P2P에서 Liar 감소를 위한 새로운 평판 시스템

신 정 화[†] · 이 경 현[††]

요 약

P2P 서비스는 서비스 참여자들의 행동을 관리하고 악의적인 행동을 수행하는 참여자들을 제어할 수 있는 별도의 관리 기관을 가지지 않기 때문에 악의적인 목적을 가진 참여자들은 더 많은 이익을 얻기 위해 올바르게 행동하는 사용자들에게 피해를 줄 수 있다. 그러므로, P2P 서비스 이용자들은 사전 트랜잭션 수행 경험이 없는 사용자들과 안전하게 트랜잭션을 수행하기 위하여 과거에 트랜잭션을 수행한 경험이 있는 사용자들에 의해 제공되는 정보인 "평판" 정보의 참조를 통해 악의적인 목적을 가진 사용자와 올바른 사용자를 구별할 수 있다. 그러나, 사용자들은 수행된 트랜잭션에 대해 고의적으로 거짓 평가를 줄 수 있고, 이러한 사용자들을 "liar"라 부른다. 본 논문에서는 평판 정보에 대한 정확성을 위해 liar를 감소시키는 새로운 평판 시스템을 제안하고 시뮬레이션을 통해 그 타당성을 보인다.

키워드 : P2P, 평판 시스템, 신뢰 관리, 거짓피어

A New Reputation System for Reducing the Liars in P2P

Jung-Hwa Shin[†] · Kyung-Hyune Rhee[††]

ABSTRACT

As the P2P service does not have any administration authorities that are able to manage the behavior of participants and control the malicious users, *malicious user can give harm to legitimate users for the benefit of themselves.* To perform the secure transaction with new members who did not have past experiences on transaction, service users can differentiate malicious users and legitimate users by referring to the reputation information that provided by users having past experience. However, users can intentionally give false evaluation to other users on performed transaction. We call these users as "liar". In this paper, we propose a new reputation system for liar reduction to guarantee an accuracy on reputation information.

Key Words : Peer-to-Peer, Reputation System, Trust Management, Liar

1. 서 론

P2P(Peer-to-Peer) 기술은 고성능 중앙 서버나 광대역 네트워크 없이도 정보를 찾는 사람과 정보를 가진 사람의 컴퓨터 간에 직접적인 연결을 통해 다양한 정보를 공유할 수 있도록 하는 기술과, 그 기술을 응용하여 제공되는 서비스들의 집합을 총칭하는 것으로 네트워크에 연결된 모든 컴퓨터가 동등한 권한과 책임을 가지고 동작하며, 신속한 정보 교환과 비용 절감, 통신 대역폭의 효율적인 사용과 효율적인 자원 관리 차원에서 "클라이언트/클라이언트" 모델이라 할 수 있다[1, 2]. 초기의 P2P 기술은 냅스터, 프루나, 소리바다 등과 같은 파일 공유를 위한 목적으로 인기를 끌었지만 현재 컴퓨팅 자원의 공유나 온라인 협업, 전자상거래 등으로 응용 분야가 확대되고 있다. 반면, P2P 기술 자체가 가진 성질로 인해 P2P 서비스에 참여하는 사용자들은 서로 다른 환경에서 동작하고, 사용자들의 서비스 이용에 특별한 제한을 두지 않기 때문에 자유로운 이용이 가능하며, 사용자들은 서비스 이용을 위해 자유롭게 가입하고 종료할 수 있다.

그러므로, 몇몇 사용자들은 호의적으로 서비스를 제공하고 다른 사용자들이 제공하는 서비스를 이용하기도 하지만, 몇몇 사용자들은 서비스를 전혀 제공하지 않거나, 잘못된 서비스를 제공할 수 있기 때문에 사용자들에 의해 제공되는 서비스나, 서비스 제공자에 대한 신뢰성 보장이 필요하다. 그 결과, P2P 서비스에서는 서비스 이용자들이 사전 트랜잭션 수행 경험이 없는 사용자들과 안전하게 트랜잭션을 수행할 수 있도록 전자상거래에서 많이 사용하고 있는 것으로 알려진 "평판(Reputation)" 정보를 참조하여 악의적인 목적을 가진 사용자와 올바른 사용자를 구별할 수 있으며, 이를 통해 서비스 제공자나 이용자는 상호 간에 신뢰를 바탕으로 서비스를 제공하거나 이용할 수 있다[3].

※ 본 연구는 한국과학재단 특정 기초 연구(R01-2006-00-10260-0) 지원으로 수행되었음.
† 준 회 원 : 부경대학교 대학원 전자계산학과 이학박사
†† 종신회원 : 한국멀티미디어학회 학술이사, (현)재무이사, 논문지 편집위원
논문접수 : 2006년 7월 28일, 심사완료 : 2006년 11월 16일

"평판" 정보는 과거에 트랜잭션을 수행한 경험이 있는 사용자들에 의해 제공되는 정보로 사용자들은 때때로 믿을 수 있는 사용자와 트랜잭션을 수행하더라도 고의적으로 상대방의 평판을 감소시키기 위해 나쁜 평판을 주거나, 악의적인 목적을 가진 사용자와 트랜잭션을 수행하더라도 고의적으로 상대방의 평판을 증가시키기 위해 좋은 평판을 줄 수 있다.

본 논문에서는 다양한 P2P 서비스 중 파일 공유 서비스에서 트랜잭션 대상을 선택할 때 참조하는 평판 정보에 대한 정확성을 위해 거짓 평가를 주는 사용자의 수를 감소시킬 수 있는 방안을 제안하고자 한다. 제안 방안은 트랜잭션 수행 후 자원 요청자들이 주는 평가 값에 따라 자원 제공자에 대한 추천자와 비 추천자로 구분하여 등록하고, 이들이 준 평가 의견과 현재 트랜잭션을 수행한 사용자가 주는 평가 의견을 함께 참조하여 거짓 평가를 주었을 가능성이 있는 사용자를 판단하고, 이들의 신뢰 값을 감소시켜 서비스 이용을 제한할 수 있다. 뿐만 아니라, 트랜잭션 대상을 선택할 때 자원 제공자의 신뢰 값과 자원 제공자를 추천한 사용자와 추천하지 않은 사용자의 신뢰 값을 함께 참조함으로써 트랜잭션 대상과 자원에 대한 신뢰성을 향상시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 P2P 서비스와 평판 시스템에 대해 설명하고, 3장에서는 파일 공유 서비스에서 사용하는 평판 정보에 대한 정확성을 위해 거짓 평가를 주는 사용자 수를 감소시키기 위한 새로운 평판 시스템을 제안한다. 4장에서는 시뮬레이션을 통해 제안 방안을 분석하고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 P2P 서비스

