Differentially Private Nash Equilibrium Seeking in Quadratic Network Games

Lei Wang, Kemi Ding, Yan Leng, Xiaoqiang Ren, and Guodong Shi

***Abstract*—In this paper, we develop distributed computation algorithms for Nash equilibriums of linear quadratic network games with proven differential privacy guarantees. In a network game with each player's payoff being a quadratic function, the dependencies of the decisions in the payoff function naturally encode a network structure governing the players' inter-personal influences. Such social influence structure and the individual marginal payoffs of the players indicate economic spillovers and individual preferences, and thus they are subject to privacy concerns. For distributed computing of the Nash equilibrium, the players are interconnected by a public communication graph, over which dynamical states are shared among neighboring nodes. When the players' marginal payoffs are considered to be private knowledge, we propose a distributed randomized gradient descent algorithm, in which each player adds a Laplacian random noise to her marginal payoff in the recursive updates. It is proven that the algorithm can guarantee differential privacy and convergence in expectation to the Nash equilibrium of the network game at each player's state. Moreover, the mean-square error between the players' states and the Nash equilibrium is shown to be bounded by a constant related to the differential privacy level. Next, when both the players' marginal payoffs and the influence graph are private information, we propose two distributed algorithms by randomized communication and randomized projection, respectively, for privacy preservation. The differential privacy and convergence guarantees are also established for such algorithms.**

***Index Terms*—Differential privacy, distributed computation, linear quadratic network game.**

L. Wang is with the College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China. Email: lei.wangzju@zju.edu.cn.

K. Ding is with Shenzhen Key Laboratory of Control Theory and Intelligent Systems, and School of System Design and Intelligent Manufacturing, Southern University of Science and Technology, Shenzhen 518055, China. E-mail: dingkm@sustech.edu.cn.

Y. Leng is with McCombs School of Business, the University of Texas at Austin, Austin, TX 78735, USA. Email: yan.leng@mccombs.utexas.edu.

X. Ren is with School of Mechatronic Engineering and Automation, Shanghai University and Key Laboratory of Marine Intelligent Unmanned Swarm Technology and System, Ministry of Education, Shanghai 200444, China. Email: xqren@shu.edu.cn.

G. Shi is with the Australian Centre for Robotics, the University of Sydney, Sydney, NSW 2006, Australia. E-mail: guodong.shi@sydney.edu.au.

The work of L. Wang was supported by the National Key R&D Program of China under Grant No. 2018YFA0703803, the National Natural Science Foundation of China under Grant No. 62203386, and Zhejiang Provincial Natural Science Foundation of China under Grant No. LZ23F030008. The work of K. Ding was supported by the National Natural Science Foundation of China under Grant No.20231120102304001, STIC under Grants No.62303212, ZDSYS20220330161800001. The work of X. Ren was supported by the National Natural Science Foundation of China under Grant 62273223 and 62336005, and the Project of Science and Technology Commission of Shanghai Municipality under Grant No. 22JC1401401. The work of Y. Leng was supported by the National Science Foundation, Division of Information and Intelligent Systems under Grant No. IIS 2153468. The work of G. Shi was supported by the Australian Research Council under Grants No. DP190103615, LP210200473, and DP230101014. (Corresponding Author: X. Ren (xqren@shu.edu.cn))

I. Introduction

In recent years, game theory has been introduced to the operation of large-scale complex network systems in emerging applications including wireless communications [3], [35], smart grids [4], [36], and electric vehicle charging [5]. In such systems, each agent (representing a user/customer/unit) makes an individual decision, and experiences a payoff which often depends only on the decisions of a few neighboring agents in large-scale networks. The inter-dependency of agents' payoffs is restricted to local views due to physical constraints. As a result, the agents are naturally organized in a game associated with a network structure, i.e., a network game [6], [7]. The notions of Nash equilibrium or the generalized one become sensible resolutions for the network operation where agents are rational players aiming at maximizing individual payoffs. The graph describing the underlying network structure becomes critical for the existence and positioning of the Nash equilibrium [7].

Linear quadratic games are a class of network games where the payoff of each player is a simple quadratic function. The dependencies among the player decisions in the quadratic function induce a network structure, determining the players' inter-personal influences. Despite its simplicity, the linear quadratic game has been a fundamental model for network games [8], [9], [42]. The Nash equilibrium of linear quadratic game can be explicitly linked to the underlying network structure, which facilitates new centrality measures [8]; linear quadratic games has been applied to characterize the user behaviors for online e-commerce platforms [9] and industrial collaboration [42].

The scalability and robustness requirements for large-scale networks have sparkled the need to develop distributed algorithms for Nash equilibrium computing. In a distributed Nash equilibrium computing algorithm, players share a sequence of decisions over the communication links of the network. Despite the payoff function for each player being private information, the decisions shared with other agents inevitably carry information about the payoff functions and the underlying influence network structure. Parameters of the individual payoff functions may consist of sensitive private information about users' preferences and economic status; the network structure further captures the inter-personal peer influence among the users over the platform, which may be sensitive trade secrets. Therefore, privacy concerns related to key user parameters and/or network structure in distributed Nash equilibrium seeking cannot be overlooked. Particularly, for linear quadratic network games, both the marginal payoffs and the influence network structure can be sensitive private information, which

may be subject to unintended leakages during distributed Nash equilibrium computing processes by eavesdroppers having access to communication messages and attempting to infer the sensitive information.

A. Related Work

For games over networks with convex payoff functions, there has been a growing line of research in the distributed computation of Nash equilibrium. For cognitive radio network games, a joint and distributed computing framework was proposed in [10] by embedding best response maps to the local states update. In [11], a simple projection-free primal-dual algorithm was proposed for incomplete information games in order to compute an approximate Nash equilibrium. In addition, in [12], [13], [31] the Nash equilibrium seeking problem was transformed into a distributed optimization problem, for which distributed gradient-descent algorithms were employed to develop both synchronous and asynchronous computation algorithms with almost-sure convergence to the Nash equilibrium. Along this line of study, several important game-theoretic models have been investigated such as quadratic games [29], aggregative games [30], [33], network games [32], [34], etc. The considered distributed Nash equilibrium seeking problem is also related to the multi-agent learning problem of continuous games where actions are taken from continuous space and each agent adopts a common policy. For such a problem, online learning algorithms have been developed with guarantees of convergence to the Nash equilibrium with feedback delays [14], lossy feedback [15] and bandit feedback [16], [17]. We note that our proposed algorithms are also established on the gradient-descent scheme, but with the aim to compute *the whole network Nash equilibrium* at each agent, which is different from these relevant results where each agent *computes its own action* at a Nash equilibrium, i.e., the corresponding entry of the network Nash equilibrium, in addition to the extra privacy requirements.

The privacy we consider is closely related to the concept of differential privacy [1]. It was originally proposed for databases of individual records subject to public queries and has been extended to different areas thereafter. Of more relevance to our paper are the works in [18]–[21] focusing on distributed differentially private optimization. Within these papers, the objective functions, the optimization constraints, and the agents states are treated as private information, respectively. The underlying commonality is the algorithm design approach based on the idea of message perturbation. To protect the differential privacy of sensitive objective functions, the authors in [19], [21] proposed to perturb the communication messages in the distributed optimization problem to address the privacy concerns for objective functions. To further improve the trade-off between the achievable privacy and accuracy, [40] develops an optimized noise injection strategy to minimize the perturbation impact and [41] proposes to employ a decaying stepsize while iteratively injecting noises to communication messages with an appropriately designed increasing variance. Of particular relevance is the work of [30], where the authors proposed a differentially private distributed Nash equilibrium seeking scheme by injecting Laplacian noise in node-to-node communications for aggregative games.

B. Contributions

We consider privacy-preserving distributed Nash equilibrium seeking algorithms for linear quadratic network games.

System and Problem Definition: The payoff function of each player is a quadratic function with a separate term representing its individual marginal benefit and cross terms capturing the inter-personal influences among players. Both can be regarded as sensitive information needed to be protected. To compute the Nash equilibrium in a distributed manner, players usually need to broadcast their local information to their neighbors through a communication graph, whereas the sensitive information would be inferred from neighboring communications. To address this, we follow the idea of injecting perturbations to tailor the distributed computation algorithm with differential privacy guarantees and establish the trade-off between the privacy level and computation accuracy.

Algorithms: The agents hold dynamical states which are updated with gradient descents and local averaging over the communication graph. We explore three different mechanisms for privacy protection in the computing process, leading to three algorithms for computing the Nash equilibrium under differential privacy.

In the case of preserving the marginal payoff privacy, a distributed randomized gradient descent algorithm is proposed where each agent computes the local gradient with the perturbed marginal payoff by a Laplacian random noise, and then updates the local state by averaging across its neighboring information. In the case of preserving marginal payoff/social-influence privacy, a distributed randomized communication algorithm is given utilizing noise injection in node-to-node communications, and a distributed randomized projection algorithm is constructed by taking perturbed marginal payoff and social influence into embedded local projections.

Privacy vs Accuracy: When the influence network structure is considered to be public knowledge, the distributed randomized gradient descent algorithm achieves ϵ-differential marginal payoff privacy regardless of the length of the computation time, and converges in expectation to the Nash equilibrium of the network game at each player's state. When both players' marginal payoffs and the influence graph are considered to be private, the distributed randomized communication algorithm is shown to achieve differential privacy with a horizon-specific privacy budget, and the distributed randomized projection algorithm is proven to be able to achieve differential privacy under a privacy budget independent with the horizon. For all algorithms, explicit bounds on the mean-square errors of the computation process are established in the asymptotic sense, revealing a clear trade-off between the privacy level and computation accuracy.

Our distributed randomized Nash equilibrium algorithm is along the same line of privacy protection ideas developed in [19], [21], [30] for distributed optimization and aggregative games. The key innovations of our framework lie in strategic privacy protections for marginal payoffs and network structure both separately and collectively, random noise injection inspired by inherent geometries in best responses, and clear structure-specific trade-off between privacy and accuracy.

C. Paper Outline

The system setup and problem statement are presented in Section II. Tow different cases where the marginal payoff function or both marginal payoff and the influence graphs are regarded as private information, are considered in Section III and Section IV, respectively. All the proofs of statements are presented in Section V, and finally a few concluding remarks are given in Section VI.

Notation: We denote by $\mathbb{R}$ the real numbers, $\mathbb{R}^n$ and $\mathbb{R}^n_+$ the real and positively real space of n dimension for any positive integer n and $\mathbb{N}_+$ the set of positive integers. For any $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$, we denote $[\mathbf{x}_1; \ldots; \mathbf{x}_m]$ as a vector $\begin{bmatrix}\mathbf{x}_1^\top & \ldots & \mathbf{x}_m^\top\end{bmatrix}^\top \in \mathbb{R}^{mn}$, and $[\mathbf{x}_1, \ldots, \mathbf{x}_m]$ as a matrix of which the i-the column is $\mathbf{x}_i$, $i = 1, \ldots, m$. For any $\mathbf{x} = [x_1; \ldots; x_n] \in \mathbb{R}^n$, we denote $\|\mathbf{x}\| = (\mathbf{x}^\top \mathbf{x})^{\frac{1}{2}}$ and $\|\mathbf{x}\|_1 = \sum_{i=1}^n |x_i|$. The maximum and minimum singular values of a matrix $\mathbf{A}$ are denoted as $\sigma_M(\mathbf{A})$ and $\sigma_m(\mathbf{A})$, respectively. For a matrix $\mathbf{A} \in \mathbb{R}^{n\times m}$, we denote $\|\mathbf{A}\| = \sigma_M(\mathbf{A})$, $\mathrm{vec}(\mathbf{A}) = [\mathbf{A}_1; \ldots; \mathbf{A}_m]$ with $\mathbf{A}_i$ being the i-th column of $\mathbf{A}$. A matrix is said to be non-negative if all its elements are equal to or greater than zero. The range of a mapping is denoted as range$(\cdot)$. For any $X \subseteq \mathbb{R}^n$, we denote $1_X(\mathbf{x})$ as a characteristic function, satisfying $1_X(\mathbf{x}) = 1$ for $\mathbf{x} \in X$ and $1_X(\mathbf{x}) = 0$ for $\mathbf{x} \notin X$.

II. Problem Formulation

In this section, we present our system setup on linear quadratic network games, and define our problem of interest.

