Game theoretical analysis of strategy changes and influence factors in Crowdsourcing IoT systems

Runbo Su, Arbia Riahi Sfar, Pascal Moyal

Game theoretical analysis of strategy changes and influence factors in Crowdsourcing IoT systems

Runbo Su*, Arbia Riahi Sfar‡ and Pascal Moyal§
*LORIA, CNRS, Université de Lorraine, France
‡Cylab, CISS, Royal Military Academy, Belgium
§IECL, INRIA, Université de Lorraine, France

***Abstract*—Crowdsourcing IoT (Crowd-IoT) can improve IoT applications but still faces challenges due to diverse service quality or IoT nodes' selfishness. For this, numerous studies introduced Game Theory to model Crowd-IoT. However, participants' strategy selection and influence factors are rarely discussed. Moreover, game players are often considered fully rational and homogeneous (holding symmetric action sets. In this context, we propose an Evolutionary Game (EG) involving four Crowd-IoT participants, namely service provider (i.e., worker), service requestor, manager, and platform, to analyze influence factors to strategy changes through both theoretical analysis and numerical results.**

***Index Terms*—Game Theory, Crowdsourcing, IoT (Internet of Things), Strategy selection, Stable Strategy,**

I. Background and motivation

A massive amount of sensitive information is being gathered and processed in Crowd-IoT systems, and since malicious or selfish Crowd-IoT participants may behave in a complex strategic manner, modeling Crowd-IoT participants' strategy selections and inter-influence becomes essential. Just to name a victim, the UCSD (University of California San Diego) team suffered from malicious crowdsourcing workers [1] in 2011. In this regard, Game Theory is viewed as an efficient tool.

In literature, many game-based solutions have been proposed to model the interactions between 'participants' in Crowd-IoT. One model considering trust between service providers and consumers is proposed in [2], where the decision-making is aided by a classification scheme to determine the evaluated participants' types. However, this work mainly focuses on trust evaluation instead of strategy changes. With the purpose of formulating participants' behaviors, Game Theory has been applied thanks to its dynamic nature. Studies adopting prisoner's dilemma (PD) game to analyze participants' behaviors in Crowd-IoT are proposed in [3, 4], but these two works are both based on a symmetric payoff matrix treating the requestor and the worker homogeneously, which does not fully suit reality. In [5], authors designed an incentive model using the repeated game for Crowd-IoT, but the strategy selection and related influence is insufficiently discussed. A very recent work in [6] utilized Stochastic Bayesian Game (SBG) to address the Byzantine Altruistic Rational (BAR) based misbehavior, where workers' behavioral types can be deduced reasonably, and the requestor can perform optimal actions accordingly by considering the long-term gain. However, this defense policy can only be applied from a single participant's vision, and the influence factors of Crowd-IoT participants' strategy selection are not addressed. Authors in [7] designed a model for a recommendation incentive mechanism by introducing EG. On the one hand, they proved that non-cooperative agents could be suppressed. On the other hand, the agents considered in their work are identical regarding strategies, and the discussion of inter-influence by strategy selection is also missing. From the above review, there are still several limitations. First, the majority of existing game theoretical solutions consider players homogeneous, which does not match the Crowd-IoT reality. Second, the inter-influence caused by the participants' strategy selection is insufficiently discussed. Third, participants are mostly regarded as fully rational in classic game theoretical modeling, but real Crowd-IoT systems do not require such an assumption. Lastly, existing models focus on interactions without involving the Crowd-IoT platform and service manager, where the latter two are important components in Crowd-IoT. In this context, the contributions of this work are fourfold: i)We involve the platform and service manager as game participants in an Evolutionary Game fitting the Crowd-IoT system's property to model participants' interactions regarding strategy changes appropriately. ii)We consider crowdsourcing participants heterogeneous to enable a more reasonable analysis of their behaviors, such that they are no longer homogeneous strategy- or action-based. iii)We analyze the unilateral stable strategy per participant and the Evolutionary Stable Strategy of the system. iv)We conduct a simulation to validate the proposed model's performance and evaluate the inter-influences of participants' strategy changes.

