A Novel Bilateral Incentive Mechanism Based on Social Relation and Evolutionary Game Theory

Wei-Chun Wong[1], Wei-Tsong Lee[1], Hsin-Wen Wei[1], Yao-Chiang Yang[1], Vooi-Voon Yap[2]

[1] Department of Electrical and Computer Engineering, Tamkang University, Taiwan
[2] Faculty of Engineering and Green Technology, Universiti Tunku Abdul Rahman, Malaysia
froggenwong@outlook.com, wtlee@mail.tku.edu.tw, hwwei@mail.tku.edu.tw,
ychiangy@gmail.com.tw, yapvv@utar.edu.my

Abstract

Peer-to-peer (P2P) file-sharing system has been developed rapidly over the past years. P2P file-sharing mechanisms such as Gnutella, BitTorrent and Private Tracker have been used popularly. The number of peers increases, the whole system for service capacity will increase accordingly. That is because that each peer can get the file content either from the server or from other peers who have the requested file. Each peer can offer upload and file sharing to other peers as well. However, the free rider and malicious node problems hinder the efficient utilization in P2P networks. Hence, this paper makes improvements on the original BitTorrent by proposing a novel bilateral incentive mechanism (NBIM) to restrain free rider and malicious nodes simultaneously. Furthermore, through the simulator with PeerSim, the simulated results prove that the proposed methodology can effectively restrain the free riders and malicious nodes via punishment and reward mechanisms.

Keywords: Peer-to-Peer, BitTorrent, Game theory

1 Introduction

In the past few years, Peer-to-Peer (P2P) technology developed rapidly and have been applied more and more popular in the world. The technology provides a useful solution as each peer becomes an interconnected node which likes a network server that sharing different resources to each other. As the interconnected application, the use of a centralized administrative system does not exist in resource sharing any more.

In practically, Several P2P protocols, such as BitTorrent [1], Gnutella [2] and Private Tracker are proposed. In the protocols, one of representative P2P file sharing protocols is called BitTorrent (BT). It has been being received a lot of attention in the computer networking researches. The performance (i.e. file downloading time) of BT-like file sharing systems will improve when the number of participants increases, it does not like the traditional way that the performance usually degrades if the number of clients increases. The main reason is relating to its cooperative mechanism. It can be explained intuitively as follows. The original file is split into many small pieces. Each peer can get the file content either from the server who has the original file, or from other peers who have those pieces. Each peer can offer upload and file sharing to other peers as well.

Consequently, each peer can contribute for the other peers by coupling as the service in the network. The BT protocol can successfully configure each peer as a client and a server at the same time. Thus, as the number of peers increases, the whole system for service capacity will increase accordingly.

Though P2P file sharing system is acclaimed, it still has several issues such as free rider and malicious node phenomenon. In respect of free rider node, the definition is that users only download files for themselves without providing uploading bandwidth for other users. In respect of malicious node, it is defined that users provide files that are inauthentic and low quality for downloading will make general users have the bad experience. Both free rider and malicious node have a problem at the service and hinder the efficient utilization of P2P networks. Hence to make improvements on the original BitTorrent to restrain free rider and malicious nodes simultaneously. To fulfill the ultimate objective, we need to achieve the following goals.

(1) To investigate the operation of existing P2P architectures.

(2) To analyze malicious behaviors and free riders in P2P file sharing system.

(3) To propose a new P2P file sharing system. The proposed system can increase the efficient utilization of P2P networks and achieve the requirements of restraining free rider and malicious nodes.

The rest of this paper is organized as follows. Section 2 provides BitTorrent introduction of P2P, overview of social network and evolutionary game

*Corresponding Author: Wei-Tsong Lee; E-mail: wtlee@mail.tku.edu.tw
DOI: 10.3966/160792642019092005011

theory. Section 3 describes the detailed design of the proposed system and implementation of the various conditions in the proposed system. The proposed system characteristics analysis and application of game theory is discussed as well. Section 4 consists of the simulation environment, simulation tool and simulation conditions. Two simulation scenarios and seven conditions are performed and discussed. Finally, Section 5 provides the conclusion.

2 Background and Related Work

2.1 BitTorrent Introduction of P2P

At first the architecture of BitTorrent (BT) in network is different from the traditional network based on client-server system. The key is that each node plays roles of client and server in the network at the same time. According to the dependability properties of P2P system classified these logical overlays into three main architectures: centralized, decentralized, and hybrid decentralized. One of hybrid decentralized P2P architectures is BT that many people know. The operation in BT is shown in Figure 1.

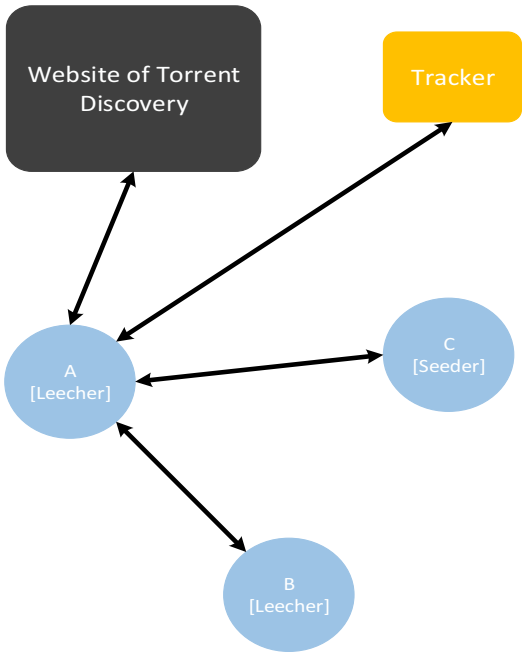

Figure 1. BT Architecture

BT is a P2P protocol that utilizes the sources of peers to distribute vast files efficiently. Peers can connect to each other directly to upload and download sections of a vast file. The protocol also makes a use of the tit-for-fat mechanism to provide altruistic peers with high download rates and penalize egoistic behavior [3-4]. It is a crucial for the BT network with fundamental fairness to have the tit-for-fat mechanism.

According to [4], peers in BT choose two strategies: selective uploading and non-discriminative uploading, as known as the tit-for-fat strategy in the BT protocol. The higher proportion of peers that use the non-discriminative uploading in the system results in better system performance but worse the system fairness since those peers do not exactly get corresponding payoff in return. Contrarily, the higher proportion of peers that use the selective uploading in the system leads to higher system fairness but worse system performance. Consequently, it is defective for tit-for-fat mechanism to restrict free riders. In addition, tit-for-fat mechanism cannot restrict malicious nodes.

