $Z(m+1) = (\Pi\widetilde{A}_{13}(m)+\Sigma\widetilde{A}_{23}(m)-\Phi(I_N\otimes A^m))/\gamma_2^m$. Let $\widetilde{C}_0 = \max_{m=0,\ldots,M}\|S(m+1)\|$ and $\widetilde{C}_1 = \max_{m=0,1,\ldots,M}\|Z(m+1)\|$. There exists a unitary matrix $\widetilde{\Psi}$ such that $\widetilde{\Psi}^{-1}(L_{\mathcal{G}}+D)\widetilde{\Psi}$ is an upper-triangular matrix whose diagonals are $\widetilde{\lambda}_i$ $(i=1,2,\ldots,N)$, which are the eigenvalues of $L_{\mathcal{G}}+D$ [28]. With the $\widetilde{\Psi}$, we define the matrices

$$\widetilde{P}(m+1) = (\widetilde{\Psi}\otimes I_n)^T P(m+1)(\widetilde{\Psi}\otimes I_n). \tag{60}$$

Then, we define the set of matrices $\mathcal{P}$ as

$$\mathcal{P} = \{\widetilde{P}(1),\ldots,\widetilde{P}(m+1),\ldots,\widetilde{P}(M+1)\} \tag{61}$$

where in particular we have

$$\widetilde{P}(1) = \begin{bmatrix} A-\widetilde{\lambda}_1 BK & \star & \star & \star \\ \mathbf{0} & A-\widetilde{\lambda}_2 BK & \star & \star \\ \mathbf{0} & \mathbf{0} & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & A-\widetilde{\lambda}_N BK \end{bmatrix} \tag{62}$$

with $\star$ presenting compatible matrices. Finally, we let

$$\widetilde{C}_3 = \max\left\{2\widetilde{C}_4\sqrt{Nn}, \frac{\widetilde{C}_2\widetilde{C}_4\sqrt{Nn}}{(1-\tilde{d})\gamma_1}\right\} \tag{63}$$

where $\widetilde{C}_2 = \widetilde{C}_0+\widetilde{C}_1$ and $\tilde{d} = \tilde{d}_0/\gamma_1$. The parameters $\rho(\widetilde{P}(1)) < \tilde{d}_0 < 1$ and $\widetilde{C}_4 \ge 1$ exist and satisfy $\|\widetilde{P}(1)^p\| \le \widetilde{C}_4\tilde{d}_0^p$ with $p\in\mathbb{Z}_{\ge 1}$.

To facilitate the proof, we first present the following lemma whose proof is provided in [29] due to space limitation.

Lemma 4: Take γ_1 and γ_2 such that

$$\tilde{d}_0 < \gamma_1 < 1, \quad \max_{m=1,\ldots,M}\|\widetilde{P}(m+1)\| \le \rho(\widetilde{P}(1))/\widetilde{C}_4 \tag{64}$$

in which M in Lemma 1, and $\widetilde{C}_4 \ge 1$ satisfying $\|\widetilde{P}(1)^p\| \le \widetilde{C}_4\tilde{d}_0^p$ with $\rho(\widetilde{P}(1)) < \tilde{d}_0 < 1$. Let $\theta_0 \ge C_{x_0}\gamma_1/\sigma$. If $\|\epsilon(s_p)\|_\infty \le \sigma/\gamma_1$ and $\|\epsilon_0(s_p)\|_\infty \le \sigma/\gamma_1$ for $p=0,\ldots,r$, then $\|[\beta^T(s_r)\ \ \epsilon^T(s_r)\ \ \epsilon_0^T(s_r)]^T\|$ is upper-bounded as

$$\|[\beta^T(s_r)\ \ \epsilon^T(s_r)\ \ \epsilon_0^T(s_r)]^T\| \le \sigma\sqrt{\widetilde{C}_3^2+2Nn}/\gamma_1 \tag{65}$$

with $\tilde{C}_3$ in (63). ■

Now, we are ready to present the leader–follower results.

Theorem 2: Consider the multiagent system (1) as the follower agent with control action (47), (12)–(13). The leader agent is given in (45). The communication attempts are periodic with sampling interval Δ. Suppose that the DoS attacks in Assumptions 1 and 2 satisfy $1/T+\Delta/\tau_D < 1$. Let θ_0, γ_1, and γ_2 be chosen as in Lemma 4. If R satisfies

$$2R+1 \ge \widetilde{\zeta}\|[-\Sigma\ \ \Omega\ \ -\Phi]\|_\infty\sqrt{\widetilde{C}_3^2+2Nn}/\gamma_1 \tag{66}$$

with bounded reals $\widetilde{\zeta} = \max\{\widetilde{\zeta}_1,\widetilde{\zeta}_2\}$ given in the proof and $\widetilde{C}_3 \in \mathbb{R}_{>0}$ in (63), then the following hold:

1) the quantizer (2) is not overflowed, and
2) if in addition the DoS attacks satisfy (40), then the leader–follower consensus as in (46) is achieved.