P2P의 일반적인 개념은 중앙 서버를 거치지 않고 정보를 찾는 사용자와 정보를 가진 사용자의 컴퓨터를 직접 연결하여 서로의 자원을 공유할 수 있도록 해주는 기술과 그 기술을 응용하여 만든 새로운 서비스의 집합이라 할 수 있다[4]. P2P는 상대적으로 클라이언트/서버 구조에서 서버가 아예 없어지거나 클라이언트의 역할이 강화된다는 가장 본질적인 특징을 가진다. P2P 서비스에서는 서비스 참여자나 통신이 가능한 모든 정보 단말기를 "피어"라고 하며, 중앙 서버가 클라이언트의 IP 주소와 파일 목록 등의 P2P 목록을 유지하면서 사용자들을 연결해 주는 역할을 하는 하이브리드 P2P 방식과 모든 이용자가 접속해 릴레이 방식으로 서로의 정보를 중개하는 순수 P2P 방식이 있다[5].

2.2 평판 시스템

평판 시스템은 "평판(Reputation)"이라 불리는 트랜잭션 참여자의 과거 행동에 관한 정보를 수집하고 관리하는 시스템으로, 전자상거래나 온라인 경매, P2P 서비스 등과 같은 분산 환경에서 서비스 참여자들에 대한 신뢰 정보를 알리기 위해 사용하고, 서비스 참여자들 간의 신뢰를 설정하는데 있어 효과적이다[3]. 서비스 참여자들은 트랜잭션 수행 후 평판 시스템을 통하여 트랜잭션 대상자를 평가할 수 있고, 이러한 평가의 합이 참여자들에 대한 "평판"을 만든다. 평판 시스템은 서비스 참여자들이 평판 정보를 자유롭게 볼 수 있도록 공개하고, 이 정보를 참조하여 신뢰할 수 있는 트랜잭션 대상자를 선택할 수 있도록 도와줌으로써 악의적인 트랜잭션 수를 감소시킬 수 있을 뿐만 아니라 트랜잭션 참여자들에 대한 신뢰성 또한 향상시킬 수 있다[6]. 평판 시스템은 사용자들의 평판 정보를 어떻게 관리하는 가에 따라 중앙 집중식 평판 시스템과 분산 평판 시스템으로 구분할 수 있다.

수행된 트랜잭션에 대해 거짓 평가를 주는 사용자의 수를 감소시키기 위하여 제안된 몇몇 방안을 살펴보면 다음과 같다. Lee 등이 제안한 FCRS(Feedback Credibility Reputation Scheme)[7]는 순수 P2P 방식으로 동작하며 파일 평판을 기반으로 신뢰할 수 없는 파일에 대한 다운로드 수를 감소시키고, 거짓 평가를 주는 피어들의 영향을 감소시키기 위한 평판 관리 방법이다. FCRS는 파일 평판 계산을 위해 피어의 신뢰성(credibility)을 이용하며, 피어의 신뢰성(credibility)은 동일한 파일을 사용한 경험이 있는 피어들이 준 평가 값과의 유사성을 이용하여 계산한다. 특정 피어가 필요로 하는 파일을 여러 피어가 제공하는 경우 해당 파일에 대한 추천 피어와 비 추천 피어의 신뢰성(credibility)를 이용하여 파일의 신뢰성을 계산하고, 계산된 신뢰 값을 파일을 제공한 피어의 신뢰 값으로 지정하므로 이용자들은 이 값을 참조하여 파일 제공자를 선택하고 다운로드를 요청한다.

L. Mekouar 등[8]이 제안한 방법은 트랜잭션을 수행한 피어들이 주는 평가에 거짓이 있는 피어들을 탐지하게 위하여 "suspicious transaction" 개념을 정의하여 사용하고 있다. 파일 제공자가 자신의 신뢰 값이 "positive"임을 알고 있는 상태에서 파일 요청자로부터 받은 자신의 신뢰 값이 "negative"라면 현재 수행된 트랜잭션이 "suspicious"한 것으로 판단한다. 특정 피어에 의해 보내진 전체 평가에서 "suspicious" 평가의 비율이 α라면 피어의 신뢰도는 $(1-\alpha)$로 표현된다. 이 방안에서는 평판이 좋은 피어는 항상 올바른 파일을 제공한다고 묵시적으로 가정함으로써 파일 제공자의 신뢰 값에 의존하여 평가의 정확성을 판단한다.

3. P2P에서 Liar 감소를 위한 새로운 평판 시스템

파일 공유 서비스를 위해 사용되는 대부분의 평판 시스템에서 트랜잭션 수행을 원하는 피어들은 과거 트랜잭션 수행 경험이 있는 피어들에 의해 남겨진 평판 값에 상당히 의존하여 트랜잭션 대상 피어를 선택하기 때문에 트랜잭션을 수행한 피어들에 의해 제공되는 평가 값의 정확성은 매우 중요하다. 그러나, 피어들은 때때로 믿을 수 있는 피어와 트랜잭션을 수행하더라도 대상 피어의 평판을 고의적으로 감소시키기 위해 나쁜 평가를 주거나, 악의적인 목적을 가진 피어와 트랜잭션을 수행하더라도 고의적으로 평판을 증가시키기 위해 좋은 평가를 줄 수 있다. 이와 같이 수행된 트랜잭

션에 대해 거짓 평가를 주는 피어를 "liar"라 하고, 피어들이 거짓 평가를 주는 형태를 다음 두 가지 용어로 구분하여 설명할 수 있다[9].

