Differentially Private Consensus With Quantized Communication

Lan Gao, Shaojiang Deng, Wei Ren, *Fellow, IEEE*, and Chunqiang Hu

***Abstract*—This paper focuses on studying the differentially private consensus problem in multiagent networks under a quantized communication environment, where the exact real-value state is not available for transmission due to the range limitation of digital channels. We first extend the differentially private consensus model to the case of a quantized communication environment integrated with a dynamic encoding/decoding scheme and propose a differentially private communication algorithm utilizing the quantized state with a bounded quantizer instead of the exact real-value state to reach an agreement while protecting the initial or current states of the participants from information disclosure. Then, the convergence analysis of mean square consensus in the case of an unbounded quantizer is given to explain the sufficiency of the extended model and convergence conditions. To overcome the uncertainty of saturation in the case of a bounded quantizer, we also give a statistical analysis on the boundedness of quantization that the bounded quantizer with a finite number of bits can remain unsaturated with a desired high probability under certain conditions. Furthermore, we provide the statistical analysis on the convergent accuracy, which shows that the agreement value just converges to a random variable that falls in the neighboring range of the initial state average and the expectation of the agreement value is equal to the initial state average exactly. In addition, we provide the differential privacy analysis for individual agents and the whole network, and then establish the potential relationship between the dynamic encoding/decoding scheme and the differential privacy mechanism. Finally, the simulation results visually show that the proposed algorithm and the main theoretical results are effective and correct.**

***Index Terms*—Differential privacy, dynamic encoding/decoding strategy, multiagent networks, quantized communication.**

I. Introduction

RECENT years have witnessed increasing attention in the study of the distributed average consensus of multiagent networks due to its broad applications in a large number of fields, such as cooperative control formation [1]–[3]; autonomous underwater vehicles [4], [5]; objective tracking [6]–[8]; distributed estimation [9], [10]; wireless sensor networks [11], [12]; and sensor fusion [13], [14]. More recently, it has also attracted much attention from the research of load balancing of smart grids [15] or plug-in hybrid vehicles [16], large-scale machine learning [17], and distributed computation and optimization [18].

In the fields of privacy preservation, an individual agent in a network may not want to disclose its sensitive information (e.g., the initial state or the current state trajectory) when it collaborates with other agents to complete a conjoint task. For example, a group of unmanned vehicles collaborate with each other to gather at a specified city while keeping their sensitive initial locations private in the process of gathering. In another example, a group of people intend to make a collective decision on some common subject by voting, but they also want to keep their personal opinions private in the process of voting [19]. To preserve the privacy of individuals, the differential privacy mechanism is introduced in [20] and [21], which shows that the proposed differential privacy mechanism has rigorous and proven security properties and its security is also independent of the attack models of adversaries. Furthermore, the differential privacy under continual observation is studied in [22], which promotes the study of the differentially private average consensus in multiagent networks [23], [24]. Then researchers further introduce the differential privacy mechanism into the study of filtering estimation [25] and the distributed optimization [26]–[28].

Most of the literature on differentially private consensus all assume, however, that the communication channels are able to transmit the exact real-value states with no errors. It is worth emphasizing that this assumption is unrealistic because some digital devices, such as analog-to-digital and digital-to-analog converters, discrete-level actuators and sensors, and digital communication channels are often embedded in real multiagent networks, which implies that the transmission of the exact real-value (analog) signal is not available. Furthermore, digital signals possess obvious advantages on robustness and security compared with analog signals. It is interesting to study differentially private consensus under a quantized communication environment where the information exchange is based on quantized digital signals.

Manuscript received March 14, 2018; revised September 26, 2018, November 19, 2018, and December 5, 2018; accepted December 19, 2018. Date of publication March 6, 2019; date of current version August 4, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61672119 and Grant 61702062, in part by the Graduate Scientific Research and Innovation Foundation of Chongqing, China, under Grant CYB16045, in part by the National Science Foundation under Grant CMMI-1537729, in part by 111 Project under Grant B17048, and in part by the Fundamental Research Funds for the Central Universities under Grant 2018CDXYRJ0030. This paper was recommended by Associate Editor Q.-L. Han. *(Corresponding author: Wei Ren.)*

L. Gao and S. Deng are with the School of Computer Science, Chongqing University, Chongqing 400044, China (e-mail: langaouc@outlook.com; sj_deng@cqu.edu.cn).

W. Ren is with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA 92521 USA (e-mail: ren@ece.ucr.edu).

C. Hu is with the School of Software Engineering, Chongqing University, Chongqing 400044, China (e-mail: chu@cqu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2019.2912806.

Digital Object Identifier 10.1109/TCYB.2018.2890645

Note that the quantized technology converting analog signals to digital signals is still an important topic in the study of consensus due to the significant advantages of digital signals on robustness and security compared with analog signals. Quantized consensus based on the integer-valued quantization is investigated in [29] and the extended real-valued quantization scheme can be found in [30]. Since the distributed averaging algorithm cannot achieve the strictly true consensus when deterministic static uniform quantizers [29], [30] are employed, dynamic quantization algorithm [31], [32] and stochastic approximation methods [33], [34] are then developed. Thereafter, a dynamic encoding/decoding scheme is proposed in [35], which employs a pair of zoom-in and zoom-out uniform encoders/decoders to deal with the information exchange. Furthermore, a finite-level quantization with a dynamic encoding/decoding scheme is proposed in [36], which not only achieves the strictly true consensus but establishes a relationship between the convergence rate and the communication data rate. To the best of our knowledge, even if [36] focuses on the finite-level quantization for deterministic systems, most existing literatures on quantized average consensus all suppose that the quantization input is bounded or the quantizer always remains unsaturated. This assumption might be possible for deterministic systems, but it is unrealistic for stochastic systems because the quantization input in a stochastic system might grow unboundedly. For a stochastic system, the bounded quantization is investigated in [37], which provides a boundedness analysis of quantization from the statistical point of view. However, this paper only focuses on the basic uniform quantizer without considering the advanced dynamic encoding/decoding scheme.

The objective of this paper is to extend the results in [23] and [24] to the case of a quantized communication environment and explore the potential relationship between the dynamic encoding/decoding scheme and the differential privacy mechanism. As mentioned previously, the existing literatures on differentially private consensus most suppose that the transmitted messages are the exact real-value states. On the other hand, the existing works on quantized consensus do not address the privacy issue. Therefore, we consider the differentially private consensus problem where the information exchange is based on the inexactly quantized (digital) data instead of the exact real-value (analog) data. Note that this extension is nontrivial and involves several issues. The first challenge is how to analyze the extended differentially private consensus model based on the quantized data to make sure that both the convergent accuracy and the privacy level for each agent can be well remained. Second, in the case of a bounded quantizer, even if the initial states are bounded, the quantization input in a quantizer might be unbounded in the evolution of the algorithm due to the addition of Laplacian noise and the presence of dynamic quantization factors. Once the quantization input goes beyond the capacity of the bounded quantizer, the quantizer will become overloaded and generate an uncontrollable quantization error consequently. Thus, how to overcome the uncertainty that the bounded quantizer with a finite number of bits might become overloaded is another challenge. Third, since the presence of Laplacian noise makes a deterministic system be a stochastic one, the statistical analysis of the stochastic convergence process should be given by employing some statistical characteristics. Finally, the relationship between the dynamic encoding/decoding scheme and the convergent accuracy or differential privacy should be discussed in this paper. In particular, a recent work that has a close relationship with this paper is our previous one [38], which mainly focuses on improving the communication efficiency of the differentially private consensus by introducing an event-triggered control strategy. It is worth emphasizing that the challenges in the previous one are different from that of this paper. The first challenge is how to combine the event-triggered control strategy with the differentially private consensus algorithm to remain the convergent accuracy and the privacy level for each agent in a network. Furthermore, the redesign of the measurement errors and the distributed event-triggering condition is another challenge. In addition, how to design the fully distributed parameters for the event-triggering condition is also a big challenge. In a word, the aims, the application scenarios and the challenges are all different in the two papers.

The main contribution of this paper is that we successfully extend the differentially private consensus to the case of a quantized communication environment, which ensures that not only the sensitive information of individual agents can be well preserved while achieving an agreement but the exact real-value transmission is avoided. Specifically, we first reformulate the differentially private consensus model integrated with a dynamic encoding/decoding scheme for digital multiagent networks, where the transmitted message is a quantized state instead of an exact real-value state. Second, we propose a differentially private communication algorithm utilizing the quantized data with a bounded quantizer to protect the initial or current states of participating agents from information disclosure. Third, the theoretical analysis of mean square convergence in the case of an unbounded quantizer is given to explain the sufficiency of the extended model and convergence conditions. To overcome the uncertainty of saturation in the case of a bounded quantizer, we also give a statistical analysis on the boundedness of quantization that the bounded quantizer with a finite number of bits can remain unsaturated with desired high probability under certain conditions. Fourth, due to the presence of Laplacian random noise in the execution of the proposed algorithm, the final convergence point is just a random variable instead of a deterministic point. Thus, we establish the statistical analysis on the convergence accuracy, which shows that the agreement value just converges to a random variable that falls in a neighbor range of the initial state average but the expectation of the agreement value equals to the initial state average exactly. Finally, we provide the differential privacy analysis for individual agents and the whole network, which shows that any individual agent is able to choose its own privacy level to keep its sensitive information private independently. Besides, the relationship between the dynamic encoding/decoding scheme and the differential privacy level is also established implicitly based on the parameter constraints in the proposed theoretical results.

This paper is organized as follows. Section II introduces some necessary preliminary knowledge about notation, graph theory, fundamental lemmas, the differentially private consensus algorithm, and the dynamic encoding/decoding scheme. Section III reformulates the problem model and introduces the differentially private consensus algorithm utilizing the quantized state in the case of a bounded quantizer. Section IV establishes some main results, including the analysis of mean square convergence, the probability bounds on the boundedness of quantization, and the analysis of convergent accuracy and differential privacy. Section V provides some simulations to verify the main results. Finally, Section VI concludes this paper.

II. Preliminaries and Background

A. Notations

The standard notations used in this paper are summarized as follows. The sets of natural numbers and positive integers are denoted by $\mathbb{N}$ and $\mathbb{N}^+$, respectively. The sets of real numbers and real vectors with p dimensions are denoted by $\mathbb{R}$ and $\mathbb{R}^p$, respectively. For a given positive real number x, the maximum integer not greater than x is denoted by $\lfloor x \rfloor$, and the minimum integer not less than x is denoted by $\lceil x \rceil$. The absolute value of a real number x is denoted by $|x|$ and the Euclidean norms of a vector v and a matrix A are, respectively, denoted by $||v||$ and $||A||$. A 1 vector and a 0 vector composed of N elements are denoted by $\mathbf{1}_N$ and $\mathbf{0}_N$, respectively. Let I_N be a unit matrix with N dimensions. Let v^{T} and A^{T} denote the transposes of a vector v and a matrix A, respectively. Let $\mathbb{P}\{X\}$, $\mathbb{E}[X]$, $\mathbb{V}[X]$, and $f(X)$ represent the probability, the expectation, the variance, and the probability density function of a random variable X, respectively.