Proof. 1) The unsaturation of the quantizer is proved by induction. Specifically, if the quantizer is not overflowed such that $\|\epsilon(s_p)\|_\infty \le \sigma/\gamma_1$ and $\|\epsilon_0(s_p)\|_\infty \le \sigma/\gamma_1$ for $p=-1,0,\ldots,r$, then the quantizer will not saturate at the transmission attempts within $]s_r,s_{r+1}]$, which implies $\|\epsilon(s_{r+1})\|_\infty \le \sigma/\gamma_1$ and $\|\epsilon_0(s_{r+1})\|_\infty \le \sigma/\gamma_1$.

a) If $s_{r+1} = s_r+\Delta$, in view of (53), it is easy to verify that the quantizer $Q_R(\Omega\epsilon(s_r)-\Sigma\beta(s_r)-\Phi\epsilon_0(s_r))$ of the follower agents is not overflowed in the sense that

$$\|[-\Sigma\ \ \Omega\ \ -\Phi]\ [\beta^T(s_r)\ \ \epsilon^T(s_r)\ \ \epsilon_0^T(s_r)]^T\|_\infty \le (2R+1)\sigma$$

by applying the bound in (65) of Lemma 4. This implies $\|\epsilon(s_{r+1})\|_\infty \le \sigma/\gamma_1$ in view of (53). It is clear that $\|A\|_\infty \le \|[-\Sigma\ \ \Omega\ \ \Phi]\|_\infty$ and $\|\epsilon_0(s_r)\|_\infty \le \sigma/\gamma_1$. Thus, in view of (54), $Q_R((I_N\otimes A)\epsilon_0(s_r))$ for the leader state is not saturated because

$$\begin{aligned}\|(I_N\otimes A)\epsilon_0(s_r)\|_\infty &\le \|A\|_\infty\sigma/\gamma_1 \\ &\le \|[-\Sigma\ \Omega\ -\Phi]\|_\infty\sigma/\gamma_1 \le (2R+1)\sigma.\end{aligned}$$

b) If $s_{r+1} > s_r+\Delta$, it means that the transmissions at $s_r+\Delta$, $s_r+2\Delta$, $\ldots$, $s_r+m\Delta$ fail, where $m\le M$. We verify that

the quantizers for the follower states are also free of overflow at those instants as well as s_{r+1} since

$$\begin{aligned}&\left\|[-\Sigma \quad \Omega \quad -\Phi]\begin{bmatrix}\beta(s_r+m\Delta)\\ \epsilon(s_r+m\Delta)\\ \epsilon_0(s_r+m\Delta)\end{bmatrix}\right\|_\infty\\ &\le \left\|[-\Sigma\ \Omega\ -\Phi]\left(\widetilde{A}/\gamma_2\right)^m[\beta^T(s_r)\ \ \epsilon^T(s_r)\ \ \epsilon_0^T(s_r)]^T\right\|_\infty\\ &\le \widetilde{\zeta}_1\|[-\Sigma \quad \Omega \quad -\Phi]\|_\infty\sigma\sqrt{\widetilde{C}_3^2+2Nn}/\gamma_1 \le (2R+1)\sigma\end{aligned}$$

where $\widetilde{\zeta}_1 = \max_{m=0,\ldots,M}\|(\widetilde{A}/\gamma_2)^m\|$. Similarly, we can also verify the unsaturation of the quantizer for the leader state in the sense that

$$\begin{aligned}&\|(I_N\otimes A)\epsilon_0(s_r+m\Delta)\|_\infty\\ &\le \|(I_N\otimes A)\,(I_N\otimes A/\gamma_2)^m\,\epsilon_0(s_r)\|_\infty\\ &\le \widetilde{\zeta}_2\|A\|_\infty\sigma/\gamma_1 \le (2R+1)\sigma \qquad (67)\end{aligned}$$

where $\widetilde{\zeta}_2 = \max_{m=0,\ldots,M}\|(A/\gamma_2)^m\|$. In view of *a)* and *b)* mentioned above, by induction, we conclude that the quantizer satisfying (66) is not overflowed for all transmissions in the scenario of leader–follower consensus.

