情報保護學會論文誌
第20卷 第3號, 2010. 6

Kad 네트워크에서 게임 이론을 바탕으로 한 인센티브 메커니즘*

왕 서,† 니 영 청, 양 대 헌‡
인하대학교 정보보호연구실

Incentive Mechanism based on Game Theory in Kad Network*

Xu Wang,† YongQing Ni, DaeHun Nyang‡
Information Security Research Laboratory INHA University

요 약

Kad 네트워크는 파일 공유 시스템 중 가장 널리 알려진 네트워크이다. 파일 공유 시스템은 사용자의 일방적 파일 다운로드 받기, 가짜파일 업로드하기, 바이러스 배포하기 등에 사용 되는 등의 문제를 가지고 있고, 이러한 문제점을 극복하기 위하여, 이 논문에서는 게임 이론을 바탕으로 하는 인센티브 메커니즘을 제안한다. 이 메커니즘은 Kad 사용자를 위하여 보다 안정적이고 효율적인 네트워크 환경을 만들어 준다. 즉, 쓸모 없고 위험한 파일 등을 제공하는 다른 사용자들이 처벌받는 것에 반하여, 가치 있는 리소스를 공유한 사용자는 신용이 증가하는 대가를 받는다. Kad 네트워크에서 이 인센티브 메커니즘은 사용자의 악의적인 행동을 찾거나 방지하고 사용자들 사이에서의 정직한 통신을 장려하는데 도움을 준다.

ABSTRACT

The Kad network is a peer-to-peer (P2P) network which implements the Kademlia P2P overlay protocol. Nowadays, the Kad network has attracted wide concern as a popular architecture for file sharing systems. Meanwhile, many problems have been coming out in these file sharing systems such as freeriding of users, uploading fake files, spreading viruses, and so on. In order to overcome these problems, we propose an incentive mechanism based on game theory, it establishes a more stable and efficient network environment for Kad users. Users who share valuable resources receive rewards by increasing their credits, while others who supply useless or harmful files are punished. This incentive mechanism in Kad network can be used to detect and prevent malicious behaviors of users and encourage honest interaction among users.

Keywords: Kad, P2P, incentive mechanism, game theory

I. Intrduction

With the development of information technology and internet, more and more information resources have been provided to online network, thus, how to get valuable information on the enormous Internet has become an increasingly concerned problem. P2P network, as a rising network computing model, moved the traditional server-and-client network model into the distributed network model. P2P becomes a powerful emerging networking paradigm which permits sharing of unlimited data and computational resources in a distributed, fault-tolerant, scalable, and

접수일(2009년 11월 26일), 수정일(1차: 2010년 3월 20일, 2차: 2010년 4월 9일), 게재확정일(2010년 5월 11일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, wmingxuan@hotmail.com
‡ 교신저자, nyang@inha.ac.kr

flexible manner. Fortune magazine calls it as one of the four technologies which will affect the future of Internet.

A variety of P2P protocols[1][2][3][4][5][6][7] have been proposed in recent years. One of them protocols is known as Kademlia[1], which is mainly based on using a distributed hash table in the protocol construction. Kademlia protocol was proposed by P. Maymounkov and D. Mazieres in 2002. Also, the protocol used a novel XOR-based technique for resources lookup. Due to its high efficient routing capability with self organizing, scalable and robust properties, many widely deployed structure overlay networks used in the Internet today(i.e. BitTorrent, OverNet and eMule) are based on the Kademlia protocol.

The Kad network is a DHT-based P2P network that implements the Kademlia protocol. Each node in the Kad network has a unique 128-bit identifier (NodeID) which is normally created by IP address. Extended to publish or query scheme, each file will also have a unique FileID which has the same length as the NodeID. The file information will be published to the nodes who have the same or similar NodeID to FileID. In addition, to enhance the search efficiency, each node has several corresponding keywords and each keyword also has a unique hash value which constructs a key-value pair.

Routing in the Kad network is performed using these identifiers and the XOR metric, which defines the distance between two nodes as the bitwise exclusive or (XOR) of these identifiers interpreted as an integer. Routing in Kademlia is done iteratively. A message to a destination key is simply forwarded to one of the peers from the bucket with the longest common prefix to the target key. To store and search a ⟨key, value⟩ pair, a node locates the closest nodes to a key. The k-bucket structure allows Kad network to contact only O(log(N)) nodes during a lookup. This brilliant design provides a highly efficient publish and search scheme.