B. Graph Theory

An undirected graph composed of N nodes is denoted as $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, W\}$, where $\mathcal{V} = \{1, 2, \ldots, N\}$ denotes the node set, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the edge set, and $W = (w_{ij}) \in \mathbb{R}^{N\times N}$ denotes the adjacency matrix of undirected graph $\mathcal{G}$. An edge $e_{ji} = (j, i)$ represents that the state information of node j can arrive to node i directly. Because $\mathcal{G}$ is undirected, $e_{ij} \in \mathcal{E}$ implies $e_{ji} \in \mathcal{E}$. That is, there is a communication channel between node i and node j, then node i and node j are neighbors of each other and accordingly $w_{ij} = w_{ji} > 0$; otherwise, $w_{ij} = w_{ji} = 0$. The neighbor set of node i is denoted by $\mathcal{N}_i$ and the number of neighbors of node i is denoted by $N_i = |\mathcal{N}_i|$. The Laplacian matrix of W is defined as $L = (l_{ij}) \in \mathbb{R}^{N\times N}$, where $l_{ij} = -w_{ij}, i \neq j$ and $l_{ii} = \sum_{j=1,j\neq i}^{N} w_{ij}$. Here, L is a symmetric positive semidefinite matrix and its eigenvalues are denoted by $0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$ in an ascending order.

C. Fundamental Lemmas

The following lemmas will be used in our analysis throughout this paper.

Lemma 1 [39]: For a given Laplacian matrix L associated with the connected undirected graph $\mathcal{G}$, if $h < 2/\lambda_N$, then

$$\rho_m = \max_{2\leq i\leq N} |1 - h\lambda_i| < 1.$$

Lemma 2 (Laplace Distribution [40]): For a given random variable X, if it obeys a Laplace distribution $\mathrm{Lap}(\mu, b)$, then its probability density function is shown as follows:

$$\mathcal{L}(x) = \frac{1}{2b}\exp\left(-\frac{|x-\mu|}{b}\right)$$

where μ is a location parameter and $b > 0$ is a scale parameter. Furthermore, we can obtain $\mathbb{E}[X] = \mu$ and $\mathbb{V}[X] = 2b^2$.

Lemma 3 (Chebyshev's Lemma [41]): Given a random variable X, then for any non-negative function $h(X)$ and constant $c > 0$

$$\mathbb{P}\{h(X) \geq c\} \leq \frac{\mathbb{E}[h(X)]}{c}.$$

In particular, let $h(X) = |X|$, then we get the Markov's inequality as follows:

$$\mathbb{P}\{|X| \geq c\} \leq \frac{\mathbb{E}[|X|]}{c}.$$

Furthermore, suppose that X is a random variable with finite expectation μ and finite variance σ^2, for $h(X) = (X-\mu)^2$ and $c = k^2\sigma^2$, then the Chebyshev's inequality is given

$$\mathbb{P}\{|X-\mu| \geq k\sigma\} \leq 1/k^2.$$

Lemma 4 (Martingale Convergence Theorem [42]): Let random variable sequence $\{X_n : n = 0, 1, \ldots\}$ be a martingale. If $\lim_{n\to\infty} \mathbb{E}[|X_n|] = M < \infty$, then there is a finite random variable X_∞ with $\mathbb{E}[|X_\infty|] \leq M$ such that

$$X_n \xrightarrow[n\to\infty]{\text{a.s.}} X_\infty.$$

D. Differentially Private Consensus

Differentially private consensus algorithms protect agents' initial sensitive states from information leakage while the individual agents are able to collaborate with each other to reach an agreement. The following discrete-time differentially private consensus model is proposed in [24] as:

$$\theta_i(t+1) = \theta_i(t) + hu_i(t) + s_i\eta_i(t) \tag{1}$$

where $\theta_i(t) \in \mathbb{R}$ is the internal state, $h > 0$ is the step size, $\eta_i(t) \in \mathbb{R}$ is the random noise obeying a Laplace distribution, and $s_i > 0$ is the noise parameter. Also, the controller $u_i(t)$ of each agent in (1) is defined as follows:

$$u_i(t) = \sum_{j\in\mathcal{N}_i} w_{ij}(x_j(t) - x_i(t)) \tag{2}$$

where $x_i(t)$ is the transmitted message and it is defined as follows:

$$x_i(t) = \theta_i(t) + \eta_i(t), \ \ i = 1, \ldots, N. \tag{3}$$

Remark 1: We here assume that the adversaries (no matter inside or outside the network) only seek to infer the sensitive information of individual agents or the agreement value of the network and do not interfere the state updates of individual agents in the network. Note that the presence of noise parameter s_i in (1) plays an important role on producing respective privacy levels for all agents without affecting other agents.

E. Dynamic Encoding/Decoding Scheme

Assume that each communication channel in a digital network is equipped with a pair of dynamic encoder and decoder which are responsible for encoding and decoding the transmitted messages. Given an exact real-value state $z(t)$ as an input, the encoder Φ proposed in [36] is defined as

$$\begin{cases} \xi(0) = 0 \\ \xi(t) = \zeta(t)\phi(t) + \xi(t-1) \\ \phi(t) = q\Big(\frac{1}{\zeta(t)}(z(t) - \xi(t-1))\Big) \end{cases} \tag{4}$$

where $\xi(t)$ is the internal state of encoder Φ, and $\phi(t)$ is the output of Φ. The function $q(\cdot)$ is a uniform quantizer which can transform a real-value state to a quantized state, and $\zeta(t)$ is a scale function which is also called the dynamic quantization factor.

Define the uniform quantizer $q(\cdot)$ as a map: $\mathbb{R} \to S$, where $S = \{0, \pm n\Delta, n = 1, 2, \ldots\}$ is the specified output set. The detailed definition of $q(\cdot)$ is given as [29]

$$q(\chi) = \begin{cases} 0, & -\frac{1}{2}\Delta < \chi < \frac{1}{2}\Delta \\ n\Delta, & \frac{2n-1}{2}\Delta \le \chi < \frac{2n+1}{2}\Delta \\ -q(-\chi), & \chi \le -\frac{1}{2}\Delta \end{cases} \tag{5}$$

where Δ is the quantization interval. Note that if the uniform quantizer $q(\cdot)$ is bounded and only takes a finite output set (e.g., $S = \{0, \pm n\Delta, n = 1, 2, \ldots, K\}$), $q(\cdot)$ is a $2K+1$-level quantizer with quantization interval Δ and it will take $\lceil \log_2(2K+1) \rceil$ bits. It is clear that the $2K+1$-level quantizer will not saturate if the quantization input falls into the range $[(-K-1/2)\Delta, (K+1/2)\Delta)$; otherwise the quantizer will reach saturation and become overloaded.

Given a signal $\phi(t)$ as an input, a decoder Ψ is designed in [36] as

$$\begin{cases} \varphi(0) = 0 \\ \varphi(t) = \zeta(t)\phi(t) + \varphi(t-1) \end{cases} \tag{6}$$

where $\varphi(t)$ is the estimate of the real-value state $z(t)$. It can be easily inferred that $\varphi(t) = \xi(t)$, which implies that encoders also possess the function of decoding besides that of encoding.

III. Problem Statement and Algorithm Design

This section focuses on how to extend the existing algorithm of differentially private consensus to the case of a quantized communication environment, where the exact real-value state is not available for transmission. In light of the dynamic encoding/decoding scheme (4)–(6), each agent i is equipped with a pair of encoder Φ_i and decoder Ψ_i. Given the exact real-value state $x_i(t)$ defined in (3) as an input to encoder Φ_i, let $\xi_i(t)$ and $\phi_i(t)$ be, respectively, the internal state and the output of encoder Φ_i. Also let $\hat{x}_i(t)$ be the output of a certain decoder with $\phi_i(t)$ being the input to the decoder. Here, $\hat{x}_i(t)$ is the estimate of $x_i(t)$. As mentioned in Section II-E, the internal state $\xi_i(t)$ is the same as the estimate $\hat{x}_i(t)$. According to (4), the encoder Φ_i is defined as

$$\begin{cases} \hat{x}_i(0) = 0 \\ \hat{x}_i(t) = \zeta(t)\phi_i(t) + \hat{x}_i(t-1) \\ \phi_i(t) = q\Big(\frac{1}{\zeta(t)}(x_i(t) - \hat{x}_i(t-1))\Big) \end{cases} \tag{7}$$

where $\zeta(t) = \zeta_0\gamma^t$ is the dynamic quantization factor. Because $\xi_i(t) = \hat{x}_i(t)$, we have simply used $\hat{x}_i(t)$ to replace $\xi_i(t)$ in (7). Each agent i implements the encoder Φ_i to encode $x_i(t)$ (analog signal) as $\phi_i(t)$ (digital signal) and then broadcasts $\phi_i(t)$ to its neighbors. Note that in implementing (7), agent i also needs to compute its own state estimate $\hat{x}_i(t)$.

For a certain agent j that is a neighbor of agent i, when agent j receives the output $\phi_i(t)$ from agent i, it decodes $\phi_i(t)$ (digital signal) as $\hat{x}_i(t)$, which is the estimate of the exact real-value state $x_i(t)$. According to (6), the decoder Ψ_j at agent j used to decode $\phi_i(t)$ is defined as

$$\begin{cases} \hat{x}_i(0) = 0 \\ \hat{x}_i(t) = \zeta(t)\phi_i(t) + \hat{x}_i(t-1). \end{cases} \tag{8}$$

It should be emphasized that the decoding operation in (8) and the encoding operation of the internal state in (7) are actually identical even if these two operations are implemented in different agents. That is, the decoded state estimate $\hat{x}_i(t)$ in neighbor $j \in \mathcal{N}_i$ equals to the internal state computed in encoder Φ_i. In summary, in the implementation of its encoder and decoder, each agent i not only needs to decode all $\phi_j(t), j \in \mathcal{N}_i$ from its neighbors but also needs to compute its own state estimate $\hat{x}_i(t)$ as the internal state of its encoder.

Since the exact real-value transmission is restricted and the available neighbor states to agent i are only their estimates decoded from decoder Ψ_i, we redesign the controller $u_i(t)$ in (2) based on the encoders and decoders implemented at each agent as follows:

$$u_i(t) = \sum_{j \in \mathcal{N}_i} w_{ij}\big(\hat{x}_j(t) - \hat{x}_i(t)\big) \tag{9}$$

where the estimate of the exact real-value state is used instead. Note that even if the exact real-value state $x_i(t)$ is available to agent i itself, the agent still uses the estimate $\hat{x}_i(t)$ in (9) to achieve a symmetric design. This symmetric design plays a key role in eliminating the accumulated estimation error, which will be introduced in the next section.

Remark 2: There are a variety of quantizers that have been investigated in the existing literature. Compared with other quantizers, the dynamic encoding/decoding scheme used in this paper has advantages on eliminating the impact of quantization errors and achieving a more accurate convergence result. Specifically, the strictly true consensus can be achieved and the final consensus value is independent of the quantization parameter Δ owing to the symmetric design of the controller and the zoom-in/zoom-out functions of the dynamic encoders/decoders. Furthermore, the assumption of the unbounded quantizer can be avoided and the probability bounds on quantization with bounded quantizers are established in this paper. Of course, compared with other simple quantization schemes, the tradeoff is the increase of computation burden for the agents in the network.