A. Quadratic Network Games

Consider a game with n players indexed in the set $\mathrm{V} = \{1, \ldots, \mathrm{n}\}$, where each player holds a decision (action) $a_i \in \mathbb{R}_{\geq 0}$. In a linear quadratic game [8], the payoff of player i is represented by

$$u_i = b_i a_i - \frac{1}{2} a_i^2 + \sum_{j \in \mathrm{V}/\{i\}} g_{ij} a_i a_j. \tag{1}$$

Here $b_i \in \mathbb{R}_{\geq 0}$, termed the marginal benefit of player i, indicates the contribution of player i's own decision in i's decision. Therefore, b_i characterizes the level of selfishness of player i. Moreover, $g_{ij} \in \mathbb{R}$ represents the particular peer influence from player j towards player i for $i, j \in \mathrm{V}$. It is noted that these data of marginal benefits and peer influences may be privacy-sensitive and need to be protected.

Let $g_{ii} = 0$ and the matrix $\mathbf{G}$ be given by $[\mathbf{G}]_{ij} = g_{ij}$ for all $i, j \in \mathrm{V}$. We term the matrix $\mathbf{G}$ the social influence matrix of the game. Then there is an induced graph from $\mathbf{G}$, denoted by $\mathrm{G} = (\mathrm{V}, \mathrm{E})$, where a directed arc $(j, i) \in \mathrm{E}$ if and only if $g_{ij} \neq 0$. The graph G is termed to be the influence graph associated with the game. Let $\mathbf{a} = [a_1; \ldots; a_n]$ and $\mathbf{b} = [b_1; \ldots; b_n]$, and let $\mathbf{a}_{-i}$ represent the action profile of $\mathbf{a}$ excluding a_i. Now under $\mathbf{a}_{-i}$, the best possible action, termed the best response, from player i that maximizes u_i is

$$\mathrm{B}_i(\mathbf{a}_{-i}) = \max\big\{b_i + \sum_{j \in \mathrm{V}} g_{ij} a_j, 0\big\}. \tag{2}$$

Let $(\mathbf{I} - \mathbf{G})^{-1}$ be well defined and nonnegative, rendering the linear quadratic game to have a unique Nash equilibrium satisfying [8]

$$(\mathbf{I} - \mathbf{G})\mathbf{a}^* = \mathbf{b}\,. \tag{3}$$

B. Distributed Nash Equilibrium Computing with Differential Privacy

A natural idea to compute the Nash equilibrium $\mathbf{a}^*$ is to directly solve the linear algebraic equation (3) in a centralized manner given a center having the whole network of data $\{\mathbf{G}, \mathbf{b}\}$. However, given the distributed nature and privacy concern of these data, such a centralized approach is less desired than a distributed and privacy-preservation approach.

Distributed computation of Nash equilibrium is equivalent to the problem where players cooperatively compute a Nash equilibrium without sharing the payoff functions with each other. We suppose there is an undirected and connected communication graph, denoted $\mathrm{G}_{\mathrm{com}} = (\mathrm{V}, \mathrm{E}_{\mathrm{com}})$, over which each player i holds a dynamical state $\mathbf{x}_i(t)$ in discrete time, broadcasts messages $\mathbf{y}_i(t)$ (which may or may not be equal to $\mathbf{x}_i(t)$) to its neighbors in $\mathrm{N}^i_{\mathrm{com}} := \big\{j : \{i, j\} \in \mathrm{E}_{\mathrm{com}}\big\}$, updates $\mathbf{x}_i(t)$ based on its received messages and local payoff function. For simplicity it is assumed that each communication edge in $\mathrm{E}_{\mathrm{com}}$ has the same weight w satisfying $0 < w \leq \frac{1}{1+\max_{i\in\mathrm{V}} |\mathrm{N}^i_{\mathrm{com}}|}$ and the structure of this communication graph is publicly known.

The objective is to develop distributed Nash equilibrium computing algorithms for the linear-quadratic game (1) with differential privacy with respect to two types of private data $\mathcal{D}$: (i) $\mathcal{D} = \mathbf{b}$ for marginal payoff privacy, and (ii) $\mathcal{D} = (\mathbf{b}, \mathbf{G})$ for complete marginal-payoff/social-influence privacy. In either case, we consider the scenario that the eavesdroppers have access to all communication messages $\mathbf{y}_i(t)$ for $i \in \mathrm{V}$ and $t \in [0, T]$ over the communication graph $\mathrm{G}_{\mathrm{com}}$ and aim to infer the sensitive data $\mathcal{D}$. Denoting $\mathbf{y}_t = (\mathbf{y}_1(t), \ldots, \mathbf{y}_n(t))^\top$, we use $\mathcal{M}$ to represent the random mapping from $\mathcal{D}$ to $\big(\mathbf{y}_t\big)_{t=0}^T$. Let $\mathbb{D}$ be the space of the private data $\mathcal{D}$, any pair $\mathcal{D}, \mathcal{D}' \in \mathbb{D}$ is termed μ-adjacent if $\|\mathrm{vec}(\mathcal{D} - \mathcal{D}')\|_1 \leq \mu$ [1]. We present the following definitions [1], [27], [28].

Definition 1. *(i) Let $\mathcal{D} = \mathbf{b}$. A distributed Nash equilibrium computation algorithm for the linear quadratic network game achieves differential marginal payoff privacy with privacy budget $\epsilon > 0$ under adjacency of $\mu > 0$ if for all $R \subseteq$ range$(\mathcal{M})$, there holds for any μ-adjacent $\mathcal{D}, \mathcal{D}'$ that*

$$\mathbb{P}\big(\mathcal{M}(\mathcal{D}) \in R\big) \leq e^\epsilon \mathbb{P}\big(\mathcal{M}(\mathcal{D}') \in R\big). \tag{4}$$

(ii) Let $\mathcal{D} = (\mathbf{b}, \mathbf{G})$. A distributed Nash equilibrium computation algorithm for the linear quadratic network game achieves differential marginal-payoff/social-influence privacy with privacy budget $\epsilon > 0$ under adjacency of $\mu > 0$ if for all $R \subseteq$ range$(\mathcal{M})$, (4) holds for any μ-adjacent $\mathcal{D}, \mathcal{D}'$.

The Nash equilibrium computation problem of the game (1) can be transformed into solving the network linear equation (3), or equivalently the following distributed optimization problem

$$\mathbf{a}^* := \mathrm{argmin}_{\mathbf{x}\in\mathbb{R}^n} \sum_{i\in\mathrm{V}} f_i(\mathbf{x})$$

where each agent holds a private cost function $f_i(\mathbf{x}) := |(\mathbf{e}_i - \mathbf{G}_i)^\top \mathbf{x} - b_i|^2$, with $\mathbf{G}_i$ the i-th column of $\mathbf{G}^\top$ and $\mathbf{e}_i \in \mathbb{R}^n$

[1]The notation vec denotes the vectorization operation, i.e., to stack all the elements into a vector.

a unit vector whose entries are all zero except the i-th being one. In the absence of privacy concern, by [22], [23] the Nash equilibrium seeking algorithm is given by

$$\mathbf{x}_i(t+1) = \mathbf{x}_i(t) - w \sum_{j\in \mathrm{N}^i_{\mathrm{com}}} [\mathbf{x}_i(t) - \mathbf{x}_j(t)] - s\mathbf{h}_i \left[\mathbf{h}_i^\top \mathbf{x}_i(t) - b_i\right] \tag{5}$$

with stepsize $s > 0$ and $\mathbf{h}_i := \mathbf{e}_i - \mathbf{G}_i$. In the following, the above distributed gradient descent algorithm (5) will be further explored to solve the differentially private Nash equilibrium computation problem in question. This thus demonstrates the difference of the proposed algorithms from other existing algorithms [30], [38], in the sense that the proposed algorithms allow each agent to compute the network Nash equilibrium $\mathbf{a}^*$ in a differentially private manner while each agent computes the local action at the Nash equilibrium in [30], [38].

Remark 1. *It is noted that the edge weight of the communication graph* $\mathrm{G}_{\mathrm{com}}$ *is assumed to be identical for computational simplicity, while the forthcoming results can be easily extended to other cases with non-identical edge weights with some additional computational complexities, once the resulting Laplacian matrix is doubly stochastic [22], [23]. On the other hand, it is also worth noting that the communication network* $\mathrm{G}_{\mathrm{com}}$ *is different from the influence network* G *whose edges are private for protection while there is no privacy requirement to the former* $\mathrm{G}_{\mathrm{com}}$.

C. Model Rationale

The class of linear quadratic games has been one of the basic models for network games [8], with applications in smart energy market [4] and social network formations in e-commerce [9]. Readers of interest can be referred to [42, Section 4] for its more explicit applications, such as crime activity, education outcomes, industrial cooperation, etc.

Our problem setup is consistent with [9] in the sense that in both works, the payoff functions of individual players are considered to be private. In [9], the agents are assumed to be playing their actions at Nash equilibriums, and the problem under investigation there is how one may recover the marginal payoffs and network structure from the observed equilibriums (in multiple independent games). Here our problem is essentially the inverse problem: agents reveal information about their payoff functions in recursive computations, with the aim to compute the network-level Nash equilibriums.

Moreover, the Nash equilibrium seeking problem of average aggregative games was studied in [30] under differential privacy and in [38] under a qualitative or binary privacy notion. Average aggregative game is a class of network games where individual agent payoff depends on agents' own actions and the average actions across the network. Therefore, linear quadratic games are not a subclass of aggregative games. The fundamental new feature in linear quadratic games arises from the clear agent interaction relations defined in the matrix $\mathbf{G}$, which has real-world implications in interpersonal influences [9]. In addition, in [30], the gradients of the payoff functions are required to be globally bounded, which, however, is not satisfied in the linear quadratic network games having unbounded gradients of the payoff functions.

III. Marginal Payoff Privacy

In this section, we consider the case where only the marginal benefit $\mathbf{b}$ is considered to be private data. In this case, we have $\mathcal{D} = \mathbf{b}$ and $\mathbb{D} = \mathbb{R}^n$, and our aim is to develop a distributed Nash equilibrium computation algorithm for the linear quadratic network game that achieves provable differential marginal-payoff privacy.

A. The Algorithm

We propose the following distributed privacy-preserving Nash equilibrium computation algorithm over the communication graph $\mathrm{G}_{\mathrm{com}}$. Note that each player (node) i has access to $b_i, \mathbf{h}_i$ from its payoff function.

Algorithm 1 Privacy-Preserving Distributed Randomized Gradient Descent Algorithm

Input: Local parameters $b_i, \mathbf{h}_i$, $i \in \mathrm{V}$, stepsize s, iteration steps T, and variance $2\sigma_\gamma^2$.
Initialize: Node i generates an i.i.d. Laplacian noise $\gamma_i \backsim \mathcal{L}(0, 2\sigma_\gamma^2)$, and chooses any $\mathbf{x}_i(0) \in \mathbb{R}^n$.
Output: $\mathbf{x}_i(T)$ at each node $i \in \mathrm{V}$.
For $t = 0, 1, \ldots, T-1$, **run**
1: Each node i sends $\mathbf{y}_i(t) = \mathbf{x}_i(t)$ to its neighbors in the set $\mathrm{N}^i_{\mathrm{com}}$ over $\mathrm{G}_{\mathrm{com}}$.
2: Each node i updates its node state according to

$$\mathbf{x}_i(t+1) = \mathbf{y}_i(t) - w \sum_{j\in \mathrm{N}^i_{\mathrm{com}}} [\mathbf{y}_i(t) - \mathbf{y}_j(t)] - s\mathbf{h}_i \left[\mathbf{h}_i^\top \mathbf{y}_i(t) - (b_i + \gamma_i)\right]. \tag{6}$$

Algorithm 1 is established on the distributed gradient descent algorithm (5) by perturbing the local marginal payoff b_i with random noise γ_i, $i \in \mathrm{V}$. By doing so, it follows that the differential privacy of b_i can be implied when releasing the resulting noisy marginal payoff. Thus the differential privacy of the marginal payoffs is still preserved when using the resulting noisy marginal payoffs in the Nash equilibrium computing process due to the resilience property of the differential privacy to post-processing [1].

B. Main Results

First of all, we establish the following result, which shows Algorithm 1 can indeed preserve the privacy of the marginal payoffs of the players against eavesdroppers having access to all node-to-node communications over the communication graph $\mathrm{G}_{\mathrm{com}}$.

