A Three-party Repeated Game Model for Data Privacy in Mobile Edge Crowdsensing of IoT

Mingfeng Zhao[1][0000−0002−1629−5793], Lei Chen[2][0000−0002−3919−8056], Jinbo Xiong[1][0000−0001−9985−1953], and Youliang Tian[3][0000−0002−5974−1570]

[1] Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University,
Fuzhou 350117, China, zmf1900953654@163.com, jbxiong@fjnu.edu.cn

[2] College of Engineering and Computing, Georgia Southern University,
GA 30458, USA, lchen@georgiasouthern.edu

[3] State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
youliangtian@163.com

Corresponding author: Jinbo Xiong (jbxiong@fjnu.edu.cn)

Abstract. The low request response delay of mobile edge crowdsensing (MECS) paradigm allows quick interactions among entities in practical scenarios. However, there often exist dishonest behaviors in such interactions, and the personal information leakage involved seriously threatens the privacy and security of sensing users. To tackle this problem, previously we had proposed a non-repeated three-party game model, without the consideration of multiple interactions in the actual scenario. Based on game theory, this research therefore proposes a three-party repeated game model. Specifically, we propose the corresponding social norms for different phases of sensing data. It analyzes all possible behaviors deviating from rationality, calculates the change of corresponding payoff function, and explores the influencing factors and constraints of players' honest behaviors based on the premise of maximizing interests. Finally, a significant number of simulations and numerical analyse indicate that the proposed model is feasible and effective in maximizing the benefits of game participants.

Keywords: Privacy protection · Mobile edge crowdsensing · Game Theory · Three-party repeated game model · Nash Equilibrium.

1 Introduction

In recent years, the popularity of wireless mobile and 5G terminal devices is growing explosively [21, 18, 30]. Smart phones, wireless Bluetooth wearable devices and other integrated sensors are becoming more abundant, making them capable of powerful sensing and computing [35, 32]. Based on this background, a paradigm MCS, mobile crowdsensing, has emerged [42, 22]. In MCS, a large number of mobile users who carry the afore mentioned IoT intelligent terminal equipment as the basic sensing unit interact with the sensing platform with the

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2295500

help of wireless sensor network to realize the collaborative work of task distribution and data collection [35, 28], so as to complete the large-scale and complex social sensing tasks under various scenarios [33]. Meanwhile, with the development of 5G base stations, the throughput of real-time data communication and link bandwidth would be greatly improved. Nowadays, we are committed to building a smart city paying more attention to strong interactions with high real-time requirements, such as intelligent transportation systems [12], crowdsourced bus service [6], connected autonomous vehicle service [4, 5, 39], and mobile health system [40, 31]. This promotes the emergence of the MECS paradigm [36], which includes sensing users, edge nodes and cloud service providers. By introducing the concept of mobile edge computing (MEC) [2, 34], it solves the communication bottleneck of traditional cloud computing. In an MEC, a large number of scattered edge nodes with different application services use their edge attributes closer to the client, combined with certain computing and storage capacity, to carry part of the functions of the remote cloud server [17].

On the other hand, the explosive growth of the number of intelligent IoT devices has also brought massive multi-dimensional and heterogeneous source data, and the sensing activities of multi-user collaboration may also expose their social association attributes and other privacy information. Specifically, on the one hand, the sensing user will choose the task published by the edge node, and upload the data collected from the real-time sensing activity to the edge node to obtain the task reward. In this process, there exist risks of user privacy leakage, such as sensing data ownership migration and adversary attacks that may be encountered in the process of data transmission. At the same time, as semi trusted and resource constrained entities, edge nodes may also have potential active disclosure behaviors and node attacks. On the other hand, in the process of the transaction between the edge node and the service provider, the data ownership has been migrated again, and the cloud service provider, as an untrusted platform, may actively disclose the user's private data to adversaries exchange benefits. Therefore, it is urgent to solve the problem of user data privacy leakage in MECS network. The center of big data privacy protection is privacy protection technology.

The current work can be divided into: data distortion (focusing on differential privacy technology), data encryption (such as homomorphic encryption, secure multi-party computing, functional encryption, etc.) and restricted publishing (focusing on data anonymity). As another hot field in the background of big data, artificial intelligence can effectively drive the level of privacy protection, while reducing the risk of privacy leakage in the application process with the help of privacy protection technology. [38] is a good example as it integrates the concept of game theory. However, it lacks the consideration of possible multiple interactions between entities in the actual scene over a period of time. In game theory, there are important differences in the nature of players in dealing with short-term and long-term relationships. A tacit or cooperative relationship that is difficult to form in the short term can constrain each other's behaviors through long-term potential retaliation, sanctions and other threatening behaviors, as shown in the work of [24], [26]. However, most of the existing work focuses on the long-term behavior relationship between the two entities. Therefore, in order to deal with data privacy of users in MECS network, this paper aims to build a repeated game model for three-party entities, in order to find the influencing factors and constraints that regulate the benign behaviors of multi-party entities in MECS. The main contributions of this paper are summarized as follows:

- Build a repeated game model based on three-party entities, and analyze the deviation behavior and payoff change among players in multiple phases of the sensing data life cycle.
- On the premise of maximizing benefits, identify the influencing factors and constraints of honest behaviors of players in different phases of MECS.
- Through a large number of simulation experiments and numerical analyse, the proposed three-party repeated game model is proofed feasible and effective, suitable for MECS paradigm.

