Liang, Xueqin; Yan, Zheng

A Survey on Game Theoretical Methods in Human-Machine Networks

Published in:
Future Generation Computer Systems

DOI:
10.1016/j.future.2017.10.051

Published: 01/03/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Liang, X., & Yan, Z. (2019). A Survey on Game Theoretical Methods in Human-Machine Networks. Future Generation Computer Systems, 92, 674-693. https://doi.org/10.1016/j.future.2017.10.051

Future Generation Computer Systems 92 (2019) 674–693

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A survey on game theoretical methods in Human–Machine Networks

Xueqin Liang [a], Zheng Yan [a,b,*]

[a] State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, China
[b] Department of Communications and Networking, Aalto University, Finland

HIGHLIGHTS

- A thorough survey on game theoretical methods in Human–Machine Networks.
- A list of criteria to evaluate the performance of game theoretical analysis.
- A number of open issues future research directions to motivate future work.

ARTICLE INFO

Article history:
Received 30 July 2017
Received in revised form 19 September 2017
Accepted 28 October 2017
Available online 7 November 2017

Keywords:
Bitcoin
Crowdsourcing
Equilibrium
Game theory
Human–Machine Networks
Internet of Things (IoT)

ABSTRACT

A number of information and resource sharing systems arise and become popular with the rapid development of communication technologies and mobile smart devices. The interactions between humans and machines are intense and their synergistic reactions have attracted special attention for the reason of forming so called Human–Machine Networks (HMN). HMNs refer to these networks where humans and machines work together to provide synergistic effects on their payoffs. Game theory, which can capture the interactions among players dexterously, has been widely used in solving various problems in HMN systems from the view of economics. In this paper, we extensively review the literature about game theoretical methods in HMNs, in particular focusing on its typical systems such as crowdsourcing, an elemental HMN and Internet of Things (IoT), a hybrid HMN, as well as Bitcoin. We propose a series of requirements to evaluate existing work. For reviewing and analyzing each system, we specify application purposes, players, strategies, game models and equilibria based on our proposed requirements. In the sequel, we identify a number of common and distinct open issues in HMNs and point out future research directions.

1. Introduction

With the appearance and development of modern communications along with network technologies and emerging resource and information sharing platforms, the distance between humans has been greatly shortened. In the sequel, modern working and service style is being tremendously evolved. The appearance of digital machines has fundamentally improved productivity efficiency and living quality of human beings. What is more, some difficult and impossible missions for manpower alone can be solved by these networked machines easily. Furthermore, the extensive usage of machine learning and data mining ensures machines to be self-organized and self-healing for offering intelligent services. The synergy and innovations brought by the interactions among humans and machines have attracted special attentions of many scholars. Lots of literatures conceptualized Human–machine networks as a collective structure where humans and machines interact to produce synergistic and often unique effects [1,2]. Tsvetkova et al. [3] identified eight types of elemental HMNs: public resource computing, crowdsourcing, crowdsensing, web search engines, online markets, social media, online games and virtual worlds and mass collaboration. Among them, crowdsourcing and crowdsensing are two typical types of HMNs. They also pointed out that more and more hybrid HMNs that consist of two or more types of HMNs will emerge as time flies, like Internet of Things (IoT) and Bitcoin. In this paper we focus on crowdsourcing, IoT and Bitcoin due to their popularity in HMN development and evolution.

The emergence of crowdsourcing provides people a new way to solve complex or massive tasks by integrating distributed powers and resources of masses. Individuals can make the best use of their spare time or extra resources to obtain profits. Mobile crowdsourcing systems become more and more popular because of the exponential growth of the number of smart mobile devices with various kinds of sensors. The mobile devices can provide useful

* Corresponding author at: State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, China.
E-mail addresses: annabella93@foxmail.com (X. Liang), zyan@xidian.edu.cn (Z. Yan).

https://doi.org/10.1016/j.future.2017.10.051

information that is needed by a service. Although this information provision could cost a little, like battery and communication consumption, the mobile device users can gain some profits in return, which motivate them to contribute. Generally, a crowdsourcing system that provides a platform for collective wisdom and resources sharing can change people's life greatly since it changes the mode of information collection, mission fulfillment and service provision. It introduces a great potential for individual business running. A term that is highly related to crowdsourcing is crowdsensing. It refers to the crowdsourcing of sensor data gained from mobile devices. In this paper, for easy presentation, we do not specially distinguish them.

The success of a crowdsourcing system depends on the collaboration among crowdsourcers and workers that are task or mission contributors. If a crowdsourcing platform cannot attract enough workers to collaborate for working out the task it outsources, it cannot fulfill its mission and obtain benefits. On the other hand, there could be too many workers working for a same task so that their average profit is lower than expectation. In addition, if the crowdsourcing platform cannot allocate workers properly, a problem may come out that the task cannot be fulfilled with high quality and efficiency. In particular, there are competitions among crowdsourcers as well. They compete with each other for limited resources (workers). In order to attract more workers, crowdsourcers should offer reasonable returns to workers. How to plan a proper budget is an important issue for crowdsourcers. Besides the competition among workers and the competition among crowdsourcers, malicious behaviors are also inevitable in a crowdsourcing system, which obviously impact the quality and final success of crowdsourcing. Social dilemma happens under the following situations. If workers can get their payment as long as they are assigned with tasks, they may refuse to work out the tasks as promised in order to reduce their costs. In another situation, if the payment is paid after the tasks have been accomplished, the crowdsourcer may refuse to pay with the excuse that the quality of worker provision is not desirable. As can be seen from the above, a specific mechanism is highly expected in crowdsourcing in order to ensure fairness, encourage honesty and loyalty, and provide essential incentive.

Another interesting HMN system is Internet of Things (IoT). According to [3], the interactions of humans and machines in IoT systems combine the characteristics of those in crowdsensing and social media. A large number of smart devices are connected with each other through the Internet. These devices can communicate with each other, collect, process and transmit data among each other. The influence of personal rationality is eliminated without direct human participation. However, massive devices also bring challenges for the management of IoT. These devices are energy-aware and demand an effective power control scheme to allocate resources and scheduling tasks. How to ensure quality of services when overloading and congestion happen and how to find an optimal topology that can improve network connectivity are two key issues in an IoT system. A robust IoT system that can attract participants needs to be secure enough to detect and mitigate attacks dynamically. Heterogeneous raw data collected from different devices in different places without a uniform standard is hard to process as well. Obviously, an IoT system requests a mechanism to protect its security and enhance its trust, which motivate many studies in the literature.

Bitcoin [4] is a decentralized cryptocurrency with no central authority to issue fiat currency. It allows two willing parties to transact directly without the existence of a trust third party. It is a typical example that applies HMNs in peer-to-peer networks. All transactions of Bitcoin are stored in Blockchain which is maintained by miners. How to ensure the participation of miners and prevent various attacks is essential in prolonging the lifetime of Bitcoin.

The essence of game theory is to study the interactions among players by analyzing their rationality. Game theory has shown its effectiveness in handling some difficult problems with ingenious designs in smart grid systems [5,6], information sharing problems [7–9], routing security [10,11], cloud computing [12], intrusion detection [13], and so on. Game theory can help designing a proper system by advising suitable system parameters and business models, thus it can highly motivate system players to choose their actions that are preferred by a system designer. The distribution and heterogeneous characteristics of crowdsourcing and IoT, as well as Bitcoin increase the difficulty to solve their common and specific problems as well as some hidden issues. Game theory offers us an effective research methodology to analyze open issues in HMNs and figure out proper solutions. However, the literature lacks a thorough survey to summarize the existing work in this field and show current state of arts for figuring out opens issues and directing future research.

In this paper, we investigate the power of game theory in solving the problems in HMNs, such as crowdsourcing, IoT and Bitcoin. We survey the game theoretical methods in HMNs published from the year 2012 to the year 2017, focusing on crowdsourcing, IoT and Bitcoin. We search papers with the following keywords: crowdsourcing, crowdsensing, IoT, Bitcoin, game theory, resource allocation, power control, routing protocol, privacy and security from the databases: IEEE Explorer, ACM Digital Library, Elsevier, ScienceDirect and Springer. We divide the studies on crowdsourcing into two parts based on whether there is a competition among workers. We also review several burning issues in IoT systems that are explored with game theory. For the convenience of literature survey, we propose a number of requirements for game theoretical analysis and incentive establishment on the basis of game theory. We extensively survey the literatures about game theoretical applications in crowdsourcing, IoT and Bitcoin and evaluate their performance by applying the proposed requirements as an evaluation measure. Specifically, the contributions of this paper can be summarized as below:

- This paper is one of the first surveys to summarize game theoretical methods in HMNs, focusing on crowdsourcing and IoT, as well as Bitcoin.
- We propose a number of requirements to evaluate the performance of game theoretical analysis and incentive mechanisms.
- We review and discuss the current literatures about game theoretical methods in crowdsourcing, IoT and Bitcoin based on the proposed requirements.
- We obtain many open issues based on our survey and propose a number of future research directions for not only crowdsourcing, IoT systems and Bitcoin, but also some other areas with similar characteristics to the above two systems.

The rest of this paper is organized as below. In Section 2, we introduce the basic of game theory and a number of typical game models that are referred in this paper. HMNs are also defined and introduced in this section. We propose a number of game model requirements in Section 3, based on which we analyze existing game theoretical methods in crowdsourcing contest systems and microtask crowdsourcing systems in Section 4. In Section 5, we research into game theoretical methods in IoT according to their application intentions and evaluate them based on the proposed requirements as well. We briefly introduce an emerging HMN system, Bitcoin and game theory usage in this system, and also discuss other elemental HMNs in Section 6. Open issues and future research directions are presented in Section 7. Finally, we draw a conclusion in the last section.

2. Overview of game theory and human–machine networks

2.1. Game theory

In order to understand game theory in a good way, we first give basic definitions about game theory.

Game theory [14], a new branch of applied mathematics, is a subject to study optimal solutions in the context of conflicts. Game refers to the procedure that some people, groups or organizations choose and carry out the strategies that they choose from their action sets synchronously or successively, once or repeatedly under certain environments and rules. Corresponding payoffs are achieved after all players choose strategies.

In order to describe a game, there are some essential elements, including players, actions, information, strategies, payoffs, outcome and equilibrium. The definitions of these elements are given as below.

Player is the entity involved in a game, namely the decision maker who chooses actions to maximize its utility or payoff in the game. What is more, the player can be an individual, a company, a nation, and so on. **Strategy** is a player's plan of action that specifies which action to take based on its knowledge of action history. Strategies can be pure or mixed, which could be dynamically changed. There are two more terms that need to be noticed. One is strategy set or strategy space, which is the set of a player's all possible action. The other is strategy profile that is a set composed by strategies from which all players choose. After all players have taken actions in the game, each of them will get either a negative or a positive return. The return of each player is its **payoff**. Apparently, the player's payoff not only depends on its own action, but also is impacted by other players' actions. Different combinations of players' strategies result in different **outcomes**. **Information** means the knowledge that the players know, especially the characteristics and the actions of other players. The characteristics of the aforementioned strategy space, payoff and players consist of the information structure of a game. **Equilibrium** is a combination of all players' strategies where each player's strategy is the best response to the strategies of other players. Equilibrium is one kind of stable outcomes. Nash Equilibrium (NE) is one kind of equilibrium that can be applied to come up with the solution of a game. It is noticeable that the definition of equilibrium cannot ensure solution uniqueness, and the lack of unique solution is exactly the main problem of game theory. What is more, we may counter an adverse problem that a game does not have an equilibrium, which means that the modeler cannot find a reasonable strategy profile. A game model with no equilibria or with multiple equilibria is an underspecified model, in which the modeler does not give a comprehensive and precise prediction about what is going to happen.

2.2. Typical game models and theories

In this section, we introduce a number of common game models and theories that will be used in the following review part.

In a game, if all players take actions at the same time, or even though players choose their strategies successively, latter players cannot know the actions of former ones, the game is a **static game**. If the latter players can observe the actions of the former ones, the game is called a **dynamic game**. If a same game has been played repeatedly, the game is called a **repeated game**, which is a special kind of dynamic game.

If each player knows all of other players' strategies, payoffs and characteristics, we say the game is with **complete information**. While if there is at least one player does not fully understand other players' strategies, payoffs and characteristics, the game is with **incomplete information**.

Table 1
Payoff matrix.

Player 1	Player 2	
	Cooperate	Defect
Cooperate	R, R	S, T
Defect	T, S	P, P

From the perspective of the purpose of action, if all players in a game choose strategies independently to maximize their own profits, the game is a **non-cooperative game**. On the contrary, if there is a binding contract among all players or all of the players have formed a coalition, the game is a **cooperative game**. The difference between cooperative game and non-cooperative game is that their focuses are different. The non-cooperative game focuses on individual rationality and the cooperative game aims to achieve group rationality.

Cournot model [15] is a non-cooperative game with complete information. The players involved in the Cournot model choose strategies at the same time. **Bargaining game** [16], which models a infinite bargaining process, is a dynamic game with complete information. Only when the players reach an agreement, this game can convergent and stop. Considering the discount factor caused by the delay in an agreement, players should accept reasonable offers as soon as possible.

The players in the Cournot model take actions synchronously. While in a real economic market situation, some small firms observe a big firm's strategies before choosing theirs. The **Stackelberg model**is named after a German economist Heinrich Freiherr von Stackelberg, who described this model in the book "Market Structure and Equilibrium". There are two kinds of players in this model, one is a leader firm who chooses strategy at first and then its follower firms choose sequentially. What is more, the Stackelberg model can be used to find the Subgame Perfect Nash Equilibrium or Equilibria (SPNE). SPNE is the strategy profile that serves best for each player, given the strategies of other players.

The Stackelberg game is one kind of**Sequential game,** which refers to a game that players choose their strategies orderly. When a player needs to decide its strategy, its chooses its action based on the reactions of other players. The former player knows the followers will choose their strategies based on its decision, so it can move firstly to restrict the others' actions. Therefore, the player who takes actions firstly in a sequential game may take an advantage and obtain more benefits. This is the characteristic of Sequential game, called first-mover advantage or pioneer advantage.

Gift-giving game contains two kinds of players. One is an employer who provides works (or wages) and the other one is a worker who decides whether accept the wages or not. If there is no workers accept the wages, the benefits of both of them are zero. If a worker accepts the wage, he should choose the level of his efforts. The more he contributes, the more the benefits the worker can obtain.

Bayesian Game, which is also called a game with incomplete information, is a game where the players have incomplete information about other players' strategies or payoffs. But they know the probability distribution of the others' strategies. The equilibrium of Bayesian Game is called Bayesian Nash Equilibrium (BNE).