Remark 3: Note that the quantization input in (7) is based on a prediction error $x_i(t) - \hat{x}_i(t-1)$ rather than the state $x_i(t)$, which will largely save the number of bits since the magnitude of the prediction error is far smaller than the state itself. Furthermore, the dynamic quantization factor $\zeta(t)$ plays a key role in the achievement of the strictly true consensus

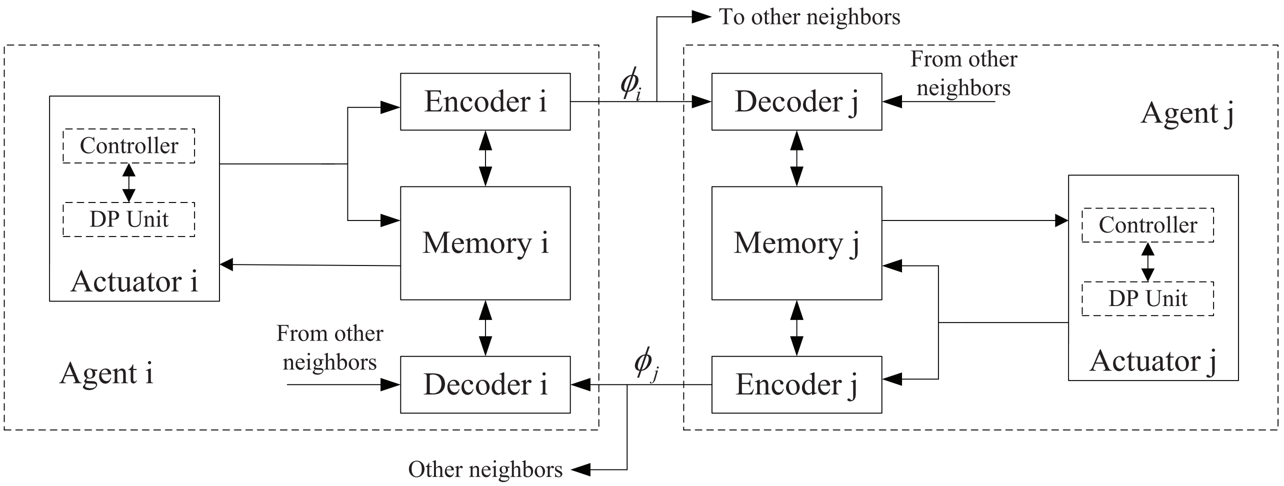


Fig. 1. Integrated communication framework.

because it can zoom in the quantization input to ensure the quantizer still remain activated so that the quantizers cannot stay in a range within one quantization interval Δ in advance. In addition, it should be pointed out that the exponentially decreasing form of $\zeta(t)$ is not originally proposed in this paper. Actually, the notion of the dynamic quantization factor and the exponentially decreasing $\zeta(t)$ can be found in [31] and [35]. This paper studies the differentially private consensus problem with the exponentially decreasing $\zeta(t)$ mainly due to its good performance in achieving a more accurate convergence result.

To illustrate the communication process more intuitively, an integrated communication framework is shown in Fig. 1. Note that the actuator of each agent is divided into two parts: 1) controller and 2) differential privacy (DP) unit, which are responsible for the state fusion and the generation of random noise, respectively. When actuator i generates an exact real-value state $x_i(t)$, this state will be first encoded as $\phi_i(t)$ by encoder Φ_i and then agent i broadcasts $\phi_i(t)$ to all its neighbors. In the meanwhile, once agent i receives the outputs $\phi_j(t)$ from its neighbors, the decoder Ψ_i decodes $\phi_j(t)$ as the estimate $\hat{x}_j(t)$, and then save it in the local memory.

According to this framework, a detailed communication algorithm employing a dynamic encoding/decoding scheme is provided in Algorithm 1. Suppose that each agent i is equipped with a local memory, which is used to store the internal state $\theta_i(t)$, state estimates $\hat{x}_i(t)$ and $\hat{x}_j(t), j \in \mathcal{N}_i$. Furthermore, the initial values of all agents' internal states are given by $\theta(0) = (\theta_1(0), \ldots, \theta_N(0))^{\mathrm{T}}$, and the initial state estimates of all agents are set to 0. After the initializations of local memory and DP units are completed at each agent i, the agent begins to implement Algorithm 1 at each time instant.

Algorithm 1 Differentially Private Consensus Algorithm With a Dynamic Encoding/Decoding Scheme

```
1: Agent $i$ updates its own internal state as follows $\theta_i(t+1) = \theta_i(t) + h\sum_{j=1}^{N} w_{ij}(\hat{x}_j(t) - \hat{x}_i(t) + s_i\eta_i(t)$
2: Produces the Laplacian noise $\eta_i(t+1)$
3: Calculates the transmitted message $x_i(t+1) = \theta_i(t+1) + \eta_i(t+1)$
4: **if** $\frac{1}{\zeta(t+1)}(x_i(t+1) - \hat{x}_i(t)) < (K + 1/2)\Delta$ **then**
5:     Encodes $x_i(t+1)$ as $\phi_i(t+1) = q\Big(\frac{1}{\zeta(t+1)}(x_i(t+1) - \hat{x}_i(t))\Big)$
6: **else**
7:     Terminates the algorithm and resets the initialization.
8: **end if**
9: Broadcasts $\phi_i(t+1)$ to the neighbors of agent $i$
10: Detects if some outputs from neighbors are received or not
11: **if** an output $\phi_j(t+1)$ from neighbor $j$ is received **then**
12:     decodes $\phi_j(t+1)$ as the state estimate $\hat{x}_j(t+1) = \zeta(t+1)\phi_j(t+1) + \hat{x}_j(t)$
13:     updates the state estimate $\hat{x}_j(t+1)$ stored in agent $i$
14: **else**
15:     keeps local memory constant
16: **end if**
```

Remark 4: It is worth emphasizing that Algorithm 1 is based on the case of a bounded quantizer. To avoid the uncertainty of saturation, we here employ a conditional statement in steps 4–8 to ensure the quantization input always falls into the prescribed range in the regular execution of Algorithm 1. Once the quantization input goes beyond the capacity of the bounded quantizer, the conditional statement in Algorithm 1 will be violated and then the algorithm is terminated. One might doubt that the quantization input will often trigger saturation so that Algorithm 1 cannot be executed continuously. In the next section, we will analytically show that this conditional statement is practical and performs well for the case of a bounded quantizer in terms of the proposed differential privacy algorithm and the dynamic encoding/decoding scheme under certain conditions.

IV. Main Results

A. Convergence Analysis With Unbounded Quantizers

Since the Laplacian random noise is added in the state updates of individual agents, the system (1) we study consequently becomes a stochastic system that is more complex than a deterministic one. In this section, we first consider the case of an unbounded quantizer and provide the theoretical analysis on the mean square convergence of system (1), (3), and (7)–(9) under a quantized communication environment. Before stating the main results, we first make some necessary definitions and assumptions as follows.

Definition 1 (Mean Square Convergence [33]): For a given initial state $x(0)$ for all agents, if there exists a random variable x^* such that

$$\lim_{t\to\infty} \mathbb{E}\big[x_i(t) - x^*\big]^2 = 0, \quad i = 1, 2, \ldots, N$$

then all agents are said to achieve mean square convergence asymptotically.

Assumption 1 (Connectivity): Suppose that the communication graph $\mathcal{G}$ is undirected and connected.

Assumption 2 (Infinity of Quantizers): Suppose that the quantizer is unbounded and has an unrestricted dynamic range. In other words, the quantized output set $S = \{n\Delta | n \in \mathbb{N}\}$ is countably infinite and the quantizer cannot reach saturation.

Theorem 1: Consider the consensus model (1) with control input (9) under a quantized communication environment. If Assumptions 1 and 2 hold, and the transmitted message $x_i(t)$ in (3) is corrupted by Laplacian noise $\eta_i(t) \sim \text{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t$, then for any given $h \in (0, 2/\lambda_N), c_i > 0, s_i \in (0, 1), q_i \in (1 - s_i, 1), \gamma \in (\max_i\{\rho_m, q_i\}, 1)$

$$\lim_{t\to\infty} \mathbb{E}[V(t)] = 0, \quad \forall\ \theta_i(0) \in \mathbb{R}$$

where the variable $V(t) = \sum_{i=1}^N (\theta_i(t) - (1/N)\sum_{j=1}^N \theta_j(t))^2$ is the energy function of consensus error.

Proof: See Appendix A. ■

Remark 5: The random noise $\eta_i(t)$ belongs to the Laplacian distribution $\text{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t$, which implies that the addition of the noise is exponentially decreasing as time goes on. In practice, the reasons to choose the exponentially decreasing noise are twofold: 1) the exponentially decreasing noise guarantees that the total additional noise of each agent is bounded and 2) it also guarantees that the variance of the noise $\eta_i(t)$ (i.e., $\mathbb{V}[\eta_i(t)] = \mathbb{E}[\eta_i^2(t)] = 2c_i^2 q_i^{2t}$) is summable in the infinite sequence of time, which produces a bounded convergence result. Otherwise, the unboundedness of the total noise might lead to the instability of the whole system. Furthermore, the constraint $\gamma \in (\max_i\{\rho_m, q_i\}, 1)$ implies that the random noise $\eta_i(t) \sim \text{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t$ should be exponentially decreasing faster than the dynamic quantization factor $\zeta(t) = \zeta_0\gamma^t$, which plays a key role in the theoretical convergence analysis of Theorem 1 and the next Theorem 2.

Remark 6: Theorem 1 shows that the mean square consensus can be achieved successfully under the assumption that the quantizer is unbounded (i.e., the quantizer cannot reach saturation), which implies that if Algorithm 1 can be executed continuously, then the proposed differentially private consensus algorithm utilizing the quantized data with a bounded quantizer can reach an agreement asymptotically in mean square. In the next section, we will show that Algorithm 1 has a good performance on the avoidance of saturation even if the quantizer is bounded and has only a finite dynamic range.

B. Probability Bounds on Boundedness of Quantization With Bounded Quantizers

Considering the limited capacity channels and load balance in digital communication networks, we here employ a bounded uniform quantizer, that is, the quantized data takes only a finite number of values (output set $S = \{0, \pm n\Delta, n = 1, 2, \ldots, K\}$ is countably finite). Note that even if the initial state is bounded, the sequence of quantization input in a quantizer can still become unbounded due to the addition of Laplacian noise and the presence of dynamic quantization factors, which means that the bounded quantizer might reach saturation and produce an uncontrollable quantization error. To avoid this uncertainty, motivated by the idea in [37], we employ a conditional statement in Algorithm 1 to ensure that the quantizers always remain unsaturated in the regular execution of the algorithm. Note that Algorithm 1 can be executed continuously means that the quantizer still remains unsaturated and the quantization error is always controllable. Once the quantization input goes beyond the capacity of the bounded quantizer, the conditional statement in Algorithm 1 will be violated and then the algorithm is terminated.

Clearly, it is impossible to ensure that Algorithm 1 is always executed continuously (i.e., the quantization input never go beyond the capacity of the bounded quantizer) because the addition of Laplace noise makes system (1) become a stochastic system which is more complex than a deterministic one. However, we can give a probability bounds on the boundedness of quantization from the statistical point of view in terms of Algorithm 1. Next, we will analytically show that Algorithm 1 has a good performance based on a fact that the bounded quantizer can remain uniformly unsaturated with high probability under certain conditions.