2.2 Social Network

Social network that likes as Facebook, Twitter and LinkedIn, with the growing popularity, people may have different accounts. These websites provide many services such as creating a public profile within social network, making connection with other users and sharing resource with other users. The level of accessibility of user's profile depends on privacy threshold user sets. According to [5], some social networks are not elastic enough to protect the information of users' profile. Facebook is one of representative social network and it provides rough privacy settings, users should adjust the privacy setting to maintain their privacy threshold. In section of social relation, besides privacy, identification is also an important mechanism. Identification system plays an important role of behavior restriction. In comparison with anonymous identification, the registrable identification is implemented in some proposed mechanisms. Users must be responsible for their identification in P2P file sharing system and can request file they are interested in through social file. Social file is seeded by file provider and consist of creator of file, location on network, file size…etc.

2.3 Evolutionary Game Theory

In past years, a lot of studies and improvements belong to game theory. For instance, since the Nash Equilibrium [6] is hard to compute and does not often depict the best strategy of both behaviors, the concept of Nash equilibrium has gradually progressed toward evolutionary stable strategy and replicator equations. Evolutionary Game Theory (EGT) [7] differs from classical game theory by focusing on the dynamics of strategy change more than the properties of strategy equilibrium. An evolutionary game depicts the models which players select their strategies by the trial-and-error process, therefore they know that some strategies work better than others. Players reproduce and pass on their strategy to their offspring. The population of offspring is related to the average payoff of their parent strategy.

2.4 Previous Study

Many other incentive mechanisms such SFTrust and NIM have been proposed to encourage peers to

cooperate by sharing their upload bandwidth for solving the issue of free rider and malicious node.

2.4.1 SFTrust

In [8], Zhang et. al. discussed SFTrust, a mechanism is a double trust metric model which maintains two trust metrics, one for service trust and the other for feedback trust. It divides service trust from feedback trust to take full excellence of all agents' service abilities even in the presence of fluctuating feedback. In this model, recommendation is aggregated through local broadcasting which can be really time-consuming. Moreover, recommendation should come from agents who have firsthand experience [9]. SFTrust computes service trust as a weighted average of recommendation trust and local trust. However, the weight itself is static and in consequence, it cannot validly accommodate the experience gained by the evaluating agent over the time. To solve efficiently the free rider and malicious node phenomenon in the current P2P file-sharing applications, this paper integrates pros and cons of various P2P architectures and presents our mechanism in section 3.

2.4.2 Novel Incentive Mechanism

In [10], Wu et al. discussed Novel Incentive Mechanism (NIM). NIM is a hybrid decentralized P2P architecture, likes as BT, has a central server with it. NIM defines mechanisms on social network, and it uses the central server of social network as the server core. Therefore, NIM can restrict the impact of free rider by using the relationships and features of social network users. Because each account of social network is irreplaceable and unique, users must take care their reputation to avoid the malicious behavior. Though NIM has incentive mechanism to restrict free riders, it is not efficient to restrict the malicious node. Many other incentive mechanisms have been proposed to encourage peers to cooperate by sharing their upload bandwidth. NIM could hardly restrict malicious nodes.

3 Methodology

3.1 Novel Bilateral Incentive Mechanism

In this section, we will discuss our methodology "Novel Bilateral Incentive Mechanism (NBIM)". The NBIM presents in this paper is a centralized P2P architecture, like BT, that has trackers. Since NBIM will be deployed within social networks, we use the central server of social network as the trackers for NBIM. The trackers store social files, including user identity, file authentication and social information. Before downloading files, the node must connect to the track to obtain the social file list to find out the source nodes having the requested file chunks.

The system architecture of NBIM is displayed in Figure 2, in which the trackers are the server cores of NBIM. The solid lines refer to communication and control signals between nodes and dash lines refer to P2P file transfers between nodes.

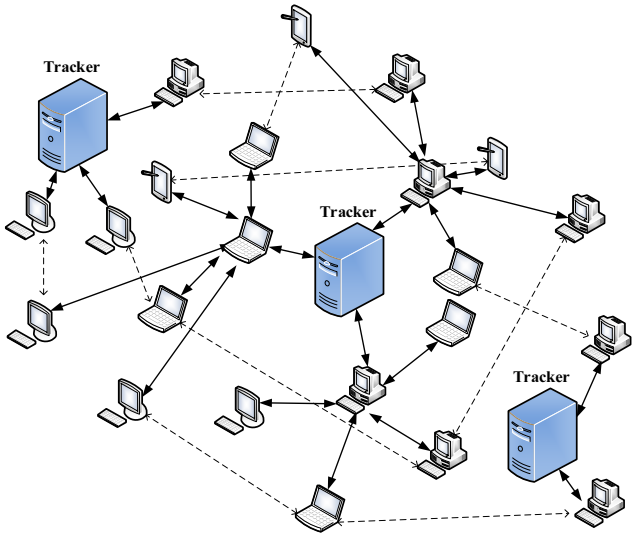

Figure 2. System architecture of NBIM

The main difference between original BT and our proposal is identification. In comparison with anonymous identification, the registration identification is implemented in NBIM. The users that have registered in NBIM must take charge of their inappropriate behavior. The file sharing and downloading process of NBIM are similar to BT. First, the node converts the information of file to share social file and saves it in the tracker of NBIM. If a node wants to download this file, it can ask the tracker for the social file. Like as BT, the node can download the file after giving a list of peers that have the requested file. In addition, NBIM uses "Distributed Hash Table" (DHT) [3, 11] technology to avoid the problem of single point of failure.

3.2 Counter Mechanism

In NBIM, the counters mechanism can make the nodes gain the counters through their own resource and bandwidth in finite cycle. The trackers give the corresponding rewards according to the counters of node in the end of the cycle. In each cycle, NBIM considers several important factors of a node and give the node corresponding counters based on the following weighted value of each factor.

According to [12], since there is a positive correlation between P2P performance and system bandwidth usage amount, system bandwidth usage amount turns into the one of weight values of equation (1). According to [13], the arctangent function can normalize equation (1) and strengthens the fairness of counter mechanism. Nc is the number of counters assigned to the node. Crmax is the maximum counter reward in the file sharing system and usually decided

by system managers. A_b is the number of available bandwidth user can exchange through trackers and E_r is the counter exchange rate in the file sharing system and usually decided by system managers. We illustrate Er through an example and supposing exchange rate is 2, player gain 100 counters in the game. According to equation (2), the player can exchange 200 Mbps available bandwidth with the 100 counters.

