P2P 파일 공유 시스템에서 평판 정보를 이용한 접근 제어

신 정 화[†] · 신 원[††] · 이 경 현[†††]

요 약

P2P 서비스는 인터넷 상에서 서버를 거치지 않고 정보를 찾는 사람과 정보를 가진 사람의 컴퓨터 간의 직접적인 연결을 통해 다양한 정보를 공유할 수 있는 방식으로, 파일의 자유로운 교환을 위한 방법으로 많은 인기를 얻고 있다. 그러나 P2P 파일 공유 시스템에서 서비스를 이용하는 모든 사용자들은 동등한 접근 권한으로 자유롭게 여러 사용자들의 공유 파일을 이용할 수 있기 때문에, 자신의 파일에 대한 공유 없이 다른 사용자들의 공유 파일을 다운로드만 하는 "free riding" 문제가 빈번하게 발생하고 있으며, 바이러스나 웜을 포함한 파일을 공유하거나 실제 내용과 다른 제목을 가지는 파일을 공유하는 사용자라 하더라도 제한 없이 파일 공유 서비스를 이용할 수 있다. 이에 본 논문에서는 파일 공유 서비스를 이용하는 사용자들의 신뢰도를 나타낼 수 있는 평판(Reputation) 정보를 이용하여 빈번한 다운로드를 행하는 "free rider"의 접근을 제한하고, 정상적인 실행이 되지 않는 파일을 공유한 사용자들에 대해서도 다른 사용자들의 공유 파일에 대한 사용을 제한하고자 한다.

키워드 : P2P, 평판, 접근제어, 파일공유시스템, free rider

An Access Control using Reputation Information in P2P File Sharing System

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

ABSTRACT

P2P service is a method that can share various information through direct connection between computer of a person who find information and a person who have information without server in the Internet and it is getting a lot of popularity by method for free exchange of file. P2P file sharing systems have become popular as a new paradigm for information exchange. Because all users who use service in P2P file sharing system can use shared files of several users freely by equal access privilege, it is happening the "free riding" that only download shared file of other users without share own files. Although a user share a malicious file including virus, worm or file that have title differing with actuality contents, can use file sharing service without limitation. In this paper, we propose a method that restrict access of "free rider" that only download using reputation information that indicate reliability of user. Also, we restrict usage on shared file of other users about users who share harmful file.

Key Words : Peer-to-Peer, Reputation, Access Control, File Sharing System, Free Rider

1. 서 론

P2P(Peer-to-Peer) 기술이란 고성능 중앙서버나 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 말한다. P2P 기술은 집중된 서버의 처리를 각각의 클라이언트들이 나누어 수행하므로 클라이언트 수가 증가할수록 많아지는 서버의 처리 용량과 통신 대역폭에 대한 제한점을 해결해주는 이점을 가지는 반면, 피어 프로그램의 유지 보수의 부담, 시스템 운영의 안정성과 신뢰도 문제, 개방되고 분산되어 있는 만큼 사용자들이 책임성을 가지고 행동해야 하는 단점을 가진다[1]. 그러나 P2P 기술은 소리바다나 Napster, e-Donkey와 같은 파일 공유 서비스와 인스턴트 메신저 같은 실시간 커뮤니케이션 서비스 등을 통해 기술적 잠재력을 입증 받았고, 저비용/고효율로 정보 확산에 탁월하다는 장점을 인정받으면서 파일 공유뿐만 아니라 CPU나 디스크와 같은 컴퓨팅 자원의 공유, 온라인 협업, 전자상거래 등 다양한 분야에 응용될 수 있다[2].

파일 공유는 가장 빈번하게 행해지고 있는 작업으로 사용자들이 손쉽게 자신이 필요로 하는 파일을 얻을 수 있는 이점을 가지는 반면, 실제적인 파일 공유에 있어 대부분 사용자들은 자신의 파일에 대한 공유 없이 다른 사용자들의 공유 파일을 다운로드만 하는 "free riding" 문제가 빈번하게 발생하고 있다[3, 4].