The rest of the paper is organized as follows. Section II details the game formulation. Section III analyzes strategies stability for each participant. Then, the system's ESS will be explained in Section IV, and the numerical results are presented in Section V. Lastly, Section VI draws the conclusion.

II. Game Formulation

Fig. 1(a) shows the overview of the considered Crowd-IoT system: **Platform** (PLT) refers to the technological infrastructure facilitating the collaboration and participation of numerous requestors and workers [8]. Most current works assume that the platform is fully trusted in Crowd-IoT, but it is also possible that the platform acts in a negligent manner during the implementation of measures. **Manager** (Mgr), also known as a broker, aims to aid the platform

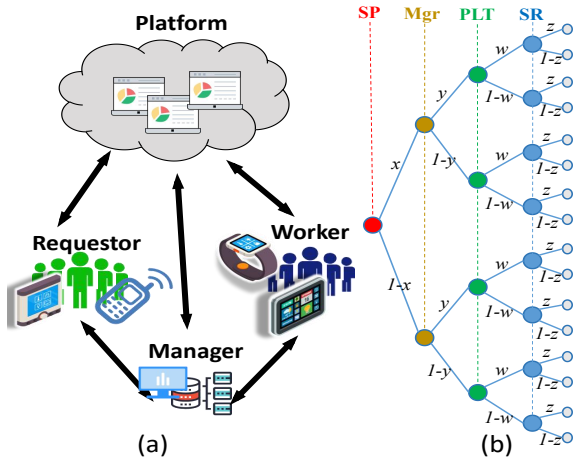

Fig. 1: (a) Considered scenario; (b) Game Tree

TABLE I: Payoff matrix

Strategy		y		$1-y$	
		z	$1-z$	z	$1-z$
w	x	G_{plt} - C_{plt}^H G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} - C_f G_{sr} - C_{sr}^H	G_{plt} - C_{plt}^H G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} - C_f G_{sr}	G_{plt} - C_{plt}^H G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} G_{sr} - C_{sr}^H	G_{plt} - C_{plt}^H G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} G_{sr}
	$1-x$	$-C_{plt}^I$ $-C_{sp}^N$ $-C_{mgr}$ - C_f $-C_{sr}^I$	$-C_{plt}^I$ $-C_{sp}^N$ $-C_{mgr}$ - C_f $-C_{sr}^I$	$-C_{plt}^H + P_{sp} + P_{mgr}$ $-C_{sp}^N - P_{sp}$ $-C_{mgr} - P_{mgr}$ $-C_{sr}^I$	$-C_{plt}^H + P_{sp} + P_{mgr}$ $-C_{sp}^N - P_{sp}$ $-C_{mgr} - P_{mgr}$ $-C_{sr}^I$
$1-w$	x	G_{plt} - C_{plt}^N G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} - C_f G_{sr} - C_{sr}^H	G_{plt} - C_{plt}^N G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} - C_f G_{sr}	G_{plt} - C_{plt}^N G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} G_{sr} - C_{sr}^H	G_{plt} - C_{plt}^N G_{sp} - C_{sp}^H G_{mgr} - C_{mgr} G_{sr}
	$1-x$	$-C_{plt}^I$ $-C_{sp}^N$ $-C_{mgr}$ - C_f $-C_{sr}^I$	$-C_{plt}^I$ $-C_{sp}^N$ $-C_{mgr}$ - C_f $-C_{sr}^I$	$-C_{plt}^N$ $-C_{sp}^N$ - T_{sp} $-C_{mgr}$ - T_{mgr} $-C_{sr}^H$	$-C_{plt}^N$ - T_{plt} G_{sp} - C_{sp}^N - T_{sp} G_{mgr} - C_{mgr} - T_{mgr} $-L_{sr} + R_{sr}$