The rest of this paper is organized as follows. Section 2 introduces the related works. Section 3 gives the preliminaries. Section 4 describe the proposed repeated game model in detail. Section 5 discusses the experimental results and theoretical analysis of the proposed model. Section 6 gives a summary of the research.

2 Related Works

As mentioned above, in the mobile edge group intelligence perception network, user privacy threats caused by perceived data leakage have attracted many scholars to conduct relevant research.

On one hand, the work mainly focuses on the application of cryptography and block chain technology. The method based on cryptography, the scheme design and construction of data encryption, anonymity, disturbance, aggregation and other aspects can be carried out. Blockchain technology provides verification support and portable management for data security sharing, high reliability, tamper resistance and so on [23],[19],[29]. In the intelligent perception paradigm of mobile edge group based on the background of Internet of things, mobile edge computing is one of the core technologies supporting the architecture, which meets the needs of low latency and fast corresponding service requests of Internet of things applications. Li et al. [16] proposed a privacy data aggregation scheme for mobile edge computing to assist Internet of things applications, which not only guarantees the data privacy of terminal equipment, but also provides source authentication and integrity check, saving half of the communication cost compared to the traditional schemes. Considering the problem of data privacy protection in the process of collecting personal information, a protection algorithm based on differential privacy model is proposed in [15], and a time window partition and a dynamic network community discovery algorithm is designed to reduce the differential privacy noise. With the help of layered sampling, the time cost and cumulative errors are reduced. Experiments show that the algorithm can keep the important structural features of the original network graph on the premise of satisfying the differential privacy protection model. In addition, users mainly collect sensor data through intelligent Internet of things devices equipped with sensors. In view of this, many methods to protect the privacy of intelligent terminal devices have been proposed. Blasco et al. [3] put forward a three-layer method to protect the privacy of citizens in order to solve the problem that personal privacy is easy to be mined and attacked due to the need of smart city services to access sensitive data of users [13, 14]. By combining the first layer and the second layer of homomorphic public key encryption, local data collection is safe, and the third layer adds differential privacy to control the spread of public information.

When users enjoy personalized services provided by various context aware applications, their sensitive information hidden in the context is exposed. Zhang et al. [41] designed a privacy protection deception strategy based on the passive defense strategy for most of the current mechanisms. They proposed a new technology: FakeMask, essentially a privacy check algorithm that can adaptively release a fake context according to the current context of the user, greatly limiting the adversary to infer the actual context. Experimental evaluation and scheme comparison in real smartphone environment show that FakeMask has outstanding performance.

On the other hand,from the perspective of game theory, through modeling and analyzing the behavior game between players, we can solve the prisoner's dilemma and other problems. In MECS network, many application scenarios involve different entities with multiple target conflicts. The process of conflicts is actually the choice and game of the best strategy, and the ultimate goal is to maximize their own interests. At present, game theory has been successfully applied in many representative communication and network scenarios, such as defenses against DoS attack in wireless network [1], data privacy protection in social networks [20] and privacy protection model in transportation systems of IoT [27]. In [25], Moura et al. investigated and studied the main challenges of mobile edge computing services to wireless resources based on game theory. They discussed the specific game strategies, model evaluation and balance constraints in the edge network scenarios by classical game and evolutionary game, and emphasized the application trend and research direction of game theory model in mobile edge computing services in the future. Jin et al. [8] considered two groups of service providers with different request strategies to obtain the reward matrix. This work aims at the problem of excessive permission request in the current smart phone terminal, thus established two groups of evolutionary game model for user privacy protection, and analyzed the stability strategy of the model. Kim [9] proposed an MCS control scheme based on multi-level game model and differential privacy concept in view of the serious loss of personal privacy in mobile group intelligence perception. From the perspective of an MCS server differential privacy(DP) controller and mobile devices, the dynamics of their interactions are captured and analyzed, and the game process is repeated step by step to explore effective solutions for promoting interaction among players. At present, many real-world application scenarios can be simulated as prisoners' dilemma, and the relevant research literature also provides a variety of strategies; however, it rarely conforms to the design objectives of the intelligent agent: reactivity and initiative. In [11], the risk attitude and reputation factors are combined into infinite repeated games, and the original game theory matrix is transformed into a new matrix with cooperative equilibrium. By analyzing the repeated prisoner's dilemma and the results of simulation experiments, it is verified that the performance of agents considering the above two factors in the decision-making process,in both active and passive manner is improved. Xiong et al. [38] propose an AI (Artificial Intelligence)-enabled three-party game framework by combining machine learning and game theory, discuss the privacy leakage problem of entity interaction in typical application scenarios of MECS, and provide an effective and efficient scheme for ensuring data privacy in the MECS of IoT.

In MECS, there are entities such as users, edge nodes, cloud service providers, attackers and so on. From the above literature, mobile edge computing, as an important component technology of MECS, has many scenarios based on game theory. [9] provides an example of a scheme combining game theory and cryptography to solve the problem of privacy protection in MCS paradigm. The repeated prisoner's dilemma game under multiple factors is considered in [11]. [38] combined the AI algorithm on the basis of game theory and cryptography, provided an effective solution to the problem of privacy leakage risk in MECS paradigm, without considering the impact of repeated interaction between entities over a period of time. In the practical application scenario of MECS, entities often interact multiple times over a period of time, and therefor it is necessary to consider the subjective and objective factors in the interaction process of multiple entities. In addition, most of the above works are repeated games between two parties, without the extension to multiple parties, which stimulates the development of our work in this paper.