Theorem 1. *Let* $\sigma_\gamma \geq \mu/\epsilon$. *Then the Algorithm 1 preserves the differential marginal-payoff privacy with a privacy budget* ϵ *for any finite time horizon* T.

The proof of Theorem 1 lies in expressing the mapping/mechanism from the sensitive data to the eavesdropped communication messages as a composition of a deterministic mapping and a randomized mapping. Then by designing the noise level σ_γ such that the latter preserves ϵ-differential privacy, the composed mechanism still preserves the ϵ-differential privacy by recalling that the differential privacy is resilient to post-processing [1].

Next, we show that with suitable step size, the node states in Algorithm 1 indeed converge to the Nash equilibrium $\mathbf{a}^*$ in expectation with an asymptotically bounded mean-square error. To this end, we introduce $d_i = w|\mathrm{N}^i_{\mathrm{com}}|$ and then $\mathbf{D} = \mathrm{diag}(d_1, \ldots, d_n)$. Denote $\mathbf{W} \in \mathbb{R}^{n\times n}$ where $[\mathbf{W}]_{ij} = w_{ij}$ with $w_{ij} = w$ if $(i,j) \in \mathrm{E}_{\mathrm{com}}$ and $w_{ij} = 0$ if $(i,j) \notin \mathrm{E}_{\mathrm{com}}$. Then $\mathbf{L} = \mathbf{D} - \mathbf{W}$ is the Laplacian of the communication graph $\mathrm{G}_{\mathrm{com}}$. We arrange the eigenvalues of $\mathbf{L}$ in the increasing order as $\lambda_1 < \lambda_2 \ldots \leq \lambda_n$. Then there hold $\lambda_1 = 0$ and $|\lambda_i| < 2$ for all $i = 1, \ldots .n$ [24]. Denote the following useful parameters

$$\begin{aligned} &\rho_m = \sigma_m\left(\textstyle\sum_{i=1}^n \mathbf{h}_i\mathbf{h}_i^\top/n\right),\\ &h_M = \max\{\|\mathbf{h}_1\|, \ldots, \|\mathbf{h}_n\|\},\\ &\alpha_1 = \frac{\lambda_n + 2sh_M^2 + \sqrt{\lambda_n^2 + 4s^2h_M^4}}{2} - 1,\\ &\alpha_2 = \frac{\sqrt{(\lambda_2 - s\rho_m)^2 + 4s^2h_M^4} - \lambda_2 - s\rho_m}{2} + 1,\\ &\alpha = \max\{|\alpha_1|, |\alpha_2|\}. \end{aligned} \tag{7}$$

Theorem 2. *Suppose the step size s is chosen in the way that*

$$0 < s < \min\left\{\tfrac{2(2-\lambda_n)}{h_M^2(4-\lambda_n)}, \tfrac{\rho_m\lambda_2}{h_M^4}\right\}$$

Then there hold for Algorithm 1 that

(i) $\lim_{t\to\infty} \mathbb{E}\mathbf{x}_i(t) = \mathbf{a}^*$*;*

(ii) $\lim_{t\to\infty} \mathbb{E}\|\mathbf{x}_i(t) - \mathbf{a}^*\|^2 \leq 2ns^2\sigma_\gamma^2 h_M^2/(1-\alpha)^2$ *with* $0 < \alpha < 1$.

The results in Theorems 1 and 2 clearly demonstrate a trade-off between the achievable privacy and accuracy. A higher differential privacy requirement (i.e., a smaller ϵ) relies on a greater injected noise variance by Theorem 1, which in turn leads to a higher computation error in the mean-square sense by Theorem 2.

C. Numerical Example

We consider three well-studied random graph models, including the Erdős-Rényi random graph, scale-free graph, and community graph for the social influence graph G. These random graphs have been widely adopted for characterizing complex networks in the real world. In our simulation, we made use of the GSP toolbox [2][2] to generate these three social influence graphs. We run the simulations in Matlab 2019b, and the code used for the numerical experiments is provided in the supplementary materials.

For the simulation setup of the game, we generate the three random graphs (each is regarded as the social influence graph G and associated with a single game) with $n = 30$ players. In particular, the edge probability of the Erdős-Rényi random graph is set as 0.5; the scale-free graph is generated from a preferential attachment dynamic where each new node establishes one edge with the existing graph, and the community graph is generated containing 5 communities based on stochastic block model. The communication graph $\mathrm{G}_{\mathrm{com}}$ is set to be fixed obtained from a sample of an Erdős-Rényi graph. For the simulation setup of Algorithm 1, we randomly generate the local parameter b_i following the uniform distribution over the interval $[0, 1]$. The stepsize s, the initial value $\mathbf{x}_0$ and iteration steps T are set as 0.3, all-zero vectors, and 16000, respectively. For each graph, the weight matrix $\mathbf{G}$ is constructed with elements $g_{ij} = \frac{1}{1+\max_{i\in\mathrm{V}}|\mathrm{N}^i|}$, where $|\mathrm{N}^i|$ is the degree of the set of player i's neighbors. Similarly, we set $w = \frac{1}{1+\max_{i\in\mathrm{V}}|\mathrm{N}^i_{\mathrm{com}}|}$.

We run Algorithm 1 over these three graphs in order to evaluate the effect of the differential privacy mechanisms. Throughout the simulations over each graph, the empirical results are based on averaging across 10000 sample trajectories. Moreover, following the standard differential privacy guideline, we set the privacy requirement as $\frac{\mu}{\epsilon} = \sigma_\gamma \in \{0.1, 0.01, 0.001\}$. The condition in Theorem 2 always holds for all simulations over the three graphs with parameters as follows: for Erdős-Rényi graph, $h_M = 1.048$, $\rho_m = 0.003$; for scale-free graph, $h_M = 1.027$, $\rho_m = 0.015$; for community graph, $h_M = 1.044$, $\rho_m = 0.002$; for communication graph, $\lambda_n = 1.245$, $\lambda_2 = 0.085$. To validate Theorem 2, we calculate the result, i.e., the averaged error variance $\mathbb{E}||\mathbf{x}_i(t) - \mathbf{a}^*||^2$. The simulation results are presented in Figure 1, which demonstrates the relationship between the resulting computation accuracy and the algorithm step t under different privacy requirements. Among all sub-figures, it is obvious that as the iteration t increases, the resulting computation accuracy decreases until a lower bound. Moreover, by comparing sub-figures in Figure 1, we can obtain the trade-off between the accuracy and the privacy requirement, as the computed solution $x_i(t)$ is more accurate with respect to a lower-level privacy requirement.

IV. Marginal-Payoff and Social-Influence Privacy

In this subsection, we study the case where both the marginal payoff and the influence network are considered to be private information. In this case, we have the private data $\mathcal{D} = (\mathbf{b}, \mathbf{G})$, and impose the following assumption on its space $\mathbb{D}$.

Assumption 1. *There holds $\mathbb{D} = \mathbb{B} \times \mathbb{G}$ with $\mathbb{B} = \{\mathbf{b} \in \mathbb{R}^n : 0 \leq b_i \leq \ell_b, i \in \mathrm{V}\}$ and $\mathbb{G} = \{\mathbf{G} \in \mathbb{R}^{n\times n} : |g_{ij}| \leq \ell_g, g_{ii} = 0, i, j \in \mathrm{V}\}$ for $\ell_b > 0$ and $\ell_g > 0$.*

A. Randomized Communication for Horizon-Specific Privacy

Before presenting the algorithm, we make the following assumption on the Nash equilibrium.

Assumption 2. *There exists a convex compact set $\mathbb{A} \subset \mathbb{R}^n$ known to all players such that $\mathbf{a}^* \in \mathbb{A}$.*

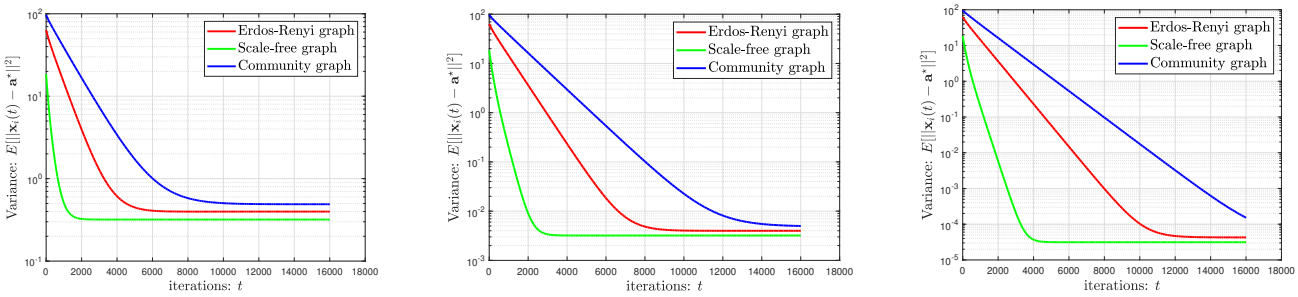
Let $\ell_{\mathbb{A}} = \max_{\mathbf{y}\in\mathbb{A}}\|\mathbf{y}\|$ and $\mathscr{P}_{\mathbb{A}}(\mathbf{y})$ be the projection of $\mathbf{y} \in \mathbb{R}^n$ on the set $\mathbb{A}$, i.e., $\mathscr{P}_{\mathbb{A}}(\mathbf{y}) := \arg\min_{\mathbf{y}'\in\mathbb{A}}\|\mathbf{y} - \mathbf{y}'\|$. We propose the distributed privacy-preserving Nash equilibrium computation algorithm in Algorithm 2.

Algorithm 2 is established on the distributed gradient descent algorithm (5), but is different from Algorithm 1. Algorithm 2 injects random noises to communication messages, yielding noisy messages for adversaries in order to preserve the differential marginal-payoff/social-influence privacy. However, as explicitly shown later, we note that the required noise level σ_γ in Algorithm 2 depends on the length of T, which is a significant difference compared to Algorithm 1.

Theorem 3. *Suppose Assumptions 1-2 hold. Let $\sigma_\nu \geq sT\mu(2\ell_{\mathbb{A}}(1+\ell_g) + \max\{1+\ell_g, \ell_b\})/\epsilon$. Then Algorithm*

[2]https://epfl-lts2.github.io/gspbox-html/, released under the GNU General Public License (GPLv3).

This article has been accepted for publication in IEEE Transactions on Control of Network Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2024.3398729



(a) Error variance under $\epsilon = 10$. (b) Error variance under $\epsilon = 100$. (c) Error variance under $\epsilon = 1000$.

Figure 1: Accuracy performance of Algorithm 1 under three differential privacy budgets.

Algorithm 2 Privacy-preserving Distributed Randomized Communication Algorithm

Input: Local parameters $b_i, \mathbf{h}_i$, $i \in \mathrm{V}$, stepsize s, iteration steps T and variance $2\sigma_\nu^2$.
Initialize: Node i selects any $\mathbf{x}_i(0) \in \mathbb{R}^n$.
Output: $\mathbf{x}_i(T)$ at each node $i \in \mathrm{V}$.
For $t = 0, 1, \ldots, T-1$, **run**

1: Each node i generates an i.i.d. Laplacian noise $\boldsymbol{\nu}_i(t) \backsim \mathcal{L}(0, 2\sigma_\nu^2\, 1_{\mathbb{N}_+}(t))^n$.

2: Each node i sends $\mathbf{y}_i(t) = \mathbf{x}_i(t) + \boldsymbol{\nu}_i(t)$ to its neighbors in the set $\mathrm{N}_{\mathrm{com}}^i$ over $\mathrm{G}_{\mathrm{com}}$.

3: Each node i updates its node state according to

$$\mathbf{x}_i(t+1) = \mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t)) - w \sum_{j \in \mathrm{N}_{\mathrm{com}}^i} \big(\mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t)) - \mathscr{P}_{\mathbb{A}}(\mathbf{y}_j(t))\big) - s\mathbf{h}_i\big(\mathbf{h}_i^\top \mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t)) - b_i\big). \quad (8)$$

2 achieves the differential marginal-payoff/social-influence privacy with a privacy budget ϵ.

The proof of Theorem 3 is established by elaborating the mapping/mechanism from the sensitive data to the eavesdropped communication messages and then deriving the required noise level σ_ν to achieve ϵ-differential privacy following the Definition 1.(ii). Further, we can also prove that each node state $\mathbf{x}_i(T)$ at the output of Algorithm 2 is within a neighborhood of the Nash equilibrium $\mathbf{a}^*$ in the mean-square error sense. The distance between $\mathbf{x}_i(T)$ and $\mathbf{a}^*$ is controlled by the magnitude of the variance σ_ν.