G =Gain; C=Cost; L=Loss; T=Trust; P=Punishment; H=High-cost; N=Neglectful; I=Insignificant; f=filtering; R=Compensation;

with a specialized interface by offering quality assurance or task results validation [9]. **Requestor** (SR), also known as crowdsourced/publisher, can be an individual or a group of individuals publishing crowdsourcing tasks for solving a relatively complex problem. **Workers** (SP), also known as service providers/solvers, accomplish dedicated tasks by deploying their own knowledge and skills. It can be noticed that crowdsourcing participants may not perform altruistically as expected during the service process due to the nature of greediness. In this context, the Evolutionary Game (EG) is advantageous in modeling Crowd-IoT.

EG was first introduced in 1973 [10], aiming to evolve populations in biology, where animals' competition can be modeled, i.e., nature selection, i.e., nature selection. In an EG, players are interpreted as populations. The probabilities in a mixed strategy of a player are defined as shares of the population, which is proved as equal to the probability of performing different actions when modeling human behaviors [11]. EG considered individuals within the same part of the population to play the same pure strategy, and the main 'solution' concept is the Evolutionary Stable Strategy (ESS). Classic Game Theory is on the basis of the assumption that players are rational, but EG games are not based on such assumption, i.e., players are regarded with bounded rationality, which suits the situation in the real world as IoT users often perform with preference, even with bias. Furthermore, since modeling the Crowd-IoT system remains challenging due to the fact that it consists of numerous nodes and complex networking architecture, by employing the 'population' notion (particularly for SR and SP), the EG enables finding the ESS focusing on the dynamics of strategy changes.

The game tree, consisting of EG players and their strategy selections, is visualized in Fig. 1(b). We consider the crowdsourcing service process as follows: The SR first publishes the task proposal via the PLT, and then the Mgr helps the PLT to recruit qualified SP after analyzing the related requirements for the dedicated service.

From the perspective of SP, we assume x and the cost C_{sp}^H of SR for performing hardworking for the dedicated task, otherwise performing poor service with $(1-x)$ by paying C_{sp}^N.

Mgr can launch a filtering scheme with an additional cost C_f to check the crowdsourced data or ignore this step by paying a relatively lower cost C_{mgr}, where the former and latter strategies are assumed respectively with probabilities y and $(1-y)$. Any non-compliant crowdsourced data detected by Mgr will make SP has no income.

To guarantee the quality of the crowdsourcing service, PLT can also investigate the crowdsourced data by paying C_{plt}^H through a strict supervision process assumed by w, or PLT maintains loose supervision assumed by $(1-w)$ probability with a lower cost C_{plt}^N. If any error or omission is captured by PLT, punishment P_{sp} and P_{mgr} will be applied to SP and Mgr. After that, the crowdsourced data will be released to SR.

SR may trust the crowdsourced data directly and utilize it for its own purposes without any verification by $(1-z)$. Or, assumed by z, SR can also mistrust the data and check the obtained crowdsourced data paying C_{sr}^H.

The bad service causes L_{sr} damage to SR. On the other hand, SR can report the issue, and then SP and Mgr will lose T_{sp} and T_{mgr} trust depending on μ in the range of [0 1] describing the importance of service, and the SR as the victim will receive compensation R_{sr} also depending on μ (i.e., μT_{sp}, μT_{mgr}, and μR_{sr}). Meanwhile, the PLT will lose T_{plt} as trust. Successful crowdsourcing services will provide PLT, Mgr, SP, and SR a gain per each accordingly as reward and incentives, namely G_{plt}, G_{mgr}, G_{sp}, and G_{sr}.

Payoffs are given in Table I. We consider several essential constraints in payoffs: $G.\text{-}C.>C.$, this is because successful crowdsourcing service should be encouraged by giving positive overall payoff. We set $C_.^I$=0 since they are 'insignificant' and to somehow simplify the following calculation. Moreover, we impose $T.>G.$ since the lost trust should never be recovered by the gain in order to punish their selfishness.

