Differentially private Nash equilibrium seeking for networked aggregative games

Maojiao Ye, Guoqiang Hu, Lihua Xie and Shengyuan Xu

Abstract—This paper considers the privacy-preserving Nash equilibrium seeking strategy design for a class of networked aggregative games, in which the players’ objective functions are considered to be sensitive information to be protected. In particular, we consider that the networked game is free of central node and the aggregate information is not directly available to the players. As there is no central authority to provide the aggregate information required by each player to update their actions, a dynamic average consensus protocol is employed to estimate it. To protect the players’ privacy, we perturb the transmitted information among the players by independent random noises drawn from Laplace distributions. By synthesizing the perturbed average consensus protocol with a gradient algorithm, distributed privacy-preserving Nash equilibrium seeking strategies are established for the aggregative games under both fixed and time-varying communication topologies. With explicit quantifications of the mean square errors, the convergence results of the proposed methods are presented. Moreover, it is analytically proven that the proposed algorithm is $\epsilon$-differentially private, where $\epsilon$ depends on the stepsize of the gradient algorithm and the scaling parameter of the random variables. The presented results indicate that there is a tradeoff between the convergence accuracy and the privacy level. Lastly, a numerical example is provided for the verification of the proposed methods.

Index Terms—Nash equilibrium seeking; privacy protection; differential privacy; random variable.

I. INTRODUCTION

Privacy has become a critical concern for many practical systems that involve sensitive data transmission and collection. Wireless sensor networks [1], smart grids [2], social networks [3], just to name a few, are typical examples that are in urgent need of privacy protection techniques. Inspired by the fact that privacy preservation is pivotal in information-sensitive systems, privacy protection methods have gained increasing attention in recent years. For instance, in the field of database and data mining, cryptographic secure multiparty computation methods, random perturbation techniques and $l$-diversity, $k$-anonymity based algorithms were adopted for information sharing systems, data collection systems and data publishing systems, respectively [1]. Homomorphic encryption was adapted for privacy protection in smart grids in [2]. Randomization, $k$-anonymity and generalization-based approaches can be utilized for privacy protection in social networks [3]. Motivated by the importance of privacy protection, this paper aims to achieve the distributed Nash equilibrium seeking for networked aggregative games with privacy guarantees.

In many practical situations, the utilities associated with the interacting decision-makers rely both on the decision-maker’s own action and an aggregate of all the decision-makers’ actions. For example, in the energy consumption model described in [8], the utilities of the electricity users are determined by the user’s own energy consumption as well as the total energy consumption in the electricity market. Cournot price/quantity competitions among multiple oligopolistic firms fall into similar scenario [4]. In factory production, the utility of each manufactory relies on the averaged output of all the engaged manufactories and the manufactory’s own production [5]. In addition, public good provision models and many other examples are also of aggregative nature, i.e., the interacting participants affect each other through a specific aggregate of their actions rather than in an arbitrary fashion [6]. Aggregative games serve as powerful game theoretic models to accommodate these competitive circumstances with aggregative interactions among multiple decision-makers. Motivated by the wide applications of aggregative games in distributed systems, Nash equilibrium seeking for aggregative games on communication graphs is attracting increasing attention in recent years [7]-[11].

A discrete-time method was proposed in [7] for networked aggregative games and a continuous-time counterpart was provided in [8] considering their applications for demand response in smart grids. A gossip-based algorithm was proposed to achieve distributed Nash equilibrium seeking in an asynchronous fashion in [9]. Coupled constraints were further addressed in [10]. The authors in [11] considered quadratic quasi-aggregative games, in which the players’ objective functions depend on the players’ actions and an aggregate of its neighbors’ actions. From the perspective of privacy issues, the works in [12][13] shed some light on the privacy protection for aggregative games. However, in the mechanisms of the game, there is a mediator/weak mediator, that can receive information from the players and give suggested actions for the players, to induce the players’ behaviours. Hence, the methods in [12][13] are not distributed. To achieve distributed Nash equilibrium seeking for networked games, the players usually need to broadcast their local information to their neighbors via local communication.
networks. The information dissemination among the players may raise privacy concern for the players. Nevertheless, to the best of the authors’ knowledge, privacy issues have rarely been explored for distributed Nash equilibrium seeking schemes though it is a problem of significant interest. Motivated by the above observation, this paper considers privacy-preserving distributed Nash equilibrium seeking for networked aggregative games by utilizing the notion of differential privacy [21].

Differential privacy has been widely adopted to describe the privacy level in many situations that include sensitive information. For example, the differential privacy of the agents engaged in distributed optimization problems was established in [14]-[17]. In [14], random noises were utilized for the protection of the agents’ objective functions. Based on the notion of differential privacy, the tradeoff between the convergence accuracy and the privacy level was analyzed. In [15], the constraints of the optimization problem were considered to be the private information to be protected. Based on the stochastic gradient method, a private optimization algorithm was developed by introducing additive noises. Instead of probing the transmitted messages, the authors in [16] proposed a functional perturbation algorithm which ensures that the inaccuracy of the optimization algorithm is only resulted from the introduced noises. In [17], both the agents’ states and moving directions were masked by random noises to achieve the privacy protection of the agents’ local objective functions. Differentially private average consensus protocols have also been widely studied (see e.g., [18]-[20], to mention just a few). For instance, the agents’ initial states were considered to be private information to be protected in the average consensus problems in [18], where the authors developed an asymptotically convergent algorithm to achieve privacy protection. Both a non-exact convergent algorithm and an almost surely convergent algorithm were established to achieve differentially private average consensus in [19]. Moreover, differential privacy has been extensively investigated in the area of database and data mining. Interested readers are referred to [21] for a survey on differential privacy.

To shed some light on privacy-protected Nash equilibrium seeking for aggregative games under distributed communication networks, this paper proposes a distributed algorithm by perturbing the transmitted information among the players using random variables. Moreover, motivated by the observation that differential privacy is robust against the auxiliary information exposed to the adversary, we adopt it to describe the players’ privacy level in this paper. In brief, the main contributions of the paper are summarized as follows.

1) This paper considers privacy-preserving distributed Nash equilibrium seeking for networked aggregative games. To achieve the goal, we employ a dynamic average consensus protocol for the distributed estimation of the players’ aggregate actions. To protect the players’ privacy, the information transmitted among the players in the consensus part is perturbed by independent random noises drawn from Laplace distributions. By utilizing the perturbed consensus protocol and a gradient method with a decaying stepsize, distributed privacy-preserving Nash equilibrium strategies are established for games under fixed and time-varying communication graphs, respectively.

2) The convergence result and the privacy level of the proposed methods are analytically investigated. In particular, the mean square error bound and privacy parameter are explicitly quantified. The presented results illustrate that the privacy level depends on the selection of the initial stepsize, the decaying rate of the stepsize as well as the scaling parameter of the random variables. Moreover, it is shown that there is a tradeoff between the convergence accuracy and the privacy level.

The rest of the paper is organized as follows. Section II provides some preliminaries and formulates the considered problem. The main results are given in Section III, where the distributed algorithm is presented with its convergence accuracy and privacy level successively investigated. Moreover, the results under fixed communication topologies are extended to time-varying communication topologies in Section IV. In Section V, a numerical example is provided to verify the effectiveness of the proposed method. Lastly, conclusions are drawn in Section VI.

Notations: In this paper, we use $\mathbb{R}$ and $\mathbb{R}_+$ to denote the set of real numbers and positive real numbers, respectively. Moreover, $\mathbb{Z}^+$ denotes the set of non-negative integers. Let $v$ be a vector or matrix, then $\|v\|$ denotes the $\ell_2$-norm of $v$. Moreover, $\|v\|_{\infty}$ denotes the $\ell_\infty$-norm of $v$. We say that a random variable $w \sim \text{Lap}(b)$, where $b \in \mathbb{R}_+$, if its probability density function is

$$
\mathcal{L}(w, b) = \frac{1}{2b} e^{-\frac{|w|}{b}}.
$$

In addition, $\mathbb{E}(\Phi)$ is the expectation of $\Phi$. The partial derivative of $f_i(x)$ with respect to $x_j$ is denoted as $\nabla_i f_i(x)$, where $x = [x_1, x_2, \cdots, x_N]^T$. Moreover, $1_N$ denotes an $N$-dimensional column vector whose elements are all 1 and the transpose of $\Psi$, where $\Psi$ is either a matrix or a vector, is denoted as $\Psi^T$. The notation $[g_i]_{vec}$ for $i \in \{1,2,\cdots,N\}$ denotes a column vector whose $i$th element is $g_i$. For a sequence $g(k)$, where $k \in \{1,2,3,\cdots\}$ and $g(k)$ is either a vector or a scalar, $g(\infty) = \lim_{k \to \infty} g(k)$ given that $\lim_{k \to \infty} g(k)$ exists. The maximum and minimum eigenvalues of a symmetric matrix $P$ are denoted as $\lambda_{\text{max}}(P)$ and $\lambda_{\text{min}}(P)$, respectively. For a matrix $Q$, $[Q]_{ij}$ denotes the entry on the $i$th row and $j$th column of $Q$. In addition, for $l_i \in \mathbb{R}$, $i \in \{1,2,\cdots,N\}$, the maximum and minimum values of $l_i$ are denoted as $\max_{i \in \{1,2,\cdots,N\}} \{l_i\}$ and $\min_{i \in \{1,2,\cdots,N\}} \{l_i\}$, respectively.

