IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 1, 2016, accepted November 9, 2016, date of publication November 22, 2016, date of current version March 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2630736

Multi-Reciprocity Policies Co-Evolution Based Incentive Evaluating Framework for Mobile P2P Systems

KUN LU[1], SHIYU WANG[1], GUANGHAI CUI[2], MINGCHU LI[1], AND HANNAN-BIN-LIAQAT[3]
[1]School of Software Technology, Dalian University of Technology, Dalian 116620, China
[2]School of Information and Electrical Engineering, Ludong University, Yantai 264025, China
[3]Department of Information Technology, University of Gujrat, Hafiz Hayat Campus, Gujrat 50700, Pakistan

Corresponding author: M. Li (mingchul@dlut.edu.cn)

This work was supported by the National Science Foundation of China under Grant 61403059 and Grant 61572095.

ABSTRACT With the development of wireless sensing technologies, numerous sensing applications from the Internet of Things (IoT) are widely used in life and industry. Mobile peer-to-peer (MP2P) system is one of the typical IoT applications, in which peers share their sensing information. Reciprocity-based incentive mechanisms are widely used to encourage cooperation among peers and maintain robustness of MP2P systems. However, the effectiveness of different reciprocity-based mechanisms is difficult to compare theoretically. In this paper, we propose a general evaluating framework to help design and analyze incentive mechanisms for which reciprocal peers can have different reciprocal policies. Using our proposed framework, the evolution dynamics of multiple incentive policies that coexist in MP2P systems can be analyzed. The simulation results show the system robustness and best strategies in various circumstances. In addition, we consider a most common attack model, whitewashing, in MP2P systems and bring in a small entry fee to defeat whitewashers. The results show that this framework can well defend whitewashing and is more suited for real MP2P systems.

INDEX TERMS Co-evolution, reciprocity-based incentive mechanism, evolutionary game, MP2P, evaluating framework.

I. INTRODUCTION

With the development of wireless communication technologies and intelligence of smart objects, the ways people exchange information are redefined [1], [2]. Devices with sensing, computing, and communication capabilities are connected to each other and form a network to collect information, such as traffic monitoring and noise map making, object tracking and identification.

A typical topology of these wireless sensing devices is a Mobile P2P (MP2P) structure, in which peers share information with each other. However, in a real MP2P system, most peers are selfish and are not generous enough to share their limited resources. Peers seek to maximize their own benefits by consuming their resources. Saroiu's study [3] showed that over 70% of peers in Gnutella are free riders who never share resources with other peers, and the proportion of free riders in Gnutella increased to 85% five years later. Thus, there is compelling need to design an effective incentive mechanism for MP2P systems.

Reciprocity-based incentive mechanisms [4]–[7] are most commonly conducted solutions to overcome free-riders in a MP2P system. By using an incentive mechanism, the service provider decides whether to serve the requester or not based on requester's prior transaction histories with other peers, which makes the MP2P system contribution-aware. To gain a better history of transactions, rational and selfish peers have motivations to cooperate with other peers, because doing so will produce direct or indirect benefits in the future. It can influence peers' behaviors and encourage them to provide services to increase the benefit of the entire MP2P system.

In realistic MP2P scenarios, peers are bounded-rational and strategic. With the former meaning, the peers want to maximize their own payoff, but their cognitive capability is limited, and they may make mistakes for some reason. The term strategic refers that peers can choose their actions (e.g., cooperation or defection) when they interact with other peers. Thus, evolutionary game theory is a quite appropriate tool to model the interaction and depict the evolutionary dynamics of

MP2P peers [8], [9]. Evolutionary game-based mathematical frameworks have been proposed by researchers to analyze the robustness of a certain mechanism (Zhao et al. [10]; Wang et al. [11]). Existing work focused mainly on a multi-round, three-strategy, evolutionary game, which contains several rounds. In each round, each peer can choose strategies from Always Cooperate (ALLC), Always Defect (ALLD), or Reciprocate (R) and decides whether to cooperate according to the requester's transaction history, i.e., a reciprocator always grants a service to an ALLC peer and denies serving an ALLD peer. In order to improve payoff in the future, peers may imitate others' strategies with better payoffs in the current round. However, previous work has two major disadvantages, i.e., in the proposed approaches, only one reciprocity policy is considered at a time, which means all the peers with R strategy have the same and the only reciprocity policy. For example, assuming A, B, and C are reciprocal peers, they have the same reciprocity policy, so A and B will respond with the same action (cooperate or defect) to a request from C. But in a realistic MP2P system, peers A and B may respond with a different action (cooperate or defect) to C although they are both reciprocators, because they may have a distinct degree of generosity or cooperation standards. Thus, for characterizing MP2P peers' intrinsic diversity, the reciprocity strategy should be expanded to contain more reciprocity policies.

Other problems of MP2P systems are malicious attacks. Whitewashing attacks [12] are most common attacks in MP2P systems, under which peers are inclined to leave the network and join again with a new identity when they have a bad transaction history. Especially in mobile environment, peers can frequently join and leave a system easily, therefore whitewashing is much more serious. These whitewashers significantly violate the fairness of MP2P networks, but most existing incentive mechanisms [8], [9] pay little attention to it.

In this paper, we propose a general evaluating framework based on evolutionary game theory to analyze and evaluate the incentive mechanisms for MP2P networks. In our framework, evolutionary game theory is used to describe peers' interaction behaviors and dynamic evolutions. More importantly, we extend the reciprocator strategy to contain multiple reciprocity policies, including the mirror reciprocity policy, proportional reciprocity policy, and indirect reciprocity policy [13]. These policies can co-exist in one MP2P network, and individual reciprocator peers can use any one of the reciprocal policies. We perform extensive simulations to analyze the robustness from many aspects, e.g., payoff-cost ratio, co-evolution of reciprocity policies, whitewashing attack, and mutation (mistake to imitate expected strategies). Simulation results show that our framework is robust and suitable for stimulating a realistic MP2P networking environment.

