Peer-to-Peer Netw. Appl. (2016) 9:599–612
DOI 10.1007/s12083-015-0416-1

# An Eigentrust dynamic evolutionary model in P2P file-sharing systems

**Kun Lu**[1] · **Junlong Wang**[1] · **Mingchu Li**[1]

Received: 6 April 2015 / Accepted: 9 October 2015 / Published online: 2 November 2015


**Abstract** Many reputation systems have been proposed to distinguish malicious peers and to ensure the quality of the service in P2P file sharing systems. Most of those reputation systems implicitly assumed that normal peers are always altruistic and provide their resources unconditionally when requested. However, as independent decision makers in real networks, peers can be completely altruistic (always cooperative, ALLC), purely selfish (always defective, ALLD), or reciprocal (R). In addition, those systems do not provide an effective method to reduce free-riders in P2P networks. To address these two problems, in this paper, we propose an EigenTrust evolutionary game model based on the renowned EigenTrust reputation model. In our model, we use evolutionary game theory to model strategic peers and their transaction behaviors, which is close to the realistic scenario. Many experiments have been designed and performed to study the evolution of strategies and the emergence of cooperation under our proposed EigenTrust evolutionary model. The simulation results showed that rational users are inclined to cooperate (enthusiastically provide resources to other peers) even under some conditions in which malicious peers try to destroy the system.

**Keywords** Evolutionary dynamics · EigenTrust · Malicious attacks · P2P file-sharing · Free-rider

✉ Mingchu Li
mingchul@dlut.edu.cn

Kun Lu
lukun@dlut.edu.cn

[1] Dalian University of Technology, Dalian, Liaoning Province, China

## 1 Introduction

Peer-to-Peer (P2P) networks have developed rapidly in the past few years, as many excellent application systems, such as Napster [1], Gnutella [2], KaZaA [3], and BitTorrent [4] have emerged. However, these networks can incur some serious problems because of their decentralized character. Scholars have claimed that P2P networks are vulnerable to attacks because malicious peers constantly harm the performance of the system or, even worse, they destroy the entire system. Some common types of familiar attacks are sybil [5], collusion [6], camouflage [7], white washing [8], and virus spreading [9]. Typical examples of spiteful actions are uploading fake resources, intercepting resources, or becoming fraudulent after a long time as a legitimate user, and camouflage of good roles for a long time.

Many reputation systems [10], such as eBay [14], ePinions [15], PeerTrust [16], Powertrust [17], and EigenTrust [7], have been proposed to defend against malicious peers. Those mechanisms calculate the reputation value of a particular peer according to her/his prior transaction history, which is visible to all other peers. Based on this, each peer can request and obtain resources from other peers with high reputation values, thereby avoiding attacks performed by malicious peers. Experience [7] has shown that reputation systems can distinguish and isolate malicious peers from the normal peers to some degree. Even so, reputation systems have some obvious disadvantages. First, most previously-proposed, reputation-based trust models simply classify peers as normal peers or malicious peers, and the normal peers are assumed to be altruistic with respect to the provision of resources when they are requested. However, in realistic scenarios, as independent decision makers, besides of being completely altruistic (always cooperative: ALLC) and purely selfish (always defective, these peers

expect to use the resources of other peers without contributing to the network: ALLD), they might also be reciprocal (decide whether or not to provide/cooperate according to the requester's transaction history, e.g., a reciprocator will always grant a service to an ALLC peer and deny serving an ALLD peer: R). That is to say, normal peers are rational and strategic. Second, those schemes always assume that the behaviors of normal peers are invariable. But as rational peers, to maximize their payoffs, they may change their strategies occasionally by imitating or learning the strategies of other peers with higher payoff. In addition, free-riders also cause serious problems in P2P file sharing systems. Studies have shown that almost 70 % of Gnutella users are free-riders [13], which can severely harm the interests of other peers and reduce the utility of the entire network. Although the proposed reputation-based trust systems can effectively discriminate malicious peers and isolate them from the network, unfortunately, they failed to provide effective methods to solve the free-riding problem.

In this paper, we present a thorough study of a most successful EigenTrust model and propose an EigenTrust evolutionary model based on evolutionary game theory. The proposed model offers three important properties, i.e., (1) Peers have natural instincts to be strategic as in realistic scenarios. To better depict the behaviors of the peers, we assumed that peers are strategic, and they are classified into four types in our model, i.e., cooperative peers, reciprocal peers, defective peers, and malicious peers. (2) Peers are rational to increase their utility, and they use a simple learning method to optimize their strategies (e.g., imitate or learn others' strategies with higher payoff). At the same time, the learning ability can provide incentives for selfish peers to contribute to the network. Thus, the EigenTrust evolutionary model can isolate the malicious peers and simultaneously solve the free-riding issue. (3) Evolutionary dynamics considers the mutation factor in the design to investigate its effect on the evolution process. Mutation can be interpreted intuitively as curiosity (or mistake) probability when peers imitate others' strategies.

Many experiments have been designed and performed to study the evolution of strategies and the emergence of cooperation under our proposed EigenTrust evolutionary model. The simulation results showed that, after a certain time, peers are inclined to cooperate (enthusiastically provide resources to other peers), and the whole system is driven into an almost full cooperation state.

The rest of this paper is organized as follows. Related work is presented in Section 2. The EigenTrust algorithm is reviewed in Section 3. Our model is presented in Section 4, and the simulation experiments and the analysis of the results are presented in Section 5. Our conclusions and future work are presented in Section 6.

## 2 Related work

Reputation systems contain the peers' reputation values obtained through the evaluation by adjacent peers based on the records of their transaction history. Many reputation systems have been proposed to restrain malicious attacks. Paul Resnick investigated the trust among strangers in eBay's reputation system [12], wherein the feedback dataset for the last six months contained more than 20 gigabytes, which is difficult for a centralized authority to maintain. J$\phi$sang and Ismail proposed a beta reputation system [11], which is implemented in a centralized way, for peers in e-commerce to build trust. In the EigenTrust reputation management system [7], each peer is assigned a global reputation score that corresponds to the information that he/she has uploaded historically, and the advantage is that both storage and time complexity are low. PeerTrust is another distributed, reputation-based, trust-supporting framework that uses three basic trust parameters, i.e., feedback, total transaction number, and the credibility of the feedback sources, and two adaptive factors, i.e., transaction context factor and community context factor, when computing the trustworthiness of peers. PowerTrust [17] is a robust and scalable P2P reputation system based on the power-law feedback characteristics on eBay. PowerTrust is adaptable to the dynamics associated with peers' joining and leaving, including preventing malicious peers from joining the network. However, these methods did not consider the dynamic and evolutionary features of networks. Therefore, they cannot stimulate peers' cooperation dynamically.

Considering the rational and strategic features of peers, game theory is an appropriate tool to model and analyze their behaviors when conflicts occur between an individual's interests and the overall public benefit [18]. Generally, scholars use classical game theory to study the behaviors of peers in P2P systems [19–23]. Ma [19] proposed a framework based on game theory and discussed its Nash Equilibrium. In [21], the authors proposed a reputation framework and designed a game based on the reputation system, wherein the level of the provider's cooperation and the ranking of the requester's reputation depend on whether the provider agrees to share her/his file with the requester. The game is organized into rounds in which peers request files from each other. At the end of each round, peers compare their success rate with a threshold value. If the rate is above the threshold, the requester reduces the cooperation level; otherwise, he/she increases the cooperation level to improve her/his reputation, which can ensure better service. Another study [23] proposed a new dilemma based on the Rock-Scissors-Paper (RSP) game to simulate the P2P network.