II. PRELIMINARIES AND PROBLEM FORMULATION

A. Preliminaries

In the following, we provide some preliminaries on game theory and differential privacy.
1) Game Theory: The following game related definitions are adopted from [8].

Definition 1: (A Normal Form Game) A game in a normal form is defined as a triple $\Gamma = \{V, X, f\}$, where $V = \{1, 2, \ldots, N\}$ is the set of players, $X = X_1 \times X_2 \cdots \times X_N$, $X_i \subseteq \mathbb{R}$ is the action set of player $i$ and $f = (f_1, f_2, \cdots, f_N)$, where $f_i$ is the cost function of player $i$.

Definition 2: (Nash Equilibrium) Nash equilibrium is an action profile on which no player can reduce its cost by unilaterally changing its own action, i.e., an action profile $x^* = (x^*_1, x^*_2) \in X$ is a Nash equilibrium if for $i \in V$,

$$f_i(x^*_1, x^*_{-i}) \leq f_i(x_i, x^*_{-i}),$$

for $x_i \in X_i$, where $x_{-i} = [x_1, x_2, \cdots, x_{i-1}, x_{i+1}, \cdots, x_N]^T$.

Definition 3: (Aggregative Game) A game $\Gamma$ is aggregative if there exists an aggregate function $l(x): X \subseteq \mathbb{R}$, which is continuous, additive and separable, such that there are functions $\tilde{f}_i(x_i, l(x))$, $i \in V$ that satisfy

$$\tilde{f}_i(x_i, l(x)) = f_i(x_i, x_{-i}), \quad \forall x \in X.$$ (2)

Without loss of generality, we consider that $l(x) = \frac{1}{N} \sum_{i=1}^{N} x_i$ in this paper.

2) Differential Privacy: Differential privacy serves as a mathematical quantification on the level of the engaged individuals’ privacy guarantee in a statistical database. It provides a rigorous and formal mathematical formulation on the privacy of the sensitive data. We refer readers to [21] for more detailed elaborations on differential privacy and give the subsequent definitions for clarity of presentation.

Definition 4: (Adjacency) Two function sets $F^{(1)} = \{f^{(1)}_1, f^{(1)}_2, \cdots, f^{(1)}_N\}$, $F^{(2)} = \{f^{(2)}_1, f^{(2)}_2, \cdots, f^{(2)}_N\}$ are said to be adjacent if there exists some $i_0 \in V$ such that $f^{(1)}_i = f^{(2)}_i$, $\forall i \neq i_0$, and $f^{(1)}_{i_0} \neq f^{(2)}_{i_0}$ [14][17].

Definition 5: ($\epsilon$-Differential Privacy) Given a positive constant $\epsilon$, adjacent function sets $F^{(1)}$, $F^{(2)}$ and any observation $O$, the algorithm is $\epsilon$-differentially private if

$$\mathbb{P}\{F^{(1)}|O\} \leq e^\epsilon \mathbb{P}\{F^{(2)}|O\},$$

where $\mathbb{P}\{F^{(j)}|O\}$ for $j \in \{1, 2\}$ is the conditional probability representing the probability of inferring $F^{(j)}$ from the observation $O$ [14][17].

Remark 1: The above defined $\epsilon$-differential privacy illustrates that from the sequences of observations, the adversary could not distinguish between the two function sets with a high probability. Hence, it is challenging for the adversary to identify the players’ sensitive information, which further indicates that the players are protected from information leakage. Note that a smaller $\epsilon$ indicates a higher level privacy.

B. Problem formulation

Problem 1: Consider an aggregative game in which player $i$ intends to

$$\min_{x_i} f_i(x_i, x_{-i})$$

where

$$f_i(x_i, x_{-i}) = \tilde{f}_i(x_i, \bar{x}),$$

and $\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$ for $i \in V$. Suppose that there is no central authority to broadcast $\bar{x}$ and the players can communicate with each other via a communication graph $G$.

The objective of this paper is to design a Nash equilibrium seeking strategy for the aggregative game such that

1) Given any positive constant $\epsilon$, the strategy can be $\epsilon$-differentially private by tuning the control parameters.
2) The players’ actions can be driven to a neighborhood of the Nash equilibrium point in the mean square sense, $\lim_{k \to \infty} \mathbb{E}[\|x(k) - x^*\|^2] \leq D$, where $D$ is a positive constant that is as small as possible;

Remark 2: Note that the considered aggregative games are practically inspired by the fact that in many decision-making processes (e.g., energy consumption control, Cournot quantity competitions, public good provision, factory production, to mention just a few), the decision-makers affect the others via their averaged/aggregate behaviors. Moreover, different from the previous works on distributed Nash equilibrium seeking for aggregative games [7]-[11], the objective of this paper includes privacy protection for the players’ cost functions $f_i(x_i, x_{-i}), i \in V$.

For notational convenience, let $x = [x_1, x_2, \cdots, x_N]^T$ and with a slight abuse of notation, $f_i(x_i, x_{-i})$ and $\nabla_i f_i(x_i, x_{-i})$ might be written as $f_i(x)$ and $\nabla_i f_i(x)$, respectively in the rest of the paper.

The following assumptions (see e.g., [25]) will be utilized to establish the main results of the paper.

Assumption 1: The players’ objective functions are twice continuously differentiable functions and $\nabla_i f_i(x)$ is globally Lipschitz for $i \in V$, i.e., there exists a positive constant $l_i$ such that

$$||\nabla_i f_i(x) - \nabla_i f_i(y)|| \leq l_i ||x - y||,$$ (6)

for $x, y \in \mathbb{R}^N, i \in V$.

Assumption 2: There exists a positive constant $m$ such that for $x, y \in \mathbb{R}^N$,

$$(x - y)^T (g(x) - g(y)) \geq m ||x - y||^2,$$ (7)

where $g(x) = [\nabla_1 f_1(x), \nabla_2 f_2(x), \cdots, \nabla_N f_N(x)]^T$.

Remark 3: The strong monotonicity condition in Assumption 2 characterizes a global Nash equilibrium, i.e., the Nash equilibrium is unique under Assumption 2. In addition, by Assumption 2

$$g(x) = 0_N,$$ (8)

if and only if $x = x^*$. Note that it is a widely adopted assumption in the existing literature and we refer interested readers to [31] for more insights on the assumption.

Assumption 3: $\nabla_i f_i(x)$ for $i \in V$ are uniformly bounded, i.e., there exists a positive constant $C$ such that for $x \in \mathbb{R}^N$,

$$|\nabla_i f_i(x)| \leq C, \quad \forall i \in V.$$

III. PRIVACY-PRESERVING NASH EQUILIBRIUM SEEKING UNDER FIXED COMMUNICATION GRAPHS

In this section, a privacy-preserving distributed Nash equilibrium seeking strategy will be proposed for games under a fixed undirected communication graph $G$, which is defined
as $G = \{V, E\}$. Moreover, $V = \{1, 2, \ldots, N\}$ denotes the set of vertices and $E \subseteq V \times V$ is the set of edges. In this way, player $j$ can communicate with player $i$ if and only if $(j, i) \in E$. Associate with $G$ a weight matrix $A = [a_{ij}]$ whose element on the $i$th row and $j$th column is $a_{ij}$. In this section, we suppose that $G$ and $A$ satisfy the following assumption:

Assumption 4: The communication graph $G$ is undirected and connected. Moreover, $A$ satisfies

1. $a_{ii} > 0$, $a_{ij} > 0$ if $(j, i) \in E$ and $a_{ij} = 0$ if $(j, i) \notin E$.
2. $A$ is doubly stochastic, i.e., $A1_N = 1_N$ and $1_N^T A = 1_N^T$.

Let $\{\lambda_i\}_{i=1}^N$ be the eigenvalues of $A$ and suppose that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. Then, by Assumption 4, $\lambda_1 = 1$, $\lambda_2 < 1$, $\lambda_N > -1$. Moreover, the following lemma holds.

Lemma 1: [32][33] Suppose that Assumption 4 is satisfied. Then,

$$\left\| \left( A^k - \frac{1}{N} 1_N^T N \right) \right\| = \left\| \left( A - \frac{1}{N} 1_N^T N \right)^k \right\| \leq \gamma^k, \quad (9)$$

where $\gamma$ is a positive constant such that

$$\rho \left( A - \frac{1}{N} 1_N^T N \right) \leq \gamma < 1, \quad (10)$$

and $\rho \left( A - \frac{1}{N} 1_N^T N \right)$ is the spectral radius of $A - \frac{1}{N} 1_N^T N$.

