A Robust Trust Management Scheme against the Malicious Nodes in Distributed P2P Network

Do-sik An[1], Byong-lae Ha[2] and Gi-hwan Cho[1,*]

[1]*Div. of Computer Science and Engineering (Cloud Open R&D Center), Chonbuk National University, Jeonju, South Korea*
[2]*Div. of IT Center, NongHyup, Seoul, South Korea*
[1]*{rokmcads, ghcho}@jbnu.ac.kr*
[2]*honest521@nonghyup.com*

Abstract

Trust management evaluates the user trust value of participating nodes in the network based on the past behaviors and satisfaction of sharing resources. However, there also exists security issue even though it has been considered to be safe because malicious user is able to affect the trust management with negative feedback. This paper aims to propose a robust trust management scheme to improve reliability and effectiveness of distributed P2P network by identifying these malicious threats and then limiting the attacker's participation. Especially, our scheme effectively manages for some attacks such as bad mouthing, on-off and sybil. The proposed scheme is expected to effectively protect attacks from malicious peers with improving credibility as well as exactness.

Keywords: *P2P network, Trust Management, bad mouthing, On-off attack, Sybil attack*

1. Introduction

Nowadays, P2P network has been prevalent due to its own inherent characteristics of load dispersion and high transmission efficiency based on abundant network resources. It is very important to retain a trust among the constituted nodes in P2P network due to the lack of central server. In addition, P2P network has advantages to overcome a single node failure, and shows great flexibility compared with the conventional client-server model. If all nodes normally participate to a network, the network status will be very safe.

However, when the resources are falsified by any peer who has a malicious intension, the mutual trust between the users is decreased to result in degrading of service quality [1]. To prevent these malicious threats, a trust evaluation scheme has been widely investigated by adapting the trust concept prevailing in human life in to computer network [2-12]. Existing researches just tried to distinguish the untrustworthy users who are sharing the same resources, but they did not consider the user who gives a trust evaluation in terms of the threat, and how the trust value itself is honesty. In addition, their works were quite unclear to distinguish the malicious users.

In this paper, we deal with a robust trust management scheme against the malicious node's attacks. The proposed scheme utilizes a time decay function to reflect much the recent trust than that of the past. It also utilized credibility as well as similarity among the users to efficiently reflect the trust value offered by adjacent nodes. As a result, it is expected to protect attacks from malicious peers with improving credibility as well as exactness.

* Corresponding author.

2. Related Work

2.1. Attack types of trust evaluation

Bad mouthing, on-off attack and Sybil are representative attacks which can be protected based on trust management. In bad mouthing attack [13], a malicious user gives a false assessment to other nodes in the network. As shown in Figure 1 (A), the node *A* has a trust value of R_C for node *C*. But, in the case of (B) which shows an attack scenario, the node *B* is assumed as a malicious node. Node *B* evaluates node *C*'s trust value as $-R_C$, that is an abnormal, to disparage node *C*'s trust, and then deliver it to node *A*. In this case, node *C* which is seen as a malicious node can be excluded from the network even though it is actually trust node. This case is called bad mouthing.