† 준 회 원 : 부경대학교 대학원 전자계산학과
†† 정 회 원 : 동명정보대학교 정보보호학과 전임강사
††† 종신회원 : 부경대학교 전자컴퓨터정보통신공학부 교수
논문접수 : 2005년 6월 22일, 심사완료 : 2005년 12월 12일

본 논문에서는 P2P 파일 공유 서비스에 참여하는 사용자들의 신뢰도를 나타낼 수 있는 "평판" 정보를 이용하여 공유 파일에 대한 자유로운 사용을 제한함으로써 파일 공유에서 빈번하게 발생하는 "free riding" 문제를 해결하고, 바이러스나 웜이 포함된 파일이나 질이 낮은 파일 또는 실제 내용과 다른 제목의 파일을 제공하는 사용자들에 대해서도 다른 사용자들의 공유 파일에 대한 사용을 제한하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 P2P 서비스 개요와 P2P 파일 공유에서의 고려사항, 기존의 평판 정보를 이용한 파일 공유 방법에 대해 살펴본다. 3장에서는 본 논문에서 제안하는 P2P 파일 공유 시스템에서 평판 정보를 이용한 접근 제어의 동작 방식을 설명한다. 4장에서는 제안 방안을 분석하고, 기존의 방법들과 비교를 다룬 다음 5장에서 결론을 맺는다.

2. 관련연구

2.1 P2P 서비스

P2P(Peer-to-Peer)는 인터넷에서 서버 컴퓨터를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 컴퓨터를 직접 연결시켜 데이터를 공유할 수 있게 해주는 기술과 그 기술을 응용해서 제공되는 서비스를 말한다. P2P가 가지는 가장 중요한 기술적 의미 중의 하나는 자원의 분산에 있다고 할 수 있다. 클라이언트/서버 방식에서는 파일을 공유하기 위해서 특정 서버에 공유할 파일을 올리고 모든 사용자들은 이 서버를 통해 다운로드를 받아야만 했다. 이러한 방식은 하나의 서버에 필요 이상의 부하를 주고, 서버에 문제가 발생할 경우 서비스 제공이 중단되는 단일지점오류가 발생할 수 있지만, P2P 방식은 사용자들 간의 직접적인 연결을 통하여 서로의 파일을 공유할 수 있기 때문에 여러 서버로 트래픽이 분산되어 병목 현상이나 단일지점오류를 피할 수 있고 확장성을 제공할 수 있다[2, 3].

P2P에서는 통신이 가능한 모든 정보 단말을 "피어"라고 하며, 기존의 네트워크 모델에서 단순히 클라이언트로 동작하던 개인용 PC, 모바일 단말 혹은 통신 가능한 가전제품도 모두 하나의 "피어"가 될 수 있다. P2P를 이용하여 제공될 수 있는 서비스로 파일 공유 및 협업, 인터넷 쇼핑 및 경매 서비스, 인터넷 콘텐츠 검색과 제공 등이 있다[2].

2.2 P2P 파일 공유에서 고려사항

P2P 파일 공유에서는 파일을 제공하는 사람 수와 제공받는 사람 수의 균형을 생각해야 한다. 양쪽 모두 충분히 참여하고 서로 협력해야만 P2P 본래의 기능을 발휘할 수 있다. 그러나, 실제 P2P 서비스 이용에 있어 서비스 참여자들은 자신의 파일에 대한 공유 없이 다운로드만 하거나, 다른 참여자로부터 온 질의를 전달하지도 않고, 응답도 하지 않으면서 자신의 질의만 보내는 경우가 빈번하게 발생한다. 이와 같은 동작을 "free riding"이라 하고, free riding을 행하는 사용자를 "free rider"라고 한다[5].

최근 분석에 의하면 Gnutella 서비스 사용자 중 70%는 자신의 파일에 대한 공유 없이 다운로드만 수행한다고 한다. "free rider"가 많아지면 많아질수록 공유를 위해 파일을 제공하는 사용자들에게는 처리 속도나 트래픽 증가로 인해 시스템 성능이 저하되는 것으로 보이고, 계속적으로 시스템 성능이 저하된다면 사용자들은 점차적으로 해당 시스템을 이용하지 않게 될 것이고, 결과적으로 사용자들의 참여를 낮추는 결과를 초래하게 된다[3, 4].

평판(Reputation)[5]은 파일이나 사용자에 대한 신뢰도를 나타낼 수 있는 정보로써 P2P 파일 공유 서비스에서 "free riding"을 해결하는 방안으로 사용될 수 있다. 예를 들면, 공유 파일 요청자는 자신이 원하는 파일을 다운로드 하기 위해 파일 제공자를 선택할 때 해당 파일이나 파일 제공자에 대한 사전 정보가 없기 때문에 대부분 파일 제공자가 제공하는 정보에 의존하여 모든 것을 판단하고 선택하게 된다. 만약, 파일 제공자가 실제 내용과 다른 파일 제목을 제공하거나 바이러스나 웜 등을 포함한 파일 또는 매우 질이 낮은 파일을 제공한다 하더라도 공유 파일 요청자는 그것을 확인할 수 있는 어떠한 정보도 가지고 있지 않다. 그러므로 공유 파일 요청자는 직접적인 다운로드를 통해 확인하지 않고서는 해당 파일에 대한 정확성 여부를 판단하기가 어렵다. 이런 경우 공유 파일 요청자는 원하는 파일과 파일 제공자를 선택할 때 해당 파일을 이미 사용한 사용자들의 경험에 의한 의견이나 소문을 참조하여 파일과 파일 제공자를 선택할 수 있을 것이다. 이때 사용되는 사용자들의 의견이나 소문이 "평판" 정보이다.