Theorem 2: Consider the multiagent network (1) with control input (9) in terms of Algorithm 1. Suppose that the initial internal state $\theta(0)$ and the initial additional noise $\eta(0)$ are both bounded. Let $h \in (0, 2/\lambda_N), c_i > 0, s_i \in (0, 1), q_i \in (1 - s_i, 1), \gamma \in (\max_i\{\rho_m, q_i\}, 1)$, then for any time t

$$\mathbb{P}\Big\{||U(t)||_\infty \leq \sqrt{M}/p\Big\} \geq 1 - p, \quad p \in (0, 1) \qquad (10)$$

when the quantization level satisfies

$$K \geq \lfloor \sqrt{M}/p - 1/2 \rfloor + 1 \qquad (11)$$

where

$$\begin{aligned} U(t) = \gamma^{-1}[(I + hL)z(t-1) - hLw(t-1) \\ + (S - I - hL)y(t-1)\big] + y(t) \end{aligned}$$

$$\begin{aligned} M = \gamma^{-2}\left(\frac{N\Delta^2\varrho_1^2}{4} + \varrho_1\varrho_2\sqrt{N}\sqrt{C}\Delta + \varrho_2^2 C\right) \\ + \frac{\sqrt{2}N\Delta\zeta_0\varrho_1\varrho_3\hat{c} + 2N\hat{c}^2\big(\varrho_3^2 + \hat{q}^2\big)}{\zeta_0^2\gamma^2}. \end{aligned}$$

Proof: See Appendix B. ■

Remark 7: Note that $U(t)$ can be seen as an input vector composed of quantization inputs of all quantizers. Consequently, $||U(t)||_\infty$ represents the maximum magnitude of the quantization inputs of all quantizers. Theorem 2 shows that when given a positive constant p, $||U(t)||_\infty$ is bounded with probability at least $1 - p$, which implies that we can select a small p to ensure that the quantization input remains bounded with high probability. It should be pointed out that the quantization level K in (11) is just a conservative estimation, which mainly provides an intuitive reference on the relation between the quantization level and the other key parameters in the network. Once the bound of the probability is determined, we can easily calculate the required number of bits to make the bounded quantizer remain unsaturated with desired high probability. On the other hand, (10) and (11) imply a tradeoff between the desired high probability and the required quantization level, which is not avoidable in the design of a quantizer.

C. Accuracy Analysis

In this section, we further provide the statistical analysis on the convergent accuracy of system (1), (3), and (7)–(9) under a quantized communication environment.

Definition 2 [23]: For a given initial state $x(0)$, if the agreement value of a stochastic system converges to a random variable x^* and the dispersion bound of x^* is r with probability at least $1-p$, where $p \in (0, 1)$, $r \geq 0$, then the (p, r)-accuracy is said to be achieved in the system.

Theorem 3: The proposed differentially private consensus protocol (1) with control input (9) under a quantized communication environment achieves

$$\left(p, \frac{1}{N}\sqrt{\frac{2}{p}\sum_{i=1}^{N}\frac{s_i^2c_i^2}{1-q_i^2}}\right)$$

accuracy. Furthermore, the expectation of the agreement value θ_∞ is unbiased and it equals to the initial state average $\bar{\theta}(0)$ exactly with a disturbance variance

$$\mathbb{V}[\theta_\infty] = \frac{2}{N^2}\sum_{i=1}^{N}\frac{s_i^2c_i^2}{1-q_i^2}.$$

Proof: See Appendix C. ■

Remark 8: Theorem 3 actually shows that the agreement value θ_∞ of the system is just a random variable that falls in a neighbor range of the initial state average, but the expectation of the agreement value θ_∞ equals to the initial state average exactly. Note that the quantization parameter Δ has no direct impact on the final private consensus results. The reasons are twofold: 1) the estimation errors of the whole network are canceled out due to the symmetric design of the controller and 2) the zoom-in/zoom-out functions of the dynamic encoders/decoders make sure that the strictly true consensus can be achieved and the final consensus value is independent of the quantization parameter Δ. Actually, the parameter Δ mainly has an impact on the necessary number of bits used for communication. When the parameter Δ becomes larger, the necessary number of communication bits increases accordingly.

Remark 9: It should be pointed out that Theorems 1–3 are based on the undirected topology. Theoretically, extending the main results to a directed topology is quite challenging. The main reason is that the symmetric property of the undirected topology plays a key role in the convergence analysis and the accuracy analysis. In contrast, it will be quite difficult to deal with the asymmetric structure of the directed topology in the theoretical analysis.

D. Analysis of Differential Privacy

In this section, we first give some necessary definitions on differential privacy and then establish the main result. The agents in a network collaborate with each other to reach an agreement value by exchanging messages with their neighbors. In the process of information exchange, the potential adversaries might be able to observe the transmitted messages (i.e., the quantized outputs), which are also called the observable parts. In contrast, the adversaries cannot observe the internal sensitive states and the additional Laplace noise since they are not transmitted directly in the communication network. For simplicity, let $\phi(t) = (\phi_1(t), \ldots, \phi_N(t))^{\mathrm{T}}$ and $\eta(t) = (\eta_1(t), \ldots, \eta_N(t))^{\mathrm{T}}$, then the possible observation sequence can be represented as $\phi = \{\phi(0), \phi(1), \ldots\}$ and the noise sequence can be represented as $\eta = \{\eta(0), \eta(1), \ldots\}$. From (3), (7), and (8), we can obtain that the quantized output sequence ϕ uniquely depends on the additional noise sequence η once the initial internal state $\theta(0)$ is given. Thus, the possible observation sequence for given $\theta(0)$ and η can be represented as $\Phi_{\theta(0)}(\eta) = \{\phi(0), \phi(1), \ldots\}$. Similarly, the possible observation sequence for given $\theta'(0)$ and η' can be represented as $\Phi_{\theta'(0)}(\eta') = \{\phi'(0), \phi'(1), \ldots\}$.

Definition 3 [20]: For a given pair of vectors x, x' with N dimensions, if there exist a $\delta \geq 0$ and a $k \in \{1, 2, \ldots, N\}$ such that

$$|x_i - x_i'| \leq \begin{cases} \delta, & i = k \\ 0, & i \neq k \end{cases}$$

then x and x' are called δ-adjacent.

Definition 4 [23]: For a given pair of initial values $\theta(0), \theta'(0)$ in a stochastic system, if they are δ-adjacent and for any possible observation sequence set $\mathcal{O} \subset (\mathbb{R}^N)^{\mathbb{N}}$ and noise sequence set $\Omega \subset (\mathbb{R}^N)^{\mathbb{N}}$ such that

$$\mathbb{P}\{\Phi_{\theta(0)}(\eta) \in \mathcal{O} | \eta \in \Omega\} \leq e^{\epsilon\delta}\mathbb{P}\{\Phi_{\theta'(0)}(\eta') \in \mathcal{O} | \eta' \in \Omega\}$$

then the ϵ-differential privacy is said to be preserved in the system.

Remark 10: From Definition 4, we can obtain that the presence or the absence of any one participant does not have obvious influence on the final query results in the implementation of the differential privacy mechanism. In other words, the δ-adjacent $\theta(0)$ and $\theta'(0)$ with noise sequences η and η' will generate the same observation sequence with high probability. As a result, even if the malicious adversaries might listen to the exchanged information between agents, they cannot infer the sensitive information of individual agents or the whole network.

Theorem 4: The proposed differentially private consensus protocol (1) with control input (9) under a quantized communication environment preserves ϵ_i-differential privacy, where

$$\epsilon_i = \frac{q_i}{c_i(q_i + s_i - 1)}, \quad q_i \in (1 - s_i, 1).$$

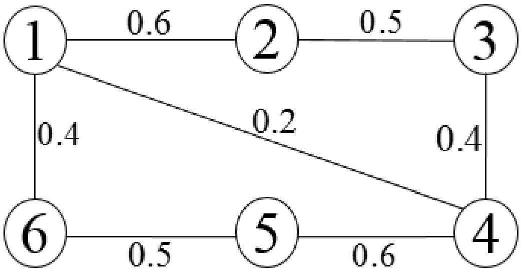


Fig. 2. Weighted undirected topology with six agents.

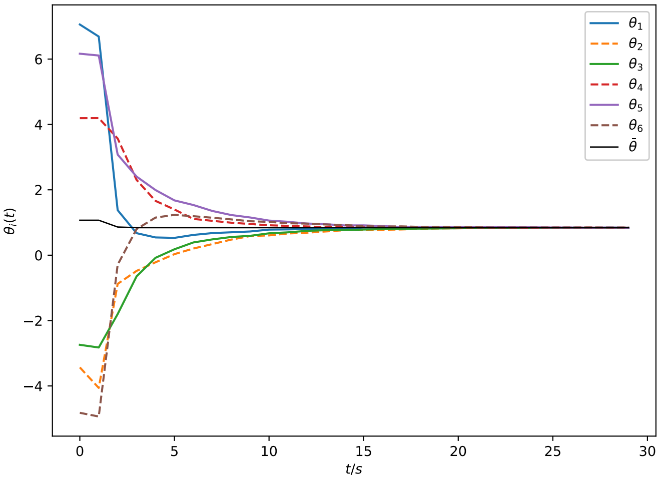


Fig. 3. Trajectory of the internal state of each agent.

Obviously, the privacy level of the whole network is $\epsilon = \max_i(\epsilon_i)$.

Proof: See Appendix D. ∎

Remark 11: Given any privacy level $\{\epsilon_i\}_{i=1}^N$, each agent $i \in 1, \ldots, N$ selects the free parameters c_i, s_i, q_i to determine the amount of noise added in the execution of the main algorithm. To minimize the impact of the dynamic encoding/decoding scheme so that the system can converge to an agreement asymptotically in mean square, Theorems 1 and 2 give the constraints that the parameter γ in dynamic quantization factor $\zeta(t)$ must be ensured that $\gamma \in (\max_i\{\rho_m, q_i\}, 1)$, which implicitly establishes a relationship between the dynamic encoding/decoding scheme and the differential privacy mechanism. Basically, this constraint implies that the Laplacian noise $\eta_i(t) \sim \text{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t$ should be exponentially decreasing faster than the dynamic quantization factor $\zeta(t) = \zeta_0\gamma^t$. That is, when γ becomes smaller, one should add Laplacian noise with smaller parameter q_i, which is corresponding to a larger privacy level when the other free parameters s_i and c_i are given and remain constant. Theorem 3 gives the relationship between the convergence accuracy and the differentially private mechanism, which implies that the convergence result becomes more accurate (i.e., less accuracy is preserved) as the parameter q_i becomes smaller.

Remark 12: Generally speaking, the added noise $\eta_i(t)$ can be drawn from various distributions, such as the Laplace distribution, the Gaussian distribution, the exponential distribution, and the geometric distribution [43]. Even if a number of mechanisms for achieving differential privacy have been investigated, there is no universally optimal mechanism (defined as the best accuracy/utility with a specified privacy level) for various application scenarios [44]. It is worth noting that the notion of differential privacy is originally introduced in [45], where the addition of Laplacian noise produces a standard ϵ-differential privacy. Take the Gaussian mechanism for example, the addition of Gaussian noise leads to a relaxed notion of

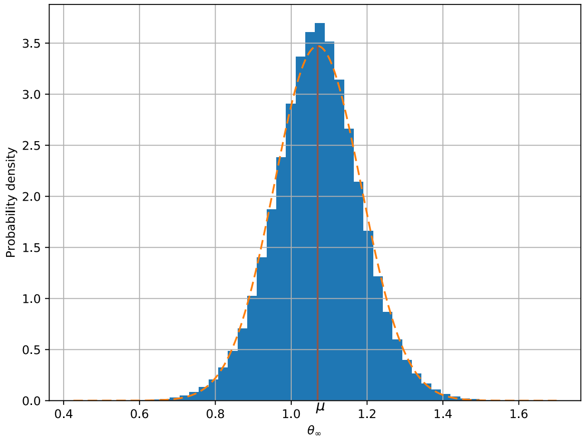


Fig. 4. Histogram of total agreement values.