III. Unilateral Strategies Stability Analysis

We apply the replication dynamics equation [12] to analyze the strategy stability. For any strategy $\{k, 1-k\}$, denoting by E_k and E_{1-k}, the payoffs of k and $1-k$ respectively, the expected payoff reads $\bar{E} = kE_k + (1-k)E_{1-k}$. Then, the replication dynamic equations, which are formally defined as $F(u) := \frac{\partial u}{\partial t}$, for $u \in \{k, 1-k\}$, are given in this case by $F(k) = k(E_x - \bar{E})$, $F(1-k) = (1-k)(E_{1-k} - \bar{E})$, that is,

$$F(k) = k(1-k)(E_k - E_{1-k}),\ F(1-k) = -F(k). \quad (1)$$

A. Platform

From (1), the PLT's replication dynamic equation is given by: for all $w \in [0,1]$,

$$\begin{aligned} F_{plt}(w) =& w(1-w) \\ &\times \Big\{[x + (1-x)(1-y)](C^N_{plt} - C^H_{plt}) \\ &\quad + (1-x)(1-y)[P_{sp} + P_{mgr} + (1-z)T_{plt}]\Big\} \\ =:& w(1-w)H_{plt}(z). \end{aligned} \quad (2)$$

In particular, we get that for all w,

$$\frac{\mathrm{d}F_{plt}(w)}{\mathrm{d}w} = (1-2w)H_{plt}(z). \quad (3)$$

Now let

$$z_0^1 = 1 - \frac{[x + (1-x)(1-y)](C^H_{plt} - C^N_{plt})}{(1-x)(1-y)T_{plt}} + \frac{P_{sp} + P_{mgr}}{T_{plt}}$$

Based on the stability theorem of dynamical systems, the strategy w of the platform corresponds to a stable strategy if it satisfies F_{plt}=0 together with $\frac{\mathrm{d}F_{plt}}{\mathrm{d}w}$<0. Therefore, it follows from (2) and (3) that i)If z<z_0^1, $F_{plt}|_{w=1}$=0, and so PLT's stable strategy is to supervise the crowdsourced data in a strict manner; ii)If z>z_0^1, $F_{plt}|_{w=0}$=0, and so PLT's stable strategy is to apply perfunctory governance; iii)If z=z_0^1, any $w \in [0,1]$ is an equilibrium point, and the stable strategy cannot be determined. We observe that $\frac{\partial H_{plt}}{\partial z}$<0 for all z, and thus H_{plt} is a decreasing function of z. The above study concerning the PLT's stable strategy demonstrates that when z increases, the SR is more inclined to check the received service, leading to the PLT carrying out more loose supervision. As the value of z declines, SR uses the crowdsourced data with less verification, and PLT implements rigorous supervision.

B. Service Provider

From (1), SP's replication dynamic equation is as follows: for all $x \in [0,1]$,

$$\begin{aligned} F_{sp}(x) =& x(1-x) \\ &\times \Big\{[1-(1-w)(1-y)(1-z)]G_{sp} + q(1-w) \\ &\quad \times (1-y)T_{sp} + w(1-y)P_{sp} - C^H_{sp} + C^N_{sp}\Big\} \\ =:& x(1-x)H_{sp}(z), \text{where } q = z + (1-z)\mu. \end{aligned} \quad (4)$$

In particular, we get that for all x:

$$\frac{\mathrm{d}F_{sp}(x)}{\mathrm{d}x} = (1-2x)H_{sp}(z). \quad (5)$$

Let

$$\begin{aligned} z_0^2 =& \frac{C^H_{sp} - C^N_{sp} - [1-(1-w)(1-y)]G_{sp} - w(1-y)P_{sp}}{(1-w)(1-y)[G_{sp} + (1-\mu)T_{sp}]} \\ &+ \frac{(1-w)(1-y)\mu T_{sp}}{(1-w)(1-y)[G_{sp} + (1-\mu)T_{sp}]} \end{aligned}$$