The rest of this paper is organized as follows. In Section 2, we summarize related work on MP2P platform and incentive mechanisms. In Section 3, we describe our model in detail. In Section 4, we present simulation results and relative analysis. In Section 5, we conclude this paper.

II. RELATED WORK

Smart mobile devices have a great potential to improve the performance of IoT applications by enabling access to their built-in sensors. In the past few years, significant research efforts have been made on IoT, mainly from a thing-oriented perspective. A wide range of areas are covered, including topology forming [2], [14]–[16], security [17], [18], robustness [19], [20] and etc.

An MP2P structure is a typical topology for these smart devices, in which peers form a ubiquitous connectivity through wireless network and share resources with each other freely [21]. In such MP2P systems, cooperation among peers are crucial to share and forward information. However, due to limited resources (such as electricity, CPU, memory, etc.), sharing resources and maintaining connection is much more costly for mobile peers. Thus, free-riding problems are much more serious in MP2P systems as compared to wired P2P systems.

Incentive mechanisms are used to solve the problem of free-riders. The concept of incentive mechanisms was borrowed from economics and management. The core thoughts of incentive mechanisms always target a specific behavior, and they sometimes induce unwanted responses from workers and produce undesired results [13]. In this way, a peer will tend to perform more cooperatively to have a better chance of receiving more services. Incentive mechanisms generally can be divided into four different types, i.e., micropayment-based mechanism, fixed contribution-based mechanism, reciprocity-based mechanism, and evolutionary game-based mechanism.

Micropayment-based schemes require payments with virtual currency when a specific service is obtained, and the peer who provides the service may get the corresponding payment. But this approach may cause problems related to setting prices, i.e., fairness [22], inflation, and deflation [23]. Fixed-contribution scheme requires peers to provide a fixed (minimum) amount of services before getting services from others. However, it mainly restricts the access rights of peers since it can never force them to cooperate after they enter the system [2]. The reciprocity-based scheme is also known as reputation-based scheme. It always has a certain algorithm to calculate peers' reputation [5]–[7], which symbolizes the amount of their service and its quality.

All of the above schemes can encourage peers to cooperate, but the schemes hardly consider the possibility that peers might change their strategies after the transaction is finished. Thus, game theory has been incorporated into the study of incentive mechanisms to better describe peers' behaviors.

In MP2P networks, peers always get rational or strategic features, and they determine their strategies independently based on the desire to maximize their profit [25]. Considering the features of peers, game theory is an appropriate tool to model and analyze their behaviors when conflicts occur between individuals' interests and the overall public benefit. Thus, game theory is used extensively in the study and analysis of cooperation in a MP2P system [26]–[28].

Different from classic game theory, the evolutionary game focuses on the dynamics of the peers' strategies and on analyzing the stability of the system after a given evolutionary period. So, in order to use the evolutionary game to solve the problem of free riders, four basic problems must be solved, i.e., 1) the composition of rational behavior; 2) how to transform rational individuals to bounded-rational individuals and how they affect the design of the incentive mechanism; 3) how to establish a common framework to evaluate and analyze a certain mechanism; and 4) the optimal contracts in different tasks and network structures [29].

Some researchers use the evolutionary game to model and analyze cooperation in both heterogeneous and homogeneous MP2P systems [10], [30]–[33]. Specially, Zhao et al. [10] proposed a mathematical framework to analyze the robustness of a certain mechanism and to consider the cost of transmitting resources. Replicator dynamics were used to analyze dynamics in an infinite, well-mixed population, but a real network has a finite population and a structured network. Thus, Wang et al. [30] proposed another mathematical method using fixed probability and discussed the important role of selection intensity in evolution. Furthermore, Wang et al. [31]–[33] considered how to promote cooperation among different groups by using co-evolution. These studies show that this research area is progressing in an interesting direction.

In addition to lack of cooperation, malicious attacks are another serious problem in MP2P networks. Due to cheap pseudonyms [9], whitewashers frequently participate and quit the system to get a new identity and profit from the system. Collusion [34] is another attack in which peers stick together to boast each other and gain a high reputation or slander someone. The Sybil attack [35] is performed as one node and produces a set of fake identities to control the entire system so that it can do whatever is desired. In the absence of a trusted central entity, Sybil attacks can never be eliminated. Due to the mobility of participants, attacks in MP2P applications are much more serious and hard to defend. Therefore, a robust and easy implemented incentive mechanism for MP2P systems is in great need.

Most of the studies that have been mentioned neglected the co-existing incentive policies and attacks in the MP2P system. In this paper, we consider multi-incentive policies and whitewashing in the system.

III. TRANSACTION GAME

The transaction game is a repeated game that consists of N players. In one single round, each player randomly sends requests to m other players. The players who receive the requests must decide whether to grant a service or not. This means that a player may be a requester and a provider in each round. The total benefit (or payoff) a player receives depends on the number of player gets a service and grants a service. To simplify the issue, we assume this MP2P network as well-mixed and each provider has all the services others may request.

Algorithm 1 Transaction Game

for All rounds **do**
  for $i = 0$ to N **do**
    for $k = 0$ to m **do**
      $provider_j \leftarrow$ random(N);
      $Player_i$ sends a request to $provider_j$;
      $provider_j$ grants or denies a service;
    end for
  end for
end for

We implemented this game in a well-mixed MP2P network. As shown in Alg. 1, in each round, each player randomly sends requests to m players (excluding itself) as a requester. Providers grant a service according to their own strategies. It won't influence the results if a player sends requests to a player for repeated times.