Game theory can depict peers' behaviors more accurately, while the evolutionary game can reflect the evolutionary dynamic character of the peers. Nowak used evolutionary dynamics to study the importance of reciprocity in human society [24]. He conducted a multi-group evolution of simulation and analysis and ultimately concluded that the emergence of indirect reciprocity was a decisive step in the development of human society.

Other authors [25] have used the evolutionary game to model the selfish routing behaviors of peers in P2P networks. Li et al. assumed that the agents in a P2P system are rational [26] when studying the evolution of P2P networks. Another application of evolutionary dynamics in research was illustrated in study [27], in which a model was applied to master-worker computing.

## 3 EigenTrust

The EigenTrust reputation management system aims to isolate malicious peers in P2P file-sharing networks by asking them to use global trust values (also called reputation values). It provides a distributed and secure way to compute the reputation values of the peers in the network. Here, we introduce the EigenTrust algorithm briefly. The details of the system can be seen in [7].

### 3.1 Local trust

A requester $i$ can store the number of satisfied and unsatisfactory transactions/downloads that he/she has performed with another peer $j$, indicated as *sat(i,j)* and *unsat(i,j)*, respectively. Then the local trust value $s_{ij}$ can be defined as:

$$s_{ij} = sat(i, j) - unsat(i, j). \tag{1}$$

### 3.2 Normalized local trust values

After a certain number of transactions, the normalized local trust value from peer $i$ to peer $j$ can be defined as:

$$c_{ij} = \begin{cases} \frac{max(s_{ij},0)}{\sum_j max(s_{ij},0)} & , if \sum_j max(s_{ij}, 0) \neq 0 \\ p_j & , \text{otherwise.} \end{cases} \tag{2}$$

Assume that some sets of peers $P$ are known to be pre-trusted, such as the network's founders. Define $p_i = 1/|P|$ if $i \in P$, otherwise $p_i = 0$. The value $p_j$ represents peer $i's$ trust in peer $j$ with a value of $p_j$ if $j$ is a pre-trusted peer. The above formula ensures that all values are between 0 and 1. In this way, peer $i$ can develop a normalized trust in peer $j$.

### 3.3 Iteration

EigenTrust uses iteration to compute the trust value. Let $t_{ik}$ denote peer $i's$ trust towards peer $k$ by asking $i's$ friends, and the mathematical expression is as follows:

$$t_{ik} = \sum_j c_{ij} c_{jk} \tag{3}$$

Let $C$ be the matrix $[c_{ij}]$ and $\mathbf{t}$ be the vector that contains $t_{ik}$, then $\mathbf{t} = (C^T)\mathbf{c_i}$. To broaden her/his horizons, peer $i$ wants to ask the friends of her/his friends ($\mathbf{t} = (C^T)^2 \cdot \mathbf{c_i}$), and, after continuous iterations ($\mathbf{t} = (C^T)^n \cdot \mathbf{c_i}$), $i$ will be able to know the reputation of the entire network. If $n$ is large enough, the trust vector $\mathbf{t}$ will converge to the same vector for all peers. That is, it will converge to the principal right eigenvector of $C$. In other words, $\mathbf{t}$ is the desired global trust vector.

To address malicious attacks, EigenTrust lets $\mathbf{t}^{(k+1)} = (1-a)C^T\mathbf{t}^{(k)} + a\mathbf{p}$, where $a$ is a constant less than 1 and $\mathbf{p}$ is the pre-trust vector that contains $p_i$.

### 3.4 Interaction among peers

The interactions among peers are divided into rounds with a fixed number of requests per round issued randomly by the peers. In each round, peers act as follows:

1) Peer $i$ issues a request, and then he/she will obtain responses after the owners receive this request and respond to peer $i$;
2) Peer $i$ sorts the responses from the peers in a descending order of global trust values (EigenTrust scores);
3) Peer $i$ selects a file owner $j$ using the roulette algorithm (with a possibility of $s_j/\sum_{j=1}^{|X|} s_j$), where $|X|$ is the number of file owners, and $s_j$ is the EigenTrust score of peer $j$) with a probability of 90 %; peer $i$ selects an owner $j$ who has an EigenTrust score of 0 with a probability of 10 %;
4) After each downloading from $j$ in round t, $i$ assesses this transaction and provides feedback;
5) At the end of each round, all the peers in the network participate to compute their EigenTrust scores and move to the next round, until right up to the end.

## 4 Our EigenTrust evolutionary model

Here, we consider a game model in the P2P file-sharing scenario, in which each peer can act as a requester and provider simultaneously. In most previous reputation systems, file owners are assumed to offer their files selflessly when requested. However, in realistic situations, a file owner can

decide whether to offer her/his file depending on her/his current strategy. In our model, we considered this characteristic and investigated it from the evolutionary dynamics perspective. To clearly differentiate the provider from the file owner, we declared that a provider is a file owner who provides her/his file to the requester. A requester obtains a benefit value $b$ after downloading a desired file, thereby incurring a cost of $c$ to the provider. We divide the interactions among peers into discrete generations divided into several rounds. In each round, randomly-chosen peers issue a fixed number of file requests (e.g., 50). At the end of each round, the peers compute their reputation scores, and, at the end of a generation, each of them learns or imitates the strategies from other peers. Here, reputation scores have a two-fold effect. Reputation values can help the requester choose a more credible file provider, while the provider can decide whether he/she should provide her/his file or reject this downloading request based on the reputation score of the requester. The details of our model are provided below.

### 4.1 Peer classification

We regard the peers as strategic. In game theory, free-riders can be considered as non-cooperative peers or defective peers. However, some peers are generally very interested in providing services, so their image and status are good and their reputation scores are high. These peers can be considered cooperative. In addition, it is reasonable that some peers are reluctant to provide their resources to other peers, so these peers can be considered as reciprocal. In addition, inevitably, there are malicious peers in P2P networks whose purpose is to reduce the performance of the application system or even destroy the system entirely.

Based on the above analysis, the peer types in our model are classified in Table 1.

A peer with the strategy of ALLC always provides files to others, while a peer with the strategy of ALLD never provides files to others; a peer with the strategy of R provides files discriminately. Note that, in spite of the malicious peers' providing a large number of untrusted files, their strategies are assumed to be ALLC all the time because of their "cooperative" character.

**Table 1** Peer classification

| Type | Cooperator | Defector | Reciprocator | Attacker |
|---|---|---|---|---|
| Strategy | ALLC | ALLD | R | ALLC |

### 4.2 Cost, payoff, and utility

The game in our model is considered to be a stochastic repeat game in which every peer can be a requester. One peer at a time is chosen randomly as a requester. Thus, in each round, peer $i$ may issue 0 or $n$ ($n > 0$) requests. In the simulation work, we set the size of a round as 50, so we had $0 \leq n \leq 50$.

Suppose that the benefit of obtaining each file is a fixed value, $b$, and that the cost of sending a file is $c$. A requester $i$ must decide from which owner to download the file after he/she gets a response list. If peer $i$ chooses owner $j$ to download the file, it cannot be downloaded immediately unless peer $j$ has decided to give the file to peer $i$. If peer $j$ denies the transmission request, peer $i$ will select the file from owner $k$ until he/she downloads the file or until no available owner is left on the response list.