평판은 과거 트랜잭션의 결과로 얻어지는 값으로 앞으로 일어날 트랜잭션을 예상하는데 많은 도움을 줄 수 있다. P2P 서비스 이용자들은 평판으로 알려진 이용자들의 과거 행동의 피드백을 수집하고, 모든 이용자들이 자유롭게 볼 수 있도록 알림으로써 평판 정보를 통해 신뢰할 수 있는 파일 및 파일 제공자 선택이 가능하다.

2.3 "평판" 정보를 이용한 파일 공유 기법

(1) P2PRep [6]

분산된 polling 알고리즘을 기반으로 피어의 평판에 관한 정보를 공유하기 위해 제안된 방법으로 피어들은 서비스를 이용중인 모든 피어들에게 필요로 하는 자원에 대한 검색 질의를 전송한다. 검색 질의를 받은 피어들은 자원 요청 피어의 요구 사항에 일치하는 자원을 가진 경우 응답하게 된다. 자원 요청 피어는 이 중 몇몇 피어를 선택하고, 선택된 피어들에 대한 신뢰도 확인을 위해 여러 피어들에게 평판을 질의하고 응답을 받는다. 피어들로부터 받은 평판에 대한 정확성을 확인하기 위해 평판을 제공한 피어에 연결하여 확인한 후 가장 높은 평판을 가지는 피어에게 자원을 요청한다. 이와 같은 평판 정보의 사용을 통해 자원 요청 피어들은 신뢰할 수 있는 자원 제공 피어 선택이 가능하다. 반면, Gnutella[8] 같은 환경으로 동작함으로 인해 자원 제공 피어에 대한 평판을 수렴하는 과정에서 통신량이 가중되고, 평판이 높은 특정 피어로만 다운로드 요청이 집중된다.

(2) XRep [7]

P2PRep를 확장한 방식으로 분산된 polling 알고리즘을 기반으로 피어 평판과 자원 평판을 함께 사용하며, P2P 서비스를 이용하는 피어가 다른 피어들에 대한 경험과 정보를 저장하고 이에 대하여 요구가 있을 때 이를 공유할 수 있도록 한다. 자원을 필요로 하는 피어는 자신의 주변에 있는 피어들에게 찾고자 하는 자원에 대한 질의를 전송한다. 질의를 받은 피어들 중 해당 자료를 가진 피어는 자료의 수, IP, port 등의 정보를 전송한다.

자원 요청 피어는 그 중 몇몇 피어를 선택하여 자원과 자원을 제공하는 피어에 대한 평판을 주변 피어들에게 질의하고 응답을 받는다. 피어들로부터 받은 평판의 정확성을 확인하기 위해 평판 제공 피어에 질의하여 평판 값에 대해 다시 한번 확인한 후 높은 평판을 가지는 최적의 피어를 선택하여 자원을 다운로드 받는다. 이때, 최적의 피어가 유일하게 선택된다면 대부분의 피어들은 높은 평판을 가지는 피어에 자원 다운로드를 요청하게 되므로 실행 효율에 있어 병목현상을 일으키게 된다. 그러므로 피어들은 최적 제공자에게 제공여부에 대한 질의를 먼저 한 후 현재 자원 제공이 불가능하다면 다른 제공자를 찾아 다운로드 받는다.

반면, Gnutella와 같은 환경으로 동작하므로 자원 제공자 선택 후 여러 피어들로부터 평판을 수렴하는 과정에서 통신량이 가중되는 단점을 가진다.

(3) EigenRep [9]

P2P 네트워크에서 인증되지 않은 파일의 다운로드 수를 감소시키기 위해 제안된 알고리즘이다. 피어들의 upload history를 기반으로 unique global trust value를 각 피어에 할당하고 다운로드를 위한 피어를 선택하기 위해 global trust value를 사용함으로써 악의적인 피어들을 효율적으로 식별하고 네트워크에서 분리 가능하다. 각 피어들의 global reputation은 다른 피어들에 의해 피어에 할당된 트랜잭션 수행 결과의 합(local trust value)에 의해 주어진다.