A. STRATEGIES

We classify available strategies in this paper into three types, according to their responses when they receive a request. These include:

ALLC: A peer with ALLC strategy always grants a service unconditionally and neglects the requester's transaction history.

ALLD: Opposite from ALLC, a peer with ALLD strategy never grants a service and neglects the requester's transaction history.

R: This player grants a service according to the requester's transaction history. For instance, a reciprocator may always serve ALLC and never serve ALLD.

However, in a real system, a reciprocator may follow different rules to decide a response when getting a request. We call these rules "reciprocal policy". In this paper, we mainly use three different reciprocal policies that may co-exist in one homogenous network. The three reciprocal policies are as follows:

(1) Power_Mirror. The mirror reciprocal policy was first proposed by Feldman et al. [36] in 2003. It is described as one's serving the requester with the same probability that the requester serves others. The probability is the ratio of the number of a requester serving others (N_{j_serve}) to the number being served by others ($N_{j\_get\_request}$)(see Eq.1).

$$p_{mirror} = \frac{N_{j\_serve}}{N_{j\_get\_request}} \tag{1}$$

However, if only the transaction history is considered to grant a service, the fairness and efficiency cannot be guaranteed. For instance, a reciprocator may serve another reciprocator with a low probability. But actually, a reciprocator is a good peer who never serves a defector. Thus, we incorporate

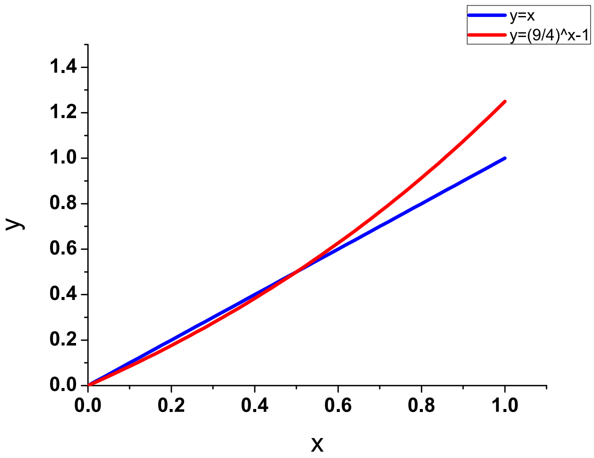


FIGURE 1. Power vs. linear function.

punish-reward in the reciprocity strategy. We assumed that 0.5 was the intermediate cooperation probability of a peer. So, we reward those who have serving probabilities greater than 0.5, and we punish those who have probabilities less than 0.5 by using the function shown in Eq.2. The curve of these two functions (power function and linear function) are shown in Fig. 1.

$$y = (\frac{9}{4})^x - 1 \tag{2}$$

Using this function, we introduce punish-reward into this strategy and modify the original strategy, as shown in Eq. 3.

$$p_{power\_mirror} = min((\frac{9}{4})^{p_{mirror}} - 1, 1) \tag{3}$$

(2) Power_proportion. Proportion policy can be described as one may serve others according to the requester's history of receiving service [28]. The probability is ratio of the number of getting service from others (*get_service*) to the number of sending service to others (*send_service*)(shown as Eq.4).

$$p_{prop} = min(\frac{get\_service}{send\_service}, 1) \tag{4}$$

For the same reason as power_mirror, we modify this strategy to power_prop, as shown in Eq.5.

$$p_{power\_prop} = min((\frac{9}{4})^{p_{prop}} - 1, 1) \tag{5}$$

(3) Indirect. This policy comes from Nowak's upstream reciprocity [37]. One may serve others only if one gets service last time. This is a weak strategy to facilitate cooperation, but it is still useful for restricting defectors.

B. PAYOFF CALCULATION

Table 1 shows the payoff matrix we use in this game. When a peer gets a service, he has a positive payoff α, and a peer gets a cost β if he grants a service. For instance, peer A shares resources with peer B, but peer B shares nothing with peer A. Thus, peer A gets a negative payoff $-\beta$ and peer B gets a positive payoff α.

TABLE 1. Payoff matrix.

	C	D
C	α-β ,α-β	-β ,α
D	-β ,α	0,0

In order to assure fairness, we consider the average payoff of each strategy [38]. The payoff of a peer with strategy *i*, i.e., $payoff_i$, is as shown in Eq.6. The ratio of the sum of peers with strategy *i* getting service (*num_get_service*) to the sum of send requests (*num_send_request*) symbolizes the probability that strategy *i* will get service. So, the first part of this equation shows the average positive payoff strategy that *i* receives. The second part of this equation is the average cost of strategy *i*.

$$payoff_i = \alpha * \frac{num\_get\_service}{num\_send\_request} - \beta * \frac{num\_send\_service}{num\_get\_request} \tag{6}$$

C. STRATEGY UPDATE

Strategy update models how peers change their strategies to acquire the maximum payoff. After each round, peers change their strategies according to their own payoff. Then, peers begin a new round of transactions until the system is dynamically stable. In this paper, we consider two learning models which are widely used (CBLM and OLM) and mutations as parts of the strategy update process.