Theorem 4. *Suppose Assumption 1 holds. Let the step-size s satisfy*

$$0 < s < \min\left\{\frac{2(2-\lambda_n)}{h_M^2(4-\lambda_n)}, \frac{\rho_m \lambda_2}{h_M^4}\right\}$$

Then there holds along Algorithm 2 that

$$\mathbb{E}\|\mathbf{x}_i(T) - \mathbf{a}^*\|^2 \leq \frac{2n\alpha^2}{1-\alpha^2}\sigma_\nu^2 + \mathcal{O}(e^{-\gamma T})$$

where $\gamma = -2\ln|\alpha| > 0$.

B. Randomized Projection for Any-time Privacy

Let $\mathbf{l}_{ij} \in \mathbb{R}^n$, $j \in \mathrm{V}$ be linearly independent vectors such that $\mathbf{l}_{ii} = \mathbf{h}_i/\|\mathbf{h}_i\|$ and $\mathbf{h}_j^\top \mathbf{l}_{ij} = 0$ for $j \neq i$, for $i \in \mathrm{V}$. For any $\mathbf{x} \in \mathbb{R}^{n(n+1)/2}$, we denote by $\mathscr{H}(\mathbf{x})$ the mapping from vector $\mathbf{x}$ to a symmetric matrix with j-th entry of the i-th row being the $i + \frac{j(j-1)}{2}$-th entry of $\mathbf{x}$. It is noted that $\mathscr{H}(\cdot)$ is invertible, whose inverse is denoted by $\mathscr{H}^{-1}(\cdot)$. For $i \in \mathrm{V}$, we let $\bar{q}_i > \|\mathbf{h}_i\|^2 > \underline{q}_i > 0$, and introduce the following convex set

$$\mathcal{C}_i = \left\{\mathbf{x} \in \mathbb{R}^{n(n+1)/2} : \sum_{j \in \mathrm{V}} x_{\frac{j(j+1)}{2}} \in [\underline{q}_i, \bar{q}_i], \ \mathscr{H}(\mathbf{x})\mathbf{l}_{ij} = 0, \forall j \in \mathrm{V}/\{i\}\right\}. \quad (9)$$

It is clear that $\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top) \in \mathcal{C}_i$. Let $\mathscr{P}_{\mathcal{C}_i}(\mathbf{y})$ be the projection of $\mathbf{y} \in \mathbb{R}^{n(n+1)/2}$ on the set $\mathcal{C}_i$, i.e., $\mathscr{P}_{\mathcal{C}_i}(\mathbf{y}) := \arg\min_{\mathbf{y}' \in \mathcal{C}_i} \|\mathbf{y} - \mathbf{y}'\|$.

We are now ready to introduce another distributed privacy-preserving Nash equilibrium computation algorithm.

Algorithm 3 Privacy-preserving Distributed Randomized Projection Algorithm

Input: Local parameters $b_i, \mathbf{h}_i$, $i \in \mathrm{V}$, stepsize s, iteration steps T and variance $2\sigma^2$.
Initialize: Node i generates i.i.d. Laplacian noises $\boldsymbol{\omega}_i \backsim \mathcal{L}(0, \sigma^2)^n$ and $\boldsymbol{\eta}_i \backsim \mathcal{L}(0, 2\sigma^2)^{\frac{n(n+1)}{2}}$, and selects any $\mathbf{x}_i(0) \in \mathbb{R}^n$.
Output: $\mathbf{x}_i(T)$ at each node $i \in \mathrm{V}$.
For $t = 0, 1, \ldots, T-1$, **run**

1: Each node i sends $\mathbf{y}_i(t) = \mathbf{x}_i(t)$ to its neighbors in the set $\mathrm{N}_{\mathrm{com}}^i$ over $\mathrm{G}_{\mathrm{com}}$.

2: Each node i updates its node state according to

$$\mathbf{x}_i(t+1) = \mathbf{y}_i(t) - \sum_{j \in \mathrm{V}} w\big(\mathbf{y}_i(t) - \mathbf{y}_j(t)\big) - s\mathscr{H} \circ \mathscr{P}_{\mathcal{C}_i}\big(\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top) + \boldsymbol{\eta}_i\big)\mathbf{y}_i(t) + s(\mathbf{h}_i b_i + \boldsymbol{\omega}_i). \quad (10)$$

Algorithm 3, inspired by Algorithm 1, employs the idea of injecting random noises to the private parameters $\mathbf{h}_i\mathbf{h}_i^\top, \mathbf{h}_i b_i$ for producing noisy parameters, which achieves the differential privacy of the data $\mathcal{D} = (\mathbf{b}, \mathbf{G})$. In this way, the differential privacy of $\mathcal{D} = (\mathbf{b}, \mathbf{G})$ is still preserved when using such noisy parameters in the computation of Nash equilibrium, due to

the robustness property of the differential privacy [1]. As a result, it follows that the differential privacy of $\mathcal{D} = (\mathbf{b}, \mathbf{G})$ is independent of the time horizon T. In addition, we also introduce a projection in (10) onto a local compact set $\mathcal{C}_i$ to ensure stability. The following result shows that a fixed level of noise injection is enough to guarantee differential privacy for any finite horizon, in contrast with Theorem 3 for Algorithm 2 by perturbing messages.

Theorem 5. *Assume Assumption 1 hold. Let $\sigma \geq \mu\big(2(1+\ell_g) + \max\{1+\ell_g, \ell_b\}\big)/\epsilon$. Then the Algorithm 3 preserves the differential marginal-payoff/social-influence privacy with a privacy budget ϵ for any finite time horizon T.*

The proof of Theorem 5 is similar to that of Theorem 1, relying on the resilience property of differential property to post-processing. Before proceeding to analyze the computation accuracy of Algorithm 3, it is important to study the properties of the following stochastic matrix

$$\mathbf{K}_{\boldsymbol{\eta}_i} := \mathscr{H} \circ \mathscr{P}_{\mathcal{C}_i}\big(\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top) + \boldsymbol{\eta}_i\big)\,, \quad i \in \mathrm{V}\,.$$

Lemma 1. *Let $\bar{\rho}_m = \min\{\frac{q_1}{\|\mathbf{h}_1\|^2}, \ldots, \frac{q_n}{\|\mathbf{h}_n\|^2}\}\rho_m$, $\bar{h}_M = \max\{\sqrt{q_1}, \ldots, \sqrt{q_n}\}$. Then there hold*

$$\begin{array}{l} \sum_{i=1}^n \mathbf{K}_{\boldsymbol{\eta}_i}/n \geq \bar{\rho}_m \mathbf{I}_n \\ \max\{\|\mathbf{K}_{\boldsymbol{\eta}_1}\|, \ldots, \|\mathbf{K}_{\boldsymbol{\eta}_n}\|\} \leq |\bar{h}_M|^2. \end{array} \tag{11}$$

With suitable step size, the node states in Algorithm 3 indeed converge to the Nash equilibrium $\mathbf{a}^*$ in expectation with an asymptotically bounded mean-square error. To this end, we introduce

$$\begin{array}{l} \bar{\alpha}_1 = \frac{\lambda_n + 2s\bar{h}_M^2 + \sqrt{\lambda_n^2 + 4s^2\bar{h}_M^4}}{2} - 1, \\ \bar{\alpha}_2 = \frac{\sqrt{(\lambda_2 - s\bar{\rho}_m^2)^2 + 4s^2\bar{h}_M^4} - \lambda_2 - s\bar{\rho}_m^2}{2} + 1, \\ \bar{\alpha} = \max\{|\bar{\alpha}_1|, |\bar{\alpha}_2|\}. \end{array} \tag{12}$$

Theorem 6. *Suppose the step size s is selected in the way that*

$$0 < s < \min\left\{\frac{2(2-\lambda_n)}{\bar{h}_M^2(4-\lambda_n)}, \frac{\bar{\rho}_m\lambda_2}{\bar{h}_M^4}\right\}$$

Then there holds for Algorithm 3 that

$$\lim_{t\to\infty} \mathbb{E}\|\mathbf{x}_i(t) - \mathbf{a}^*\|^2 \leq (2s^2\sigma^2 n^4\|\mathbf{a}^*\|^2 + 2ns^2\sigma^2)/(1-\bar{\alpha})^2$$

with $0 < \bar{\alpha} < 1$.

In view of Theorems 5 and 6, given any noise level σ according to Theorem 5, the desired ϵ-differential privacy can always be preserved, and one can increase the time horizon T to improve the computation accuracy with no effect on the privacy guarantee.

V. Proofs of Statements

In this section, we prove the various statements claimed in the previous discussions.

A. Proof of Theorem 1

We begin the proof by representing the mapping $\mathcal{M}$ into a recursive algebraic from Algorithm 1. For convenience of the subsequent analysis, the following matrices are introduced:

$$\begin{array}{l} \mathbf{F} = \mathbf{I}_{n^2} - \mathbf{L}\otimes\mathbf{I}_n - s\mathbf{H}\mathbf{H}^\top, \\ \mathbf{H} = \begin{bmatrix} \mathbf{h}_1 & & \\ & \ddots & \\ & & \mathbf{h}_n \end{bmatrix}, \quad \boldsymbol{\gamma} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}. \end{array} \tag{13}$$

Now under Algorithm 1, we can obtain the following compact form for the evolution of the observations $\mathbf{y}_t$ as

$$\mathbf{y}_{t+1} = \mathbf{F}\,\mathbf{y}_t + s\mathbf{H}(\mathbf{b}+\boldsymbol{\gamma})\,, \qquad 0 \leq t \leq T-1\,. \tag{14}$$

By defining the random mapping $\widehat{\mathcal{M}}(\mathbf{b}) := \mathbf{b} + \boldsymbol{\gamma}$, (14) can be rewritten as

$$\mathbf{y}_{t+1} = \mathbf{F}\,\mathbf{y}_t + s\mathbf{H}\widehat{\mathcal{M}}(\mathbf{b})\,.$$

It immediately follows that there exists a *deterministic* mapping $\Psi : \mathbb{R}^n \to \mathbb{R}^{n^2(T+1)}$ such that

$$\big(\mathbf{y}_t\big)_{t=0}^T := \mathcal{M}(\mathbf{b}) = \Psi \circ \widehat{\mathcal{M}}(\mathbf{b})\,.$$

According to [1], it is known that ϵ-differential privacy is resilient to a deterministic post-processing. That is, $\mathcal{M}(\mathbf{b})$ achieves an ϵ-differential privacy under μ-adjacency if so does the $\widehat{\mathcal{M}}(\mathbf{b})$.

With this in mind, the proof reduces to show that the $\widehat{\mathcal{M}}(\mathbf{b})$ is ϵ-differentially private. Note that the sensitivity of mechanism $\widehat{\mathcal{M}}$ equals to the adjacency μ. According to [1], given any two μ-adjacent $\mathbf{b}, \mathbf{b}' \in \mathbb{R}^n$, there holds

$$\begin{aligned} \mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b}) \in \hat{R}\big) &\leq \exp\left(\frac{\|\mathbf{b}-\mathbf{b}'\|_1}{\sigma_\gamma}\right)\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b}') \in \hat{R}\big) \\ &\leq \exp(\mu/\sigma_\gamma)\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b}) \in \hat{R}\big) \end{aligned}$$

for all $\hat{R} \subseteq \mathrm{range}(\widehat{\mathcal{M}})$. This indicates that $\widehat{\mathcal{M}}(\mathbf{b})$ is ϵ-differentially private under μ-adjacency for all $\sigma_\gamma \geq \mu/\epsilon$, which thus completes the proof.

B. Proof of Theorem 2

Instrumental to the proof is the following technical lemma.