Considering there are two players whose strategies are cooperate and defect, the payoff matrix of them is presented in Table 1. If T >R >P >S, then this situation is called the **prisoner's dilemma**. The best outcome of a player is unilateral defection (defect while the other player chooses to cooperate) while the equilibrium of this game is mutual defection due to the higher potential benefits of defection. Zero-Determinant (ZD) strategy was first proposed by Press and Dyson [17] to solve 2-player iterated prisoner's dilemma. A player with ZD strategy can make its own payoff have a linear relationship with the other's payoff. The other player has no idea about this ZD player. Thus the ZD player can take this advantage to force the opponent to choose the strategy that the ZD player wants the other player to choose (e.g., cooperation) by setting the relationship properly. What is more, recent research shows this strategy can be extended to larger application scenarios with multiple players [18].

If Table 1 presents the payoff matrix of the **chicken game**, T >R >S >P should be satisfied. The difference between the prisoner's dilemma and the game of chicken is that the outcome of unilateral cooperation is higher than mutual defection in the chicken game. There are two Nash Equilibria, mutual cooperation and mutual defection in the chicken game.

Stochastic game [19], which consists of finite or infinite number of stages, refers to a dynamic game with probabilistic transitions played by one or more players. In each stage, the game begins at an uncertain state, and then its players choose their strategies and obtain payoffs according to a current state and the strategies they choose. The state of each stage does not have to be the same and if they are the same, the game is a repeated game. If the number of players in a stochastic game is finite and the number of possible states in each stage is finite, it must have a NE, which may not be the optimal strategies for both players. Stochastic game is also called Markov game.

Potential game [20] is a very helpful game in designing schemes and instructing players in choosing strategies. The most important notion in the potential game is potential function, which is a global function related to each player's payoff function. A significant property of potential game is that the NE must exist and it can achieve maximize overall profits.

Differential game [21] is a kind of cooperative game, where players interact with each other continuously to achieve their own optimal objectives. It can be widely used in addressing optimal control problems.

Colonel Blotto game [22] is a zero-sum game within two players who distribute their limited forces to some battlefields at the same time. Each player has no idea about the strategies of another. In each battlefield, the player who allocates more forces will win. They need to figure out the most optimal allocation plan in order to win as more battlefields as possible.

Behavioral game [23] is different from traditional games that assume players to be rational and unwilling to believe in others. However, behavioral economists proved that traditional games are impractical in modeling actions of humans. Behavioral game takes irrational factors into consideration and makes a game model more socialized. This kind of game can be used to model interactions with many human participations.

In most research, players are assumed to be overly reasoning, which is not reasonable in some practical scenarios. Players in **evolutionary game** are bounded rational. A player with bounded rational will not change its strategy until its benefit decreases significantly. Evolutionary game takes various factors that may influence a player's decisions into consideration and analyzes the evolution of player actions. Evolutionarily Stable Strategy (ESS) is a strategy adopted by most members of the population. When most players in a system choose the ESS, the system is strong enough to resist small turbulence.

Shapley value [24] is a concept in cooperative game. It is a value to evaluate the contribution of each player. With the help of Shapley value, the overall utility of all players can be distributed to a coalition fairly.

Sealed-bid auction is a type of auction process where every buyer (e.g., worker) submits its sealed bid to an auctioneer (e.g., a platform) simultaneously, and then the auctioneer sells its product (task) to the buyer who has offered the highest bid and publishes it to the public after comparison. **Vickery–Clarke–Groves (VCG) mechanism** is one kind of sealed-bid auctions. This mechanism can alleviate players to tell the truth and distribute the items bided optimally.

2.3. Human–machine networks

HMNs refer to the networks where humans and machines work together to provide synergistic effects that are higher than those if they work independently [3]. It refers to a situation where humans and machines can interact with each other and produce more significant influences than themselves. An object that has unpredictable behaviors like emotions, preferences, and decision-making is what we called human here. Machines are the entities that have no preferences or emotions. Due to deep research in machine learning and data mining, which require a large amount datasets collected from humans or through humans' machines, the ties between humans and machines are becoming closer.

Tsvetkova et al. divided HMNs into eight types, public resource computing, crowdsourcing, web search engines, crowd sensing, online markets, social media, online games and virtual worlds, and mass collaboration, based on the interactions among humans and machines. This classification evolves with the emergence and development of new technologies. IoT is a hybrid HMNs that has the characteristics of crowdsensing and social media, while Bitcoin combines public resource computing with online markets. Concrete introductions to these systems and current research in them can be found in [3].

In this paper, we focus on crowdsourcing and IoT which have been widely studied. They are most attractive and typical HMN systems than the other types.

3. Model requirements

We propose a number of requirements with regard to game modeling and game theoretical analysis in this section. They can be used as an evaluation measure to comment and justify the pros and cons of each existing study. The first six requirements are given to evaluate game theoretical analysis and the rests are proposed as the requirements for incentive mechanisms designed based on game theory.

Privacy Preservation (PP): A common feature of crowdsourcing systems and IoT systems is that workers or nodes provide information that contains or reveals their privacy. The perfect performance of these systems depends on the high level of participation. Participants demanding for privacy protection are not willing to take part in systems without privacy preservation concerns. Therefore, it is essential to consider privacy preservation when designing a game model to attract system participants. In addition, it can enhance system trust and service quality in the long term.

Stability (ST): The game model should eventually enter a stable state that all of the players are satisfied with their payoffs and have no incentive to betray unilaterally. This requirement is essential for formulating a successful game model. An easy way to judge whether a model satisfies this requirement is to figure out the number of equilibrium of the model. If there are two or more equilibria, it is difficult to decide which equilibrium would be achieved. If there is no equilibrium, the game model provides no guides to the modeler. Thus, a game model that can achieve a unique equilibrium is preferred during game theoretical modeling and analysis.

Applicability (A): The goal of game modeling is to solve some practical problems in a concrete system. For example, in a crowdsourcing system, game theory could be used to enhance the participation level of workers or suppress the malicious actions of players. If a game model can be theoretically or practically illustrated to be efficient in solving its target problems, we say this game model satisfies the requirement of applicability.

Efficiency (E): It is difficult to give a precise definition of efficiency as this requirement is related to the goals of models. In Wikipedia, efficiency is defined as the ability to avoid wasting materials, energy, efforts, money, and time in doing something or in producing a desired result. Therefore if the cost to conduct a game is low, the payoffs of players can increase, the calculation of NE can be finished in polynomial time and there is not unnecessary dissipation of resources, then the game model is satisfied with this requirement. This requirement can make sure that the game is designed with not only effectiveness but also high efficiency so that it can be widely used.

Feasibility (F): A feasible model refers to a situation that the payoff functions of players are defined according to the obtainable information and the cost of the designed game should not be too exorbitant to conduct. Otherwise, the game cannot be executed to analyze the interactions between players and provide instructions to them.

Scalability (SC): This requirement ensures that a designed game model can be extended to a large scale scenario with more players participating in and less restrictions on experimental conditions. A scalable model can fit into other application scenarios easily without too much modification. Notably, some solutions can only effectively address problems in theory in the condition of very strict assumptions, which is not easy to fit into a real-world environment. Therefore, we should take scalability into serious consideration when designing a feasible game.

Individual Rationality (IR): It is unreasonable that a player has incentive to take part in a game where it can only obtain negative utility. Therefore, a helpful model should guarantee that its equilibrium is a state where any players can obtain non-negative profits. In a non-cooperative game, all players choose strategies from the view of maximizing their own profits, therefore this requirement is satisfied in each non-cooperative game. We say a cooperative game is individual rationality when the players in grand coalition can obtain more profits than it can obtain on his own (without cooperation with anyone else).

Truthfulness (T): A game-based incentive mechanism is designed to impel players to tell truth. Thus, it should make sure that there is no individual can obtain more profits than others by cheating no matter what strategies the other players choose. The possibility of profiting from dishonest actions will encourage unhealthy tendencies, thus affect the quality of service, and eventually make the system crash.

Robustness (R): It is unavoidable that there may exist more or less deviations, especially in practical scenarios. A robust model should have the ability to resist deviations and reach a stable state in a short time. Some random variables can be introduced to express the disturbances of an environment or internal participants.

Profitability (P): Let us assume that there is such a service platform that can serve its own users. These users will choose this platform only when they can obtain more profits in this platform. However, if the platform sacrifices its utility to attract more users, then this platform cannot survive for a long time. Therefore we propose the requirement of profitability to ensure that the non-negative utility of each player is not built on the decrease of other incoherent entities' utilities.

4. Crowdsourcing systems and their economic models

Crowdsourcing refers to an approach that a company or institution outsources its tasks that were executed by its employees in the past to voluntaries and non-specific crowds. In a general crowdsourcing system, there are three participants: crowdsourcers (i.e., requesters), workers (i.e., providers) and a crowdsourcing platform. The crowdsourcer refers to a player who has one or more tasks that need to outsource and workers are the players who have extra resources or abilities to conduct these tasks. All of these crowdsourcers and workers register with a third party, which is what we call the crowdsourcing platform herein. The task distribution and reward allocation are performed by this platform. To model the relationship of these participants from the view of economics, lots of experts used sealed-bid auction to model the interactions among them [25–28]. Crowdsourcing systems can be generally divided into two types: crowdsourcing contest and microtask crowdsourcing based on the types of tasks. In this section, we discuss the economic models of these two kinds of crowdsourcing systems.

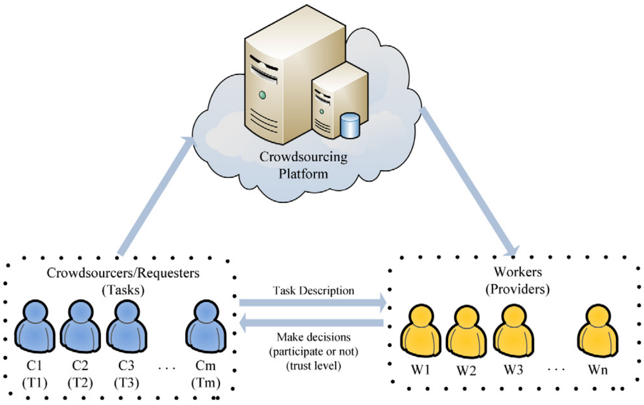

Fig. 1. The structure of crowdsourcing contest system.

4.1. Crowdsourcing contest system

Crowdsourcing Contest System (CCS) refers to a situation where multiple workers compete with each other to provide solutions to the tasks outsourced by crowdsourcers. These tasks are very challenging and significant and it will take the workers a long time or big costs to complete them. The workers who win the contest can obtain high profits. There are two modes of payment: winner-take-all mode [29] and all-pay mode [30]. If a crowdsourcing system applies the winner-take-all mode, only the winner or winners can obtain profits while the efforts of the other workers are vain, which is also the mainstream auction. If a crowdsourcing system applies the all-pay mode, all of the workers who have struggled to work out the tasks will be paid according to their efforts. Luo et al. [31] stated that the all-pay mode is more natural than the winner-take-all mode when the bid we take into consideration is the actual contribution efforts of workers instead of the willingness to make contribution.

We assume a general crowdsourcing system $N = (CP, C, W)$, where CP stands for a crowdsourcing platform, $C = \{C_1 C_2, \ldots, C_m$ is the set of m crowdsourcers and $W = \{W_1 W_2, \ldots, W_n$ is the set of n workers, as shown in Fig. 1. We assume each worker cannot do more than one task at the same time due to the limitation of its ability and resources.

For each crowdsourcer $C_i i = 1, 2, \ldots, m$ [25]:

1. C_i has a task T_i need to be completed and it cannot do it by itself;
2. If T_i is completed, C_i can obtain benefit v_i;
3. The highest fee that C_i would like to pay for workers to complete T_i is presented as b_i It is the bid of each crowdsourcer. As there are m crowdsourcers, we can get a bid vector $\beta = (b_1 b_2, \ldots, b_m)$;
4. C_i needs to pay guarantee fee w_i^C to the CP in case it does not pay for the workers after they finished T_i;
5. In order to restrain the dishonest actions of crowdsourcer, CP collects feedback from every worker and returns a certain fee p_i to C_i on the basis of the feedback.

Based on the above modeling, we can conclude the utility function of C_i as follows:

$$U_i^C = v_i - (w_i^C - p_i).$$

For each worker $W_j j = 1, 2, \ldots, n$:

1. It takes W_j a cost $c_j^i > 0$ to complete task T_i. We get a cost vector $\sigma_j = (c_j^1 c_j^2, \ldots, c_j^m)$ for W_j;
2. W_j gives a ask price a_j^i for each task T_i based on its cost and W_j will not complete T_i if $a_j^i > b_i$. We can obtain a ask vector $\alpha_j = (a_j^1 a_j^2, \ldots, a_j^m)$ for W_j and an ask matrix $A = (\alpha_1; \alpha_2; \ldots; \alpha_n)$;
3. A set Δ consists of winning crowdsourcer–worker pairs is defined in [25]. If $(C_i W_j) \in \Delta$, it means W_j is assigned to complete T_i. In addition function $\delta(\bullet) : C \to W$ is also defined in [25]. If $\delta(j) = i$, we can know that W_j is assigned to complete T_i, which can be represented as $(C_i W_j) \in \Delta$. And if $\delta(j) = 0$, it means W_j is not assigned to any tasks. The parameter $y_j^{\delta(j)} \in \{0, 1\}$ is used to indicate whether W_j has been assigned a task. $y_j^{\delta(j)} = 1$ indicates that W_j has been assigned a task;
4. W_j needs to pay guarantee fee w_j^W to CP as well to ensure it can complete tasks;
5. CP collects reports about W_j from all crowdsourcers and decides return fee $p_j^{\delta(j)}$ paid back to W_j based on these reports.

We can give the utility function of W_j on the basis of the above analysis as below:

$$U_j^W = \left(p_j^{\delta(j)} - w_j^W\right) - y_j^{\delta(j)} c_j^{\delta(j)}.$$

Besides the guarantee fees CP obtains from crowdsourcers and workers and the return fees paid back to crowdsourcers and workers, it also takes a cost for CP to execute auction and operate the service. Parameter τ_i stands for the auction and operation fee that CP should pay for the task T_i. And then the utility function of CP can be presented as:

$$U_{CP} = \sum_{(C_i, W_j) \in \Delta} [\left(w_i^C - p_i\right) + (w_j^W - p_j^{\delta(j)}) - \tau_i].$$

4.2. Microtask crowdsourcing system

Different from the crowdsourcing contest system, there is no competition among workers in a Microtask Crowdsourcing System (MCS) (see Fig. 2). A crowdsourcer publishes a number of small tasks that are cockamamie and inefficient but straightforward to accomplish [32]. A situation where the task outsourced by the crowdsourcer can be divided into a series of small tasks and need the workers to make joint efforts can also be regarded as a microtask crowdsourcing problem [33]. Note that in a microtask crowdsourcing system, the border between crowdsourcer and crowdsourcing platform is blurred. The crowdsourcer can publish its tasks and reward workers on its own or can ask a third party (i.e., the crowdsourcing platform) to fulfill this job.