Algorithm 2 CBLM

```
for each peer do
  //randomly select a float prob1 ∈ (0,1)
  prob1 ← random(0,1);
  if prob1 < γa then
    Calculate p_{i→best};
    prob2 ← random(0,1);
    if prob2 < p_{i→best} then
      Change to strategy best
    else
      Maintain strategy i
    end if
  else
    Maintain strategy i
  end if
end for
```

Current best-learning Model (CBLM). As described in Alg. 2, after each round, each node considers whether to change its strategy with the probability γ_a, which is called the adaptive rate. A peer changes to the most profitable strategy with the probability as the sensitivity γ_s to payoff gap [10] (Eq.7).

$$p_{i \rightarrow best} = \gamma_s * (payoff_{best} - payoff_i) \tag{7}$$

Opportunistic Learning Model (OLM). As shown in Alg. 3, after each round, each node chooses a teacher node with

Algorithm 3 OLM

for each peer **do**
  Choose a teacher with probability γ_a
  Calculate $p_{i \rightarrow teacher}$
  $prob1 \leftarrow$ random(0,1)
  if $prob1 < p_{i \rightarrow teacher}$ **then**
    Change to teacher's strategy
  else
    Maintain strategy i
  end if
end for

probability γ_a and change to the teacher's strategy if the teacher's payoff is better than its own payoff with probability as the sensitivity γ_s to payoff gap [10] (Eq.8).

$$p_{i \rightarrow teacher} = \gamma_s * (payoff_{best} - payoff_i) \tag{8}$$

IV. SIMULATION AND ANALYSIS

We conduct our experiment in four basic steps:

(1) Initialization: Initialize peers' strategies according to the proportion of each strategy and set other attributes of a peer to 0.

(2) Warming up: In order to simulate real MP2P transactions, a warming-up process is necessary. During the warming-up phase, each peer sends 100 requests to other peers randomly (excludes itself) and gets responses. For power_mirror and power_prop strategies, one may never know whether the requester is good or not when there is no transaction history. So, they may serve the requester once before they have the transaction history.

(3) Strategy update: In this phase, each peer chooses to learn others' strategies under different learning models (CBLM or OLM). After learning strategies, mutation begins (optional in different experiments), and each peer may have 1% probability of mutating to other strategies (including its own strategy). To get a stable situation, we perform 10,000 rounds.

(4) Statistic: Collect information of the system status, including fractions of each strategy and the average payoff of the system.

We explore some key factors that impact the system robustness to the greatest extent, i.e., 1) the payoff-cost ratio (α/β), 2) the cost when getting transaction information from the system, and 3) the co-evolution of various reciprocity strategies. In addition, whitewashing attacks can harm the system, and the main method we use in the simulation is to add the cost of getting a new identity. To simplify the experiment, we set β to 1. According to the definition of robustness [39], we consider the proportion of cooperation and peers with incentive strategies as the metric to evaluate the system robustness. The initial proportion of each strategy was equally large without specially illustrate. Without special emphasis, we use the parameters shown in Table 2.

TABLE 2. Parameters.

name of the parameters	value
Size of network	500
Warming_Up requests	100 times/node
Steps	10000
Mutation Rate	0.01
γ_a	0.1
γ_s	0.04

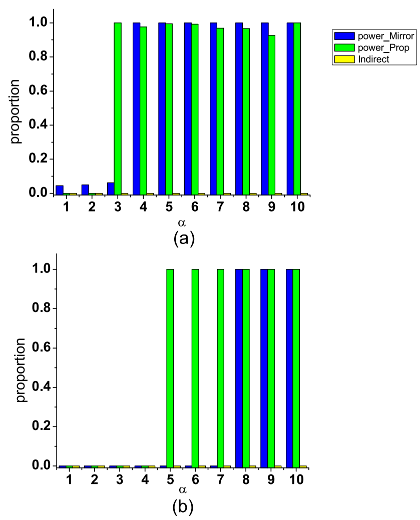


FIGURE 2. Proportion of C + R under stable status: (a) CBLM; (b) OLM.

A. IMPACT OF α/β

First, we consider the situation with the power_mirror strategy. Zhao et al. [10] gave a specific mathematical proof when using the mirror and proportion strategy. We obtained similar results using an improved strategy. Fig.2 shows that, for the CBLM learning model, when α is small ($\alpha < 4$), defectors are always dominant in the system. But, when α is relatively large ($\alpha > 4$), the dilemma is weak. Thus, since we have incentive strategies, the defectors may be eliminated. Similar results are obtained with OLM. For the power_prop strategy, generally, as long as the initial proportion of R strategy is larger than $1/(\alpha - 1)$, the system is always robust. So, with only one reciprocity strategy in the system, under the same condition, the power_prop strategy is better than the power_mirror strategy. As for the indirect strategy, it could restrict defect behaviors to some extent, but it is a very weak strategy to facilitate cooperation.

Mutation is an important mechanism to ensure the diversity species throughout the world. We consider mutation in our model. At the end of each round, after the peers changing strategies using the learning model, each peer has the same probability of changing its strategy to any of the available strategies (including his or her own strategy). In this paper, we set this probability to 0.01. As shown in Figs. 3-5, the presence of mutation in the system may always help to keep system stable after a short period of evolution. But the proportion of each strategy at stable status depends on the payoff-to-cost ratio. In both the CBLM and OLM learning

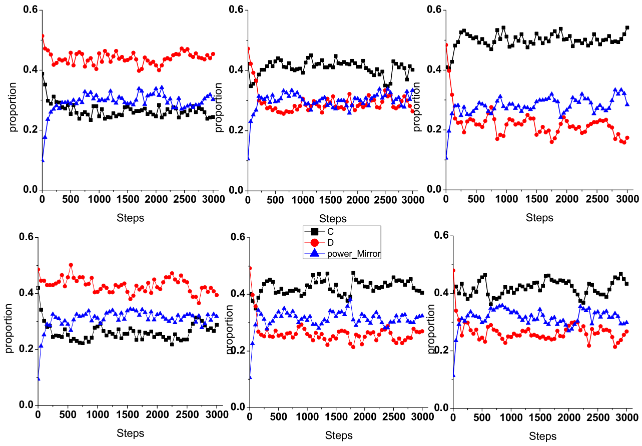


FIGURE 3. **Power_mirror under mutation: Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.**