(4) 대부분 P2P 파일 공유 네트워크는 서비스를 이용하는 모든 피어들에게 모든 파일을 다운로드 할 수 있는 권한을 부여하므로 악의적인 사용자의 파일이나 올바르지 않은 파일의 공유가 빈번하게 발생할 수 있다. 이를 막기 위해 [10]에서는 개별 피어들이 자신의 공유 파일에 대해 자율적인 접근 제어가 가능하도록 DAC(Discretionary Access Control) 모델[11]을 기반으로 신뢰(trust)와 평판 모델, 접근 제어 기능을 통합하여 P2P 파일 공유 네트워크에 적용함으로써 서비스를 이용하는 개별적인 피어들에 대한 접근 제어가 가능하도록 하였다. [10]의 방법은 일반적인 방법이기 때문에 특별한 수정 없이 다른 분산 애플리케이션에도 적용 가능하다.

3. P2P 파일 공유 시스템에서 평판 정보를 이용한 접근 제어

본 논문은 혼합형(Hybrid) P2P 방식을 기반으로 피어들의 신뢰도를 나타낼 수 있는 평판 정보를 이용한 접근 제어를 통해 파일 공유시 빈번하게 발생하는 "free riding" 문제를 해결하는데 목적이 있다. 또, 바이러스나 웜이 포함된 파일을 공유하거나 질이 낮은 파일 또는 내용과 다른 제목의 파일을 제공하는 피어들에 대하여 다른 피어들의 공유 파일에 대한 사용을 제한하고자 한다.

본 논문에서는 개별 피어들에 대한 평판 정보는 서버가 관리하고, 피어들 간의 접근 제어를 위해 공유 파일에 가중치를 설정한다. 특정 피어가 필요로 하는 파일에 대해 질의할 때 서버는 해당 파일을 가진 피어 목록과 피어들에 대한 평판 값을 함께 알려준다. 특정 파일을 요청한 피어들은 파일 제공 피어들의 신뢰도를 나타내는 평판 값을 참조하여 다운로드를 원하는 대상 피어를 선택한 후 파일을 요청하고, 파일 제공 피어는 파일 요청 피어의 평판과 요청한 파일의 가중치를 비교하여 다운로드 요청을 승인하거나 거부한다.

본 논문에서 사용되는 표기법과 세부적인 동작 방식은 다음과 같다.

3.1 표기법

〈표 1〉 표기법

Notation	설명
S	서비스 이용 피어들의 공유 파일 목록 및 평판 정보를 관리하는 서버
P_i	피어 i의 ID
RV_{P_i}	피어 i에 대한 최종 평판 값
RV_{P_i}'	업데이트하기 이전의 피어 i의 평판 값
f_{P_i}	피어 i가 등록한 공유 파일 목록
r_{P_i}	공유 파일을 다운로드 한 피어 i로부터 받는 평판 값
n_{P_i}	피어 i의 공유 파일 수
α_{P_i}	피어 i의 공유 파일의 가중치

3.2 동작 방식

제안 방안은 3단계로 동작이 이루어진다. 먼저 서비스에 참여하는 모든 피어들은 파일 공유 서비스를 이용하기 위해 최초에 서버에 접속할 때 사용자 인증 절차를 통해 인증서를 발급 받는다. 인증서는 피어간의 상호 인증을 위해 사용한다. 첫 번째 단계는 로그인과 공유 파일 목록 등록 단계로 서비스 이용을 원하는 피어들은 서버에 로그인하여 다른 피어들과 공유 하고자 하는 파일 목록을 등록한다. 두 번째 단계는 파일 검색과 다운로드 단계로 피어들은 필요한 파일에 대한 검색 질의를 서버로 전송하고, 서버는 해당 파일을 가진 피어 목록과 피어에 대한 평판 값을 알려준다. 질의를 요청한 피어는 피어들의 평판 값을 참조하여 하나의 피어를 선택하고, 해당 피어로 자신이 필요로 하는 파일에 대한 다운로드를 요청한다. 파일 제공 피어는 파일 요청 피어의 평판 값과 요청 대상 파일의 가중치를 비교하여 다운로드 요청을 승인하거나 거부한다. 세 번째 단계는 평가 단계로 파일을 다운로드 받아 이용한 요청 피어는 해당 파일이 올바르게 실행되고 서버에 등록된 제목과 동일한 내용을 가진 파일인지 확인하여 서버로 해당 피어에 대한 평판을 전송하고, 서버는 트랜잭션이 일어난 피어들에 대한 평판 값과 피어들의 공유 파일에 대한 가중치를 업데이트 한다.