2) Following the calculation similar to that after (43) in the proof of Theorem 1, one can obtain that $\|\beta(k)\|_\infty$ is upper-bounded. When (40) is satisfied, one has $\theta(k)\to 0$ and hence $\|\widetilde{\delta}(k)\|_\infty \to 0$ with $k\to\infty$, which implies that the leader–follower consensus in (46) is achieved. ■

Similar to the leaderless consensus scenario, it is good to have small γ_1 that results in large data rate, and small γ_2 for improving the robustness. Here, for the ease of analysis, we have taken the quantizers for the leader and followers to be identical. If one deploys nonidentical quantizers, then there might be another tradeoff in terms of data rates. By increasing the data rate for the leader quantization, more accurate estimation of $x_0(k)$ is possible. In turn, we may be able to reduce the data rate among the followers. By doing so, if the number of the follower agents is not that small, we expect that the overall communication load can be reduced while in contrast the resilience of the systems is not affected. For leader–follower consensus, Remark 4 still holds, i.e., it is good to keep γ_1 and γ_2 small, and have a fast consensus speed for DoS-free periods. For more details, we refer the readers to Remark 4 in this article and Section IV in [13].

V. Numerical Example

In this section, we conduct simulations to verify our results. We consider eight agents in the leaderless consensus and also eight follower agents in the leader–follower consensus (i.e., $N = 8$ in both cases). Each agent has four states with $A\in\mathbb{R}^{4\times 4}$ given below, whose spectral radius is $\rho(A) = 1.1025$. The sampling period is given by $\Delta = 0.1$ s.

$$A = \begin{bmatrix}1.1052 & 0.1105 & -0.1 & 0\\ 0 & 1.1052 & 0 & 0\\ 0.1 & 0 & 0.25 & 0.1\\ 0.1 & 0.3 & 0 & 0.2\end{bmatrix}$$

$$B = \begin{bmatrix}0.1052 & 0.0053\\ 0 & 0.1052\\ 0 & 0\\ 0 & 0\end{bmatrix},\quad K_1 = \begin{bmatrix}3&0&0&0\\0&3&0&0\end{bmatrix}\quad K_2 = \begin{bmatrix}2.9&0&0&0\\0&2.9&0&0\end{bmatrix}.$$

For leaderless consensus, the eight agents exchange data through an undirected and connected communication graph $\mathcal{G}$. For leader–follower consensus, the communication topology among the followers is the same as the one in the leaderless consensus, that is $\mathcal{G}$. The leader agent has interactions with some of the follower agents, which is specified by the matrix D. The matrices $L_\mathcal{G}\in\mathbb{R}^{8\times 8}$ and $D\in\mathbb{R}^{8\times 8}$ are given by

$$L_\mathcal{G} = \begin{bmatrix}3&-1&-1&0&0&0&0&-1\\ -1&4&-1&-1&-1&0&0&0\\ -1&-1&3&-1&0&0&0&0\\ 0&-1&-1&3&-1&0&0&0\\ 0&-1&0&-1&4&-1&-1&0\\ 0&0&0&0&-1&3&-1&-1\\ 0&0&0&0&-1&-1&3&-1\\ -1&0&0&0&0&-1&-1&3\end{bmatrix} \qquad (68)$$

and $D = \mathrm{diag}(1,1,0,0,1,0,0,2)$. With such $L_\mathcal{G}$ and D, we select the state-feedback gains K_1 for leaderless consensus and K_2 for leader–follower consensus, which can be found previously.

For leaderless consensus, since $\rho(J(1)) = 0.77$, by Theorem 1, we choose $d_0 = 0.785$, $C_2 = 1.7977$, and $\gamma_1 = 0.8$, and $\gamma_2 = 6.7244$. With such parameters, the number of quantization levels should satisfy $2R+1\ge 10222$, which can be encoded by 14 bits, and the sufficient DoS-bound condition for consensus is $1/T+\Delta/\tau_D < 0.1048$. For leader–follower consensus, since $\rho(\widetilde{P}(1)) = 0.9485$, according to Theorem 2, we choose $\tilde{d}_0 = 0.96$, $\tilde{C}_4 = 2.2247$, $\gamma_1 = 0.965$, and $\gamma_2 = 7.96$. The number of quantization levels must satisfy $2R+1\ge 15150$ and can be encoded by 14 bits. The theoretical DoS-bound sufficient condition for leader–follower consensus is $1/T+\Delta/\tau_D < 0.0169$.