E_s is the bandwidth improvement rate of the P2P system that correlates closely with system bandwidth usage amount in recently cycles. B_{now} is the total bandwidth usage amount of the P2P file-sharing system in the end of the current cycle and B_{past} is the total bandwidth usage amount of the P2P file-sharing system in the end of previous cycle. Supposing the total downloaded traffic of NBIM in the previous cycle is higher than the average downloaded traffic, as shown in equation (3), E_s increases and brings about better payoff to the node. Bc refers to the bandwidth contribution of the node. B_{share} is the contributing upload bandwidth of the node and B_{have} is the total available bandwidth of the node. Equation (4) reveals that the closer the upload bandwidth it has, the higher the value of B_c will be. D_p means the data popularity, which correlates with how many times the node's data has been downloaded by each downloader, as shown in equation (5). D_t means the number of download times and D_n means the number of downloaders. D_p is the average downloads per user. The data popularity is recorded by the trackers of NBIM, the counters are managed by the trackers, allowing users to have varied strategic decision-making in NBIM.

$$Nc = \frac{2}{\pi} \times \tan^{-1}(Es \times Bc \times Dp) \times Cr_{\max} \quad \textbf{(1)}$$

$$A_b = Nc \times Er \quad \textbf{(2)}$$

$$Es = \frac{B_{now}}{B_{post}} \quad \textbf{(3)}$$

$$Bc = \frac{B_{share}^{15}}{B_{have}} \quad \textbf{(4)}$$

$$Dp = \frac{D_t}{D_n} \quad \textbf{(5)}$$

In our proposed NBIM, nodes get more counters by contributing resources to system so that they can gain more bandwidth by the tracker. We illustrate Counter mechanism through an example and supposing every node is rational. Suppose exchange rate, the bandwidth improvement rate of the P2P system, system bandwidth usage amount in the end of the previous cycle and maximum counter reward are 2, 1.5, 75 and 90 respectively. For instance, there are two nodes A and B. First, they have 100 Mbps available bandwidth respectively. Node A is willing to share resources and node B is a normal user. Node A shares other users in this P2P file-sharing system with the resources it has and contributes its 80 Mbps available bandwidth to upload its resources. Just right, Node B is interested in one of the resources node A shares and downloads twice the file it is interested with 80 Mbps download bandwidth.

The above condition can draw several conclusions. Since node A contributed the 80 Mbps available bandwidth it has, the Bc of node A is 7.15. The D_p of node A is 2 because node B has downloaded twice from node A. Therefore node A can gain 174 Mbps available bandwidth. The friendly behavior of node A result in not only other user have good experience in this P2P file-sharing system but also improving indirectly system bandwidth usage amount(80 Mbps upload bandwidth + 80 Mbps download bandwidth). Due to the improvement of system bandwidth, the E_s also increases from 1.5 to 2.1. The E_s of the next cycle is 2.1. Consequently, those nodes help each other to not only obtain resources but also have great experience. The friendly behavior of nodes promotes the bandwidth usage amount. P2P file-sharing system can give users better rewards. NBIM realizes the virtuous cycle between users in P2P file-sharing system and P2P file-sharing system. In the method of NBIM, it is encouraged that increasing the sharing times from every node. If the node contributes more by the sources of file-sharing in network, the contributing node will be rewarded with more bandwidth at downloading the expected data. As well as that node will be remarked as "Friendly Node".

3.3 Reward and Punishment Mechanism

The NBIM presented in this paper refers to the behavior of users to give. them a reward or punishment. The Reward and Punishment mechanism has two main systems such bandwidth contribution system and evaluation system. In NBIM, the peers can be divided into four kinds of nodes: malicious node, free rider, normal node and friendly node according to the definitions in Table 1. These kinds of node have respective properties. We illustrate their properties separately. Normal node is the user has no extreme behavior. Friendly node is the user willingly contributes resource he has. Free rider is the user enjoys the benefits of an activity without paying for it. Malicious node is the user has malevolent behavior such as disperse virus file. In order to determine properties of node, we define the friendly threshold, mean threshold and file authentication. Friendly threshold is the boundary utilized to decide the node is normal node or friendly node and mean threshold is the boundary utilized to decide the node is normal node or free rider. File authentication is the integer divided sum of evaluation of downloaders by number of evaluation and the result of the calculation is called "FA" and Bc

refers to the bandwidth contribution of the node, as shown in equation (4). File authentication is the boundary utilized to decide the node is normal node or malicious node.

Table 1. Definition of node type

	Definition
Friendly-nodes	$Bc \geq FriendlyThreshold$
Normal-nodes	$MeanThreshold < Bc < FriendlyThreshold$
Free-riders	$MeanThreshold < Bc$
Malicious-nodes	$FA < 0$

Trackers can differentiate friendly node, normal node and free rider according to bandwidth contribution, the friendly threshold, and mean threshold. Trackers will give corresponding rewards or punishments to them in terms of equation (2). The experiment demonstrates when the friendly threshold and mean threshold is equal to 1.2 and 0.6 respectively, behavior judgement of tracker approach to reality closely.

Figure 3 depicts the flow diagram of Bandwidth Contribution system in terms of users. We illustrate Bandwidth contribution system through an example. Suppose exchange rate, the bandwidth improvement rate of the P2P system and maximum counter reward are 1, 1.5 and 90 respectively, there are three nodes A, B and C.

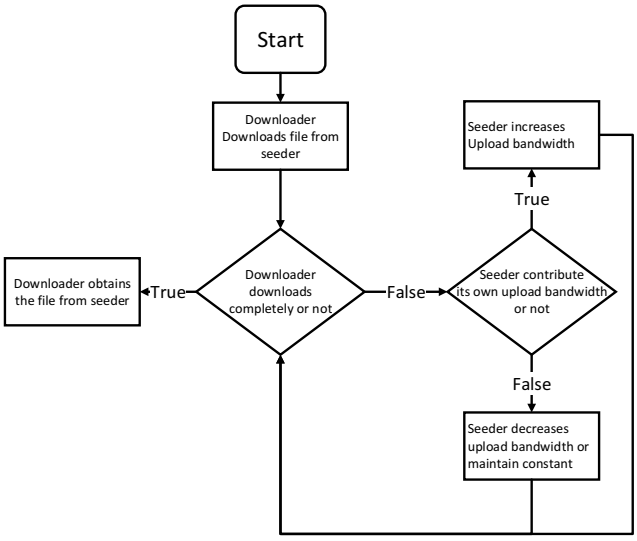

Figure 3. System flow diagram of bandwidth contribution mechanism in terms of user

The node A has 100Mbps bandwidth totally and contributes its 80 Mbps bandwidth. The popularity of data the node shares is 1.03. The result shows that the node can obtain 60 Mbps available bandwidth because it voluntarily contributes its bandwidth to gain 85 counters. The Bc of node A is 7.16 and it is greater than friendly threshold. Consequently, the node A we call friendly node.