Utility is a very important concept in evolutionary game theory. A generalized opinion is that one with more utility will generate more offspring, thus becoming more adaptive among the population. In one-off settings, game players may request or serve only once, hence the utility may be equal to the difference between the payoff and the cost. However, in the other settings, the case may be a little complex. Assume that in round $t$, player $i$ requests $m$ times and provides $n$ times, then the total utility of player $i$ in round $t$ is defined as:

$$u_i^t = m \cdot b - n \cdot c \tag{4}$$

### 4.3 Discussion of the R strategy

We have already addressed the three strategies in Section 4.1. However, some concerns about strategy R may not be very clear. Hence, we discuss the specific issues of R in the section. To an owner of an R strategy, the probability of sending the file is:

$$p = \begin{cases} 1 \ , if \ c_r \in C_p \\ 0 \ , \text{otherwise.} \end{cases} \tag{5}$$

where $c_r$ represents the condition that reflects the EigenTrust score and/or the contribution level, and $C_p$ is the condition set that contains all of the conditions. As long as the requester satisfies one of these conditions, the owner will permit the requester to download the file.

#### *4.3.1 The simple strategy of reciprocal peers*

Consider the strategy of reciprocal peers mentioned above. In a simple scenario, strategy R is only to provide files to peers whose reputations are higher than R's peers.

**Table 2** Results of 100 runs of our model

| Strategy | Times |
|---|---|
| ALLD | 18 |
| ALLC | 76 |
| R | 6 |

The experimental results show that the evolution reaches a stable state after 200 generations (only a certain strategy left), and, in most cases, the ALLD peers are eliminated in the process of evolution. We ran our model 100 times, and Table 2 compares the times of evolving into one of three strategies in the absence of malicious peers.

Table 2 shows that a certain strategy will dominate. In this case, strategy ALLC makes up 76 % of the 100 runs. But this is not the desired result, because there is a probability that 18 % of all of the cases will reflect strategy D, which is not the true steady state.

*4.3.2 The modified strategy of reciprocal peers*

From the analysis of the simple strategy of reciprocal peers, we can derive that the results of this strategy are unfavorable to the overall performance of the system. In order to improve those negative results, we need to release the restrictions on having R peers provide services to other peers. From the definition, ALLC peers always upload authentic files when requested. However, R peers may be reluctant to cooperate with the ALLD peers, resulting in their having a lower EigenTrust score than the ALLC peers. So, under the mechanism of the simple strategy of R peers, R's strategy is inferior to ALLC's strategy, and it can be dominated by ALLC's strategy in the evolutionary process. A feasible adjustment scheme can be described by considering the reputation via EigenTrust scores of each peers and also the contribution of the peer. The contribution here is defined as the ratio of upload times to request times. (Note that, if the number of requests is 0, the contribution rate is defined as 0.) If a peer contributes more to the system, he/she can obtain more from others. This releases the restriction of an R peer, allowing her or him to obtain files from other R peers. But, since ALLD peers never provide files, their contribution is 0, and they do not have the opportunity of obtaining files from R peers. Thus, we give the following modified version.

Assuming the EigenTrust score of peer $i$ is expressed as $eig_i$, peer $j's$ EigenTrust score is $eig_j$; similarly, and the contribution rate of $i$ is denoted as $con_i$, the contribution rate of j is $con_j$. Further, we assume that R peers provide others with service under the following conditions:

Cond 1: $eig_i \geq eig_j$
Cond 2: $con_i \geq con_j$.

To further relax the limitation, peer $j$ with strategy R provides files to a requester $i$ with a probability of 10 % if $i$ satisfies neither of the conditions. Otherwise, $i$ will not obtain the desired file from $j$. Table 3 provides a summary of the condition space ($C_p$) of R.

Hence, in Section 5, we used the modified R strategy to conduct our simulation experiments and analyse the robustness of our model.

### 4.4 Learning model

In the evolutionary process, peers will learn another peer's strategy with a certain probability at the end of each generation. It makes sense that the correlation between the learning possibility and the utility difference of two peers is positive. Peer $i$ can use the strategy of peer $j$ with a probability determined by the Fermi function [28–31], which is presented by the following formula:

$$p_{i\to j} = \frac{1}{1 + e^{(u_i - u_j)/k}} \tag{6}$$

where $p_{i\to j}$ is the probability of peer $i$ learning from peer $j$ in a generation, $u_i - u_j$ is the utility difference between $i$ and $j$, and $k$ is a regulatory factor. In the simulation work, we set $k = 0.1$, implying that a peer prefers to use the strategy of a peer that has a significantly higher utility than her/him. Also, we assumed that each rational peer would select another rational peer randomly to learn her/his strategy with a probability of $p_{i\to j}$. We used a synchronized learning style in our simulation work.

### 4.5 Mechanisms of the algorithm

To clarify our model, we provided a detailed description of the algorithm. For requester $i$, it performs as the requesting algorithm (Algorithm 1), while it performs as the providing algorithm (Algorithm 2) for every owner $j$; each of the rational peers performs the same learning algorithm

**Table 3** Condition space of R

| Condition | Service probability |
|---|---|
| Cond1 | 100 % |
| Cond2 | 100 % |
| Otherwise | 10 % |

(Algorithm 3) at the end of each generation. Algorithm 4 is the evolutionary algorithm used in our simulation work.

**Algorithm 1** Requesting Algorithm

```
issue a request: Request(R_i, f_α) // f_α: a file
receive a response list RL {O_1, O_2, ..., O_n}
sort O_i in RL by EigenTrust score
while have not gotten a valid file do
    choose a O_j using roulette alg
    if O_j will provide her/his file then
        download
        feedback
        update utility
    else
        delete O_j from RL and choose O_k
    end if
end while
if reach the end of a round then
    compute EigenTrust scores
end if
if reach the end of a generation then
    execute alg3
end if
```

**Algorithm 2** Providing Algorithm

```
receive a request from a requester R_i
reply a response: Request(O_j, f_α)
sort O_i in RL by EigenTrust score
if receive a download request then
    if C_{R_i} ∈ C_p then
        provide the file with R_i
        update utility
    else
        deny the request
    end if
end if
if reach the end of a round then
    compute EigenTrust scores
end if
if reach the end of a generation then
    execute alg3
end if
```

**Algorithm 3** Learning Algorithm

```
for i = 1 to N do
    temp strategy ← strategy of P_i
    P_i select a learning target P_j randomly
    P_i learns strategy of P_j with a probability of p_{i→j}
    if P_i will change her/his strategy then
        temp strategy ← strategy of P_j
    end if
end for
for i = 1 to N do
    strategy of P_i ← temp strategy
end for
```

**Algorithm 4** Evolution Algorithm

```
for i = 1 to 200 do
    for j = 1 to 1000 do
        for k = 1 to 50 do
            requester performs alg1
            owners performs alg2
        end for
        compute EigenTrust scores
    end for
    every rational peer performs alg3
end for
```

## 5 Simulations

### 5.1 Simulation parameters

The graphs show the data for the simulation results. We focused on the metric of the emergency of cooperation and the proportion of each strategy, which can represent the ratio of each kind of peer. We also depicted inauthentic downloading to compare it with EigenTrust and another reputation system called PETS (Personalized EigenTrust using Social network) [33]. Table 4 provides the simulation parameters we used here.

### 5.2 Performance of our model

The results of our experiments showed that the modified strategy of R peers can yield good results even in the presence of malicious attacks. Because individual malicious peers and malicious collectives yield similar results, we mainly focused on individual malicious peers in this paper.

We assumed that every peer gets the same payoff of 1.0 when he/she downloads an authentic file. In other words, all satisfactory downloads have the same value. Each peer provides a file with the same cost of 0.1. Also we assumed that if the downloaded file is inauthentic, then the benefit the requester got is 0 while the cost of the provider is 0.1. To avoid negative values, we added a benefit value of 0.1 to the interacting parties after every interaction. The simulations showed that, after 200 generations, the network can reach a steady state. We conducted two groups of experiments, i.e., experiments with and without mutations.