3 Preliminaries

In this section, we formally define our system model, threat models and assumptions. We then introduce the problem description and design goals.

3.1 System Model

As shown in Fig.1, in MECS paradigm, there exist entities such as sensing users (SUs), edge nodes (ENs) and cloud service providers (CSPs), which are described as follows.

(1) Sensing users (SUs): a large number of ordinary people who apply smart phones, tablets, wearable devices and other mobile devices as basic perceptual units. After selecting the sensing task independently, they utilize various sensors integrated on the device to carry out sensing activities, and upload the data to ENs with the help of wireless network.

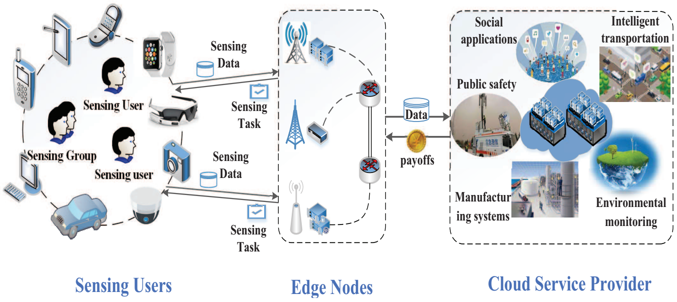

Fig. 1: System model of MECS

(2) Edge nodes (ENs): With the help of mobile Internet, sensing tasks are distributed to SUs and sensing data are collected and processed by ENs. A large number of nodes with different functions and dispersions cooperate to complete large-scale and complex social sensing tasks, and employ the processed data to trade with CSPs.

(3) Cloud service providers (CSPs): provide real-time services to SUs to meet their personalized needs by using sensing data or service models obtained from transactions with ENs.

In our system model, the life cycle of sensing data in an MECS network is divided into sensing data uploading phase and sensing data trading phase. In practical application scenarios, there may exist adversaries who attempt to obtain the user private data in each phase.

3.2 Infinitely Repeated Game

An infinite number of repeated games is a game process in which players repeat the same structure for many times and there is no fixed time to end the game. The behavior process of repeated implementation is called stage game. The specific definition is as follows:

Definition 1: An infinite number of repeated games can be expressed as a tuple $< N, S_i, P_i, H, \delta, T >$, where,

- N: a finite set of n players
- S_i: action strategy sets of n players, where $i \in N$, and action profile could be denoted as $S = \times_{i \in N} S_i$
- P_i: the payoff function of $i \in N$ at every stage
- H: $S \to R^n$, the set of players' payoffs at the end of each stage game
- δ: the discount factor of players to evaluate the payoffs, $0 \leq \delta \leq 1$
- T: the number of the stages

Definition 2: The stage game G is a strategic game. Combined with its repetition times T, we can determine a ”T-repeated game” process, and denoted as $G(T)$.

$$G = \{S_i, \pi_i; i = 1, ..., n\}. \tag{1}$$

In (1), G is the original game of $G(T)$, and each repetition in $G(T)$ is called a stage of $G(T)$. It can be seen from the above that S_i is the strategy set of player i; π_i is his/her payoff at each stage, and it depends on $(S_1, S_2, ..., S_n)$.

According to the system model architecture shown in Fig.1, it is obvious that there is a chronological order for the players' strategy selection. We assume that player 1 has the priority to choose strategies, and there is no limit on player 2's strategy choice. This is also true between player 2 and player 3. In view of this situation, the expansion form of the game is commonly used to analyze [10]. The possible behaviors of the players are represented in the form of the behavioral game tree, and the payment of each stage of the game process is given at the leaf node of each branch, as shown in Fig.2. Here, $t \in T$, obviously, when $t = T = 1$, it means that each player has played a single game.

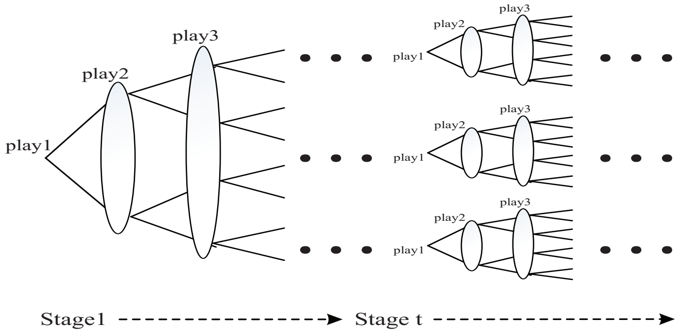

Fig. 2: Extended behavioral game tree

3.3 Single-stage Game

Here, we will describe the behavior of the initial stage game based on the work of [38]. For the sensing data uploading phase and the sensing data trading phase, there are two different player sets N' and N'': SUs, adversary $\mathcal{A}_1$, ENs, and ENs, CSPs and adversary $\mathcal{A}_2$. The player's strategy set of two phases $S_i(i \in (N', N'')$ correspond to $(M,\ M')$ in [38]. Based on the structure of payoff function of players in different phases, we respectively obtain the player's payoff set $(h,\ h')$ at the end of the first stage game from [38]. It is worth noting that we all abide by two hypothesis: ① SUs will not carry out sensing activities at any cost, and the adversary will not blindly launch unprofitable attacks; ② the accuracy of data largely determines the privacy of user information, so the payoff function of each player will be constructed based on this. Thus, It is easy to know that the adversary $\mathcal{A}_1$ will not launch an attack when SUs do not upload their sensing data, so play2 in Fig.2 has only three behavior branches, and affected play3 has six behavior choices.