The time responses of $\|\delta_i(k)\|_\infty$ and $\theta(k)$ for leaderless consensus, and those of $\|\widetilde{\delta}_i(k)\|_\infty$ and $\theta(k)$ for leader–follower consensus are shown in Figs. 1 and 2, respectively, in which the DoS attacks are generated randomly. In Fig. 1 over the time horizon 12 s, the DoS signal yields $|\Xi(0,12)| = 0.9$ s and $n(0,12) = 8$. This corresponds to averaged values of $\tau_D\approx 1.5$, $T\approx 13.33$, and $1/T+\Delta/\tau_D\approx 0.1417$ for the case of leaderless consensus. Similarly, in Fig. 2, the DoS signal yields $|\Xi(0,25)| = 0.4$ s and $n(0,12) = 4$. This corresponds to averaged values of $\tau_D\approx 6.25$, $T\approx 62.5$, and $1/T+\Delta/\tau_D\approx 0.032$ for the case of leader–follower consensus. Though the theoretical bounds regarding $1/T+\Delta/\tau_D$ are violated, by the first plots in Figs. 1 and 2, respectively, one can see that both $\|\delta_i(k)\|_\infty$ and $\|\widetilde{\delta}_i(k)\|_\infty$ converge to zero. This implies that both the leaderless and leader–follower consensus are still successfully achieved.

The developed dynamic quantization with zooming-in and out capabilities can be clearly seen from the second plots in Figs. 1 and 2. One can see that $\theta(k)$ increases when transmissions fail due to the presence of DoS, and decreases during the DoS-free periods. Meanwhile in the leaderless consensus simulation, the actual quantization output (i.e., $Q_R(\cdot)$) ranges from -6 to 6

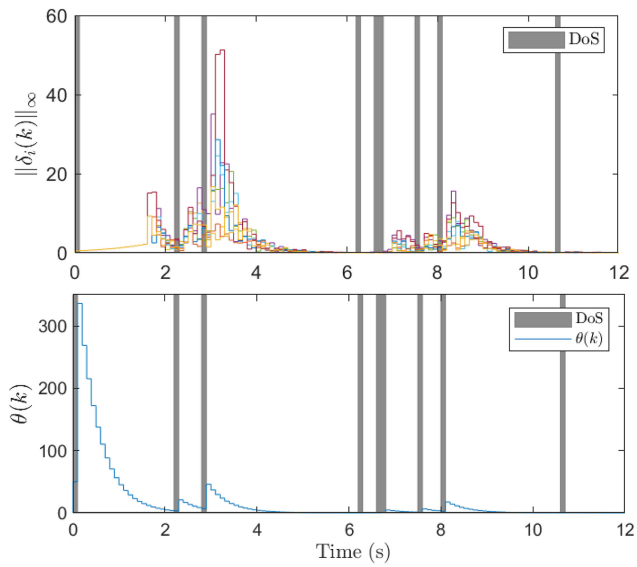

Fig. 1. Top: Time response of $\|\delta_i(k)\|_\infty$ in leaderless consensus; Bottom: Time response of $\theta(k)$ in leaderless consensus.

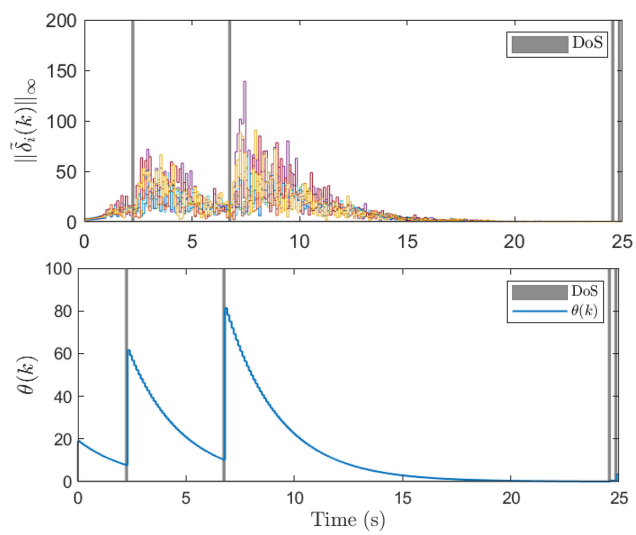

Fig. 2. Top: Time response of $\|\widetilde{\delta}_i(k)\|_\infty$ in leader–follower consensus. Bottom: Time response of $\theta(k)$ in leader–follower consensus.

during the simulation. This amounts to the number of quantization levels 13, which is much smaller than the corresponding theoretical value 10222. In the leader–follower consensus simulation, the actual followers' quantizer output ranges only from -8 to 6 (15 quantization levels), and the quantization for the leader state takes only the values $-1, 0$, and 1 (3 quantization levels). This is also much smaller than the obtained theoretical value 15150.