#### *5.2.1 Evolution results without mutations*

Figure 1 describes the status of time-varying rational evolution of the three types of peers. The ordinate represents the number of rational peers in the network.

**Table 4** Configuration of the simulation parameters

| Category | Parameter | Value |
|---|---|---|
| Network Structure | No. of good peers | 60 |
| | No. of pre-trusted peers | 3 |
| | No. of initial neighbors of good peers | 2 |
| | No. of initial neighbors of malicious peers | 10 |
| | No. of initial neighbors of pre-trusted peers | 10 |
| | query hops | 7 |
| File distribution | file distribution at good peers | 20 file, Zipf distribution |
| | No. of distinct files at rational peers | uniform random distribution |
| | top % of queries for most popular files malicious peers response to | 20 % |
| | top % of queries for most popular files pre-trusted peers response to | 5 % |
| Peer behaviour | % of download request in which rational peers return bad file | 5 % |
| | download source selection algorithm | roulette algorithm |
| | probability of 0 reputation peers are selected as download source | 10 % |

Figure 1a–h show that the proportion of the three types of rational peers in the initial condition is the same (1/3). However, only the ALLC peers survive with the evolution of the network. The relationship between the result of the evolution and the proportion of malicious peers was not significant. Subsequently, we conducted qualitative analyses.

ALLD peers who never provide services have a reputation value of 0. Therefore, they could obtain service only from ALLC peers. Thus, a large percentage of the ALLD peers benefited less than the other two types of peers at the end of a generation, which eventually leads to the elimination of the ALLD peers.

Because the R peers' strategy is to provide services under certain conditions, they consider both the reputation and extent of the contributions of the requester; therefore, unlike considering only the reputation of the requester, this can reduce the misjudgment rate and improve the degree of the rationality of R peers, thereby increasing the probability of providing services to other R peers. Assume that both a peer $i$ of ALLC and a peer $j$ of R issue a request to another R peer $k$. Because the possibility of reputation of ALLC peers is higher than that of R peers (because ALLC peers provide more service than R peers), then $i$ should have a greater probability of obtaining the file from $k$. In this way, the ALLC peers can obtain more benefit, on average, than the R peers; thus, in the process of evolution, the three types of rational peers will gradually evolve into ALLC peers.

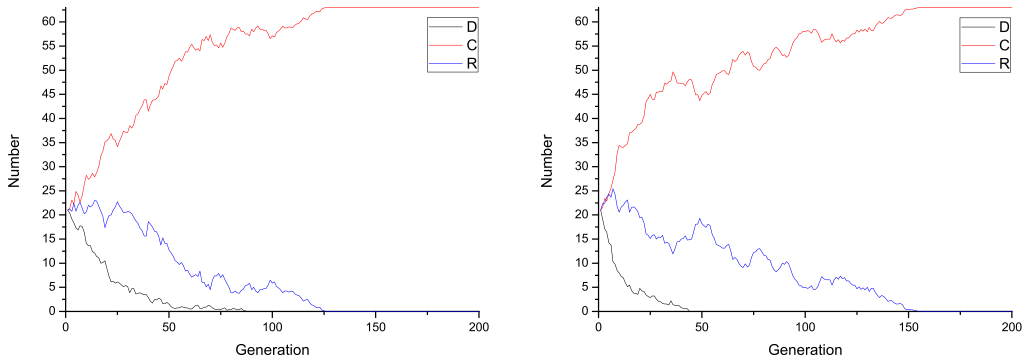
Obviously, malicious peers have no significant influence on the results of the evolution. This is mainly due to the EigenTrust reputation system, since peers select a non-reputable peer with a very low probability, while the malicious peers' reputations are always 0 in attack model of individual malicious peers [7]. Therefore, in our model, the malicious peers also will be inhibited because the existence of malicious peers will not have much influence on the evolution of the results.

Our evolutionary model can facilitate the emergence of a large scale of cooperation in the P2P file-sharing network in spite of the bad initial scenario in which more than 50 % of the peers were reluctant to cooperate, which indicates the effectiveness of our proposed model. Compared with other well-known reputation systems, such as EigenTrust [7], PeerTrust [16], PowerTrust [17], the Beta Reputation System [11], and CuboidTrust [32], the latter of which takes peers' contributions into account, our model emphasizes the evolutionary dynamic characters of the strategies of the peers in the network. In addition, our model promotes cooperation among peers, which is vital in addressing the free-riding issue. Later, we provide additional information concerning the inhibition of free-riding by comparing the inauthentic downloads of the three reputation systems.

#### *5.2.2 Evolution results with mutation added*

The major factors that influence the evolution of the population generally are considered to be selection and mutation. The preceding section discusses the experiments that were conducted without mutation. This section discusses the scenario with mutation. Simulations have shown that adding a small amount of mutations only produces a small influence on performance, even if there are many malicious peers.We present results of 0 % to 50 % malicious peers participant in the system, with the condition of 1 % mutation rate (Fig. 2).

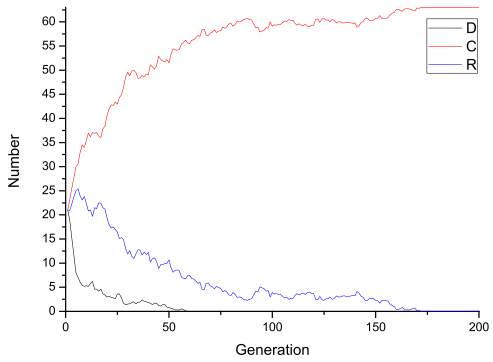
The results show that ALLC strategy dominate in the evolution even there are 50 % malicious peers. This is mainly because the rational peers always select a peer with high reputation. While the reputation of malicious peers in



