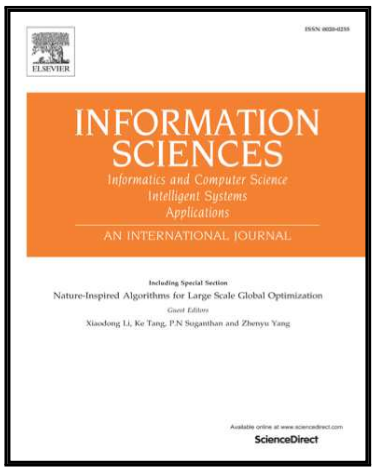


Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model

Morteza Babazadeh Shareh , Hamidreza Navidi ,
Hamid Haj Seyyed Javadi , Mehdi HosseinZadeh

PII: S0020-0255(18)30672-8
DOI: https://doi.org/10.1016/j.ins.2018.08.054
Reference: INS 13898

To appear in: *Information Sciences*

Received date: 29 December 2017
Revised date: 19 August 2018
Accepted date: 24 August 2018

Please cite this article as: Morteza Babazadeh Shareh , Hamidreza Navidi , Hamid Haj Seyyed Javadi , Mehdi HosseinZadeh , Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.08.054

Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model

Morteza Babazadeh Shareh[1], Hamidreza Navidi[2,*], Hamid Haj Seyyed Javadi[2], Mehdi HosseinZadeh[3, 4]

[1]Department of Computer, Science and Research Branch, Islamic Azad University, Tehran, Iran
[2]Department of Mathematics and Computer Sciences, Shahed University, Tehran, Iran
[3]Iran University of Medical Sciences, Tehran, Iran
[4]Computer Science, University of Human Department, Sulaimanieh, Iraq

Babazadeh@baboliau.ac.ir, Navidi@shahed.ac.ir, H.S.Javadi@shahed.ac.ir, Hosseinzadeh.M@iums.ac.ir

Corresponding Author: Hamidreza Navidi

Abstract

In cooperative Peer-to-Peer (P2P) networks, a number of users, called Free-riders, try to receive service from others without cooperating with them. Some others, called Sybil nodes, break the rules of the system by colluding and showing fake identities. P2P networks are highly vulnerable to these attacks. In previous research, no method has been suggested to counter these two attacks simultaneously. In the proposed method, a new centrality relationship has been used in the incentive mechanism to deal with both problems at the same time. In this regard, the more varied the nodes receiving service from a peer are, the better the peer reputation will be. The results show that the longer the network life goes on, the more Free-riders are detected, and the number of services delivered to the collusive nodes will also be reduced.

Keywords: Sybil Attacks, Evolutionary Game Model, Peer-to-Peer File Sharing, Free Rider

1. Introduction

Peer-to-Peer (P2P) networks are considered as an effective way to organize distributed systems, which allow a group of users to communicate with each other and share their resources. They are mainly built on a network like the Internet. Deploying networks such as CAN, (Content Addressable Network), Chord, Pastry and Tapestry on a large scale has enabled millions of nodes (users) to be able to share their data [32].

P2P architecture was a revolution in sharing large files on the Internet. This architecture provided the opportunity for each peer to contribute to both uploading and downloading files. This contribution is autonomous, and each user decides on which level to contribute. The success of a P2P file sharing system depends on the contribution of users [18].

The open and dynamic nature of P2P networks can be both useful and dangerous. Problems such as free-riders and malicious users can cause a lot of problems in the proper functioning of the system [8].

In this infrastructure, nodes provide or use resources. The nodes can request the service from others or provide a service for others. Each node acquires benefit by receiving the service and pays a price by providing it for other nodes. In this cooperative model, each node usually tries to receive the most service possible. Defectors, also known as Free-riders, are only looking to download their own resources among shared ones. They also avoid offering services to other nodes [37, 7].

The spread of such a phenomenon can be destructive. It might also reduce the value of file sharing in the network and further turn it into a sick network. According to a study conducted in 2005, 85% of Gnutella network users are free riders, and only 1% of the users share files and resources spontaneously [37].

Unfortunately, the P2P system does not have a central controller capable of monitoring user performance. Therefore, detection and prevention of malicious behaviors in this environment has become a major challenge. How to manage nodes and encourage them to cooperate is a fundamental issue in this open system. Trust and reputation techniques are the key ways to create collaborating behavior in P2P systems. Many solutions have so far been proposed based on these techniques, each with their own trust estimation, reputation dissemination and response to non-cooperative behavior methods [27].

In decentralized, distributed and uncontrolled systems, a user can pose a problem for the system by gaining and controlling a large number of IDs [38, 28]. This type of attack is called a Sybil attack and is known as a major threat to P2P systems. In this attack, a user with several fake identities exists on the network. Douceur [15] has proven that it is impossible to completely eliminate Sybil nodes, thus great efforts were made to minimize the malicious effects of the Sybil attack.

Much research has been done to identify free riders in P2P file sharing networks. Some of the most important papers in this area have been discussed in Section 2. In all these researches, a method has been proposed to detect the presence of a free rider in the network. After detecting the free riders, providing service for them can be stopped, or the quality of the service can be reduced. This will create an incentive for network users to cooperate. On the other hand, other papers focused on the identification of Sybil attacks. Some of these papers have been reviewed in Section 2. These researches focus on identifying users who are trying to violate the rules governing the network.

Accordingly, the main questions in this research that we are looking for include the following:

• How can we design a mechanism that can detect free riders in as well as confront Sybil attacks?

• How can a robust incentive mechanism be designed to help users cooperate with the network?

• What parameters affect the network users' incentive?

None of the previous methods simultaneously deal with Free riders and Sybil nodes. In this paper, a reputation-based approach is proposed that can identify these two types of malicious behaviors simultaneously.

The rest of the paper is organized as follows: Section 2 contains previous relevant work. Section 3 contains the system model. Section 4 describes the structure of the proposed incentive mechanism and information on how to calculate the centrality. In Section 5, simulation results of this game are presented. Section 6 reports on the conclusion drawn from this research.

2. Related Studies

This research focuses on detecting free riders and identifying Sybil attacks. Therefore, it is necessary to review previous methods in this area briefly. Given that all research worked either on the identification of a free rider or on confronting a Sybil attack, the two sets of methods are studied separately.

2.1. Detecting Free Riders

In order to avoid the selfish behavior of the defector nodes, there should be a mechanism to ensure the efficiency of a P2P network. The reputation mechanism [19, 43] generates a history of the activity of a node during the system lifetime.

Therefore, a node with the highest credit could be selected for the exchange of resources. In [31], the author uses an economic model and proposes a P2P framework based on the cooperative model.

However, in most papers, the incentive mechanism based on a cooperative or non-cooperative game model is used to solve such a problem. In some studies, the evolutionary game model has been used to analyze the incentive mechanism to cover the disadvantages of the classic game model [9, 35]. The present paper also uses an evolutionary game model to examine change in the behavior of users. It should be noted that this is not possible in the classic game model. The advantage of the evolutionary game model over the classic one is its focus on change in the user's strategy [35].

Chang et al. [8] designed a reputation-based incentive mechanism for P2P systems. This mechanism has two characteristics: (1) For each recommender, a trust value is considered in order to calculate the reputation more accurately and fairly. (2) A different service is offered to reliable and honest users. The amount of service depends on the amount of contribution and peer credit.

GaMe-PLive is a game theoretical framework for peer-to-peer live video streaming. Prevention of free-riding and minimization of loss rate in video data transmission are the important objectives of this framework [22]. Mahini proposed a novel peer-assisted video streaming based on game theory and network coding. Communications between peers are modeled by a famous signaling game called Beer-Quiche. The Nash equilibrium analysis of the proposed game provides a reward and punishment mechanism which detects the free-riders and works as an incentive mechanism [23].

Few papers have worked on comparing proposed incentive mechanisms. In [18], some of these mechanisms are compared with the help of shared scenarios in order to determine their efficiencies. A user association map has been used to judge the efficiency and fairness of each method.

In [20] a game-based approach is proposed to model user behavior and compute their contributions in live sharing. At first, Nash equilibrium and Pareto Optimality are calculated for two individuals and then expanded to all actors. Selfish, cheat, malicious and attack behaviors are considered.