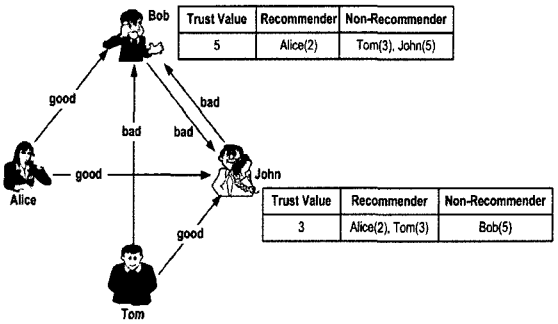
- Bad Mouthing : 파일 요청 피어가 올바른 파일을 받았다면 파일 제공 피어에 대해 나쁜 평가를 주지 않아야 한다.
- Ballot Stuffing : 파일 요청 피어는 잘못된 파일을 보낸 파일 제공 피어에 대해 좋은 평가를 주지 않아야 한다.

피어들의 거짓 평가는 다른 피어의 평판에 부정하게 영향을 미침으로써 악의적인 피어들의 좋은 평판을 증가시키고, 올바르게 동작하는 피어들의 좋은 평판을 감소시키는 것과 같이 평판 시스템 자체에 문제가 생기도록 만들 수 있다. 현재 사용되고 있는 대부분의 평판 시스템은 신뢰할 수 없거나 사용자 시스템에 해를 끼칠 수 있는 파일을 전송하는 피어를 탐지하고, 처벌하는 것을 목적으로 하며, 거짓 평가를 보내는 피어를 탐지하고, 처벌하기 위해 제안된 메커니즘은 거의 없는 실정이다. 따라서, 본 논문에서는 거짓 평가를 주는 피어들의 수를 감소시키기 위한 새로운 방안을 제안함으로써 평판 정보에 대하여 정확성을 제공하고자 한다.

3.1 제안 방안의 특징

제안 방안은 하이브리드 P2P 방식을 기반으로 동작하고, 피어들이 공유하는 파일의 정확성과 질을 기반으로 피어가 제공하는 파일을 평가하여, 평가된 값을 피어에 대한 평판으로 지정한다. 해당 파일이 올바른 경우 평가 값으로 1을 주고, 그렇지 않은 경우 평가 값으로 -1을 준다. 거짓 평가를 주는 피어들의 수를 감소시키기 위하여 파일 요청 피어들이 주는 평가 값에 따라 파일 요청 피어를 파일 제공 피어에 대한 추천 피어와 비 추천 피어로 구분한다. 트랜잭션 수행 후 파일 요청 피어가 파일 제공 피어에 대해 좋은 평가(1)를 준다면 파일 제공 피어의 추천 피어 목록에 등록하고, 나쁜 평가(-1)를 준다면 비 추천 피어 목록에 등록한다. 피어들에 대한 평판과 신뢰 값은 중앙 서버가 관리하고, 서버는 파일 제공 피어가 이전에 수행된 여러 트랜잭션에서 받은 평가와 현재 수행된 트랜잭션에서 받은 평가를 비교하여 파일 요청 피어의 평가에 대한 거짓 여부를 판단하고, 이미 수행된 트랜잭션에서 거짓 평가를 준 피어들도 판단하여, 이들에 대한 신뢰 값을 감소시켜 서비스 참여를 제한함으로써 거짓 평가를 주는 피어들의 수를 감소시킬 수 있다.

제안 방안의 기본 동작을 예를 들어 설명하면 (그림 1)과 같다. 그림에서 괄호안의 숫자는 각 피어들이 가지는 신뢰 값을 의미한다. Bob과 Alice, Bob과 Tom, Bob과 John이 서로 트랜잭션을 수행하고, Alice는 Bob에 대해 좋은 평가를 주고 Tom과 John은 Bob에 대해 나쁜 평가를 준 경우 서버는 이들로부터 받은 평가에 따라 Bob의 추천 피어 목록에 Alice를 등록하고, 비 추천 피어 목록에 Tom과 John을 등록한다. 트랜잭션 대상 피어를 선택할 때 피어들은 Bob에



(그림 1) 제안 방안의 동작 예

대한 신뢰 값과 추천 피어 목록에 있는 Alice의 신뢰 값, 비 추천 피어 목록에 있는 Tom과 John의 신뢰 값 모두를 참조하여 트랜잭션 대상을 선택한다.

제안 방안에서 거짓 평가를 주는 피어를 판단하는 기준은 다음과 같다. 트랜잭션을 수행한 피어들이 주는 평가 값에 따라 파일 제공 피어에 대한 추천 피어와 비 추천 피어로 등록하고, 파일 제공 피어가 이전에 수행된 n번의 트랜잭션에서 받은 평가와 현재 트랜잭션 수행 결과로 받은 평가를 참조하여 좋은 평가를 받은 횟수와 나쁜 평가를 받은 횟수를 계산하여, $n/2$ 이상인 평가 의견에 따라 현재 수행된 트랜잭션에서 받은 평가의 거짓 여부를 판단하고, 이전에 수행된 n번의 트랜잭션에서 받은 평가에 대해서도 거짓이 있는지 판단한다.

트랜잭션 수행 후 평가 값을 주는 피어들이 liar로 판단되는 경우를 예를 들어 설명하면 다음과 같다. 특정 피어가 이전에 수행된 n번의 트랜잭션에서 모두 좋은 평가를 받았고, 현재 트랜잭션 수행 결과로 나쁜 평가를 받았다면, liar 판단 기준에 의해 현재 평가를 준 피어가 liar로 판단된다. 반대로, 이전에 수행된 n번의 트랜잭션에서 모두 나쁜 평가를 받았고, 현재 트랜잭션에서 좋은 평가를 받았다면, 현재 평가를 준 피어가 liar로 판단된다.

이전에 수행된 n번의 트랜잭션에서 $n/2$ 이상의 좋은 평가와 $n-n/2$ 미만의 나쁜 평가를 받았고, 현재 수행된 트랜잭션에서 좋은 평가를 받았다면 최근 수행된 트랜잭션에서 나쁜 평가를 준 피어들이 liar로 판단된다. 이때, 현재 수행된 트랜잭션에서 나쁜 평가를 받았다면 나쁜 평가를 준 피어들과 현재 평가를 준 피어 모두 liar로 판단된다. 반대로 $n-n/2$ 미만의 좋은 평가와 $n/2$ 이상의 나쁜 평가를 받고, 현재 수행된 트랜잭션에서 나쁜 평가를 받았다면 좋은 평가를 준 피어들이 liar로 판단된다. 만약, 현재 수행된 트랜잭션에 대해 피어가 좋은 평가를 주었다면, 이전 트랜잭션에서 좋은 평가를 준 피어와 현재 평가를 준 피어가 liar로 판단된다.