Lemma 2. With $\mathbf{F}$ defined in (13), there holds

$$-\mathbf{I} < -\alpha_1\mathbf{I} \leq \mathbf{F} \leq \alpha_2\mathbf{I} < \mathbf{I}\,. \tag{15}$$

Proof. First of all, we recall that

$$\begin{array}{l} \rho_m = \sigma_m\left(\sum_{i=1}^n \mathbf{h}_i\mathbf{h}_i^\top/n\right), \\ h_M = \max\{\|\mathbf{h}_1\|, \ldots, \|\mathbf{h}_n\|\}, \\ \alpha_1 = \frac{\lambda_n + 2sh_M^2 + \sqrt{\lambda_n^2 + 4s^2h_M^4}}{2} - 1, \\ \alpha_2 = \frac{\sqrt{(\lambda_2 - s\rho_m)^2 + 4s^2h_M^4} - \lambda_2 - s\rho_m}{2} + 1, \\ \alpha = \max\{|\alpha_1|, |\alpha_2|\}. \end{array} \tag{16}$$

By some simple but lengthy computations, it can be found that $\alpha_1 < 1$, $\alpha_2 < 1$, and $\alpha_1 + \alpha_2 \geq 0$ by $\rho_m \leq h_M^2$.

Then the proof reduces to show (i) $\mathbf{F} + \alpha_1\mathbf{I} \geq 0$ and (ii) $\alpha_2\mathbf{I} - \mathbf{F} \geq 0$. Before proceeding to show the both cases, we denote by $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ a set of the orthogonal unit eigenvectors of $\mathbf{L}$ with each $\mathbf{u}_i$ corresponding to the eigenvalue λ_i and $\mathbf{u}_1 =$

$$\mathbf{U}^\top\mathbf{F}\mathbf{U}+\alpha_1\mathbf{I}=\begin{bmatrix}(1+\alpha_1)\mathbf{I}-s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1 & -s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2\\ -s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1 & (1+\alpha_1)\mathbf{I}-\Lambda-s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2\end{bmatrix}. \tag{17}$$

$$(1+\alpha_1)\mathbf{I}-\Lambda-s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2-s^2\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\left((1+\alpha_1)\mathbf{I}-s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\right)^{-1}\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2$$
$$\geq\left(1+\alpha_1-\lambda_n-sh_M^2-\frac{s^2h_M^4}{(1+\alpha_1-sh_M^2)}\right)\mathbf{I}=0 \tag{18}$$

$$\alpha_2\mathbf{I}-\mathbf{U}^\top\mathbf{F}\mathbf{U}=\begin{bmatrix}(\alpha_2-1)\mathbf{I}+s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1 & s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2\\ s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1 & (\alpha_2-1)\mathbf{I}+\Lambda+s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2\end{bmatrix}\geq 0\,. \tag{19}$$

$$(\alpha_2-1)\mathbf{I}+\Lambda+s\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2-s^2\mathbf{U}_2^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\left((\alpha_2-1)\mathbf{I}+s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\right)^{-1}\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_2$$
$$\geq\left(\lambda_2+\alpha_2-1-\frac{s^2h_M^4}{s\rho_m+\alpha_2-1}\right)\mathbf{I}=0\,. \tag{20}$$

$\mathbf{1}_n/\sqrt{n}$, and let $\Lambda=\mathrm{diag}\{\lambda_2,\ldots,\lambda_n\}\otimes\mathbf{I}_n$, $\mathbf{U}=[\mathbf{U}_1,\,\mathbf{U}_2]$ with $\mathbf{U}_1=\mathbf{u}_1\otimes\mathbf{I}_n$ and $\mathbf{U}_2=[\mathbf{u}_2,\ldots,\mathbf{u}_n]\otimes\mathbf{I}_n$. It is noted that $\mathbf{U}^\top\mathbf{U}=\mathbf{I}$.

We now prove $\mathbf{F}+\alpha_1\mathbf{I}\geq 0$, which is equivalent to proving $\mathbf{U}^\top(\mathbf{F}+\alpha_1\mathbf{I})\mathbf{U}=\mathbf{U}^\top\mathbf{F}\mathbf{U}+\alpha_1\mathbf{I}\geq 0$. To show this, we first give the expression of $\mathbf{U}^\top\mathbf{F}\mathbf{U}+\alpha_1\mathbf{I}$ as (17).

Bearing (16) in mind, we then observe that

$$\begin{array}{rl}&(1+\alpha_1)\mathbf{I}-s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\\ =&(1+\alpha_1)\mathbf{I}-s\sum_{i=1}^n\mathbf{h}_i\mathbf{h}_i^\top/n\mathbf{I}\\ \geq&(1+\alpha_1-sh_M^2)\mathbf{I}\\ =&\frac{\lambda_n+\sqrt{\lambda_n^2+4s^2h_M^4}}{2}\mathbf{I}\\ >&0\end{array}$$

and (18), where the definition of α_1 in (16) is used. Thus, according to the Schur Complement, it can be concluded that $\mathbf{U}^\top\mathbf{F}\mathbf{U}+\alpha_1\mathbf{I}\geq 0$, proving $\mathbf{F}\geq-\alpha_1\mathbf{I}$.

Similarly, we proceed to prove $\alpha_2\mathbf{I}-\mathbf{F}\geq 0$, which is equivalent to proving (19). To prove this, with (16) we notice that

$$\begin{array}{rl}&(\alpha_2-1)\mathbf{I}+s\mathbf{U}_1^\top\mathbf{H}\mathbf{H}^\top\mathbf{U}_1\\ =&(\alpha_2-1)\mathbf{I}+s\sum_{i=1}^n\mathbf{h}_i\mathbf{h}_i^\top/n\\ \geq&(\alpha_2-1+s\rho_m)\mathbf{I}>0\end{array}$$

and (20). Again, according to the Schur complement, it can be concluded that $\alpha_2\mathbf{I}-\mathbf{U}^\top\mathbf{F}\mathbf{U}\geq 0$, proving $\mathbf{F}\leq\alpha_2\mathbf{I}$. The proof is thus completed. □

Now we are ready to establish the theorem. According to Algorithm 1, the evolution of the network state $\mathbf{x}_t=(\mathbf{x}_1(t),\ldots,\mathbf{x}_n(t))^\top$ can be described by

$$\mathbf{x}_{t+1}=\mathbf{F}\mathbf{x}_t+s\mathbf{H}(\mathbf{b}+\boldsymbol{\gamma}) \tag{21}$$

where $\mathbf{F}$ is defined in (13) and satisfies (15).

Define the error between the network state and the Nash equilibrium as $\mathbf{z}_t:=\mathbf{x}_t-\mathbf{1}_n\otimes\mathbf{a}^*$, whose evolution along (21) can be described by

$$\mathbf{z}_{t+1}=\mathbf{F}\mathbf{z}_t+s\mathbf{H}^\top\boldsymbol{\gamma}\,,$$

yielding

$$\mathbf{z}_t=\mathbf{F}^t\mathbf{z}_0+s\sum_{j=0}^{t-1}\mathbf{F}^j\mathbf{H}^\top\boldsymbol{\gamma}\,. \tag{22}$$

Note that $\|\mathbf{F}\|\leq\alpha:=\max\{|\alpha_1|,|\alpha_2|\}<1$ by (15) and $\mathbf{z}_0$ is deterministic. Thus, we have $\mathbb{E}\mathbf{z}_t=\mathbf{F}^t\mathbf{z}_0$, which proves that $\lim_{t\to\infty}\mathbb{E}\mathbf{z}_t=0$, and thus $\lim_{t\to\infty}\mathbb{E}\mathbf{x}_i(t)=\mathbf{a}^*$.

Moreover, by (22), there hold

$$\begin{array}{rcl}\mathbb{E}\|\mathbf{z}_t\|^2&=&\mathbb{E}\|\mathbf{F}^t\mathbf{z}_0+s\sum_{j=0}^{t-1}\mathbf{F}^j\mathbf{H}^\top\boldsymbol{\gamma}\|^2\\ &=&\|\mathbf{F}^t\mathbf{z}_0\|^2+s^2\mathbb{E}\|\sum_{j=0}^{t-1}\mathbf{F}^j\mathbf{H}^\top\boldsymbol{\gamma}\|^2\\ &\leq&\alpha^{2t}\|\mathbf{z}_0\|^2+2ns^2\sigma_\gamma^2h_M^2\frac{1}{(1-\alpha)^2}\,.\end{array}$$

Therefore, it can be seen that

$$\lim_{t\to\infty}\mathbb{E}\|\mathbf{x}_t-\mathbf{1}_n\mathbf{a}^*\|^2=\lim_{t\to\infty}\mathbb{E}\|\mathbf{z}_t\|^2\leq 2ns^2\sigma_\gamma^2h_M^2\frac{1}{(1-\alpha)^2}\,.$$

The proof is completed.

C. Proof of Theorem 3

We proceed the proof of Theorem 3 by deriving the mapping $\mathcal{M}$ from the sensitive dataset $(\mathbf{b},\mathbf{G})$ to the eavesdropped messages $(\mathbf{y}_t)_{t=0}^T$. We first introduce the following evolution of the messages $\mathbf{y}_i(t)$ of node i according to Algorithm 2 as

$$\begin{array}{rcl}\mathbf{y}_i(t+1)&=&\mathcal{M}_{i,t+1}(b_i,\mathbf{G}_i)\\ &:=&\mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t))-\sum_{j\in\mathrm{V}}w_{ij}\big(\mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t))-\mathscr{P}_{\mathbb{A}}(\mathbf{y}_j(t))\big)\\ &&-s\mathbf{h}_i\big(\mathbf{h}_i^\top\mathscr{P}_{\mathbb{A}}(\mathbf{y}_i(t))-b_i\big)+\boldsymbol{\nu}_i(t+1)\end{array}$$

where we denote $\mathbf{G}_i$ by the i-th column of $\mathbf{G}^\top$, and $\boldsymbol{\nu}_i(t+1)\backsim\mathcal{L}(0,\sigma_\nu^2\mathbf{I}_n)$ for $t=0,1,\ldots,T-1$ and $i\in\mathrm{V}$. Then we can denote the mapping $\mathcal{M}=\big[\mathcal{M}_0;\mathcal{M}_1;\cdots;\mathcal{M}_T\big]$ with $\mathcal{M}_0=\mathbf{y}_0$ and $\mathcal{M}_t=\big[\mathcal{M}_{1,t};\cdots;\mathcal{M}_{n,t}\big]$ for $t=1,\ldots,T$. Note that the mapping $\mathcal{M}_0$ is deterministic and independent of $(\mathbf{b},\mathbf{G})$. Correspondingly, for any $R\subseteq\mathrm{range}(\mathcal{M})$, we denote $R=R_0\times R_1\times\cdots\times R_T$ with $R_t=R_{1,t}\times\cdots\times R_{n,t}\subseteq\mathbb{R}^{n^2}$, and $R_{i,t}\subseteq\mathbb{R}^n$ for $i=1,\ldots,n$, and $t=0,1,\ldots,T$.

Thus for all $R\subseteq\mathrm{range}(\mathcal{M})$, we have

$$\begin{array}{l}\dfrac{\mathbb{P}\big(\mathcal{M}(\mathbf{b},\mathbf{G})\in R\big)}{\mathbb{P}\big(\mathcal{M}_0(\mathbf{b},\mathbf{G})\in R_0\big)}\\ =\prod_{t=1}^T\mathbb{P}\left(\mathcal{M}_t(\mathbf{b},\mathbf{G})\in R_t|\mathcal{M}_{t-1}(\mathbf{b},\mathbf{G})\in R_{t-1}\right)\\ =\prod_{t=1}^T\prod_{i=1}^n\mathbb{P}\big(\mathcal{M}_{i,t}(b_i,\mathbf{G}_i)\in R_{i,t}|\mathbf{y}_{t-1}\in R_{t-1}\big)\,.\end{array}\tag{23}$$

$$
\begin{aligned}
&\mathbb{P}\big(\mathcal{M}_{i,t}(b_i,\mathbf{G}_i)\in R_{i,t}|\mathbf{y}_{t-1}\in R_{t-1}\big)\\
=&\frac{\int_{R_{t-1}} f_{t-1}(y)\int_{R_{i,t}}(2\sigma_\gamma)^{-n}\exp\left(-\left\|x-g_i(y)+s\mathbf{h}_i\big(\mathbf{h}_i^\top\mathscr{P}_{\mathbb{A}}(y)-b_i\big)\right\|_1/\sigma_\nu\right)dx\,dy}{\mathbb{P}\big(\mathbf{y}_{t-1}\in R_{t-1}\big)}\\
\le&\int_{R_{t-1}} f_{t-1}(y)\int_{R_{i,t}}(2\sigma_\gamma)^{-n}\exp\left(-\left\|x-g_i(y)+s\mathbf{h}_i'\big(\mathbf{h}_i'^{\top}\mathscr{P}_{\mathbb{A}}(y)-b_i'\big)\right\|_1/\sigma_\nu\right)dx\\
&\exp\left(\left\|s\mathbf{h}_i\big(\mathbf{h}_i^\top\mathscr{P}_{\mathbb{A}}(y)-b_i\big)-s\mathbf{h}_i'\big(\mathbf{h}_i'^{\top}\mathscr{P}_{\mathbb{A}}(y)-b_i'\big)\right\|_1/\sigma_\nu\right)dy\Big/\mathbb{P}\big(\mathbf{y}_{t-1}\in R_{t-1}\big)\\
\le&\exp\left(s\ell_{\mathbb{A}}\|\mathrm{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top})\|_1/\sigma_\nu+s\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1/\sigma_\nu\right)\mathbb{P}\big(\mathcal{M}_{i,t}(b_i',\mathbf{G}_i')\in R_{i,t}|\mathbf{y}_{t-1}\in R_{t-1}\big),
\end{aligned}
\tag{24}
$$