This method has modeled both optimistic and regular unckoking cases (modes). Results are compared with choking algorithm in Bit Torrent [5].

Designing a mechanism to detect Free-riders does not guarantee the efficiency of a cooperative system, mainly because there are users who try to break the rules of the game and earn more by means of collusion and fake identity [12].

In one study, Rowaihy et al. [29] showed that the original identity of the malicious user could probably be identified by its IP address. Dinger and Hartenstein [12] presented a new method called self-registration.

In [13], the notion of co-utility was suggested which indicated that mutual cooperation is the best decision for all users (even selfish users). All co-utility methods are not necessarily self-enforcing. In this paper, a study of how to make the existing protocol self-enforcing is carried out using the reputation mechanism. For this purpose, the Egen-Trust reputation mechanism is used. This method can be applied to different scenarios. Selfish users and free-riders are also willing to follow this method.

2.2. Confronting a Sybil Attack

The lack of central control in peer-to-peer networks makes these networks vulnerable to malicious attacks such as Sybil ones. That is why some users try to disrupt the system's rules with collusion and obtain the highest service. In Sybil attacks, a user can have several fake identities in the network. Although Douceur has proven that completely destroying the Sybil nodes is impossible, much effort has been made to minimize the damaging effects of Sybil attacks [15]. Rowaihy has shown that the identity of a malicious user could possibly be identified by its IP address [29]. Dinger and Hartenstein provide a method called "self-registration" where one identity registers its identity with r nodes [12].

In [36], using social networks, a method of dealing with a Sybil attack is proposed. In this method, the relationships used in social network graphs are used to discover colluding users. A social network graph shows all relationships between network members.

Dinger et al. [12] have developed a modified routing strategy for the Chord network. The routing strategies are based on a graph called the bootstrap graph which derives from the relationship between the participants [32]. In [39], the authors proposed the SybilGuard algorithm, which is a distributed algorithm for restricting Sybil logs.

By building the edges (Attack Edge) between the nodes and creating a path between them, the present paper shows that establishing a reliable relationship between true nodes is possible. Provided there are too many edges, Sybil nodes cannot have a reliable relationship. Therefore Sybil nodes will not achieve their goals [39].

In [33] attempts were made to identify Sybil nodes by tracking the nodes. In this regard, all incoming and outgoing nodes are monitored by predefined neighboring nodes. A copy of these messages will be sent from the receiver and sender to the monitor node.

By storing information such as the link between the sender and the recipient, the time of the connection and the response deadline, the monitor node can identify the Sybil node that publishes advertisements for its own purposes or sends malicious files. The drawbacks to this approach are that some nodes must be equally considered for monitoring the network, and that a significant amount of information should constantly be stored (for each send and receive) [33].

In general, the solution to the Sybil attacks is classified into two categories. One is to add a central control to the system [40], and the other is to limit the resources available to each user by using rules. In this way, resources available to Sybil users are gradually limited by network users, thereby helping the network regain its health.

In [36], using social networks, a method of dealing with a Sybil attack is proposed. In this method, the relationships used in social network graphs are used to discover colluding users. A social network graph shows all relationships between network members. One type of attack that threatens the security of social networks is the Sybil attack [26]. The Sybil attack also threatens ad-hoc networks like VANET. A method called ASAP-V has been proposed to detect Sybil attacks on VANET networks by identifying unknown individuals [11]. Recommender systems are designed to offer the best option based on user characteristics. Some users attempt to perform a Sybil attack with fake identities to make changes to the results of the recommender systems. Two methods have been proposed, namely Dysy-Rec and FDysy-Rec which can deal with dynamic Sybil attacks [25].

As discussed in Section 2 of the paper, some studies have focused on the detection of a free rider, and others are struggling to deal with Sybil attacks. The main difference between the proposed method and the previous methods is that this method simultaneously solves both problems. In fact, the process of confronting the Sybil attack has entered the mechanism of the file sharing incentive. For this purpose, an innovative function was proposed to calculate the centrality of the peers in the chunk exchange graph which has two unique features:

- It shows the impact of a peer on file sharing.
- It calculates the willingness of a peer to serve all other peers.

In fact, by applying this function to the game file sharing calculations, it attempts to solve two network problems simultaneously.

The main similarity of the proposed method with some of the previous methods is in the chosen strategy it applies to solve the problem. Many of the previous papers used reputation-based methods to solve the free rider problem. In these methods, a function is proposed to calculate the reputation of each peer. The proposed method, as in all these papers, is based on reputation. Of course, the proposed function for calculating the reputation is a new function specific to this method. In addition to detecting the free-riders, this function also includes an approach to combat the Sybil attack. In other words,

the proposed method is a reputation-based approach to which rules have been added to combat Sybil attacks.

2.3. The Effect of Topology

An important feature of a peer-to-peer file sharing network is network topology. The network topology heavily affects the methods of confronting the free-riders. In other words, a particular method may have a good performance on one topology and a poor performance on another.

The effect of topology on the method exists not only in peer-to-peer file sharing networks but in all peer-to-peer structures and graphs. For example, in pattern recognition systems that work on semi-supervised learning, the topology of the graph created from the data will greatly affect the performance of the learning algorithm. In addition, a number of researches have been conducted in this area to find the optimal graph [6,34].

As another example, the graph topology affects the text analysis process. In recent years, many studies have been carried out to explore the properties of languages using graph theory. For this purpose, a graph is made up of the words of a language. Subsequently, the main features of the language are extracted based on the topological features of the graph [2,3,30].

Another area in which the topology of the graph has a significant effect is bioinformatics. Many of the structures in the bioinformatics are in the form of a graph. The topological properties of these graphs play a crucial role in detecting and predicting. The importance of the properties of these graphs has led to the presentation of a tool, in article [4], for analyzing and extracting all the properties in biological graphs. With the help of this tool, all the features of these huge graphs such as the number of nodes, edges and connected components, diameter, radius, centrality, heterogeneity, clustering coefficient, and so forth can be calculated. Using the same tool in paper [14], a comprehensive analysis was carried out on the structure of proteins.

Like all the systems mentioned, the efficiency of peer-to-peer networks is affected by the communication topology. For example, in article [21], the authors presented a method for extracting optimal topology in peer-to-peer streaming networks. The network structure studied is distributed and wireless. The network infrastructure communication model is in the form of a mesh topology. However, researchers were looking for an overlay network on this infrastructure to maximize system performance. Peer-to-peer streaming networks, like peer-to-peer file sharing networks, function through peer cooperation.

3. System Model

3.1. Peer to Peer (P2P) Network

The P2P network is a decentralized structure in which resources and services are distributed among users. Information and services are transmitted directly between peers.

The P2P network allows users to share their resources and simultaneously connect to multiple sources [35].

The management style of this network enables it to expand significantly and increase its resources. As each new user enters the network and exchanges data in it, the network strength increases accordingly. We will not have a single point of failure if the information is duplicated between users. Behaviors such as competition and cooperation are among the ones present in these networks [35].

3.2. P2P File Sharing Network

In past years, P2P technology has been used extensively for file sharing. Based on the presence or absence of a central server, P2P file sharing systems are divided into three categories: pure, centralized, and hybrid. The system discussed in this paper is a hybrid file sharing network.

In this network, peers enter the network or leave it at their discretion. The amount of shared bandwidth and how to service other peers are completely optional. Communication topology of peers is a non-structured random graph. Connection between nodes is established according to the requested files. This graph is dynamic and changes in each round of file sharing. The chunks of a file are provided for a set of peers that applied for that file. Then peers exchange the chunks, this way all applicants will be the owner of the file.

Some servers are distributed on the network, whose duties are to store the performance of any peers in the past. By examining information stored on the servers, we can identify users who have been operating maliciously on the network and limit their services. To maintain scalability in the P2P network, connection between servers is organized using the Chord algorithm. Therefore, data recovery from servers is done by peers with a low cost. Each peer can decide on how to respond to another peer based on fetched information form a server. Figure 1 shows an overall structure of the model.