The node B has 100Mbps bandwidth totally and contributes its 22 Mbps bandwidth. The popularity of data the node shares is 1.03. The result show that the node has no reward from system because the bandwidth it contributes is not enough to get reward. The Bc of node B is 1.03 and it is between friendly threshold and mean threshold. Consequently, the node B we call normal node.

The node C has 100Mbps bandwidth totally and contributes its 15 Mbps bandwidth. The popularity of data the node shares is 1.03. The result shows that the available 42 Mbps bandwidth of node C is retrieved by system because the bandwidth it contributes is not enough to system demand. The Bc of node B is 0.58 and it is smaller than mean threshold. Consequently, the node C we call free rider.

In the portion of malicious node, after file downloader obtain the files, it can give seeders evaluation. If the files are authentic file or computer virus, downloader can give seeders evaluation. The evaluation of downloader is validation or incorrectness. The validation will increase the file authentication value of seeders by one and incorrectness will decrease the file authentication value of seeders by one. Therefore, the trackers collect all evaluations and divide sum of evaluation by the number of evaluations, the result of the calculation is called "file authentication". Trackers judge malicious node by file authentication. If the user is judged to be malicious node by tracker, he will be retrieved its half available bandwidth by tracker. Figure 4 depicts the flow diagram of Evaluation system in terms of users and the whole process of NBIM is depicted in Figure 5.

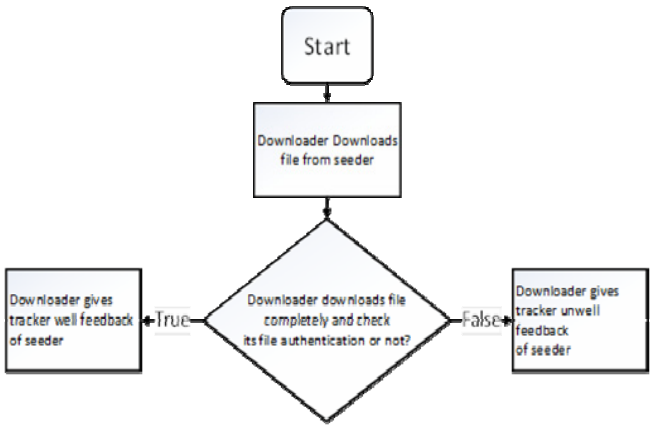

Figure 4. System flow diagram of evaluation system in terms of user

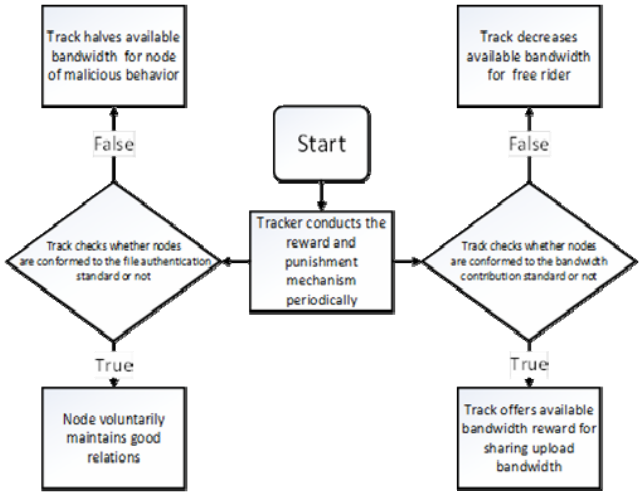

Figure 5. System flow diagram of NBIM

3.4 Incentive Mechanism Analysis

To prove the incentive effectiveness of NBIM on promoting nodes to contribute their available bandwidth, we analyze node behaviors by evolutionary game theory and discuss the system fairness in NBIM. Evolutionary game theory is made for the use of studying and predicting the evolution of social interactions. As time goes on, the behaviors of interacting nodes keep evolving and influencing the nodes. The assumption is that the node has good behaviors can reproduce in proportion to their average fitness such that the node has good behaviors become a large number over time.

For example, we analyze the behavior of both player A and the player B in NBIM with game theory. We assume that nodes are rational can choose the strategies that can maximize their benefit. Table 2 lists their corresponding payoff after making different strategies. At first, we define notation in an interaction between players.

Table 2. Payoff table of the example

		Player B	
		Cooperation	Non-cooperation
Player A	Cooperation	$B_A + r_{Ab}, B_B + R_{Bb}$	$B_A + R_{Ab}, B_B - P_{Bb}$
	Non-cooperation	$B_A - r_{Ab}, B_B + R_{Bb}$	$B_A + P_{Ab}, B_B - P_{Bb}$

Bi is the available bandwidth of player i and Rib is the reward of player i and will be given available bandwidth by bandwidth contribution system. Pib is the punishment of player i and will be retrieved available bandwidth by bandwidth contribution system or evaluation system. The strategy of cooperation is to contribute the bandwidth of the node and will help each other obtain file as soon as possible. The strategy of non-cooperation is to enjoy the upload bandwidth benefits of other node without contributing for it or spread virus and will damage experience of user. Based on the above design, the overall benefits between players after one interaction are depicted in Table 2.

We demonstrate the effectiveness of incentive mechanism through following discussion. There are two groups of users in NBIM. One group is the set of friendly users is called "group A" and another is the set of malicious users and free riders is called "group B". The user of group A is like player A of above example and always shares his own resource with other users. The user of group B is like player B of above example and often enjoys the upload bandwidth benefits of other node without contributing for it or spreads virus and will damage experience of user.

In NBIM, the users voluntarily contributing their own resource will be given corresponding reward; on the other hand, the users enjoying the benefits without contributing for it and the users destroying the experience of other user will be inflicted corresponding punishment. Above condition can corresponds the instance of evolutionary game theory. The behavior of sharing resource can be considered cooperation selection and the behavior damaging experience of users can be considered non-cooperation selection. Since the user of group A frequently selects cooperation strategy, he/she will gain the reward of R_{Ab}; on the other hand, the user of group B is always inflicted punishment of P_{Bb} because he/she often selects non-cooperation strategy. After several interaction, user knows that cooperation strategies work better than others. User reproduces and passes on their strategy to their offspring. Consequently, the tendency of strategy selection of user will toward gradually cooperation strategy.

The NBIM presented in this paper is a fair P2P system. First, the nodes are rational and have the same initial value of system. In NBIM, the counters mechanism can make the nodes gain the counters through their own resource and bandwidth. The trackers give the corresponding rewards according to the counters of node; however, if some nodes have amounts of resource and bandwidth and gain more and more rewards according to their own huge resources at the beginning, then the disadvantaged group cannot gain corresponding rewards because the former create the snowball effect.