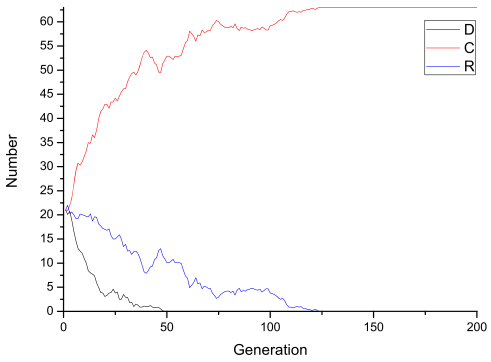

(a) 0% malicious peers



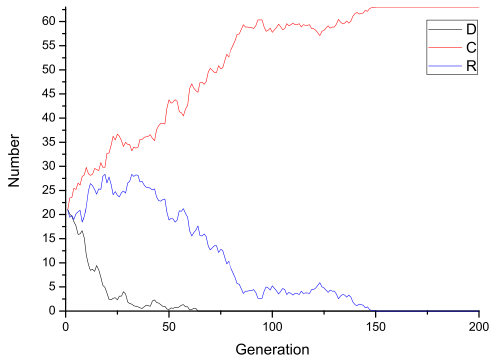

(b) 10% malicious peers



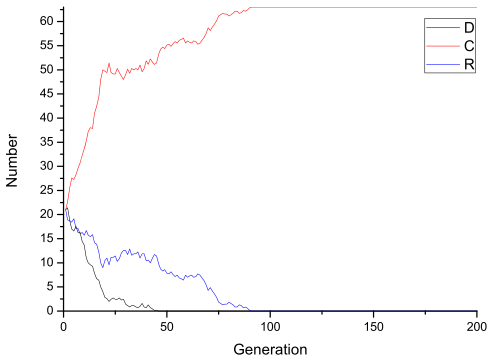

(c) 20% malicious peers



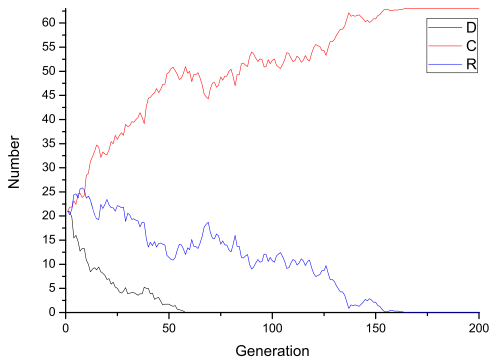

(d) 30% malicious peers



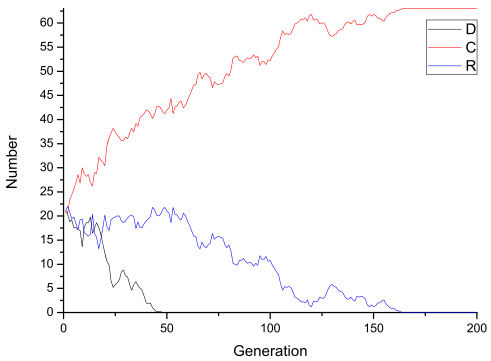

(e) 40% malicious peers




(f) 50% malicious peers

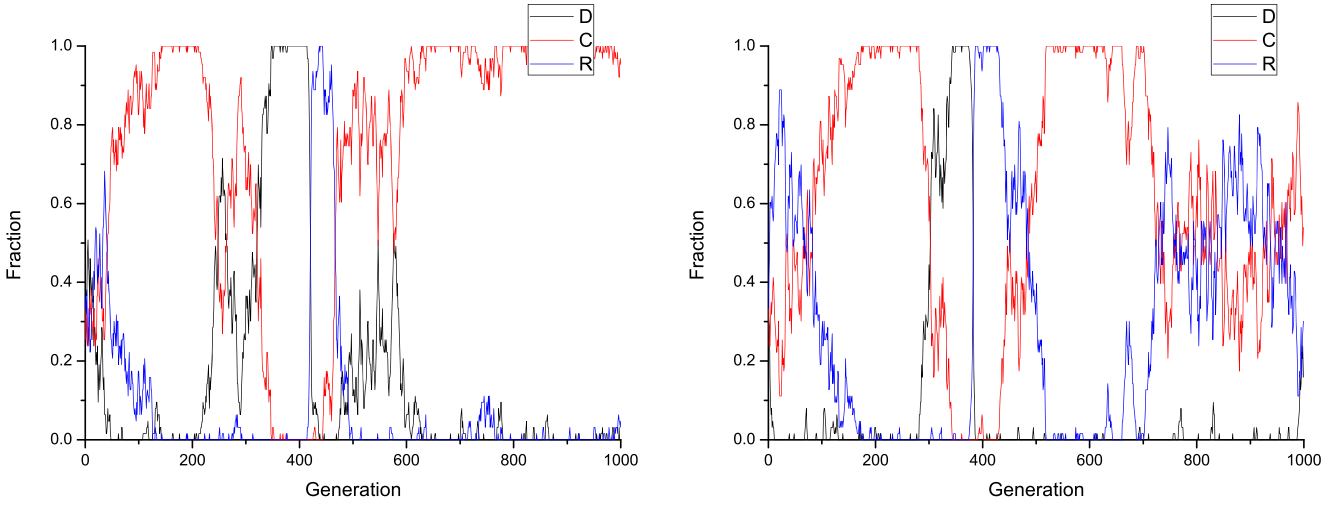



(g) 60% malicious peers




(h) 70% malicious peers

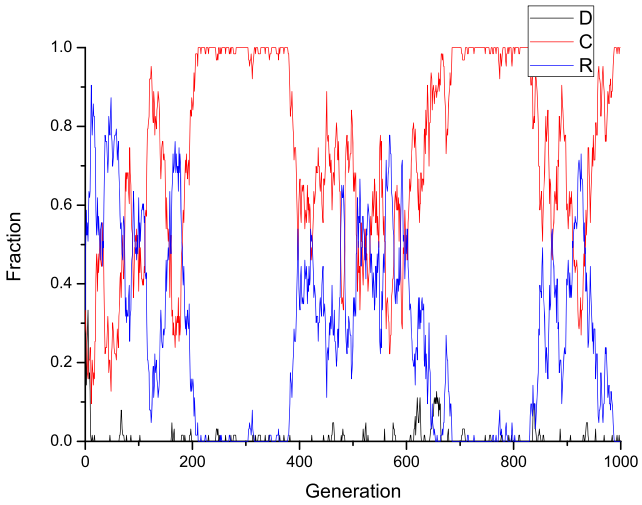
**Fig. 1** Proportion of three kinds of peers under different proportion of malicious peers



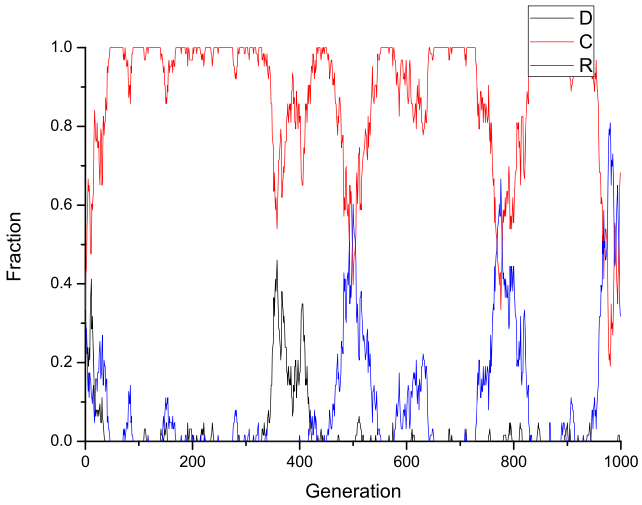

(a) 0% malicious peers



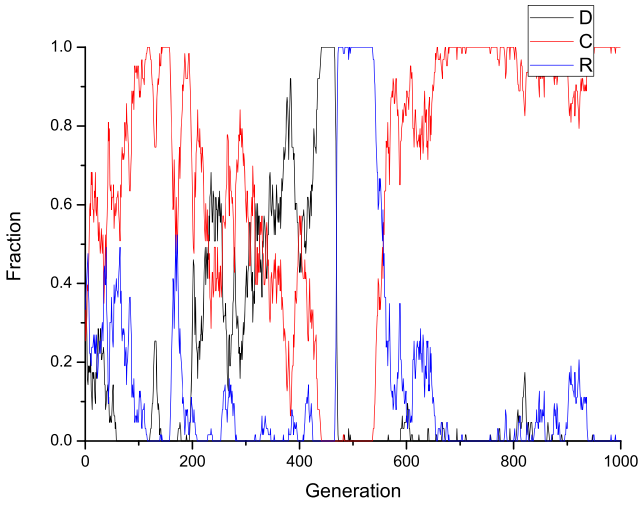

(b) 10% malicious peers



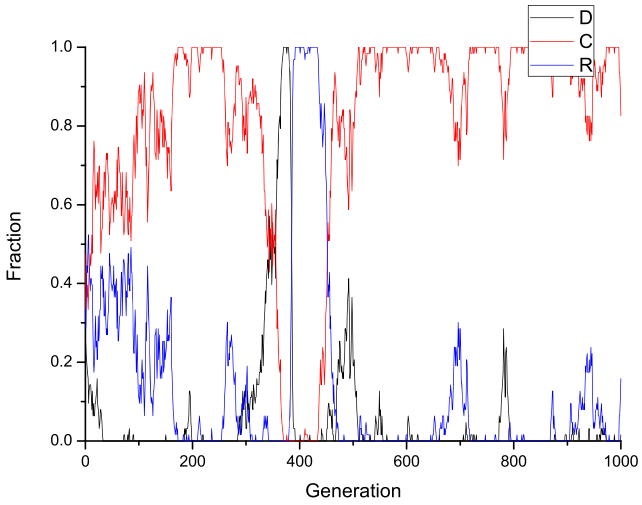

(c) 20% malicious peers




(d) 30% malicious peers




(e) 40% malicious peers




(f) 50% malicious peers

**Fig. 2** The evolution results of 1 % mutation rate with 0–50 % malicious peers in the network

the network is always 0, the rational peers choose an ALLC and R peers more often. So the simulation results show the increase of malicious peers did not have a significant effect on the whole system.