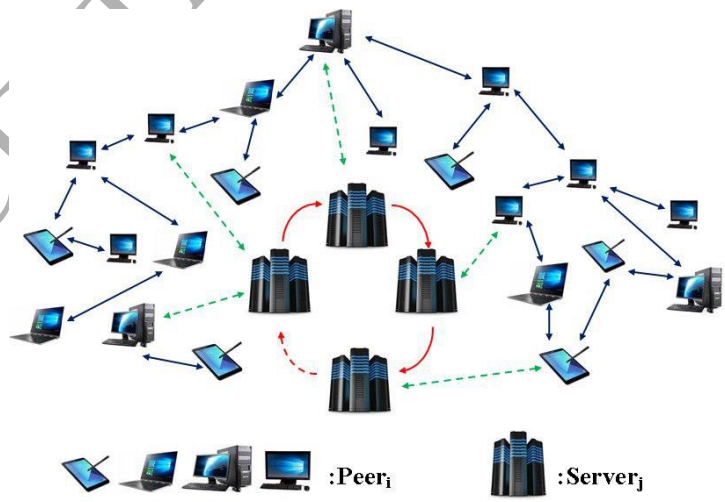


Fig.1. Overall structure of P2P file sharing network

4. The Proposed Game

In this section, a new incentive mechanism based on reputation is proposed. This method has been proposed to be implemented on the network model presented in Section 3. This network model is the basis of many collaborative systems that are used in practice. Therefore, the proposed method has the ability to be used in actual file sharing scenarios. Section 4.1 introduces a strategy for network users. The two bad strategies for the system are the defector (free-rider) and colluder, respectively. In addition, relation 1 from this section is used as the reputation formula in the incentive mechanism. In Section 4.2, a game was introduced that could deal with defectors. This game only shows one stage of the file sharing game. In Section 4.3, an evolutionary model was introduced that shows how users change their strategy at different stages of the game to gain more benefit from the system. In Section 4.4, a new relation was introduced that replaces a part of relation 1 from Section 4.1. This relation (relation 2) adds the ability to deal with Sybil attacks to the proposed method.

4.1. Incentive Mechanism

In a P2P network, like a customer, users are typically looking forward to receive services from the network. But most of them are reluctant to give the service. Whether or not they, like a server, would want to offer a service, the users' strategy could be divided into three broad categories. These strategies are outlined below:

Cooperator: The user provides the service without any conditions and does not seek further profit.

Defector: The user never provides a service.

Reciprocator: The user based on Pr_i will provide the service for the requestor. The Pr_i relation is calculated as Equation (1):

$$\mathrm{Pr}_i = \frac{time\ of\ serving}{time\ of\ consume} + \frac{shared\ bandwidth}{total\ bandwidth} \tag{1}$$

Where Pr_i is the value of generosity of user i. Any value greater than 1 is set to 1. Average value Pr_i is calculated for all users. This value is called $\overline{\mathrm{Pr}}$. Any user whose Pr_i value is smaller than $\overline{\mathrm{Pr}}$ is known as a defector or free-rider. Based on the numerator and denominator variables in relation 1, one can understand that users are known as defectors if their service utilization rates are much higher than those of their service delivery to others or if they made a small portion of their bandwidth available to the file sharing system. The value of this relationship is important only for Reciprocators because the Cooperators provide the service in any case; and Defectors will also avoid giving the service in any case. Therefore only the Reciprocators calculate the value of this relationship by referring to the requesting user's history, and then decide on the service. The condition of providing service to user i is the correctness of the relation $\overline{\mathrm{Pr}} < \mathrm{Pr}_i$.

These three categories are a general classification of the strategies users adopt in dealing with the service request. In most papers, these three types of users are considered. However these are not the only strategies that users select in a P2P network. As already mentioned, users who are already aware of network rules and collude with each other intend to maximize their benefits. The present paper also considers this kind of user strategy.

In Section 4.2, a game is introduced which identifies only the free-riders based on relation 1. There is no discussion about colluding users in the game. However, in Section 4.4, a formula (relation 2) is introduced which gives the proposed method the ability to deal with the Sybil attack if replaced with the "times of serving" variable in relation 1. This discussion is given in full with an example in Section 4.4.

Colluder (Sybil): This category of users only serves its fellow colluder in an unrealistic way. The user intends to increase its own Pr_i by means of collusion, and urges Reciprocators to provide their requested services.

Regarding the rationality of network users, they are constantly changing their strategy. They learn from neighbors who have the highest payoff score and change their strategy to the neighbor's strategy. Maintaining a long history of previous and new user's behavior makes the system vulnerable to malicious users [16]. In order to encourage defectors to change their behavior, their history is cleared after proof of strategy change [10]. As soon as the users' history is deleted, their Pr_i will also increase and so will the probability of the Reciprocators' giving them services.

4.2. The Game Model

In this game model, players are the same network users each of whom adopts a particular strategy for their game. As mentioned in previous sections, player strategy is the unconditional provision of service(cooperator), defecting(defector or free-rider), or reciprocating(reciprocator). The rules of the game are described below:

In each round of the game, the network user requests service from their neighbors. Each node of this network is a neighbor of n other nodes. Therefore each node in each round makes n requests from its neighbors. The receiver of the request will incur the C cost upon the provision of the service, and the receiver will gain the B profit. The value of B is greater than C.

To test the impact of profits on user strategy, a parameter called Q is defined equal to the ratio between C and B. This parameter accepts values between 0 and 0.9. The value of C is set to 1. The Reciprocator needs to have the applicant's history information in order to decide whether to give the service which calls for C_r cost information. In this paper, C_r is initialized to 0.1. The matrix of the game is given in Equation (2). Since it is the reciprocators' duty to identify and restrict defector users, this matrix is written only for defector and reciprocator users. Cooperator users provide services under any circumstances, so they are not allowed to contribute to the game matrix.

$$\begin{matrix} & \begin{matrix} defect & reciprocate \end{matrix} \\ \begin{matrix} defect \\ reciprocate \end{matrix} & \begin{bmatrix} \underline{0}/\underline{0} & 0/-C_r \\ -C_r/0 & \underline{\underline{B-C}} \end{bmatrix} \end{matrix} \quad (2)$$

The main actors include Defectors and Reciprocators. For this reason, the matrix of the game has been drawn for these two types of actors. This game has two equivalence points. Defect equivalence is not desirable. Users who choose the defect strategy are the same free-riders. These users are not optimal for the network and have a detrimental effect on the file sharing process. The proposed method tries to stop providing service for them by identifying users who have chosen the defect strategy. After having been denied access to the service, these users are convinced that they will change their strategy and choose to cooperate with the system. A change in strategy occurs during an evolutionary process by imitating users who receive a better service from the system. A description of how to change user strategy during the game has been given in the following section.

4.3. Evolutionary Model

An important aspect of a network with rational users is propagating a behavior among users. As the common cold is transmitted from breathing in a joint space, the behavior of the network users is also spread with a specific pattern [24]. In the game model, as described in Section 4.2, each user's profit rate was calculated according to the strategy of that user in one round of the game. Users in the P2P file sharing network change their strategy according to the pattern of behavior propagation and opt for a new method. The social planner tries to propagate the best behavior within the network by choosing a suitable mechanism and persuades users to choose a behavior that is useful for network sustainability. Using the evolutionary game model, the effect of this behavior change can be analyzed over the lifetime of the network.

An evolutionary game theory was first proposed by Maynard Smith. He combined the game model analysis with the dynamic evolution process to examine complex systems [17]. In recent years, due to complex and hard computations in the Nash equilibrium, the evolutionary game theory has been used to solve various problems.

In addition to the complexity of the calculations, Nash equilibrium is not able to provide the best solution in terms of optimality and stability [42]. The evolutionary game theory is inspired by the genetic population model. Unlike the classical method that is based on the balance of strategy, this model focuses on strategy change [42]. Despite its name, evolutionary game theory is more concerned with economists than biologists.

The evolutionary game theory is a model for games in which players choose their strategies in a trial and error process and, over time, change their decision by discovering better strategies [42].

The proposed method investigates the process of strategy changing in P2P file sharing network users based on the evolutionary game model.