A. Method development

As there is no central authority to broadcast $\bar{x}(k)$ to the players, we design a strategy by utilizing a synthesis of consensus protocols and optimization algorithms as in [7]-[8]. Moreover, to protect the players’ privacy, we utilize independent random variables to perturb the transmitted information among the players in the average consensus protocol. More specifically, each player $i, i \in V$ can update its action according to

$$x_i(k+1) = x_i(k) - \alpha_k g_i(x_i(k), y_i(k)), \quad (11)$$

where $k \in \mathbb{Z}^+$, $\alpha_k = cq^k$, $c \in \mathbb{R}^+$, $q \in (0, 1)$ and $g_i(x_i, y_i) = \left( \frac{\partial l_i(x_i, \bar{x})}{\partial x_i} + \frac{\partial l_i(x_i, \bar{x})}{\partial x_i} \right) \big|_{\bar{x}=y_i}$. Moreover, $y_i(k)$ is an intermediate variable updated according to

$$y_i(k+1) = \sum_{j=1}^N a_{ij} p_j(k) + x_i(k+1) - x_i(k), \quad (12)$$

in which $y_i(0) = x_i(0)$, $p_j(k) = y_i(k) + w_i(k)$, $w_i(k) \sim Lap(\theta_k)$ for $i \in V$ are independent random variables, $\theta_k = dq^k$, $d \in \mathbb{R}^+$ and $q \in (q, 1)$. The steps of the designed algorithm are described as follows.

Privacy-preserving distributed Nash seeking:

Initialization: Choose $x_i(0) \in \mathbb{R}$ and $y_i(0) = x_i(0)$. Iterations:

1. Define $p_i(k) = y_i(k) + w_i(k)$
2. Update $x_i(k)$ according to
   $$x_i(k+1) = x_i(k) - \alpha_k g_i(x_i(k), y_i(k))$$
3. Update $y_i(k)$ according to
   $$y_i(k+1) = \sum_{j=1}^N a_{ij} p_j(k) + x_i(k+1) - x_i(k)$$

Let $x(k) = [x_1(k), x_2(k), \ldots, x_N(k)]^T$, $y(k) = [y_1(k), y_2(k), \ldots, y_N(k)]^T$, $w(k) = [w_1(k), w_2(k), \ldots, w_N(k)]^T$ and $p(k) = [p_1(k), p_2(k), \ldots, p_N(k)]^T$. Then, the concatenated vector form of (11)-(12) is

$$x(k+1) = x(k) - \alpha_k [g_i(x_i(k), y_i(k))]_{vec}$$
$$y(k+1) = A p(k) + x(k+1) - x(k). \quad (13)$$

Remark 4: In this paper, we suppose that there is no central authority to broadcast $\bar{x}(k)$ to the players. Hence, player $i, i \in V$ would generate a local variable $y_i(k)$ to estimate $\bar{x}(k)$. Moreover, the update of $y_i(k)$ in (12) is motivated by the dynamic average consensus protocol in [8][23]. However, in the dynamic average consensus protocol of [8], the players communicate with their neighbors on their estimates of $x(k)$, which may raise privacy concern. Hence, in (12), we perturb their transmitted information by utilizing independent random variables. Moreover, different from the continuous-time scenario proposed in our previous work in [8], we adopt a decaying stepsize in the presented algorithm to release the side-effect of the random noises on the convergence properties to some extent.

Remark 5: In [28], the authors provided necessary and sufficient conditions for general noise adding mechanisms to achieve differential privacy. It was shown that the probability density function of the added noises should have zero measure for the set of zero-points and the relative probability density in the considered adjacent sets should be upper bounded by a positive constant (see the conditions in Theorem 3.1 of [28] for accurate mathematical descriptions on the conditions). In addition, Laplace distribution was shown to satisfy the given conditions. Hence, we follow the existing works to adopt noises drawn from Laplace distributions with a decaying parameter to mask the transmitted information.

B. Analysis on the disagreement of estimates

In this section, we provide a bound for the expectation of the absolute difference between $y_i(k)$ and the actual aggregate action $\bar{x}(k)$. The following lemma is given to support the quantification of the estimation error.

Lemma 2: Suppose that Assumption 4 is satisfied. Then, for each nonnegative integer $k$,

$$E(\left| \left[ 1_N^T y(k) - 1_N^T x(k) \right] \right|) \leq \frac{Nd(1-q^k)}{1-q}. \quad (14)$$

Proof: By (13), we see that

$$1_N^T y(k+1) = 1_N^T (y(k) + w(k)) + 1_N^T (x(k+1) - x(k)). \quad (15)$$
Hence,
\[ 1_{N}^{T}y(k+1) - 1_{N}^{T}x(k+1) = 1_{N}^{T}(y(k) - x(k)) + 1_{N}^{T}w(k), \]
and
\[ |1_{N}^{T}y(k+1) - 1_{N}^{T}x(k+1)| \leq |1_{N}^{T}(y(k) - x(k))| + |1_{N}^{T}w(k)|. \]
Taking expectations on both sides of (16) gives
\[ \mathbb{E}(|1_{N}^{T}y(k+1) - 1_{N}^{T}x(k+1)|) \leq \mathbb{E}(|1_{N}^{T}(y(k) - x(k))|) + \mathbb{E}(|1_{N}^{T}w(k)|), \]
Noticing that \( y(0) = x(0), \)
\[ \mathbb{E}(|1_{N}^{T}y(k+1) - 1_{N}^{T}x(k+1)|) \leq \sum_{j=0}^{k} \mathbb{E}(1_{N}^{T}w(j)) = \frac{Nd(1 - \bar{q}^{k+1})}{1 - \bar{q}} \]
where the last inequality is derived by utilizing \( \mathbb{E}(|w(j)|) = dq^{j} \) for \( j \in \mathcal{V}. \)

Remark 6: Actually, by mathematical induction, it can be obtained that
\[ \mathbb{E}(1_{N}^{T}y(k) - 1_{N}^{T}x(k)) = 0, \]
for all nonnegative integer \( k. \) However, due to the effect of the added noises, we can only conclude that \( \mathbb{E}(1_{N}^{T}y(k) - 1_{N}^{T}x(k)) \) is bounded by \( \frac{Nd(1 - \bar{q}^{k})}{1 - \bar{q}} \) as indicated in Lemma 2. The bias of \( \mathbb{E}(|1_{N}^{T}y(k) - 1_{N}^{T}x(k)|) \) would result in a convergence error as indicated in the following theorems.

Based on Lemma 2, the following theorem which establishes the estimation error bound can be obtained.

Theorem 1: Suppose that Assumptions 3 and 4 are satisfied.
Then, for each positive integer \( k, \)
\[ \mathbb{E}(|y_{i}(k) - \bar{y}(k)|) \leq \sqrt{N} \left( \frac{(N-1)}{N} C_{1} \gamma^{k+1} + \frac{2(N-1)\sqrt{Nd}}{\gamma - \bar{q}} \sum_{l=0}^{k} \gamma^{k-l} \right) \]
where \( i \in \mathcal{V}, \) and \( C_{1} = \max_{n \in \mathcal{V}} |y_{n}(0)|, \) \( n \in \mathcal{V}. \)