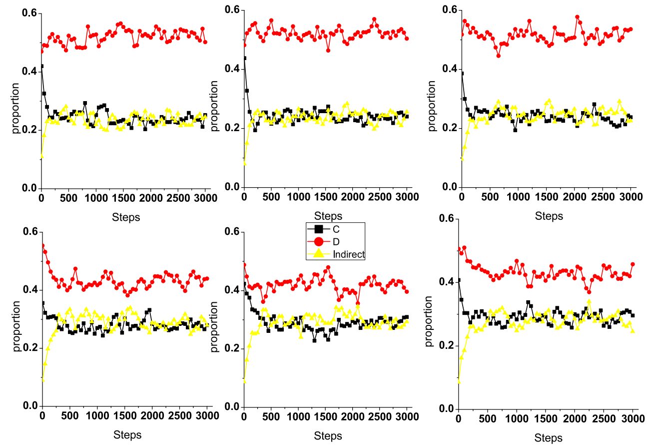


FIGURE 5. **Indirect under mutation:Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.**

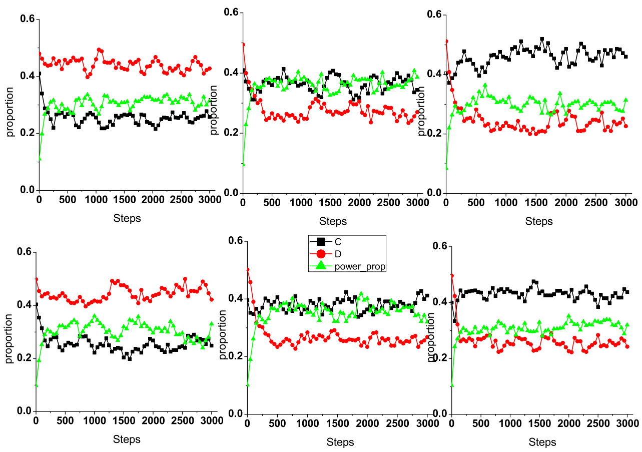


FIGURE 4. **Power_prop under mutation:Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.**

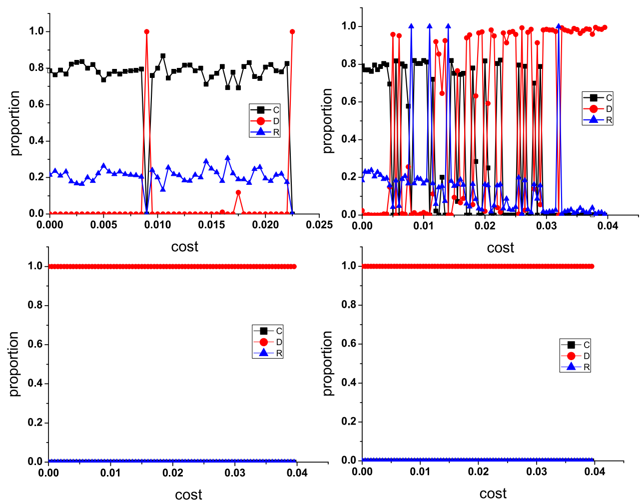


FIGURE 6. **Effect of info_cost on power_mirror: Top, CBLM; bottom, OLM; Left to right $\alpha = 4\alpha = 7$.**

models, when α is small, defectors dominate the system. As α increases, the proportions of C and R also increase. The indirect strategy may survive under mutation, but a proportion of it is maintained around the point of the initial proportion. Still, it shows that the indirect strategy is a weak incentive strategy.

B. COST OF GETTING TRANSACTION INFORMATION

In a real network, peers who get information from the system have to cost more or less. So, we consider these costs in our simulation to determine how these costs affect robustness of the system. The modified payoff for incentive strategy is shown by Eq.9.

$$payoff_{new} = payoff_{old} - info\_cost * \alpha \tag{9}$$

Adding *info_cost* means lowering the payoff of strategies power_mirror and power_prop; the indirect strategy uses its own information, so *info_cost* cannot affect it. Figs. 6 and 7 show the proportions of each strategy at stable status with different *info_cost*. When the *info_cost* is low, the incentive strategy can work well with high α. But when *info_cost* is rather large, peers with the reciprocity strategy get very low payoff, so that they cannot survive in the system.

So, in order to fulfill the need of information cost and maintain the robustness of the system, we only need a tiny *info_cost*.

C. RECIPROCITY STRATEGIES CO-EVOLUTION

As we discussed earlier, the expanded strategy set can provide a better description of the peers' behaviors. In this simulation, we did not consider *info_cost*.

Fig.8 shows that, under CBLM, when $\alpha = 1$, the power_mirror strategy is the best, and the power_prop strategy will be eliminated. However, the indirect strategy can co-exist with the power_prop strategy. After an indirect peer receives a service, it may continue to serve and deny serving when gets rejection. As α increases, the situation changes, and power_prop keeps dominating the system and takes over the system at stable status. We obtain similar results for OLM.

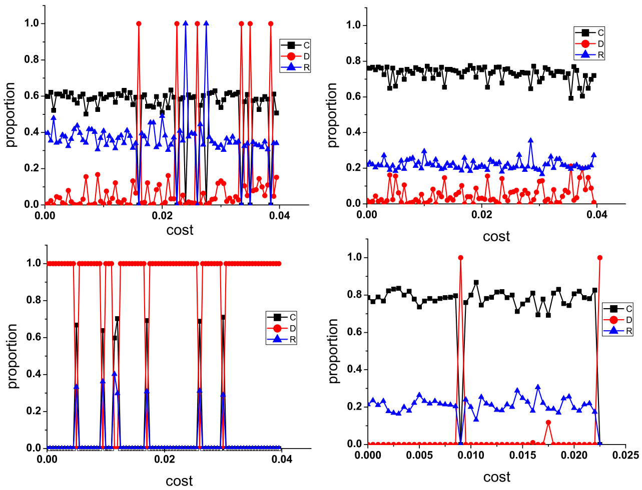


FIGURE 7. Effect of info_cost on power_prop: Top, CBLM; bottom, OLM; Left to right $\alpha = 4\alpha = 7$.