Due to the fact that users do not have comprehensive network information, they try to imitate their neighbor's model in order to maximize their payoff. They learn from a neighbor with higher payoff and change their strategy to their neighbor’s strategy.

A user randomly selects a neighbor and, with the probability of which its relationship is given below, changes its strategy. The rule according to which a user learns from a neighbor based on the Fermi process is as follows: user i randomly selects user j from among his neighbors and learns from them with the probability that depends on the difference in their payoffs [10]. This probability is calculated from the following Equation (3):

$$W(S_i \to S_j) = \frac{1}{1+\exp[(P_i - P_j)/k]} \quad (3)$$

Where K denotes the intensity of selection (noise or mistake rate). Noise permits peers to make an irrational selection; that is, some peers may occasionally not follow the perfect rationality, and arbitrarily change their strategies due to curiosity or mistakes. P_i and P_j are payoffs of peer i and peer j, respectively. For $K=0$, peer i will adopt j's strategy deterministically when $P_j > P_i$. For $K>0$, peer i will also adopt the j's strategy with a certain probability, although j's strategy performs worse. Selfish and rational peers prefer the strategies of more successful neighbors. Here k is set to 0.1 for all simulations by referring to the research.

The $B - C$ value in relation (2) is greater than zero, and players change their strategy based on their neighbors' profits. Therefore, it is expected that the balance point will converge to deal/deal as the game progresses.

4.4. Detecting Sybil Attacks

Being aware of the rules of the network, users who engage in collusive practices try to seek more services while not serving others. They do not want to change their strategy. These users will maintain their strategy until the end of the game, and will not serve other users except their colluding accomplices. On the other hand, these users pretend to cooperate, and their neighbors learn cooperation while learning. These users are called colluders. In other words, colluders are users who try to perform a Sybil attack by creating a few fake identities or in cooperation with several other users. The purpose of these users is to breach the rules that the social planner has set up for the better functionality of the file sharing network.

By providing unrealistic services, the Sybil user increases the ratio of the number of services provided (Ps_i) to the number of served services (Cs_i), i.e. Pr_i Equation (1). Reciprocators who decide based on this ratio are deceived and provide their desired service.

Previously, we have stressed that we consider the value of any service that the user provides to be 1. Now some of them are assigned a weight less than one. In doing so, the number of times a user gives service to their neighbors is maintained. Using Equation (4), you can prevent Reciprocators from offering their services to colluders.

$$PS_i = \sum_{j=1}^{nc} \sum_{k=1}^{psc[j]} \theta^k \qquad (4)$$

Where Ps_i is the weight of the number of services that user i provides. nc denotes the number of neighbors of the user i, and $PSC[j]$ shows the number of services the user i has given to neighbor j. θ is the value of a service that is set to a value less than 1 ($\theta = 0.9$). In addition, Ps_i value in Equation (1) is replaced with the times of serving.

This Equation clearly shows that Ps_i value is different with regard to the equal number of services that user i provides in two different conditions: 1-only for one user 2-for different users. This value is greater for the second mode. The more services are provided for more users, the greater the value of this equation. In this way, users who respond only to their peer-to-peer service requests will gradually have lower Ps_i value. In addition, they will not receive service from the traders. Any reduction in Ps_i value reduces the Pr_i value. This amount is very effective for the decision of the Reciprocators.

Here is a description of the functionality of the proposed function. By carefully analyzing the functionality of this function, how the incentive mechanism recognizes the Sybil attack can be understood.

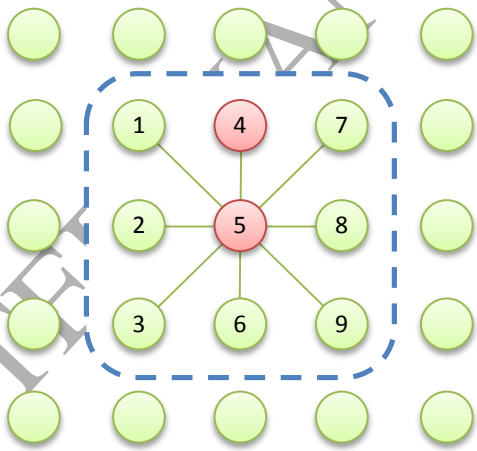


Fig.2. The two red nodes represent the colluders and the other nodes are the true ones

A profile of the network is shown in Figure 2. The red nodes represent the Sybil nodes and other true nodes. In this model, each node communicates with its 8 neighboring nodes. Each node stores a record of the number of services provided to its neighbors. A structure like Table 1(a) can store this information.

Table 1. A structure for storing the number of services provided to neighbors of node number 5

	1	2	3	4	5	6	7	8	9
A	**0**	**0**	**0**	**16**	**-**	**0**	**0**	**0**	**0**
B	**2**	**2**	**2**	**2**	**-**	**2**	**2**	**2**	**2**

Table 1(a) shows the information related to the number of services provided to each of the neighbors. A sample of this information has been registered for neighbors of node number 5. It can be seen that the colluder number 5 only provides service to colluder number 4.

To better understand the functionality of function 4, assume that user 5 is a normal user and has provided the same number of services to all requester users. In this case, the service providing history is in the form given in Table 1(b). Calculation of value Ps_i for both *a* and *b* modes indicates that colluder users get fewer privileges. In *a* mode $Ps_i = 7.26$, and in *b* mode $Ps_i = 13.68$. The values obtained clearly show that users performing the Sybil attack receive fewer rewards than other users and are eventually identified.

By adding the relations from this section to the proposed method, it is now possible to detect the free-riding and Sybil attack at the same time using an incentive mechanism. Comparing the proposed method with the methods studied in the literature review section suggests that unlike the proposed method, all previous methods are designed either to discover free-riding or to focus on confronting Sybil attacks. None of the methods resolve both problems simultaneously. This is the main difference between the proposed method and the previous ones.

4.5. Server and Peer Algorithm

According to the concepts described in the previous sections, the pseudo-code of the function of the peers and servers is presented in this section. In each round of file sharing, each peer that is faced with the chunk request, first asks the status of the applicant from the server. If the applicant user is not a free rider, then the service will be provided to him/her. The chunk requester sends a report for receiving or not receiving the service to the server. Pseudo-code 1 shows the function of a peer as a server in each round of the game.

```
Algorithm 1: Peer_i as a Server
1: do{
2:     if(Peer_j requestchunk_k){
3:         if(strategy_i = Defector or strategy_i = Colluder)
4:             reject(peer_j)
5:         elseif(strategy_i = Cooperator)
6:             send(chunk_k, Peer_j)
7:         elseif(strategy_i = Reciprocator)
8:             fetchProfile(Peer_j)
9:             if(Peer_j ≠ free−rider)
10:                send(chunk_k, Peer_j)
11:    }//end if
12:    update(strategy_i)//Basedon Evolutionary gameModel
13:}while(true)
```

If a peer needs a file, and sends a request to another peer, it reports that peer's function to the server. If a file is received, a positive report will be sent to the server, otherwise a negative report will be sent. The colluder peers that perform Sybil attacks send a positive report to their partner in way. Pseudo-code 2 shows the peer function as a client.

```
Algorithm 2: Peer_i as a Client
1: do{
2:     Parallelsend request(Peer_j, Chunk_k) forsome j, k
3:     if(recieved(chunk_k))
4:         report(positiveSharedBandwidth_j, Peer_j)
5:     else
6:         report(negative,0, Peer_j)
7:     if(strategy_i = Colluder)
8:         foreach j thatPeer_j ColludePeer_i
9:             reprort(positive,Bandwidth_j, Peer_j)
10:}while(true)
```

On the other hand, servers receive the peer performance reports in each round of the game and save them on each user's profile. At the end of each round, the service graph is updated and its centrality is calculated. Given the amount of shared bandwidth, the value of each peer's reputation is calculated. Any peer with less reputation than average reputation of all peers is known as a free rider and will not receive a service. Pseudo-code 3 shows the server performance in each round of the game.