We consider a simple microtask crowdsourcing model with one CP and n workers $W = W_1 W_2, \ldots, W_n$ [34]. There are two kinds of economic models constructed from the perspective of CP and workers respectively [35].

We first introduce the procedure of the CP-centric model:

1. CP publishes its total reward $R >$ based on which worker W_i decides its participation level (time or ability) $t_i \geq 0$;
2. The cost and the reward of participating in completing the task are related to total participating time. Let c_i represent the unit cost of W_i.

Through the above analysis, the utility function of W_i can be summed up as

$$U_i^W = \frac{t_i}{\sum_{i \in W} t_i} R - t_i c_i.$$

The utility of CP is related to the schedule of task completion. CP can obtain huge profits if all of its tasks are accomplished in a short time. Yang et al. [35] used a logistic function to describe the decay of the utility of CP over time. The detailed utility function of CP was designed as

$$U_{CP} = \lambda \log \left(1 + \sum_{i \in W} \log\left(1 + t_i\right)\right) - R,$$

where $\lambda > 1$ is a system parameter.

The objective of this model is to maximum U_{CP} and each worker will choose appropriate t_i to optimize U_i^W accordingly.

The procedure of the worker-centric Model is:

1. CP publishes a series of tasks $T = \{T_1 T_2, \ldots, T_m$, each task can bring$CP$ benefit v_i;
2. Each worker W_j chooses its task set $T_j \in T$ according to its preference. The cost of W_j is c_j, which is private information. And then W_j sends its task–bid pair $(T_j a_j)$ to the platform, where a_j is the least ask price of W_j;
3. CP chooses a winner set S according to all the task–bid pairs it receives and make sure the payoff p_j for each worker.

The utility function of worker is

$$U_j^W = \begin{cases} p_j - c_j, & j \in S \\ 0, & otherwise, \end{cases}$$

And the utility function of CP can be set as

$$U_{CP} = \sum_{t_i \in \bigcup_{j \in S} T_j} v_i - \sum_{j \in S} p_j.$$

4.3. Game theoretical methods for crowdsourcing systems

Crowdsourcing systems have shown their power in solving some intractable problems [36–38]. In order to make them able to meet the needs of economic development, a number of incentive mechanisms and algorithms came out recently. Some of them can increase the efficiency and quality of existing solutions [26,32,39–41], some can suppress various malicious behaviors conducted by crowdsourcers or workers [25,42,43] and some can also reduce the cost of executing such a crowdsourcing system [27,28,44]. In this section, we discuss the game theoretical methods designed for crowdsourcing systems and analyze them based on the requirements as proposed in Section 3. Our analysis results are presented in Table 2.

4.3.1. Game theoretical methods for CCSs

As stated before, crowdsourcing systems can be divided into CCSs and MCSs based on whether there is competition among workers. We first overview the applications of game theory in the CCSs.

Hu and Wu [45] formed a static game with complete information to model the interactions among workers of crowdsourcing for software engineering. The authors analyzed the pure strategy NE and mixed strategy NE under different conditions, which then can give players instructions when choosing strategies. Even though this can help attract more workers to participate, the parameters and impact factors the authors considered were limited and there was no concrete experiments conducted to support their conclusion. Thus the requirement of SC cannot be satisfied in [45]. What'

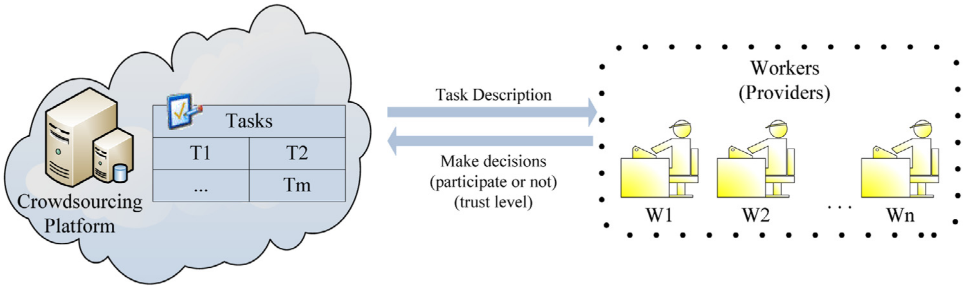

Fig. 2. The structure of microtask crowdsourcing system.

Table 2
Summary of game theoretical methods for crowdsourcing systems based on model requirements.

Ref.	Application scenario	Requirements									
		PP	ST	A	E	F	SC	IR	T	R	P
36	CCS	U	Y	Y	Y	Y	U	Y	Y	U	Y
37	MCS	U	Y	Y	Y	Y	Y	Y	Y	Y	Y
29	MCS	U	Y	Y	Y	Y	U	Y	Y	U	Y
42	CCS	U	Y	Y	Y	Y	N	–	–	–	–
39	CCS	U	Y	Y	Y	Y	U	–	–	Y	–
41	CCS	U	Y	Y	Y	Y	Y	Y	Y	U	Y
22	CCS	U	Y	Y	Y	Y	U	Y	Y	Y	Y
26	CCS	U	Y	Y	Y	Y	N	Y	U	U	Y
38	MCS	U	Y	Y	Y	Y	Y	Y	Y	U	Y
43	CCS	U	Y	Y	Y	Y	Y	–	–	–	–
23	MCS	U	Y	Y	Y	Y	Y	Y	Y	U	Y
28	MCS	U	Y	Y	Y	Y	Y	–	–	–	–
24	MCS	U	Y	Y	Y	Y	Y	Y	U	U	Y
40	CCS	U	Y	Y	U	Y	U	Y	Y	U	Y
45	MCS	U	Y	Y	Y	Y	Y	–	–	Y	–
46	MCS	U	Y	Y	Y	Y	N	Y	Y	U	Y
47	MCS	Y	Y	Y	U	Y	U	Y	Y	U	Y
44	CCS	U	Y	Y	Y	Y	Y	Y	Y	Y	Y
25	MCS	U	Y	Y	N	Y	U	Y	Y	U	Y

Y: yes with support; N: no without support or considerations; U: unknown.

more, whether it can guarantee the privacy of workers is beyond consideration.

A crowdsourcer may be attacked by other malicious crowdsourcers due to the openness of crowdsourcing. Naroditskiy et al. [42] used a non-cooperative sequential game to analyze the interaction between two crowdsourcers. At first, a crowdsourcer chooses to crowdsource its task or work it out by itself and then the others choose to attack it or not. Theoretical analysis showed the mix strategy equilibrium of this game is that the weak player's payoff is zero while the strong one's payoff is related to the cost and success probability of attacks. Malicious actions were inevitable and it was not efficient to suppress selfish actions by adding the cost of attack. While these findings were not illustrated in experiments and PP, SC were not considered.

A scheme that can ensure the quality of solutions is difficult to design. Moshfeghi et al. [46] modeled the interactions among workers as a reversed form of an n-person chicken game with imperfect information to eliminate the situation that immoral workers may try to finish tasks as soon as possible to increase the number of tasks that they can complete in a fixed time without considering the quality of the tasks they complete. The task that workers need to complete in this paper was relevance assessment and the game was named as Fast Relevance Assessment (FRA) game where the players' best strategy was to answer fast and accurately. The authors proposed some matrices to evaluate the effectiveness of this method and stated that this model is suitable for other crowdsourcing experiments. Overall, ST, A, E, F, SC were satisfied except PP.

Designing incentive mechanisms is an effective and efficiency way to achieve different purposes. Most of existing incentive mechanisms for crowdsourcing depends on monetary rewards. However, without efficient pricing schemes, the social dilemma between crowdsourcers and workers is difficult to eliminate. Crowdsourcers may obtain more profits by falsely reporting and lazy workers can increase their profits by free-riding.

When workers and crowdsourcers take strategies rationally to maximize their own benefits, the interaction between crowdsourcers and workers is modeled as an asymmetric gift-giving game if crowdsourcers pay at first [39]. The time-dependency of their present and prospective actions was investigated by repeatedly playing this game. The authors presented a flat-rate pricing scheme based on a reputation mechanism. The reputation value of a crowdsourcer would increase if he paid a worker as the agreement stated and vice versa. When a crowdsourcer's reputation decreased to a certain threshold, he was forbidden to post tasks for a while. Social optimization is achieved, which means every player can maximize its payoff without reducing the profits of other players that are not involved in this game model. All of the requirements were satisfied except that the authors did not take PP, SC and R into consideration.

Anta et al. [44] designed an algorithmic mechanism to solve the collusion among workers. The interactions among crowdsourcer and rational workers were modeled as a Stackelberg game. The procedures can be described as follows: the crowdsourcer outsourced tasks to a number of workers. Each worker had a possibility to cheat. Considering the cost to verify the workers' answers, the crowdsourcer just verified the workers' answers with some possibility. If the crowdsourcer verified, it rewarded honest workers and punished dishonest ones. If it did not verify the answers it received from workers, it regarded the answer of the majority as the correct one and rewarded the majority only. By theoretical analysis, the authors induced a condition under which the crowdsourcer can obtain the correct answers with large probability and maximize its utility. The authors conducted two specific experiments to illustrate the effectiveness and practice of this method. Parameters selected from a wide range imply its support on scalability as well. However, privacy protection and robustness were not considered.

The prediction of many auction mechanisms and incentive mechanisms is that all participants are satisfied, which means all crowdsourcers are satisfied with the outcome of tasks and all workers are willing to complete their tasks as promised. However, these researches ignored the situations of free-riding and false-reporting. Zhang et al. [25] defined the utilities of all participants: the platform, the crowdsourcers and the workers. And then they proposed two novel mechanisms to eliminate free-riding and false-reporting in a crowdsourcing system. No crowdsourcers can obtain more profits by taking dishonest actions and the workers can be incentivized to complete their promised tasks at the same time. PP and SC were not considered in this paper while the other requirements were satisfied according to the above analysis.

Behavior biases in prospect theory and the uncertainty of decision making in standard economic model may affect the design of mechanisms. What is more, how to choose the most suitable mechanisms is significantly crucial. Easley and Ghosh [29] modeled the interactions among crowdsourcers and workers as a principal-agent problem. Considering a simple model that there was a principal, who has a task to outsource, and a number of workers who decide the quality of task strategically with an opportunity cost. The principal has many kinds of incentive contracts to choose, for example, fixed prices to a fixed number of workers, or winner-take-all strategy. Game theory was used to help principal choose an optimal contract by calculating equilibria under different situations. The results showed that if workers choose actions according to expected utility theory, the optimal strategy for principal is the fix-payment contract and if the workers choose actions according to prospect theory preferences, the best strategy of principal is winner-take-all contest. All the above conclusions stay at a theoretical level without any practical analysis. PP, T and R were beyond the authors' consideration as well.

It is possible that malicious workers may attack others. Even if this malicious worker cannot increase its own profit, it can decrease the profit of the target being attacked. An iterated prisoner's dilemma game was modeled to capture the interaction between workers who would be malicious [43]. The loss incurred by malicious actions of workers motivated crowdsourcer to prevent attacks from the workers and punish them by economic penalties. By analyzing the expected payoff of crowdsourcer and worker, Zero-Determinant (ZD) strategy can be calculated. If a player adopted ZD strategy, the expected payoff of the other player is fixed. This means that a crowdsourcer can unilaterally force worker to cooperate by applying ZD strategy. The authors did not consider PP, E, SC and R in this method.

Lu et al. [47] proposed a novel socially optimal rating protocol to eliminate crowdsourcing contest dilemma, such as free-riding or attacking others players. Each player was given a rate initially, and the value of the rate would change after each time generation according to their own actions. A player can only try to provide good solutions to increase its rate and profits. The authors illustrated that this protocol can suppress the malicious actions of workers and the achieved social optimum is robust. They stated their work is scalable. Thus this method takes all of these requirements into consideration but PP.

4.3.2. Game theoretical methods for MCSs

There are lots of tasks in a MCS. Each worker chooses its ideal tasks based on the rewards and its own ability. There is no competition among workers. In this section, we investigate the applications of game theory in MCSs.

TruCentive [40] was an incentive platform, on which each mobile user can get or submit parking information. There were two kinds of participants: workers who provide parking information and crowdsourcers who want to find parking places through this platform. The transaction between them can be described as: workers provide parking information to the TruCentive platform, and then crowdsourcers pay for the information and report whether they had parked successfully. The authors used game theory to design the incentive protocol that can encourage workers to provide high utility data (telling truth) even if the mobile users are unauthentic. Experiments showed the feasibility, stability and robustness of this method. It is also scalable since it can be applied to other practical MCSs. While the privacy of mobile users was not considered.

Considering the cost of verifying the quality of tasks completed by workers may be significantly high, existing incentive mechanisms for solving the problem of low quality of completed tasks are unable to control the cost of crowdsourcers in a low level. Authors in [32] presented a cost-effective incentive mechanism based on game theory. This mechanism can incent workers to supply solutions with high quality and arbitrarily low cost by adopting quality-aware worker training. The authors also demonstrated the effective of this mechanism through theoretical analysis and simulations. Nevertheless, PP, SC and R were beyond consideration.

Luo et al. [41] used Stackelberg game to model the interactions between crowdsourcers and workers for multiple collaborative tasks in mobile crowdsourcing. The authors illustrated that design the reward function based on the quality of task is fairer than that based on the number of users. NE that can maximize the benefit of crowdsourcer exists under different situations no matter the cost of mobile user is complete information or not and no matter the tasks that need to be completed is homogeneous or not. The authors also proposed online mechanisms that can process real time tasks based on a Markov model without high computational complexity. All the requirements except PP and R were considered in this paper.

Yang et al. [26] modeled the incentive mechanism that can maximize the crowdsourcer's utility as a Stackelberg game. In this game, the crowdsourcer is the leader whose strategy is to decide its rewards and the mobile users are the followers who choose their working time. Stackelberg Equilibrium is achieved and no worker can obtain more benefits by unilaterally changing its strategy. And then they formed a user-centric auction mechanism that can make sure each player can obtain non-negative profits and asking price based on their costs (telling truth) is the only way to maximum their utilities. Even if this mechanism is user-centric, it does not decrease crowdsourcer's utility. Other requirements were satisfied as well except PP and R that were not considered in this study.