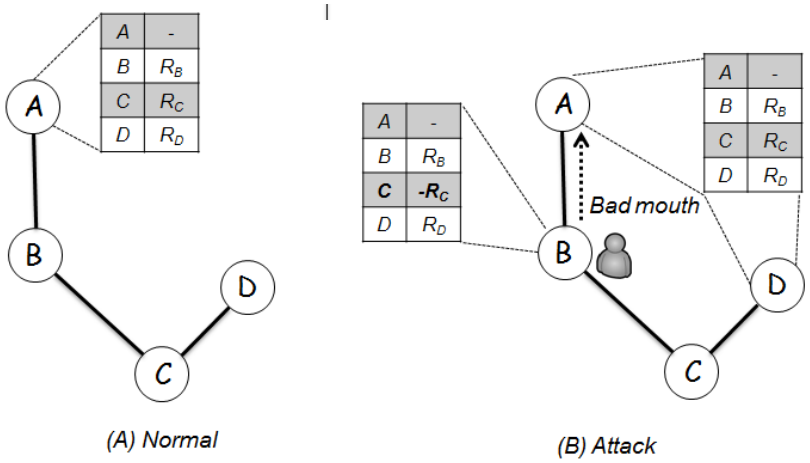

Figure 1. Example of bad mouthing attack

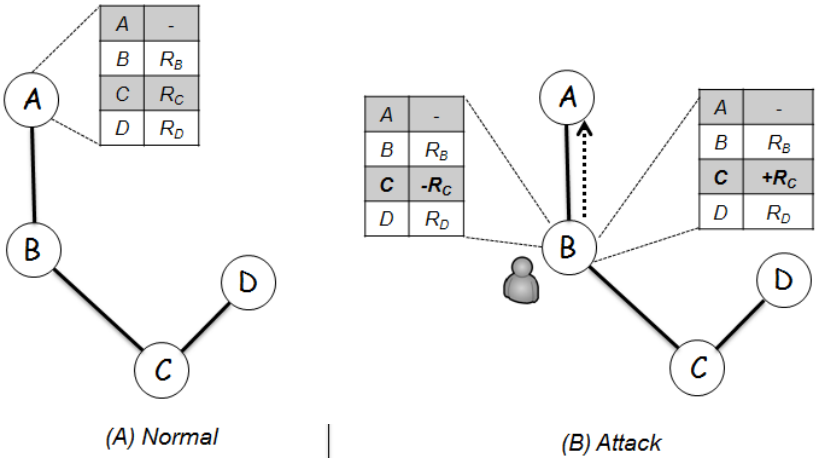

Figure 2. Example of on-off attack

On-off attack is one of the most hazardous trust based attacks [14]. It acts normal or abnormal behavior in turn so that a malicious user can consistently be participated in the network – it is similar to Sybil attack. In Figure 2, if node *B* is regarded as a malicious node,

the trust value of node *C* evaluated by node *B* is delivered to node *A*. In the case of (B), Node *B* delivers the trust value of $+R_C$(normal) and $-R_C$(abnormal) in turn to consistently participate in the network. That is an on-off attack and greatly influences the trust management. Therefore, this malicious attack behavior should be identified and prevented in advance.

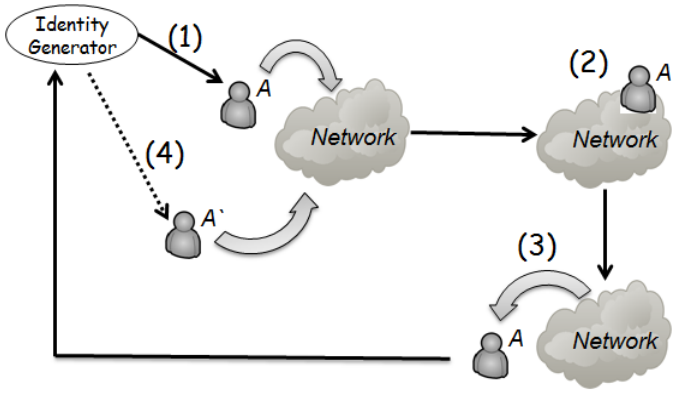

Figure 3. Example of sybil attack

Sybil obtains a number of legitimate node's ID and make use of it to the attack. Figure 3 shows the procedure in which a malicious user attempts the Sybil attack.

(1) A malicious node participates in the network with newly created node ID (A) using an identity generator.

(2) The participated node influences the network with normal or abnormal behavior in turn.

(3) If a malicious behavior is detected, it is excluded from the network.

(4) By using the other node's ID (A'), the malicious user participates again in the network.

2.2. Existing trust management schemes

EigenTrust [2] is a well-known method not only to reduce malicious node sharing the untrustworthy resources, but also to limit the participation of malicious node by referring the peer's trust value when a peer selects its transaction counterpart. However, the function of distinguishing the user giving false rating to the transaction result is not discussed in detail. Due to the use of iterative matrix multiplication as it assumes that there exists trustworthy node a priori, it results in high cost. PeerTrust [6] leads the user to actively participate on evaluation by giving an adjacent node incentive, but the problem is that it gives the incentive without considering of credibility to evaluation value itself.