Algorithm3: Server

```
1: do{
2:     foreach fetchProfile(Peer_i)
3:         if(retutation_i < \overline{reputation})
4:             send(free-rider)
5:         else
6:             send(not free-rider)
7:     wait for reports
8:     forech Peer_i in P2P filesharing network{
9:         update(Ps_i) // Based on proposed centrality
10:        update(Pr_i) // Based on proposed reputation formula
11:    }// end for
12:    update(\overline{reputation}) // \overline{reputation} is average of Pr
13: while(true)
```

5. Simulation and Analysis

In this section, simulation results of the proposed method are presented. To better understand the simulation results, firstly, how to design and simulate the parameters are explained. In the following, the objectives and metrics of the problem are examined. In the following sections, simulation results for different modes are given. Finally, at the end of this section, the degree of adaptation of the obtained results is evaluated with the objectives of the research.

5.1. Simulation Design

In order to implement the proposed method, the MATLAB programming language was used. The program was run on a computer with a 2.2 GHz processor and 4 GB of RAM. The test data is generated randomly based on the network topology under study. The file sharing process is assumed to be a game and each stage of file sharing is known as one round of the entire game. There is a function to simulate the performance of each peer in one round of the game. One round of the game ends when all peers decide on how to respond to requests. Another function is designed that simulates the process of users' strategy change based on the evolutionary game model. At the end of each round of the game and before the start of the next round, this function is executed and will be updated by running those strategies. Each player, at the end of every round of the game, sends a report to the server about the performance of the users who are requesting a chunk.

5.2. Objectives and Metrics

The simulation objectives determine what features to evaluate in the proposed method. The simulation output should be in such a way that it leads us to these objectives. The main objectives of the simulation can be summarized in the following three cases:

- Calculation of users' willingness to choose the optimal strategy

• Checking the extent to which colluders are limited in file sharing networks

• Specification of a threshold limit for the correct operation of the proposed method

To achieve these goals in simulation, a series of metrics is used. Each of these metrics measures a certain value for us. Using these values, you can achieve simulation objectives. The main metrics used are:

• User strategy: This metric contains three numbers per round of the game. These numbers indicate the number of users who have chosen the strategy of cooperators, defectors and reciprocator respectively in this round.

• Successful download rate: Users send requests for other peers in each round of the game. Some of these requests are accompanied by a positive response and some others are rejected. The successful download rate indicates what percentage of the requests have been answered in a single round of the game. This metric can be calculated for any kind of strategy.

• The average consumed service: This metric is calculated in one round of the game for a specific type of users which indicates the number of services that each user has received on average by choosing this strategy. The number of services received from the start of the game to this round is further considered.

5.3. Simulation data and protocols

The main feature of the simulation data is the user strategy and its communication topology. Users are organized based on the network properties that were introduced in Section 3. To arrive at real scenarios, the type of user relationship is considered to be completely random. When entering a peer-to-peer file sharing system, each user selects a strategy randomly. The rate of selection of different strategies is related to the trends of network users. However, to achieve a fair simulation, at the first moment, an equal number of each strategy is selected that is uniformly distributed over the network. For better analysis, these percentages are changed in different simulations. Subsequently, the simulation parameters and how to run the file sharing game are described below.

In this simulation, the size of the network is 100×100 square; that is, the network has 10,000 users. Each node in this network is a neighbor of at most 8 other nodes. Each user in each round sends a request to each of its neighbors. Each neighbor further responds according to its own strategy. In this network, neighbors may change, that is, from the beginning to the end of the game; each node will not have the same neighbors as it did at the beginning of the game. Nodes' bandwidth is between 100 and 5000kbps, and shares a portion of it randomly. The game starts with equal percentages of cooperators, defectors and Reciprocators. Only 2 colluders are assumed to be on the network. These users, i.e. colluders, are randomly distributed on the network (Figure 3a).

The simulation parameters have sometimes been changed to obtain more accurate results and to achieve better evaluation. For example, the number of colluders has increased, or the percentage of strategy selection has been changed at the beginning of the game. These changes are mentioned in the respective sections.

5.4. Simulation Results

Initially, we implemented the program with an equal percentage of strategies in two hundred rounds. The simulation shows that with every increase in rounds, nodes move forward toward cooperation or reciprocate through changing their strategy with the aim of maximizing their benefits. This is clearly evident in Figure 3. Blue nodes are cooperators; green nodes are defectors; and red nodes are reciprocators.

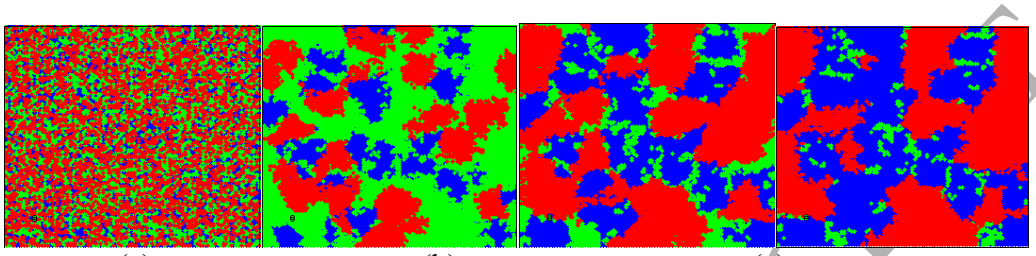


Fig.3. Blue:Cooperators; Green:Defectors; Red:Reciprocator, a) Users Strategy in Round 1; b) Users Strategy in Round 50; c)Users Strategy in Round 100; d)Users Strategy in Round 200

In this simulation, parameter Q is set to be $Q=0.35$. For this reason, it was initialized as such, assuming the value Q, the number of Reciprocators on the network gradually increases.

The number of free riders increases at the beginning of the game, but after detecting the malicious behavior of these nodes, the tendency to free rider becomes less and users tend to cooperate. Figure 4 shows the strategy changing of users.

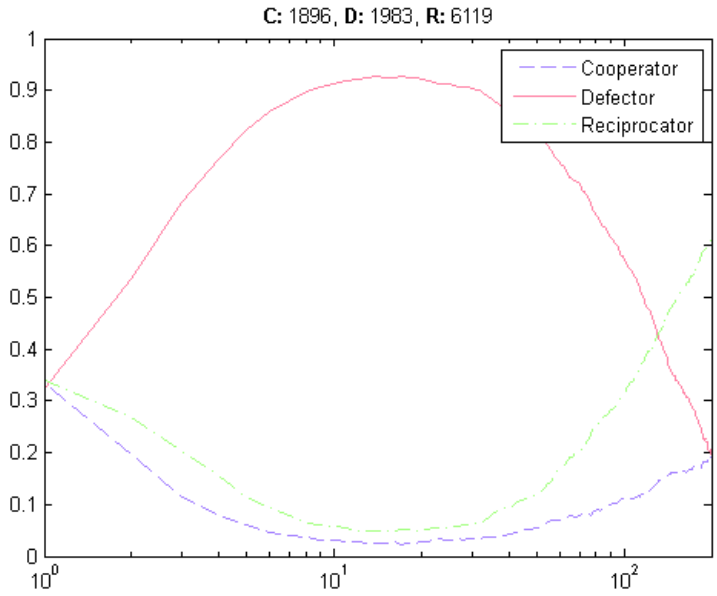


Fig.4. Users strategy during the game (x-axis: game round, y-axis: percentage of selecting each strategy)

Due to the fact that at the beginning of the game, the cost-free download rate at Free riders is high, the tendency for free riders is higher. Then these users are identified and fewer services are provided to them. Therefore, the tendency towards the Reciprocator is increased. Figure 5 shows the percentage of successful downloads in different rounds based on the strategy.