A dynamic non-cooperative game was formulated to model the interactions among crowdsourcers [31]. Each crowdsourcer compete for the limited number of workers. This study focused on how crowdsourcers can price smartly. Through theoretical analysis, NE (cooperative) always exists, no matter the strategies of other crowdsourcers is complete information or not. However, the NE is inefficient because it cannot obtain the maximum overall benefits. This is called the Prisoner's Dilemma in economics. By repeatedly playing this game, if a crowdsourcer deviated from NE, the others would punish it. Rational crowdsourcers would choose NE to achieve long-term benefits. This model can also be used in lots of practical environments. It fulfills the requirements of ST, A, E, F and SC, respectively. Nevertheless, whether this method can protect the privacy of all the participants is unknown.

Peng et al. [48] considered the bounded rationality of workers and modeled the interactions between workers as an evolutionary game and the interactions between crowdsourcers as a non-cooperative game. The overall procedure can be described as following. At first, each worker chooses a crowdsourcer and completes the task this crowdsourcer allocated to it. And then the workers compare their profits with the average profit of all workers. If a worker's profit is lower than the average value, it would choose another crowdsourcer. Crowdsourcers changed their strategies (budgets) as well according the others' strategies to appear more workers. Once a crowdsourcer changes its strategy, workers changed theirs correspondingly. A stable state is that all the crowdsourcers choose the same budget and achieved the same profits and all the workers obtain the same rewards. The authors stated that this method can be applied into many practical MCSs with different crowdsourcing objectives. ST, A, E, F and SC were satisfied. However, the effectiveness of this approach in terms of preserving privacy is unknown.

It is reasonable that the types of all the crowdsourcers subscribed to the same platform could be different, different tasks may need different number of workers. What is more, the types of workers could be different as well. Different workers may have different abilities and the costs to complete the same task may also be different. Koutsopoulos [28] designed a mechanism from the perspective of minimizing the cost of crowdsourcers and guaranteeing the experience of workers. The interaction among workers was modeled as a repeated Bayesian game that each player is not familiar with other players' characteristics. The author used a second-price auction mechanism that can help crowdsourcers decide participation level and payment allocation based on the quality of the completed work of workers. Through concrete analysis, the proposed mechanism can motivate workers to participate in and report their costs truthfully. And the cost of crowdsourcer is minimized while its revenue is kept constant. A concrete example showed this mechanism was feasible. While there may exist a data redundancy problem, thus the effectiveness may not be satisfied. PP, SC and R were not considered in this method, either.

Anta et al. [27] modeled the interaction among arbitrary number of agents as a Bayesian game that the information about players was incomplete. This makes this model scalable. Different from [28], this model was from the perspective of maximizing the profit of crowdsourcers with the help of reward tuple. An auction mechanism used in this paper is an asymmetric all-pay contest. The authors proved the existence of the only equilibrium of this game and listed the characteristics of this equilibrium. And the optimal reward tuple was calculated as well. Unfortunately, PP, T and R were not considered in this method.

Rational mobile users may have no incentive to participate in a crowdsourcing system when the cost of participation is high. Ma et al. [49] proposed an incentive mechanism based on game theory to solve this problem. It can promote players to act honestly. The authors also designed an evolutionary game to help players choose optimal strategies by deriving Evolutionarily Stable Strategies (ESS). Nevertheless, this mechanism cannot be applied to more complicated crowdsourcing systems and privacy protection and robustness are beyond the authors' consideration.

Wang et al. [50] focused on privacy preservation problems in context-aware crowdsourcing systems. They modeled the interactions among system players as a repeated game and proposed a reputation system. NE was calculated and analyzed in this paper. Through careful design, CP can be encouraged to protect the worker's privacy and its own profits can be guaranteed as well. E, SC and R were not considered by the authors.

5. Game modeling in IoT

Depending on advanced sensing and communication technologies, a large number of smart devices are connected with each other through the Internet to form various IoT systems. These devices can communicate with each other, collect, process and transmit data among each other and eliminate the influence of personal rationality without direct human participation. Nowadays, IoT has been widely applied in lots of areas for different purposes, like transportation control, energy management, smart cities and health care, etc. [51,52]. As a rising but complicated technology, there is no unified and specific definition of IoT. One relatively accurate definition is given in [53], which says that IoT envisions a self-configuring, adaptive, complex network that interconnects "things" to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, own sensing/actuating capability, hold a programmability feature and are uniquely identifiable.

In a lot of literatures, IoT can be divided into three layers: perception layer, network layer and application layer [54]. The perception layer consists of various kinds objects [51], like sensors, camera, GPS, Radio Frequency Identification (RFID) tags, Near Field Communication (NFC) devices, actuators and so on. These objects sense data in a distributed manner and collect information and data. Various communication networks like cellular networks and sensor networks converge in the network layer. IoT management and information operation happens in the network layer as well [55]. Data and information gathered, analyzed and processed in the former two layers are applied in the application layer.

Due to the large-scale and distributed architecture of IoT, data is collected from different devices with various qualities. The data should be cleaned and standardized before putting into use. How to design a proper and lightweight way to arrange communication and computation resources and scheduling tasks to ensure least resource consumption, power waste and fast task accomplishment is a great challenge in IoT network arrangement. IoT is a large network that consists of various and distributed network entities with high mobility and different kinds of protocols. In order to formulate an effective IoT, its topologic architecture should be optimized. A designer should take Quality of Service (QoS) into consideration with respect to communication problems. With large amount data operated and transmitted among different entities, data security should be ensured to keep high participation rate of objects, especially in the situation that sensitive and personal data are collected, transmitted and processed. IoT should have the capability of preventing intrusions and Deny of Service (DoS) or Distributed Deny of Service (DDoS) to keep the network work properly with long lifetime. There are also some challenges in IoT applications, e.g., competition among IoT service providers and optimal pricing design.

Game theory has also been applied into IoT in order to overcome some of its challenges. An effective IoT system should fulfill some non-trivial demands for ensuring system performance, lightweight communication overhead, and high level of security. We research on game theoretical methods applied in the area of IoT for different applications and give a brief summary in Table 3 about application purposes and applied game models. In what follows, we review the existing work about applying game theory to solve IoT problems. Our review consists of the following parts: Game Theoretical Methods for Network Arrangement; Game Theoretical Methods for Communications; Game Theoretical Methods for Network Security and Game Theoretical Methods for Application (see Table 4 that summarises the review based on game model requirements).

Table 3
General usages of game theory in IoT.

	Purpose	Game model	Reference
Network arrangement	Power control	Non-cooperative game	[56,57]
		Cooperative game	[58]
	Selection problem	Non-cooperative game	[59–61]
		Cooperative Game	[62]
	Task scheduling	Non-cooperative game	[63]
		Cooperative game	[64–66]
	Resource allocation	Non-cooperative game	[62,67–70]
Communications	QoS	Cooperative Game	[58,67,71,72]
		Non-cooperative game	[64,68,73,74]
		Cooperative Game	[75–79]
	Topology optimization	Non-cooperative game	[80]
	Routing protocol	Non-cooperative game	[81–83]
Network security	Honeypot	Non-cooperative game	[84]
	Security problems	Non-cooperative game	[85–87]
	Trust	Non-cooperative game	[56]
	Anomaly detection	Non-cooperative game	[88,89]
Application	Data process	Cooperative Game	[90,91]
	Service provision	Non-cooperative game	[51]
		Cooperative Game	[92]

5.1. Game theoretical methods for network arrangement

Massive smart devices are connected in IoT. It is significant and essential to arrange resources and power in a proper way to avoid unnecessary waste and enlarge system lifetime as long as possible. Multi-tasks consist in IoT systems and smart devices may join and leave the systems frequently due to their mobility and unpredictability. An effective and rational task scheduling scheme can help task providers complete their tasks in a short time and enhance IoT performance. More and more objects can be involved for achieving a high task accomplishment rate. Game theory, as a powerful tool in capturing players' interactions and helping players make optimal decisions, has been widely used to solve one or more problems in IoT. In this section, we research on the game theoretical methods about network arrangement in IoT.

Power Control (PC)

Cryptographic is a widely recognized approach to achieve the requirement of security in many fields. However, in IoT, there is no sufficient computational capabilities and power to execute complicated cryptographic algorithms. Duan et al. [56] proposed an energy-aware trust derivation scheme with game theory that can control the power consumption to a low level without compromise of system security. Players in this model are all the neighbors of evaluated nodes. After receiving a trust request, the players choose to reply or not based on their remaining energy. Hop limitation is used in this scheme as well to reduce latency. Considering that the players may act selfishly, the authors established a dilemma game to calculate the optimal number of recommendations. The requesters just trust the nodes that gain more recommendations than this optimal number, otherwise, the scheme is not secure. The effectiveness of this scheme is demonstrated through experiments and performance evaluation. The performance needs to be improved by adjusting this scheme to reduce the overhead of trust request in order to achieve profitability. PP, SC, R and P were not considered in this scheme.

Kim proposed an adaptive power control scheme based on a behavioral game, which can capture the bounded intelligence of players [57]. Mobile nodes are the players in this game and the strategies of these players are related to the levels of power. In each time generation, every player observes the current Signal-to-Interference-plus-Noise Ratio (SINR) and packet delivery ratio and calculates their payoffs individually. Background noise was considered in calculating SINR to increase the robustness of this method. Response sensitivity is decided by the player's thinking level, which varies with each individual. Combining all the above information, the players can calculate a Mutually Consistent Behavior Equilibrium (MCBE), which is a near-Nash equilibrium that no players have incentive to change their strategies. Each player in this scheme can monitor the payoff constantly and if his payoff changes a lot, the algorithm will calculate another strategy for him. Besides power control, the method designed can also be used in other situations, where cooperation and conflict exist simultaneously. Through the above analysis, all of the proposed requirements were satisfied except PP and P.

Considering the energy used to transmit signals and data is more than that used to receive signals or data, Xiao et al. [58] proposed a system where receivers can transfer their surplus power to transmitters in order to extend the lifetime of the system. The authors formed a collaborative stochastic game to model the interactions between transmitters and receivers. In order to prolong the lifetime of the system, the players should not only consider some current parameters, like their batteries, energies and communication overhead, but also predict their future evolution based on those of the past using Markov property. Concert theoretical analysis and numeric experiments showed that the optimal actions (NE) of the players calculated in this paper can improve the expected discounted payoff of the system. Whether this method can be applied to another application scenarios (i.e., SC) and resist destabilizations (i.e., R) and privacy intrusion was not considered by the authors.

Selection Problem (SP1)

There are massive nodes existing in an IoT system and no effective or lightweight ways have been developed to ensure the quality of them all. If a node chooses some "friend" nodes and communicate or share information with them, each node could achieve their goals in an efficient and inexpensive way. Militano et al. designed a friend selection mechanism that combines a cooperative game and a Shapley-value based algorithm [62]. The general procedure of this scheme is when a node decides whether involve a new candidate as its friend, it first checks if the number of its friends has reached the largest number n. If not, it tries to make a friendship with this candidate directly, otherwise, it calculates and ranks the marginal contributions of existing friends and this new candidate. If this new candidate is the first n nodes with largest contribution, it tries to make a friendship with the candidate. The evaluation results showed that the mechanism can manage friendship selection properly with little overhead. Thus

Table 4
Summary of game theoretical methods for IoT systems based on model requirements.

Ref.	Application Scenarios												Requirements									
	Network Arrangement				Communication			Network Security				A	PP	ST	A	E	F	SC	IR	T	R	P
	PC	SP1	TS	RA	QoS	TO	RP	H	SP2	T	AD	p										
53	√								√	√			U	Y	Y	N	Y	U	Y	Y	U	U
54	√												U	Y	Y	Y	Y	Y	Y	Y	Y	U
55	√			√									U	Y	Y	Y	Y	U	Y	Y	U	Y
59		√		√									U	U	Y	Y	U	U	Y	Y	U	Y
56	√	√											U	Y	Y	Y	Y	U	Y	Y	U	Y
57	√	√											U	Y	Y	Y	Y	N	Y	Y	U	Y
58		√											U	Y	Y	Y-	U	Y	Y	Y	Y	N
61			√		√								U	Y	Y	Y	Y	U	Y	Y	U	Y
62	√		√										U	Y	Y	Y	Y	U	Y	Y	U	Y
63	√		√										U	Y	Y	Y	Y	U	Y	Y	U	Y
60			√										U	Y	Y	Y	Y	Y	Y	Y	U	U
65				√	√								U	Y	Y	Y	Y	U	Y	Y	U	Y
66	√			√									U	Y	Y	Y	Y	U	Y	Y	U	Y
67	√			√									U	Y	Y	Y	Y	N	Y	Y	U	Y
68				√									U	Y	Y	Y	Y	U	Y	Y	U	Y
69	√			√									U	Y	Y	Y	Y	U	Y	Y	U	Y
70	√				√								U	Y	Y	Y	Y	N	Y	N	U	Y
71	√				√								U	Y	Y	Y	Y	U	Y	Y	Y	Y
72	√				√								U	Y	Y	Y	Y	U	Y	Y	U	Y
73	√				√								U	U	Y	Y	Y	U	Y	U	U	Y
74					√								U	Y	Y	Y	Y	U	Y	Y	U	U
75					√								U	U	Y	Y	Y	Y	Y	Y	U	Y
75	√				√								U	U	Y	Y	Y	U	Y	Y	U	Y
77						√							U	Y	Y	Y	Y	U	Y	Y	U	N
78		√					√						U	Y	Y	Y	Y	U	Y	Y	Y	N
79	√						√						U	Y	Y	Y	Y	U	Y	Y	U	Y
80	√						√				√		U	Y	Y	Y	Y	U	Y	Y	U	Y
81								√	√				U	Y	Y	Y	Y	Y	Y	Y	U	U
82									√				U	Y	Y	Y	Y	Y	Y	Y	Y	Y
83	√								√				U	Y	Y	Y	Y	U	Y	Y	Y	Y
84				√	√				√				U	Y	Y	Y	Y	N	Y	Y	U	U
85	√										√		U	Y	Y	Y	Y	N	Y	Y	U	Y
86											√		U	Y	Y	Y	Y	N	Y	Y	U	U
87		√										√	U	Y	Y	Y	Y	Y	Y	Y	U	Y
88		√										√	U	Y	Y	Y	Y	Y	Y	Y	U	Y
89										√		√	U	Y	Y	Y	Y	U	Y	Y	Y	Y

Y: yes with support; N: no without support or considerations; U: unknown.

the effectiveness of this method is based on a little sacrifice of feasibility. However, the authors did not consider node similarity and the influence of "friend" nodes on choosing new friends. More parameters can be added to evaluate the nodes as well. The authors did not prove the stability and robustness of this method and the ability of preserving the privacy of the shared information was not considered.