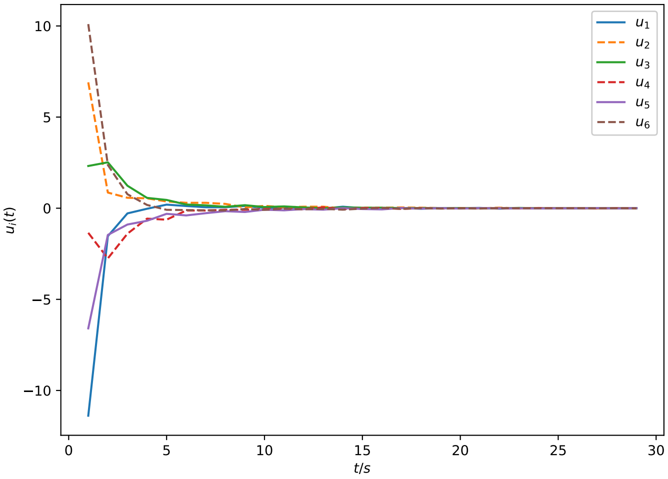


Fig. 5. Trajectory of the controller state of each agent.

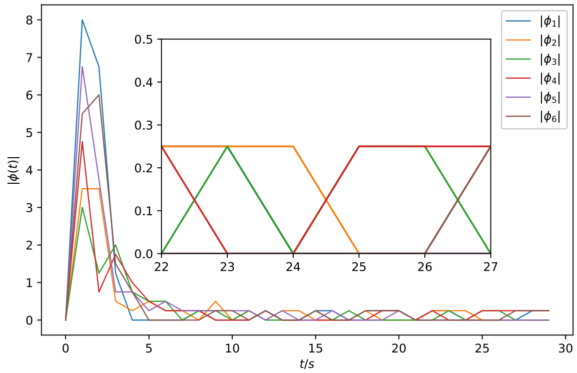


Fig. 6. Quantized output of each agent.

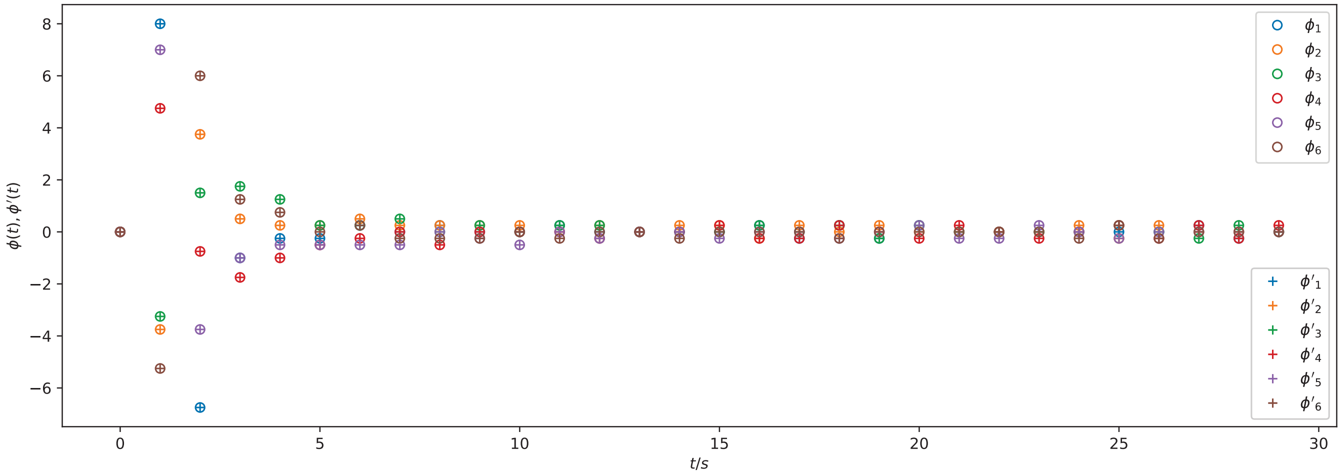


Fig. 7. Observation sequences $\phi(t), \phi'(t)$ corresponding to the δ-adjacent $\theta(0), \theta'(0)$.

privacy denoted by (ϵ, δ)-differential privacy. Compared with the Gaussian mechanism, the Laplacian mechanism allows $\delta = 0$, which implies that more privacy can be preserved in the practical implementation [46]. Furthermore, it is proved that the Laplacian mechanism (among other possible distributions) shows good performance in minimizing the entropy of the transmitted messages while preserving differential privacy in a discrete-time linear feedback system [47]. Therefore, we choose the Laplacian mechanism to establish the standard ϵ-differential privacy in this paper.

V. Simulations

In this section, we provide some simulations to illustrate the main results. Consider a communication network with graph $\mathcal{G}$ given in Fig. 2, and the initial internal state is randomly generated as $\theta(0) = (7.0573, -3.4323, -2.7413, 4.1917, 6.1636, -4.8213)$, then we can obtain $\lambda_N = 2.18$. Letting $c_i = 0.2$, $q_i = 0.1$, $s_i = 0.99$, we can get $h \in (0, 0.92)$, $\gamma \in (0.78, 1)$ according to Theorems 1 and 2. Thus, we can set $h = 0.46$, $\gamma = 0.89$, $\zeta_0 = 0.9$, $\Delta = 0.25$. Then, the necessary quantization level $K \geq 216$ is calculated for a given constant $p = 0.05$. In practice, we choose $K = 200$ for the following simulations. In contrast, if a too small K (e.g., $K = 50$) is chosen, Algorithm 1 is often terminated so that we cannot obtain any simulation results.

The internal state trajectory of each agent is shown in Fig. 3. It should be pointed out that the agreement value of the network does not converge to the initial state average of all agents and it only falls in a neighbor range of the initial state average. Besides, the trajectory of the real-time state average in this paper is time varying instead of a constant initial state average. In other words, the trajectory of the real-time state average might be disturbed at the start time and then gradually tends to be stable as time goes on. For example, the black line in Fig. 3 shows the trajectory of the real-time state average. To obtain the explicit distribution of the agreement value in a stochastic system, we run the algorithm with 10^6 times and we obtain the distribution results as shown in Fig. 4. We can see that all the agreement values of 10^6 runs mainly fall in an interval [0.6, 1.5] and the mean of the histogram equals to the initial state average exactly. It is worth emphasizing that the 0-mean and the diminishing scale function $b_i(t) = c_i q_i^t, q_i \in (0, 1)$ of the additional Laplace noise play key roles on the stability of the real-time state average.

The state trajectory of the controller of each agent is shown in Fig. 5, which shows that the state trajectories of all controllers finally converge to zero asymptotically. The quantized outputs of all agents are shown in Fig. 6, which obviously shows that all outputs are bounded in one quantization interval ($\Delta = 0.25$) finally. Note that even if the quantized outputs cannot reach an exact consensus, the internal states and the state estimates are able to achieve an agreement value asymptotically as shown in Figs. 3 and 5. This is due to the introduction of the dynamic encoding/decoding scheme which employs a dynamic quantization factor so that each agent can obtain a more exact state estimate instead of a directly quantized output.

To show the features of the differential privacy, we choose a pair of δ-adjacent $\theta(0) = (7.0573, -3.4323, -2.7413, 4.1917, 6.1636, -4.8213)$ and $\theta'(0) = (0, -3.4323, -2.7413, 4.1917, 6.1636, -4.8213)$, which implies that only the internal states of the first agent in $\theta(0)$ and $\theta'(0)$ are different. Then we can obtain $\delta = 7.0573$. Based on the δ-adjacent $\theta(0)$ and $\theta'(0)$, the possible observation sequences (i.e., the quantized outputs) between agents are shown in Fig. 7, which shows that the two different observation sequences $\phi(t)$ and $\phi'(t)$ are exactly fitted. That is, the malicious adversaries cannot distinguish the difference between these two observation sequences and then they cannot infer the sensitive information of individual agents or the whole network.

VI. Conclusion

We first reformulate the differentially private consensus model integrated with a dynamic encoding/decoding scheme for digital multiagent networks. Second, we proposed a differentially private communication algorithm utilizing the quantized data with a bounded quantizer to preserve the initial states' privacy of participants. Third, the theoretical analysis on the mean square convergence was provided to explain the feasibility of the extended model and convergence conditions in the case of an unbounded quantizer. Fourth, we gave a statistical analysis that the bounded quantizer with a finite number of bits can remain unsaturated with desired high probability in the execution of the proposed algorithm. Finally, the statistical analysis on the convergent accuracy and the differential privacy was provided and the potential relationship between the dynamic encoding/decoding scheme and the differential privacy was also established. In the future, we will consider to extend the main results to the directed graph and the switching topology conditions.

Appendix A
Proof of Theorem 1

Define consensus error as follows:

$$\delta_i(t) = \theta_i(t) - \frac{1}{N}\sum_{j=1}^{N}\theta_j(t). \tag{12}$$

Let $J = (1/N)\mathbf{1}\mathbf{1}^{\mathrm{T}} \in \mathbb{R}^{N\times N}$. Note that $JL = \mathbf{0}$. Multiplying J on both sides of (36), we have $J\theta(t+1) = J(\theta(t) + S\eta(t))$. Then it follows that:

$$\begin{aligned}\delta(t+1) &= \theta(t+1) - J\theta(t+1)\\ &= (I-hL)\theta(t) + (S-hL)\eta(t) + hLe(t)\\ &\quad - J\theta(t) - JS\eta(t)\\ &= (I-hL)\delta(t) + (S-hL-JS)\eta(t) + hLe(t)\end{aligned} \tag{13}$$

$$\begin{aligned}x(t+1) - \hat{x}(t) &= \theta(t+1) + \eta(t+1) - \hat{x}(t)\\ &= (I-hL)\theta(t) + (S-hL)\eta(t) + hLe(t)\\ &\quad + \eta(t+1) - \hat{x}(t)\\ &= (I+hL)e(t) - hL\delta(t)\\ &\quad + (S-I-hL)\eta(t) + \eta(t+1)\end{aligned} \tag{14}$$

where $\delta(t) = (\delta_1(t), \ldots, \delta_N(t))^{\mathrm{T}}$.

Let $\zeta(t) = \zeta_0\gamma^t$ and denote $w(t) = (1/\zeta(t))\delta(t), z(t) = (1/\zeta(t))e(t), y(t) = (1/\zeta(t))\eta(t)$, then we can have

$$\begin{aligned}w(t+1) &= \gamma^{-1}\big[(I-hL)w(t) + hLz(t) + (S-hL-JS)y(t)\big]\\ z(t+1) &= U(t+1) - Q(U(t+1))\end{aligned} \tag{15}$$

where the quantization input

$$\begin{aligned}U(t+1) = {}&\gamma^{-1}\big[(I+hL)z(t) - hLw(t) + (S-I-hL)y(t)\big]\\ &+ y(t+1)\end{aligned} \tag{16}$$

and $Q(U(t)) = (q(U_1(t)), \ldots, q(U_N(t)))^{\mathrm{T}}$. Note that $z(t+1)$ can be called the quantization error at time $t+1$.