NBIM uses the arctangent function to normalize counters mechanism and strengthens the fairness of the P2P system. The curve of arctangent is displayed in Figure 6. Even if the node has amount of resources and bandwidth at beginning, they cannot gain lots of rewards because the reward range tends to grow limited. This proves NBIM can prevent the snowball effect and improve the fairness of the P2P system.

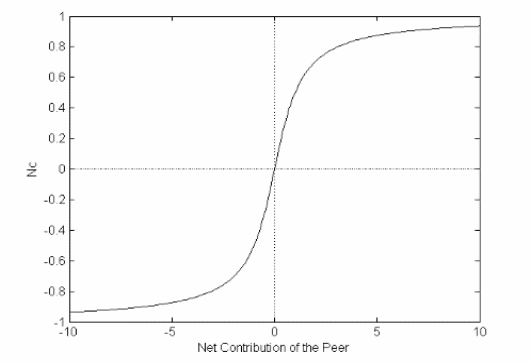

Figure 6. Curve of arctangent function

We illustrate why NBIM can prevent snowball effect through Figure 7. The solid curve is the equation (1) without arctangent and will grow fast when users continuously contribute many resources. Consequently, the above condition will lead to snowball effect. The dotted curve is the equation (1) with arctangent and will prevent snowfall effect when wealth user continuously contributes many resources. Therefore, users cannot continuously obtain a great quantity of reward by contributing many resources.

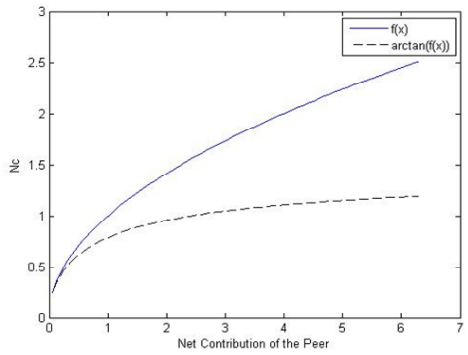

Figure 7. Comparison graph

The Trackers trace the nodes who have crime behavior in each time slot. If the nodes still have crime behavior, the tracker will give them double penalty. Recidivist punishment can inhibit the node who has crime behavior such as malicious node or free rider effectively.

4 Simulation Results and Performance Analysis

4.1 Simulation Environment

In our simulated scenarios, we assume that all system users are rational players. Because our proposed NBIM is based on social networks, packet loss between nodes or between nodes and servers are not taken into account. Therefore, all nodes exist in the network since the beginning and will stay even after downloads are completed. The first scenario is single behavior mode in every circumstance of each mechanism. The first condition in the first scenario is the stand comparative condition. The second and third condition in the first scenario is in order to analyze performance of each mechanism when the number of free rider or malicious node is increased. The second and third condition in the first scenario is in order to analyze performance of each mechanism when the number of free rider and malicious node is increased substantially. The first condition in the second scenario is in order to analyze performance of NBIM when users have multi-behaviors. The scenarios are displayed in Table 3 to Table 4.

Table 3. The first simulation scenario

Condition	Normal	Friendly	Free rider	Malicious
1	60%	20%	10%	10%
2	60%	20%	5%	15%
3	60%	20%	15%	5%
4	40%	20%	20%	20%
5	30%	20%	25%	25%

Table 4. The second simulation scenario

Condition	Normal	Friendly	Free rider	Malicious
1	60%	20% (10% Mal)	10%	10%

4.2 P2P Simulator

In our simulated environment we had to work with the PeerSim environment, one of the leading P2P simulators and used by researchers from all around the world. [14-17].

PeerSim is written in the Java language. The philosophy of PeerSim is to use a modular approach, as the preferred way of coding with it is to re-use existing modules such as BitTorrent, bandwidth management protocol and Chord. The default simulation parameters used in the simulations are summarized in Table 5.

Table 5. Simulation parameters

Definition	Value
Round	200
Record time	10 sec
Number of peers	1000
Number of trackers	100
File size	250 KB
Block size	256B
Initial Bandwidth	2Kb
File Authentication	0
Friendly threshold	1.2
Mean threshold	0.8
Maximum counter reward	90

4.3 Simulation Results and Performance Analysis

In this section, we analyze utilization of NBIM

against original-BT, NIM, and SFTrust through two scenarios. The first scenario is single behavior mode and the average bandwidth of every kinds of node in every circumstance of each mechanism are shown as Figure 8 to Figure 12. The second scenario is multiple-behavior mode and the average bandwidth of every kinds of node in every circumstance of NBIM is shown as Figure 13.