We also want to investigate the impact of mutation rate on the evolution process. This paper considers two scenarios, i.e., 0 and 50 % of malicious peers in the network. Charts (a)–(d) in Figs. 3 and 4 both show a significant increase in fluctuation with time. In the end of every generation, each rational peer has the same probability (say, 5 %) to change into a stochastic strategy because of mutation character. The higher the mutation rate, the more likely a rational peer change into the other two strategies takes place. In light of the discussion in Section 5.2.1, we can show that ALLD peers have an advantage over ALLC peers. Therefore the emergence of ALLD peers has an obvious impact on evolution, and with the increase of mutation rate, the fluctuation phenomenon is more obvious.

Figure 3 shows that the evolution of the network without malicious peers in the network. Charts (a)–(d) represent the scenarios under the mutation rates of 2–5 %, respectively. The number of generations was set at 1,000. The configurations of the other parameters are the same as in Table 4.

It is apparent that the rational peers in the network changed dynamically with time, while ALLD peers appear at a low frequency. In other words, ALLC and R peers are more dominant. Furthermore, as the mutation rate increased, the dynamic character became more apparent. When the network comprises almost all ALLC peers and only a small number of ALLD peers emerge because of mutation, ALLD peers increased rapidly, but, once some R peers emerged,

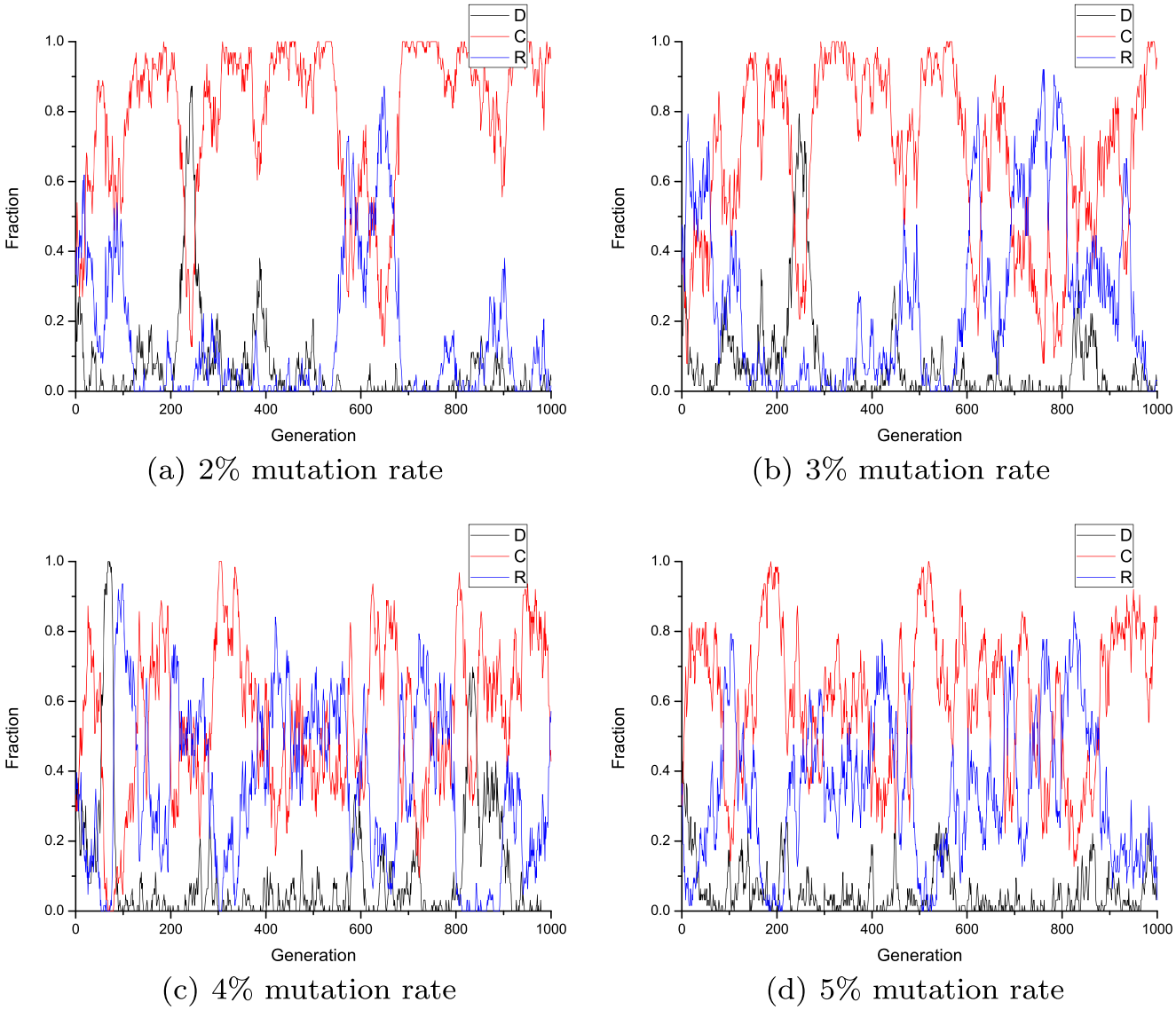



**Fig. 3** The evolution results of no malicious peers in the network

ALLD peers were eliminated quickly, and R peers became dominant. However, after the re-emergence of ALLC peers, the R peers became less dominant.

Since ALLC peers are purely cooperative, they enjoy the best reputation among the three types of rational peers. Consequently, they would be the most likely to obtain service when requesting a file, and, thus, at the end of the generation, the payoff of ALLC peers should be greater than that of R peers. Therefore, R peers will have a greater probability of changing into ALLC peers. Considering ALLC and ALLD peers, if ALLD peers appear in the system, they will always request files from ALLC peers (depending on the request service selection algorithm), while ALLC peers often provide files to others. Therefore, ALLD peers should benefit more than ALLC peers; hence, ALLC peers gradually will become ALLD peers. From R peers' strategy, we know that R peers would not share their files with ALLD peers, so, if the mutations result in R peers, ALLD peers will be eliminated, as shown in Fig. 3.

Figure 4 shows the evolution of the network when 50 % of the peers in the network are malicious. Compared with Fig. 3, the emergence of malicious peers (even 50 %) does not make a significant difference in the evolution of the network, that is, the evolution with mutation also could restrain the attacks of the isolated malicious peers. Because the analysis is similar with the scenarios in Section 5.2.1, so we omit the explanation here.