PowerTrust [3] has a difficulty to apply it in distributed network because it is originally proposed based on DHT (Distributed Hash Table). Generally, there exists a problem that the subjective point of view of each node is ignored and all participating nodes in whole network have a same trust value. In SFTrust [7], the proposed framework just evaluated a satisfaction of the communication. It paid no attention not only to transition according to time variance, but did not consider the quality of transaction and times of communication, *etc.* FileTrust [8] calculates the honesty of the corresponding user with reference to the evaluation value offered by user sharing same resources in order to distinguish the user's false rating. But, if there is no evaluation on the resources, it is difficult to be honesty.

3. Robust Trust Management Scheme

To propose a robust trust management scheme against malicious users, our proposed scheme utilizes similarity of trust among the participating users, which is a direct trust value with subjective trust of users.

3.1. Trust management

The trust of neighboring node, that is, direct trust management, is based on its own experience. But, in indirect trust, a neighboring node evaluates the trust of its adjacent node. The whole trust management is as equation (1). T_{ij} means node *i* evaluates trust for node *j*.

$$T_{ij} = \alpha \times DT_{ij} + (1-\alpha) \times IdT_{ij} \tag{1}$$

DT_{ij} is a direct trust value which node *i* evaluates node *j* based on node *i* experiences. Idt_{ij} is an indirect trust value by adjacent nodes, α is a confidence factor which means how the node *i* is able to be convinced for the direct trust value by itself. If the node *i* communicates with node *j* k^{th} times, the confidence factor can be calculated like equation (2) and here, the threshold stands for the number of communication.

$$a = \begin{cases} k^{th} / Threshold, & k^{th} < Threshold \\ 1 \quad\quad\quad\quad\quad\quad , & else \end{cases} \tag{2}$$

3.2. Direct trust

When node *i* communicates with another node directly, node *i* is able to evaluate it based on his experiences. This direct trust is presented as DT_{ij}. If node *i* communicates with node *j* k^{th} times, we are able to calculate the satisfaction value, that is, ex_{ij}^{k}, which is expressed as equation (3) bellow. Using this satisfaction value, we can calculate the direct trust value for node *j*, that is, DT_{ij}, which follows as equation (4). The number of communication *k* has the value of $k = 1, 2, ..., n$.

$$ex_{ij}^{k} = \begin{cases} 1, & satisfactory \\ 0, & unsatisfactory \end{cases} \tag{3}$$

$$DT_{ij} = \frac{\sum_{k=1}^{n} f(x) \times ex_{ij}^{k}}{\sum_{k=1}^{n} f(x)} \tag{4}$$

The satisfaction value of each communication is obtained by mapping the time decay function $f(x)$ as $f(x) = \lambda^{n-k}$. Thus, *n* means the number of communications, which has a range of $0.5 \leq \lambda \leq 1$, $1 \leq k$.

We made use of a time decay function where the example is shown in Figure 4 to effectively reduce the influence of on-off attack. In example, λ and *k* have a value of 0.8 and 4 respectively. Even though case 1 and case 2 have the same satisfaction value, their results are different according to the communication order. In this case, the direct trust value can be effectively managed by giving a weight to recent communication value than that of past one.

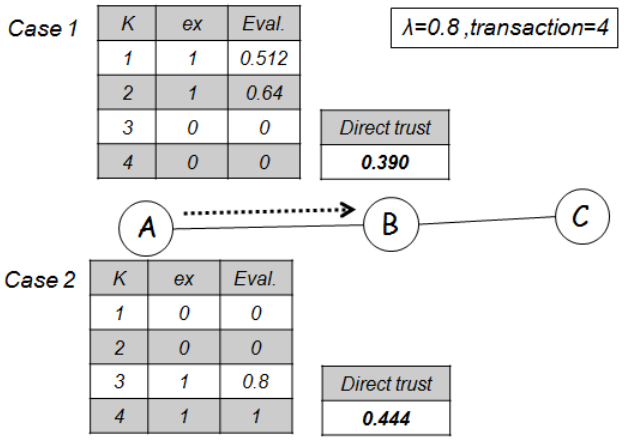

Figure 4. Example of time decay function

3.3. Indirect trust

Indirect trust can be calculated based on similarity of two nodes and the trust value of node offering confidential value. The indirect trust expressed as Figure 5 can be evaluated by utilizing equation (5).