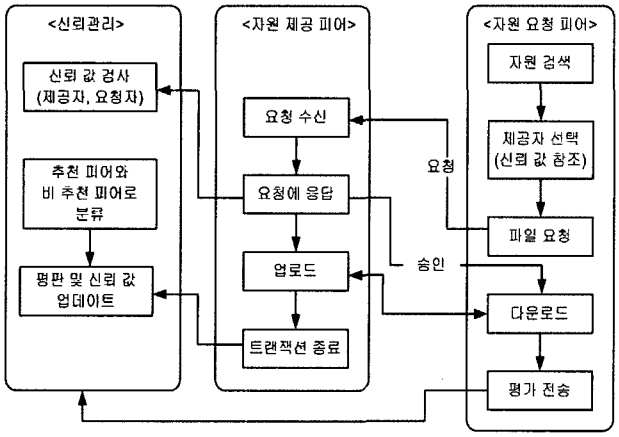
이와 같이 파일 제공 피어가 트랜잭션을 수행한 피어들로부터 받은 평가 값의 비교를 통해 liar를 판단함으로써 현재 수행된 트랜잭션에 대해 거짓 평가를 주는 피어뿐만 아니라, 이전에 수행된 트랜잭션에 대해 거짓 평가를 준 피어들에 대한 판단도 가능하다.

3.2 제안 방안의 동작

제안 방안의 세부적인 동작을 설명하기 위해 사용하는 용어는 다음과 같다.

- MS : 피어들의 공유 파일 목록 및 평판, 신뢰 값을 관리하는 서버
- P_X : 피어 X의 아이디
- r_{old_X} : 피어 X가 이전 트랜잭션 수행 결과로 받은 평가
- r_{new_X} : 피어 X가 현재 트랜잭션 수행 결과로 받은 평가
- fn_{old_X} : 트랜잭션 수행 전 피어 X의 공유 파일 수
- $fn_{new\ X}$: 트랜잭션 수행 후 피어 X의 공유 파일 수
- GR_{old_X} : 피어 X가 이전 트랜잭션까지 받은 좋은 평가의 합
- $GR_{new\ X}$: 피어 X가 현재 트랜잭션까지 받은 좋은 평가의 합
- BR_{old_X} : 피어 X가 이전 트랜잭션까지 받은 나쁜 평가의 합
- $BR_{new\ X}$: 피어 X가 현재 트랜잭션까지 받은 나쁜 평가의 합
- TP_X : 피어의 신뢰 값
- β : 피어의 신뢰 값 계산시 참조하는 가중치 (예를 들면, 참여 시간, 공유 자원 수, 통신 대역폭 등)
- α_X : 피어 X의 공유 파일 비율
- R_X : 추천 피어의 아이디
- NR_X : 비 추천 피어의 아이디
- TP_{R_X} : 추천 피어의 신뢰 값
- TP_{NR_X} : 비 추천 피어의 신뢰 값

제안 방안의 전체적인 동작을 살펴보면 (그림 2)와 같다.



(그림 2) 제안 방안의 동작

[단계 1] 로그인과 등록

① $P_i \cdots P_n \rightarrow MS$: $Login$

서비스 이용을 원하는 피어들은 서버에 로그인하고, 서버는 올바른 사용자임을 확인한 후 로그인이 정상적으로 되었음을 알리는 메시지를 전송한다.

② $P_i \cdots P_n \rightarrow MS$: $Registration(f_i \cdots f_n)$

서버로부터 응답 메시지를 받은 피어들은 공유 하고자 하는 파일 목록을 서버에 등록한다. 서버는 각 피어에 대하여 다음 정보를 검색에 용이한 구조로 데이터베이스화해서 저장하며, 피어가 새로 접속할 때마다 목록은 갱신된다. 각 피어에 대해 서버가 관리하는 정보는 다음과 같다.

$$< P_X, f_i \cdots f_n, r_X, GR_X, BR_X, TP_X, R_i \cdots R_n, NR_i \cdots NR_n >$$

[단계 2] 질의 및 응답

① $P_i \rightarrow MS$: $Query(f)$

파일 요청 피어인 P_i는 필요한 파일을 얻기 위해 해당 파일에 관한 검색 요청을 서버로 전송한다.

② $MS \rightarrow P_i$: $Send$

$$((P_j, TP_j, < R_i, TP_{R_i} >, < NR_i, TP_{NR_i} >),$$
$$\vdots$$
$$(P_n, TP_n, < R_n, TP_{R_i} >, < NR_n, TP_{NR_i} >))$$

검색 요청을 받은 서버는 저장된 목록에서 검색 요청에 일치하는 파일을 가진 피어들의 접속 여부 등을 바탕으로 피어 목록과 피어의 신뢰 값, 해당 피어를 추천한 피어와 피어의 신뢰 값, 비 추천 피어와 피어의 신뢰 값 목록을 전송한다.

[단계 3] 선택 및 다운로드

① $P_i : Selection(P_j, TP_j, < R_i, TP_{R_i} > \cdots < R_n, TP_{R_n} >,$
$< NR_i, TP_{NR_i} > \cdots < NR_n, TP_{NR_n} >)$

P_i는 식 (1)을 이용하여 파일 제공 피어의 신뢰 값과 파일 제공 피어를 추천한 피어와 추천하지 않은 피어의 신뢰 값을 함께 참조하여 파일을 요청하기 위해 하나의 피어(P_j)를 선택한다. 트랜잭션 대상을 선택하기 위해 참조하는 피어의 신뢰 값은 서버로부터 받은 정보에서 피어의 신뢰 값과 해당 피어를 추천한 피어들의 신뢰 값, 비추천 피어들의 신뢰 값을 참조하여 다음과 같이 계산한다.

$$\begin{aligned} & TP_j + (TP_{R_i} + \cdots + TP_{R_n}) - (TP_{NR_i} + \cdots + TP_{NR_n}) \\ & \vdots \\ & TP_n + (TP_{R_i} + \cdots + TP_{R_n}) - (TP_{NR_i} + \cdots + TP_{NR_n}) \end{aligned} \quad (1)$$

② P_i는 P_j에 연결을 위해 필요한 정보를 서버에 요청하고, 서버는 P_j의 IP address와 포트 번호 등 관련 정보를 전송한다.