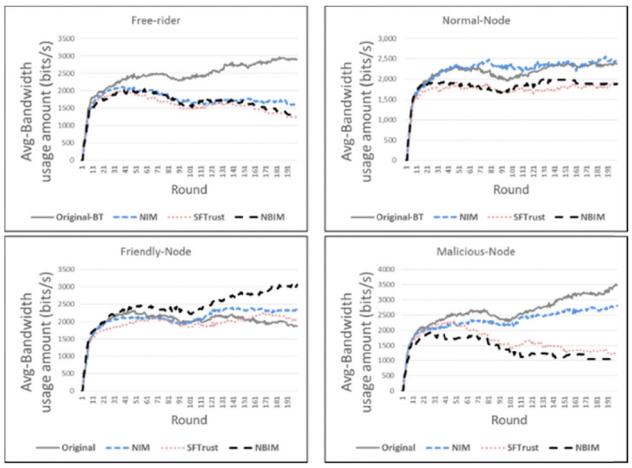

Figure 8. The node classified result of condition 1

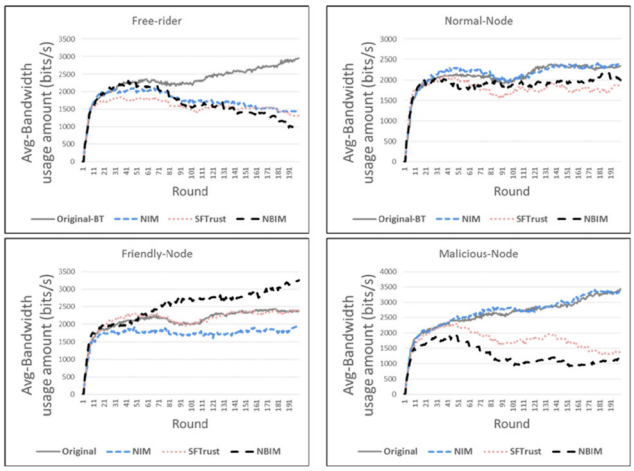

Figure 9. The node classified result of condition 3

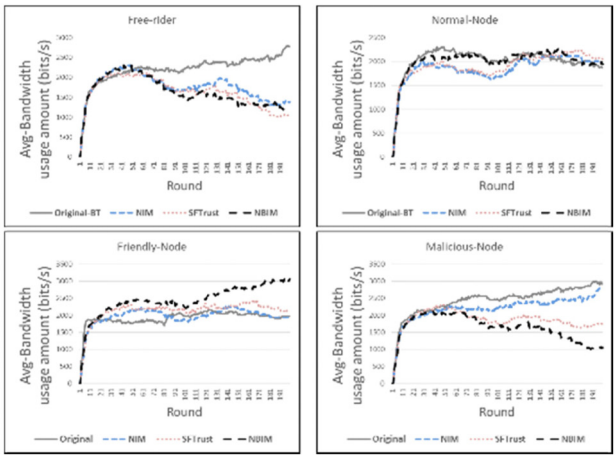

Figure 10. The node classified result of condition 3

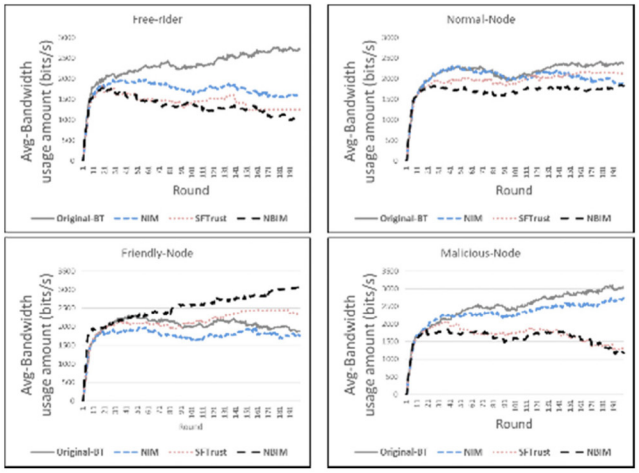

Figure 11. The node classified result of condition 4

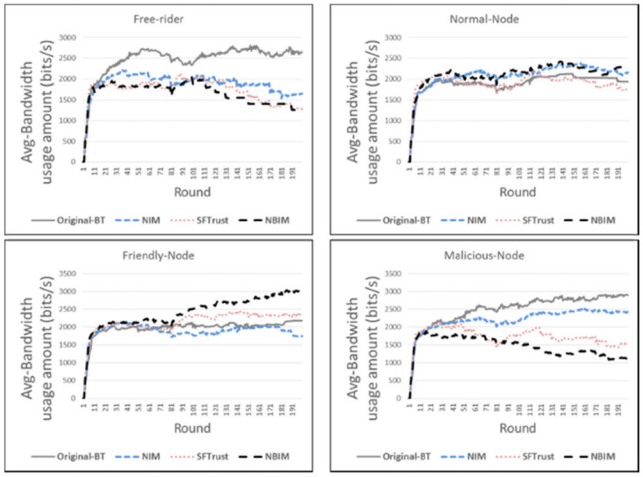

Figure 12. The node classified result of condition 5

The simulation results are arranged as shown in Table 6 to Table 10. In Table 6 to Table 10, each condition and percentage indicate the variances between Original-BT and other mechanism. Comparison percentage is displayed in the following equation:

$$\text{Comparison Percentage} = \frac{\text{Other Mechanism}}{\text{Original BT}} \quad \textbf{(6)}$$

Table 6. Average bandwidth in condition 1 comparison

	Condition 1			
	Original-BT	NIM	SFTrust	NBIM
Free rider (bits/s)	2435	1753	1660	1593
Comparison percentage	100%	72%	68%	65%
Bandwidth variant	0%	-28%	-35%	-32%
Malicious-node (bits/s)	2602	2302	1629	1375
Comparison percentage	100%	88%	63%	53%
Bandwidth variant	0%	-12%	-37%	-47%

Table 6. Average bandwidth in condition 1 comparison (continue)

Condition 1				
	Original-BT	NIM	SFTrust	NBIM
Friendly-node (bits/s)	2012	2096	1931	2439
Comparison percentage	100%	104%	96%	121%
Bandwidth variant	0%	4%	-4%	21%

Table 7. Average bandwidth in condition 2 comparison

Condition 2				
	Original-BT	NIM	SFTrust	NBIM
Free rider (bits/s)	2326	1727	1575	1650
Comparison percentage	100%	74%	68%	71%
Bandwidth variant	0%	-26%	-32%	-29%
Malicious-node (bits/s)	2615	2673	1756	1259
Comparison percentage	100%	102%	67%	48%
Bandwidth variant	0%	2%	-33%	-52%
Friendly-node (bits/s)	2112	1727	2136	2497
Comparison percentage	100%	82%	101%	118%
Bandwidth variant	0%	-18%	1%	18%

Table 8. Average bandwidth in condition 3 comparison

Condition 3				
	Original-BT	NIM	SFTrust	NBIM
Free rider (bits/s)	2196	1756	1632	1629
Comparison percentage	100%	80%	74%	74%
Bandwidth variant	0%	-20%	-26%	-24%
Malicious-node (bits/s)	2430	2196	1865	1632
Comparison percentage	100%	90%	77%	67%
Bandwidth variant	0%	-10%	-23%	-33%
Friendly-node (bits/s)	1910	1960	2128	2439
Comparison percentage	100%	103%	111%	128%
Bandwidth variant	0%	3%	11%	28%

Table 9. Average bandwidth in condition 4 comparison

Condition 4				
	Original-BT	NIM	SFTrust	NBIM
Free rider (bits/s)	2313	1723	1334	1442
Comparison percentage	100%	75%	58%	61%
Bandwidth variant	0%	-25%	-42%	-39%
Malicious-node (bits/s)	2470	2278	1663	1595
Comparison percentage	100%	92%	67%	65%
Bandwidth variant	0%	8%	-33%	-35%
Friendly-node (bits/s)	2012	1756	2126	2497
Comparison percentage	100%	87%	106%	124%
Bandwidth variant	0%	-13%	6%	24%

Table 10. Average bandwidth in condition 5 comparison

Condition 5				
	Original-BT	NIM	SFTrust	NBIM
Free rider (bits/s)	2469	1880	1723	1653
Comparison percentage	100%	76%	70%	67%
Bandwidth variant	0%	-24%	-30%	-33%
Malicious-node (bits/s)	2489	2200	1621	1450
Comparison percentage	100%	88%	70%	58%
Bandwidth variant	0%	-12%	-30%	-42%
Friendly-node (bits/s)	1963	1879	2135	2418
Comparison percentage	100%	96%	109%	123%
Bandwidth variant	0%	-4%	9%	23%

Bandwidth variant means the available bandwidth percentage difference between Original-BT and other mechanism. The available bandwidth per second of particular type-player is described as type-player (bits/s), e.g., Free-rider (bits/s).