VI. Conclusion

In this article, we presented results for the leaderless and leader–follower consensus problems of linear multiagent 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 were given. In particular, we provided a feasible way of designing dynamic quantized control with zooming-in and zooming-out capabilities for the multiagent systems with general dynamics, and such dynamic quantization makes finite data rate control possible without quantizer overflow under malicious DoS attacks. We also characterized the bound of DoS attacks under which consensus of the multiagent systems can be guaranteed. Discussions were given on the tradeoffs between bit rates and robustness against DoS.

The results in this article can be extended in several directions. One can consider to relax the assumption on the global knowledge about the communication topology by referring to [30] and [15] and also consider the case of digraph by referring to [31]. It is also worthwhile considering the case of transmission delays [32].

Appendix

Proof of Lemma 3. In view of the dynamics of α in (27) and ξ in (28), it is easy to obtain such a form

$$\begin{bmatrix} \alpha(k+m) \\ \xi(k+m) \end{bmatrix} = \frac{\overline{A}(m)}{\gamma_2^m} \begin{bmatrix} \alpha(k) \\ \xi(k) \end{bmatrix} \tag{69}$$

where $0 \le m \le M$ (in Lemma 1) denotes the number of consecutive unsuccessful transmissions after k and $\overline{A}(m)$ is given in (29). If $k+m+1$ is an instant of successful transmission, in view of (25) and (69), one has

$$\begin{aligned} \alpha(k+m+1) &= ([G \;\; L]/\gamma_1)[\alpha^T(k+m) \;\; \xi^T(k+m)]^T \\ &= ([G \;\; L]/\gamma_1)(\overline{A}(m)/\gamma_2^m)[\alpha^T(k) \;\; \xi^T(k)]^T \\ &= \frac{G(m+1)}{\gamma_1}\alpha(k) + \frac{L(m+1)}{\gamma_1}\xi(k) \end{aligned} \tag{70}$$

with $G(m+1)$ and $L(m+1)$ in (30) and (34), respectively.

It is worth mentioning that (70) is a general form to incorporate the scenarios of successful and unsuccessful transmissions. If $m=0$, then in view of (29), $\overline{A}_{11}(m)$ and $\overline{A}_{22}(m)$ become identity matrices and $\overline{A}_{12}(m)$ and $\overline{A}_{21}(m)$ are matrices with all zero entries. That is, $m=0$ indicates zero unsuccessful transmission between k and $k+1$, and hence (70) is reduced to (25) as a nominal update situation.

Recall the unitary matrix U in (32), where one has $U^T L_{\mathcal{G}} U = \mathrm{diag}(0, \lambda_2, \ldots, \lambda_N)$. It is easy to verify that $(U \otimes I_n)^T (I_N \otimes A - L_{\mathcal{G}} \otimes BK)(U \otimes I_n) = \mathrm{diag}(A, A - \lambda_2 BK, \ldots, A - \lambda_N BK)$. With such U, we let $\overline{\alpha}(k) := (U \otimes I_n)^T \alpha(k) = [\overline{\alpha}_1^T(k) \; \overline{\alpha}_2^T(k)]^T$ and let $\overline{\xi}(k, m+1)$ depending on k and $m+1$ be $\overline{\xi}(k, m+1) := (U \otimes I_n)^T L(m+1)\xi(k) = [\overline{\xi}_1^T(k, m+1) \; \overline{\xi}_2^T(k, m+1)]^T$, where $\overline{\alpha}_1(k)$ and $\overline{\xi}_1(k, m+1)$ represent vectors of the first n elements of $\overline{\alpha}(k)$ and $\overline{\xi}(k, m+1)$, respectively. One can verify that $\overline{\alpha}_1(k) = \mathbf{0}$ for all k. Equation (70) can be transformed to

$$\begin{aligned} \overline{\alpha}(k+m+1) &= \frac{\overline{G}(m+1)}{\gamma_1}\overline{\alpha}(k) + \frac{(U \otimes I_n)^T L(m+1)}{\gamma_1}\xi(k) \\ &= \frac{\overline{G}(m+1)}{\gamma_1}\overline{\alpha}(k) + \frac{1}{\gamma_1}\overline{\xi}(k, m+1) \end{aligned} \tag{71}$$

where $\overline{G}(m+1)$ is given in (31).