③ P_i는 서버로부터 받은 정보를 참조하여 P_j에게 파일을 요청한다.

④ $P_j \rightarrow MS$: $Request(TP_i, TP_j)$
$P_j : Compare(TP_i, TP_j)$

P_j는 P_i의 요청에 응답하기 전 자신과 P_i의 신뢰 값을 확인하고 비교하여 비교 결과에 따라 다운로드 요청을 승인하거나, 거부하기 위해 서버로 자신과 P_i의 신뢰 값을 요청한다. 서버로부터 받은 신뢰 값을 비교하여 식 (2)와 같이 P_i의 신뢰 값이 자신의 신뢰 값 보다 크거나 같다면, 요청 파일을 전송하고 그렇지 않다면 파일을 전송할 수 없음을 알리는 메시지를 보낸다.

$$TP_i \geq TP_j : \text{파일 전송} \quad (2)$$

$$TP_i < TP_j : \text{다운로드 요청 거부} \quad (3)$$

피어들은 자신의 신뢰 값에 따라 파일을 다운로드 받을 수 있는 권한을 가지게 되므로, 거짓 평가를 주는 피어들은 많은 수의 파일을 공유하고 다른 피어들로부터 공유 파일에 대해 좋은 평가를 받는다 하더라도 liar로 판단될 경우 평판 및 신뢰 값 업데이트 식에 의해 나쁜 평판의 증가로 신뢰 값이 감소하므로 다른 피어들의 공유 파일을 다운로드 받을 수 있는 기회가 점차적으로 감소하고, 다른 피어들로부터 자신의 공유 파일에 대한 요청도 거의 일어나지 않게 되므로 이들의 참여를 감소시킬 수 있다.

[단계 4] 평가 및 업데이트

① $P_j \rightarrow MS: Notify(finish)$

트랜잭션 종료 후 P_i가 P_j에 대한 평가 값을 전송하지 않는 경우를 대비하여 P_j는 P_i로 다운로드가 종료되면, 서버에게 P_i와의 트랜잭션이 종료되었음을 알린다. 트랜잭션을 수행한 피어들로부터 받은 평가를 기반으로 계산되는 평판은 피어의 신뢰 값 계산을 위해 사용하고, 피어의 신뢰 값은 트랜잭션 참여 피어들이 신뢰할 수 있는 피어를 선택하기 위해 참조하는 값이므로, 파일 요청 피어는 다운로드 종료 후 해당 파일에 대한 평가를 전송함으로써 트랜잭션 참여 피어들이 항상 가장 최근에 업데이트 된 신뢰 값을 참조할 수 있도록 한다.

② $P_i \rightarrow MS: Send(r_j : 1 \text{ or } -1)$

P_i는 다운로드 받은 파일을 실행하여 파일이 올바르게 동작하고, 자신이 요청한 파일이 맞을 경우 1, 그렇지 않은 경우 -1을 P_j의 파일에 대한 평가 값으로 전송한다. 서버는 P_i로부터 받은 평가 값에 따라 P_i를 P_j의 추천 피어 목록 또는 비 추천 피어 목록에 등록하고, P_i로부터 받은 평가 값과 이전에 수행된 n번의 트랜잭션에서 P_j가 받은 평가 값을 비교하여, 좋은 평가의 횟수가 $n/2$ 이상인데 P_i가 나쁜 평가를 주거나, 나쁜 평가의 횟수가 $n/2$ 이상인데 P_i가 좋은 평가를 준다면, 거짓 피어 판단 기준에 의해 P_i가 liar로 판단되므로, P_i의 나쁜 평판을 다음 식과 같이 증가시킨다.

$$BR_{new_i} = BR_{old_i} + 1 \quad (4)$$

③ $MS: Update(GR_i, BR_i, TP_i, \alpha_i, GR_j, BR_j, TP_j, \alpha_j)$,
$(< GR_{R_1} \cdots GR_{R_n}, BR_{R_1} \cdots BR_{R_n}, TP_{R_1} \cdots TP_{R_n} >,$
$< GR_{NR_1} \cdots GR_{NR_n}, BR_{NR_1} \cdots BR_{NR_n}, TP_{NR_1} \cdots TP_{NR_n} >)$

<표 1> 파일 제공 피어의 평판 업데이트

이전	현재	GR	BR
$r_{old_j}=1$	$r_{new_j}=1$	$GR_{old_j}+\lvert r_{new_j}\rvert\times\alpha_j$	BR_{old_j}
$r_{old_j}=1$	$r_{new_j}=-1$	GR_{old_j}	$BR_{old_j}+\lvert r_{new_j}\rvert$
$r_{old_j}=-1$	$r_{new_j}=1$	$GR_{old_j}+\lvert r_{new_j}\rvert$	BR_{old_j}
$r_{old_j}=-1$	$r_{new_j}=-1$	GR_{old_j}	$BR_{old_j}+\lvert r_{new_j}\rvert\times\alpha$

서버는 P_i로부터 평가 값을 받고, P_j로부터 트랜잭션 종료 메시지를 받은 다음, 트랜잭션 대상 피어들의 평판과 신뢰 값을 업데이트 하고, P_j의 추천 피어와 비 추천 피어들에 대한 평판과 신뢰 값을 업데이트 한다. 파일 제공 피어의 평판은 이전에 수행된 트랜잭션과 현재 수행된 트랜잭션에서 받은 평가 값에 따라 <표 1>과 같이 4가지 방법으로 나누어 좋은 평판과 나쁜 평판을 업데이트 한다.