On the basis of the stability theorem for dynamical systems, the strategy x corresponds to a stable strategy if it satisfies F_{sp}=0 together with $\frac{\mathrm{d}F_{sp}}{\mathrm{d}x}$<0. Therefore, it follows from (4) and (5) that i)If z<z_0^2, $F_{sp}|_{x=0}$=0, and so SP's stable strategy is providing 'poor' service; ii)If z>z_0^2, $F_{sp}|_{x=1}$=0, and so the stable strategy of the SP is performing high-quality service; iii)If z=z_0^2, any $x \in [0,1]$ is an equilibrium point, and the stable strategy cannot be determined. It can be noted that $\frac{\partial H_{sp}}{\partial z}$>0 for all z, and so H_{sp} is an increasing function of z. The SP's stable strategy analysis explains the SP is more likely to deliver satisfactory service when SR is more cautious rather than placing direct trust in it. As z decreases, SP becomes increasingly irresponsible by performing perfunctory service.

C. Service Manager

From (1), Mgr's replication dynamic equation is given as: for all $y \in [0,1]$,

$$\begin{aligned} F_{mgr}(y) =& y(1-y) \\ &\times \Big\{(q(1-w)(1-x)T_{mgr} + w(1-x)P_{mgr} \\ &\quad - (1-w)(1-x)(1-z)G_{mgr} - C_f\Big\} \\ =:& y(1-y)H_{mgr}(w), \text{where } q \text{ same in (4).} \end{aligned} \quad (6)$$

In particular, we get that for all y,

$$\frac{\mathrm{d}F_{mgr}(y)}{\mathrm{d}y} = (1-2y)H_{mgr}(w). \quad (7)$$

Now let

$$w_0 = \frac{C_f + (1-x)(1-z)G_{mgr} - q(1-x)T_{mgr}}{(1-x)((1-z)G_{mgr} + P_{mgr} - qT_{mgr})}$$

According to the stability theorem for dynamical systems, the strategy y corresponds to a stable strategy if it satisfies F_{mgr}=0 together with $\frac{\mathrm{d}F_{mgr}}{\mathrm{d}y}$<0. Therefore, it follows from (6) and (7) that i)If w>w_0, $F_{mgr}|_{y=1}$=0, and so Mgr's stable strategy will be launching the filter function; ii)If w<w_0, $F_{mgr}|_{y=0}$=0, and Mgr's stable strategy will be disabling the filter function; iii)If w=w_0, any $y \in [0,1]$ is an equilibrium point, and the stable strategy cannot be determined. It can be seen that $\frac{\partial H_{mgr}}{\partial w}$>0 for all w, and so H_{mgr} is an increasing function of w. The above Mgr's stable strategy analysis indicates that the Mgr is more willing to launch the filtering process when the PLT prefers strict supervision. With decreasing w, PLT governs less the crowdsourced data, consequently resulting in a more negligent performance by Mgr.

D. Service Requestor

Based on (1), SR's replication dynamic equation is:

$$\begin{aligned} F_{sr}(z) &= z(1-z) \\ &\quad \times \Big\{(1-w)(1-x)(1-y) \\ &\qquad \times (L_{sr} - \mu R_{sr} - C_{sr}^{H}) - xC_{sr}^{H}\Big\} \\ &=: z(1-z)H_{sr}(y). \end{aligned} \tag{8}$$

In particular, we get that for all z:

$$\frac{\mathrm{d}F_{sr}(z)}{\mathrm{d}z} = (1-2z)H_{sr}(y). \tag{9}$$

Let

$$y_0 = 1 - \frac{xC_{sr}^{H}}{(1-w)(1-x)(L_{sr} - \mu R_{sr} - C_{sr}^{H})}$$

As analyzed by the stability theorem for dynamical systems, the strategy z corresponds to a stable strategy if it satisfies F_{sr}=0 together with $\frac{\mathrm{d}F_{sr}}{\mathrm{d}z}$<0. Therefore, it follows from (8) and (9) that i)If $y<y_0$, $F_{sr}|_{z=1}$=0, and so the stable strategy of SR is doubting the crowdsourced data; ii)If $y>y_0$, $F_{sr}|_{z=0}$=0, and thus the SR's stable strategy will be trusting directly without checking; iii)If y=y_0, any $z \in [0,1]$ is an equilibrium point, and the stable strategy cannot be determined. We notice that $\frac{\partial H_{sr}}{\partial y}$<0 for all y when $L_{sr}>\mu R_{sr}$+C_{sr}^{H}, and so H_{sr} is an increasing function of y. The above analysis of SR's stable strategy explicates that SR will believe more in crowdsourcing services if Mgr performs more filtering processes. Otherwise, SR will choose to mistrust due to decreasing y.

IV. Evolutionary Stable Strategy Analysis

Based on the nonlinear function stability discrimination in the first rule of Lyapunov stability theorem [13], the equilibrium points (EP) can be viewed as stable when eigenvalues of the Jacobian matrix derived from the above-calculated replication equations are less than 0, and the corresponding strategy combination is the ESS of the system. Table II presents calculated EPs, where ①: $\mu T_{sp}<C_{sp}^{H}$-C_{sp}^{N} and $L_{sr}<\mu R_{sr}$+C_{sr}^{H}; ②: $\mu T_{sp}>C_{sp}^{H}$-C_{sp}^{N};

It can be seen that there are two possible stable ESS points, namely EP_1 and EP_5. EP_1 indicates a situation in which SP always performs 'poor' service, and then Mgr and PLT never engage in the data verification, and finally, SR becomes blind in a manner that the received crowdsourced data will be utilized directly without any investigation. This is the worst case but a potential ESS point in the system. When ① is met, showing that the penalty in terms of trust is insufficient, and the cost of SR verifying the crowdsourced data becomes difficult to afford as it must be greater than the damage to SR caused by poor service. The situation brought by EP_1 must be avoided, meaning that parameters concerning ① should be carefully configured. EP_5 represents the equilibrium that SP provides high-quality crowdsourcing service thanks to its hardworking strategy selection, Mgr and PLT participate less in data verification, and the SR holds high confidence in SP's service, in a way that Mgr, PLT, and SR can save cost somehow and at the same time the crowdsourcing service is released correctly and successfully. Apparently, this is the ideal ESS point in the Crowd-IoT system. Meeting condition ② means the lost trust due to bad service should be greater than the gap between hardworking and neglectful performance for SP, which is reasonable that the penalty in terms of trust shall be large enough.

TABLE II: Stabilization table, *=uncertain

Equilibrium Point	(λ_1, λ_2, λ_3, λ_4) Symbol	Stability Analysis
EP_1(0,0,0,0)	(−, *, −, *)	ESS if ①
EP_2(0,0,0,1)	(+, +, +, *)	Unstable
EP_3(0,0,1,0)	(0, +, *, 0)	Unstable
EP_4(0,0,1,1)	(0, +, −, 0)	Unstable
EP_5(0,1,0,0)	(−, *, −, −)	ESS if ②
EP_6(0,1,0,1)	(−,−,−,+)	Unstable
EP_7(0,1,1,0)	(−,−, +, −)	Unstable
EP_8(0,1,1,1)	(−,−,+,+)	Unstable
EP_9(1,0,0,0)	(*, +, +, 0)	Unstable
EP_{10}(1,0,0,1)	(−, +, +, 0)	Unstable
EP_{11}(1,0,1,0)	(0, +, −, 0)	Unstable
EP_{12}(1,0,1,1)	(0, +, −, 0)	Unstable
EP_{13}(1,1,0,0)	(+, −, −, −)	Unstable
EP_{14}(1,1,0,1)	(+,−, −,+)	Unstable
EP_{15}(1,1,1,0)	(+,−,+,−)	Unstable
EP_{16}(1,1,1,1)	(+,−,+,+)	Unstable

For other unstable EPs, taking EP_{16} as an example, this ESS point describes a situation in which the SP provides high-level service; only PLT verifies the crowdsourced data to guarantee the service quality; however, if we return to the stable strategy analysis for PLT and SP, where we clearly explain that high-quality service provided by SP and the mistrust strategy of SR will cause PLT to be more inclined to implement loose supervision, which contradicts the situation depicted by E_{16}.