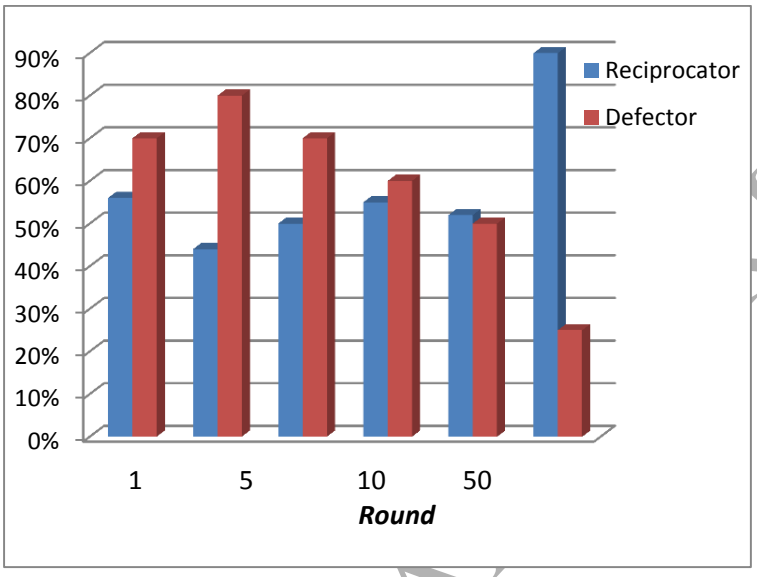


Fig.5. Successful downloads percentage

As shown in Figure 6, the number of real services that colluders received at the beginning of the game is higher than the average number of services that other users did. However, as the game continues, the proposed solution given in (3) restricts the service of these users.

The important parameters that will be evaluated are: 1. The average service consumed by colluders (Ls) 2. The average service consumed by all users (La) 3. The average service consumed by colluders without using the proposed solution (Lo).

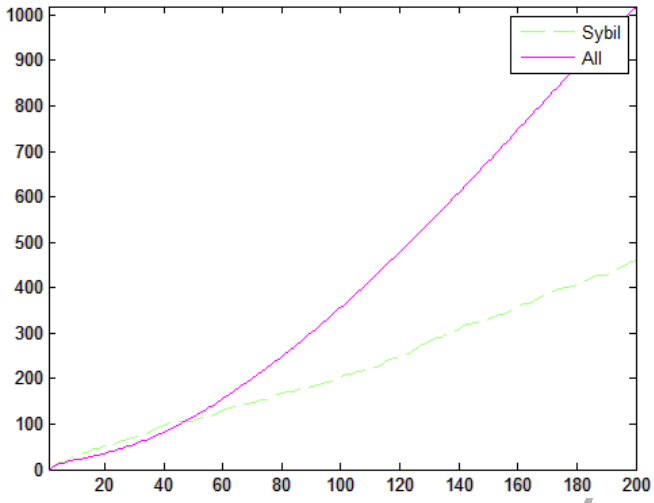


Fig.6. The average number of services received by colluders and other users (x axis: round, y axis: number of services)

As shown in Figure 3, the Ls value up to round 50 is greater than La. The value significantly decreases continuing the game compared to La.

In Figure 4, it is evident how the proposed relationship functions. Assuming an equal number of rounds, Ls shows smaller values than Lo. This value will even decrease as the number of rounds increases.

Although the proposed solution presented in [10] increases the number of Cooperators and Reciprocators and forces defectors to change strategy (Figure 3), it is vulnerable to the Sybil attack. As shown in Figure 7, it is clear that without changing their strategy, they benefit from a great number of services. However, in the proposed method, these nodes are detected and the longer the network life goes on, the lower the number of services they provide.

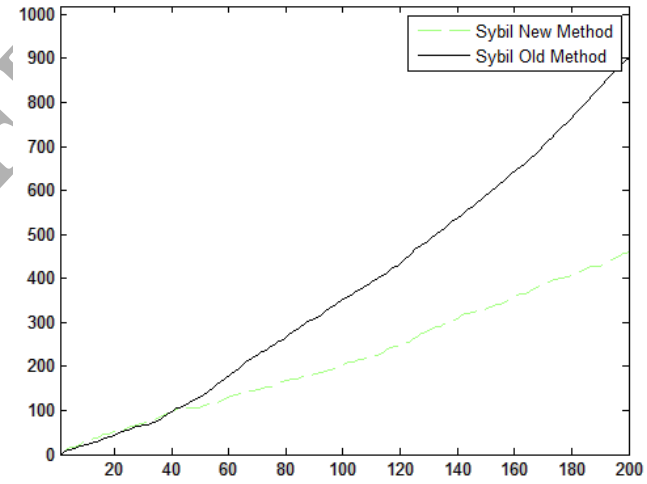


Fig.7. Average number of services received by colluders when using or not using the centrality relationship(x axis: round, y axis: number of services)

The proposed method is investigated by assuming two Colluders. The large number of Colluder users who collaborate on Sybil attacks will affect the performance of the proposed method. Figure 8 shows the average user-received services in round 200 of the game for different numbers of Colluders. Of course, given that P2P file sharing network users are Rational, the possibility of user collusion is limited.

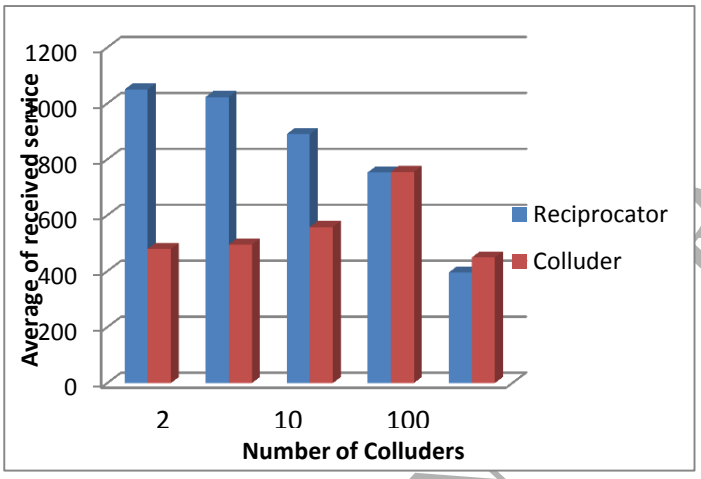


Fig.8. Average received service for different number Colluders in round 200

The proposed method is investigated at the beginning of the game by assuming that 30% of users are free riders. If the number of free riders changes at the beginning of the game, the performance of the proposed incentive mechanism will change as well. Figure 9 shows the percentage of selecting each strategy in round 200 for different initial percentage of free riders. If the number of free riders is between 0 and 50% of the total peers at the beginning, then the proposed incentive mechanism has a good performance. Between 50 to 70% is ineffective, and the network will be destroyed for more than that.

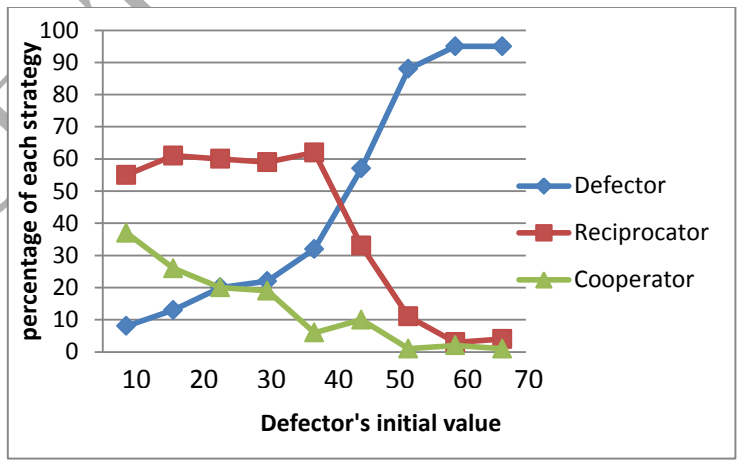


Fig.9. The effect of the number of free riders on strategy selection

Figure 10 shows the process of destroying the network and choosing the defector strategy by the users. In this simulation, seventy-five percent of the users are free riders at the beginning of the game; that is, their strategy is of the defector type. As can be seen, at the end of the game, most of the cells have become green which represent the defectors.