파일 제공 피어가 이전에 수행된 트랜잭션과 현재 수행된 트랜잭션 모두에서 좋은 평가를 받았다면, 좋은 평판은 이전의 값에 더하여 α만큼 증가시키고 나쁜 평판은 이전의 값을 유지한다. 이전에 수행된 트랜잭션과 현재 수행된 트랜잭션 모두에서 나쁜 평가를 받았다면, 나쁜 평판은 이전의 값에 더하여 α만큼 증가시키고, 좋은 평판은 이전의 값을 유지한다. 이전에 수행된 트랜잭션과 현재 트랜잭션에서 서로 다른 평가를 받았다면, 현재 트랜잭션의 결과로 받은 평가 값에 따라 평판을 계산한다. 즉, 좋은 평가를 받았다면, 좋은 평판은 증가시키고 나쁜 평판은 이전의 값을 유지하고, 나쁜 평가를 받았다면, 나쁜 평판은 증가시키고 좋은 평판은 이전의 값을 유지한다.

이와 같은 업데이트 방법을 이용함으로써 계속적으로 좋은 평가를 받는 피어의 좋은 평판은 점차적으로 증가하고, 계속적으로 나쁜 평가를 받는 피어는 나쁜 평판이 점차적으로 증가한다. 평판 업데이트에 사용하는 α는 피어들이 공유하는 파일 수에 대한 비율을 나타내는 값으로, 자신의 자원을 많이 공유하고, 공유하는 자원들이 올바르게 동작함으로써 트랜잭션마다 좋은 평가를 받는 피어들에게 인센티브를 주기 위해 사용할 수 있으며, 다음 식을 사용하여 계산한다.

$$\alpha_X = \frac{fn_{old_X}}{fn_{new_X}} \quad (5)$$

fn_{new}는 트랜잭션 수행 후 피어가 가지는 공유 파일 수를 나타내고, fn_{old}는 트랜잭션 수행 전 피어가 가지는 공유 파일 수를 나타내는 값으로, 일반적으로 피어들 간에 업로드/다운로드 트랜잭션이 일어날 때 파일 제공 피어의 공유

파일 수는 변함이 없고, 파일 요청 피어의 공유 파일 수가 늘어나지만, 이론적으로 파일 제공 피어의 공유 파일 수는 감소하고, 파일 요청 피어의 공유 파일 수는 증가하는 것으로 볼 수 있다. 이러한 원리를 이용하여 식 (5)와 같이 피어들의 공유 파일 수에 대한 비율을 계산하면, 파일을 계속 제공하는 피어의 α 값은 증가하고, 파일을 계속 요청하는 피어의 α 값은 감소한다. 그러므로, 피어들이 많은 수의 파일을 제공하고, 제공된 파일에 대해 좋은 평가를 받는다면 <표 1>의 업데이트 식에 의해 좋은 평판이 α 만큼 증가하고, 이 값을 기반으로 계산되는 피어의 신뢰 값 또한 증가한다. 반면, 많은 수의 파일을 제공하여 α 값은 증가했지만, 파일을 이용한 피어들로부터 나쁜 평가를 받는다면, 나쁜 평판이 α 값만큼 증가하므로 신뢰 값은 감소한다.

파일 요청 피어의 평판은 트랜잭션을 수행한 대상에 대한 평가 값의 전송 여부에 따라 다음 식을 사용하여 업데이트 한다.

$$GR_{new\ i} = GR_{old_i} \times \alpha_i \tag{6}$$

$$BR_{new\ i} = BR_{old_i} + 1 \tag{7}$$

파일 제공 피어로부터 자원을 받고 확인한 다음 해당 자원에 대한 평가를 서버로 전송하면, 파일 요청 피어의 좋은 평판을 식 (6)과 같이 α 만큼 감소시키고, 새로운 트랜잭션을 위하여 검색을 요청할 때까지 평가를 전송하지 않거나, 평가의 전송 없이 서비스를 종료하면 식 (7)과 같이 나쁜 평판을 증가시킨다. 특정 피어가 계속적으로 다운로드 트랜잭션을 수행하는 것을 제한하고, 업로드 트랜잭션을 수행하는 피어에 대해서는 가산점을 주는 등 파일 제공 피어와 요청 피어의 서비스 이용에 대해 공정성을 제공하기 위해 평가 값을 전송하더라도 다운로드 트랜잭션을 수행하였기 때문에 좋은 평판을 감소시킨다.

업데이트된 피어들의 좋은 평판과 나쁜 평판을 기반으로 트랜잭션 대상 선택을 위해 참조하는 피어의 신뢰 값은 식 (8)을 사용하여 계산한다.

$$TP_X = \frac{GR_{new\ x} - |BR_{new\ x}|}{GR_{new\ x} + |BR_{new\ x}|} \times \beta \tag{8}$$

신뢰 값 계산에 사용하는 β는 피어의 좋은 평판과 나쁜 평판 뿐만 아니라 트랜잭션 참여 시간이나 공유 파일의 크기, 다운로드 속도 등의 다른 파라메터를 추가함으로써 피어의 신뢰성을 향상시키기 위해 사용하는 값이다. 식 (8)을 통해 파일 제공 피어가 계속되는 트랜잭션에서 좋은 평가를 받는다면 좋은 평판의 증가로 신뢰 값이 함께 증가하고, 나쁜 평가를 받는다면 나쁜 평판의 증가로 신뢰 값이 감소함을 알 수 있다. 트랜잭션 대상을 선택하기 위해 피어들의 신뢰 값을 참조함으로써 악의적인 목적을 가진 피어들의 참여를 감소시킬 수 있고, 올바른 자원을 가진 피어들과 트랜잭션 수행이 가능하다. 평판 정보를 이용하여 계산되는 신뢰 값이 피어들에 대한 절대적인 신뢰를 제공하는 것은 아니지만, 트랜잭션 실행시 발생할 수 있는 위험을 최소화하는데 도움을 줄 수 있다.