The rapid growth of Kad network also brings some problems, such as uploading fake files, spreading viruses, freeriding and whitewashing[8]. It is well known that Kad network is widely used as file sharing system. Each user acts as both client and server, it benefits from each other and serves others correspondingly. But, not all of users are selfless. In a technical report [9], it mentioned that there are nearly 70% of users do not want to share any file, about 50% of all file searching responses come from the top 1% of file sharing users. Even worse, a considerable portion of the files which few users are willing to share are fake or infected files. So our target is to encourage users share their own resources and guarantee its quality.

We adopt game-theoretic incentive solution to encourage the cooperation between users. Game Theory[10] is proved as an effective tool to enhance the stability of a system to handle selfish or dishonest users. In particular, we introduce Prisoners' dilemma as a basic framework to achieve our proposal.

In this paper, a game-theoretic incentive mechanism in Kad network is proposed. Our scheme is to encourage the file requester to give the honest evaluation to the files. Meanwhile the file provider should make sure the file is correct and the sharing time of the file is as long as possible. According to this mechanism, we expect to build an honest, high efficient Kad network.

The rest of this paper is organized as follows. Section II, we introduce some related works. The detailed design of our incentive mechanism is described in section III. In section IV we evaluate our proposal by simulation. Finally, we make conclu-

sions and future works in section V.

II. Relative Works

Many works focused on two terms. One is building trust models to support trust establishment, such as reputation based trust mechanisms. The EigenTrust scheme[11] is a distributed and secure method to compute global trust values, based on Power iteration. The author of PeerTrust [12] presents a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system and a decentralized implementation of such a model over a structured P2P network. The PowerTrust[13] system dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. By using a lookahead random walk strategy and leveraging the power nodes, the PowerTrust significantly improves in global reputation accuracy and aggregation speed. The FileTrust[14] classifies reputation objects into a shared resource and a peer respectively. This scheme reduces the ratio of downloading untrustworthy resources and conducts dishonest feedback. R. Zhou and K. Hwang also present GossipTrust[15], the model computes a global reputation vector through a recursive process motivated by aMarkov random walk among nodes of the network. TrustMe[16] offers another approach toward anonymous trust management.

Another solution is to build an incentive mechanism to encourage users to cooperate with each other. To our best knowledge, a micro-payment mechanism[17] is probably the earliest work on designing incentive protocol for P2P network. It relies on a centralized server and uses virtual currency to provide incentive for sharing resource. A first attempt to formally prove the efficiency of such differentiation mechanisms, using a game theoretic framework, has been proposed by Buragohain et al.[18]. The next year, the paper [19] modeled the P2P systems using the Generalized Prisoner's Dilemma(GPD), and proposes the Reciprocative decision function as the basis of a family of incentives techniques. In [20], the authors model the system as an infinitely repeated game. In addition, Richard T. B. Ma and his research team successively published three papers focus on game theoretic approach by providing incentive and service differentiation in P2P Network[21][22][23].

Actually, most of these works discuss trust and incentive mechanisms separately. In a real situation, a trust mechanism without incentive would face lack of users' enthusiasm and sparse relationship of direct trust while an incentive mechanism without trust could induce users' bad behavior. Our work draws inspiration from theses woks, we combine trust and incentive mechanisms and create a more active and trustworthy Kad network based on Game theory.

III. Our Incentive mechanism description

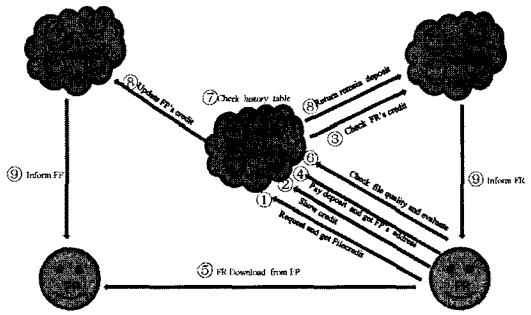
In this section, we first introduce data structure and terminology used in our proposal, which is based on Kad network. Then, we will illustrate interactive processing and algorithm in detail.