3.2.1 로그인과 등록 단계

(1) $P_A \rightarrow S : Login$, $S \rightarrow P_A : Success$

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

(2) $P_A \rightarrow S : Register(f_{P_A})$

서버로부터 응답 메시지를 받은 피어들은 자신이 가진 파일 중 공유 하고자 하는 파일 목록을 서버에 등록한다. 개별 피어에 대해 서버가 관리하는 정보는 다음과 같다.

$< P_A, f_{P_A}, RV_{P_A} >$

- P_A : 공유 파일을 등록한 피어의 아이디
- f_{P_A} : 피어 P_A의 공유 파일 목록
- RV_{P_A} : 피어 P_A의 평판 값

서버는 피어들이 등록한 공유 파일 수와 공유 파일의 가중치를 기반으로 피어에 대한 초기 평판 값을 계산한다. 본 논문에서 공유 파일에 대한 초기 가중치는 0.1로 설정하고, 피어들 간의 트랜잭션 발생에 따라 평판 값을 공유 파일수로 나누어 설정한다. 파일 가중치 계산식은 다음과 같다.

$$\alpha_{P_A} = RV_{P_A} / n_{P_A} \quad (1)$$

피어들에 대한 초기 평판은 아래 식과 같이 공유 파일 수에 파일 가중치를 곱해서 계산한다.

$$RV_{P_A} = n_{P_A} \times \alpha_{P_A} \quad (2)$$

피어가 처음 로그인한 경우는 해당 피어에 대한 사전 정보가 없기 때문에 공유 파일 수와 파일의 초기 가중치 값을 기반으로 평판을 설정하지만, 여러 피어들과 트랜잭션이 발생하게 되면 이전에 받은 평판 값과 현재 트랜잭션의 결과로 받은 평판 값, 공유 파일의 가중치 값의 조합으로 피어의 평판을 재계산한다.

3.2.2 파일 검색과 다운로드 단계

(그림 1)은 이 단계에 대한 개략적인 순서를 나타낸다.

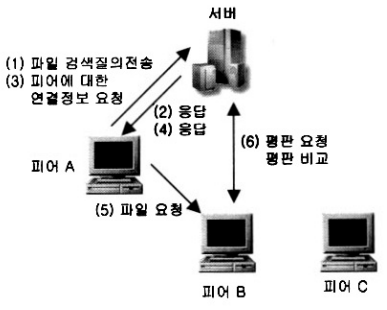
(1) $P_A \rightarrow S : Query(f)$

P_A는 필요한 파일에 대한 검색을 위해 서버로 파일 검색에 관련된 질의를 전송한다.

(2) $S \rightarrow P_A : Info((P_1, RV_{P_1}), \cdots (P_n, RV_{P_n}))$

서버는 P_A의 질의에 일치하는 파일을 가진 피어 목록과 피어의 신뢰도를 나타내는 평판 값을 함께 전송한다.

(3) P_A는 각 피어에 대한 평판 값을 참고하여 하나의 피어(P_B)를 선택하고, 해당 피어로 연결을 위해 필요한 정보를 서버에 요청한다.



(그림 1) 파일 검색과 다운로드

(4) $S \rightarrow P_A : Send(IP_{P_B}, port\_num_{P_B})$

서버는 P_B의 IP address와 포트 번호를 포함하는 메시지를 전송한다.

(5) $P_A \rightarrow P_B : File\_request(f)$

P_A는 서버로부터 받은 정보를 이용하여 P_B에게 파일 다운로드 요청 메시지를 전송한다.

(6) $P_B \rightarrow S : RV_{P_A}$, $P_B : Compare(RV_{P_A}, \alpha_{P_B})$

P_B는 다운로드 요청을 승인하기 전 P_A의 신뢰도를 알기 위해 서버로 P_A의 평판 정보를 요청한다. P_B는 서버로부터 받은 P_A의 평판과 다운로드를 요청한 파일의 가중치(α_{P_B})를 비교하여 P_A의 평판이 파일의 가중치보다 크거나 같은 경우 다운로드 요청을 승인하고, 작은 경우 다운로드 요청을 거부한다.

$$RV_{P_A} \geq (\alpha_{P_B} \times n_{P_B}) : \text{다운로드 요청 승인} \quad (3)$$

$$RV_{P_A} < (\alpha_{P_B} \times n_{P_B}) : \text{다운로드 요청 거부} \quad (4)$$

3.2.3 평가 단계

(1) P_A가 P_B로부터 파일을 다운로드 받은 후 P_B에 대한 평판을 전송하지 않는 경우가 발생하는 것을 막기 위하여 P_B는 서버에게 P_A로 다운로드가 종료되었음을 알리는 메시지를 전송한다.