P_j에 대한 추천 피어와 비 추천 피어들의 평판과 신뢰 값에 대한 업데이트는 다음과 같이 수행한다. 이전에 수행된 n번의 트랜잭션에서 P_j가 받은 좋은 평가 횟수가 $n/2$ 이상이고, 현재 수행된 트랜잭션에 대해서도 좋은 평가를 받는다면, P_j의 비 추천 피어 목록에 있는 피어들이 liar로 판단되므로, 추천 피어들에 대해서는 좋은 평판을 증가시키고 liar로 판단된 비 추천 피어들에 대해서는 나쁜 평판을 증가시킨다. 추천 피어와 비 추천 피어의 평판은 식 (9)를 사용하여 업데이트하고, 이들의 신뢰 값은 식 (10)을 사용하여 업데이트 한다.

$$\begin{aligned} &R_i \cdots R_n :\ GR_{new} = GR_{old} + 1,\ BR_{new} = BR_{old} \\ &NR_i \cdots NR_n :\ GR_{new} = GR_{old},\ BR_{new} = BR_{old} + 1 \end{aligned} \tag{9}$$

$$TP_X = \frac{GR_{new} - |BR_{new}|}{GR_{new} + |BR_{new}|} \tag{10}$$

이전에 수행된 n번의 트랜잭션에서 P_j에 대해 나쁜 평가를 준 피어 수가 $n/2$ 이상이고, 현재 수행된 트랜잭션에 대해서도 나쁜 평가를 받는다면, P_j의 추천 피어 목록에 있는 피어들이 liar로 판단되므로, 비 추천 피어들에 대해서는 좋은 평판을 증가시키고, liar로 판단된 추천 피어들에 대해서는 나쁜 평판을 증가시킨다. 비 추천 피어와 추천 피어의 평판은 식 (11)을 사용하여 업데이트하고, 이들의 신뢰 값은 식 (10)을 사용하여 업데이트 한다.

$$\begin{aligned} &R_i \cdots R_n : GR_{new} = GR_{old},\ BR_{new} = BR_{old} + 1 \\ &NR_i \cdots NR_n :\ GR_{new} = GR_{old} + 1,\ BR_{new} = BR_{old} \end{aligned} \tag{11}$$

이와 같이 제안 방안에서는 특정 피어에 대한 추천 피어와 비 추천 피어 정보를 이용함으로써 현재 수행된 트랜잭션에 대해 거짓 평가를 주거나 이전에 수행된 트랜잭션에서 거짓 평가를 준 피어들에 대한 판단이 가능하다.

4. 제안 방안의 분석

제안 방안은 파일 공유 서비스에서 신뢰할 수 있는 트랜잭션 대상자 선택을 위해 참조하는 평판 정보에 대하여 신뢰성을 제공하기 위해 특정 피어와 트랜잭션을 수행한 경험이 있는 피어들이 준 평가 값의 참조를 통해 특정 피어가 거짓 평가를 주거나 주었을 가능성이 있음을 판단하고, 이들의 신뢰 값을 감소시켜 서비스 참여를 제한하고자 한다.

제안 방안과 유사한 2장의 관련 연구에서 설명한 FCRS 방안[7]과 비교하면 제안 방안은 중앙 서버가 존재하는 하이

〈표 2〉 제안 방안과 FCRS의 비교

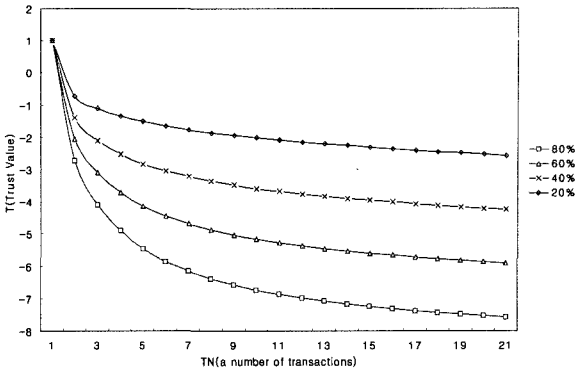
	FCRS[7]	제안 방안
서비스 방식	순수 P2P	하이브리드 P2P
평가 대상	파일	피어
Liar를 찾는 방법	추천 피어와 비 추천 피어 정보 참조	추천 피어와 비 추천 피어 정보 참조
트랜잭션 대상 선택 방법	추천피어, 비 추천 피어의 신뢰 값 참조	추천 피어, 비 추천 피어, 트랜잭션 대상 피어의 신뢰 값 모두 참조
이전 트랜잭션에서 거짓 평가를 준 피어에 대한 처리	고려하지 않음	평가 값의 비교를 통해 liar 판단 가능

브리드 P2P 방식으로 동작하며 파일 제공 피어의 신뢰 값과 해당 파일을 사용한 경험이 있는 피어들이 제공하는 평가에 따라 구분된 추천 피어와 비 추천 피어의 신뢰 값을 함께 참조하여 트랜잭션 대상 피어를 선택함으로써 신뢰할 수 없는 파일에 대한 다운로드 수를 감소시킬 수 있고, 현재 트랜잭션을 수행한 피어들의 평가 의견과 이전에 트랜잭션을 수행한 피어들의 평가 의견의 비교를 통해 평가에 대한 거짓 여부를 판단할 수 있다. 또, 트랜잭션 대상을 선택할 때 추천/비 추천 피어들의 정보뿐만 아니라 해당 파일을 가진 피어의 신뢰 값도 함께 참조하며, 트랜잭션을 수행한 피어들 간의 의견 비교를 통해 현재 수행된 트랜잭션에서 거짓 평가를 주는 피어에 대한 판단뿐만 아니라 이전에 수행된 트랜잭션에서 거짓 평가를 준 피어들에 대한 판단도 가능하다. <표 2>에서는 제안 방안과 유사한 FCRS 방안의 차이를 설명하고 있다.

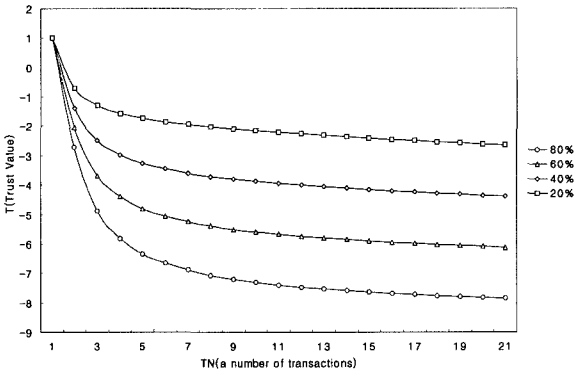
4.1 시뮬레이션 결과

시뮬레이션을 통해 다운로드 트랜잭션에 대해 거짓 평가를 주는 피어들의 신뢰 값의 변화를 살펴보면 (그림 3)과 같다. 트랜잭션에 참여한 전체 피어 수는 100 피어이고, 피어별 공유 파일 수는 100개로 동일하며, 초기 평판과 신뢰 값은 1로 설정하였고, 거짓 평가를 주는 피어의 비율을 <80%, 60%, 40%, 20%>로 지정하여 시뮬레이션 하였다. x축은 liar들이 수행한 트랜잭션 횟수를 나타내고, y축은 liar들의 신뢰 값의 합을 나타내며, liar의 수가 많아질수록 신뢰 값의 감소가 더 많이 일어남을 알 수 있다.