### *5.2.3 Inauthentic downloads*

One of the goals of the EigenTrust model was to decrease the inauthentic downloads of the network. To illustrate its

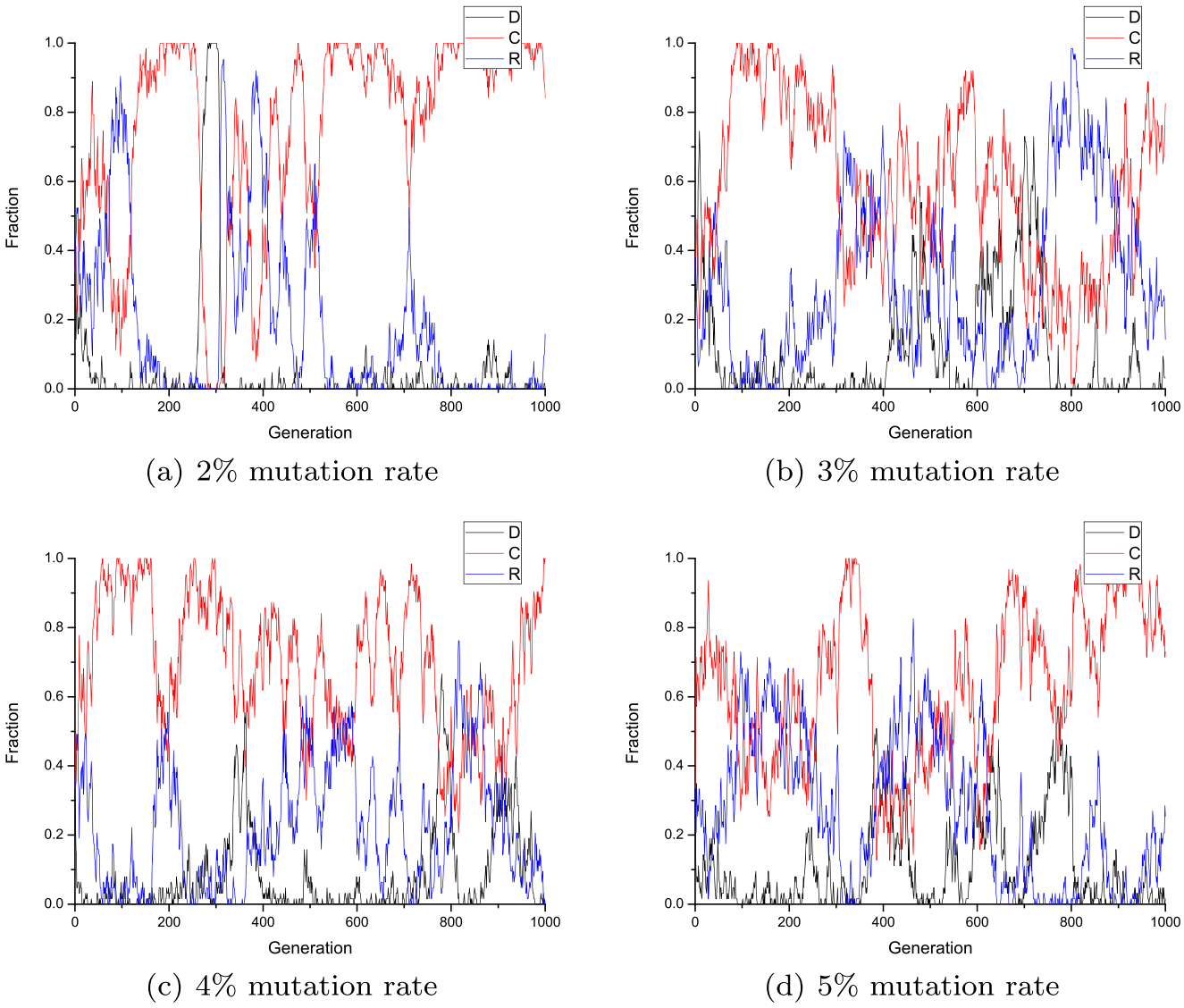



**Fig. 4** The evolution results with 50 % malicious peers in the network

effectiveness in doing so, we also counted the inauthentic downloads, but, due to the space limitation, we only present the situation in which 70 % of peers in the network are malicious.

Figure 5 shows that the inauthentic download rate is very high when malicious peers occupy 70 % of the network; this is due to the existence of large numbers of malicious peers and ALLD peers. During the evolution process, ALLC peers dominate the network; thus, the inauthentic download rate declines to about 10 %, which is similar to the simulation results of EigenTrust.

### *5.2.4 Free-riding issues*

It has been reported previously [17] that many free-riders exist in P2P networks, and this is a severe restraining factor to the further development of P2P. If there are many free-riders in the network, there would be less desired resources available, so more inauthentic files would be downloaded from untrusted peers, including malicious peers.

To illustrate the robustness of our model at weakening the effect of the free-riding behavior, we compared our model with the EigenTrust and PETS reputation systems by artificially adding some free-riders into the systems. Specifically, we set 1/3 of the normal peers in the EigenTrust model and PETS system to be ALLD peers (free-riders), while another 1/3 was designated as R peers with the rest being ALLC peers. Figure 6 shows the fraction of inauthentic downloads by the EigenTrust model, PETS, and our model depending on the percentage of malicious peers in the network. The data plotted in Fig. 6 for our model is based on the average download rate of inauthentic files by the last five generations.

Figure 6 shows that, as the percentage of malicious peers increased, the download rate of inauthentic files in the

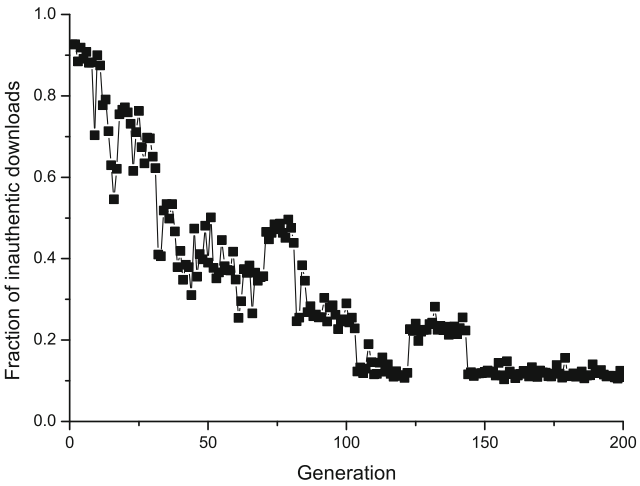



**Fig. 5** The evolution results of inauthentic download in the network

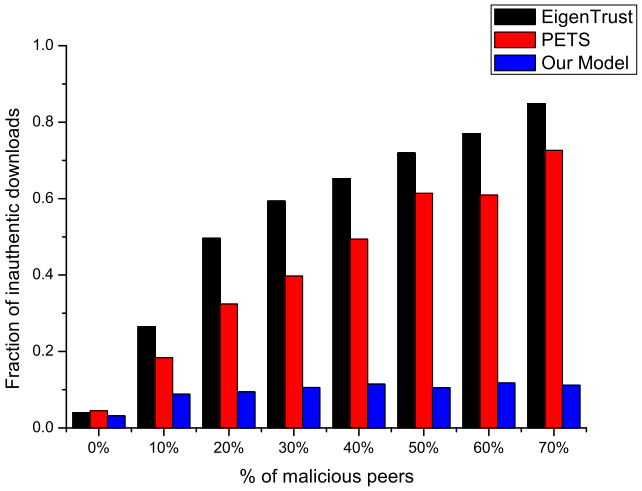



**Fig. 6** The evolution results of inauthentic download in the network

EigenTrust and PETS models increased to 85 % and 70 %, respectively, while our model limited the download rate of inauthentic files to about 10 %. The results of the EigenTrust and PETS models were caused mainly by free-riders. And peers in PETS can have a better judgment concerning other peers due to the personal perspective to the network by trusting her/his own pre-trusted peers. Therefore, PETS had a lower download rate of inauthentic files than EigenTrust. If only free-riders own some files and never share them with others, the requesters could obtain these files only from malicious peers, and such files are likely to be inauthentic. This phenomenon also indicates that (1) free-riders can have a serious effect on the performance of the system and (2) the EigenTrust and PETS models had no mechanisms for suppressing free-riders effectively, although Kamvar et al. [7] pointed out that incentives encourage peers to share resources and inhibit free-riding peers. Figure 6 shows that the inauthentic downloads were kept at a low level by our model, as was the case in the original simulations in the EigenTrust. The reason for this was that there are no free-riding peers when the evolution in in a stable status, so the downloads of inauthentic files were maintained at a low level, even when the number of malicious peers increased.