Since L is a symmetric matrix, then we can define the unitary matrix $\phi = (\mathbf{1}/\sqrt{N}, \phi_2, \ldots, \phi_N)$, where $\phi_i^{\mathrm{T}}L = \lambda_i\phi_i^{\mathrm{T}}$. Denote

$$\begin{aligned}&\tilde{\phi} = (\phi_2, \ldots, \phi_N)\\ &D = \mathrm{diag}(0, \lambda_2, \ldots, \lambda_N),\ \tilde{D} = \mathrm{diag}(\lambda_2, \ldots, \lambda_N).\end{aligned}$$

Let $\tilde{w}(t) = \phi^{-1}w(t) = \phi^{\mathrm{T}}w(t)$, then we decompose $\tilde{w}(t)$ as follows:

$$\tilde{w}(t) = \phi^{\mathrm{T}}w(t) = \begin{pmatrix}\tilde{w}_1(t)\\ \tilde{w}_2(t)\end{pmatrix}$$

where the scalar $\tilde{w}_1(t) = 0$ and the vector $\tilde{w}_2(t) = \tilde{\phi}^{\mathrm{T}}w(t)$. Then we have

$$\tilde{w}(t+1) = \phi^{\mathrm{T}}w(t+1) = \begin{pmatrix}0\\ \tilde{w}_2(t+1)\end{pmatrix}$$

where

$$\begin{aligned}\tilde{w}_2(t+1) = {}&\gamma^{-1}\big(\tilde{I} - h\tilde{D}\big)\tilde{w}_2(t) + h\gamma^{-1}\tilde{D}\tilde{\phi}^{\mathrm{T}}z(t)\\ &+ \gamma^{-1}\Big[\tilde{\phi}^{\mathrm{T}}(I-J)S - h\tilde{D}\tilde{\phi}^{\mathrm{T}}\Big]y(t).\end{aligned} \tag{17}$$

Denote $P_1 = \gamma^{-1}(\tilde{I} - h\tilde{D})$, $P_2 = h\gamma^{-1}\tilde{D}\tilde{\phi}^{\mathrm{T}}$, $P_3 = \gamma^{-1}[\tilde{\phi}^{\mathrm{T}}(I-J)S - h\tilde{D}\tilde{\phi}^{\mathrm{T}}]$, and $||P_1|| = \rho_1$, $||P_2|| = \rho_2$, $||P_3|| = \rho_3$. In light of Lemma 1, $\rho_1 = \gamma^{-1}\max_{2\le i\le N}|1 - h\lambda_i| = \gamma^{-1}\rho_m$, $\rho_2 = h\gamma^{-1}\lambda_N$, $\rho_3 \le \gamma^{-1}(||(I-J)S|| + h\lambda_N)$. Then it follows that:

$$\begin{aligned}\tilde{w}_2(t+1) &= P_1\tilde{w}_2(t) + P_2z(t) + P_3y(t)\\ &= P_1^{t+1}\tilde{w}_2(0) + \sum_{k=0}^{t}P_1^{t-k}P_2z(k) + \sum_{k=0}^{t}P_1^{t-k}P_3y(k).\end{aligned} \tag{18}$$

It is worth emphasizing that: 1) $\eta_i(t)$ is independent of $\theta_i(t)$; 2) $\eta_i(t)$ is independent of $\eta_j(t)$ for $i \ne j$; and 3) the expectation $\mathbb{E}[\eta_i(t)] = 0$. Thus, we have

$$\mathbb{E}\big[\tilde{w}_2^{\mathrm{T}}(t+1)\tilde{w}_2(t+1)\big] = \mathbb{E}[T_1 + T_2 + T_3 + T_4 + T_5] \tag{19}$$

where

$$\begin{aligned}T_1 &= \tilde{w}_2^{\mathrm{T}}(0)P_1^{2(t+1)}\tilde{w}_2(0)\\ T_2 &= 2\tilde{w}_2^{\mathrm{T}}(0)P_1^{t+1}\sum_{k=0}^{t}P_1^{t-k}P_2z(k)\\ T_3 &= \sum_{k=0}^{t}z^{\mathrm{T}}(k)P_2^{\mathrm{T}}P_1^{t-k}\sum_{k=0}^{t}P_1^{t-k}P_2z(k)\\ T_4 &= \sum_{k=0}^{t}y^{\mathrm{T}}(k)P_3^{\mathrm{T}}P_1^{t-k}P_1^{t-k}P_3y(k)\\ T_5 &= 2\sum_{k=0}^{t}z^{\mathrm{T}}(k)P_2^{\mathrm{T}}P_1^{t-k}P_1^{t-k}P_3y(k).\end{aligned}$$

Following Assumption 2, the quantizer cannot reach saturation, that is, the quantization error $|z_i(t)| \le \Delta/2$ for any time t. In light of Lemma 2, we obtain $\mathbb{E}[\eta_i^2(t)] = \mathbb{V}[\eta_i(t)] = 2c_i^2q_i^{2t}$ because the random noise $\eta_i(t) \sim \mathrm{Lap}(b_i(t))$ with $b_i(t) = c_iq_i^t, q_i \in (0,1)$. Denote $\hat{c} = \max_i\{c_i\}, \hat{q} = \max_i\{q_i\}$. According to Theorem 1, the parameters satisfy $h \in (0, 2/\lambda_N), \gamma \in (\max\{\rho_m, \hat{q}\}, 1)$, that is, $\rho_1 < 1, \hat{q}/\gamma < 1$. Thus, we further have

$$\mathbb{E}[T_1] \le \rho_1^{2(t+1)}||\tilde{w}_2(0)||^2 \le \rho_1^2||\tilde{w}_2(0)||^2 \tag{20}$$

$$\begin{aligned}\mathbb{E}[T_2] &\le \sqrt{N}\Delta||\tilde{w}_2(0)||\rho_1^{t+1}\rho_2\sum_{k=0}^{t}\rho_1^{t-k}\\ &\le \sqrt{N}\Delta||\tilde{w}_2(0)||\frac{\rho_1\rho_2}{1-\rho_1}\end{aligned} \tag{21}$$

$$\begin{aligned}\mathbb{E}[T_3] &\le \mathbb{E}\left[\sum_{k=0}^{t} ||z^{\mathrm{T}}(k)||\rho_2\rho_1^{t-k}\sum_{k=0}^{t}\rho_1^{t-k}\rho_2||z(k)||\right]\\ &\le \frac{N\Delta^2\rho_2^2}{4(1-\rho_1)^2} \end{aligned}\tag{22}$$

$$\begin{aligned}\mathbb{E}[T_4] &\le \rho_3^2\sum_{k=0}^{t}\rho_1^{2(t-k)}\mathbb{E}\big[y^{\mathrm{T}}(k)y(k)\big]\\ &\le \frac{2N\rho_3^2\hat{c}^2}{\zeta_0^2}\sum_{k=0}^{t}\left(\frac{\hat{q}}{\gamma}\right)^{2k} \le \frac{2N\rho_3^2\hat{c}^2}{\zeta_0^2\big(1-\hat{q}^2\gamma^{-2}\big)} \end{aligned}\tag{23}$$

$$\begin{aligned}\mathbb{E}[T_5] &\le 2\rho_2\rho_3\sum_{k=0}^{t}\rho_1^{2(t-k)}\frac{1}{\zeta(k)}\mathbb{E}\big[||z^{\mathrm{T}}(k)||\cdot||\eta(k)||\big]\\ &\le \frac{\sqrt{N}\Delta\rho_2\rho_3}{\zeta_0}\sum_{k=0}^{t}\frac{1}{\gamma^k}\Big(\mathbb{E}\Big[||\eta(k)||^2\Big]\Big)^{\frac{1}{2}} \le \frac{\sqrt{2}N\Delta\rho_2\rho_3\hat{c}}{\zeta_0\big(1-\hat{q}\gamma^{-1}\big)}. \end{aligned}\tag{24}$$

In conclusion, we have

$$\begin{aligned}&\mathbb{E}\big[\tilde{w}_2^{\mathrm{T}}(t+1)\tilde{w}_2(t+1)\big]\\ &\le \rho_1^2||\tilde{w}_2(0)|| + \sqrt{N}\Delta||\tilde{w}_2(0)||\frac{\rho_1\rho_2}{1-\rho_1} + \frac{N\Delta^2\rho_2^2}{4(1-\rho_1)^2}\\ &\quad + \frac{2N\rho_3^2\hat{c}^2}{\zeta_0^2\big(1-\hat{q}^2\gamma^{-2}\big)} + \frac{\sqrt{2}N\Delta\rho_2\rho_3\hat{c}}{\zeta_0\big(1-\hat{q}\gamma^{-1}\big)}\\ &< \infty. \end{aligned}\tag{25}$$

Consider the candidate Lyapunov function $V(t) = \sum_{i=1}^{N}\delta_i^2(t) = \delta^{\mathrm{T}}(t)\delta(t)$. Then it follows that as $t \to \infty$:

$$\mathbb{E}[V(t)] = \zeta^2(t)\mathbb{E}\big[w^{\mathrm{T}}(t)w(t)\big] = 0.\tag{26}$$

The proof is completed.

Appendix B
Proof of Theorem 2

From (15) and (16), it follows that:

$$\begin{aligned}\mathbb{E}\Big[||U(t+1)||_\infty^2\Big] &\le \mathbb{E}\Big[||U(t+1)||^2\Big]\\ &= \mathbb{E}[M_1+M_2+M_3] \end{aligned}\tag{27}$$

where

$$\begin{aligned}M_1 &= \gamma^{-2}[(I+hL)z(t)-hLw(t)]^{\mathrm{T}}[(I+hL)z(t)-hLw(t)]\\ M_2 &= 2\gamma^{-2}z^{\mathrm{T}}(t)(I+hL)(S-I-hL)y(t)\\ M_3 &= \gamma^{-2}\zeta^{-2}(t)\eta^{\mathrm{T}}(t)(S-I-hL)^2\eta(t)\\ &\quad + \zeta^{-2}(t+1)\eta^{\mathrm{T}}(t+1)\eta(t+1). \end{aligned}$$

Let $\varrho_1 = ||I+hL||$, $\varrho_2 = h||L||$, $\varrho_3 = ||S-I-hL||$, according to (18) and (25), we have

$$\begin{aligned}\mathbb{E}[M_1] &\le \gamma^{-2}\mathbb{E}\Big[\varrho_1^2||z(t)||^2 + 2\varrho_1\varrho_2||z(t)||\cdot||w(t)||\\ &\qquad + \varrho_2^2||w(t)||^2\Big]\\ &\le \gamma^{-2}\left(\frac{N\Delta^2\varrho_1^2}{4} + \varrho_1\varrho_2\sqrt{N}\sqrt{C}\Delta + \varrho_2^2C\right) \end{aligned}\tag{28}$$

where

$$\begin{aligned}C &= \rho_1^2||\tilde{w}_2(0)|| + \sqrt{N}\Delta||\tilde{w}_2(0)||\frac{\rho_1\rho_2}{1-\rho_1} + \frac{N\Delta^2\rho_2^2}{4(1-\rho_1)^2}\\ &\quad + \frac{2N\rho_3^2\hat{c}^2}{\zeta_0^2\big(1-\hat{q}^2\gamma^{-2}\big)} + \frac{\sqrt{2}N\Delta\rho_2\rho_3\hat{c}}{\zeta_0\big(1-\hat{q}\gamma^{-1}\big)}. \end{aligned}\tag{29}$$

Furthermore,

$$\mathbb{E}[M_2] \le \frac{\sqrt{2}N\Delta\varrho_1\varrho_3\hat{c}}{\zeta_0\gamma^2},\quad \mathbb{E}[M_3] \le \frac{2N\hat{c}^2\big(\varrho_3^2+\hat{q}^2\big)}{\zeta_0^2\gamma^2}\tag{30}$$

then it follows that:

$$\mathbb{E}\Big[||U(t+1)||_\infty^2\Big] \le M\tag{31}$$

where

$$\begin{aligned}M &= \gamma^{-2}\left(\frac{N\Delta^2\varrho_1^2}{4} + \varrho_1\varrho_2\sqrt{N}\sqrt{C}\Delta + \varrho_2^2C\right)\\ &\quad + \frac{\sqrt{2}N\Delta\zeta_0\varrho_1\varrho_3\hat{c} + 2N\hat{c}^2\big(\varrho_3^2+\hat{q}^2\big)}{\zeta_0^2\gamma^2}. \end{aligned}\tag{32}$$

By Lemma 3, we thus have

$$\mathbb{P}[||U(t+1)||_\infty \ge c] \le \sqrt{M}/c.\tag{33}$$

Let $p = \sqrt{M}/c$, then (10) in Theorem 2 follows. The proof is completed.