$$
\begin{aligned}
\mathbb{P}\big(\mathcal{M}(\mathbf{b},\mathbf{G})\in R\big)\le&\prod_{t=1}^{T}\prod_{i=1}^{n}\exp\left(s\ell_{\mathbb{A}}\|\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top}\|_1/\sigma_\nu+s\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1/\sigma_\nu\right)\\
&\mathbb{P}\big(\mathcal{M}_0(\mathbf{b}',\mathbf{G}')\in R_0\big)\prod_{t=1}^{T}\prod_{i=1}^{n}\mathbb{P}\big(\mathcal{M}_{i,t}(b_i',\mathbf{G}_i')\in R_{i,t}|\mathbf{y}_{t-1}\in R_{t-1}\big)\\
=&\exp\left(\sum_{i=1}^{n}Ts\ell_{\mathbb{A}}\|\mathrm{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top})\|_1/\sigma_\nu+\sum_{i=1}^{n}Ts\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1/\sigma_\nu\right)\mathbb{P}\big(\mathcal{M}(\mathbf{b},\mathbf{G}')\in R\big).
\end{aligned}
\tag{25}
$$

Denote by $f_t(\mathbf{y}_t)$ the probability density function of $\mathbf{y}_t$ for $t=1,\ldots,T$, and let $g_i(y)=\mathscr{P}_{\mathbb{A}}(y)-\sum_{j\in\mathrm{V}}w_{ij}\big(\mathscr{P}_{\mathbb{A}}(y)-\mathscr{P}_{\mathbb{A}}(y)\big)$ for $i\in\mathrm{V}$. Then, for $t=1,\ldots,T$ and any $(\mathbf{b}',\mathbf{G}')\in\mathbb{B}\times\mathbb{G}$, we have (24), where the first inequality is obtained by using the triangle inequality, and the second is obtained by using the triangle inequality again and the fact that $\|\mathscr{P}_{\mathbb{A}}(y)\|\le\ell_{\mathbb{A}}$ for all $y\in\mathbb{R}^n$. Here $\mathbf{h}_i'=\mathbf{e}_i-\mathbf{G}_i'$ with $\mathbf{e}_i\in\mathbb{R}^n$ is a unit vector whose entries are all zero except the i-th being one and $\mathbf{G}_i'$ is the i-th column of $\mathbf{G}'^{\top}$.

By combining the above inequality (24) with (23) and recalling that $\mathcal{M}_0(\cdot)$ is independent of $\mathbf{G},\mathbf{b}$, it immediately follows (25).

Towards this end, it is clear that the proof is completed if there holds

$$
\begin{aligned}
&\textstyle\sum_{i=1}^{n}Ts\ell_{\mathbb{A}}\|\mathrm{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top})\|_1/\sigma_\nu\\
&\quad+\textstyle\sum_{i=1}^{n}Ts\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1/\sigma_\nu\le\epsilon
\end{aligned}
\tag{26}
$$

for any two μ-adjacent $(\mathbf{b},\mathbf{G}),(\mathbf{b}',\mathbf{G}')\in\mathbb{B}\times\mathbb{G}$.

We now proceed to show (26) and recall that $\mathbf{h}_i=\mathbf{e}_i-\mathbf{G}_i$ and $\mathbf{h}_i'=\mathbf{e}_i-\mathbf{G}_i'$, which yields

$$
\begin{aligned}
\mathbf{h}_i\mathbf{h}_i^\top&=\mathbf{e}_i\mathbf{e}_i^\top-\mathbf{G}_i\mathbf{e}_i^\top-\mathbf{e}_i\mathbf{G}_i^\top+\mathbf{G}_i\mathbf{G}_i^\top\\
\mathbf{h}_i'\mathbf{h}_i'^{\top}&=\mathbf{e}_i\mathbf{e}_i^\top-\mathbf{G}_i'\mathbf{e}_i^{\top}-\mathbf{e}_i\mathbf{G}_i'^{\top}+\mathbf{G}_i'\mathbf{G}_i'^{\top}
\end{aligned}
\tag{27}
$$

Hence, we have

$$
\begin{aligned}
&\textstyle\sum_{i=1}^{n}\|\mathrm{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top})\|_1\\
=&\textstyle\sum_{i=1}^{n}\|\mathrm{vec}((\mathbf{G}_i-\mathbf{G}_i')\mathbf{G}_i^\top)-\mathrm{vec}((\mathbf{G}_i-\mathbf{G}_i')\mathbf{e}_i^\top)\\
&-\mathrm{vec}(\mathbf{e}_i(\mathbf{G}_i-\mathbf{G}_i')^\top)+\mathrm{vec}(\mathbf{G}_i'(\mathbf{G}_i-\mathbf{G}_i')^\top)\|_1\\
\le&\textstyle\sum_{i=1}^{n}\|\mathrm{vec}((\mathbf{G}_i-\mathbf{G}_i')\mathbf{G}_i^\top)\|_1+2\sum_{i=1}^{n}\|\mathbf{G}_i-\mathbf{G}_i'\|_1\\
&+\textstyle\sum_{i=1}^{n}\|\mathrm{vec}(\mathbf{G}_i'(\mathbf{G}_i-\mathbf{G}_i')^\top)\|_1\\
\le&\ 2\mu\ell_g+2\mu\,,
\end{aligned}
\tag{28}
$$

and

$$
\begin{aligned}
&\textstyle\sum_{i=1}^{n}\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1\\
=&\textstyle\sum_{i=1}^{n}\|(b_i-b_i')\mathbf{e}_i-(\mathbf{G}_ib_i-\mathbf{G}_i'b_i')\|_1\\
\le&\textstyle\sum_{i=1}^{n}|b_i-b_i'|+\sum_{i=1}^{n}\|\mathbf{G}_ib_i-\mathbf{G}_i'b_i'\|_1\\
\le&\textstyle\sum_{i=1}^{n}(1+\ell_g)|b_i-b_i'|+\sum_{i=1}^{n}\|\mathbf{G}_i-\mathbf{G}_i'\|_1\ell_b\\
\le&\ \max\{1+\ell_g,\ell_b\}\mu\,.
\end{aligned}
\tag{29}
$$

Therefore, there holds

$$
\begin{aligned}
&\textstyle\sum_{i=1}^{n}Ts\ell_{\mathbb{A}}\|\mathrm{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^{\top})\|_1/\sigma_\nu\\
&\quad+\textstyle\sum_{i=1}^{n}Ts\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1/\sigma_\nu\\
\le&\ 2sT\mu\ell_{\mathbb{A}}(\ell_g+1)/\sigma_\nu+sT\mu\max\{1+\ell_g,\ell_b\}/\sigma_\nu\\
\le&\ \epsilon\,.
\end{aligned}
$$

This proves (26) and thus completes the proof.

D. Proof of Theorem 4

We begin the proof by presenting the evolution of node state $\mathbf{x}_t$ under Algorithm 2 as

$$
\mathbf{x}_{t+1}=\mathbf{F}\mathcal{P}_{\mathbb{A}^n}(\mathbf{x}_t+\boldsymbol{\nu}_t)+s\mathbf{H}\mathbf{b}\,,
\tag{30}
$$

where $\mathbf{F}$ and $\mathbf{H}$ are given by (13), and $\boldsymbol{\nu}_t=[\boldsymbol{\nu}_1(t);\ldots;\boldsymbol{\nu}_n(t)]$ with $\boldsymbol{\nu}_0=0$ and $\boldsymbol{\nu}_t\backsim\mathcal{L}(0,\sigma_\nu^2\mathbf{I}_{n^2})$ for $t=1,\ldots,T-1$. Denote the error between the network node state and the Nash equilibrium as $\mathbf{z}_t:=\mathbf{x}_t-\mathbf{1}_n\otimes\mathbf{a}^*$, which along (30) satisfies

$$
\mathbf{z}_{t+1}=\mathbf{F}[\mathcal{P}_{\mathbb{A}^n}(\mathbf{z}_t+\mathbf{1}_n\otimes\mathbf{a}^*+\boldsymbol{\nu}_t)-\mathbf{1}_n\otimes\mathbf{a}^*]\,.
$$

Recalling that the set $\mathbb{A}$ is a convex compact set and $\|\mathbf{F}\|\le\alpha:=\max\{|\alpha_1|,|\alpha_2|\}<1$ by Lemma 2, we thus have

$$
\begin{aligned}
\|\mathbf{z}_{t+1}\|^2&\le\|\mathbf{F}\|^2\|\mathcal{P}_{\mathbb{A}^n}(\mathbf{z}_t+\mathbf{1}_n\otimes\mathbf{a}^*+\boldsymbol{\nu}_t)-\mathbf{1}_n\otimes\mathbf{a}^*\|^2\\
&\le\alpha^2\|\mathbf{z}_t+\boldsymbol{\nu}_t\|^2\\
&=\alpha^2\|\mathbf{z}_t\|^2+\alpha^2\|\boldsymbol{\nu}_t\|^2+2\alpha^2\mathbf{z}_t^\top\boldsymbol{\nu}_t\,.
\end{aligned}
$$

It then follows that

$$
\|\mathbf{z}_t\|^2\le\alpha^{2t}\|\mathbf{z}_0\|^2+\sum_{k=0}^{t-1}\alpha^{2(t-k)}\|\boldsymbol{\nu}_k\|^2+2\sum_{k=0}^{t-1}\alpha^{2(t-k)}\mathbf{z}_k^\top\boldsymbol{\nu}_k\,.
$$

By taking the expectation on both sides of the above inequality, we can obtain

$$
\mathbb{E}\|\mathbf{z}_t\|^2\le\alpha^{2t}\|\mathbf{z}_0\|^2+\sum_{k=1}^{t-1}\alpha^{2(t-k)}n2\sigma_\nu^2\,,\qquad t=0,1,\ldots,T-1\,,
$$

where we have used the facts that $\mathbf{z}_k$ is independent of $\boldsymbol{\nu}_k$ and $\mathbf{z}_0,\mathbf{z}_1$ are deterministic.

$$\begin{aligned}\frac{\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})\in\hat{R}\big)}{\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b}',\mathbf{G}')\in\hat{R}\big)}&\leq\exp\left(\frac{1}{\sigma}\sum_{i=1}^{n}\|\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)-\mathscr{H}^{-1}(\mathbf{h}_i'\mathbf{h}_i'^\top)\|_1+\frac{1}{\sigma}\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1\right)\\&=\exp\left(\frac{1}{\sigma}\sum_{i=1}^{n}\|\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^\top)\|_1+\frac{1}{\sigma}\|\mathbf{h}_ib_i-\mathbf{h}_i'b_i'\|_1\right)\end{aligned}\tag{31}$$

Therefore, with $\gamma=-2\ln(|\alpha|)$, we have

$$\begin{aligned}\mathbb{E}\|\mathbf{z}_t\|^2&\leq\alpha^{2t}\|\mathbf{z}_0\|^2+2n\alpha^2(1-\alpha^{2(t-1)})\sigma_\nu^2/(1-\alpha^2)\\&\leq\exp\big(-\gamma t\big)\|\mathbf{z}_0\|^2+2n\alpha^2\sigma_\nu^2/(1-\alpha^2)\,,\end{aligned}$$

completing the proof.

E. Proof of Theorem 5

Similar to the proof of Theorem 1 in Section 5.1, we will employ the resilient property of ϵ-differential privacy to a deterministic post-processing. To be precise, we proceed the proof by firstly representing the mapping $\mathcal{M}$ into a composition of a deterministic mapping and a random mapping, and then establishing the ϵ-differential privacy of the random mapping.