In a Wireless Sensor Network (WSN) based IoT network, the way for sensors and other objects to communicate is through Access Points (AP). When a sensor is making a decision about which AP to choose, it not only needs to consider the characteristics of each AP, like bandwidth resources and distributions, the position of itself and the qualities of communication channels, the actions of other sensors also play a nontrivial role. Ju and Shao [59] modeled the interactions among every sensor as a potential game, which has at least one NE point. An algorithm to compute NE was proposed in this paper as well. This method can achieve high efficiency with low computational complexity and all APs can achieve their optimal utilities. Nevertheless, this method can be further optimized by enhancing SC and R.

The emergence of IoT provides people a new way to provide and request services. These services are supported by all devices involved. If something happened to these devices, like power off and system crash, service supply may also be interrupted. Such a situation may exist that a device obtains more services than it requests. This causes unnecessary energy consumption and could reduce system lifetime. An evolutionary game was proposed to solve multi-application service selection from an overall view in IoT [60]. Each node that needs to select services is a player and the utility of each player is its estimated lifetime. All players' payoffs (lifetime) are computed and stored at a centralized controller. And then this controller computes the average payoff and broadcasts it to everyone. Only the player whose payoff is less than the average one will select another service randomly. The evolutionary equilibrium state can balance each player's payoff. This method is proved to be effective in preventing congestion in popular nodes and can handle the service selection problem globally. The experiment results prove the efficiency of this method for its solution is easy to compute. The authors also proposed a future direction to save communication overhead by studying group-based service selection. This method cannot satisfy the requirement of SC because its time cost increased sharply when the number of devices reaches to a certain number. PP and R were not considered by the authors as well.

Different from [60], Guijarro et al. studied the competition among service providers with a non-cooperative game [61]. These service providers compete for limited information rate in WSNs and the requirements from users. And these two competitions are assumed to happen at the same time. The authors also calculated Nash Equilibrium and gave specific explanation on how user sensitivity to the value-to-price ratio (i.e., the information rate a provider can get divided by the price a user can pay) and the number of service providers influences the existence and uniqueness of equilibrium in this game. Unfortunately, the utilities of service providers and users are increased based on the decrease of WSNs' benefit. And when users' sensitivity grows higher and higher, the feasibility of NE decreased. Thus, this proposed method cannot satisfy F and P. It did not take PP, R into consideration either.

Task Scheduling (TS)

In current IoT applications, nodes involved are more and more intelligent and autonomous. They can communicate and exchange information with other nodes and then change their strategies to achieve high profits. This could cost energy and reduce the nodes' lifetime as well. In addition, due to the powerful ability of IoT, tasks are heterogeneous with different computation requirements, storage costs and different purposes. Nodes in IoT cannot be fully trusted as well. The node connectivity is influenced by their mobility and then can join or leave the network at any time. The mobility also causes computation burden. Therefore formulating an effective and energy-aware task scheduling scheme is an inevitable problem in IoT.

Task cluster [64] is an important term in IoT. It consists of a number of nodes equipped with the same sensors to accomplish a certain task, like traffic monitoring and temperature monitoring, in a specific area. Each cluster has a cluster head to track and monitor and manage all involved nodes to share the burden of task loads.

Haghighi et al. [65] proposed a non-cooperative game with perfect information to formulate the interactions between base station and cluster-heads. The utilities of players and NE are calculated by an auction-based algorithm. The utility function of the cluster-head is related to its operation time. The longer it can survive, the more profits it can get. And the base station can only make profits when it serves the end-user's request. NE point is where all network entities maximize their profits. It is proved that this method can distribute multiple tasks optimally with little energy consumption. Comparing to our proposed requirement, PP, SC and R were not considered in this method.

A novel paradigm called Mobile-IoT-Federation-as-a-Service (MIFaaS) was proposed in [66]. An IoT Cloud Providers (ICPs) can involve all of its devices into a federation formed by a lot of cooperative ICPs. All resources in this federation can be shared by all participants. A repeated coalition formation game was formed by Farris et al. to prevent selfish actions of ICPs. Selfish ICPs can obtain more utilities at the NE point of this game than they can obtain when acting independently. A proof-of-concept performance evaluation showed this cooperative game can improve all players' payoffs and can accomplish more tasks than other non-cooperative game approaches. In simulations, the authors showed the efficiency and feasibility of this method in improving the rate of successful completion of tasks and improving the utilities of ICPs. The scalability was validated by applying this approach to a large application scenario with a big number of mobile devices. But the authors ignored privacy protection, security problems and the cooperation between ICPs from different clouds. Overall, the requirements that were not considered in this study are PP and R.

A collaborative stochastic game as introduced in [62] can also arrange tasks properly. In this scenario, task refers to arranging the receivers' energy reasonable, which can prolong system lifetime. There are also some non-cooperative solutions in the literature [63,64].

The authors in [64] formulated a non-cooperative game with auction to solve task scheduling problems in IoT with exploited D2D communications. In this paper, all the nodes that have the ability to accomplish the same task compete with each other to join a cluster. All the nodes choose strategies to maximum their own utilities. The Nash equilibrium point calculated from this game was proved to be optimal in the nodes' utility functions. The simulation results illustrated the efficiency and feasibility of this method even though the requirements of PP, SC and R are beyond consideration.

Bui et al. [63] gave a game theoretical solution about real-time IoT-based traffic light control. At first, they set up a connect intersection system for all entities to share information so that a controller can make real-time decision making efficiently. And then they proposed Cournot Model to provide control for normal situations. The Stackelberg game was applied to help the controller make decisions when there are priority vehicles, like ambulances and police cars, in this intersection. This approach can make the average waiting time of vehicles at a low level in comparison with other approaches. While it may not be profitable for all entities, it can be extended to a more complicated situation with multiple crossroads and different levels of emergency vehicles. The requirements that have not been considered in this paper are PP, R and P.

Resource Allocation (RA)

Various studies applied game theoretical methods in addressing resource allocation problems in IoT. We think most of them can also be used to achieve such objectives as power control, QoS and security.

Safdar et al. investigated in resource allocation problem for uplink Machine-to-Machine (M2M) communications in cellular networks [67] and heterogeneous cellular networks [60] from the perspective of game theory. They used both cooperative and non-cooperative games and the results showed that non-cooperative game can help players gain more profits while the cooperative one is fairer.

Kim proposed a Markov game based scheme [68] to allocate IoT resources and this scheme can also improve system performance while satisfying QoS. The players in this game are QoS schedulers who are instructed by the learning Markov game to choose optimal strategies. In each time generation, players estimate their own utilities and change their state transition probability. This game does not stop until all the players attain a stable status. The evaluation results showed that this approach can make more full use of resources with lower service delay in comparison with other approaches. Nevertheless, PP, SC and R were not considered.

Kim [69] presented a two-stage nested game to assign computation resource dynamically in Mobile Cloud IoT (MCIoT). In the first stage, the author used a non-cooperative bargaining game for partial offloading of applications in each mobile device. Each device chooses strategies to maximize its own utility. After repartition, one part of applications is computed locally while the other part is computed by computation resources allocated by an auction game. This is a distributed approach that can reduce computational complexity. The performance evaluation showed that this approach can save energy consumption, shorten application execution time and improve QoS satisfaction with low packet loss probability. However, this approach did not take the requirements of PP, SC and R into consideration.

Huang et al. exploited a location-awareness resource allocation approach based on a repeated non-cooperative game with complete information for D2D communications [70]. The players in this game are base stations and they compete for resource allocation quota with each other. The authors also provided a NE derivation algorithm. And then they extended this approach in an IoT environment and considered the situation that the NE does not exist [71]. The authors used a cooperative game to capture the interaction between two base stations, whose objective is to maximize the utilities of both. These two studies did not consider PP, SC and R.

Considering a number nodes connected by wireless networks in an IoT system, the neighboring nodes cannot use the same communication channel at the same time. Ju and Shao [72] addressed the distributed energy efficient channel management in IoT with a cooperative game. That is to say, the objective of all nodes is to maximize their total utilities. The authors summed up a conclusion that the NE of this game can achieve global optimization through theoretical analysis. Furthermore, they designed an efficient algorithm to compute this NE point. Experiment results showed that this cooperative game is efficient and stable due to the existence of collaboration. Nevertheless, PP, SC and R were not considered in this work.

5.2. Game theoretical methods for communications

QoS

Quality of Service (QoS) is an evaluation criterion for the overall performance of network services. Different users may have different requirement for QoS, which makes it difficult to control QoS, especially in a large-scale system, like IoT. Many literatures have taken QoS control into consideration while improving the performance of the IoT system.

The Markov game in [68] is formulated from the perspective of QoS control by Kim. This scheme can model environment uncertainties effectively and help IoT system agents dynamically change strategies with learning algorithms.

Abuzainab et al. [73] proposed a behavioral game based Cognitive Hierarchy (CH) theory to capture IoT nodes' characteristics like resource constraints, QoS needs and bandwidth requirements. The players in this game are IoT devices and they choose transmission probability and service rate to maximum their utilities respectively. Limited to finite computational resources and capabilities of IoT devices, some NE points cannot be reached. The authors used a CH-based iterative process to compute an optimal strategy for every player based on its beliefs. Simulation results showed that this solution can save more energy than traditional NE-based solutions. However, when more nodes are involved, the successful packet transmission rate decreases, which will cause decline of players' utilities. Thus the requirement of SC and T were not satisfied in this method. What is more, this game model did not take PP and R into consideration.

IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) is one of the most significant protocols in IoT. The authors in [74] modeled the congestion problem of nodes in 6LoWPAN as a non-cooperative game. The nodes in 6LoWPAN can be divided into sink nodes, intermediate nodes and leaf nodes. In this paper, the leaf nodes are the players who may act selfishly to send packets as many as they can without considering the network conditions when congestion happens. The payoff function of each node is its utility minus congestion cost and priority cost, which can be regarded as a constrained nonlinear optimization problem that can be solved by a mathematic solution. NE point can mitigate congestions and ensure profit of each player. Simulations executed in a real IoT application platform showed that this scheme can improve the QoS of the network, with regard to end-to-end delay, energy consumption, throughput, packet loss and weighted fairness index, according to other existing schemes. PP and SC were not considered in this work.

In order to achieve good performance with low energy and bandwidth consumption, authors in [75] found that all nodes cooperate with each other can save bandwidth and energy. They modeled the interactions among IoT nodes as a cooperative differential game and they used Shapley value to compute other nodes' impacts. Experiment results showed that the number of services is optimal when the factor of bandwidth cost and energy cost are the same. Nevertheless, this model can be improved by considering PP, SC and R.

The requirements and sensitivities on QoS parameters are different in different applications. Liu et al. [76] designed a multiple layer solution to channel congestion caused by mass data transmission. A game theoretical method was used to achieve dynamic spectrum sharing. The players in this game are primary users (PU) and Secondary users (SU). The interaction between PU and SU is modeled as principal–agent behaviors, and PU is the principal who has priority in using specific spectrum while SU is the agent who wants to buy PU's resource. Uncertain information was regarded as random variables to ensure the feasibility of this model. Simulations showed that the performance of this new network can be optimized. However, the existence of NE was beyond discussion. The utility of PU may decrease in some situations and how to find proper values of parameters should be explored. Therefore, PP, ST, SC, T and R were not considered in this paper.

Heterogeneous types of intelligent devices share information with each other in IoT. Kumar et al. [77] proposed a performance evaluation scheme based on a Bayesian coalition game. Each player in this game joins a coalition and has different conditional probability of transmitting data packets because the probability is related to distance. Different probabilities bring players different payoffs and they may choose to leave one coalition to anther for maximizing their payoffs. The authors found that this game can achieve its NE points in shorter time if the learning rates of the players are not constant. They evaluated the performance of this scheme with regard to end-to-end delay, packet delivery ratio and routing overhead. The requirements of PP, SC, R and P were not considered.

Traffic overload problem becomes more and more serve due to an excessive traffic demand. Park and Kim [78] proposed a Rubinstein bargaining game with the Vickery–Clarke–Groves(VCG) mechanism to solve the traffic congestion problem in IoT and improve QoS. The players in this game are Mobile Network Operator (MNO), Access Point Owners (APOs) and Internet of Things Modules (IoTMs). Each APO covers a number of IoTMs, which want to offload their cellular traffics. The VCG mechanism can help APO choose the most adaptable IoTM to maximize its profit. The cooperation between MNO and APOs is modeled as a Rubinstein bargaining game where they negotiate with each other to maximize their payoff synchronously and fairly. The discussion about NE is missed. This scheme is proved to be effective and feasible in alleviating network congestion and improving the QoS of network through theoretical analysis and simulations. It can also be applied into other application scenarios. Overall, the requirements that were not considered by the authors are PP, ST and R, respectively.

How to associate different types of devices with a correct base station is a significant task in heterogeneous cellular networks integrated with IoT. Elhattab et al. [79] proposed a cooperative Nash bargaining game among two groups of base stations to model this association problem. They negotiate and exchange players with each other until they both satisfy with their own payoffs. Simulation results showed that this scheme is correct and fair in device association with high QoS. With regard to our proposed requirements, the main shortcomings of this method are there is no research on the existence of NE and it did not take PP, SC and R into consideration.

Topology Optimization (TO)

Some researchers realized that special attention should be paid to topology control in the field of IoT. An efficient topology control scheme can improve node connectivity with little energy consumption. Zhao et al. [80] used a non-cooperative potential game to capture the selfishness and mobility of IoT nodes. The utility function of player is related to various factors, e.g., node connectivity and energy consumption. Due to the mobility of nodes, the network topology changes as time goes by and each node needs to change its transmission power to achieve an optimal utility. The NE point calculated in this game is energy efficiency. The simulation results illustrated that the scheme proposed in this scheme can enhance network connectivity with little compromise in energy consumption, thus profitability was not satisfied. What' more, the requirements of PP, SC and R were beyond the authors' consideration.

Routing Protocol Design (RP)

In order to prolong the lifetime of IoT networks, many researchers focus on designing energy efficient routing protocols that can save energy in transmitting data.