## 6 Conclusion

In this paper, we proposed an EigenTrust evolutionary model. We considered the non-malicious peers of the P2P network as bounded rational peers, namely cooperative peers, reciprocal peers, and defective peers, which was very close to the realistic scenario. In addition, these rational peers were strategic, and their strategies changed throughout the learning process. We also investigated the influence of

mutation on the evolutionary process. The simulation results showed that, after a certain period, the rational peers were inclined to cooperate; also, the system can resist some malicious attacks, which means our model effectively enhanced the performance of the system.

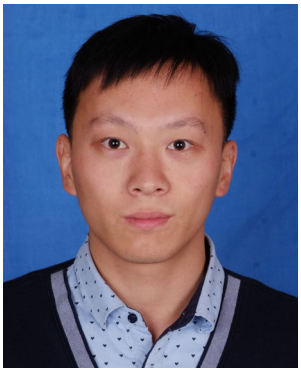
In future work, we will study other evolution parameters, such as different network structures and the dynamics of the network scale. Also, we may focus on different malicious attacks to investigate the robustness of our model, and we will strive to provide a more thorough evolutionary game framework.

**Acknowledgments** This work is supported by Nature Science Foundation of China (61272173, 61403059, 61572095).

## References


1. Napster. http://www.napster.com/
2. Gnutella. http://gnutella.wego.com/
3. KaZaA. http://www.kazaa.com/
4. BitTorrent. http://www.bittorrent.com/
5. Douceur JR (2002) The sybil attack. In: Peer-to-peer Systems. Springer, pp 251–260
6. Ciccarelli G, Cigno RL (2011) Collusion in peer-to-peer systems. Comput Netw 55(15):3517–3532
7. Kamvar SD, Schlosser MT, Garcia-Molina H (2003) The eigentrust algorithm for reputation management in p2p networks. In: Proceedings of the 12th international conference on World Wide Web 2003. ACM, pp 640–651
8. Feldman M, Papadimitriou C, Chuang J, Stoica I (2006) Free-riding and whitewashing in peer-to-peer systems. IEEE J Sel Areas Commun 24(5):1010–1019
9. Thommes R, Coates M (2005) Modeling virus propagation in peer-to-peer networks. In: 2005 Fifth International Conference on Information, Communications and Signal Processing 2005, IEEE, pp 981-985
10. Resnick P, Kuwabara K, Zeckhauser R, Friedman E (2000) Reputation systems. Commun ACM 43(12):45–48
11. Jsang A, Ismail R (2002) The beta reputation system. In: Proceedings of the 15th bled electronic commerce conference 2002, pp 2502–2511
12. Resnick P, Zeckhauser R (2002) Trust among strangers in internet transactions: empirical analysis of ebay's reputation system. The Economics of the Internet and E-commerce 11(2):23–25
13. Adar E, Huberman BA (2000) Free riding on Gnutella. First Monday 5(10)
14. eBay. http://www.ebay.com
15. ePinions. http://www.epinions.com
16. Xiong L, Liu L (2004) Peertrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans Knowl Data Eng 16(7):843–857
17. Zhou R, Hwang K (2007) Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans Parallel Distrib Syst 18(4):460–473
18. Cui G, Li M, Wang Z, Ren J, Jiao D, Ma J (2014) Analysis and evaluation of incentive mechanisms in P2P networks: a spatial evolutionary game theory perspective. Concurrency and Computation: Practice and Experience
19. Ma RT, Lee S, Lui J, Yau DK (2006) Incentive and service differentiation in P2P networks: a game theoretic approach. IEEE/ACM Trans Networking (TON) 14(5):978–991
20. Gupta R, Somani AK (2005) Game theory as a tool to strategize as well as predict peers' behavior in peer-to-peer networks. In: 11th International Conference on Parallel and Distributed Systems, 2005. Proceedings. IEEE, pp 244–249
21. Mortazavi B, Kesidis G (2006) Cumulative reputation systems for peer-to-peer content distribution. In: 2006 40th Annual Conference on Information Sciences and Systems. IEEE, pp 1546–1552
22. Buragohain C, Agrawal D, Suri S (2003) A game theoretic framework for incentives in P2P systems. arXiv:cs/0310039
23. Mejia M, Pea N, Muoz JL, Esparza O, Alzate MA (2011) A game theoretic trust model for on-line distributed evolution of cooperation inMANETs. J Netw Comput Appl 34(1):39–51
24. Nowak MA, Sigmund K (1998) Evolution of indirect reciprocity by image scoring. Nature 393(6685):573–577
25. Zuo F, Zhang W (2014) An Evolutionary Game-Based Mechanism for Routing P2P Network Flow among Selfish Peers. Journal of Networks 9(1):10–17
26. Li Y-M, Tan Y, De P (2013) Self-organized formation and evolution of peer-to-peer networks. INFORMS Journal on Computing 25(3):502–516
27. Christoforou E, Anta AF, Georgiou C, Mosteiro MA, Snchez A (2013) Applying the dynamics of evolution to achieve reliability in masterworker computing. Concurrency and Computation: Practice and Experience 25(17):2363–2380
28. Traulsen A, Nowak MA, Pacheco JM (2006) Stochastic dynamics of invasion and fixation. Phys Rev E 74(1):011909
29. Wang Z, Szolnoki A, Perc M (2012) Evolution of public cooperation on interdependent networks: The impact of biased utility functions. EPL (Europhysics Letters) 97(4):48001
30. Altrock PM, Traulsen A (2009) Deterministic evolutionary game dynamics in finite populations. Phys Rev E 80(1):011909
31. Gmez-Gardees J, Romance M, Criado R, Vilone D, Snchez A (2011) Evolutionary games defined at the network mesoscale: the public goods game. Chaos: An Interdisciplinary Journal of Nonlinear Science 21(1):016113
32. Chen R, Zhao X, Tang L, Hu J, Chen Z (2007) CuboidTrust: a global reputation-based trust model in peer-to-peer networks. In: Autonomic and Trusted Computing. Springer, pp 203–215
33. Chiluka N, Andrade N, Gkorou D, Pouwelse J (2012) Personalizing eigentrust in the face of communities and centrality attack. In: 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA) 2012. IEEE, pp 503–510


**Kun Lu** born in 1980, PhD Candidate. Lecture in the Dalian University of Technology. His main research interest include distribute system, incentive mechanism, reputation system.



**Junlong Wang** born in 1990, Master degree candidate in School of Software, DUT. His main research interests include trust and mechanism in P2P networks.

**Mingchu Li** born in 1963, Professor and PhD supervisor in Dalian University of Technology. His main research interests include theoretical computer science and cryptography.