Proof: For each positive integer \( k, \)
\[ \mathbb{E}(|y_{i}(k) - \bar{y}(k)|) = \mathbb{E}(|y_{i}(k) - 1_{N}^{T}y(k) + 1_{N}^{T}y(k) - 1_{N}^{T}x(k)|) \leq \frac{1}{N} \sum_{j=1}^{i} \mathbb{E}(|y_{j}(k) - y_{i}(k)|) \]
By (13), we get that
\[ y(k+1) = Ay(k) + w(k) + x(k+1) - x(k) = A^{2}y(k-1) + A^{2}w(k-1) + Aw(k) + A(x(k) - x(k-1)) + x(k + 1) - x(k) \]
By repeating the above process, it can be obtained that
\[ y(k+1) = A^{k+1}y(0) + \sum_{j=0}^{k} A^{k+1-j}w(j) + \sum_{j=1}^{k+1} A^{k+1-j}(x(j) - x(j-1)). \]
Hence, by (24),
\[ |y_{i}(k+1) - y_{j}(k+1)| \leq \sum_{n=1}^{N} |[A^{k+l}]_{in} - [A^{k+l}]_{jn}| |y_{n}(0)| \]
\[ + \sum_{n=1}^{N} \sum_{l=0}^{k} |[A^{k+l}]_{in} - [A^{k+l}]_{jn}| w_{n}(l) \]
\[ + \sum_{n=1}^{N} \sum_{l=1}^{k+1} |[A^{k+l}]_{in} - [A^{k+l}]_{jn}| |x_{n}(l) - x_{n}(l-1)|. \]
Note that
\[ \sum_{n=1}^{N} |A^{k+l} - \frac{1}{N}| \leq \left\| A^{k+l} - \frac{1}{N} \right\|_{\infty} \leq \sqrt{N} \left( \frac{\gamma^{k}}{\gamma - \bar{q}} \right) \]
where the last inequality is obtained by Lemma 4. Hence,
\[ |y_{i}(k+1) - y_{j}(k+1)| \leq 2\sqrt{NC_{1}} \gamma^{k+1} + 2\sqrt{NC} \sum_{l=1}^{k+1} \gamma^{k-l} \alpha_{l-1} \]
\[ + \sum_{n=1}^{N} \sum_{l=0}^{k} \left| [A^{k+l}]_{in} - [A^{k+l}]_{jn} \right| \left| w_{n}(l) \right|, \]
where \( C_{1} = \max_{n \in \mathcal{V}} |y_{n}(0)|, \) as \( |y_{n}(0)| \) for \( n \in \mathcal{V} \) are bounded.
Taking expectations on both sides of (27) gives
\[ \mathbb{E}(|y_{i}(k+1) - y_{j}(k+1)|) \leq 2\sqrt{NC_{1}} \gamma^{k+1} + 2\sqrt{NC} \sum_{l=1}^{k+1} \gamma^{k-l} \alpha_{l-1} \]
\[ + \sum_{n=1}^{N} \sum_{l=0}^{k} \left| [A^{k+l}]_{in} - [A^{k+l}]_{jn} \right| \mathbb{E}(|w_{n}(l)|). \]
Recalling that \( \mathbb{E}(|w_{n}(l)|) = dq^{l}, \) for \( n \in \mathcal{V}, \)
\[ \sum_{n=1}^{N} \sum_{l=0}^{k} \left| [A^{k+l}]_{in} - [A^{k+l}]_{jn} \right| \mathbb{E}(|w_{n}(l)|) \]
\[ = 2\sqrt{N} \gamma^{k+1} \gamma^{k+1} - \bar{q}^{k+1}. \]
Similarly,
\[
2\sqrt{NC} \sum_{t=1}^{k+1} \alpha_{t-1} = 2\sqrt{NCc(\gamma-1)}.
\] (30)

Hence,
\[
\mathbb{E}(\|y_t(k) - x_t(k)\|) \leq 2\sqrt{N(N-1)C_1} \gamma + 2\frac{(N-1)\sqrt{Nd\gamma}}{(\gamma-q)N} \gamma - q^k
\] (31)

by further utilizing the results in Lemma [2].

\[\hfill\]

C. Convergence analysis

In this section, we establish the convergence results for the proposed method.

**Theorem 2:** Suppose that Assumptions [1][4] are satisfied. Then,
\[
\lim_{k \to \infty} \mathbb{E}(\|x(k) - x^*\|^2) \leq C_2 e^{-\frac{\alpha_k}{\gamma}} + c^2 NC^2 \frac{1}{1-q^2} \Phi_1 + \Phi_2,
\] (32)

where
\[
\Phi_1 = 4 \max_{i \in V} \{l_i\}(N-1) \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) \times \left( \frac{C_1c}{1-q} + \frac{C_2q}{(1-q)(1-q^2)} \right),
\] (33)

and
\[
\Phi_2 = \max_{i \in V} \{l_i\} \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) \sqrt{N} \frac{2(N-1)\gamma}{(1-q)(1-q^2)} + \frac{\sqrt{N}}{(1-q)(1-q^2)},
\] (34)

where \(C_2 = \|x(0) - x^*\|\).

**Proof:** By (13), we can get that
\[
\|x(k+1) - x^*\| = \|x(k) - x^* - \alpha_k[g_t(x_t(k), y_t(k))]\|_{vec}.
\] (35)

Hence,
\[
\|x(k+1) - x^*\|^2 = \|x(k) - x^* - \alpha_k[g_t(x_t(k), y_t(k))]\|^2_{vec}
\] (36)

Noticing that \(g_t(x_t(k), y_t(k))\) is uniformly bounded by \(C\), we can get that \(\|g_t(x_t(k), y_t(k))\|_{vec} \leq NC^2\). Hence
\[
\|x(k+1) - x^*\|^2_{vec} \leq \alpha_k^2 NC^2.
\] (37)

Moreover,
\[
-2\alpha_k(x(k) - x^*)^T [g_t(x_t(k), y_t(k))]_{vec} = -2\alpha_k(x(k) - x^*)^T g_t(x(k))
\] (38)

\[
+ 2\alpha_k(x(k) - x^*)^T (g_t(x(k)) - [g_t(x_t(k), y_t(k))]_{vec})
\]

\[
\|x(k) - x^*\|^2 + 2\alpha_k(x(k) - x^*)^T (g_t(x(k)) - [g_t(x_t(k), y_t(k))]_{vec}).
\] (39)

Noticing that \(g_t(x_t(k))\) is globally Lipschitz with constant \(l_t\), we get that
\[
\|g_t(x(k)) - [g_t(x_t(k), y_t(k))]_{vec}\|_{vec} \leq \max_{i \in V} \{l_i\} \|y(k) - 1_N x_t(k)\|.
\] (40)

Therefore,
\[
-2\alpha_k(x(k) - x^*)^T [g_t(x_t(k), y_t(k))]_{vec}
\]

\[
\leq -2\alpha_k m \|x(k) - x^*\|^2 + 2\max_{i \in V} \{l_i\} \|x(k) - x^*\|^2 \|y(k) - 1_N x_t(k)\|
\] (41)

Moreover, as \(x(k+1) = x(k) - \alpha_k[g_t(x_t(k), y_t(k))]\|_{vec}
\]

\[
\|x(k+1) - x^*\| \leq \|x(k) - x^*\| + \alpha_k \sqrt{NC}.
\] (42)

Let \(C_2 = \|x(0) - x^*\|\), we have
\[
\|x(k+1) - x^*\|^2 \leq \|x(k) - x^*\|^2 - 2\alpha_k m \|x(k) - x^*\|^2 + \alpha_k^2 NC^2
\]

\[
+ 2\alpha_k \max_{i \in V} \{l_i\} \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) \|y(k) - 1_N x_t(k)\|
\] (43)

Taking expectations on both sides of (43) gives
\[
\mathbb{E}(\|x(k+1) - x^*\|^2) \leq (1 - 2\alpha_k m) \mathbb{E}(\|x(k) - x^*\|^2) + \alpha_k^2 NC^2
\]

\[
+ 2\alpha_k \max_{i \in V} \{l_i\} \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) \mathbb{E}(\|y(k) - 1_N x_t(k)\|)
\] (44)

By Theorem [1]
\[
2\alpha_k \max_{i \in V} \{l_i\} \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) \mathbb{E}(\|y(k) - 1_N x_t(k)\|)
\]