Congestion problem is difficult to avoid and hard to be eliminated by existing protocols in low-power and lossy networks. Ma et al. [81] focused on addressing the congestion problem in networks with a tree topology. A tree-like network consists of a large number of nodes. If a node A is extended from another node B, then B is A's parent node and A is B's child node. They used net packet flow rate, which is the difference between packet generation rate and packet service rate, as a metric to evaluate and detect congestions on parent nodes. When congestion is detected, a parent node informs all of its children nodes to take the advantage of a potential game to find a new parent node for improving network performance. Due to the characteristic of potential game, NE always exists. A rank was added in designing payoff functions to make the model robust. If the congestion problem cannot be addressed by the parent-selection procedure successfully, the parent node chooses a rate adjustment scheme [93–95], which may decrease the QoS of this network. Thus, P is not satisfied. PP and SC were not considered as well.

Lin and Wang [82] used an evolutionary game to formulate the competition between nodes with low or high energy. The players choose to be either a cluster head or members according to the strategies derived from game theory to maximum their utilities. The NE point of this game can also prolong the system's lifetime. Experiment results proves the effectiveness of this protocol in saving energy consumption and improving network performance. Nevertheless, PP, SC and R were not considered.

Elsemary [83] designed a routing protocol in D2D communications with IoT applications that can detect malware attacks using a non-cooperative zero-sum repeated game. Different from previous work [96–98], this protocol can capture and reduce the influence of the dynamic and unpredictable changes of the malware. The general procedure of this protocol can be described as follows. At first, a node broadcasts its route request and the devices received this message would relay it until the message is received by a target device. The node that broadcasts information receives route detection capability from every involved device and calculates an overall detection rate. And then the node chooses the best route from all of the routes it receives under the instruction of game theory. NE exists in this game and provides optimal defend strategies. Unfortunately, this protocol is built on the trustworthiness of every device and cannot resist internal attacks. What is more, the authors did not consider PP and R when designing this model. And whether this model is scalable is beyond discussion.

5.3. Game theoretical methods for network security

Smart devices in IoT are limited in terms of resources and energy. They are easily to be compromised. Compromised devices could destroy the IoT system from within. In this section, we investigate into game theoretical methods in addressing IoT security problems.

Honeypot (H)

Honeypot, as a computer security mechanism, has been widely used in detecting network attacks. Honeypot is the same as normal computer entities except that it is managed and monitored independently. Setting a honeypot with some faultiness can allure attackers and then monitors can collect their information. La et al. [84] designed a honeypot-based deception mechanism in IoT. The interaction between a defender and an attacker was formulated as a repeated Bayesian game with incomplete information because the defender does not know the attacker's type. An attacker can get rewards by executing attacks successfully and gain benefits by probing at a regular target with a little cost. But it will be punished if it is caught by a honeypot. The payoff of the defender consists of the revenue for detecting a normal user, the reward for capturing an attacker, the cost for deploying honeypots, the loss caused by probed targets and the punishment when the attacker conducts a successful attack. By deriving NE, the authors gave a defender instruction about which strategies it should choose under different situations. This method can be adapted to suit other IoT networks. Unfortunately, honeypot can only identify and analyze attacks without defending them effectively. The requirements that need to take into consideration in the future are PP, R and P.

Security Problems (SP2)

Chen et al. [85] proposed a zero-sum game based on an information fusion defense mechanism to model the interaction between attackers and defenders. Information fusion alleviates the damage caused by intentional attacks with little communication overhead. The existence of NE proves the robustness and the stability of this mechanism. The authors applied this mechanism in Internet-oriented networks and cyber-physical system-oriented networks (e.g., smart grid) to verify its effectiveness and performance. And the results showed that this mechanism is efficiency and feasible in analyzing network robustness and enhancing performance in large-scale networks. PP is the only requirement that the authors did not consider.

Hamdi and Abie [86] used a Markov game to model uncertain and dynamic parameters, like memory resources, communication environments, energy depletion models and threat models for solving security problems. The existence of NE was proved but it is difficult to calculate. Therefore, the authors proposed Pareto-efficient solutions, where at least one player can obtain the highest benefit. This adaptive game theoretical model cannot only hide players' mutual actions, but also extend the system's lifetime by almost 50%, which is the result of the simulations showed in this paper. This method is scalable that can be applied to other threat models. However, PP and R were not considered by the authors.

Namvar et al. proposed a Colonel Blotto game [87] to defend jamming in IoT. In this model, the authors assumed IoT nodes to be passive, which cannot defend jamming due to limited resources. An anti-jamming procedure is executed by an IoT controller independently. The players employ a mixed strategy because there is no pure NE in the Blotto game. An evolutionary-based algorithm is used to compute an optimal strategy in this model. The simulation results illustrated this method to be powerful in maintaining the performance of the network and the average payoff of IoT nodes were increased. When applying this method to a network with a large size, its efficiency in defending jamming decreases. Thus this method cannot satisfy the requirement of SC. Other requirements that the authors did not consider are PP, R and P.

The energy-aware trust derivation scheme [56] as introduced before can also ensure the security of IoT systems. In this approach, replying to a trust request may not always happen to save energy. When the number of participating nodes is less than that of recommendations, calculated by a method of risk strategy analysis, all nodes need to reply the trust request to ensure the security of the network. A new scheme that can reduce the cost for trust requests is needed to enhance its efficiency. In addition, PP, SC, R and P should be considered as well.

Anomaly Detection (AD)

A smart attacker has potential to hind its property and a normal node may act as an attacker when suffering from malfunctions. Effective and lightweight anomaly detection mechanisms are needed.

Sedjelmaci et al. [88] proposed an anomaly detection approach based on a learning algorithm under the situation where a new attack pattern is detected. Considering IoT devices with low resources cannot attend anomaly detection all the time, the authors proposed a game theoretical way to only activate anomaly detection when a new attack happens. Reputation was introduced in this paper as well to evaluate the actions of intrusion detection systems and attackers. Simulation results showed this method can detect anomaly with high accuracy and little energy consumption by comparison with existing anomaly detection schemes. Unfortunately, the efficiency and accuracy of this method decrease as the scale of the network increases. Thus it cannot fulfill the requirement of SC for now. PP and R were beyond the authors' consideration as well.

It is difficult to identify and mitigate attacker tags in a passive RFID network in IoT, which consists of one tag reader and a large number of tags. Tsiropoulou et al. [89] modeled the interaction among normal and attacker tags as a non-cooperative game and proposed a distributed but lightweight algorithm to derive the NE point of this game. Simulation results showed the efficiency and feasibility of this method. More types of attacks should be considered to make it scalable. PP, R and P are the requirements that the authors did not take into consideration.

5.4. Game theoretical methods for other applications (Ap)

Internet of Vehicles (IoV) appears with the rapid development of IoT, where a large number of vehicles connect, communicate and share information with each other. After collecting and processing this information, relay nodes will help broadcast this synthetic information to different destinations. It is difficult to process such a large number of heterogeneous data transmitted at different time and from different places. The existence of uncooperative relay nodes also increases the complexity in computation. Kumar et al. [90] used a Bayesian coalition game to address this problem and the players are the vehicles deployed with Learning Automata (LA). Each player uses a learning algorithm to make decisions by considering the strategies of the other players and they will get a reward or a punishment based on their strategies. A reward and punishment mechanism was proposed to regulate the actions of players. Experimental results showed the relationship among learning rate, the number of actions and successful transmission. What is more, they also analyzed the probability to achieve NE with complete or incomplete information. The authors stated this method can be used to set up a secure RFID system. Nevertheless, PP and R were beyond consideration.

Then Kumar et al. [91] proposed a stochastic coalition game for data dissemination in IoV. Vehicles with LA choose their strategies according to the feedback from an environment and past actions, which is the same as that in [90]. Simulation results illustrated that this proposed scheme can achieve a high packet delivery ratio because of the formation of coalition. Bayesian coalition structure ensures players to join and leave coalition flexibly, which makes the coalition structure stable with reduced delay. The complexity of calculating NE is low by applying an adaptive learning mechanism, which in turn reduces maintenance cost. The authors stated that their method is scalable. The punishment and reward mechanism can induce players to tell the truth. Unfortunately, PP and R were beyond consideration in this method.

A non-cooperative game based IoT service pricing competition among service providers is proposed in [51]. The payoff of each service is the total benefits of all demanded number of this service minus the cost to execute it. The best strategy of each service provider is to choose the price that can maximum its payoff. This is just a very simple example. The authors pointed out several future directions.

Pouryazdan et al. [92] considered mobile crowdsensing problems in cloud-centric IoT applications. The exact problem they wanted to tackle was how to attract more trustworthy mobile users. The authors proposed a repeated game to induce users to act honestly. In each sub-game, each user decides to participate in a sensing task or not and whether acts honestly and Subgame Perfect Nash Equilibrium (SPNE) can be obtained. After that, the quality of its sensed data is calculated to define its trustworthiness. Each user needs to vote the others and is voted as well. The vote-based reputation of each user consists of the trustworthiness of its sensed data and its vote capacity (i.e., T). The simulation results showed the effectiveness of this method in ensuring the utilities of users and the platform (i.e., P). More significantly, it can accurately avoid paying reward to malicious users. The authors stated their reward allocation to be robust. PP and SC were the two requirements that the authors did not consider.

6. Game modeling in a bitcoin system and other HMNs

6.1. Game theoretical methods for bitcoin systems

Bitcoin [4] is an emerging monetary mechanism, which is one kind of decentralized cryptocurrencies without central authority. Every transaction is recorded in a public distributed ledger named blockchain. The blockchain is kept and updated by miners that try to solve mathematical problems. Only the first one who finds the answer (proof-of-work) can be awarded with a certain amount of Bitcoin. Recently, a number of miners start to join mining pools and work the mathematical problems together. All miners in the awarded pool share the overall utility according to their contributed computation powers.

Several attacks have been investigated by researchers with regard to Bitcoin. The decentralization and anonymity in a Bitcoin system makes dishonest actions untraceable. If an attacker can bribe a certain number of miners to work for him [99], he can change any transactions and obtain illegal wealth. A mining pool may suffer from DDoS attacks, the mining power is cut down and miners in it would leave for another reliable pool to chase higher rewards. Another kind of attack is called Sybil attack [100] that refers to a situation where a mining pool does not immediately publish the blocks it discovers. Then, honest miners continue to waste resources on these discovered blocks and forking happens. When the length of the pool's private chain reaches a certain value, the selfish pool publishes its private chain to invalid other chains. A large and open mining pool without verifying miners may suffer from such a block withholding attack [101] from small pools. An attacker in a mining pool pretends to be a normal miner by reporting partial but meaningless proof-of-work. Game theory starts to be used in the Bitcoin system for overcoming the above attacks.

Johnson et al. [102] used game theory to model the interaction between a big mining pool and a small mining pool. Each mining pool chooses to execute a DDoS attack to other players or not. The authors analyzed the NE under different success probability of DDoS with or without an attack cost. The results showed that a larger mining pool is more likely to attack and to be attacked than a small pool.

Laszka et al. [103] extended [102] with consideration of mining pool migration. They calculated under which condition these two players will or will not attack each other and under which condition only one player chooses to attack. Their results can help mining pools choose proper parameters to avoid being attacked.

Luu et al. [104] presented a possible situation that a miner may divide its computation power into several parts and join into different mining pool in order to obtain as more as possible profits. They formulated this as a game and used it to analyze the security of existing protocols in mining pools. It shows that most pool protocols cannot resist block withdraw attacks and the best strategy for a player is to attack at a random probability.

Eyal [105] found the competition among miner pools, which was modeled as the prisoner's dilemma. The best choice for each player is not to attack but this is not a NE point. Attacking each other is NE, but this reduces their profits simultaneously. A mining pool attacked by block withholding attacks can be identified as being attacked by suffering a long-term revenue density decline. However, there are still no effective approaches to detect and remove the attackers. Therefore, honest miners in an attacked mining pool would leave for private pools that only trusted miners can join.

Kim [106] proposed a novel protocol based on a group bargaining game model. It shows all miners in a mining pool share computation powers with each other to obtain the highest profits. Unfortunately, this protocol suffers from security issues as well.

6.2. Game theoretical methods for other HMNs

In this section, we briefly discuss the usage of game theory in the other HMNs: public-resource computing, web search engines, online markets, social media, multiplayer online games and virtual worlds and mass collaborations.

With keywords public resource computing and game theory, we find that most literatures are relevant with cloud computing. Some works can manage trading and allocate computing power fairly with game theory [107], some can estimate the cost of redundancy in resource allocation [108] and prevent attacks [109] and some can help each user find optimal allocation of resources [110]. When reviewing game theoretical methods in web search engines, we find that game theory has been used in analyzing the competition among engines and motivating them to provide high-quality products [111]. It can also help search engines find the optimal auction mechanism [112]. Based on our exploration, we found that there are few literatures about game theoretical methods in the other four types of HMNs.

Throughout our research, we found that game theoretical study in HMNs is still a new research area, which attracts our efforts to explore. HMNs evolves from the existing elemental types when modern technologies develop as time goes by. Having a general overview and detailed understanding of these elemental HMNs could greatly help future research on evolved HMNs.

7. Open issues and future directions

7.1. Open issues

Through the above survey on game theoretical methods in different types of HMNs, game theory has shown its advantages in capturing, modeling and analyzing the interactions among players, helping player make decisions, selecting behaving strategies and regulating their actions. For example, game theory has been used to enhance the level of participation in crowdsourcing systems and help design efficient incentive mechanisms to solve the social problems in crowdsourcing systems, such as free-riding and false-reporting problems. In IoT systems, lots of game theoretical methods have been designed to allocate resource and scheduling tasks effectively while improving the performance of IoT. Some methods can solve unavoidable security problems as well. Even in the emerging Bitcoin system, game theory has also showed it power for solving some critical issues. However, we also find a number of open issues in our survey.

First, most of reviewed work in crowdsourcing cannot satisfy or do not consider all the requirements as we proposed in Section 3, especially the requirements on scalability and robustness. A number of incentive mechanisms cannot guarantee robustness, which means the designed mechanisms cannot reach an equilibrium state quickly or some unintentional errors may significantly impact the final results of the games. All of these methods are suitable for the situations that the authors considered. However, whether these methods can be extended to a scalable situation was beyond discussion.

Second, none of existing work in crowdsourcing achieves design objectives in a holistic manner. Some approaches in the literatures can enhance the participation level of workers by designing incentive mechanisms and some can reduce the cost of crowdsourcing platform. Some can suppress malicious actions of selfish players by applying punishment mechanisms and some can make sure the workers provide high-quality solutions to every task and induce them to finish tasks as soon as possible through incentive or payment methods. Nevertheless, none of them can achieve all the above objectives simultaneously.

Third, existing game theoretical methods in a crowdsourcing system, especially a mobile crowdsourcing system, seldom took privacy into consideration. The workers may provide solutions that include personal and sensitive information, like personal locations. The crowdsourcer may show its intention and interests to the crowdsourcing platform. If a crowdsourcing system cannot preserve worker privacy and crowdsourcer privacy, potential risks will cause low participation level with poor efficiency.