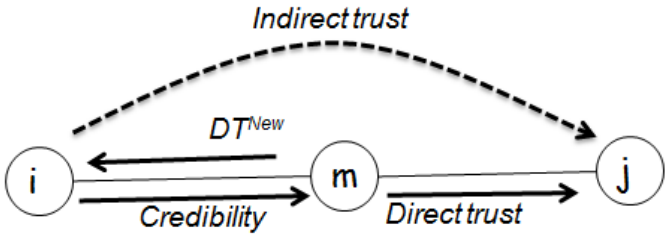

Figure 5. Outline of indirect trust

$$IdT_{ij} = \frac{\sum_{k=1}^{n} CR_{im} \times DT_{mj}^{New}}{\sum_{k=1}^{n} CR_{im}} \tag{5}$$

DT_{mj}^{New} reflects the number of communication with the direct trust value of node *m*, which is calculated as equation (6). Thus, *n* indicates the communication times between the node *m* and the node *j*. β is a scaling factor to keep the direct trust, and it has the range as $0.5 < \beta \leq 1$.

$$DT_{mj}^{New} = DT_{mj} \times \beta^{\frac{1}{n}} \tag{6}$$

Credibility presented as CR_{im} is an evaluated value for node *m* in the node *i* point of view. When the node *m* offers an indirect trust value of the node *i*, node *i* decides the indirect trust value to be applied according to the trust value of node *m*.

4. Experiment and Analysis

To validate our proposed scheme, we compared it with EigenTrust [2] and one without any trust method. The evaluation was conducted in a various attack scenarios and based on file sharing. According to the attack scenario, we prescribed user behavior model and evaluated it. To do this, QTM simulator [15] which is well known user behavior model is used to evaluation. The simulator uses the three user types described in Table 1. In Table 1, the cleanup mean the probability to remove dead file from the library by user, and the honesty is a probability that user gives an honest opinion to the others. The experiment makes use of the parameters as shown in the Table 2.

Table 1. The user model initial parameters

User type	Cleanup (%)	Honesty (%)	Source
Good	90-100	100	Best
Bad mouthing	90-100	0	Random
On-Off	50-100	50-100	Random

Table 2. Simulation parameters

Parameter	Value	Parameter	Value
Number of users	100	Max. of neighbor	2
Number of transactions	10000	λ	0.5
Number of files	5000	β	0.8
Zipf ‘s of coefficient	0.4	EigenTrust pre-trust	0, 2
Threshold	50		

The evaluation about the experimental result focused on success rate of good user and adopted the validity measurement proposed in [16]. This can be described as follow equation (7), which is also presented as SRT(Success Rate of Transmission).

$$SRT = \frac{\#of\ valid\ \ file\ received\ by\ good\ users}{\#of\ transactions\ attempted\ by\ good\ users} \tag{7}$$

For all experimental results, x-axis shows the percentage of the attackers and y-axis means the evaluation metric. If the metric is close to 1, the success rate is higher.

In the first scenario, we measured the transaction success rate of good user when there exists bad mouthing, that means a false rating, defined in Table 1. The evaluation result shows nearly the same success rate as shown in Figure 6, even though the number of malicious nodes is increased. However, EigenTrust shows a significant decline when it exceeds 70%. This is because all values are reflected in the trust evaluation, and normal communication is possible under the assumption there exist trustworthy node a priori.