4.3.1 Simulation Analysis of Single Behavior

The condition 1 of single behavior peer simulation is shown in Figure 8 and the node proportions of normal node, friendly node, free rider and malicious node are 60%, 20%, 10%, and 10% respectively.

In the condition 1 of single behavior peer simulation, we can observe that original-BT does not restrain free rider and malicious node and consequently they can gain amount of bandwidth improperly. NIM restrains free rider but not malicious node. NBIM and SFTrust restrain free rider and malicious node bilaterally. In respect of free rider, SFTrust can restrain free rider through decreasing their 35% available bandwidth. SFTrust restrain free rider effectively than NBIM and NIM; however, it is not fair for node to restrain free rider by SFTrust because SFTrust stop services when recognize node as free rider. In respect of malicious node, NBIM make use of evaluation system to restrict malicious node. The 47% available bandwidth of malicious node is decreased by NBIM. NBIM restrict malicious node effectively than SFTrust and NIM. In respect of friendly node, NBIM make use of reward and punishment mechanism to improve the sharing and cooperative behavior. Friendly node can obtain 21% available bandwidth through reward and punishment mechanism.

The condition 2 of single behavior peer simulation are shown in Figure 9 and the node proportions of normal node, friendly node, free rider and malicious node are 60%, 20%, 5%, and 15% respectively.

In the condition 2 of single behavior peer simulation, obviously we can observe that NIM cannot restrain malicious at all when the number of malicious node increase; therefore, malicious node can gain amount of bandwidth improperly. NIM restrains free rider but not malicious node. NBIM and SFTrust restrain free rider and malicious node bilaterally. In respect of free rider, SFTrust can restrain free rider through decreasing their 32% available bandwidth. In respect of malicious node, NBIM make use of evaluation system to restrict malicious node. The 52% available bandwidth of malicious node is decreased by NBIM. Even through the proportion of malicious node is increased, NBIM still can restrict malicious nodes efficaciously. In respect of friendly node, NBIM make use of reward and punishment mechanism to improve the sharing and cooperative behavior. Friendly node can obtain 18% available bandwidth through reward and punishment mechanism.

The condition 3 of single behavior peer simulation is shown in Figure 10 and the node proportions of normal node, friendly node, free rider and malicious node are 60%, 20%, 15%, and 5% respectively.

In the condition 3 of single behavior peer simulation, obviously we can observe that SFTrust restrain free rider obviously when the proportion of free rider increases. In respect of free rider, SFTrust can restrain free rider through decreasing their 26% available bandwidth. Even through the proportion of free rider is increased, all proposals still can restrict free rider. In respect of malicious node, NBIM make use of evaluation system to restrict malicious node. The 33% available bandwidth of malicious node is decreased by NBIM. In respect of friendly node, NBIM make use of reward and punishment mechanism to improve the sharing and cooperative behavior. Friendly node can obtain 28% available bandwidth through reward and punishment mechanism.

The condition 4 of single behavior peer simulation are shown in Figure 11 and the node proportions of normal node, friendly node, free rider and malicious node are 40%, 20%, 20%, and 20% respectively.

In the condition 4 of single behavior peer simulation, obviously we can observe that NIM is unable to restrain free rider gradually when the proportion of free rider increase continuously; on the other hand, NBIM and SFTrust restrain the high proportion of free rider of malicious node effectively.

In respect of free rider, SFTrust can restrain free rider through decreasing their 42% available bandwidth. Even through the proportion of free rider is increased, all proposals still can restrict free rider. In respect of malicious node, NBIM make use of evaluation system to restrict malicious node. The 35% available bandwidth of malicious node is decreased by NBIM. Even through the proportion of malicious node is increased, NBIM also can restrict malicious node efficaciously. In respect of friendly node, NBIM make use of reward and punishment mechanism to improve the sharing and cooperative behavior. Friendly node can obtain 24% available bandwidth through reward and punishment mechanism.

The condition 5 of single behavior peer simulation are shown in Figure 12 and the node proportions of normal node, friendly node, free rider and malicious node are 30%, 20%, 25%, and 25% respectively.

In the condition 5 of single behavior peer simulation, obviously we can observe that NBIM restrain free rider and malicious node better than SFTrust in this condition. In the foregoing condition SFTrust restrain free rider better than NBIM; however, NBIM restrain free rider better than SFTrust after the proportion of free rider arrives at 25%.

In respect of free rider, NBIM can restrain free rider through decreasing their 33% available bandwidth. Even through the proportion of free rider is increased, all proposals still can restrict free rider. In respect of malicious node, NBIM make use of evaluation system to restrict malicious node. The 42% available bandwidth of malicious node is decreased by NBIM. Even through the proportion of malicious node is increased, NBIM also can restrict malicious node efficaciously. In respect of friendly node, NBIM make use of reward and punishment mechanism to improve the sharing and cooperative behavior. Friendly node can obtain 23% available bandwidth through reward and punishment mechanism.

We classify all simulation results and make a conclusion. In most part of simulation conditions, SFTrust restrain free rider effectively better than NBIM and NIM; however, it is not fair for node to

restrain free rider by SFTrust because SFTrust stop services when recognize node as free rider. SFTrust do not make node correct it error and make a fresh at all. NBIM and NIM restrain fee rider fairly better than SFTrust and NBIM is better than NIM. No matter what free rider or malicious node, NBIM is more effective than NIM, and also productive than SFTrust in rare part of simulation conditions. For example, NBIM restrains free rider better than SFTrust in condition 6 of single behavior mode. On the other hand, NBIM restrains malicious node better than other mechanisms in all case.

Finally, the average bandwidth of friendly node only increases in every circumstance of NBIM because friendly node can gain counters to obtain available bandwidth by the reward mechanism of NBIM.

4.3.2 Simulation Analysis of Multiple-Behavior

The average bandwidth curve in the second scenario is shown as Figure 13 and the node proportions of normal node, friendly node, free rider and malicious node are 60%, 20%, 10%, and 10% respectively. 10 percent of friendly node includes malicious behavior. We can make a conclusion through Table 11. NBIM can restrain multiple-behavior node effectively. Even though friendly node who has malicious behavior is willing to sharing its own bandwidth to increase performance of system, friendly node who has malicious behavior is still punished as because of malicious file they shared.