3.1 Data Structure and Terminology

There are two basic and crucial concepts should be introduced firstly.

NID: the identity of a node, which has a unique 160-bit length hash value.

FID: 160-bit long unique identifier that denotes a certain file.



[Figure 1] The whole interaction between users

Secondly, five entities act different roles in our proposal.

FP: file provider, acts as server.

FR: file requester, acts as client.

JN: judge node, a group of nodes whose NID are same or similar to a specific FID, that means FP publish its file in JN node.

FPN: file provider's neighbor group, which means FPN's NID similar to FP's NID, and store FP's credit.

FRN: file requester's neighbor group, which means FRN's NID similar to FR's NID, and store FR's credit.

The next, we extend Kad data structure as follows:

Node: ⟨NID, SFNumber, SValue, RValue, Credit⟩

File: ⟨FID, FCredit , STime⟩

We can learn how many numbers of files are shared by node from SFNumber value. SValue stands for the contribution of the node share its files. RValue means reputation value, which denotes the reputation of node. Credit likes a kind of e-currency which is used for insuring a node that has the right to download the resources. Actually, the e-currency can be used on the internet related commercial applications such as shopping on the internet and doing personal investment via internet. It is not the real money but stands for the money. In our paper, the Credit stands for the reputation value.

Meanwhile, FCredit means the quality of file, and it is equal to the cost of file, which FR should pay for download the file. In particular, we confine the FCredit between 0 and 10. STime, it records duration time that a file has been shared, and its unit is hour.

Furthermore, the JN node also stores a history table for the purpose of judging the given evaluation is honest or not. The history table records the feedback which is FR's evaluation to the file according to the file quality: 1 is good and -1 is bad or fake file.

3.2 Incentive Protocol

Based on Kad protocol, our proposal improves validity by adding game theory during the interaction of nodes in Kad network. File verification and user reputation mechanism are founded on game theory is introduced into Kad protocol. The model of the whole interaction is shown in Figure 1 as follows:

The details will be described step by step in the following section.

3.2.1 Interactive Processing

We divide the whole interaction among users into three phases: 3.2.1.1 Query and download phase. 3.2.1.2 Evaluation phase. 3.2.1.3 Update phase.

3.2.1.1 Query and download Phase

Step 1: To download a file, FR sends a request to JN whose NID is the

same or similar to FID of the file. From the active node in JN, FR obtains FCredit that it should pay for downloading the file. FCredit also stands for the quality of the file. If the file quality is high, FR should pay more Credit.

Step 2: FR demonstrates that it has enough Credit to pay for the file. FR shows a certificate to JN.

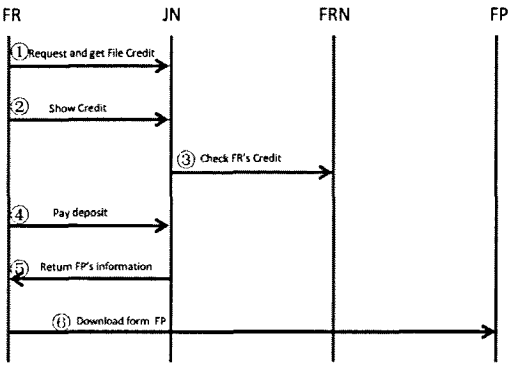
Step 3 & Step 4: JN receives the certificate and then go to FRN to check FR if FR is honest. Because FRN has FR's real credit, JN asks FR to pay 10 Credit as a deposit if FR has enough Credit. After finishing this interaction, JN returns remaining Credit. This step resembles to the relation between bank and depositor in the real world. FRN likes bank which store depositor's saving. FR has certificate like bankbook. JN likes a shop. If the depositor wants to buy something, he first shows his bankbook to the shop, and then the shop goes to bank to check whether the depositor's bankbook is true or not. If he has enough money, business will proceed.

Step 5: After JN gets the FR's deposit, JN returns FP's information such as IP address, UDP port, NID, etc.

Step 6: FR starts to download.

3.2.1.2 Evaluation Phase

Step 1: After finishing download, FR should check the quality of the file and send the evaluation to JN, 1 is good and -1 is bad. There is another case, when FR finished downloading the file, it doesn't evaluate the file, and in this case, JN does not return the deposit to FR as punishment.