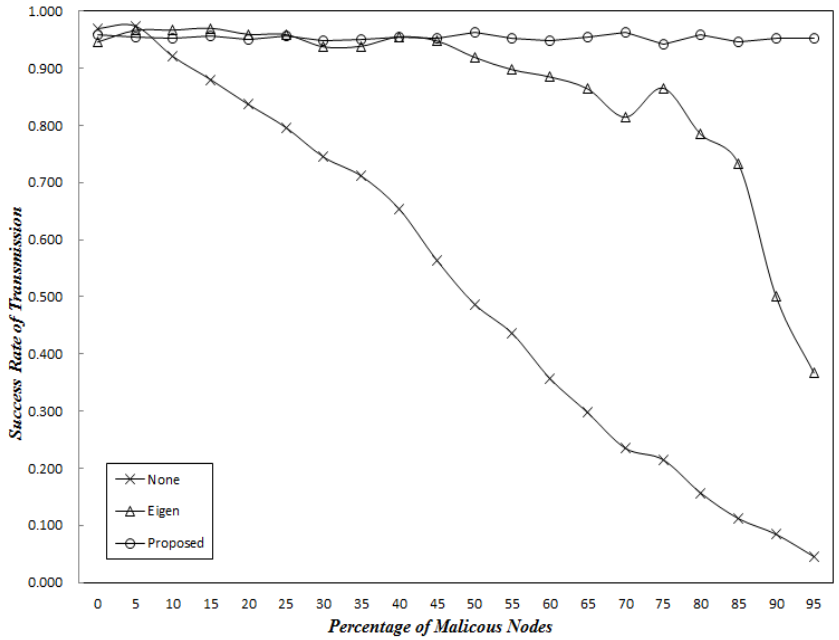

Figure 6. Success rate in case of bad mouthing

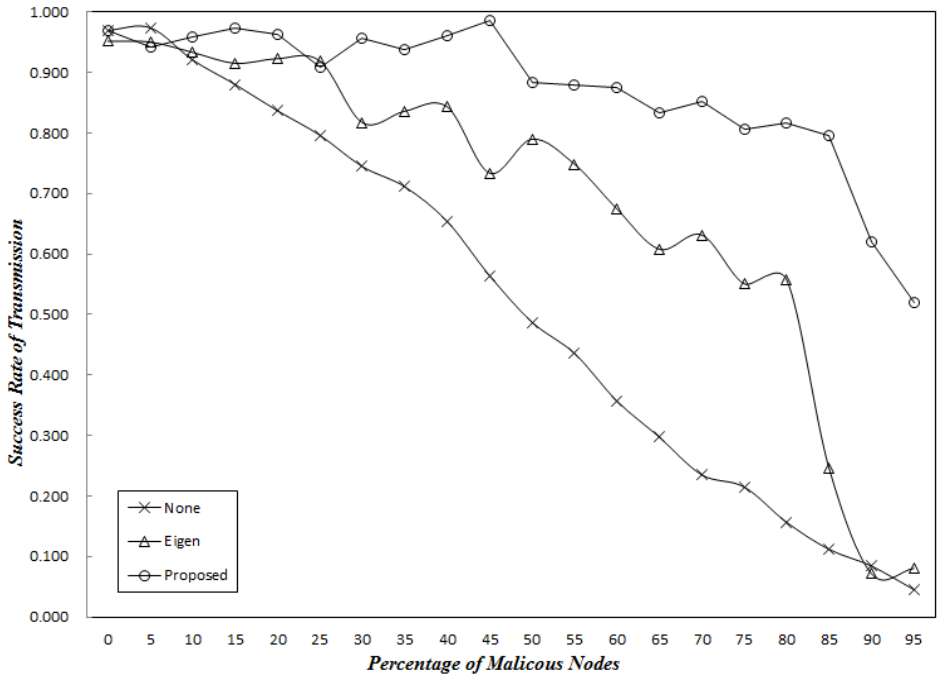

Figure 7. Success rate in case of on-off attack

The second scenario is measured on assumption of on-off attack. Here, the measurement of STR is the result to transaction success rate of good user. Evaluation result shows the similar decrease as shown in Figure 7 according to the proportion, but the success rate is high in a proposed scheme.

Likewise the Bad mouthing, EigenTrust reflecting all trust values is not able to correspond to the on-off attack which affects in the network for a long time. In this paper, it is considered to be normally communicated because we reflected the trust value with time variance and enhanced the accuracy of indirect trust value.