Fourth, current game theoretical methods lacks concern on balancing between privacy and traceability, e.g., in IoT systems. According to our review on game theory usage in the IoT systems, most researchers focused on how to arrange each nodes and required tasks properly. Existing solutions can save energy consumption and prolong system lifetime. How to ensure QoS by inducing more participants and detect or even defend attacks to ensure the security of the systems have aroused researchers' attentions as well. However, as we stated before, IoT integrates the characteristics of crowdsensing and social media together. Therefore, privacy should be considered, especially in designing content-aware schemes and sensing-task-based schemes. The services provided by different devices should be traceable so that when non-cooperative action happens, selfish and harmful players can be traced and punished. The balance between privacy and traceability should be paid special attention.

Fifth, scalability and robustness are not well supported in the mechanisms derived by the game theory. There is a common problem in game theoretical usage in both crowdsourcing and IoT. Most existing researches did not take scalability and robustness into consideration. If the parameters selected in one method cannot be collected in another application scenario, the method is limited in a certain situation. IoT is a massive network that consists of thousands, millions or even trillions of smart devices. Such a system should be robust enough to resist turbulences. Otherwise, it cannot survive in different situations for a long time.

Sixth, the literature lacks a uniform standard to compose information or data that are collected by different machines. Different smart devices provide different kinds of information or data, how to combine these data with a uniform standard when they cooperate with each other to complete a task is beyond consideration. The computation cost and time should be controlled under a certain degree to ensure real-time services. What is more, the proposed methods should support big data, especially when the method needs the participation of some central controllers. Otherwise, it cannot cater for the rapid development of IoT systems and HMNs.

Seventh, how to solve dilemma when there are multiple equilibria is still an open problem. Traditional game theory works excellently when the number of players is not too big. However, in IoT systems, massive smart devices are mostly involved and it is really hard to predict all players' actions preciously. It is impractical to assume all players are completely rational to choose proper strategies according to the instructions of NE. Evolutionary game has been used in various application scenarios and it has been used to predict the development trend of populations in large-scale networks. However, dilemma happens when there are two equilibria in these games.

Eighth, there are many open issues related to security, privacy and efficiency in the Bitcoin systems. Bitcoin is the most important distributed digital currency that has attracted the attention of people all over the world. Now it has been highly recognized and can be changed into other currencies, products and services. Because of its anonymity, it can be made use of doing illegal things such as extortion and money laundering. The operations in Bitcoin are accompanied with a great of computation power consumption as well. Further research is needed in Bitcoin, especially its security, privacy and efficiency.

Last but not the least, we believe some open issues exist in other types of HMNs in terms of game theoretical studies. The interactions among humans and machines in these HMNs that have not been considered in our paper are different but similar to those in crowdsourcing, crowdsensing and IoT. Similar opens issues exist in other types of HMNs. But additional open issues could exist due to special characteristics of other types of HMNs. We leave this in our future study.

7.2. Future directions

In order to improve the performance of HMNs, we further propose several future research directions, focusing more on game theoretical studies. Inspired by the above analysis, we point out some possible applications of game theory in several emerging areas as well.

First, a concrete and generic trust management system is highly expected in the design of HMN. Few existing studies in crowdsourcing and IoT systems have taken privacy preservation into consideration. In order to tackle this problem, trust and reputation can be used to build a multi-layer service provision mechanism. Only requesters with high reputation can obtain privacy-related services and betrayals will be punished. Reasonable reward and punishment mechanisms can encourage players to choose strategies cooperatively without compromise system performance. Trust management is a difficult but essential part in preserving privacy, which should be seriously studied in game theoretical modeling.

Second, some perturbation parameters should be considered in game modeling when designing the payoff functions of players in order to improve the fault tolerance or robustness of a designed game. Perturbation can guarantee the robustness of proposed methods due to the universal existence of accidents in practical society. The method of standardizing network and data parameters are also needed for making game-based methods adaptive so that it can be used in various application scenarios.

Third, we still need to make efforts to solve open issues as listed in Section 7.1. We can use undetermined parameters to indicate each game designer's preference for every problem that should be solved. We can make full use of the related knowledge about equilibrium and derive the parameter intervals for different strategies. By correctly setting relevant parameters, we can force players to choose the strategies that can meet our requirements.

Fourth, game theoretical analysis with consideration on privacy and traceability is an interesting research topic worth our investigation. With more and more smart devices are involved in IoT systems, light-weight big data processing methods based on information composition and fusion are needed. The methods should be able to protect the privacy of these devices. The actions of each device should also be tracked to ensure the implementation of subsequent rewards and punishment mechanisms.

Fifth, evolutionary game should be widely adopted in analyzing interactions in different systems with a large number of participants since it can direct the development trend of the participants' strategy choices. This is a new research direction that requests deep insight investigation in the future.

Sixth, Bitcoin security and privacy request serious research. Applying game theory could be a good research method in this study. Bitcoin is built based on the structure of a decentralized P2P network. Transactions can be conducted and spread in such a system. This system can be executed because there are a large number of miners who are working hard to complete mathematic problems. How to induce more and more miners to participate in and how to prevent miners from being attacked are crucial in terms of maintaining this system in a healthy and secure manner.

Finally, game theoretical analysis with regard to other types of HMNs should be researched. Game theory can work as a bedrock for handling problems in hybrid HMNs.

8. Conclusions

Profiting from the inherent advantage of game theory in capturing the interactions among players and providing comprehensive guides in strategy selections, plenty of problems in various HMN application scenarios have been solved skillfully from the view of economics. In this paper, we proposed a number of requirements on game theoretical modeling and analysis and thoroughly investigated into existing work about game theoretical methods in such HMNs as crowdsourcing and IoT, as well as Bitcoin. Bitcoin is an emerging technology that has not yet been widely investigated, so we just briefly introduced some game theoretical studies for the Bitcoin system. Through our survey, we found a number of open issues. For important examples, the existing literatures in crowdsourcing and IoT cannot address all the requirements emerged in practical applications. Scalability and robustness were often missed when formulating a game model or an incentive mechanism. Privacy preservation was generally ignored by most existing studies. Based on our survey and findings, we proposed a number of future research directions. We think game theoretical study in HMNs is still a new research area that attracts our efforts to explore.

Acknowledgments

This work is sponsored by the National Key Research and Development Program of China (grant 2016YFB0800704), the NSFC (grants 61672410 and U1536202), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), the 111 project (grants B08038 and B16037), and Academy of Finland (grant 308087).

References

[1] A. Eide, J. Pickering, T. Yasseri, G. Bravos, A. Istad, V. Engen, M. Tsvetkova, E. Meyer, P. Walland, M. Luders, Human-machine networks: Towards a typology and profiling framework, in: International Conference on Human-Computer Interaction, Springer, 2016, pp. 11–22.

[2] V. Engen, J. Pickering, P. Walland, Machine agency in human-machine networks; impacts and trust implications, in: International Conference on Human-Computer Interaction, Springer, 2016, pp. 96–106.
[3] M. Tsvetkova, T. Yasseri, E.T. Meyer, J.B. Pickering, V. Engen, P. Walland, M. Luders, A. Folstad, G. Bravos, Understanding human-machine networks: A cross-disciplinary survey, ACM Comput. Surv. 50 (2017).
[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).
[5] Y. Mo, H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyberphysical security of a smart grid infrastructure, Proceedings of the IEEE 100 (1) (2011) 195–209.
[6] S. Zonouz, P. Haghani, Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior, Comput. Secur. 39 (2013) 190–200.
[7] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, A. Martin, An evolutionary game-theoretic framework for cyber-threat information sharing, in: IEEE International Conference on Communications, 2015, pp. 7341–7346.
[8] D. Tosh, S. Sengupta, C.A. Kamhoua, K.A. Kwiat, Establishing evolutionary game models for cyber security information exchange (cybex), Journal of Computer and System Sciences.
[9] D.K. Tosh, S. Sengupta, S. Mukhopadhyay, C.A. Kamhoua, K.A. Kwiat, Game theoretic modeling to enforce security information sharing among firms, in: IEEE International Conference on Cyber Security and Cloud Computing, 2016, pp. 7–12.
[10] Q. Zhu, J.B. Song, T. Basar, Dynamic secure routing game in distributed cognitive radio networks, in: Global Telecommunications Conference, 2011, pp. 1–6.
[11] W. Wang, A. Kwasinski, Z. Han, A routing game in cognitive radio networks against routing-toward-primary-user attacks, in: Wireless Communications and NETWORKING Conference, 2014, pp. 2510–2515.
[12] L. Gao, Z. Yan, L.T. Yang, Game theoretical analysis on acceptance of a cloud data access control system based on reputation, IEEE Transactions on Cloud Computing.
[13] Y. Shen, Z. Yan, R. Kantola, Analysis on the acceptance of global trust management for unwanted traffic control based on game theory, Comput. Secur. 47 (2014) 3–25.
[14] R.B. Myerson, Game Theory: Analysis of Conflict, Harvard University Press, 1997.
[15] C. Davidson, R. Deneckere, Long-run competition in capacity, short-run competition in price, and the cournot model, The Rand J. Econ. (1986) 404–415.
[16] S.A. Matthews, Veto threats: Rhetoric in a bargaining game, Q. J. Econ. 104 (2) (1989) 347–369.
[17] W.H. Press, F.J. Dyson, Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent, Proceedings of the National Academy of Sciences of the United States of America 109 (26) (2012) 10409–10413.
[18] C. Hilbe, B. Wu, A. Traulsen, M.A. Nowak, Evolutionary performance of 1540 zero-determinant strategies in multiplayer games, Journal of Theoretical Biology 374 (2015) 115–124.
[19] L.S. Shapley, Stochastic games, Proceedings of the National Academy of Sciences 39 (10) (1953) 1095–1100.
[20] J.R. Marden, G. Arslan, J.S. Shamma, Cooperative control and potential games, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 39 (6) (2009) 1393–1407.
[21] N.N. Krasovskii, A positional differential game, Trudy Matematicheskogo Instituta Imeni VA Steklova 169 (1985) 159–179.
[22] B. Roberson, The colonel blotto game, Econ. Theory 29 (1) (2006) 1–24.
[23] C.F. Camerer, Progress in behavioral game theory, J. Econ. Perspect. 11 (4) (1997) 167–188.
[24] S. Hart, Shapley value, Discussion Paper.
[25] X. Zhang, G. Xue, R. Yu, D. Yang, J. Tang, Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing, IEEE Internet of Things Journal 2 (6) (2015) 562–572.
[26] D. Yang, G. Xue, X. Fang, J. Tang, Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones, Biol. Cybern. 24 (3) (2016) 1732–1744.
[27] T. Luo, S.S. Kanhere, S.K. Das, H.-P. Tan, Incentive mechanism design for heterogeneous crowdsourcing using all-pay contests, IEEE Trans. Mob. Comput. 15 (9) (2016) 2234–2246.
[28] I. Koutsopoulos, Optimal incentive-driven design of participatory sensing systems, in: INFOCOM 2013 Proceedings IEEE, IEEE, 2013, pp. 1402–1410.
[29] D. Easley, A. Ghosh, Behavioral mechanism design: Optimal crowdsourcing contracts and prospect theory, 2015, pp. 679–696.
[30] Y. Lewenberg, O. Lev, Y. Bachrach, J.S. Rosenschein, Agent failures in all-pay auctions, IEEE Intell. Syst. 32 (1) (2017) 8–16.
[31] J. Peng, Y. Zhu, W. Shu, M.Y. Wu, Behavior dynamics of multiple crowdsourcers in mobile crowdsourcing markets, IEEE Network PP (99) (2016) 12–16.
[32] Y. Gao, Y. Chen, K.J.R. Liu, On cost-effective incentive mechanisms in microtask crowdsourcing, IEEE Transactions on Computational Intelligence and Ai in Games 7 (1) (2015) 3–15.
[33] X. Xu, W. Wu, Y. Wang, Y. Wu, Software crowdsourcing for developing software-as-a-service, Front. Comput. Sci. 9 (4) (2015) 554–565.
[34] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han, Y. Li, Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems, Sensors 16 (4).
[35] D. Yang, G. Xue, X. Fang, J. Tang, Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing, in: International Conference on Mobile Computing and Networking, 2012, pp. 173–184.
[36] B.A. Huberman, D.M. Romero, F. Wu, Crowdsourcing, attention and productivity, CoRR abs/0809.3030. URL arXiv://arxiv.org/abs/0809.3030.
[37] H. Zhang, E. Horvitz, Y. Chen, D.C. Parkes, Task routing for prediction tasks, in: International Conference on Autonomous Agents and Multiagent Systems, 2012, pp. 889–896.
[38] J.M. Hellerstein, D.L. Tennenhouse, Searching for jim gray: A technical overview, Communications of the ACM 54 (7) (2011) 77–87.
[39] Y. Zhang, M. van der Schaar, Reputation-based incentive protocols in crowdsourcing applications, in: INFOCOM, 2012 Proceedings IEEE, IEEE, 2012, pp. 2140–2148.
[40] B. Hoh, T. Yan, D. Ganesan, K. Tracton, T. Iwuchukwu, J.-S. Lee, Trucentive: A game-theoretic incentive platform for trustworthy mobile crowdsourcing parking services, in: Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on, IEEE, 2012, pp. 160–166.
[41] S. Luo, Y. Sun, Y. Ji, D. Zhao, Stackelberg game based incentive mechanisms for multiple collaborative tasks in mobile crowdsourcing, Mobile Netw. Appl. 21 (3) (2016) 506–522.
[42] V. Naroditskiy, N.R. Jennings, P. Van Hentenryck, M. Cebrian, Crowdsourcing contest dilemma, J. Royal Soc. Interface 11 (99) (2014) 20140532.
[43] Q. Hu, S. Wang, L. Ma, X. Cheng, R. Bie, Solving the crowdsourcing dilemma using the zero-determinant strategy: Poster, in: Proceedings of the 17th ACM International Symposium on Mobile *Ad Hoc* Networking and Computing, ACM, 2016, pp. 373–374.
[44] A.F. Anta, C. Georgiou, M.A. Mosteiro, D. Pareja, Algorithmic mechanisms for reliable crowdsourcing computation under collusion, PloS one 10 (3) (2015) e0116520.
[45] Z. Hu, W. Wu, A game theoretic model of software crowdsourcing, in: Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on, IEEE, 2014, pp. 446–453.
[46] Y. Moshfeghi, A.F.H. Rosero, J.M. Jose, A game-theory approach for effective crowdsource-based relevance assessment, ACM Trans. Intell. Syst. Technol. (TIST) 7 (4) (2016) 55.
[47] J. Lu, C. Tang, X. Li, Q. Wu, Designing socially-optimal rating protocols for crowdsourcing contest dilemma, IEEE Trans. Inf. Forensic Secur. 12 (6) (2017) 1330–1344.
[48] J. Peng, Y. Zhu, W. Shu, M.-Y. Wu, When data contributors meet multiple crowdsourcers: Bilateral competition in mobile crowdsourcing, Comput. Netw. 95 (2016) 1–14.
[49] X. Ma, J. Ma, H. Li, Q. Jiang, S. Gao, Rtrc: A reputation-based incentive game model for trustworthy crowdsourcing service, China Commun. 13 (12) (2016) 199–215.
[50] S. Wang, L. Li, W. Sun, J. Guo, R. Bie, K. Lin, Context sensing system analysis for privacy preservation based on game theory, Sensors 17 (2) (2017) 339.
[51] D. Niyato, X. Lu, P. Wang, D.I. Kim, Z. Han, Economics of internet of things: An information market approach, IEEE Wirel. Commun. 23 (4) (2016) 136–145.
[52] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[53] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the internet of things (iot), IEEE Internet Initiative (1).
[54] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (3) (2014) 120–134.
[55] M. Yun, B. Yuxin, Research on the architecture and key technology of internet of things (iot) applied on smart grid, in: Advances in Energy Engineering (ICAEE), 2010 International Conference on, IEEE, 2010, pp. 69–72.
[56] J. Duan, D. Gao, D. Yang, C.H. Foh, H.-H. Chen, An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications, IEEE Internet of Things Journal 1 (1) (2014) 58–69. 1645.
[57] S. Kim, Cognitive hierarchy thinking based behavioral game model for iot 1650 power control algorithm, Comput. Netw. 110 (2016) 79–90.
[58] Y. Xiao, Z. Xiong, D. Niyato, Z. Han, L.A. DaSilva, Full-duplex machine-to-machine communication for wireless-powered internet-of-things, in: Communications (ICC), 2016 IEEE International Conference on, IEEE, 2016, pp. 1–6.
[59] C. Ju, Q. Shao, Energy efficiency oriented access point selection for cognitive sensors in internet of things, Int. J. Distrib. Sensor Netw. 11 (10) (2015) 619546.
[60] J. Na, K.-J. Lin, Z. Huang, S. Zhou, An evolutionary game approach on iot service selection for balancing device energy consumption, in: e-Business Engineering (ICEBE), 2015 IEEE 12th International Conference on, IEEE, 2015, pp. 331–338.
[61] L. Guijarro, V. Pla, J.-R. Vidal, M. Naldi, Game theoretical analysis of service provision for the internet of things based on sensor virtualization, IEEE J. Sel. Areas Commun. 35 (3) (2017) 691–706.