Appendix C
Proof of Theorem 3

Define the estimation error

$$e_i(t) = x_i(t) - \hat{x}_i(t).\tag{34}$$

Combining (1), (3), and (9), it follows that:

$$\begin{aligned}\theta_i(t+1) &= \theta_i(t) + h\sum_{j\in\mathcal{N}_i}w_{ij}\big(\hat{x}_j(t)-\hat{x}_i(t)\big) + s_i\eta_i(t)\\ &= \theta_i(t) + h\sum_{j\in\mathcal{N}_i}w_{ij}\big(\theta_j(t)-\theta_i(t)\big)\\ &\quad + h\sum_{j\in\mathcal{N}_i}w_{ij}\big(\eta_j(t)-\eta_i(t)\big)\\ &\quad - h\sum_{j\in\mathcal{N}_i}w_{ij}\big(x_j(t)-\hat{x}_j(t)\big)\\ &\quad + h\sum_{j\in\mathcal{N}_i}w_{ij}\big(x_i(t)-\hat{x}_i(t)\big) + s_i\eta_i(t) \end{aligned}\tag{35}$$

which can be further written as follows:

$$\theta(t+1) = (I-hL)\theta(t) + (S-hL)\eta(t) + hLe(t)\tag{36}$$

where $\theta(t) = (\theta_1(t),\ldots,\theta_N(t))^{\mathrm{T}}$, $\eta(t) = (\eta_1(t),\ldots,\eta_N(t))^{\mathrm{T}}$, $e(t) = (e_1(t),\ldots,e_N(t))^{\mathrm{T}}$, $S = \mathrm{diag}(s_1,\ldots,s_N)$.

Denote $J = (1/N)\mathbf{1}\mathbf{1}^{\mathrm{T}} \in \mathbb{R}^{N\times N}$, $\bar{\theta}(t) = (1/N)\mathbf{1}^{\mathrm{T}}\theta(t) \in \mathbb{R}$. Obviously, we obtain $JL = \mathbf{0}$. Multiplying J on both sides of (36) leads to $J\theta(t+1) = J(\theta(t)+S\eta(t))$, which is equivalent to

$$\bar{\theta}(t+1) = \bar{\theta}(t) + \frac{1}{N}\sum_{i=1}^{N}s_i\eta_i(t).\tag{37}$$

Note that the noise $\eta_i(t) \sim \mathrm{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t, q_i \in (0, 1)$, and $\mathbb{E}[\eta_i(t)] = 0, \mathbb{V}[\eta_i(t)] = \mathbb{E}[\eta_i^2(t)] = 2c_i^2 q_i^{2t}$ according to Lemma 2. Taking expectations on the both sides of (37), we get $\mathbb{E}[\bar{\theta}(t + 1)] = \bar{\theta}(t)$ and the random sequence $\{\bar{\theta}(t)\}$ is a martingale according to the definition in [42].

From (37), we further have

$$\bar{\theta}(t) = \bar{\theta}(0) + \frac{1}{N}\sum_{k=0}^{t-1}\sum_{i=1}^{N} s_i \eta_i(k). \tag{38}$$

Then it follows that:

$$\mathbb{E}\Big[\bar{\theta}^2(t)\Big] \leq \bar{\theta}^2(0) + \frac{2}{N^2}\sum_{i=1}^{N}\frac{s_i^2 c_i^2}{1 - q_i^2} \tag{39}$$

which implies that the average state sequence $\{\bar{\theta}(t)\}$ converges to a finite random variable θ_∞ almost surely according to Lemma 4.

Denote the convergence point $\theta_\infty = \lim_{t\to\infty}\bar{\theta}(t)$, then we have

$$\begin{aligned}\mathbb{E}[\theta_\infty] &= \bar{\theta}(0)\\ \mathbb{V}[\theta_\infty] &= \frac{2}{N^2}\sum_{i=1}^{N}\frac{s_i^2 c_i^2}{1 - q_i^2}.\end{aligned}$$

By Lemma 3, we obtain

$$\mathbb{P}\big\{|\theta_\infty - \bar{\theta}(0)| \leq r\big\} \geq 1 - \frac{\mathbb{V}[\theta_\infty]}{r^2}. \tag{40}$$

Furthermore, we choose $r = (1/N)\sqrt{(2/p)\sum_{i=1}^{N}[(s_i^2 c_i^2)/(1 - q_i^2)]}$, then $\mathbb{P}\{|\theta_\infty - \bar{\theta}(0)| \leq r\} \geq 1 - p$ is obtained. The proof is completed.

Appendix D
Proof of Theorem 4

For a given pair of δ-adjacent $\theta(0)$ and $\theta'(0)$, suppose that they are different only at the kth agent, that is, $\theta_k(0) = \theta_k'(0) + \delta$ and $\theta_i(0) = \theta_i'(0), i \neq k$. For two different noise sequences $\eta = \{\eta(0), \eta(1), \ldots\}$ and $\eta' = \{\eta'(0), \eta'(1), \ldots\}$, we define a bijection as follows:

$$\eta_i'(t) = \begin{cases}\eta_i(t) + \delta(1 - s_i)^t, & i = k\\ \eta_i(t), & i \neq k.\end{cases}$$

Proposition 1: For any agent k at all time t, the following propositions hold under the above bijection: 1) $\theta_k(t) = \theta_k'(t) + \delta(1 - s_k)^t$; 2) $x_k'(t) = x_k(t)$; 3) $\hat{x}_k'(t) = \hat{x}_k(t)$; and 4) $\phi_k'(t) = \phi_k(t)$, where $\theta_k'(t), x_k'(t), \phi_k'(t)$, and $\hat{x}_k'(t)$ are the internal state, transmitted message, quantized output, and state estimation corresponding to initial state $\theta'(0)$ for agent k, respectively.

Proof: We employ mathematical induction to complete the proof. For the case $t = 0$, it is easy to see that Proposition 1 holds. Assume Proposition 1 also holds for time t, then for time $t + 1$, we have

$$\begin{aligned}&\theta_k(t+1) - \theta_k'(t+1)\\ &\quad= \theta_k(t) - \theta_k'(t) + h\big(u_k(t) - u_k'(t)\big) + s_k\big(\eta_k(t) - \eta_k'(t)\big)\\ &\quad= \delta(1 - s_k)^t + h\left(\sum_{j\in\mathcal{N}_k} w_{ij}\big(\hat{x}_j(t) - \hat{x}_k(t)\big)\right.\\ &\qquad\qquad \left. - \sum_{j\in\mathcal{N}_k} w_{ij}\Big(\hat{x}_j'(t) - \hat{x}_k'(t)\Big)\right)\\ &\qquad + s_k\big(\eta_k(t) - \eta_k'(t)\big)\\ &\quad= \delta(1 - s_k)^t + s_k\big(-\delta(1 - s_k)^t\big)\\ &\quad= \delta(1 - s_k)^{t+1}\\ &x_k'(t+1) = \theta_k'(t+1) + \eta_k'(t+1)\\ &\quad= \theta_k(t+1) - \delta(1 - s_k)^{t+1} + \eta_k(t+1) + \delta(1 - s_k)^{t+1}\\ &\quad= \theta_k(t+1) + \eta_k(t+1)\\ &\quad= x_k(t+1)\\ &\hat{x}_k'(t+1) = \zeta(t+1)q\left(\frac{x_k'(t+1) - \hat{x}_k'(t)}{\zeta(t+1)}\right) + \hat{x}_k'(t)\\ &\quad= \zeta(t+1)q\left(\frac{x_k(t+1) - \hat{x}_k(t)}{\zeta(t+1)}\right) + \hat{x}_k(t)\\ &\quad= \hat{x}_k(t+1)\\ &\phi_k'(t+1) = q\left(\frac{x_k'(t+1) - \hat{x}_k'(t)}{\zeta(t+1)}\right)\\ &\quad= q\left(\frac{x_k(t+1) - \hat{x}_k(t)}{\zeta(t+1)}\right)\\ &\quad= \phi_k(t+1).\end{aligned}$$

The proof is completed. ■

Denote

$$\begin{aligned}\Phi_{\theta(0)}(\eta) &= \{\phi(0), \ldots, \phi(T)\} = \{\rho_0, \ldots, \rho_T\}\\ \Phi_{\theta'(0)}\big(\eta'\big) &= \big\{\phi'(0), \ldots, \phi'(T)\big\} = \big\{\rho_0', \ldots, \rho_T'\big\}\end{aligned}$$

then we have $\Phi_{\theta(0)}(\eta) = \Phi_{\theta'(0)}(\eta')$ according to Proposition 1, which implies that the malicious adversaries cannot distinguish the difference between these two observation sequences and then they cannot infer the sensitive information of individual agents or the whole network.

The joint probability density of observation sequences $\Phi_{\theta(0)}(\eta)$ and $\Phi_{\theta(0)}(\eta)$ can be denoted as follows:

$$\begin{aligned}f\big(\Phi_{\theta(0)}(\eta) \in \mathcal{O}\big) &= \prod_{t=0}^{\mathrm{T}} f(\rho_t|\rho_0, \ldots, \rho_{t-1})\\ f\big(\Phi_{\theta'(0)}\big(\eta'\big) \in \mathcal{O}\big) &= \prod_{t=0}^{\mathrm{T}} f\big(\rho_t'|\rho_0', \ldots, \rho_{t-1}'\big).\end{aligned}$$

It should be pointed out that the quantized output $\phi(t)$ uniquely depends on the additional noise $\eta(t)$ once the initial internal state $\theta(0)$ is given. Besides, the additional random noise $\eta_i(t)$ obeys the Laplacian distribution $\eta_i(t) \sim \mathrm{Lap}(b_i(t))$ with $b_i(t) = c_i q_i^t, q_i \in (0, 1)$. Thus, the joint probability density can be further denoted as follows:

$$\begin{aligned}f\big(\Phi_{\theta(0)}(\eta) \in \mathcal{O}\big) &= \prod_{t=0}^{\mathrm{T}}\prod_{i=1}^{N}\mathcal{L}(\eta_i(t))\\ f\big(\Phi_{\theta'(0)}\big(\eta'\big) \in \mathcal{O}\big) &= \prod_{t=0}^{\mathrm{T}}\prod_{i=1}^{N}\mathcal{L}\big(\eta_i'(t)\big).\end{aligned} \tag{41}$$

When the time sequence $T \to \infty$, it follows that:

$$\begin{aligned}\frac{f\left(\Phi_{\theta(0)}(\eta) \in \mathcal{O}\right)}{f\left(\Phi_{\theta'(0)}(\eta') \in \mathcal{O}\right)} &= \frac{\prod_{t=0}^{\mathrm{T}} \prod_{i=1}^{N} \mathcal{L}(\eta_i(t))}{\prod_{t=0}^{\mathrm{T}} \prod_{i=1}^{N} \mathcal{L}\left(\eta_i'(t)\right)} \\ &= \frac{\prod_{t=0}^{\mathrm{T}} \mathcal{L}(\eta_k(t))}{\prod_{t=0}^{\mathrm{T}} \mathcal{L}\left(\eta_k'(t)\right)} = \prod_{t=0}^{\mathrm{T}} e^{\frac{|\eta_k'(t)|-|\eta_k(t)|}{c_k q_k^t}} \\ &\le \prod_{t=0}^{\mathrm{T}} e^{\frac{|\eta_k'(t)-\eta_k(t)|}{c_k q_k^t}} = \prod_{t=0}^{\mathrm{T}} e^{\frac{\delta}{c_k}\left(\frac{1-s_k}{q_k}\right)^t} \\ &= e^{\epsilon_k \delta}. \end{aligned} \tag{42}$$

Taking integrations on both sides of (42), we can have the following probability:

$$\mathbb{P}\left\{\Phi_{\theta(0)}(\eta) \in \mathcal{O}\right\} \le e^{\epsilon_k \delta}\mathbb{P}\left\{\Phi_{\theta'(0)}\left(\eta'\right) \in \mathcal{O}\right\} \tag{43}$$

where $\epsilon_k = [q_k/(c_k(q_k + s_k - 1))]$, $q_k \in (1 - s_k, 1)$.