(2) $P_A \rightarrow S : Send(r_{P_A} : 1 \text{ or } -1)$

P_A는 P_B 로부터 파일을 다운로드 받은 후 실행하여 확인한 다음 P_B에 대한 평판을 서버로 전송한다. 다운로드 받은 파일이 올바르게 동작하고 요청한 파일과 일치할 경우 1, 그렇지 않을 경우 -1을 전송한다. 서버는 P_B로부터 다운로드 종료 메시지를 받은 후 일정 시간이 지나도 P_B에 대한 평판 값이 전송되지 않을 경우, P_A의 평판 값을 1만큼 감소시킨다. 평판 값은 특정 한 피어만 사용하는 값이 아니라 트랜잭션에 참여하는 모든 피어들이 신뢰할 수 있는 파일 제공 피어를 선택하기 위해 참조하는 값이므로, 트랜잭션이 종료되면 항상 서버로 전송하여 서비스를 이용 중인 피어들이 다음 트랜잭션에 참조할 수 있도록 한다.

(3) $S : Update(RV_{P_B}, RV_{P_A}, \alpha_{P_A}, \alpha_{P_B})$

서버는 P_B의 이전 평판 값, 트랜잭션의 결과로 P_A로부터 받은 평판 값과 파일 가중치를 이용하여 P_B의 평판을 업데이트한다. 공유 파일을 다운로드 받은 P_A의 평판 역시 이전 평판 값과 트랜잭션 대상 파일의 가중치를 사용하여 업데이트한다. 트랜잭션 종료 후 피어들의 평판 값은 다음 식에 의해 업데이트 되고 피어들의 평판 값에 따라 공유 파일의 가중치는 식 (1)에 의해 업데이트 된다.

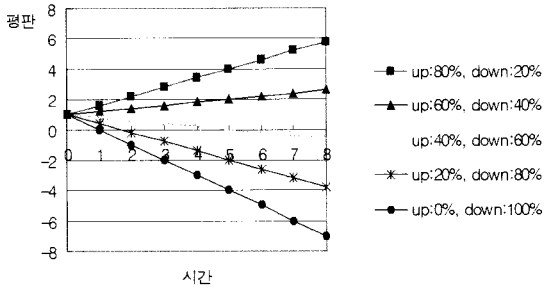
$$RV_{P_B} = RV_{P_B}' + \sum_{i=1}^{m} r_{P_A} \times \alpha_{P_B} \quad (5)$$

$$RV_{P_A} = RV_{P_A}' - \alpha_{P_B} \quad (6)$$

평판 계산에 트랜잭션 대상 파일의 가중치를 사용하여 평판 값을 증가시키거나 감소시키는 이유는 파일 제공 피어와 파일 요청 피어 간에 공정한 파일 교환이 이루어지도록 하기 위함이다. 즉, 계속적으로 다운로드만 행하는 피어의 평판

값을 트랜잭션 대상 파일의 가중치만큼 감소시켜 "free riding"을 행하는 피어들의 접근을 제어하고, 파일 제공 피어는 파일의 가중치만큼 평판 값을 증가시켜 다른 피어들의 공유 파일을 자유롭게 이용할 수 있도록 한다.

그러나 특정 피어가 파일을 계속적으로 제공은 하지만 공유 파일을 이용한 피어들로부터 나쁜 평판을 받을 경우 평판 값은 감소하게 된다. 그러므로 피어들은 많은 수의 파일을 공유하는 것도 좋지만 공유 파일에 대한 신뢰성 또한 보장할 수 있어야 한다.



(그림 2) 업로드/다운로드 비율에 따른 평판의 변화

4. 제안 방안의 분석

본 논문의 제안 방법은 피어들의 신뢰도를 나타내는 평판 값을 이용한 접근 제어를 통해 P2P 파일 공유에서 빈번하게 발생하는 "free riding" 문제를 해결하고, 바이러스나 웜을 포함한 파일을 공유하거나 실제 내용과 다른 제목의 파일을 제공한 피어들에 대하여 다른 피어들의 공유 파일에 대한 사용을 제한하는데 목적이 있다.