Recall that matrix $J(m+1) \in \mathbb{R}^{n(N-1)\times n(N-1)}$ in (33) denotes the remaining parts of $\overline{G}(m+1)$ after deleting the first n rows and columns from $\overline{G}(m+1)$, which is a block diagonal matrix [29]. Then, one can obtain the following equation from (71) such that $\overline{\alpha}_2(k+m+1) = \dfrac{J(m+1)}{\gamma_1}\overline{\alpha}_2(k) + \dfrac{1}{\gamma_1}\overline{\xi}_2(k, m+1)$. Recall that s_r denotes the instant of successful transmissions for $r = 0, 1, \ldots$, and s_{-1} denotes $k = 0$. Thus, we have $s_r = k + m + 1$, and $s_{r-1} = k$ if k is a successful transmission instant. Hence, one has

$$\overline{\alpha}_2(s_r) = \frac{J(m+1)}{\gamma_1}\overline{\alpha}_2(s_{r-1}) + \frac{1}{\gamma_1}\overline{\xi}_2(s_{r-1}, m+1). \quad (72)$$

For distinguishing $J(m+1)$ in iteration steps, we let $J_{r-1}(m_{r-1}+1)$ denote the $J(m+1)$ in (72) used for the iteration from s_{r-1} to s_r with $s_r - s_{r-1} = (m_{r-1}+1)\Delta$. To reduce notation burden, we further let J_{r-1} represent $J_{r-1}(m_{r-1}+1)$. Then, (72) is written as $\overline{\alpha}_2(s_r) = \frac{J_{r-1}}{\gamma_1}\overline{\alpha}_2(s_{r-1}) + \frac{1}{\gamma_1}\overline{\xi}_2(s_{r-1}, m+1)$ for $r = 0, 1, \ldots$. By iteration, it is easy to obtain

$$\overline{\alpha}_2(s_r) = \prod_{p=0}^{r}\frac{J_{p-1}}{\gamma_1}\overline{\alpha}_2(s_{-1}) + \sum_{p=0}^{r-1}\left(\prod_{q=p}^{r-1}\frac{J_q}{\gamma_1}\right)\frac{\overline{\xi}_2(s_{p-1}, m+1)}{\gamma_1} + \frac{\overline{\xi}_2(s_{r-1}, m+1)}{\gamma_1}. \quad (73)$$

In case the networked multiagent systems are not subject to DoS attacks, then J_{p-1} and J_q in (73) are equal to $J(1)$, and there exist $C_2 \geq 1$ and $\rho(J(1)) < d_0 < 1$ such that $\|(J(1))^p\| \leq C_2 d_0^p$ $(p = 1, 2, \cdots)$. This implies that $\|(J(1)/\gamma_1)^p\| \leq C_2\, d^p$, where $\gamma_1 > d_0$ and $0 < d = d_0/\gamma_1 < 1$. Therefore, the type of calculation reduces to the one in [21].

Recall that we have selected γ_2 in Lemma 3, which can make $\|J(m+1)\| \leq \rho(J(1))/C_2$ hold for $m = 1, \ldots, M$. By such γ_2, one has that the iteration of J_{p-1}/γ_1 in (73) yields

$$\|\prod_{p=0}^{r}(J_{p-1}/\gamma_1)\| \leq \prod_{p=0}^{r}\|(J_{p-1}/\gamma_1)\| \leq C_2\, d^r. \quad (74)$$

Notice that C_2 does not accumulate in the iteration because the C_2 caused by $\|(J(1)/\gamma_1)^p\| \leq C_2\, d^p$ (iteration in a DoS-free interval) is canceled out by the C_2 in $\|J(m+1)/\gamma_1\| \leq \rho(J(1))/(\gamma_1 C_2) < d_0/(\gamma_1 C_2) = d/C_2$ ($m = 1, \ldots, M$ representing the number of iteration during a DoS interval). Similarly, one can obtain the results for $\|\prod_{q=p}^{r-1} J_q/\gamma_1\|$.