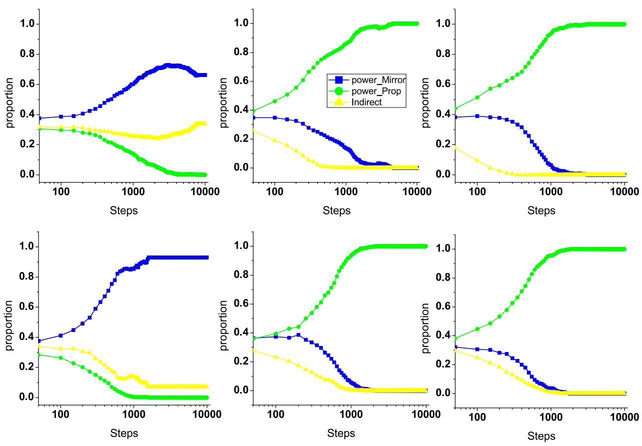


FIGURE 8. Competition among three incentive strategies:Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.

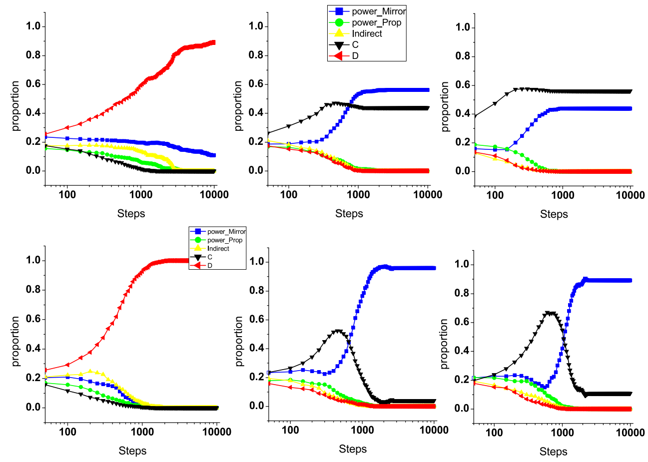


FIGURE 9. Competition among five incentive strategies: Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.

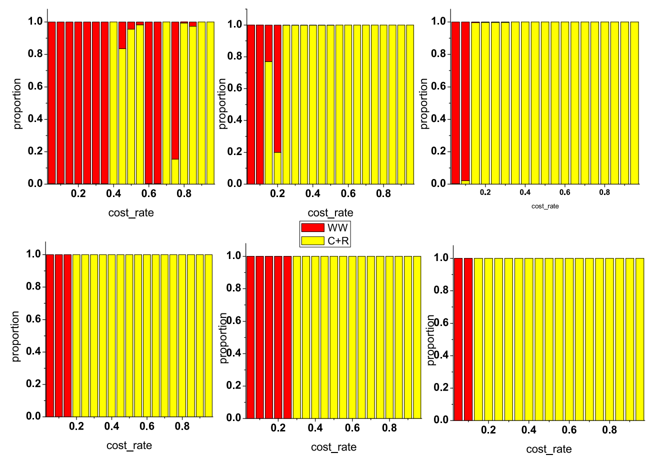


FIGURE 10. Restrict whitewashers with ID_cost(no pure): Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.

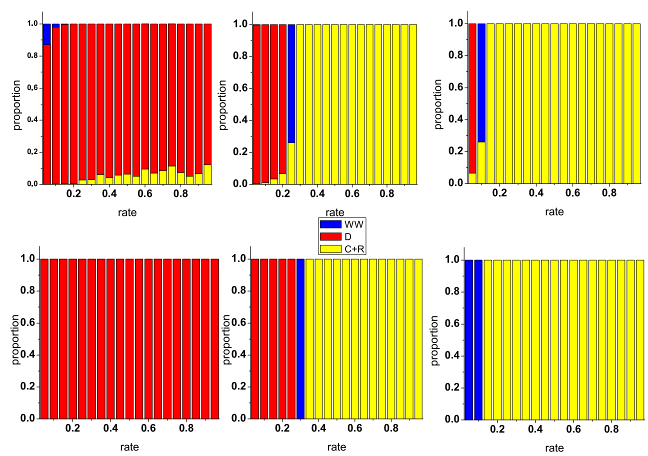


FIGURE 11. Restrict whitewashers with ID_cost(with pure): Top, CBLM; bottom, OLM; Left to right $\alpha = 1\alpha = 5\alpha = 9$.

In the real world, we may always see role models or selfish people. So, adding pure strategies is reasonable. Fig.9 shows that, whether under CBLM or OLM, power_Mirror is always the best strategy when α is larger than 1. But the proportion of cooperators may vary for different values of α, and they may increase following the rule we found in the first experiment. Overall, with pure strategies in the system, when α is larger than 1, the system is always robust.

D. WHITEWASHING ATTACK AND DEFENSE

Whitewashing is the most common attack in a MP2P system due to cheap pseudonyms [30]. They frequently join and leave the system to eliminate their transaction history to cheat and get more services. In this paper, we assume that whitewashers may wipe out their history to get a new identity every time they receive a request or a service. Under free identity, whitewashers always can dominate the system and cause the entire system to collapse.