According to Definition 4, the agent k has its own privacy level ϵ_k. It is obvious that any agent $i \in \{1, \dots, N\}$ is able to preserve ϵ_i-differential privacy with its own privacy level

$$\epsilon_i = \frac{q_i}{c_i(q_i + s_i - 1)},\ \ q_i \in (1 - s_i, 1). \tag{44}$$

Consequently, the privacy level of the whole network is the maximum one of all ϵ_i, $i = \{1, \dots, N\}$, that is, $\epsilon = \max_i(\epsilon_i)$. The proof is completed.

References

[1] D. M. Stipanović, G. Inalhan, R. Teo, and C. J. Tomlin, "Decentralized overlapping control of a formation of unmanned aerial vehicles," *Automatica*, vol. 40, no. 8, pp. 1285–1296, 2004.

[2] W. Ren and E. Atkins, "Distributed multi-vehicle coordinated control via local information exchange," *Int. J. Robust Nonlin. Control*, vol. 17, nos. 10–11, pp. 1002–1033, 2007.

[3] X. Ge, Q.-L. Han, D. Ding, X.-M. Zhang, and B. Ning, "A survey on recent advances in distributed sampled-data cooperative control of multi-agent systems," *Neurocomputing*, vol. 275, pp. 1684–1701, Jan. 2018.

[4] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multivehicle cooperative control," *IEEE Control Syst.*, vol. 27, no. 2, pp. 71–82, Apr. 2007.

[5] A. Bahr, J. J. Leonard, and M. F. Fallon, "Cooperative localization for autonomous underwater vehicles," *Int. J. Robot. Res.*, vol. 28, no. 6, pp. 714–728, 2009.

[6] W. Ren, "Distributed cooperative attitude synchronization and tracking for multiple rigid bodies," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 2, pp. 383–392, Mar. 2010.

[7] Z. Li, X. Liu, W. Ren, and L. Xie, "Distributed tracking control for linear multiagent systems with a leader of bounded unknown input," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 518–523, Feb. 2013.

[8] L. Ding, Q.-L. Han, and G. Guo, "Network-based leader-following consensus for distributed multi-agent systems," *Automatica*, vol. 49, no. 7, pp. 2281–2286, 2013.

[9] R. Olfati-Saber, "Distributed Kalman filter with embedded consensus filters," in *Proc. 44th IEEE Conf. Decis. Control Eur. Control Conf. (CDC-ECC)*, 2005, pp. 8179–8184.

[10] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," in *Proc. 46th IEEE Conf. Decis. Control*, 2007, pp. 5492–5498.

[11] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 1, pp. 171–183, Jan. 2019.

[12] X. Ge and Q.-L. Han, "Consensus of multiagent systems subject to partially accessible and overlapping Markovian network topologies," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 1807–1819, Aug. 2017.

[13] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw.*, 2005, p. 9.

[14] R. Olfati-Saber and J. S. Shamma, "Consensus filters for sensor networks and distributed sensor fusion," in *Proc. 44th IEEE Conf. Decis. Control Eur. Control Conf. (CDC-ECC)*, 2005, pp. 6698–6703.

[15] L. Ding, Q.-L. Han, L. Wang, and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3924–3935, Sep. 2018.

[16] E. Sortomme, M. M. Hindi, S. J. MacPherson, and S. S. Venkata, "Coordinated charging of plug-in hybrid electric vehicles to minimize distribution system losses," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 198–205, Mar. 2011.

[17] K. I. Tsianos, S. Lawlor, and M. G. Rabbat, "Consensus-based distributed optimization: Practical issues and applications in large-scale machine learning," in *Proc. 50th Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, 2012, pp. 1543–1550.

[18] W. Shi, Q. Ling, G. Wu, and W. Yin, "Extra: An exact first-order algorithm for decentralized consensus optimization," *SIAM J. Optim.*, vol. 25, no. 2, pp. 944–966, 2015.

[19] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[20] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.*, 2008, pp. 1–19.

[21] C. Dwork and J. Lei, "Differential privacy and robust statistics," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2009, pp. 371–380.

[22] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proc. 42nd ACM Symp. Theory Comput.*, Cambridge, MA, USA, 2010, pp. 715–724.

[23] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proc. ACM Workshop Privacy Electron. Soc.*, 2012, pp. 81–90.

[24] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus with optimal noise selection," *IFAC PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[25] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[26] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," in *Proc. Int. Conf. Distrib. Comput. Netw.*, 2015, p. 4.

[27] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 395–408, Mar. 2018.

[28] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 50–64, Jan. 2017.

[29] A. Kashyap, T. Başar, and R. Srikant, "Quantized consensus," *Automatica*, vol. 43, no. 7, pp. 1192–1203, 2007.

[30] P. Frasca, R. Carli, F. Fagnani, and S. Zampieri, "Average consensus on networks with quantized communication," *Int. J. Robust Nonlin. Control*, vol. 19, no. 16, pp. 1787–1816, 2009.

[31] R. Carli, F. Fagnani, P. Frasca, and S. Zampieri, "Efficient quantized techniques for consensus algorithms," in *Proc. NeCST Workshop*, vol. 3. Nancy, France, 2007.

[32] Q. Zhang, B.-C. Wang, and J.-F. Zhang, "Distributed dynamic consensus under quantized communication data," *Int. J. Robust Nonlin. Control*, vol. 25, no. 11, pp. 1704–1720, 2015.

[33] M. Huang and J. H. Manton, "Coordination and consensus of networked agents with noisy measurements: Stochastic algorithms and asymptotic behavior," *SIAM J. Control Optim.*, vol. 48, no. 1, pp. 134–161, 2009.

[34] T. Li and J.-F. Zhang, "Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2043–2057, Sep. 2010.

[35] R. Carli, F. Bullo, and S. Zampieri, "Quantized average consensus via dynamic coding/decoding schemes," *Int. J. Robust Nonlin. Control*, vol. 20, no. 2, pp. 156–175, 2010.

[36] T. Li, M. Fu, L. Xie, and J.-F. Zhang, "Distributed consensus with limited communication data rate," *IEEE Trans. Autom. Control*, vol. 56, no. 2, pp. 279–292, Feb. 2011.

[37] S. Kar and J. M. Moura, "Distributed consensus algorithms in sensor networks: Quantized data and random link failures," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1383–1400, Mar. 2010.

[38] L. Gao, S. Deng, and W. Ren, "Differentially private consensus with event-triggered mechanism," *IEEE Trans. Control Netw. Syst.*, to be published. doi: 10.1109/TCNS.2018.2795703.

[39] C. Godsil and G. F. Royle, *Algebraic Graph Theory*, vol. 207. New York, NY, USA: Springer, 2013.

[40] S. Kotz, T. Kozubowski, and K. Podgorski, *The Laplace Distribution and Generalizations: A Revisit With Applications to Communications, Economics, Engineering, and Finance*. New York, NY, USA: Springer, 2012.

[41] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. Boston, MA, USA: Tata McGraw-Hill Edu., 2002.

[42] M. B. Nevel'son and R. Z. Khaśminskij, *Stochastic Approximation and Recursive Estimation*, vol. 47. Providence, RI, USA: Amer. Math. Soc., 1976.

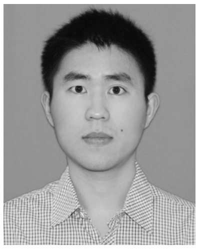
[43] J. Cortés *et al.*, "Differential privacy in control and network systems," in *Proc. 55th IEEE Conf. Decis. Control*, 2016, pp. 4252–4272.

[44] H. Brenner and K. Nissim, "Impossibility of differentially private universally optimal mechanisms," *Found. Comput. Sci.*, 2010, pp. 71–80.

[45] C. Dwork, "Differential privacy," in *International Colloquium on Automata, Languages, and Programming*. Venice, Italy: Springer, 2006, pp. 1–12.

[46] C. Dwork, K. Kenthapadi, F. Mcsherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT)*, May/Jun. 2006, pp. 486–503.

[47] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Entropy-minimizing mechanism for differential privacy of discrete-time linear feedback systems," in *Proc. 53rd IEEE Conf. Decis. Control*, 2014, pp. 2130–2135.

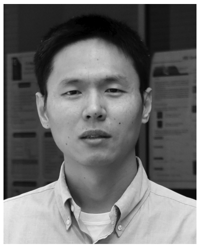


Lan Gao received the B.S. degree in information and computing science from Shengli College, China University of Petroleum, Dongying, China, in 2012. He is currently pursuing the Ph.D. degree in computer science and technology from Chongqing University, Chongqing, China.

His current research interests include multiagent networks, differential privacy, and distributed optimization.

Shaojiang Deng received the B.S. degree in computer science and technology from Chongqing Jianzhu University, Chonqing, China, in 1993 and the Ph.D. degree in computer science and technology from Chongqing University, Chongqing, in 2005.

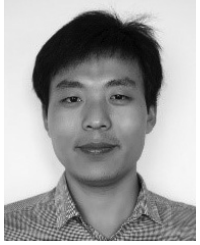
He is currently a Professor with the College of Computer Science and Technology, Chongqing University. His current research interests include neural networks, wireless sensor networks, and wireless body area networks.



Wei Ren (F'16) received the Ph.D. degree in electrical engineering from Brigham Young University, Provo, UT, USA, in 2004.

He was a Faculty Member with Utah State University, Logan, UT, USA, and a Post-Doctoral Researcher with the University of Maryland at College Park, College Park, MD, USA. He is currently a Professor with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA, USA. He has authored two books entitled *Distributed Coordination of Multiagent Networks* (Springer-Verlag, 2011) and *Distributed Consensus in Multivehicle Cooperative Control* (Springer-Verlag, 2008). His current research interests include distributed control of multiagent systems and autonomous control of unmanned vehicles.

Dr. Ren was a recipient of the Antonio Ruberti Young Researcher Prize in 2017 and the National Science Foundation CAREER Award in 2008. He is currently an Associate Editor of *Automatica* and *Systems and Control Letters*.



Chunqiang Hu received the B.S. degree in computer science and technology from Southwest University, Chongqing, China, in 2006, the M.S. and Ph.D. degrees in computer science and technology from Chongqing University, Chongqing, China, in 2009 and 2013, respectively, and the Ph.D. degree in computer science from George Washington University, Washington, DC, USA, in 2016.

He is currently a Faculty Member with the School of Software Engineering, Chongqing University. His current research interests include privacy-aware computing, big data security and privacy, wireless and mobile security, applied cryptography, and algorithm design and analysis.

Dr. Hu was a recipient of the Hundred-Talent Program by Chongqing University. He is a member of ACM.