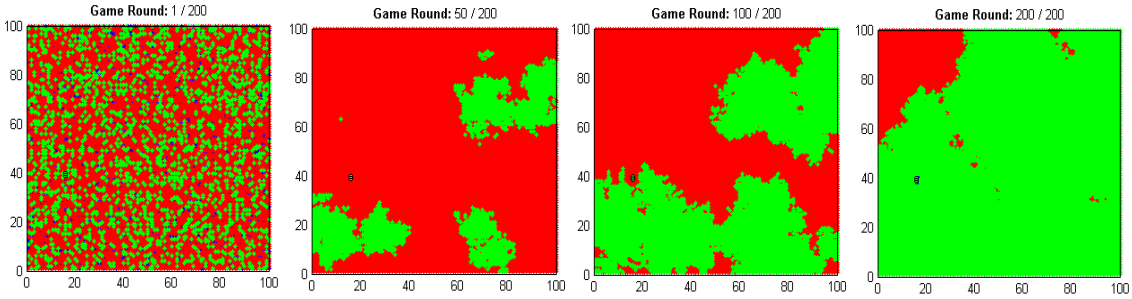
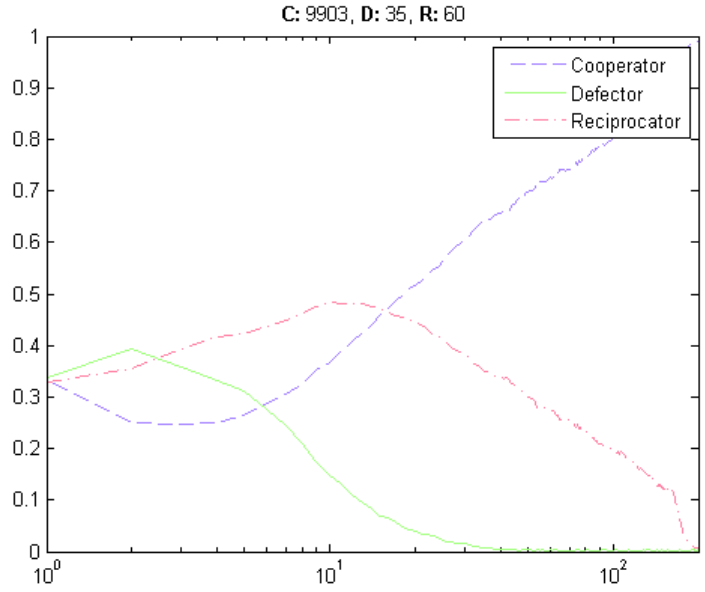


Fig.10. Blue:Cooperators; Green:Defectors; Red:Reciprocator,

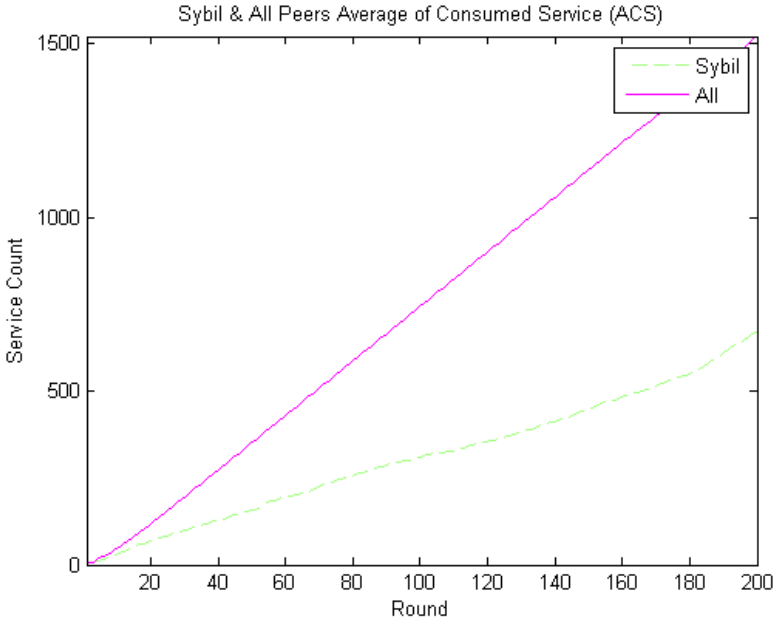
5.5. The Effect of Network Topology on the Proposed Method

All simulations conducted in previous sections are based on the network model presented in Section 4. In this network, the nodes' relational topology is of mesh type. In this section, we examine the effect of a topology change in the proposed method. Types of relational topologies in peer-to-peer networks are presented in paper [1]. Accordingly, we need to consider two tree and multi-tree topologies.

We first examine the tree topology. In this topology, nodes are organized as a tree from server to leaves. File chunks are sent from the server to the children. Also, each node sends it to its children besides using the chunk. Once a node has been corrupted or has been identified as a free-rider, the tree must be restored. There are various ways to restore a tree. In this simulation, a node-to-grandfather connection method is used. Figure 11(a) shows the process of strategy selection in different game periods. Figure 11(b) specifies the amount of service provided for the Sybil nodes.



a) Users strategy during the game (x-axis: game round, y-axis: percentage of selecting each strategy)



b) Average number of services received by colluders when using or not using the centrality relationship(x axis: round, y axis: number of services)

Fig.11. Performance of the proposed method in tree structure

A careful scrutiny of Figure 11 shows that the proposed method has had a better performance in the tree structure of the network. The main reason for this lies in the shape of the network. In peer-to-peer networks of trees, leaf nodes have no effect on file sharing and are only receivers. All requests are limited to internal tree nodes. Therefore, there are more requests per node which leads to the better identification of the free-riders. On the other hand, the number of negative reports for the colluder node is so high that it is well-identified. This in turn leads to a sharp decline in the average number of its received services. Examining the structure of the network in the form of a multi-tree displays results similar to tree.

5.6. Comparison with Previous Methods

After carefully reviewing the performance of the proposed method, we should compare its performance with those of some of the previous papers to determine the position of this method. The data used in this paper was generated randomly. Therefore, to evaluate previous methods, we must apply these methods to the data of this research. This comparison has been done in four different metrics and in the 200th round of the game. The first is the number of free-riders; the second is the average service received by all nodes; the third is the average service received by Sybil nodes, and fourth is the percentage of successful downloads of reciprocators. The results of the comparison are shown in Table 2.

Table.2. result of simulation in round 200

Method	Number of Free-riders	Average of received service	Average of received service in Sybil nodes	Percentage of successful download in reciprocators
[10]	2095	1003	998	82%
[37]	1992	1017	1035	87%
[41]	2129	995	1000	80%
Proposed	1980	1024	465	88%

A careful review of the values listed in Table 2 shows that the proposed method has had relative success in restricting free-riders compared to the remaining methods. The strength of the proposed method is its ability to detect Sybil attacks. Methods that are close to the proposed method in restricting free riders lack the ability to detect Sybil attacks. Therefore, the average number of services received in Sybil nodes is approximately equal to those of other nodes. On the other hand, this value is very different in the proposed method since Sybil nodes receive fewer services.

6. Conclusion

In this paper, it has been shown that by quantifying the weight for each service and initializing the dispersion of the services provided, Sybil attacks can be rendered ineffective. The proposed incentive mechanism has forced free riders to send chunks to other nodes and share their resources in order to get services. To better demonstrate how the proposed solution functions, $Q = 0.35$ was used. However, the effect of this relationship can be examined by using different Q. In the proposed method, users are known by their history. So users can clean their history and get services for a while by logging off and then logging in with a new id. In the future, this weakness can be overcome by adding a stability factor to reputation. In addition, regarding the logic in this solution, it seems that its performance in networks with larger dimensions and more neighbors yields better results. As a future work, the convergence speed can be increased by creating trusted nodes in the network.

References

[1] W. AlTuhafi, S. Ramadass, Y. Chong, "Concepts and types of peer-to-peer network topology for live video streaming", IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 1-4, 2013.

[2] D. R. Amancio, "A complex network approach to stylometry". PLoS One, Vol. 10, 1-21, 2015. doi:10.1371/journal.pone.0136076.

[3] D. R. Amancio, "Probing the topological properties of complex networks modeling short written texts", PloS one, Vol. 10, 1-17, 2015.

[4] Y. Assenov, F. Ramírez, S. E. Schelhorn, T. Lengauer, M. Albrecht, "Computing topological parameters of biological networks. Bioinformatics", Vol. 24, 282-284, 2007.

[5] F. Azzedin, M. Yahaya, "Modeling BitTorrent choking algorithm using game theory", Future Generation Computer Systems, Vol. 55, 255-265, 2016.

[6] J. R. Bertini, A. A. Lopes, L. Zhao, "Partially labeled data stream classification with the semi-supervised K-associated graph", Journal of the Brazilian Computer Society, Vol. 18, 299-310, 2012.