\[
\leq 2\alpha_k \max_{i \in V} \{l_i\} \left( \frac{C_2 + \frac{cC\sqrt{N}}{1-q}}{1-q} \right) (2N-1) \frac{\gamma^k}{\gamma - q^k} \gamma - q + \sqrt{N} \frac{2(N-1)\gamma}{\gamma - q^k} \frac{\gamma}{1-q}
\] (45)
Therefore,
\[
\mathbb{E}((x(k+1) - x^*)^2) \leq \prod_{j=0}^{\infty} (1 - 2\alpha_j m) \mathbb{E}((x(0) - x^*)^2) + \sum_{j=0}^{\infty} \alpha_j^2 NC^2 \\
+ \sum_{j=0}^{k} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) (2(N-1)\gamma^2 C_1 \\
+ \frac{2(N-1)\gamma^2}{\gamma - q^2} \left( \gamma^2 - q^2 \right) + \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} \right) .
\]
Let \( k \to \infty \), then
\[
\lim_{k \to \infty} \mathbb{E}((x(k) - x^*)^2) \leq \prod_{j=0}^{\infty} (1 - 2\alpha_j m) \mathbb{E}((x(0) - x^*)^2) + \sum_{j=0}^{\infty} \alpha_j^2 NC^2 \\
+ \sum_{j=0}^{\infty} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) (2(N-1)\gamma^2 C_1 \\
+ \frac{2(N-1)\gamma^2}{\gamma - q^2} \left( \gamma^2 - q^2 \right) + \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} \right) .
\]
in which
\[
\sum_{j=0}^{\infty} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) (2(N-1)\gamma^2 C_1 \\
+ \frac{2(N-1)\gamma^2}{\gamma - q^2} \left( \gamma^2 - q^2 \right) + \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} \right) = 4(N-1)C_1 \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{c}{1 - q}\gamma .
\]
and
\[
\sum_{j=0}^{\infty} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) 2(N-1)\gamma^2 \frac{\gamma^2 - q^2}{\gamma - q^2} \left( \gamma^2 - q^2 \right) + \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} = 4(N-1) \max_{i \in \mathcal{V}} \{l_i\} d\gamma \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{c\gamma}{(1-q)(1-q^2)} .
\]
In addition,
\[
\sum_{j=0}^{\infty} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{2(N-1)C_2 \gamma^2}{\gamma - q^2} \left( \gamma^2 - q^2 \right) = 4 \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{(N-1)C_2^2 q}{(1-q)(1-q^2)} ,
\]
and
\[
\sum_{j=0}^{\infty} 2\alpha_j \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} = 2 \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{\sqrt{N}d\gamma}{(1-q)(1-q^2)} .
\]
Rearranging these terms gives
\[
\lim_{k \to \infty} \mathbb{E}((x(k) - x^*)^2) \leq \prod_{j=0}^{\infty} (1 - 2\alpha_j m) \mathbb{E}((x(0) - x^*)^2) + \sum_{j=0}^{\infty} \alpha_j^2 NC^2 \\
+ \sum_{j=0}^{\infty} \frac{c^2 NC^2}{(1-q^2)^2} \frac{\gamma^2 - q^2}{\gamma - q} \left( \gamma^2 - q^2 \right) + \frac{\sqrt{N}d(1 - q^2)}{1 - q^2} .
\]
in which the last inequality is derived by utilizing \( 1 - \alpha_j m \leq e^{-\alpha_j m} \) and \( \mathbb{E}((x(0) - x^*)^2) \leq C_2^2 \). Moreover,
\[
\Phi_1 = 4 \max_{i \in \mathcal{V}} \{l_i\} \left( N-1 \right) \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) \frac{C_1 c}{(1-q)(1-q^2)} + \frac{C_2 q^2}{(1-q)(1-q^2)} ,
\]
and
\[
\Phi_2 = 2 \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{c\sqrt{N}}{1-q} \right) d\gamma \frac{2(N-1)\gamma}{(1-q)(1-q^2)} + \frac{\sqrt{N}d\gamma}{(1-q)(1-q^2)} .
\]
Remark 7: From the above analysis, it is clear that \( \lim_{k \to \infty} \mathbb{E}((x(k) - x^*)^2) \) is bounded by \( C_2^2 e^{-\alpha m} + \frac{e^2 NC^2}{1-q^2} + \Phi_1 + \Phi_2 \), where \( C_2^2 e^{-\alpha m} \) is resulted from the initial error. Moreover, \( e^2 NC^2 \) and \( \Phi_1 \) depend on stepsize selection. In addition, \( \Phi_2 \) is resulted from the added noises \( w_i(k), i \in \mathcal{V} \).

D. Differential privacy

In this section, we show that the proposed method is \( \varepsilon \)-differentially private. To analyze the privacy level for the proposed Nash equilibrium seeking strategy, we consider two adjacent function sets \( F^{(1)} = \{f^{(1)}_i\}_{i \in \mathcal{V}}, F^{(2)} = \{f^{(2)}_i\}_{i \in \mathcal{V}} \) where \( f^{(1)}_i = f^{(2)}_i \), \( \forall i \neq i_0 \), and \( f^{(1)}_i \neq f^{(2)}_i \) for some \( i_0 \in \mathcal{V} \). Note that if \( \nabla_i f^{(1)}_i = \nabla_i f^{(2)}_i \) for \( i = i_0 \), the two sequences generated by the proposed method under \( F^{(1)} \) and \( F^{(2)} \) would be the same by enforcing the added noises to be the same, indicating that the proposed method is of complete privacy. Hence, in the rest, we only consider the case in which \( \nabla_i f^{(1)}_i \neq \nabla_i f^{(2)}_i \) for \( i = i_0 \). In addition, the worst case scenario is considered, i.e., the adversary knows \( \mathcal{A}, x(0), \{f_i\}_{i \in \mathcal{V}}, \alpha_k \) and the distributions of the random variables. Moreover, the observations are \( \mathcal{O} = \{\mathcal{O}_k\}_{k=0}, \) where \( \mathcal{O}_k = \{p_k\} \).

Then, the following theorem can be derived.

Theorem 3: Suppose that Assumption 3 is satisfied. Then, the proposed method in (11)-(12) is \( \varepsilon \)-differentially private, where
\[
\epsilon = \frac{2eCq}{d\gamma(1-q^2)} .
\]

Proof: For any fixed initial state \( x(0) \), we see from (11)-(12) that
\[
x_i(1) = x_i(0) - \alpha_0 g_i(x_i(0), y_i(0)) ,
\]
and hence \( x_i(1) \) and \( x_i(1) - x_i(0) \) are fixed. Moreover,
\[
y_i(1) = \sum_{j=1}^{N} a_{ij} p_j(0) + x_i(1) - x_i(0),
\]
and hence if \( p_j(0) \) for \( j \in V \) are fixed, we get that \( w_i(0) \) and \( y_i(1) \) are fixed. Repeating the above analysis, we get that for any set of objective functions, if we fix the observation sequence, then, there exists a unique sequence \( x(k), y(k), w(k) \) for \( k \in \{0, 1, 2, \cdots \} \) that can generate the sequence of observation. Hence, under the set of objective functions \( F(l) \), \( l \in \{1, 2\} \), there exists a bijective mapping from the noise sequence to the set of observations. For notational convenience, denote the mapping as \( \Omega(l)(w), l \in \{1, 2\} \).

Moreover, for presentation clarity, we denote the sequence generated by the proposed method under \( F(1) \) as
\[
\begin{align*}
x_i(1)(k+1) &= x_i(1)(k) - \alpha_k g_i(1)(x_i(1)(k), y_i(1)(k)), \\
y_i(1)(k+1) &= \sum_{j=1}^{N} a_{ij} p_j(1)(k) + x_i(1)(k+1) - x_i(1)(k).
\end{align*}
\]
(58)

Correspondingly, the sequence generated by the proposed method under \( F(2) \) is given by
\[
\begin{align*}
x_i(2)(k+1) &= x_i(2)(k) - \alpha_k g_i(2)(x_i(2)(k), y_i(2)(k)), \\
y_i(2)(k+1) &= \sum_{j=1}^{N} a_{ij} p_j(2)(k) + x_i(2)(k+1) - x_i(2)(k).
\end{align*}
\]
(59)

As \( x_i(1)(0) = x_i(2)(0), y_i(1)(0) = y_i(2)(0) \), it can be easily obtained that for \( i \neq i_0 \),
\[
\begin{align*}
x_i(1)(k) &= x_i(2)(k), \\
y_i(1)(k) &= y_i(k)(k),
\end{align*}
\]
(60)

for all nonnegative integer \( k \), given that the two function sets generate the same observations. Therefore, to ensure that \( y_i(1)(k) + w_i(1)(k) = y_i(2)(k) + w_i(2)(k) \), we only need to enforce that
\[
w_i(1)(k) = w_i(2)(k),
\]
(61)
for \( i \neq i_0 \).

Moreover, for \( i = i_0 \), we enforce that
\[
\Delta w_i(k) = -\Delta y_i(k),
\]
and
\[
\Delta y_i(k+1) = \Delta x_i(k+1) - \Delta x_i(k) = -\alpha_k \Delta g_i(k),
\]
(63)

where
\[
\Delta g_i(k) = g_i(1)(x_i(1)(k), y_i(1)(k)) - g_i(2)(x_i(2)(k), y_i(2)(k))
\]
and \( x_i(1)(k) = x_i(2)(k) \).

Let \( w_i^{(l)}(k) = \left[w_i^{(l)}, w_i^{(l)}, \cdots, w_i^{(l)}(k)^T \right] \) and \( w_i^{(l)} = \left[w_i^{(l)}(k) \right]_{k=0}^{\infty} \) for \( l \in \{1, 2\} \). Moreover, let \( O^{(l)} \) be the sequence of observations under the function set \( F^{(l)} \). According to \([61]-[63]\), we know that for each \( w_i^{(1)} \), there exists a unique \( w_i^{(2)} \) such that \( O^{(1)} = O^{(2)} \). Let \( B(\cdot) \) be a mapping such that \( w_i^{(2)} = B(w_i^{(1)}) \) if and only if \( O^{(1)} = O^{(2)} \). Then, it is clear that \( B(\cdot) \) is bijective. Let \( \Gamma(l) = \{w_i^{(l)}(k)\}^{\infty}_{k=0} \), then, following the analysis in [17], it can be obtained that
\[
\begin{align*}
P \{ F^{(1)} | O \} &= \int_{\Gamma(1)} \prod_{i=1}^{N} \prod_{k=0}^{\infty} \mathcal{L}(w_i^{(1)}(k), \theta_k) d\omega^{(1)} \leq \prod_{k=0}^{\infty} e^{\frac{\Delta w_i(k)}{\alpha_k}},
\end{align*}
\]
(64)
in which
\[
\begin{align*}
\prod_{k=1}^{N} \prod_{k=0}^{\infty} \mathcal{L}(w_i^{(1)}(k), \theta_k) \\
&\leq \sum_{k=0}^{\infty} e^{-\frac{\Delta w_i(k)}{\alpha_k}} \leq e^{\sum_{k=0}^{\infty} \frac{\Delta w_i(k)}{\alpha_k}}.
\end{align*}
\]
(65)

By the boundedness of the gradient value, we get that
\[
\Delta w_i(k) \leq 2C\alpha_k.
\]

Therefore,
\[
e^{\sum_{k=0}^{\infty} \frac{\Delta w_i(k)}{\alpha_k}} \leq e^{2C\alpha_k}. \tag{66}
\]

By further noticing that \( \bar{q} \in (q, 1) \), we get that
\[
e^{\sum_{k=0}^{\infty} \frac{\Delta w_i(k)}{\alpha_k}} \leq e^{2C\alpha_k}. \tag{67}
\]

Note that \( i_0 \in V \) stands for any player engaged in the game, we can conclude that the privacy level of the whole system is \( \epsilon = \frac{2C\alpha_k}{\bar{q}(q-\bar{q})} \), i.e., the proposed method is \( \epsilon \)-differentially private.