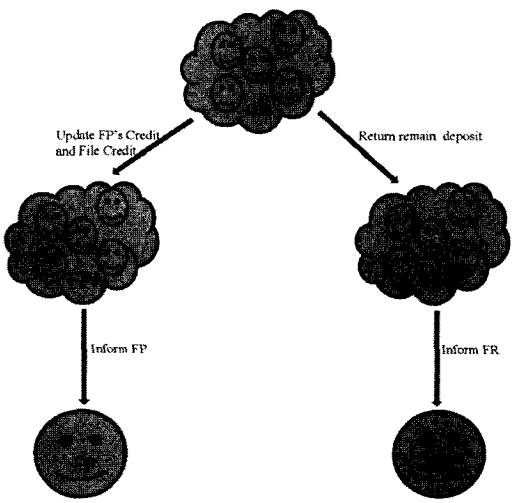


(Figure 2) Query and download Phase

Step 2: When JN receives the evaluation from FR. It judges FR whether it is honest or not, but how to judge it? We adopt History Table to record the latest evaluation to the file. Comparing to the majority evaluation, JN can judge both of sides is honest or not. JN uses the payoff matrix (shown in Table 1) to calculate the payoff to FP and FR.

3.2.1.3 Update Phase.

After one procedure finished, JN updates the value to FP and FR separately.



(Figure 3) Update Phase

		FR honest	FR dishonest
FP	honest	3, 3	3, -4
	dishonest	-4, 3	-4, -4

(Table 1) The Payoff value

Step 1: According to the calculate result, JN updates the Credit and RValue to the node, at the same time, JN updates the FCredit to the file. The update process is that JN sends the result to FPN, FPN updates the node Credit and FCredit, and then FPN informs FP to update them.

Step 2: JN returns the extra Credit to FRN and FRN updates the Credit to FR.

3.2.2 Algorithm

To well evaluate the RValue and Credit, we propose two algorithms.

When every procedure finished, JN will start the Algorithm 1 to calculate the reputation value.

Algorithm 1: Reputation value Calculate

while (one procedure is finished)

{

if (Node act as FP)

{

$$RValue_{up,i} = PayoffValue_{FP} * FCredit + RValue_{up,i-1}$$

$$FCredit_i = \frac{PayoffValue_i}{1000} + FCredit_{i-1}$$

}

Else//Node act as FR

{

$$RValue_{down,i} = PayoffValue_{FP} * FCredit + RValue_{down,i-1}$$

}

Update: $RValue = RValue_{up} + RValue_{down}$

$Credit = RValue - FCredit$

}

End while

Algorithm 2: Shared value Calculate

When (every 30 minutes)

{

$$SValue = SFNumber + \int_0^{SFNumber} FCredit_k * STime_k$$

Update: $Credit = SValue + Credit$

}

End

In Algorithm 1, due to the basic structure in Kad network, nodes acts as both server and client. So RValue consists of two values RValueup and RValuedown. We calculate the RValueup and FCredit when a user acts as FP, and calculate the RValuedown when a user acts as FR. Based on those calculations, RValue, FCredit and Credit update its values after each interaction.

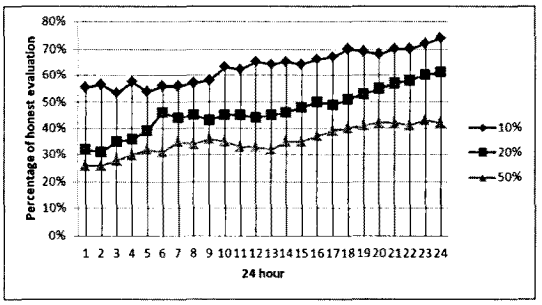
Our purpose of define SValue is to encourage FP provide better service. Node sharing its resources also can get SValue to increase its Credit. And for that reason, we propose Algorithm 2 which JN to calculate the shard value every 30 minutes.

In Algorithm 2, the number of shared files and the length of time every file shared are two important factors affecting the Credit. The more files are shared, the more Credit will be increased.

3.2.3 The Payoff value

In addition, there is another terminology PayoffValue, which indicates the payoff of FP and FR gained form game theory. Compare the majority of the feedback, we can determine which side is honest or dishonest. The value of payoff we used in two algorithms shows in Table 1.