By Lemma 3, we have selected $d_0 < \gamma_1 < 1$ and $\theta_0 \geq C_{x_0}\gamma_1/\sigma$. By such θ_0, we have $\|\alpha(0)\| = \|\delta(0)\|/\theta_0 \leq \sqrt{Nn}\|\delta(0)\|_\infty/\theta_0 \leq 2\sqrt{Nn}C_{x_0}/\theta_0 \leq 2\sqrt{Nn}\sigma/\gamma_1$, where we use the fact $\|\delta(0)\|_\infty \leq 2C_{x_0}$. By noting that $\|(U\otimes I_n)^T\| = 1$, we have $\|\overline{\alpha}_2(s_{-1})\|$ that satisfies

$$\|\overline{\alpha}_2(s_{-1})\| = \|\overline{\alpha}_2(0)\| \leq \|\overline{\alpha}(0)\| \leq \|(U\otimes I_n)^T\|\|\alpha(0)\| \leq 2\sqrt{Nn}\sigma/\gamma_1. \quad (75)$$

Furthermore, one has $\|\xi(s_{-1})\|_\infty = \|\xi(0)\|_\infty \leq \|(\hat{x}(0) - x(0))/\theta_0\|_\infty = \|x(0)/\theta_0\|_\infty \leq C_{x_0}/\theta_0 \leq \sigma/\gamma_1$. By assumption, we have $\|\xi(s_p)\|_\infty \leq \sigma/\gamma_1$ for $p = 0, 1, \ldots, r$. Incorporating $\|\xi(s_{-1})\|_\infty$, overall one has $\|\xi(s_p)\|_\infty \leq \sigma/\gamma_1$ for $p = -1, 0, \ldots, r$. Hence, we obtain

$$\|\overline{\xi}_2(s_p, m+1)\| \leq \|(U\otimes I_n)^T L(m+1)\|\|\xi(s_p)\| = \|L(m+1)\|\|\xi(s_p)\| \leq C_0\sqrt{Nn}\sigma/\gamma_1 \quad (76)$$

for $p = -1, 0, \ldots$, where C_0 is given by (35).

Substituting (74), (75), and (76) into (73), we have $\|\overline{\alpha}_2(s_r)\| \leq 2C_2\sqrt{Nn}\frac{\sigma}{\gamma_1}d^r + \frac{C_0 C_2\sqrt{Nn}\sigma}{(1-d)\gamma_1^2}(1-d^r) \leq C_1\sigma/\gamma_1$ for $r = 0, 1, \ldots$, where C_1 is as in (36). Incorporating (75), it is obvious that $\|\alpha(s_r)\| \leq \|((U\otimes I_n)^T)^{-1}\|\|\overline{\alpha}(s_r)\| = \|\overline{\alpha}_2(s_r)\| \leq C_1\sigma/\gamma_1$, $r = -1, 0, \ldots$ with the facts that $\|((U\otimes I_n)^T)^{-1}\| = 1$ and $\overline{\alpha}_1(k) = \mathbf{0}$. Finally, one has

$$\|[\alpha^T(s_r)\ \ \xi^T(s_r)]^T\| = \sqrt{\|\alpha(s_r)\|^2 + \|\xi(s_r)\|^2} \leq \sigma\sqrt{C_1^2 + Nn}/\gamma_1,\ r = -1, 0, \ldots$$

where $\|\xi(s_r)\| \leq \sqrt{Nn}\|\xi(s_r)\|_\infty \leq \sqrt{Nn}\sigma/\gamma_1$. ■

References

[1] F. Bullo, *Lectures on Network Systems*. Seattle, WA, USA: Kindle Direct Pub., 2019.

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

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

[4] A. Y. Lu and G. H. Yang, "Secure state estimation for multiagent systems with faulty and malicious agents," *IEEE Trans. Autom. Control*, vol. 65, no. 8, pp. 3471–3485, Aug. 2020.

[5] X. Wang, H. Ishii, L. Du, P. Cheng, and J. Chen, "Privacy-preserving distributed machine learning via local randomization and ADMM perturbation," *IEEE Trans. Signal Process.*, vol. 68, pp. 4226–4241, 2020.

[6] S. Amin, A. Càrdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid Systems: Computation and Control* (Lecture Notes Computer Science Series). Berlin, Germany: Springer, 2009, pp. 31–45.

[7] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

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

[9] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. De Persis, "Networked control under DoS attacks: Tradeoffs between resilience and data rate," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 460–467, Jan. 2021.

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

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

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

[13] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

[14] Z. Feng, G. Hu, and G. Wen, "Distributed consensus tracking for multiagent systems under two types of attacks," *Int. J. Robust Nonlinear Control*, vol. 26, no. 5, pp. 896–918, 2016.