Under Algorithm 3, we can obtain the following form for the evolution of the observations as

$$\begin{aligned}\mathbf{y}_i(t+1)=\mathbf{y}_i(t)-\textstyle\sum_{j\in\mathrm{V}}w_{ij}\big(\mathbf{y}_i(t)-\mathbf{y}_j(t)\big)\\-s\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}\big(\widehat{\mathcal{M}}_{1,i}(b_i,\mathbf{G}_i)\big)\mathbf{y}_i(t)+s\widehat{\mathcal{M}}_{2,i}(b_i,\mathbf{G}_i)\,.\end{aligned}$$

where we have defined

$$\begin{aligned}\widehat{\mathcal{M}}_{1,i}(b_i,\mathbf{G}_i)&:=\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)+\boldsymbol{\eta}_i\\\widehat{\mathcal{M}}_{2,i}(b_i,\mathbf{G}_i)&:=\mathbf{h}_ib_i+\boldsymbol{\omega}_i\,.\end{aligned}\qquad\forall i\in\mathrm{V}\,.$$

Let

$$\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})=\begin{bmatrix}\widehat{\mathcal{M}}_1(\mathbf{b},\mathbf{G})\\\widehat{\mathcal{M}}_2(\mathbf{b},\mathbf{G})\end{bmatrix}$$

with

$$\widehat{\mathcal{M}}_k(\mathbf{b},\mathbf{G})=\begin{bmatrix}\widehat{\mathcal{M}}_{k,1}(b_1,\mathbf{G}_1)\\\cdots\\\widehat{\mathcal{M}}_{k,n}(b_n,\mathbf{G}_n)\end{bmatrix}\qquad k=1,2\,.$$

It then follows from (V-E) that there exists a *deterministic* mapping $\Psi:\mathbb{R}^n\to\mathbb{R}^{n^2(T+1)}$ such that

$$\big(\mathbf{y}_t\big)_{t=0}^{T}:=\mathcal{M}(\mathbf{b},\mathbf{G})=\Psi\circ\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})\,.$$

By [19, Proposition IV.3], $\mathcal{M}(\mathbf{b},\mathbf{G})$ achieves an ϵ-differential privacy under μ-adjacency if so does the $\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})$.

With this in mind, we now proceed to show that the $\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})$ is ϵ-differentially private. According to [1], given any two μ-adjacent $(\mathbf{b},\mathbf{G}),(\mathbf{b}',\mathbf{G}')$, there holds (31) for all $\hat{R}\subseteq\text{range}(\widehat{\mathcal{M}})$.

By $\|\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^\top)\|_1\leq\|\text{vec}(\mathbf{h}_i\mathbf{h}_i^\top-\mathbf{h}_i'\mathbf{h}_i'^\top)\|_1$, and using (28) and (29), we can further obtain

$$\begin{aligned}&\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})\in\hat{R}\big)\\&\leq\exp\left(\frac{2\mu\ell_g+2\mu+\max\{1+\ell_g,\ell_b\}\mu}{\sigma}\right)\mathbb{P}\big(\widehat{\mathcal{M}}(\mathbf{b}',\mathbf{G}')\in\hat{R}\big)\end{aligned}$$

which indicates that $\widehat{\mathcal{M}}(\mathbf{b},\mathbf{G})$ is ϵ-differentially private under μ-adjacency for all $\sigma\geq\frac{2\mu(\ell_g+1)+\max\{1+\ell_g,\ell_b\}\mu}{\epsilon}$. This thus completes the proof by [19, Proposition IV.3].

F. Proof of Lemma 1

For convenience of subsequent analysis, we give the definitions of $\mathcal{C}_i$ and $\mathbf{K}_{\boldsymbol{\eta}_i}$ below

$$\begin{aligned}\mathcal{C}_i&=\Big\{\mathbf{x}\in\mathbb{R}^{n(n+1)/2}:\textstyle\sum_{j\in\mathrm{V}}x_{j(j+1)/2}\in[\underline{q}_i,\bar{q}_i],\\&\qquad\mathscr{H}(\mathbf{x})\mathbf{l}_{ij}=0,\forall j\in\mathrm{V}/\{i\}\Big\}\\\mathbf{K}_{\boldsymbol{\eta}_i}&=\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}\big(\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)+\boldsymbol{\eta}_i\big),\quad i\in\mathrm{V}\,.\end{aligned}\tag{32}$$

Before proceeding to the explicit upper and lower bounds of $\mathbf{K}_{\boldsymbol{\eta}_i}$, we note some properties on the composite mapping $\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}$. From the definition of $\mathcal{C}_i$ and $\mathscr{H}$, it is observed that $\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathbf{x})$ is a symmetric matrix and has only one non-zero eigenvalue as $\text{Trace}\big(\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathbf{x})\big)\in[\underline{q}_i,\bar{q}_i]$, for any $\mathbf{x}\in\mathbb{R}^{n(n+1)/2}$. Thus, there must exist a vector $\mathbf{m}_i$ such that $\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathbf{x})=\mathbf{m}_i\mathbf{m}_i^\top$. It is also noted that $\{\mathbf{l}_{i1},\ldots,\mathbf{l}_{in}\}$ are linearly independent, which implies that there exist c_{ij} such that $\mathbf{m}_i=\sum_{j=1}^n c_{ij}\mathbf{l}_{ij}$. By (32), we know that $\mathbf{m}_i\mathbf{m}_i^\top\mathbf{l}_{ij}=0$ for all $j\neq i$, which yields $c_{ij}=0$ for all $j\neq i$ using the equality that $\mathbf{l}_{ii}^\top\mathbf{l}_{ij}=0$ for all $j\neq i$. Namely, we have $\mathbf{m}_i=c_{ii}\mathbf{l}_{ij}=c_{ii}\frac{\mathbf{h}_i}{\|\mathbf{h}_i\|}$. Hence, there must hold

$$\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathbf{x})=\frac{\text{Trace}\big(\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathbf{x})\big)}{\|\mathbf{h}_i\|^2}\mathbf{h}_i\mathbf{h}_i^\top\,.\tag{33}$$

With this in mind, we are now ready to derive upper and lower bounds of $\mathbf{K}_{\boldsymbol{\eta}_i}$. By (33), we can obtain

$$\begin{aligned}&\textstyle\sum_{i=1}^n\mathbf{K}_{\boldsymbol{\eta}_i}/n\\=&\textstyle\sum_{i=1}^n\frac{\text{Trace}\big(\mathbf{K}_{\boldsymbol{\eta}_i}\big)}{n\|\mathbf{h}_i\|^2}\mathbf{h}_i\mathbf{h}_i^\top\\\geq&\min\{\tfrac{\underline{q}_1}{\|\mathbf{h}_1\|^2},\ldots,\tfrac{\underline{q}_n}{\|\mathbf{h}_n\|^2}\}\textstyle\sum_{i=1}^n\mathbf{h}_i\mathbf{h}_i^\top/n\geq\bar{\rho}_m\mathbf{I}\end{aligned}$$

where the latter inequality is obtained based on (16). This proves the lower bound.

We then proceed to show the upper bound, and by (33), there holds

$$\|\mathbf{K}_{\boldsymbol{\eta}_i}\|\leq\text{Trace}\big(\mathbf{K}_{\boldsymbol{\eta}_i}\big)\leq\bar{q}_i\,.$$

This proves the upper bound with $\bar{h}_M:=\max\{\sqrt{\bar{q}_1},\ldots,\sqrt{\bar{q}_n}\}$.

G. Proof of Theorem 6

According to Algorithm 3, the evolution of the network node state $\mathbf{x}_t=(\mathbf{x}_1(t),\ldots,\mathbf{x}_n(t))^\top$ can be described by

$$\mathbf{x}_{t+1}=\mathbf{F}_{\boldsymbol{\eta}}\mathbf{x}_t+s(\mathbf{H}\mathbf{b}+\boldsymbol{\omega})\tag{34}$$

where $\mathbf{F}_{\boldsymbol{\eta}}=(\mathbf{I}_n-\mathbf{L})\otimes\mathbf{I}_n-s\mathbf{K}_{\boldsymbol{\eta}}$ with $\mathbf{K}_{\boldsymbol{\eta}}=\text{diag}(\mathbf{K}_{\boldsymbol{\eta}_1},\ldots,\mathbf{K}_{\boldsymbol{\eta}_n})$. It is noted that following the arguments of Lemma 2 and using Lemma 1, one can easily conclude the following upper and lower bounds of the stochastic matrix $\mathbf{F}_{\boldsymbol{\eta}}$.

Lemma 3. There holds

$$-\mathbf{I} < -\bar{\alpha}_1\mathbf{I} \leq \mathbf{F}_{\boldsymbol{\eta}} \leq \bar{\alpha}_2\mathbf{I} < \mathbf{I}\,. \tag{35}$$

With this lemma in mind, we express $\mathbf{x}_t$ as a mapping of the deterministic initial state $\mathbf{x}_0$ and random noises $(\boldsymbol{\eta}, \boldsymbol{\omega})$, i.e.,

$$\begin{array}{rl} & \mathbf{x}_t \\ = & \mathbf{F}_{\boldsymbol{\eta}}^t\mathbf{x}_0 + s\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k(\mathbf{H}\mathbf{b}+\boldsymbol{\omega}) \\ = & \mathbf{F}_{\boldsymbol{\eta}}^t\mathbf{x}_0 + \sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k(\mathbf{I}-\mathbf{F})(\mathbf{1}_n\otimes\mathbf{a}^*) + s\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k\boldsymbol{\omega} \end{array}$$

where $\mathbf{F}$ is defined in (13), and to obtain the second equality, we have used

$$s\mathbf{H}\mathbf{b} = s\mathbf{H}\mathbf{H}^\top(\mathbf{1}_n\otimes\mathbf{a}^*) = (\mathbf{I}-\mathbf{F})(\mathbf{1}_n\otimes\mathbf{a}^*)\,.$$

This then yields

$$\begin{array}{rl} & \mathbf{x}_t - \mathbf{1}_n\otimes\mathbf{a}^* \\ = & \mathbf{F}_{\boldsymbol{\eta}}^t\mathbf{x}_0 + \left(\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k(\mathbf{I}-\mathbf{F}) - \mathbf{I}\right)(\mathbf{1}_n\otimes\mathbf{a}^*) \\ & +s\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k\boldsymbol{\omega} \\ = & \mathbf{F}_{\boldsymbol{\eta}}^t\mathbf{x}_0 + \left(\sum_{k=1}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k - \sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k\mathbf{F}\right)(\mathbf{1}_n\otimes\mathbf{a}^*) \\ & +s\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k\boldsymbol{\omega} \\ = & \mathbf{F}_{\boldsymbol{\eta}}^t[\mathbf{x}_0 - (\mathbf{1}_n\otimes\mathbf{a}^*)] + \sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k(\mathbf{F}_{\boldsymbol{\eta}}-\mathbf{F})(\mathbf{1}_n\otimes\mathbf{a}^*) \\ & +s\sum_{k=0}^{t-1}\mathbf{F}_{\boldsymbol{\eta}}^k\boldsymbol{\omega}\,. \end{array}$$

By (35) and recalling that the set $\mathcal{C}_i$ is constructed to be convex, we have

$$\begin{array}{rl} & \lim_{t\to\infty}\mathbb{E}\|\mathbf{x}_t - \mathbf{1}_n\otimes\mathbf{a}^*\|^2 \\ \leq & \frac{n^2\|\mathbf{a}^*\|^2}{(1-\bar{\alpha})^2}\mathbb{E}\|\mathbf{F}_{\boldsymbol{\eta}}-\mathbf{F}\|^2 + 2ns^2\sigma^2/(1-\bar{\alpha})^2 \\ \leq & \frac{s^2n^2\|\mathbf{a}^*\|^2}{(1-\bar{\alpha})^2}\max_{i\in\mathrm{V}}\{\mathbb{E}\|\mathscr{H}\circ\mathscr{P}_{\mathcal{C}_i}(\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)+\boldsymbol{\eta}_i) \\ & -\mathbf{h}_i\mathbf{h}_i^\top\|^2\} + 2ns^2\sigma^2/(1-\bar{\alpha})^2 \\ = & \frac{s^2n^2\|\mathbf{a}^*\|^2}{(1-\bar{\alpha})^2}\max_{i\in\mathrm{V}}\{\mathbb{E}\|\mathscr{H}\big(\mathscr{P}_{\mathcal{C}_i}(\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)+\boldsymbol{\eta}_i) \\ & -\mathscr{H}^{-1}(\mathbf{h}_i\mathbf{h}_i^\top)\big)\|^2\} + 2ns^2\sigma^2/(1-\bar{\alpha})^2 \\ \leq & 2s^2\sigma^2n^4\|\mathbf{a}^*\|^2/(1-\bar{\alpha})^2 + 2ns^2\sigma^2/(1-\bar{\alpha})^2 \end{array}$$

The proof is thus completed.