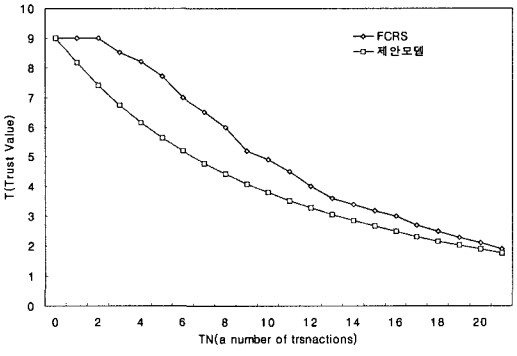
(그림 4)는 트랜잭션에 참여하는 피어들이 다운로드 트랜잭션에 대해 거짓 평가를 주고, 업로드 트랜잭션에 대해 신뢰할 수 없는 파일을 제공한 경우 신뢰 값의 변화를 나타낸 그래프이다. 트랜잭션에 참여한 전체 피어 수는 100 피어이고, 피어별 공유 파일 수는 100개로 동일하며, 초기 평판과 신뢰 값은 1로 설정하였고, 거짓 평가를 주는 피어의 비율과 신뢰할 수 없는 파일을 제공하는 피어의 비율은 <80%, 60%, 40%, 20%>로 지정하여 시뮬레이션 하였다. x축과 y축은 (그림 3)과 동일하며, liar의 비율과 잘못된 파일의 업로드에 대한 비율이 증가할수록 신뢰 값이 계속적으로 감소함을 알 수 있다.



(그림 3) liar의 신뢰 값의 변화



(그림 4) 신뢰할 수 없는 파일 제공, liar의 신뢰 값의 변화



(그림 5) 제안 방안과 FCRS의 비교

(그림 5)는 제안 방안과 FCRS에서 거짓 평가를 주는 피어의 신뢰 값 변화를 보여주고 있다. 트랜잭션에 참여한 전체 피어 수는 100 피어이고, 피어별 공유 파일 수는 100개로 동일하며, 초기 평판은 좋은 평판의 경우 공유 파일의 개수를 기반으로 파일 하나당 0.1로 지정하여 10으로 지정하고, 나쁜 평판은 1로 지정하였다. 거짓 평가를 주는 피어의 비율은 50%로 지정하여 시뮬레이션 하였다. x축과 y축은 (그림 3)과 동일하며, 동일한 비율의 liar가 있을 때 제안 방안의 신뢰 값의 변화가 더 큰 것을 알 수 있다.

5. 결 론

본 논문에서는 P2P 파일 공유 서비스에서 참여자들이 트랜잭션 대상을 선택하기 위해 참조하는 평판 정보에 대한 정확성을 위해 수행된 트랜잭션에 대해 거짓 평가를 주는 피어들을 판단하여 트랜잭션 참여를 제한함으로써 이들의 수를 감소시키기 위한 방안을 제안하였다. 뿐만 아니라 제안 방안은 트랜잭션 대상을 선택할 때 파일 제공 피어의 신뢰 값뿐만 아니라 파일 제공 피어에 대한 추천 피어와 비추천 피어의 신뢰 값을 함께 참조함으로써 트랜잭션 대상에 대한 신뢰성을 향상시킬 수 있다.

참 고 문 헌

[1] D. S. Milojicic, V. Kalogeraki, R. Lukose, K. Nagaraja, J. Pruyne, B. Richard, S. Rollins, and Z. Xu, "Peer-to-Peer Computing," HPTechReport HPL-2002-57, 2002.

[2] 신정화, 이영경, 이경현, "P2P 환경에서 SPKI 인증서를 이용한 접근 제어", 정보처리학회논문지 C 제10-C권 제6호, pp.793-798, 2003.

[3] A. Josang, R. Ismail, and C. Bboyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, 2005.

[4] 이계완, "P2P 비즈니스 모델과 관련 동향", SKC&C R&D 부문 기술동향 보고서, 2001.

[5] J. Aslund, "Authentication in Peer-to-Peer Systems", Undergraduate thesis, Linkoping University, 2002.

[6] S. Saroiu, P.K. Gummadi, and S. D. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proceedings of Multimedia Computing and Networking 2002(MMCN'02), 2002.

[7] S. Y. Lee, O. H. Kwon, J. Kim, and S. J. Hong, "A Trust Management Schemes in Structured P2P Systems," Fourth International Workshop on Agents and Peer-to-Peer Computing(AP2PC 2005), pp.37-50, 2005.

[8] L. Mekouar, Y. Iraqi, and R. Boutaba, "Peer-to-Peer's most wanted: Malicious peers," In International Computer Networks Journal, Special Issue on Management in Peer-to-Peer Systems:Trust, Reputation and Security, Vol.50, No.4, pp.545-562, 2006.

[9] Y. Wand and J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks," Proceedings of IEEE Conference on P2P Computing, pp.150-157, 2003.

신 정 화

e-mail : shinjh@pknu.ac.kr

1997년 한국방송통신대학교 컴퓨터과학과 (이학사)

2000년 부경대학교 전산정보학과(이학석사)

2006년 8월 부경대학교 전자계산학과 (이학박사)

관심분야 : 암호이론, 네트워크 보안, P2P Security, Reputation Management System

이 경 현

e-mail : khrhee@pknu.ac.kr

1982년 경북대학교 수학교육과(학사)

1985년 한국과학기술원 응용수학과(이학석사)

1992년 한국과학기술원 수학과(이학박사)

1982년~1993년 3월 한국전자통신연구소 선임연구원

1993년 3월~현재 부경대학교 전자컴퓨터정보통신공학부 교수

1997년 12월~현재 한국멀티미디어학회 학술이사, (현)재무이사, 논문지 편집위원

관심분야 : 암호이론, 멀티미디어 정보보호, 네트워크 보안, 암호프로토콜