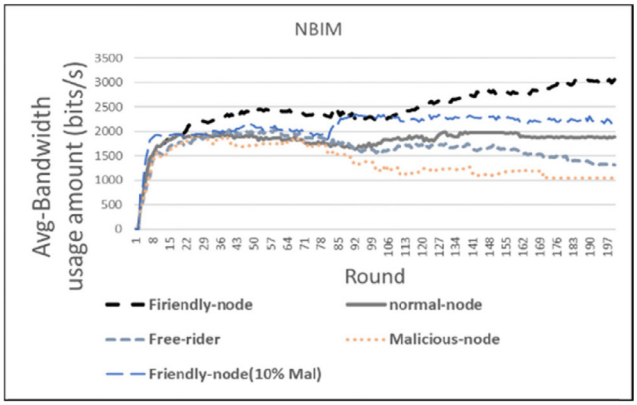

Figure 13. The node classified result of condition 6

Table 11. Average bandwidth of multiple behavior comparison

	Friendly node	
Condition	Condition 1	Condition 2
Bandwidth (bits/s)	2439	2114
Comparison percentage	100%	87%
Bandwidth variant	0%	-13%

5 Conclusion

In this paper, as to solve the free rider and malicious node phenomenon in the current P2P file-sharing applications, this paper integrates pros and cons of various P2P architectures and presents a methodology of Novel Bilateral Incentive Mechanism (NBIM) which is based on social network and evolutionary game theory for P2P file-sharing.

Our simulation results and scenario analyses show that by considering different conditions and contributions of all players and providing players with more strategy space of game theory by counters. Our proposed methodology with NBIM can restrain the number of free riders and malicious nodes efficiently; also, to encourage the nodes to contribute resources as much as possible, distribute the resources to all nodes more fairly via punishment and reward mechanisms. Moreover, the simulated results prove that the proposed mechanism can restrain average 31 percent behavioral capability of free riders and average 41 percent behavioral capability of malicious nodes to improve the performance in P2P network.

For future work, it will be to quantify the parameters concretely and determine the range of the parameters for counters in case of any unexpected parameters affect the system excessively. Moreover, users' habits with friendship building and utilization status in social networks are remained as future work.

Acknowledgements

This work is supported partially by the Ministry of Science and Technology, Taiwan, R.O.C., under the grant No. MOST 107-2221-E-032-020.

References

[1] B. Cohen, Incentives Build Robustness in BitTorrent, *Workshop on Economics of Peer-to-Peer systems*, Berkeley, California, USA, 2003, pp. 68-72.

[2] M. Ripeanu, Peer-to-Peer Architecture Case Study: Gnutella Network, *Proceedings First International Conference on Peer-to-Peer Computing*, Linkoping, Sweden, 2001, pp. 99-100.

[3] M. Steiner, T. En-Najjary, E. W. Biersack, A Global View of KAD, *Proceedings of the ACM Internet Measurement Conference (IMC)*, San Diego, California, USA, 2007, pp. 117-122.

[4] B. Fan, J. C. S. Lui, D.-M. Chiu, The Design Trade-Offs of BitTorrent-Like File Sharing Protocols, *IEEE/ACM Transactions on Networking (TON)*, Vol. 17, No. 2, pp. 365-376, April, 2009.

[5] A. Ho, A. Maiga, E. Aïmeur, Privacy Protection Issues in Social Networking Sites, *IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, Morocco, 2009, pp. 271-278.

[6] M. J. Osborne, *An Introduction to Game Theory*, Oxford University Press, 2009.

[7] J. W. Weibull, *Evolutionary Game Theory*, M. I. T. Press, 1995.

[8] Y.-C. Zhang, S.-S. Chen, G. Yang, SFTrust: A Double Trust Metric Based Trust Model in Unstructured P2P System, *IEEE International Symposium on Parallel & Distributed Processing*, Rome, Italy, 2009, pp. 1-7.

[9] J.-J. Qi, Z.-Z. Li, Managing Trust for Secure Active Networks, *Multi Agent Systems and Applications IV*, Budapest, Hungary, 2005, pp. 628-631.

[10] 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, pp. 47-55, May, 2014.

[11] M. Mani, A.-M. Ngyuen, N. Crespi, What's Up: P2P Spontaneous Social Networking, *IEEE International Conference on Pervasive Computing and Communications*, Galveston, Texas, USA, 2009, pp. 1-2.

[12] D. Qiu, R. Srikant, Modeling and Performance Analysis of BitTorrent-Like Peer-to-Peer Networks, *ACM SIGCOMM Conference*, Portland, Oregon, USA, 2004, pp. 367-378.

[13] F. Qin, J. Liu, L. Zheng, Improving Robustness and Fairness on BitTorrent-Like P2P Systems, *Fourth International Conference on Communications and Networking*, Xian, China, 2009, pp. 1-5.

[14] R. Centeno, H. Billhardt, R. Hermoso, Persuading Agents to Act in The Right Way: An Incentive-based Approach, *Engineering Applications of Artificial Intelligence*, Vol. 26, No. 1, January 2013, pp. 198-210.

[15] K. Islam, *A Cost-Effective Distributed Architecture for Content Delivery and Exchange over Emerging Wireless Technologies*, Ph.D. Thesis, George Mason University, Fairfax, Virginia, USA, 2013.

[16] H. Salah, M. Eltoweissy, Towards A Personalized Trust Management System, *International Conference on Innovations in Information Technology (IIT)*, Abu Dhabi, United Arab Emirates, 2012, pp. 373-378.

[17] Y. Zhu, Y. Yang, Reseach on LT-based Communication between Peers in BT System, *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, April 2012, pp. 1980-1983.

Biographies

Wei-Chun Wong received his M.S. degree in Electrical Engineering from Tamkang University, Taiwan. His research interests include multimedia systems, wireless networks.

Wei-Tsong Lee received his B.S., M.S. and Ph.D. degrees in Electrical Engineering from National Cheng Kung University, Tainan, Taiwan. He is currently a professor in the Department of Electrical and Computer Engineering, Tamkang University. His research interests include computer architecture, micro-processor interface and computer networks.

Hsin-Wen Wei received the Ph.D. degree in Computer Science from National Tsing Hua University, Hsinchu, Taiwan in 2008. She is currently an Associate Professor in the Department of Electrical and Computer Engineering, Tamkang University. Her research interests include storage systems, cloud computing, wireless networking, and real-time systems.

Yao-Chiang Yang received his M.S. degree in Electrical Engineering from Tamkang University, Taiwan. He is currently a doctoral student in the Department of Electrical and Computer Engineering, Tamkang University, New Taipei City, Taiwan, His research interests include wireless networking, and computer networks.

Vooi-Voon Yap is currently an Associate Professor and Dean of Faculty of Engineering and Green Technology at Universiti Tunku Abdul Rahman (UTAR). He received his PhD in Wavelet-based Image Compression for Mobile Devices from Middlesex University, London. He has over 30 years teaching experience in colleges and universities both in the United Kingdom and Malaysia, with special interest in embedded systems and video surveillance. He is also a Fellow of the Institution of Engineering and Technology (FIET) and a Charter Engineer (CEng).