Remark 8: In many existing works on distributed optimization and Nash equilibrium seeking, the decaying stepsize is required to satisfy
\[
\sum_{k=0}^{\infty} \alpha_k = \infty, \sum_{k=0}^{\infty} \alpha_k^2 < \infty, \tag{68}
\]
to establish the convergence results (see, e.g., [7][34]). However, in this paper, we adopt a decaying stepsize that satisfies
\[
\sum_{k=0}^{\infty} \alpha_k < \infty. \tag{69}
\]
Note that this is required to establish the \( \epsilon \)-differential privacy of the proposed method, i.e., differential privacy is not achievable with not summable stepsize in the proposed method. Therefore, the convergence accuracy is sacrificed to some extent for differential privacy. Note that this is in accordance with the “impossibility result for 0-LAS message perturbing algorithms” in [16] and some other existing results on differential privacy (see, e.g., [14]). The tradeoffs between the convergence property and differential privacy will be discussed in more details later.

Remark 9: In reality, communication channels are often subject to various kinds of noises during information dissemination (see e.g., [29]-[30] and the references therein). Therefore, if we can do some experiments to investigate the characteristics and properties of communication noises
in real communication channels, it would be an interesting open question to study whether it is possible to employ the noises in the communication channels to achieve differentially private Nash equilibrium seeking or not.

E. Tradeoffs between the accuracy and privacy level

From (72), it can be seen that

\[
\lim_{k \to \infty} E(\|x(k) - x^*\|^2) \leq D,
\]

where \(D = C_2^2 e^{-\frac{2\epsilon}{C_1}} + \frac{e^2 NC^2}{1 - q^2} + \Phi_1 + \Phi_2\) and is resulted from the added noises.

By Theorem 3 \(\epsilon = \frac{2\epsilon C q}{(q - q)}\). Therefore,

\[
d = \frac{2\epsilon C q}{(q - q)}.
\]

To see the tradeoff between the convergence accuracy and the privacy level, the accuracy bound \(D\) can be restated in terms of \(\epsilon\) as:

\[
D = C_2^2 e^{-\frac{2\epsilon}{C_1}} + \frac{e^2 NC^2}{1 - q^2} + \Phi_1 + \Phi_2,
\]

where \(\Phi_1\) is defined in (33) and,

\[
\Phi_2 = 2 \max_{i \in V}\left(\frac{C_2 + Cq\sqrt{N}}{1 - q} \frac{2Cq\tilde{q}q}{2(1 - q^2)}\right) \left(\frac{\sqrt{N}}{(1 - q^2)(1 - q^2)} + \frac{\sqrt{N}}{(1 - q)(1 - q)}\right).
\]

From (72), it can be seen that with \(q, \tilde{q}, c, q\) being fixed, \(D = O(\frac{1}{\epsilon})\), indicating that the accuracy of the proposed method becomes arbitrarily bad when the method is of complete privacy. Hence, there is a tradeoff between the convergence accuracy and the privacy level. However, the presented result preserves the following properties:

1) For any given \(\epsilon > 0\), \(c, d, \tilde{q}, q\) can be tuned such that the proposed method is \(\epsilon\)-differentially private;

2) If privacy is not concerned, then, for any given positive constant \(D, c, \tilde{q}, q\) can be tuned such that

\[
\lim_{k \to \infty} E(\|x(k) - x^*\|^2) \leq D.
\]

The first property can be easily obtained by (33). The second property is derived following the subsequent observations.

- For any bounded initial condition, \(C_2^2 e^{-\frac{2\epsilon}{C_1}}\) can be tuned to be arbitrarily small by adjusting \(c\) and \(q\) such that \(\frac{C_2^2}{1-q^2}\) is sufficiently large;

- Denote \(\frac{C_2^2}{1-q^2} = \zeta\). Then, for fixed and sufficiently large \(\zeta\),

\[
\frac{c}{1 - q^2} = \frac{\zeta(1 - q)}{1 - q^2},
\]

and

\[
\frac{C_2^2(1-q)}{1 - q^2} = \frac{\zeta^2(1 - q)}{1 - q^2}.
\]

Noticing that the partial derivatives of \(\frac{\zeta(1-q)}{1-q^2}\) and \(\frac{\zeta^2(1-q)}{1-q^2}\) with respect to \(q\) are negative for \(q \in (0, 1)\) and \(\lim_{q \to 1} \frac{\zeta(1-q)}{1-q^2} = 0, \lim_{q \to 1} \frac{\zeta^2(1-q)}{1-q^2} = 0\), it can be concluded that \(c\) and \(q\) can be adjusted such that \(\frac{c}{1-q^2}\) and \(\frac{C_2^2}{1-q^2}\) are sufficiently small with fixed \(\zeta\). Therefore, by such a tuning rule, \(\frac{C_2^2}{1-q^2} + \frac{e^2 NC^2}{1 - q^2} + \Phi_1\) can be adjusted to be arbitrarily small.

- \(\Phi_2\) depends on the level of privacy \(\epsilon\) and if privacy is not of concern, \(\epsilon\) can be chosen to be sufficiently large such that \(\Phi_2\) is sufficiently small.

From (72), we see that the accuracy of the proposed method depends on \(c, \epsilon, \tilde{q}, q\) and hence, we write \(D\) as \(D(c, \epsilon, \tilde{q}, q)\). With fixed requirement of privacy level (i.e., \(\epsilon\)), one can tune \(c, \tilde{q}, q\) by solving

\[
\min_{c, \tilde{q}, q} D(c, \epsilon, \tilde{q}, q),
\]

s.t. \(c > 0, q \in (0, 1), \tilde{q} \in (q, 1)\).

Moreover, noticing that for any fixed \(c\) and \(q\),

\[
\frac{\partial D}{\partial \tilde{q}} < 0,
\]

indicating that \(D\) is monotonically decreasing with any fixed \(c, q\). Hence, one can choose \(\tilde{q}\) to be sufficiently close to 1 as \(\tilde{q} \in (q, 1)\) and solve

\[
\min_{c, q} D(c, q),
\]

s.t. \(c > 0, q \in (0, \tilde{q})\),
to get the optimal \(c, q\).

IV. EXTENSIONS TO TIME-VARYING COMMUNICATION TOPOLOGIES

In the previous section, we suppose that the communication topology among the players is fixed, undirected and connected for presentation clarity. Actually, the proposed method can be slightly adapted to accommodate time-varying communication graphs that satisfy the following conditions:

Assumption 5: There exists a positive integer \(z\) such that \((\mathcal{V}, \bigcup_{k=1}^z \mathcal{E}_l)\) is connected for all nonnegative integer \(k\), in which \(\mathcal{G}_l = (\mathcal{V}, \mathcal{E}_l)\) is the undirected communication graph at time \(l\) and \(\mathcal{E}_l\) is the corresponding edge set at time \(l\).

Note that in Section III the communication graph is supposed to be connected at each time instant \(k = \{0, 1, 2, \cdots\}\). However, in this section, the communication condition is generalized to be time-varying and it is only required that there exists a positive integer \(z\) such that the joint graph \(\bigcup_{l=1}^z \mathcal{G}_l + k\) is connected for nonnegative integer \(k\).

Assumption 6: Let \(A(l)\) be the weight matrix associated with \(G_l\) that satisfies:

1) There exists a positive constant \(\delta\) such that \(a_{ii}(l) > \delta, a_{ij}(l) > \delta\) if \((j, i) \in \mathcal{E}_l\) and \(a_{ij}(l) = 0\) if \((j, i) \notin \mathcal{E}_l\);

2) \(A(l)\) is doubly stochastic, i.e., \(\sum_l A(l) = 1_N, A(l)1_N = 1_N\).