VI. Conclusions

We have developed distributed computation algorithms for Nash equilibrium of quadratic network games with proven differential privacy guarantees. In such network games, the underlying social influence structure and the individual marginal payoffs are subject to privacy concerns since they encode economic dependencies and preferences. The players interconnected by a public communication graph over which dynamical states are shared among neighboring nodes, were shown to be able to compute the Nash equilibrium with differential privacy guarantees. Three algorithms were proposed for preserving only the privacy of marginal payoffs only, or the privacy of both the marginal payoffs and the social influence structure. Their achievable differential privacy level and convergence properties were systematically established. Future work includes generalization of the differentially private Nash equilibrium computing framework to general continuous network games, and implementation of the results in real-world applications.

References

[1] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[2] N. Perraudin, J. Paratte, D. Shuman, L. Martin, V. Kalofolias, P. Vandergheynst, and D. K. Hammond, *GSPBOX: A toolbox for signal processing on graphs*. ArXiv e-prints, Aug. 2014.

[3] T. Alpcan, and T. Basar, *Distributed algorithms for Nash equilibria of flow control games*. In Advances in dynamic games. Boston: Birkhauser, pp. 473498, 2005.

[4] S. Li, J. Lian, A. J. Conejo, and W. Zhang, Transactive energy systems: the market-based coordination of distributed energy resources, *IEEE Control Systems Magazine*, vol. 40, no. 4, pp. 2652, 2020.

[5] S. Grammatico, F. Parise, M. Colombino, and J. Lygeros, "Decentralized convergence to Nash equilibria in constrained deterministic mean field control. *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp.33153329, 2016.

[6] M. Kearns, M. Littman, and S. Singh, "Graphical models for game theory". *In Proceedings of the 17-th Conference on Uncertainty in Artificial Intelligence*, pp.253-260, 2001.

[7] M. O. Jackson, and Y. Zenou, *Games on networks*. Handbook of Game Theory with Economic Applications. Elsevier, vol. 4, pp. 95-163, 2014.

[8] C. Ballester, A. Calvo-Armengol, and Y. Zenou, "Whos who in networks. Wanted: The key player". *Econometrica*, vol. 74, no. 5, pp.14031417, 2006.

[9] Y. Leng, X. Dong, J. Wu, and A. Pentland. Learning Quadratic Games on Networks. *In International Conference on Machine Learning*, pp. 5820-5830, 2020.

[10] G. Scutari, J. S. Pang, "Joint sensing and power allocation in nonconvex cognitive radio games: Nash equilibria and distributed algorithms". *IEEE Trans. Inform. Theory*, vol.59, no.7, pp.4626-4661, 2013.

[11] E. Dohmatob, "A simple algorithm for computing Nash-equilibria in incomplete information games". *OPT2016–NIPS workshop on optimization for machine learning*, 2016.

[12] C. K. Yu, M. van der Schaar, and A. H. Sayed, "Distributed learning for stochastic generalized Nash equilibrium problems," *IEEE Transactions on Signal Processing*, vol.65, no.15, pp.38933908, 2017.

[13] J. Koshal, A. Nedic, and U. V. Shanbhag, "Distributed algorithms for aggregative games on graphs," *Operations Research*, vol. 64, no. 3, pp. 680-704, 2016.

[14] Z. Zhou, P. Mertikopoulos, N. Bambos, P. W. Glynn, and C. Tomlin, "Countering feedback delays in multi-agent learning." In *the 31st Conference on Neural Information Processing Systems*, 2017.

[15] Z. Zhou, P. Mertikopoulos, S. Athey, et al. "Learning in games with lossy feedback". In *the 32nd Conference on Neural Information Processing Systems*, pp. 1-11, 2018.

[16] M. Bravo, D. S. Leslie, and P. Mertikopoulos, "Bandit learning in concave N-person games", In *the 32nd Conference on Neural Information Processing Systems*, 2018.

[17] S. Bervoets, M. Bravo, and M. Faure, "Learning with minimal information in continuous games," *Theoretical Economics*, vol. 15, pp. 1471-1508, 2020.

[18] M. T. Hale and M. Egerstedt, "Cloud-enabled differentially private multiagent optimization with constraints." *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 1693-1706, 2018.

[19] E. Nozari, P. Tallapragada, and J. Cortes, "Differentially private distributed convex optimization via functional perturbation." *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 395-408, 2018.

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

[21] Z. Huang, S. Mitra, N. Vaidya, "Differentially private distributed optimization." In *Proceedings of the 2015 International Conference on Distributed Computing and Networking*, pp.1-10, 2015.

[22] G. Shi, B. D. Anderson and U. Helmke, "Network flows that solve linear equations, *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 26592674, 2017.

[23] A. Nedic, A. Ozdaglar and P. A. Parrilo, Constrained consensus and optimization in multi-agent networks, *IEEE Trans. Autom. Control*, vol. 55, no. 4, pp. 922938, 2010.

[24] M. Mesbahi, M. Egerstedt. *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.

[25] C. Zhang, M. Ahmad, and Y. Wang, "ADMM based privacy-preserving decentralized optimization, *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 565580, 2019.

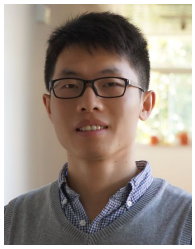
[26] Q. Li, H. Richard and M.G. Christensen. “Privacy-preserving distributed optimization via subspace perturbation: a general framework." *IEEE Transactions on Signal Processing*, vol. 68, pp. 5983-5996, 2020.
[27] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis." In *Proc. 3rd Theory of Cryptography Conference*, pp. 265-284, 2006.
[28] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, “Our data, ourselves: Privacy via distributed noise generation." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 486-503, 2006.
[29] Ye, M., and Hu, G, “Distributed Nash equilibrium seeking by a consensus based approach." *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp 4811-4818, 2017.
[30] Ye, M., Hu, G., Xie, L., and Xu, S, “Differentially Private Distributed Nash Equilibrium Seeking for Aggregative Games." *IEEE Transactions on Automatic Control*, 2021.
[31] Salehisadaghiani, F., and Pavel, L, “Distributed Nash equilibrium seeking: A gossip-based algorithm." *Automatica*, vol. 72, pp 209-216, 2016.
[32] Salehisadaghiani, F., and Pavel, L. “Distributed Nash equilibrium seeking in networked graphical games." *Automatica*, vol. 87, pp 17-24, 2018.
[33] Liang, S., Yi, P., and Hong, Y. “Distributed Nash equilibrium seeking for aggregative games with coupled constraints." *Automatica*, vol. 85, pp 179-185, 2017.
[34] Yi, P., and Pavel, L. “An operator splitting approach for distributed generalized Nash equilibria computation." *Automatica*, vol. 102, pp 111-121, 2019.
[35] Wahab, O. A., Bentahar, J., Otrok, H., and Mourad, A. “Resource-aware detection and defense system against multi-type attacks in the cloud: Repeated bayesian stackelberg game." *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 22, pp 605-622, 2019.
[36] Kumar, N., Misra, S., Chilamkurti, N., Lee, J. H., and Rodrigues, J. J. “Bayesian coalition negotiation game as a utility for secure energy management in a vehicles-to-grid environment". *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp 133-145, 2015.
[37] Pathak, M. A., and Raj, B. “Large margin Gaussian mixture models with differential privacy." *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp 463-469, 2012.
[38] S. Gade, A. Winnicki, and S. Bose, “On Privatizing Equilibrium Computation in Aggregate Games over Networks." In *Proc. of IFAC World Congress*, vol. 53, no.2, pp. 3272-3277, 2020.
[39] Leng, Y., Chen, Y., Dong, X., Wu, J., Shi, G. “Privacy Risks of Social Interaction Structure: Network Learning in Quadratic Games." *Available at SSRN*, 3875878, 2021.
[40] L. Xiang, J. Yang, B. Li, “Differentially-private deep learning from an optimization perspective." *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pp. 559-567, 2019.
[41] Y. Wang, A. Nedić, “Tailoring gradient methods for differentially-private distributed optimization." *IEEE Transactions on Automatic Control*, DOI: 10.1109/TAC.2023.3272968.
[42] M. O. Jackson, and Y. Zenou, *Games on Networks*. Handbook of Game Theory, vol. 4, Peyton Young and Shmuel Zamir, eds., 2014.

Lei Wang received the B.Eng. degree in automation from Wuhan University, China, in 2011, and Ph.D. degree in Control Science and Engineering from Zhejiang University, China in 2016. From December 2014 to December 2015, he visited C.A.SY.-DEIS, University of Bologna as a visiting PhD student.

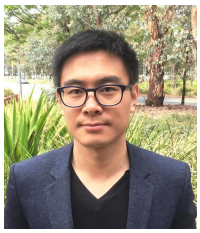
Lei held research positions with School of Electrical and Electronic Engineering at Nanyang Technological University, Singapore, School of Electrical Engineering and Computing at University of Newcastle, Australia, and Australian Centre for Field Robotics, The University of Sydney, Australia. Since November 2021 he has been a Hundred-Talent Researcher at College of Control Science and Engineering, Zhejiang University, China. His current research interests include robust nonlinear estimation and control, distributed computation and learning, privacy analysis and protection, with applications to fuel-cell systems, power systems and robotics.

Kemi Ding received the B.S. degree in Electronic and Information Engineering from Huazhong University of Science and Technology, China, in 2014 and the Ph.D. degree in the Department of Electronic and Computer Engineering from Hong Kong University of Science and Technology in 2018. Currently she is an Associate Professor in the department of System Design and Industrial Manufacturing. Prior to this, she was a postdoctoral researcher in the School of Electrical, Computer and Energy Engineering, Arizona State University from September 2018 to August 2019, and a postdoctoral researcher at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from August 2019 to October 2021. Her current research interests include security and privacy in Cyber-physical systems/Internet-of-things, intelligent control and decision, networked state estimation, game theory, and graph signal processing

Yan Leng is an Assistant professor in McCombs School of Business, the University of Texas at Austin. She is a core member in UT Machine Learning Lab. She is affiliated with the UT AI and Misinformation Initiative and MIT Media Lab. She received B.S. degree from School of Science at Beijing Jiaotong University. She received a Ph.D. degree from MIT Media Lab and dual Masters from Transportation engineering and Computer Science, both from MIT. She is a computational social scientist and network scientist. She is interested in using econometrics and developing machine learning tools to study human and organizational behaviors over networks.



Xiaoqiang Ren is a professor at the School of Mechatronic Engineering and Automation, Shanghai University, China. He received the B.E. degree in Automation from Zhejiang University, Hangzhou, China, in 2012 and the Ph.D. degree in control and dynamic systems from Hong Kong University of Science and Technology in 2016. Prior to his current position, he was a postdoctoral researcher in the Hong Kong University of Science and Technology in 2016, Nanyang Technological University from 2016 to 2018, and KTH Royal Institute of Technology from 2018 to 2019. His research interests include security of cyber-physical systems, sequential decision, and networked estimation and control.



Guodong Shi received the B.Sc. degree in mathematics and applied mathematics from the School of Mathematics, Shandong University, Jinan, China in 2005, and the Ph.D. degree in systems theory from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China in 2010.

From 2010 to 2014, he was a Postdoctoral Researcher at the ACCESS Linnaeus Centre, KTH Royal Institute of Technology, Stockholm, Sweden. From 2014 to 2018, he was with the Research School of Engineering, The Australian National University, Canberra, ACT, Australia, as a Lecturer and then Senior Lecturer, and a Future Engineering Research Leadership Fellow. Since 2019 he has been with the Australian Center for Field Robotics, The University of Sydney, NSW 2008, Sydney, Australia. His research interests include distributed control systems, quantum networking and decisions, and social opinion dynamics.