In order to restrict whitewashers, we give all newcomers an identity cost. The payoff is modified as Eq.10. For whitewashers, it is Eq.11. When the cost is low, whitewashing is still worthwhile, but, when the cost is large, whitewashers can be eliminated (as shown in Fig.10), but good newcomers are hurt in the process.

$$payoff_{i_{new}} = payoff_i - \frac{ID\_cost * change\_times}{num\_transaction} \quad (10)$$

$$payoff_{whitewasher} = payoff_i - ID\_cost \quad (11)$$

When we consider pure strategies, D can defeat whitewashers because they have low ID_cost. But when the ID_cost is large, whitewashers are eliminated due to the cost. ALLD are eliminated because of large α (shown in Fig.11).

V. CONCLUSIONS

In this paper, we present a simulation framework to analyze the evolution dynamics of bounded rationality peers in a MP2P incentive system. In the framework, different reciprocal peers have different reciprocity policies, which more precisely characterize the intrinsic diversity in a realistic scenario. The reciprocity policies are used in the framework, including the mirror reciprocal policy, the proportion reciprocal policy, and the indirect policy. The proposed simulation framework can analyze the evolution dynamics of multiple incentive policies that co-exist in the MP2P incentive system. Through various experiments, we find that with larger payoff getting service, using incentive strategies may facilitate cooperation. Adding info_cost may be better suited for a real system, but a small rate is required to help both cooperation and the simulation of a real circumstance. Whitewashing harm the benefits of the entire system, and adding a large ID_cost may effectively restrict whitewashing behaviors while maintaining the robustness of the system.

REFERENCES

[1] T. Qiu, L. Chi, W. Guo, and Y. Zhang, "STETS: A novel energy-efficient time synchronization scheme based on embedded networking devices," *Microprocess. Microsyst.*, vol. 39, no. 8, pp. 1285–1295, 2015.

[2] T. Qiu, W. Sun, Y. Bai, and Y. Zhou, "An efficient multi-path self-organizing strategy in Internet of Things," *Wireless Pers. Commun.*, vol. 73, no. 4, pp. 1613–1629, Dec. 2013.

[3] S. Saroiu, P. K. Gummadi, and S. D. Gribble, "Measurement study of peer-to-peer file sharing systems," in *Proc. Electron. Imag. Int. Soc. Opt. Photon.*, Dec. 2001, pp. 156–170.

[4] K. G. Anagnostakis and M. B. Greenwald, "Exchange-based incentive mechanisms for peer-to-peer file sharing," in *Proc. 24th Int. Conf. Distrib. Comput. Syst.*, Mar. 2004, pp. 524–533.

[5] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web*, May 2003, pp. 640–651.

[6] R. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 4, pp. 460–473, Apr. 2007.

[7] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.

[8] D. Qiu and R. Srikant, "Modeling and performance analysis of BitTorrent-like peer-to-peer networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, pp. 367–378, Oct. 2004.

[9] M. Feldman and J. Chuang, "The evolution of cooperation under cheap pseudonyms," in *Proc. 7th IEEE Int. Conf. E-Commerce Technol. (CEC)*, Jul. 2005, pp. 284–291.

[10] B. Q. Zhao, J. C. S. Lui, and D.-M. Chiu, "A mathematical framework for analyzing adaptive incentive protocols in P2P networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 2, pp. 367–380, Apr. 2012.

[11] Y. Wang, A. Nakao, A. V. Vasilakos, and J. Ma, "Overview of modeling and analysis of incentive mechanisms based on evolutionary game theory in autonomous networks," in *Proc. 10th Int. Symp. Auto. Decentralized Syst.*, Mar. 2011, pp. 659–664.

[12] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "A survey on trust and reputation models for Web services: Single, composite, and communities," *Decision Support Syst.*, vol. 74, pp. 121–134, Jun. 2015.

[13] F. L. Haddi and M. Benchaïba, "A survey of incentive mechanisms in static and mobile P2P systems," *J. Netw. Comput. Appl.*, vol. 58, pp. 108–118, Dec. 2015.

[14] Y. Zhang, X. Sun, and B. Wang, "Efficient algorithm for k-barrier coverage based on integer linear programming," *China Commun.*, vol. 13, no. 7, pp. 16–23, Jul. 2016.

[15] T. Qiu, X. Liu, L. Feng, Y. Zhou, and K. Zheng, "An efficient tree-based self-organizing protocol for Internet of Things," *IEEE Access*, vol. 4, pp. 3535–3546, 2016.

[16] S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 78, no. 1, pp. 231–246, 2014.

[17] C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Commun.*, vol. 13, no. 7, pp. 60–65, Jul. 2016.

[18] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *J. Internet Technol.*, vol. 15, no. 6, pp. 929–935, 2014.

[19] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolb, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things," *Comput. Netw.*, vol. 101, pp. 127–143, Jun. 2016.

[20] Y. Zheng, J. Byeungwoo, D. Xu, Q. M. J. Wu, and H. Zhang, "Image segmentation by generalized hierarchical fuzzy C-means algorithm," *J. Intell. Fuzzy Syst.*, vol. 28, no. 2, pp. 961–973, 2015.

[21] Y. Wang, A. V. Vasilakos, Q. Jin, and J. Ma, "Survey on mobile social networking in proximity (MSNP): Approaches, challenges and architecture," *Wireless Netw.*, vol. 20, no. 6, pp. 1295–1311, Aug. 2014.

[22] P. Antoniadis and C. Courcoubetis, "Enforcing efficient resource provisioning in peer-to-peer file sharing systems," *ACM SIGOPS Oper. Syst. Rev.*, vol. 40, no. 3, pp. 67–72, Jul. 2006.

[23] N. Padhariya, A. Mondal, and S. K. Madria, "Top-*k* query processing in mobile-P2P networks using economic incentive schemes," *Peer-Peer Netw. Appl.*, vol. 9, no. 4, pp. 731–751, Jul. 2016.