V. Numerical Results

TABLE III: Initial simulation parameter values

Parameter	Value	Parameter	Value	Parameter	Value
μ	0.3	C_{plt}^{N}	2	T_{plt}	20
G_{mgr}	12	C_{mgr}	1	T_{mgr}	15
G_{sp}	25	C_f	4	T_{sp}	26
P_{mgr}	5	C_{sp}^{H}	10	L_{sr}	15
P_{sp}	10	C_{sp}^{N}	2	R_{sr}	5
C_{plt}^{H}	12	C_{sr}^{H}	12		

By respecting the constraints of payoffs mentioned in Section II and two conditions in Seciont IV (meet ② and avoid ①), the parameters are set initially as in table III. With the purpose of observing the inter-influence between participants in terms of trust, in our work, we consider varying the following values to visualize how participants' strategies are influenced: μ=$\{0.1, 0.3, 0.5\}$; T_{sp}=$\{22, 26, 27\}$; C_f=$\{4, 0.5, 0\}$; C_{plt}^{H}=$\{12, 4, 3\}$

It can be seen from Fig. 2, as μ increases, i.e., higher-importance tasks are proposed, the probability that the SP

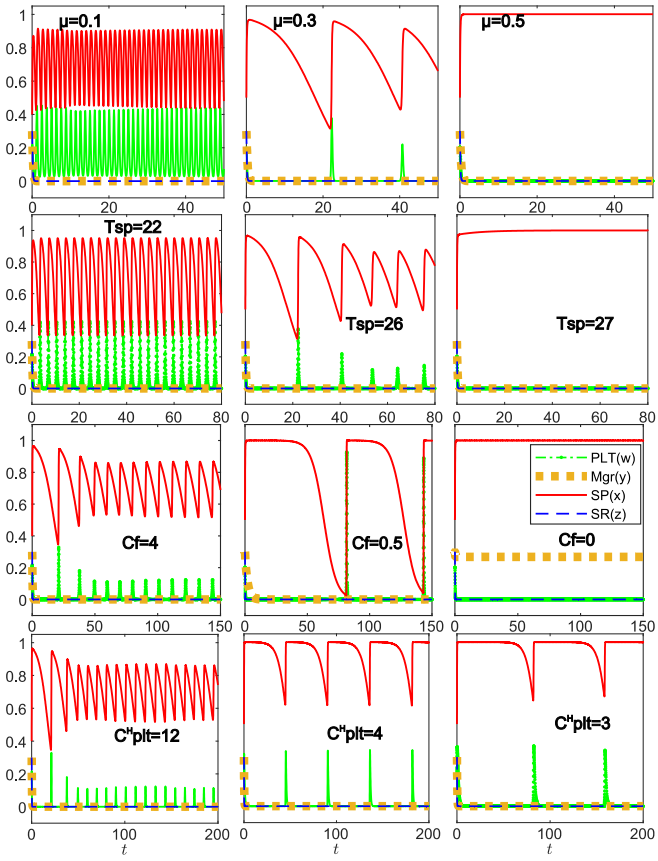

Fig. 2: Strategy changes by varying relevant values

will work conscientiously will increase. This is because the punishment and distrust received due to poor services are unaffordable for SP. Meanwhile, the PLT and Mgr will perform less investigation to save costs. As for strategy changes by varying Tp_{SP}, an increase in T_{sp} forces SP to be more willing to choose x strategy, i.e., hardworking for service. x values converge to 1 in figures of μ=0.5 and T_{sp}=27, and they both fit the condition ② studied in the previous section, i.e., μT_{sp}>C^H_{sp}-C^N_{sp}. This also shows the Crowd-IoT system becomes stable, matching EP_5 in Table II.