(1) 시뮬레이션을 통하여 "free riding"을 수행하는 피어들의 평판 값의 변화를 살펴보았다. 주어진 시간 동안 한번의 업로드와 다운로드가 실행되는 것으로 가정한다. 시뮬레이션에 참여하는 전체 피어수는 100 피어이고, 피어별 공유 파일 수는 10개이고, 공유 파일에 대한 가중치는 0.1이고, 피어들의 초기 평판은 1로 동일하다. 전체 피어 중 업로드/다운로드를 수행하는 피어 비율은 (80:20), (60:40), (40:60), (20:80), (0:80)으로 지정한다.

(그림 2)는 주어진 시간 동안 업로드와 다운로드 트랜잭션이 일어날 때 피어 평판 값의 변화를 나타내고 있다. 트랜잭션에 참여하는 모든 피어가 동일한 평판을 가지고 시작할 때 다운로드를 행하는 피어의 수가 많아질수록 평판 값이 감소하는 것을 알 수 있다. 이를 통해 초기에는 다른 피어들의 공유 파일에 대한 다운로드 권한을 얻을 수 있지만, 트랜잭션 횟수가 많아질수록 평판 값이 낮아지므로 공유 파일에 대한 사용이 제한된다. 그러므로 피어들은 다른 피어들의 공유 파일에 대한 다운로드 권한을 얻기 위해서는 자신의 파일 또한 공유해야 한다.

(2) 제안 방안에 따르면, 자신의 파일을 전혀 공유하지 않는 피어의 초기 평판 값은 식 (2)에 의해 0으로 설정된다. 다른 피어의 공유 파일에 대한 다운로드 권한은 피어의 평판 값에 의해 결정되므로, 초기 평판 값이 0인 피어의 경우 트랜잭션이 거의 일어나지 않기 때문에 피어의 평판 값은 변화 없이 계속 초기값으로 유지된다. 피어들이 공유 파일에 대한 다운로드 권한을 얻기 위해서는 식 (3)을 만족해야 하지만 트랜잭션이 발생하지 않아 초기 평판 값을 유지할 경우 다른 피어들의 공유 파일에 대한 사용 기회를 얻을 수 없다. 그러므로, 자신의 파일에 대한 공유 없이 "free riding"을 행하는 피어에 대한 접근 제어가 가능하다.

(3) 제안 방안은 [10]과 달리 최소한의 기능을 수행하는 서버를 포함시켜 피어들에 대한 평판 값을 관리하게 함으로써, 피어들 간의 직접적인 통신 이전에 항상 서버를 거쳐야 하는 번거로움은 있지만, 피어들 스스로 자신의 평판 값에 대한 조작이 불가능하고, 트랜잭션을 수행하는 피어들은 서버가 제공하는 평판 값을 신뢰하고 사용할 수 있다. 또, 트랜잭션 후 파일 제공 피어에 대한 평판 값을 전송하지 않을 경우 서버 측에서 파일 요청 피어의 평판 값을 감소시키므로 트랜잭션이 종료되면 다른 피어들이 참조할 수 있도록 트랜잭션 대상 피어에 대한 평판을 서버로 전송해야 한다. 피어의 평판 값에 대한 동적인 반영이 가능하므로, 파일 요청 피어는 최신의 평판 정보를 이용하여 트랜잭션 대상 피어를 선택할 수 있고, 파일 제공 피어 역시 최신의 정보를 이용하여 다운로드 권한을 부여한다.

(4) 기존의 평판 기반 파일 공유 시스템과 제안 방안을 비교하면 <표 2>와 같다.

기존의 평판 기반 파일 공유 시스템은 대부분 중앙 서버 없이 서비스를 이용하는 모든 피어들이 상황에 따라 클라이언트 또는 서버로 동작하는 순수 P2P 방식을 기반으로 파일이나 피어에 대한 신뢰성 보장을 위해 평판 정보를 사용하고 있다. 순수 P2P 방식에서는 필요한 자원에 대한 검색 질의나 평판에 대한 요청이 여러 피어들로부터 발생하므로 네트워크 트래픽의 증가로 네트워크의 전체적인 효율성이 저하될 뿐만 아니라 질의를 수행하는 시간 또한 오래 걸린다.