4 Repeated-stages Game Model

In a single-stage game, each participant only pays attention to the current payoff. However, the interactions between these participants are long-term and repetitive in practice. Under these circumstances, participants will consider the impact of current behavioral strategies on future payoffs. Therefore, based on the situation of single-stage strategy game [38], we model their multiple interaction processes as a repeated game model.

4.1 Sensing Data Uploading Phase

When $\mu_5 < \mu_3$, the optimal strategy profile $\ell = 1$, $\sigma = 0$, $\tau = 0$ is the only pure strategy Nash Equilibrium solution. If there is only one pure strategy NE solution in the original game, each participant would adopt the NE strategy profile of the original game in the next stage [7]. Therefore, the result of repeated game in this case is that SU uploads sensing data, $\mathcal{A}_1$ does not launch an attack and EN does not leak privacy, so the user's private information is well protected.

When $\mu_5 > \mu_3$, the optimal strategy profile $\ell = 1$, $\sigma = \frac{G(d)}{\mu_2 Sens(d)} - \frac{\mu_1}{\mu_2}$, $\tau = 1$ is the mixed strategy NE solution. We introduce a discount factor δ [37] due to the payoff of infinitely repeated games being endless. We can use the same discount factor δ to discount the future payoff of each stage, so that the total payoff can be limited and comparable.

Given $\delta = e^{-r\Delta}$, where r is the preference rate for time and Δ is the length of a period. For one path of infinitely repeated games, we assume that the payoff of participants at each stage are $\pi_1, \pi_2, \pi_3 ...$, respectively. Also, we use $\delta_{SU}, \delta_{\mathcal{A}_1}, \delta_{EN}$ to denote the discount factor of SU, $\mathcal{A}_1$, EN, respectively. Therefore, the total payoff of participants is shown in Formula (2).

$$\pi = \pi_1 + \delta\pi_2 + \delta^2\pi_3 + \cdots = \sum_{i=1}^{\infty} \delta^{i-1}\pi_i. \tag{2}$$

For the case of $\mu_5 > \mu_3$, we propose social norms that are in line with the actual situation. Usually, an SU always uploads sensing data, and refuses to upload until n_1 times leakage behaviors are discovered. For $\mathcal{A}_1$, the initial strategy is not to attack. It would switch to attack strategy and sustain n_3 times until the SU uploads data n_2 times continuously. Additionally, if the SU does not upload data, $\mathcal{A}_1$ would not launch an attack. EN chooses not to leak at the moment. Once EN finds that $\mathcal{A}_1$ launch n_3 consecutive attacks, it would switch to leak strategy. Because the SU could not determine who committed the dishonest act at this time, and EN refuses to admit. Also, when $\mathcal{A}_1$ does not launch an attack for n_4 consecutive times, EN switches to the behavior of not leaking. The more the participants deviated from the social norms, the more their later payoffs decreased. In order to facilitate the analysis of problems without losing generality, we assume that $n_1 = 1, n_2 = 1, n_3 = 2, n_4 = 2$.

If all participants abide by the initial behavior of the above social norms, the strategic path in infinitely repeated games would be $(\ell = 1, \sigma = 0, \tau = 0) \rightarrow$

$(\ell = 1, \sigma = 0, \tau = 0) \to (\ell = 1, \sigma = 0, \tau = 0) \to \cdots$ (ℓ, σ, τ are omitted in the following text). Therefore, we can calculate the total payoffs of SU, $\mathcal{A}_1$ and EN as follows:

$$\begin{cases} u_{SU^*}(d) = G(d)(1 + \delta_{SU} + \delta_{SU}^2 + \delta_{SU}^3 + \cdots) = \frac{G(d)}{1-\delta_{SU}} \\ u_{EN^*}(d) = G(d)(1 + \delta_{EN} + \delta_{EN}^2 + \delta_{EN}^3 + \cdots) = \frac{G(d)}{1-\delta_{EN}} \\ u_{\mathcal{A}_1^*}(d) = 0(1 + \delta_{\mathcal{A}_1} + \delta_{\mathcal{A}_1}^2 + \delta_{\mathcal{A}_1}^3 + \cdots) = 0 \end{cases} \tag{3}$$

① Considering the deviation of $\mathcal{A}_1$'s behavior

Assume that starting from the first round of the game, the new strategy path of the game would be described as follows:

$$\begin{aligned} &(1,1,0) \to (1,1,0) \to (1,1,1) \to (0,0,1) \to (0,0,1) \\ &\to (0,0,0) \to (0,0,0) \cdots \end{aligned}$$