[15] W. Xu, G. Hu, D. W. Ho, and Z. Feng, "Distributed secure cooperative control under denial-of-service attacks from multiple adversaries," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3458–3467, Aug. 2020.
[16] C. Deng and C. Wen, "Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 3, pp. 1308–1318, Sep. 2020.
[17] S. Tatikonda and S. Mitter, "Control under communication constraints," *IEEE Trans. Autom. Control*, vol. 49, no. 7, pp. 1056–1068, Jul. 2004.
[18] G. N. Nair and R. J. Evans, "Stabilizability of stochastic linear systems with finite feedback data rates," *SIAM J. Control Optim.*, vol. 43, no. 2, pp. 413–436, 2004.
[19] R. Carli, F. Fagnani, P. Frasca, and S. Zampieri, "Gossip consensus algorithms via quantized communication," *Automatica*, vol. 46, no. 1, pp. 70–80, 2010.
[20] A. Kashyap, T. Başar, and R. Srikant, "Quantized consensus," *Automatica*, vol. 43, no. 7, pp. 1192–1203, 2007.
[21] K. You and L. Xie, "Network topology and communication data rate for consensusability of discrete-time multi-agent systems," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2262–2275, Oct. 2011.
[22] Z. Qiu, L. Xie, and Y. Hong, "Quantized leaderless and leader-following consensus of high-order multi-agent systems with limited data rate," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2432–2447, Sep. 2016.
[23] S. Feng and H. Ishii, "Dynamic quantized consensus of general linear multi-agent systems under denial-of-service attacks," in *Proc. IFAC World Congr.*, 2020, pp. 3533–3538.
[24] S. Feng and H. Ishii, "Dynamic quantized leader-follower consensus under denial-of-service attacks," in *Proc. IEEE Conf. Decis. Control*, 2020, pp. 488–493.
[25] J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Proc. IEEE Conf. Decis. Control*, 1999, pp. 2655–2660.
[26] Z. Li, Z. Duan, G. Chen, and L. Huang, "Consensus of multiagent systems and synchronization of complex networks: A unified viewpoint," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 57, no. 1, pp. 213–224, Jan. 2010.
[27] R. W. Brockett and D. Liberzon, "Quantized feedback stabilization of linear systems," *IEEE Trans. Autom. Control*, vol. 45, no. 7, pp. 1279–1289, Jul. 2000.
[28] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[29] S. Feng and H. Ishii, "Dynamic quantized consensus of general linear multi-agent systems under denial-of-service attacks," 2020, *arXiv:2004.13815*.
[30] Z. Li, G. Wen, Z. Duan, and W. Ren, "Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1152–1157, Apr. 2015.
[31] Z. Feng and G. Hu, "Distributed secure leader-following consensus of multi-agent systems under DoS attacks and directed topology," in *Proc. IEEE Int. Conf. Inf. Automat.*, 2017, pp. 73–79.
[32] J. Xu, H. Zhang, and L. Xie, "Consensusability of multiagent systems with delay and packet dropout under predictor-like protocols," *IEEE Trans. Autom. Control*, vol. 64, no. 8, pp. 3506–3513, Aug. 2018.

Shuai Feng received the B.Eng. degree in mechatronics engineering from the Wuhan University of Science and Technology, Wuhan, China, in 2011, and M.Eng. degree in mechatronics engineering from the Northeastern University, Shenyang, China, in 2013, and the Ph.D. degree in systems and control from the University of Groningen, Groningen, The Netherlands, in 2018.

He was a Postdoctoral Researcher with the Tokyo Institute of Technology, Tokyo, Japan, in 2019, and with the University of Groningen in 2020 and 2021. His research interests include security of cyber-physical systems, networked control systems, and multiagent systems.

Hideaki Ishii (Fellow IEEE) received the M.Eng. degree in applied systems science from Kyoto University, Kyoto, Japan, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2002.

He was a Postdoctoral Research Associate with the University of Illinois at Urbana-Champaign, Urbana, IL, USA, from 2001 to 2004 and a Research Associate with The University of Tokyo, Tokyo, Japan, from 2004 to 2007. He is currently a Professor with the Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan. He has held visiting positions with CNR-IEIIT at the Politecnico di Torino, Technical University of Berlin, University of Stuttgart, and the City University of Hong Kong. His research interests include networked control systems, multiagent systems, distributed algorithms, and cyber-security of control systems.

Dr. Ishii was a recipient of the *IEEE Control Systems Magazine* Outstanding Paper Award in 2015. He has served as an Associate Editor for the IEEE Control Systems Letters and the *Mathematics of Control, Signals, and Systems*, and previously for *Automatica*, the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, and IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He is the Chair of the IFAC Coordinating Committee on Systems and Signals since 2017. He is the IPC Chair for the IFAC World Congress 2023 to be held in Yokohama, Japan.