We set up the experiment environment to measure Sybil attack as follow. The malicious user attempting the Sybil attack cancels the network access after transaction and approaches the network with newly created identity. The setting up about the Sybil attack is provided in QTM. In the experimental result as like Figure 8, the proposed method and EigenTrust show the similar falling rate. However, as to the success rate of the transaction, the proposed method is more excellent.

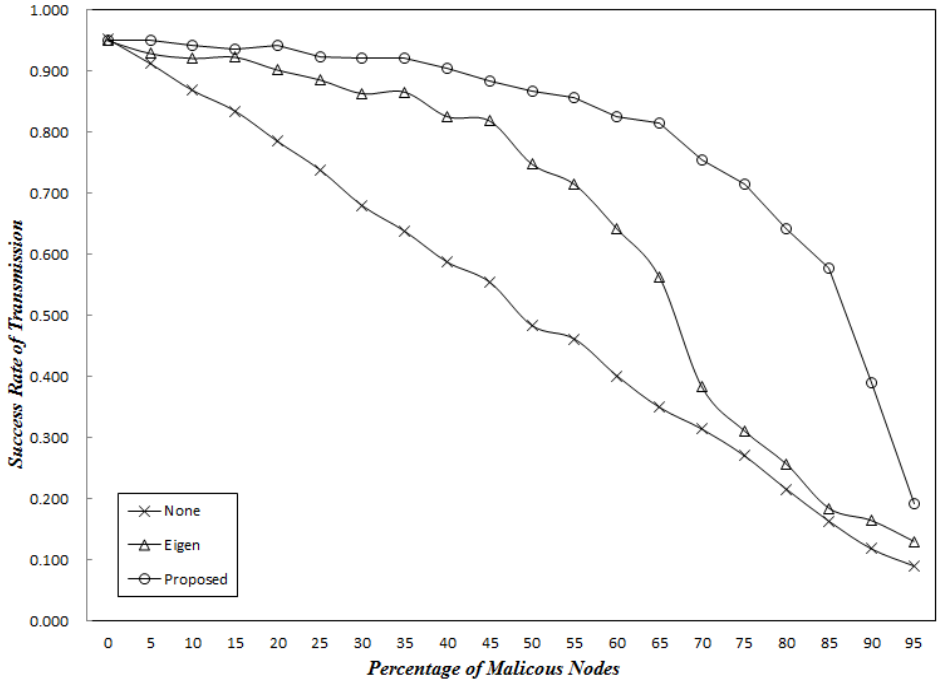

Figure 8. Success rate in case of sybil attack

5. Conclusion

In this paper, we proposed a robust trust management scheme to treat attack against malicious nodes based on user's trust value in distributed P2P network environment. Especially, our scheme is focused on protecting bad mouthing, on-off attack, and sybil attack. We utilized the user credibility as well as the similarity among the users to efficiently reflect the trust value offered by adjacent nodes. To evaluate the proposed scheme, the network environment with malicious node is constituted. Here, we used three kinks of user behavior models and evaluated proposed method under the prescribed attack scenarios. Evaluation results show our scheme is so superior then that of the others

For the future work, we are going to apply the proposed method with more sophisticate scheme to various attack scenarios, and to design an adaptive security model to effectively treat malicious users in computer network other than distributed network environment.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(KRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2042035).