[24] P. Antoniadis and B. L. Grand, "Incentives for resource sharing in self-organized communities: From economics to social psychology," in *Proc. 2nd Int. Conf. Digit. Inf. Manage. (ICDIM)*, vol. 2. Oct. 2007, pp. 756–761.

[25] G. Cui, M. Li, Z. Wang, J. Ren, D. Jiao, and J. Ma, "Analysis and evaluation of incentive mechanisms in P2P networks: A spatial evolutionary game theory perspective," *Concurrency Comput., Pract. Exper.*, vol. 27, no. 12, pp. 3044–3064, Aug. 2015.

[26] F. Saab and M.Awad, "Modeling attacks on MANET using an incomplete repeated Bayesian game," in *Proc. 7th Int. Conf. Intelligent Syst.*, Sep. 2014, pp. 269–288.

[27] X. Kang and Y. Wu, "Incentive mechanism design for heterogeneous peer-to-peer networks: A Stackelberg game approach," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1018–1030, May 2015.

[28] Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1287–1303, Aug. 2012.

[29] M. Feldman and J. Chuang, "Overcoming free-riding behavior in peer-to-peer systems," *ACM SIGECOM Exchanges*, vol. 5, no. 4, pp. 41–50, Jul. 2005.

[30] Y. Wang, A. Nakao, A. V. Vasilakos, and J. Ma, "P2P soft security: On evolutionary dynamics of P2P incentive mechanism," *Comput. Commun.*, vol. 34, no. 3, pp. 241–249, Mar. 2011.

[31] Z. Wang, A. Szolnoki, and M. Perc, "Self-organization towards optimally interdependent networks by means of coevolution," *New J. Phys.*, vol. 16, no. 3, p. 033041, Mar. 2014.

[32] Z. Wang, L. Wang, and M. Perc, "Degree mixing in multilayer networks impedes the evolution of cooperation," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 89, no. 5, p. 052813, May 2014.

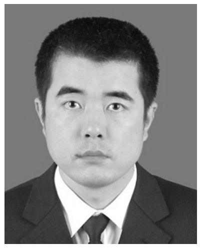
[33] Z. Wang, A. Szolnoki, and M. Perc, "Rewarding evolutionary fitness with links between populations promotes cooperation," *J. Theor. Biol.*, vol. 349, pp. 50–56, May 2014.

[34] G. Ciccarelli and R. L. Cigno, "Collusion in peer-to-peer systems," *Comput. Netw.*, vol. 55, no. 15, pp. 3517–3532, Oct. 2011.

[35] A. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Open Distrib. Process.*, Nov. 2001, pp. 329–350.
[36] K. Lai, M. Feldman, I. Stoica, and J. Chuang, "Incentives for cooperation in peer-to-peer networks," in *Proc. Workshop Econ. Peer-Peer Syst.*, Jun. 2003, pp. 1243–1248.
[37] M. A. Nowak and K. Sigmund, "Evolution of indirect reciprocity," *Nature*, vol. 437, no. 7063, pp. 1291–1298, 2005.
[38] M. A. Nowak, "Five rules for the evolution of cooperation," *Science*, vol. 314, no. 5805, pp. 1560–1563, Dec. 2006.
[39] Y. Liu, J. Zhang, B. An, and S. Sen, "A practical robustness measure of incentive mechanisms," in *Proc. Int. Conf. Auto. Agents Multi-Agent Syst.*, May 2014, pp. 1379–1380.

KUN LU received the B.S. and M.S. degrees in computer science from the Dalian University of Technology, Dalian, China, in 2002 and 2005, respectively, where he is currently pursuing the Ph.D. degree in computer science. Since 2005, he has been a Lecturer with the School of Software, Dalian University of Technology. His main interests include distribute system and incentive mechanism.

SHIYU WANG received the B.S. degree in software engineering from the Dalian University of Technology in 2014, where he is currently pursuing the M.S. degree in software engineering. His interests are in evolutionary game dynamics, network theory, and trust.



GUANGHAI CUI is currently a Lecturer with the School of Information and Electrical Engineering, Ludong University, China. His current research interests mainly focus on network economics, including incentive mechanism design, application of evolutionary game theory on communication networks and security issues, performance evaluation, and social network analysis.

MINGCHU LI received the B.S. degree in mathematics from Jiangxi Normal University in 1983, the M.S. degree in applied science from the University of Science and Technology Beijing in 1989, and the Ph.D. degree in mathematics from the University of Toronto in 1997. He was an Associate Professor with the University of Science and Technology Beijing from 1989 to 1994. He was with Longview Solution Inc. and Compuware Inc. from 1997 to 2002, where he was involved in research and development on information security. In 2002, he was a Full Professor with the School of Software, Tianjin University. Since 2004, he has been with the School of Software Technology, Dalian University of Technology, as a Full Professor, Ph.D. Supervisor, and Vice Dean. His main research interests include theoretical computer science and cryptography.

HANNAN-BIN-LIAQAT received the B.S. degree in information technology from the COMSATS Institute of Information Technology, Lahore, Pakistan, in 2006, the M.S. degree in computer networks from the COMSATS Institute of Information Technology in 2009, and the Ph.D. degree from the Dalian University of Technology, Dalian, China, in 2016. From 2009 to 2011, he was a Lecturer with the Computer Science Department, University of Gujrat, Gujrat, Pakistan. He is currently with the Department of Information Technology, University of Gujrat, as an Assistant Professor, Ph.D., and M.Phil. Supervisor.

Dr. Hannan has a number of publications to his credits in international journals and conferences. He is the Reviewer of several international journals. His research interests include ad hoc social networks, IoT, cloud computing, mobile computing, and social computing.