[62] L. Militano, M. Nitti, L. Atzori, A. Iera, Using a distributed shapley-value based approach to ensure navigability in a social network of smart objects, in: Communications (ICC), 2015 IEEE International Conference on, IEEE, 2015, pp. 692–697.
[63] K.-H.N. Bui, J.E. Jung, D. Camacho, Game theoretic approach on real-time decision making for iot-based traffic light control, Concurrency and Computation: Practice and Experience 29 (11).
[64] E. Abd-Elrahman, H. Afifi, L. Atzori, M. Hadji, V. Pilloni, Iot-d2d task allocation: An award-driven game theory approach, in: Telecommunications (ICT), 2016 23rd International Conference on, IEEE, 2016, pp. 1–6.
[65] M. Haghighi, K. Maraslis, T. Tryfonas, G. Oikonomou, A. Burrows, P. Woznowski, R. Piechocki, Game theoretic approach towards optimal multi-tasking and data-distribution in iot, in: Internet of Things (WFIoT), 2015 IEEE 2nd World Forum on, IEEE, 2015, pp. 406–411.
[66] I. Farris, L. Militano, M. Nitti, L. Atzori, A. Iera, Mifaas: A mobile-iot-federation-as-a-service model for dynamic cooperation of iot cloud providers, Future Gener. Comput. Syst. 70 (2017) 126–137.
[67] H. Safdar, N. Fisal, R. Ullah, W. Maqbool, F. Asraf, Z. Khalid, A. Khan, Resource allocation for uplink m2m communication: A game theory approach, in: Wireless Technology and Applications (ISWTA), 2013 IEEE Symposium on, IEEE, 2013, pp. 48–52.
[68] S. Kim, Learning-based qos control algorithms for next generation internet of things, Mobile Information Systems (2015).
[69] S. Kim, Nested game-based computation offloading scheme for mobile cloud iot systems, EURASIP Journal on Wireless Communications and Networking 2015 (1) (2015) 229.
[70] J. Huang, Y. Yin, Y. Zhao, Q. Duan, W. Wang, S. Yu, A game-theoretic resource allocation approach for intercell device-to-device communications in cellular networks, IEEE Transactions on Emerging Topics in Computing 4 (4) (2016) 475–486.
[71] J. Huang, Y. Yin, Q. Duan, H. Yan, A game-theoretic analysis on context-aware resource allocation for device-to-device communications in cloud-centric internet of things, in: International Conference on Future Internet of Things and Cloud, 2015, pp. 80–86.
[72] C. Ju, Q. Shao, Global optimization for energy efficient resource management by game based distributed learning in internet of things, KSII Transactions on Internet and Information Systems (TIIS) 9 (10) (2015) 3771–3788.
[73] N. Abuzainab, W. Saad, H.V. Poor, Cognitive hierarchy theory for heterogeneous uplink multiple access in the internet of things, in: Information Theory (ISIT), 2016 IEEE International Symposium on, IEEE, 2016, pp. 1252–1256.
[74] H. Al-Kashoash, M. Hafeez, A. Kemp, Congestion control for 6lowpan networks: A game theoretic framework, IEEE Internet of Things Journal.
[75] F. Lin, Q. Liu, X. Zhou, Y. Chen, D. Huang, Cooperative differential game for model energy-bandwidth efficiency tradeoff in the internet of things, China Commun. 11 (1) (2014) 92–102.
[76] Y. Liu, Z. Chen, X. Lv, F. Han, Multiple layer design for mass data transmission against channel congestion in iot, Int. J. Commun. Syst. 27 (8) (2014) 1126–1146.
[77] N. Kumar, N. Chilamkurti, S.C. Misra, Bayesian coalition game for the internet of things: An ambient intelligence-based evaluation, IEEE Commun. Mag. 53 (1) (2015) 48–55.
[78] Y. Park, S. Kim, Game-based data offloading scheme for iot system traffic congestion problems, EURASIP Journal on Wireless Communications and Networking 2015 (1) (2015) 192.
[79] M. Elhattab, M.M. Elmesalawy, I.I. Ibrahim, A game theoretic framework for device association in heterogeneous cellular networks with h2h/IoT co-existence, IEEE Commun. Lett. 21 (2) (2017) 362–365.
[80] X. Zhao, Y. Zhang, C. Jiang, J. Yuan, J. Cao, Mobile-aware topology control potential game: Equilibrium and connectivity, IEEE Internet of Things Journal 3 (6) (2016) 1267–1273.
[81] C. Ma, J.-P. Sheu, C.-X. Hsu, A game theory based congestion control protocol for wireless personal area networks, J. Sensors (2016).
[82] D. Lin, Q. Wang, A game theory based energy efficient clustering routing protocol for wsns, Wirel. Netw. 23 (4) (2017) 1101–1111.
[83] H. Elsemary, Mitigating malware attacks via secure routing in intelligent device-to-device communications, in: International Conference on Advanced Intelligent Systems and Informatics, Springer, 2016, pp. 205–214.
[84] Q.D. La, T.Q. Quek, J. Lee, S. Jin, H. Zhu, Deceptive attack and defense game in honeypot-enabled networks for the internet of things, IEEE Internet of Things Journal 3 (6) (2016) 1025–1035.
[85] P.-Y. Chen, S.-M. Cheng, K.-C. Chen, Information fusion to defend intentional attack in internet of things, IEEE Internet of Things Journal 1 (4) (2014) 337–348.
[86] M. Hamdi, H. Abie, Game-based adaptive security in the internet of things for ehealth, in: Communications (ICC), 2014 IEEE International Conference on, IEEE, 2014, pp. 920–925.
[87] N. Namvar, W. Saad, N. Bahadori, B. Kelley, Jamming in the internet of things: A game-theoretic perspective, in: Global Communications Conference (GLOBECOM), 2016 IEEE, IEEE, 2016, pp. 1–6.
[88] H. Sedjelmaci, S.M. Senouci, M. Al-Bahri, A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology, in: Communications (ICC), 2016 IEEE International Conference on, IEEE, 2016, pp. 1–6.
[89] E.E. Tsiropoulou, J.S. Baras, S. Papavassiliou, G. Qu, On the mitigation of interference imposed by intruders in passive rfid networks, in: International Conference on Decision and Game Theory for Security, Springer, 2016, pp. 62–80.
[90] N. Kumar, S. Misra, J.J. Rodrigues, M.S. Obaidat, Coalition games for spatio-temporal big data in internet of vehicles environment: A comparative analysis, IEEE Internet of Things Journal 2 (4) (2015) 310–320.
[91] N. Kumar, R.S. Bali, R. Iqbal, N. Chilamkurti, S. Rho, Optimized clustering for data dissemination using stochastic coalition game in vehicular cyber-physical systems, J. Supercomput. 71 (9) (2015) 3258–3287.
[92] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, P. Bouvry, Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric internet-of-things (iot) applications, in: Globecom Workshops (GC Wkshps), 2016 IEEE, IEEE, 2016, pp. 1–6.
[93] C.-Y. Wan, S.B. Eisenman, A.T. Campbell, Energy-efficient congestion detection and avoidance in sensor networks, ACM Transactions on Sensor Networks (TOSN) 7 (4) (2011) 32.
[94] N. Tsiftes, J. Eriksson, A. Dunkels, Low-power wireless ipv6 routing with contikirpl, in: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, ACM, 2010, pp. 406–407.
[95] J. Jin, M. Palaniswami, B. Krishnamachari, Rate control for heterogeneous wireless sensor networks: Characterization, algorithms and performance, Comput. Netw. 56 (17) (2012) 3783–3794.
[96] S. Bohacek, J. Hespanha, J. Lee, C. Lim, K. Obraczka, Game theoretic stochastic routing for fault tolerance and security in computer networks, IEEE Transactions on Parallel and Distributed Systems 18 (9).
[97] E. Panaousis, T. Alpcan, H. Fereidooni, M. Conti, Secure message delivery games for device-to-device communications, in: International Conference on Decision and Game Theory for Security, Springer, 2014, pp. 195–215.
[98] H. Elsemary, D. Hogrefe, Malware-defense secure routing in intelligent device-to-device communications, in: The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), November 28–30, 2015, Beni Suef, Egypt, Springer, 2016, pp. 485–495.
[99] J. Bonneau, E.W. Felten, S. Goldfeder, J.A. Kroll, A. Narayanan, Why buy when you can rent? Bribery attacks on bitcoin consensus.
[100] I. Eyal, E.G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, in: International COnference on Financial Cryptography and Data Security, Springer, 2014, pp. 436–454.
[101] M. Rosenfeld, Analysis of bitcoin pooled mining reward systems, arXiv preprint arXiv:1112.4980.
[102] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, T. Moore, Game theoretic analysis of ddos attacks against bitcoin mining pools, in: International Conference on Financial Cryptography and Data Security, Springer, 2014, pp. 72–86.
[103] A. Laszka, B. Johnson, J. Grossklags, When bitcoin mining pools run dry, in: International Conference on Financial Cryptography and Data Security, Springer, 2015, pp. 63–77.
[104] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, A. Hobor, On power splitting games in distributed computation: The case of bitcoin pooled mining, in: Computer Security Foundations Symposium (CSF), 2015 IEEE 28th, IEEE, 2015, pp. 397–411.
[105] I. Eyal, The miner's dilemma, in: Security and Privacy (SP), 2015 IEEE Symposium on, IEEE, 2015, pp. 89–103.
[106] S. Kim, Group bargaining based bitcoin mining scheme using incentive payment process, Transactions on Emerging Telecommunications Technologies 27 (11) (2016) 1486–1495.
[107] R. Gupta, V. Sekhri, A.K. Somani, Compup2p: An architecture for internet computing using peer-to-peer networks, IEEE Trans. Parallel Distrib. Syst. 17 (11) (2006) 1306–1320.
[108] M. Yurkewych, B.N. Levine, A.L. Rosenberg, On the cost-ineffectiveness of redundancy in commercial p2p computing, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, 2005, pp. 280–288.
[109] H. Hu, Z. Li, H. Hu, An anti-cheating bidding approach for resource allocation in cloud computing environments, Journal of Computational Information Systems 8 (4) (2012) 1641–1654.
[110] P. Khethavath, J. Thomas, E. Chan-Tin, H. Liu, Introducing a distributed cloud architecture with efficient resource discovery and optimal resource allocation, in: Services (SERVICES), 203 IEEE Ninth World Congress on, IEEE, 2013, pp. 386–392.
[111] R. Telang, U. Rajan, T. Mukhopadhyay, The market structure for internet search engines, J. Manage. Inf. Syst. 21 (2) (2004) 137–160.
[112] B. Edelman, M. Ostrovsky, M. Schwarz, Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords, Am. Econ. Rev. 97 (1) (2007) 242–259.

Xueqin Liang received the B.Sc. degree on Applied Mathematics from Anhui University, Anhui, China, 2015. She is currently working for her Ph.D. degree in Cyberspace Security at Xidian University, Xi'an, China. Her research interests are in game theory based security solutions, cloud computing security and trust, and IoT security.

Zheng Yan received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China in 1994 and 1997, respectively, the second M.Eng. degree in information security from the National University of Singapore, Singapore in 2000, and the licentiate of science and the doctor of science in technology in electrical engineering from Helsinki University of Technology, Helsinki, Finland. She is currently a full professor at the Xidian University, Xi'an, China and a visiting professor at the Aalto University, Espoo, Finland. Her research interests are in trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She has authored 170+ peer-reviewed journal and conference papers and invented 60+ patents and patent applications. She solely authored two books about trust management. Prof. Yan serves as an organization and program committee member for 70+ international conferences and workshops. She is also an associate editor of many reputable journals, e.g., Information Sciences, Information Fusion, JNCA, IEEE Access, IEEE IoT Journal, SCN, Soft Computing, etc. She is a senior member of the IEEE.