Let \(\Psi(k, s) = A(k)A(k-1)\cdots A(s)\) where \(k \geq s \geq 0\).

Then, under Assumptions 5 and 6, the following lemma can be obtained.

Lemma 3: [35] Let Assumptions 5 and 6 be satisfied. Then,

1) \(\lim_{k \to \infty} \Psi(k, s) = \frac{1}{N^{s+1}} 1_N\), \(\forall s \geq 0\);

2) For \(k \geq s \geq 0\), \(\|\Psi(k, s)\|_{\infty} \leq \frac{1}{\delta}, \|\Psi(k, s\|_{\infty} \leq \frac{1}{\delta} \sqrt{N^2 + N^2}\), where

\(\theta = (1 - \frac{\delta}{N^2})^{-\frac{1}{2}}, \beta = (1 - \frac{\delta}{N^2})\).
With time-varying communication topologies, the Nash equilibrium seeking strategy should be adapted as
\[
\begin{align*}
    x(k+1) &= x(k) - \alpha_k [g_i(x_i(k), y_i(k))]_{vec} \\
    y(k+1) &= A(k)p(k) + x(k+1) - x(k).
\end{align*}
\] 
(79)

Note that the variations of the communication graph will only affect the convergence results but not the differential privacy of the proposed method. Hence, in the following, only the convergence results are presented.

First, following the proof of Theorem 1, the subsequent result can be obtained.

**Theorem 4**: Suppose that Assumptions 5-6 are satisfied. Then, for each positive integer \(k\),
\[
\begin{align*}
    \mathbb{E}(\|y_i(k) - \bar{x}(k)\|) \\
    \leq & 2(N-1)\theta \beta^k C_1 + \frac{2(N-1)q\beta}{\beta - q}(\beta^k - \hat{q}^k) \\
    &+ \frac{2\theta(N-1)C\beta(\beta^k - q^k)}{\beta - q} + d(1 - q^k)\frac{1}{1 - \hat{q}}.
\end{align*}
\] 
(80)
for \(i \in \mathcal{V}\).

**Remark 10**: From Theorem 4, it can be seen that compared with the results under fixed communication topologies, the time-varying communication topology would affect the estimation speed.

Moreover, following Theorem 2, the subsequent convergence result can be obtained.

**Theorem 5**: Suppose that Assumptions 1-3 and 5-6 are satisfied. Then,
\[
\begin{align*}
    \lim_{k \to \infty} \mathbb{E}(\|x(k) - x^*\|^2) \\
    \leq & C_2^2 e^{-\frac{\bar{d}\beta}{2\beta - q}} + \frac{c^2 N C^2}{1 - \mu^2} + \Phi_1 + \Phi_2,
\end{align*}
\] 
(81)
where
\[
\Phi_1 = 4(N-1)\sqrt{N}\theta \max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{cC\sqrt{N}}{1 - \mu} \right)
\] 
(82)
and
\[
\Phi_2 = 2\max_{i \in \mathcal{V}} \{l_i\} \left( C_2 + \frac{cC\sqrt{N}}{1 - \mu} \right) \sqrt{N} \frac{\mu q^2}{1 - \mu^2} \\
\times \left( \frac{2(N-1)\theta \beta}{(1 - \mu)(1 - \beta \mu)} + 1 \right).
\] 
(83)

In this section, we consider the 5-player energy consumption game studied in [8]. In the energy consumption game, player \(i\)'s objective function is given by
\[
f_i(x) = (x_i - \hat{x}_i)^2 + (0.04 \sum_{i=1}^{5} x_i + 5) x_i,
\] 
(84)
in which \(\hat{x}_1 = 50, \hat{x}_2 = 55, \hat{x}_3 = 60, \hat{x}_4 = 65, \hat{x}_5 = 70\). As demonstrated in [8], the game has a unique pure-strategy Nash equilibrium at \(x^* = \{41.5, 46.4, 51.3, 56.2, 61.1\}\). In the following, fixed communication topologies and time-varying communication topologies will be considered successively.

**A. Nash equilibrium seeking under fixed communication topologies**

In the simulation, the players are supposed to communicate via a cycle depicted in Fig. 1. Correspondingly, the weight matrix is given as
\[
A = \begin{bmatrix}
0.5 & 0.2 & 0 & 0 & 0.3 \\
0.2 & 0.5 & 0.3 & 0 & 0 \\
0 & 0.3 & 0.5 & 0.2 & 0 \\
0 & 0 & 0.2 & 0.5 & 0.3 \\
0.3 & 0 & 0 & 0.3 & 0.4
\end{bmatrix},
\]
and \(c = 1, q = 0.9, d = 1, \bar{q} = 0.99\). Moreover, the proposed method is run for 2000 times for the observation of the simulation results. Fig. 2 shows the expectations of the players’ squared Nash equilibrium seeking errors, i.e., \(\mathbb{E}((x_i(k) - x_i^*)^2)\) for \(i \in \{1, 2, \cdots, 5\}\) from which we see that the proposed method drives \(\mathbb{E}((x_i(k) - x_i^*)^2)\) to a small neighborhood of zero. Fig. 3 (1) plots \(\mathbb{E}((y_i(k) - \bar{x}^*)^2)\) for \(i \in \{1, 2, \cdots, 5\}\) generated by the proposed method and Fig. 3 (2) shows \(\bar{y}_i(k) - \bar{x}^*\) for \(i \in \{1, 2, \cdots, 5\}\), where \(\bar{y}_i(k)\) denotes the averaged value of \(y_i(k)\) for the 2000 running times and \(\bar{x}^* = \frac{1}{5} \sum_{i=1}^{5} x_i^*\).

![Fig. 1: The communication graph for the players.](image)

![Fig. 2: The expectations of the players’ squared Nash equilibrium seeking errors, i.e., \(\mathbb{E}((x_i(k) - x_i^*)^2)\), \(i \in \{1, 2, \cdots, 5\}\), generated by the proposed method in (11)-(12).](image)
results. Fig. 4 plots $\mathbb{E}(\|x(\infty) - x^*\|^2)$. Roughly speaking, the figure shows that as $d$ increases, the upper bound of $\mathbb{E}(\|x(\infty) - x^*\|^2)$ increases, which illustrates the tradeoff between the privacy level and the convergence accuracy.

Fig. 4: The plot of $\mathbb{E}(\|x(\infty) - x^*\|^2)$ with $d$ varying from 0 to 3.

To observe the data distributions generated by the proposed method, we fix $d = 1$, $\tilde{q} = 0.99$ and run the proposed method for 20000 times. Fig. 5 plots the data distributions of $x_i(\infty)$ and its corresponding fitted density functions for $i \in \{1, 2, \cdots, 5\}$. Fig. 6 shows the data distributions of $y_i(\infty)$ and the plots of the corresponding fitted density functions for players 1-5, respectively. From Figs. 5-6, we see that the players’ actions converge to a small neighborhood of the Nash equilibrium with a high probability under the given parameters.

B. Nash equilibrium seeking under time-varying communication topologies

In the simulation, we suppose that the communication topology among the players switches between the two graphs depicted in Fig. 7. Correspondingly, we define

$$
A(k) = \begin{bmatrix}
0.3 & 0.3 & 0 & 0 & 0.4 \\
0.3 & 0.5 & 0.2 & 0 & 0 \\
0 & 0.2 & 0.5 & 0 & 0.3 \\
0 & 0 & 0 & 1 & 0 \\
0.4 & 0 & 0.3 & 0 & 0.3
\end{bmatrix},
$$

for $k \in \{0, 2, 4, 6, \cdots\}$. In addition,

$$
A(k) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0.7 & 0.3 \\
0 & 0 & 0 & 0.3 & 0.7
\end{bmatrix},
$$
for $k \in \{1, 3, 5, 7, \ldots \}$. For comparison convenience, the parameters are chosen as those in Section V-A. Moreover, the proposed method is run for 2000 times for the observation of the simulation results. Fig. 8 plots $E((x_i(k) - x^*)^2)$, $i \in \{1, 2, \cdots, 5\}$, and the two sub-figures in Fig. 9 depict $E((y_i(k) - \bar{x}^*)^2)$ and $\bar{y}_i(k) - \bar{x}^*$ for $i \in \{1, 2, \cdots, 5\}$, respectively. From Figs. 8-9 it can be seen that driven by the proposed method, $E((x_i(k) - x^*_i)^2)$, $E((y_i(k) - \bar{x}^*)^2)$ and $\bar{y}_i(k) - \bar{x}^*$ for $i \in \{1, 2, \cdots, 5\}$ would converge to a small neighborhood of zero. In addition, comparing Fig. 8 (2) with Fig. 9 (2), it is clear that the players can achieve the aggregate estimation at a faster speed under the fixed communication topology given in Fig. 1.