Now, the total payoffs $u_{\mathcal{A}_{1_d}}(d)$ after $\mathcal{A}_1$'s behavior deviates would be:

$$u_{\mathcal{A}_{1_d}}(d) = (\mu_6 Sens(d) - R)(1+\delta_{\mathcal{A}_1}+\delta_{\mathcal{A}_1}^2). \tag{4}$$

② Considering the deviation of EN's behavior

Similarly, starting from the first round of the game, the new strategy path of the game would be described as follows:

$$(1,0,1) \to (0,0,1) \to (0,0,1) \to (0,0,0) \to (0,0,0) \cdots$$

Now, the total payoffs $u_{EN_d}(d)$ after EN's behavior deviates would be:

$$u_{EN_d}(d) = G(d) + (\mu_5 - \mu_3)Sens(d). \tag{5}$$

③ Considering the simultaneous deviation of $\mathcal{A}_1$ and EN's behaviors

The behavior of both deviates simultaneously in the first round, and the strategy profile is (1, 1, 1); the new game strategy path would be described as follows:

$$(1,1,1) \to (0,0,1) \to (0,0,1) \to (0,0,0) \to (0,0,0) \cdots$$

Now, the total payoffs of $\mathcal{A}_1$ and EN would be described as follows respectively:

$$\begin{cases} u_{\mathcal{A}_1'{}_d}(d) = \mu_6 Sens(d) - R \\ u_{EN'_d}(d) = G(d) + (\mu_5 - \mu_3)Sens(d) \end{cases} \tag{6}$$

In order to restrain the game participants from choosing deviation behaviors, their payoff function should satisfy the following inequalities:

$$\begin{cases} u_{\mathcal{A}_{1_d}}(d) < u_{\mathcal{A}_1^*}(d) \\ u_{EN_d}(d) < u_{EN^*}(d) \\ u_{\mathcal{A}_1'{}_d}(d) < u_{\mathcal{A}_1^*}(d) \\ u_{EN'_d}(d) < u_{EN^*}(d) \end{cases} \tag{7}$$

We can have the following inequalities:

$$\begin{cases} \mu_6 < \frac{R}{Sens(d)} \\ \delta_{EN} > \frac{(\mu_5-\mu_3)Sens(d)}{G(d)+(\mu_5-\mu_3)Sens(d)} \end{cases} \tag{8}$$

Obviously, When the discount factor δ_{EN} of EN and μ_6 satisfy the relevant range, the game participants will not choose to deviate from the social norms, so as to protect the sensing user's personal private information.

4.2 Sensing Data Trading Phase

The analysis method of this phase is similar to that of the uploading phase. We use δ_{CSP} and $\delta_{\mathcal{A}_2}$ to denote the discount factor of CSP and $\mathcal{A}_2$ respectively. For the case of $k_3 > k_2$, we also propose social norms that are in line with the actual situation. Usually, an EN always chooses to trade data, and refuses to trade until m_1 disclosures are found. A CSP would firstly chooses not to leak any data, and switches to leakage behavior once finds out that $\mathcal{A}_2$ has launched m_2 times of attacks. Additionally, if EN chooses not to trade, the CSP would not leak any data. Furthermore, $\mathcal{A}_2$'s initial strategy is not to attack. And they would launch m_3 times of attacks continuously once found that CSP have leaked data. Meanwhile, when $\mathcal{A}_2$ finds that the CSP no longer leak data m_4 times, if will choose not to attack for maximized payoffs. In order to support a complete strategy transformation process, we assume that $m_1 = 1, m_2 = 1, m_3 = 1, m_4 = 2$.

Similarly, we can have that when $k_4 < \frac{3C}{Sens(d)}$, the range of discount factor is:

$$\delta_{CSP} > \frac{(k_3 - k_2)Sens(d)}{G(d) + (k_3 - k_2)Sens(d)} \tag{9}$$

Whereas, in the case of $k_4 > \frac{3C}{Sens(d)}$, the range of discount factors are:

$$\begin{cases} \delta_{ASP} > \frac{(k_3-k_2)Sens(d)}{G(d)+(k_3-k_2)Sens(d)} \\ \delta_{\mathcal{A}_2} < \frac{k_4Sens(d)-C-\sqrt{k_4^2Sens(d)^2-2k_4Sens(d)C-3C^2}}{2C} \end{cases} \tag{10}$$

As the range of k_4 changes, when the discount factors range of relevant game participants are satisfied, they would not have any reason to deviate from social norms. In this way, it prevents the private information of users from being leaked.

5 Model Analysis and Validation

In this section, we conduct numerical analysis on the proposed three-party repeated game model, including sensing data uploading phase and sensing data trading phase. The experiments were carried out on a desktop computer running Window 7 system, which was configured with Intel core i5-5200U, 2.20 GHz CPU and 8 GB RAM, and the software used is MATLAB R2016a.