From Table 1, we can see that if the two nodes are both honest they will obtain 3 Credit simultaneously. Meanwhile, the both dishonest nodes will be punished and get -4. Besides, if one node is honest and the



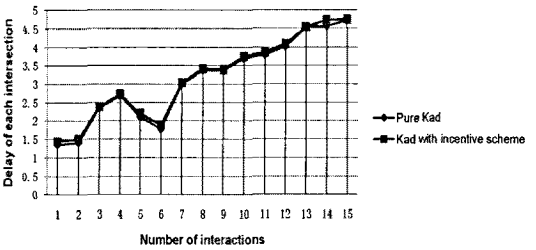
(Figure 5) Percentage of honest evaluation with different ratios of malicious nodes

other is dishonest, the honest one will get 3 Credit while the dishonest will be punished to lose 4 Credit. As we know, incentive and punishment are two effective approaches to regulating node's behavior. Therefore, we introduce PayoffValue based on game theory in Kad network to evaluate peers' behaviors and build a stable and efficient network environment.

This process is based on Kad protocol. We introduce game theory into the interaction among nodes. Our purpose is to build a dedicated and honest P2P network. We use Credit as deposit in our life to regulate the behavior of the node. In order to increase Credit, one way is to share its own resources as many as possible and as long as possible, and another way is to be an honest node which provide honest evaluation. As a file provider supplies the correct and high quality resources, and as a file requester feedback an honest evaluation to the file, the Credit can be increased. On the contrary, the Credit will be decreased.

IV. Evaluation

To evaluate the performance of our incentive mechanism, we launched two series of simulations based on OverSim[24]. In terms of the first one, we evaluated the quality of service provided by our incentive scheme in Kad network. To guarantee the



(Figure 6) Comparison of delay between pure Kad and Kad with incentive scheme

efficiency and feasibility of our incentive scheme in the practical implementation, we monitored the delay happened and made a comparison between pure Kad network and the one with our incentive scheme.

4.1 Quality of service on improving percentage of honest evaluation

Since there are potential selfish or malicious nodes existing in P2P network environment, we launched three series of simulations with different ratios of selfish and malicious nodes: 10%, 20% and 50% respectively. We monitored and evaluated the percentage of honest evaluation from the whole network for 24 hours. Figure 4 and Figure 5 shows the trends of variation on percentage of honest evaluation for 24 hours (i.e. the simulation time). We can learn that the higher percentage of malicious nodes give the more dishonest evaluation. Meanwhile, the overall trends show growth since our scheme can help nodes autonomously adjust their own judgment based on each history log.

4.2 Comparison of delay

In order to evaluate the efficiency and feasibility of our incentive scheme in the practical implementation, we randomly selected 15 interactions happened among 1000 nodes and monitored the delay happened.

As we mentioned in section III, the extra delay is only happened in Query Phase and Evaluation Phase. We launched a test message in OverSim and monitored its processing procedure. Figure 6 in below shows the simulation time of delay happened in pure Kad network and Kad network with our incentive scheme. Compared to the pure Kad network, the delay of Kad with incentive scheme is negligible.

V. Conclusions and Future Work

With the popularity of Kad network, more and more fake files and useless resources appeared. Thus, we proposed an incentive mechanism based on game theory to encourage users share resources and feedback honest evaluation. In order to achieve this goal, we applied payoff matrix in game theory to our mechanism by increasing and decreasing credit as rewards and punishment to stimulate users be honest, finally build a honest and stable Kad network. In our future work, we will focus on how to improve network load balance and on the other hand, we would pay more attention to defending possible attacks such as Sybil attack, Middle attack, etc.

참 고 문 헌

[1] P. Maymounkov and D. Mazieres, "Kademlia: A peer to peer information system based on the xor metric," In Proceedings of IPTPS02, Cambridge, USA, pp. 53-65, Mar. 2002.

[2] Napster, http://www.napster.com/

[3] Gnutella, http://gnutella.wego.com/

[4] KaZaA, http://www.kazaa.com/

[5] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A Scalable Peer to peer Lookup Protocol for Internet Applications," in Proc. of ACM SIGCOMM, pp. 149-160, Aug. 2001.