References

[1] Y. Liu, "A Two-hop Solution to Solving Topology Mismatch", IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 11, **(2008)**, pp. 1591-1600.
[2] S. Kamvar, M. Schlosser and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks", Proceedings of the 12th International Conference on World Wide Web, **(2003)**, pp. 640-651; NY, USA.
[3] R. F. Zhou and K. Hwang, "PowerTrust: a Robust and Scalable Reputation System for Trusted Peer-to-peer Computing", IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 4, **(2007)**, pp. 460-473.
[4] Z. Abrams, R. McGrew and S. Plotkin, "A Non-manipulable Trust System based on EigenTrust", ACM SIGecom Exchanges, vol. 5, no. 4, **(2005)**, pp. 21-30.
[5] S. Rao, Y. Wang and X. Tao, "The Comprehensive Trust Model in P2P Based on Improved EigenTrust Algorithm", Proceedings of the International Conference on Measuring Technology and Mechatronics Automation, **(2010)** March, pp. 822-825.
[6] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation based Trust for Peer-to-Peer Electronic Communities", IEEE Transaction on Knowledge and Data Engineering, vol. 16, no. 7, **(2004)**, pp. 843-857.
[7] Y. C. Zhang, S. S. Chen and G. Yang, "SFTrust: a Double Trust Metric based Trust Model in Unstructured P2P System", Proceedings of the 23rd IEEE International Parallel & Distributed Processing Symposium, **(2009)**, pp. 1-7.
[8] O. Kwon, S. Lee and J. Kim, "FileTrust: Reputation Management for Reliable Resource Sharing in Structured Peer-to-Peer Networks", IEICE Transaction on Communication, vol. E90-B, no. 4, **(2007)**, pp. 826-835.
[9] X. Dong, W. Yu and Y. Pan, "A Dynamic Trust Management Scheme to Mitigate Malware Proliferation in P2P Network", Proceedings of the IEEE International Conference on Communications (ICC), **(2008)**, pp. 1605-1609.
[10] Y. F. Wang and A. Nakao, "Poisonedwater: an Improved Approach for Accurate Reputation Ranking in P2P Networks", Future Generation Computer System, vol. 26, no. 8, **(2010)**, pp. 1317-1326.
[11] C. Tian and B. Yangc, "R2Trust, a Reputation and Risk based Trust Management Framework for Large-scale, Fully Decentralized Overlay Networks", Future Generation Computer Systems, vol. 27, no. 8, **(2011)**, pp. 1135-1141.
[12] Z. Q. Liang and W. S. Shi, "PET: a Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing", Proceedings of the 38th International Conference on System Science, **(2005)**, pp. 1-10.
[13] A. K. Pathan, "Security of Self-Organizing Networks", CRC Press, **(2010)**.
[14] W. Miao, T. Fei, Z. Yujun and L. Guojie, "An Adaptive and Robust Reputation Mechanism for P2P network", Proceedings of the IEEE International Conference on Communications, **(2010),** pp. 1-5.
[15] QTM: Quantitative Trust Management, http://rtg.cis.upenn. edu/qtm.
[16] A. G. West, S. Kannan, I. Lee and O. Sokolsky, "An Evaluation Framework for Reputation Management Systems", Working Chapter for Trust Modeling and Management in Digital Environments: From Social Concept to System Development, **(2009)** May.

Authors

Do-sik An received his B.S. and M.S. degree in computer science and engineering from Chonbuk National University, Jeonju, Korea, in 2008 and 2010. Currently, he is a Ph.D. student in Chonbuk National University, Jeonju, Korea. His current research interests include bulk data transfer protocol, routing protocols, vehicular network, and security of P2P network.

Byong-lae Ha received his B.S. and M.S. degree in computer science and engineering from Chonbuk National University, Jeonju, Korea, in 2009 and 2013. At Jan. 2013, he joined the Division of IT Center at NongHyup, Seoul, Korea. His current research interests include P2P network, trust evaluation method, and routing protocols.

Gi-hwan Cho received his B.S. degree from Chonnam National University, Gwangju, Korea, in 1985, and his M.S. degree from Seoul National University, Seoul, Korea, in 1987, both in computer science and statistics. He received his Ph.D. degree in computer science from the University of Newcastle, Newcastle Upon Tyne, England, in 1996. He worked for the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, as a Senior Member of the Technical Staff from Sep. 1987 to Aug. 1997, for the Department of Computer Science at Mokpo National University, Mokpo, Korea, as a Fulltime Lecturer from Sep. 1997 to Feb. 1999. In Mar. 1999, he joined the Division of Computer Science and Engineering at Chonbuk National University, Jeonju, Korea, and he is currently serving as a professor. His current research interests include mobile computing, computer communication, security framework, wireless security, sensor networks, and distributed computing systems.