5.1 Sensing Data Uploading Phase

In this section, the parameter settings are the same as above. In the sensing data uploading phase, Fig.3(a) illustrates that when δ_{EN} exceeds a certain value, EN would change from the leaking strategy to the non-leaking strategy, and this value depends on $\mu_5 - \mu_3$. With the increase of $\mu_5 - \mu_3$, the critical value also increases, which is consistent with formula (8). μ_5 is the positive influence coefficient reflecting the payoff obtained by EN's leakage behavior, and μ_3 is the reputation punishment coefficient of EN's leakage behavior. μ_5 is a constant value for the sensing data of certain accuracy. By increasing μ_3, that is, increasing the punishment for EN on users' side, the critical value goes down, which makes the

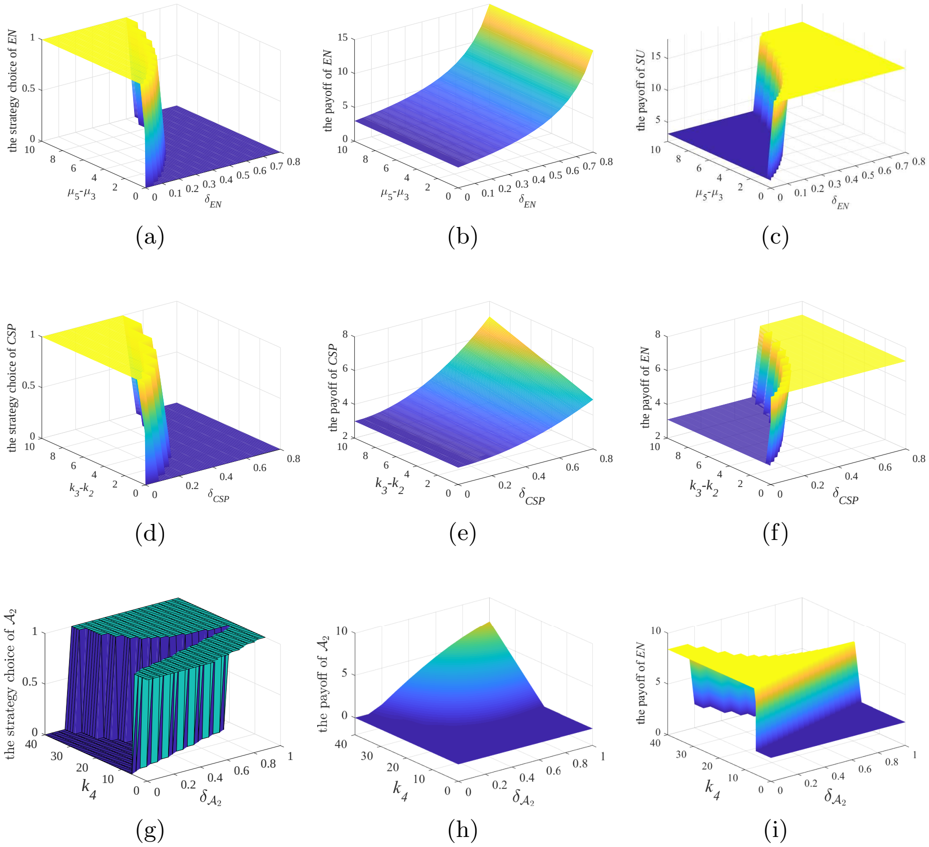

Fig. 3: Performance evaluation results:(a) shows the influence of $\mu_5 - \mu_3$ and δ_{EN} on strategy selection of EN; (b) and (c) show the influence of $\mu_5 - \mu_3$ and δ_{EN} on payoffs of EN and SU; (d) shows the influence of $k_3 - k_2$ and δ_{CSP} on strategy selection of CSP; (e) and (f) show the influence of $k_3 - k_2$ and δ_{CSP} on payoffs of CSP and EN; (g) shows the influence of k_4 and $\delta_{\mathcal{A}_2}$ on strategy selection of $\mathcal{A}_2$; (h) and (i) show the influence of k_4 and $\delta_{\mathcal{A}_2}$ on payoffs of $\mathcal{A}_2$ and EN.

constraint conditions in equation (8) easier to be reached, forcing EN to choose the non-leaking strategy. Fig.3(b) and Fig.3(c) show that the payoff of EN and SU increases with the increase of δ_{EN}. At the critical value, the payoff of SU will increase greatly with the change of strategy choice of EN. It is verified that EN would be more inclined to comply with social norms within the range of constraint conditions.

5.2 Sensing Data Trading Phase

In the sensing data trading phase, Fig.3(d) shows that CSP will be more prone to non-leakage behavior with the increase of δ_{CSP}, and its critical value depends on $k_3 - k_2$. k_2 is the punishment coefficient for CSP's leakage behavior, and k_3 is the positive influence coefficient reflecting the payoff of CSP obtained through the leakage behavior. Similarly, we can adjust k_2 on the side of EN to reduce the critical value according to formula (9), forcing CSP to comply with social norms and choose not to leak. As can be seen from Fig.3(e) and Fig.5(f), the payoff of CSP and EN are increasing with the rise of δ_{CSP}. In detail, Fig.3(e) shows in the case that the value of $k_3 - k_2$ increases, the payoff of CSP increases with the rise of δ_{CSP}, which indicates that the smaller k_2 is, the lighter the punishment on CSP is, and CSP is more likely to choose the leakage strategy. It is verified that k_2 is the critical factor influencing CSP's choice of leakage and non-leakage strategy. Additionally, when δ_{CSP} is at the critical value, the payoff remains the same regardless of whether CSP chooses the leakage behavior or not. When δ_{CSP} exceeds the critical value, CSP would gain more from choosing non-leakage behavior over leakage behavior, which verifies CSP's corresponding constraint conditions on compliance with social norms in formula (10). Fig.3(f) shows that EN's payoff has a significant change at the critical value, which also reveals the key influence of CSP's leakage and non-leakage behavior on EN's payoff.