[6] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A Scalable Content Addressable Network," in Proc. of ACM SIGCOMM, pp. 161-172, Aug. 2001.

[7] A. Rowstron and P. Druschel, "Pastry: Scalable, distributed object location and routing for large scale peer to peer systems," in Proc. IFIP/ACM Middleware 2001, Heidelberg, Germany, pp. 329-350, Nov. 2001.

[8] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Freeriding and whitewashing in peer to peer systems," Proc. ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems, pp. 228-236, Aug. 2004.

[9] E. Adar and B. Huberman, "Free riding on Gnutella," SSL-00 - 63, Xerox PARC, Aug. 2000.

[10] D. Fudenberg and J. Tirole, Game Theory, MIT press, Oct. 1991.

[11] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," In Proc. of 12th International Conference on World Wide Web (WWW 2003), Budapest, Hungary, pp. 640-651, May. 2003.

[12] L. Xiong and L. Liu, "PeerTrust:Supporting Reputation Based Trust for Peer to Electronic Communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, July 2004.

[13] R. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted peer to peer computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, no. 4, pp. 460-473, Apr. 2007.

[14] O. Kwon, S. Lee, and J. Kim, "FileTrust:Reputation Management for Reliable Resource Sharingin Structured

Peer to Peer Networks," IEICE Transactions on Communication, vol. E90-B, no. 4, pp. 826-835, Apr. 2007.

[15] R. Zhou and K. Hwang, "GossipTrust for Fast Reputation Aggregation in P2P Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sep. 2008.

[16] A. Singh and L. Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems," IEEE Intl. Conf. on Peer to Peer Computing, pp. 142-149, Sep. 2003.

[17] P. Golle, K.L. Brown, and I. Mironov, "Incentives for sharing inP2P networks," In 3rd ACM Conf. on Electronic Commerce, pp. 264-267, Oct. 2001.

[18] C. Buragohain, D. Agrawal, and S. Suri, "A game theoretic framework for incentives in p2p systems," In Proc. of the 3rd Int. Conference on P2P Computing, p. 48, Sep. 2003.

[19] M. Feldman, K. Lai, I. Stoica, and J. Chuang, "Robust incentive techniques for peer to peer networks," In ACM EC'04, pp. 102-111, May 2004.

[20] R. Gupta and A.K. Somani, "Game theory as a tool to strategize as well as predict nodes behavior in peer to peer networks," Parallel and Distributed Systems, International Conference on, pp. 244-249, July 2005.

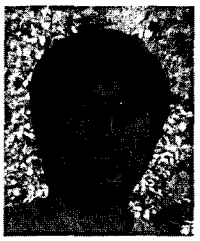
[21] T.B. Ma, C.M. Lee, J.C.S. Lui, and K.Y. Yau, "A Game Theoretic Approach to Provide Incentive and Service Differentiation in P2P Networks," In ACM Sigmetrics'04, pp. 189-198, June 2004.

[22] T.B. Ma, C.M. Lee, J.C.S. Lui, and K.Y. Yau, "An Incentive Mechanism for P2P Networks," In IEEE ICDCS, pp.516-523, Mar. 2004.

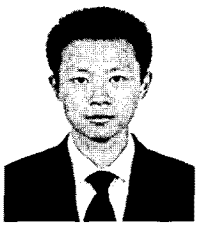
[23] T.B. Ma, C.M. Lee, J.C.S. Lui, and K.Y. Yau, "Incentive and Service Differentiation in P2P Networks: A Game Theoretic Approach," IEEE/ACM Trans. on Networking, vol. 14, no. 5, pp. 978-991, Oct. 2006.

[24] Oversim, http://www.oversim.org/

〈著者紹介〉



왕 서 (Wang Xu) 학생회원
2005년 7월: Shandong Jianzhu University, 컴퓨터공학과 졸업
2010년 2월: 인하대학교 정보통신대학원 석사 졸업
〈관심분야〉 암호 프로토콜, 네트워크 보안, 암호학, 인증 프로토콜



니 영 청 (Ni YongQing) 학생회원
2007년 7월: TianJin University 졸업
2010년 2월: 인하대학교 정보통신대학원 석사 졸업
〈관심분야〉 네트워크 보안, 인터넷 보안, 시스템 보안

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터 정보공학부 부교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안