The impact of varying the additional cost of the filtering process, specifically from C_f=4 to C_f=0.5, reveals that cost reductions have a positive effect on improving the frequency of poor-quality services provided by SP. Furthermore, when C_f=0, the probability of Mgr implementing the filtering process remains constant, resulting in a high level of service from SP, i.e., x=1. Likewise, as the variable C^H_{plt} lowers, it is obvious that SP is more likely to provide services in a diligent manner. (It should be noted that the situation where C_f=0 is impossible in the real world, and the purpose of testing this value is to show effects caused by varying related costs.) By manipulating these two parameters, it becomes evident that the only way to reach the EP_5 without changing other configurations of the Crowd-IoT system is to reduce the cost associated with the verification of the crowdsourced data conducted by Mgr or PLT.

VI. Conclusion and Future Work

In this paper, a EG game is employed to model Crowd-IoT participants' interactions and to observe their strategy changes. In this EG-based model, participants are considered heterogeneous in terms of strategy, and participants are bounded rational, which fits the reality in true Crowd-IoT systems. Moreover, EG game modeling enables stable strategy analysis for each participant, where we give a preliminary but essential theoretical analysis. Based on this, the ESS of the system is also discussed. Finally, the numerical results demonstrate the changes in participants' strategy selection by varying different influence factors. In our future work, we consider combining SP and SR as IoT devices that can simultaneously both consume and provide services and apply the proposed model with real-world devices.

References

[1] *UC San Diego team's effort in DARPA's shredder challenge derailed by sabotage*. URL: https://jacobsschool.ucsd.edu/news/release/1150. (accessed: 03.02.2023).

[2] Runbo Su et al. "PDTM: Phase-based dynamic trust management for Internet of things". In: *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE. 2021, pp. 1–7.

[3] Victor Naroditskiy et al. "Crowdsourcing contest dilemma". In: *Journal of The Royal Society Interface* 11.99 (2014), p. 20140532.

[4] Victor Naroditskiy et al. "Crowdsourcing dilemma". In: *arXiv preprint arXiv:1304.3548* (2013).

[5] Chuanxiu Chi et al. "Multistrategy repeated game-based mobile crowdsourcing incentive mechanism for mobile edge computing in Internet of Things". In: *Wireless Communications and Mobile Computing* 2021 (2021), pp. 1–18.

[6] Runbo Su et al. "A Game Theoretical Model addressing Misbehavior in Crowdsourcing IoT". In: *2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE. 2023, pp. 195–203.

[7] Mingchu Li et al. "RIMNet: Recommendation Incentive Mechanism based on evolutionary game dynamics in peer-to-peer service networks". In: *Knowledge-Based Systems* 166 (2019), pp. 156–169.

[8] Shahzad Sarwar Bhatti, Xiaofeng Gao, and Guihai Chen. "General framework, opportunities and challenges for crowdsourcing techniques: A Comprehensive survey". In: *Journal of Systems and Software* 167 (2020), p. 110611.

[9] Daniel Schall. *Service-oriented crowdsourcing: architecture, protocols and algorithms*. Springer Science & Business Media, 2012.

[10] J Maynard Smith and George R Price. "The logic of animal conflict". In: *Nature* 246.5427 (1973), pp. 15–18.

[11] John Maynard Smith. "Evolution and the Theory of Games". In: *Did Darwin get it right? Essays on games, sex and evolution*. Springer, 1982, pp. 202–215.

[12] Carlos P Roca, José A Cuesta, and Angel Sánchez. "Evolutionary game theory: Temporal and spatial effects beyond replicator dynamics". In: *Physics of life reviews* 6.4 (2009), pp. 208–249.

[13] Ross Cressman. *The stability concept of evolutionary game theory: a dynamic approach*. Vol. 94. Springer Science & Business Media, 2013.