When $k_4 > \frac{3C}{Sens(d)}$, formula (10) indicates that a smaller discount factor $\delta_{\mathcal{A}_2}$ is required to satisfy the constraint. Fig.3(g) manifests that $\mathcal{A}_2$'s strategy is more inclined to leak with the increase of k_4, forcing us to choose smaller $\delta_{\mathcal{A}_2}$. Additionally, Fig.3(h) shows that when k_4 is at a small value and $\delta_{\mathcal{A}_2}$ does not meet the constraint conditions, the payoff from $\mathcal{A}_2$'s choice of leakage is much less than the choice of non-leakage. Therefore, on the premise of meeting the constraint conditions, the adversary $\mathcal{A}_2$ after repeated games would not deviate from the social norms. In this case, EN's payoff would also increase significantly in this range, which is consistent with the results in Fig.3(i).

6 Conclusion

In view of the user data privacy problem of two-party interactions discussed in most of the existing work, based on game theory, we constructed a three-party repeated game model for sensing data uploading phase and the sensing data trading phase in MECS. By considering the possible interaction strategies among participants in different phases, analyzing their potential deviation strategies, and calculating the change of payoff, this paper further explores the influencing factors and constraints that regulate participants' honest behaviors in the game. Finally, through simulation experiments and numerical analysis, our proposed model shown feasible and has a certain guiding significance for user data privacy protection in MECS applications.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (61872088, 61872090, U1905211, 61772008); the Natural Science Foundation of Fujian Proince (2019J01276); the Science and Technology Major Support Program of Guizhou Province (20183001); and the Guizhou Provincial Key Laboratory of Public Big Data Research Fund (2019BDKFJJ004).

References

1. Agah, A., Das, S.K.: Preventing dos attacks in wireless sensor networks: a repeated game theory approach. IJ Network Security **5**(2), 145–153 (2007)
2. Bi, S., Zhang, Y.J.: Computation rate maximization for wireless powered mobile-edge computing with binary computation offloading. IEEE Transactions on Wireless Communications **17**(6), 4177–4190 (2018)
3. Blasco, S., Javier, B.J., Font, G., et al.: A three-layer approach for protecting smart-citizens privacy in crowdsensing projects. In: 2015 34th International Conference of the Chilean Computer Science Society (SCCC). pp. 1–5. IEEE (2015)
4. Chen, Q., Ma, X., Tang, S., et al.: F-cooper: feature based cooperative perception for autonomous vehicle edge computing system using 3d point clouds. In: Proceedings of the 4th ACM/IEEE Symposium on Edge Computing. pp. 88–100 (2019)
5. Chen, Q., Tang, S., Yang, Q., et al.: Cooper: Cooperative perception for connected autonomous vehicles based on 3d point clouds. In: Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). pp. 514–524 (2019)
6. He, Y., Ni, J., Niu, B., et al.: Privbus: A privacy-enhanced crowdsourced bus service via fog computing. Journal of Parallel and Distributed Computing **135**, 156–168 (Jan 2020). https://doi.org/10.1016/j.jpdc.2019.09.007
7. Ichiishi, T.: Game theory for economic analysis. Elsevier (2014)
8. Jin, J., Ye, A., Yang, Z., et al.: Evolutionary game analysis on permission request policy of service providers. In: 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB). pp. 1–6. IEEE (2018)
9. Kim, S.: A new differential privacy crowdsensing scheme based on the multilevel interactive game. Wireless Communications and Mobile Computing **2018** (2018)
10. Koller, D., Megiddo, N., Bernhard, V.S.: Efficient computation of equilibria for extensive two-person games. Games and economic behavior **14**(2), 247–259 (1996)
11. Lam, K.m., Leung, H.f.: Incorporating risk attitude and reputation into infinitely repeated games and an analysis on the iterated prisoner's dilemma. In: 19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2007). vol. 1, pp. 60–67. IEEE (2007)