Fig. 7: (a) is the communication graph for the players at $k = \{0, 2, 4, 6, \cdots \}$ and (b) is the communication graph for the players at $k = \{1, 3, 5, 7, \cdots \}$.

Fig. 8: The expectations of the players’ squared Nash equilibrium seeking errors, i.e., $E((x_i(k) - x^*)^2)$, $i \in \{1, 2, \cdots, 5\}$, generated by the proposed method in (79).

To show the tradeoff between the privacy level and the convergence accuracy under the time-varying communication topologies, we vary $d$ from 0 to 3. Correspondingly, the plot of $E(||x(t) - x^*||^2)$ with different values of $d$ is given in Fig. 10 from which we see that $E(||x(t) - x^*||^2)$ increases with $d$.

Likewise, to observe the data distributions generated by the proposed method, we fix $d = 1$, $q = 0.99$ and run the proposed method for 20000 times. The data distributions of $x_i(\infty)$ and $y_i(\infty)$ for $i \in \{1, 2, \cdots, 5\}$, together with their corresponding fitted density functions are plotted in Figs. 11-12. Figs. 11-12 show that the players’ actions converge to a small neighborhood of the Nash equilibrium with a high probability under the given parameters.
Fig. 11: The plots of data distributions of $x_i(\infty)$ and the corresponding fitted density functions for players 1-5, generated by the proposed method in (79).

Fig. 12: The plots of data distributions of $y_i(\infty)$ and the corresponding fitted density functions for players 1-5, generated by the proposed method in (79).

VI. CONCLUSIONS

This paper considers privacy-preservation in the distributed Nash equilibrium seeking problem for networked aggregative games. To estimate the averaged value of the players’ actions, a dynamic average consensus protocol is employed in which the transmitted information is masked by independent random noises drawn from Laplace distributions. The random noises are included for the protection of the players’ objective functions. Moreover, with the estimated information, the gradient descent method with a decaying stepsize is implemented to optimize the players’ objective functions. The convergence property as well as the privacy level of the proposed method are analytically investigated. It is shown that there is a tradeoff between the convergence accuracy and the privacy level. Fixed communication topologies and time-varying communication topologies are addressed successively in the paper. Privacy-preserving Nash equilibrium seeking for more general games (see e.g., the games considered in [25]-[27]) will be included in our future works.

REFERENCES

[1] N. Li, N. Zhang, S. Das, B. Thuissingh, “Privacy preservation in wireless sensor networks: A state-of-the-art survey,” Ad Hoc Networks, vol. 7, no. 8, pp. 1501-1514, 2009.
[2] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, “UDP: Usage-based dynamic pricing with privacy preservation for smart grid,” IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 141-150, 2013.
[3] X. Wu, X. Ying, K. Liu, L. Chen, A Survey of Privacy-Preservation of Graphs and Social Networks, In: C. Aggarwal, H. Wang (eds) Managing and Mining Graph Data. Advances in Database Systems, vol. 40, Springer, Boston, MA, 2010.
[4] H. Agiza, A. Elsadany “Nonlinear dynamics in the Cournot duopoly game with heterogeneous players,” Physica A: Statistical Mechanics and its Applications, vol. 320, pp. 512-524, 2003.
[5] X. Wang, N. Xiao, L. Xie, E. Frazzoli, D. Rus, “Decentralised dynamic games for large population stochastic multi-agent systems,” IET Control Theory and Applications, vol. 9, no. 3, pp. 503-510, 2014.
[6] R. Corne, R. Hartley, “Aggregative public good games,” Journal of Public Economic Theory, vol. 9, no. 4, pp. 201-219, 2007.
[7] J. Koschal, A. Nedic, U. Shanbhag, “Distributed algorithms for aggregative games on graphs,” Operations Research, vol. 64, no. 3, pp. 680-704, 2016.
[8] M. Ye, G. Hu, “Game design and analysis for price-based demand response: an aggregate game approach,” IEEE Transactions on Cybernetics, vol. 47, no. 3, pp. 720-730, 2017.
[9] F. Salehisadaghiani and L. Pavel, “Distributed Nash equilibrium seeking: a gossip-based algorithm,” Automatica, vol. 72, pp. 209-216, 2016.
[10] S. Liang, P. Yi and Y. Hong, “Distributed Nash equilibrium seeking for aggregative games with coupled constraints,” Automatica, vol. 85, pp. 179-185, 2017.
[11] F. Parise, B. Gentile, S. Grammatico and J. Lygeros, “Network aggregative games: distributed convergence to Nash equilibria,” IEEE Conference on Decision and Control, pp. 2295-2300, 2015.
[12] R. Cummings, M. Kearns, A. Roth and Z. Wu, Privacy and Truthful Equilibrium Selection for Aggregative Games, in E. Markakis, G. Schaefer (eds) Web and Internet Economics, Lecture Notes in Computer Science, vol. 9470, Springer, Berlin, Heidelberg, 2015.
[13] P. Zhou, W. Wei, K. Bian, D. Wu, Y. Hu, Q. Wang, “Private and truthful aggregative game for large-scale spectrum sharing,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 2, pp. 463-477, 2017.
[14] Z. Huang, S. Mitra and N. Vaidya, “Differentially private distributed optimization,” International Conference on Distributed Computing and Networking, 2015.
[15] S. Han, U. Topcu, G. Pappas, “Differentially private distributed constrained optimization,” IEEE Transactions on Automatic Control, vol. 62, no. 1, pp. 50-64, 2017.
[16] E. Nozari, P. Tallapragada, 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.
[17] T. Ding, S. Zhu, J. He, C. Chen and X. Guan, “Consensus-based distributed optimization in multi-agent systems: convergence and differential privacy,” IEEE Conference on Decision and Control, pp. 3409-3414, 2018.
[18] Y. Mu, R. Murray, “Privacy preserving average consensus,” IEEE Transactions on Automatic Control, vol. 62, pp. 753-765, 2017.
[19] E. Nozari, P. Tallapragada, J. Cortes, “Differentially private average consensus: obstructions, trade-offs, and optimal algorithm design,” Automatica, vol. 81, pp. 221-231, 2017.
[20] N. Manita, C. Hadjicostis, “Privacy-preserving asymptotic average consensus,” European Control Conference, pp. 760-765, 2013.
[21] C. Dwork, Differential Privacy: A Survey of Results, in Theory and Applications of Models of Computation. New York, NY, USA: Springer-Verlag, pp. 1-19, 2008.
[22] Y. Lu and M. Zhu, “Privacy preserving distributed optimization using homomorphic encryption,” *Automatica*, vol. 96, pp. 314-325, 2018.

[23] M. Zhu, S. Martinez, “Discrete-time dynamic average consensus” *Automatica*, vol. 46, pp. 322-329, 2010.

[24] K. Ogata, *Discrete-time Control Systems*, 2nd Edition, Prentice Hall, 1994.

[25] M. Ye, G. Hu, “Distributed Nash equilibrium seeking by a consensus based approach,” *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4811-4818, 2017.

[26] M. Ye, G. Hu, and F. Lewis, “Nash equilibrium seeking for N-coalition non-cooperative games,” *Automatica*, vol. 95, pp. 266-272, 2018.

[27] M. Ye, G. Hu, F. Lewis, L. Xie, “A unified strategy for solution seeking in graphical N-coalition noncooperative games,” *IEEE Transactions on Automatic Control*, accepted, published online, DOI:10.1109/TAC.2019.2901820.

[28] J. He and L. Cai, “Differential private noise adding mechanism: basic conditions and its applications,” *Americal Control Conference*, pp. 1673-1678, 2017.

[29] T. Li and J. Zhang, “Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises,” *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2043-2057, 2010.

[30] Y. Long, S. Liu, and L. Xie, “Distributed consensus of discrete-time multi-agent systems with multiplicative noises,” *International Journal of Robust and Nonlinear Control*, vol. 25, pp. 3113-3131, 2015.

[31] F. Facchinei, J. Pang, *Finite-dimensional variational inequalities and complementarity problems-Volume I*, Springer, New York, NY, 2003.

[32] L. Xiao and S. Boyd, “Fast linear iterations for distributed averaging,” *Systems and Control Letters*, vol. 53, no. 1, pp. 65-78, 2004.

[33] B. Johansson, T. Keviczky, M. Johansson, and K. H. Johansson, “Subgradient methods and consensus algorithms for solving convex optimization problems,” *IEEE Conference on Decision and Control*, pp. 4185-4190, 2008.

[34] S. Ram, A. Nedic and V. Veeravalli, “Distributed stochastic subgradient projection algorithms for convex optimization,” *Journal of optimization theory and Applications*, vol. 147, no. 3, pp 516-545, 2010.

[35] A. Nedic, A. Ozheevsky, A. Ozdaglar, and J. Tsitsiklis, “Distributed Subgradient Methods and Quantization Effects,” *IEEE Conference on Decision and Control*, pp. 4177-4184, 2008.