[7] S. M. Bozorgi, A. S. Rostami, A. R. Hosseinabadi, V. E. Balas, "A New Clustering Protocol Based on Renewable Energy and Multi-Hop Routing for Energy Harvesting-Wireless Sensor Networks", Computers & Electrical Engineering, Elsevier, Vol. 64, 233-247, 2017.

[8] J. Chang, Z. Pang, W. Xu, H. Wang, G. Yin, "An incentive compatible reputation mechanism for P2P systems", The Journal of Supercomputing, Vol. 69, 1382-409, 2014.

[9] Z. Chen, Y. Qiu, J. Liu, L. Xu, "Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game", Computers & Mathematics with Applications, Vol. 62, 3378-3388, 2011.

[10] G. Cui, M. Li, Z. Wang, L. Tian, J. Ma, "Analysis and evaluation framework based on spatial evolutionary game theory for incentive mechanism in peer-to-peer network, IEEE 11th International Conference on InTrust, Security and Privacy in Computing and Communications (TrustCom), 287-294, 2012.

[11] T. B. M. de Sales, A. Perkusich, L. M. de Sales, H. O. de Almeida, G. Soares, M. de Sales. "ASAP-V: A privacy-preserving authentication and sybil detection protocol for VANETs", Information Sciences, Vol. 372, 208-224, 2016.

[12] J. Dinger, H. Hartenstein, "Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration", First International Conference on Availability, Reliability and Security (ARES'06), 1-8, 2006.

[13] J. Domingo-Ferrer, O. Farràs, S. Martínez, D. Sánchez, J. Soria-Comas, "Self-enforcing protocols via co-utile reputation management", Information Sciences, Vol. 367, 159-175, 2016.

[14] N. T. Doncheva, Y. Assenov, F. S. Domingues, M. Albrecht, "Topological analysis and interactive visualization of biological networks and protein structures", Nature protocols, Vol. 7, 670-685, 2012.

[15] J. R. Douceur, "The sybil attack. In International Workshop on Peer-to-Peer Systems", Springer, Berlin, Heidelberg, 251-260, 2002.

[16] M. Feldman, K. Lai, I. Stoica, J. Chuang, "Robust incentive techniques for peer-to-peer networks", In ACM Proceedings of the 5th ACM conference on Electronic commerce, 102-111, 2004.

[17] H. Feng, S. Zhang, C. Liu, J. Yan, M. Zhang, "P2P incentive model on evolutionary game theory", In 4th International Conference on Wireless Communications Networking and Mobile Computing, 1-4, 2008.

[18] D. Guo, Y. K Kwok, X. Jin, J. Deng, "A performance study of incentive schemes in peer-to-peer file-sharing systems", The Journal of Supercomputing, Vol. 72, 1152-1178, 2016.

[19] S. D. Kamvar, M. T Schlosser, H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks", ACM In Proceedings of the 12th international conference on World Wide Web, 640-651, 2003.

[20] W. S. Lin, H. V. Zhao, K. R. Liu, "Incentive cooperation strategies for peer-to-peer live multimedia streaming social networks", IEEE transactions on multimedia, Vol. 11,3 96-412, 2009. doi:10.1109/TMM.2009.2012915.

[21] L. Maccari, N. Facchi, L. Baldesi, R. L. Cigno, "Optimized P2P streaming for wireless distributed networks", Pervasive and Mobile Computing, Vol. 42, 335-350, 2017.

[22] H. Mahini, M. Dehghan, H. Navidi, A. M. Rahmani, "GaMe-PLive: a new game theoretic mechanism for P2P live video streaming", International Journal of Communication Systems, Vol. 29, 1187-1203, 2016.

[23] H. Mahini, M. Dehghan, H. Navidi, A. M. Rahmani, "Peer-assisted video streaming based on network coding and Beer-Quiche game", AEU-International Journal of Electronics and Communications, Vol. 73, 34-45, 2017.

[24] MEJ. Newman, "Networks: an introduction." 1-720, ISBN: 9780199206650, 2010.

[25] G. Noh, H. Oh, Y. Kang, C. Kim, "PSD: Practical Sybil detection schemes using stickiness and persistence in online recommender systems," Information Sciences, Vol. 281, 66-84, 2014.

[26] S. Rathore, P. K. Sharma, V. Loia, Y. Jeong, J. H. Park, "Social network security: Issues, challenges, threats, and solutions", Information Sciences, Vol. 421, 43-69, 2017.

[27] Y. Ren, M. Li, Y. Xiang, Y. Cui, K. Sakurai, "Evolution of cooperation in reputation system by group-based scheme", The Journal of Supercomputing, 1-20, 2013.

[28] S. Rostami, M. Badkoobe, F. Mohanna, H. keshavarz, A. R. Hosseinabadi, A. Kumar Sangaiah, "Survey on Clustering in Heterogeneous and Homogeneous Wireless Sensor Networks", The Journal of Supercomputing, Vol. 74, 277-323, 2018.

[29] H. Rowaihy, W. Enck, P. McDaniel, T. La Porta, "Limiting sybil attacks in structured p2p networks", 26th IEEE International Conference on Computer Communications, 2596-2600, 2007.

[30] F. N. Silva, D. R. Amancio, M. Bardosova, L. D. F. Costa, O. N. Oliveira Jr, "Using network science and text analytics to produce surveys in a scientific topic", Journal of Informetrics, Vol. 10, 487-502, 2016.

[31] B. Strulo, A. Smith, J. Farr, "An architecture for peer-to-peer economies", Proceedings of the Third International Conference on Peer-to-Peer Computin, 208-209, 2003.

[32] Z. Trifa, M. Khemakhem, "Mitigation of sybil attacks in structured P2P overlay networks", Eighth International Conference on Semantics, Knowledge and Grids, 245-248, 2012.

[33] Z. Trifa, M. Khemakhem, "Sybil Nodes as a Mitigation Strategy against Sybil Attack", Procedia Computer Science, Vol. 32, 1135-1140, 2014.

[34] A. Vega-Oliveros, L. Berton, A. M. Eberle, A. de Andrade Lopes, L. Zhao, "Regular graph construction for semi-supervised learning", In Journal of physics: Conference series, Vol. 490, IOP Publishing, 2014.

[35] Y. Wang, A. Nakao, A. V. Vasilakos, J. Ma, "On the effectiveness of service differentiation based resource-provision incentive mechanisms in dynamic and autonomous P2P networks", Computer Networks, Vol. 55, 3811-3831, 2011.

[36] F. Wang, "Preventing Sybil Attacks in Structured P2P Networks using Social Network", Boletín Técnico, Vol. 55, 424-429, 2017.

[37] T. Y. Wu, W. T. Lee, N. Guizani, T. M. Wang, "Incentive mechanism for P2P file sharing based on social network and game theory", Journal of Network and Computer Applications, Vol. 41, 47-55, 2014.

[38] L. Xu, S. Chainan, H. Takizawa, H. Kobayashi, "Resisting sybil attack by social network and network clustering", 10th IEEE/IPSJ International Symposium In Applications and the Internet (SAINT), 15-21, 2010.

[39] H. Yu, M. Kaminsky, P. B Gibbons, A. D. Flaxman, "Sybilguard: defending against sybil attacks via social networks", IEEE/ACM Transactions on networking, Vol. 16, 576-89, 2008.

[40] H. Yu, C. Shi, M. Kaminsky, P. B Gibbons, F. Xiao, "Dsybil: Optimal sybil-resistance for recommendation systems", 30th IEEE Symposium on In Security and Privacy, 283-298, 2009.

[41] M. Zghaibeh, "O-Torrent: A fair, robust, and free riding resistant P2P content distribution mechanism", Peer-to-Peer Networking and Applications, 1-13, 2018.

[42] Q. Zhang, H. F. Xue, X. D. Kou, "An evolutionary game model of resources-sharing mechanism in P2P networks", Workshop on InIntelligent Information Technology Application, 282-285, 2007.

[43] R. Zhou, K. Hwang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing", IEEE Transactions on parallel and distributed systems. Vol. 18, 460-473, 2007.