12. Li, D., Deng, L., Cai, Z., et al.: Intelligent transportation system in macao based on deep self-coding learning. IEEE Transactions on Industrial Informatics **14**(7), 3253–3260 (2018)
13. Li, Q., Ma, J., Li, R., et al.: Large universe decentralized key-policy attribute-based encryption. Security and Communication Networks **8**(3), 501–509 (2015). https://doi.org/10.1002/sec.997
14. Li, Q., Ma, J., Li, R., et al.: Provably secure unbounded multi-authority ciphertext-policy attribute-based encryption. Security and Communication Networks **8**(18), 4098–4109 (2015). https://doi.org/10.1002/sec.1326
15. Li, S., Dong, K., Liu, Z., et al.: Dynamic network data protection algorithm using differential privacy in internet of things. In: 2019 IEEE International Conference on Smart Internet of Things (SmartIoT). pp. 306–313. IEEE (2019)
16. Li, X., Liu, S., Wu, F., et al.: Privacy preserving data aggregation scheme for mobile edge computing assisted iot applications. IEEE Internet of Things Journal (2018)
17. Lin, L., Liao, X., Jin, H., et al.: Computation offloading toward edge computing. Proceedings of the IEEE **107**(8), 1584–1607 (2019). https://doi.org/10.1109/JPROC.2019.2922285
18. Lin, Y., Zhu, X., Zheng, Z., et al.: The individual identification method of wireless device based on dimensionality reduction and machine learning. The Journal of Supercomputing **75**(6), 3010–3027 (2019). https://doi.org/10.1007/s11227-017-2216-2
19. Liu, C.H., Lin, Q., Wen, S.: Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning. IEEE Transactions on Industrial Informatics (2018)
20. Liu, F., Pan, L., Yao, L.h.: Evolutionary game based analysis for user privacy protection behaviors in social networks. In: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). pp. 274–279. IEEE (2018)
21. Luo, C., Ji, J., Wang, Q., et al.: Channel state information prediction for 5g wireless communications: A deep learning approach. IEEE Transactions on Network Science and Engineering (2018)
22. Ma, R., Xiong, J., Lin, M., et al.: Privacy protection-oriented mobile crowdsensing analysis based on game theory. In: 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, August 1-4, 2017. pp. 990–995. IEEE Computer Society (2017). https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.342
23. Ma, Z., Wang, X., Jain, D.K., et al.: A blockchain-based trusted data management scheme in edge computing. IEEE Transactions on Industrial Informatics (2019)
24. Mokhonko, E.: Repeated game with the undergoing changes set of choices of the second player. In: 2017 Tenth International Conference Management of Large-Scale System Development (MLSD). pp. 1–4. IEEE (2017)
25. Moura, J., Hutchison, D.: Game theory for multi-access edge computing: survey, use cases, and future trends. IEEE Communications Surveys & Tutorials **21**(1), 260–288 (2018)
26. Paul, S., Ni, Z.: A strategic analysis of attacker-defender repeated game in smart grid security. In: 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5. IEEE (2019)
27. Sfar, A.R., Challal, Y., Moyal, P., et al.: A game theoretic approach for privacy preserving model in iot-based transportation. IEEE Transactions on Intelligent Transportation Systems (2019)

28. Tewari, A., Gupta, B.: A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices. International Journal of Advanced Intelligence Paradigms **9**(2-3), 111–121 (2017)
29. Tian, Y., Wang, Z., Xiong, J., et al.: A blockchain-based secure key management scheme with trustworthiness in dwsns. IEEE Transactions on Industrial Informatics pp. 1–1 (2020). https://doi.org/10.1109/TII.2020.2965975
30. Wang, H., Hempel, M., Peng, D., et al.: Index-based selective audio encryption for wireless multimedia sensor networks. IEEE Transactions on Multimedia **12**(3), 215–223 (2010)
31. Wang, H., Peng, D., Wang, W., et al.: Resource-aware secure ecg healthcare monitoring through body sensor networks. IEEE Wireless Communications **17**(1), 12–19 (2010)
32. Wang, R., Yang, H., Wang, H., et al.: Social overlapping community-aware neighbor discovery for d2d communications. IEEE Wireless Communications **23**(4), 28–34 (2016)
33. Wu, D., Liu, B., Yang, Q., et al.: Social-aware cooperative caching mechanism in mobile social networks. J. Netw. Comput. Appl. **149** (2020). https://doi.org/10.1016/j.jnca.2019.102457
34. Wu, D., Si, S., Wu, S., et al.: Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. IEEE Internet of Things Journal **5**(4), 2958–2970 (2018). https://doi.org/10.1109/JIOT.2017.2768073
35. Xiong, J., Chen, L., Bhuiyan, A., et al.: A secure data deletion scheme for iot devices through key derivation encryption and data analysis. Future Generation Computer Systems (Early Access) **PP**, 1–13. https://doi.org/10.1016/j.future.2019.10.017
36. Xiong, J., Chen, X., Yang, Q., et al.: A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. IEEE Transactions on Network Science and Engineering (2019)
37. Xiong, J., Ma, R., Chen, L., et al.: A personalized privacy protection framework for mobile crowdsensing in iiot. IEEE Transactions on Industrial Informatics (2019). https://doi.org/10.1109/TII.2019.2948068
38. Xiong, J., Zhao, M., Bhuiyan, M., et al.: An ai-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of iot. IEEE Transactions on Industrial Informatics (2019). https://doi.org/10.1109/TII.2019.2957130
39. Yang, Q., Lim, A., Li, S., et al.: Acar: Adaptive connectivity aware routing for vehicular ad hoc networks in city scenarios. Mobile Networks and Applications **15**(1), 36–60 (2010)
40. Yang, Y., Liu, X., Deng, R.H., et al.: Lightweight sharable and traceable secure mobile health system. IEEE Trans. Dependable Secur. Comput. **17**(1), 78–91 (2020). https://doi.org/10.1109/TDSC.2017.2729556
41. Zhang, L., Cai, Z., Wang, X.: Fakemask: a novel privacy preserving approach for smartphones. IEEE Transactions on Network and Service Management **13**(2), 335–348 (2016)
42. Zhao, C., Yang, S., Yan, P., et al.: Data quality guarantee for credible caching device selection in mobile crowdsensing systems. IEEE Wireless Communications **25**(3), 58–64 (2018)