반면, 본 논문의 제안 방안은 혼합형 P2P 방식을 기반으로 최소한의 기능을 수행하는 서버를 포함함으로써 피어들 간의 통신량을 줄일 수 있으며, 피어들의 평판 정보를 이용하여 "free riding"을 수행하는 피어와 올바르지 않은 파일을 공유하는 피어들에 대한 접근 제어가 가능하고, 피어들의 공유 파일에 대한 신뢰성을 보장할 수 있다. 뿐만 아니라, 현재 사용되고 있는 프루나, 당나귀 등의 혼합형 P2P 방식에 적용 가능하다.

〈표 2〉 기존 방법과 제안 방안의 비교

	free riding	Access Control	통신량	방식
P2PRep[7]	×	×	많음	순수 P2P
Xrep[6]	×	×	많음	순수 P2P
EigenRep[9]	×	×	많음	순수 P2P
TAC]10]	×	○	많음	순수 P2P
제안 방안	○	○	보통	혼합형 P2P

5. 결론 및 향후 연구

본 논문에서는 P2P 응용 분야로 활발하게 사용되고 있는 파일 공유에서 발생하는 "free riding" 문제를 해결하고, 피어들 간의 공유 파일에 대한 신뢰성을 높이기 위해 피어들의 평판 정보를 이용하여 공유 파일에 대한 다운로드를 제한하는 것을 목적으로 한다.

제안 방안에서 피어들이 자신의 파일을 전혀 공유하지 않을 초기 평판 값이 0으로 설정되므로 "free riding"을 행하는 피어들의 경우 다른 피어들의 공유 파일에 대한 다운로드 권한을 얻기가 어렵다. 또, 정상적으로 동작하지 않는 파일을 공유한 피어들의 경우 파일 요청 피어들로부터 나쁜 평판을 받게 되므로 다른 피어들의 공유 파일에 대한 다운로드 권한이 제한되므로, 피어들 간의 공유 파일에 대한 신뢰성을 높일 수 있다.

대부분 P2P 파일 공유 시스템에서 많은 피어들이 "free riding"을 행하고 있으므로, 실제 구현에 있어 "free riding" 피어들이 시스템에 미치는 영향에 대한 추가적인 분석과 그에 따른 해결책에 대한 연구가 계속적으로 필요하다. 피어들의 신뢰도를 나타내는 평판 정보에 대한 체계적인 관리 방법과 평판 계산을 위한 방법 등에 관한 연구도 필요할 것으로 판단된다. 본 논문에서는 모든 공유 파일에 대한 가중치를 동일하게 설정했지만 향후 파일의 인기도 등을 고려하여 공유 파일마다 가중치를 다르게 지정하여 "free riding"을 방지하고 접근 제어를 수행할 수 있는 방법에 관해 연구할 것이다.

참 고 문 헌

[1] Dejan S.Milojicic, Vana Kalogeraki, Rajan Lukose, Kiran Nagaraja, Jim Pruyne, Bruno RIchard, Sami Roolins, Zhichen Xu, "Peer-to-Peer Computing," HP TechReport HPL-2002-57, 2002. http://www.hpl.ph.com/techreports/2002/HPS-2002-57.pdf

[2] "세상을 바꾸는 힘의 중심 P2P", 프로그램 세계, 2002, 7월호

[3] 팀 오라일리 외 24인 저, 전현성 외 4인 역, "차세대 인터넷 P2P", O'RELLY, 2001.

[4] E.Adar and B.Huberman, "Free riding on gnutella," September 2000. Available at http://www.firstmonday.dk/issues/issue5_10/adar/index.html

[5] YangBin Tang, HuaiMin Wang, Wen Dou, "Trust Based Incentive in P2P Network," Proceeding of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business, 2004.

[6] Ernesto Damiani, De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, Fabio Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Conference on Computer and Communications Security archive Proceedings of the 9th ACM conference on Computer and communications security, pp.207-216, 2002.

[7] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani di Vimercati, "Choosing Reputable Servents in a P2P Network," WWW2002, pp.376-386, 2002.

[8] Gnutella, http://www.gnutella.com

[9] Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia- Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," In Proceedings International WWW Conference, 2002.

[10] Huu Tran, Michael Hitchens, Vijay Varadharajan, Paul Watters, "A Trust based Access Control Framework for P2P File-Sharing Systems," HICSS 2005, pp.302c-311c, 2005.

[11] J.McLean, "The Specification and Modeling of Computer Security," IEEE Computer, Jan., 1990.

[12] Nazareno Andrade, Miranda Mowbray, Walfredo Cirne, Franciso Brasileiro, "When Can an Autonomous Reputation Scheme Discourage Free-riding in a Peer-to-Peer System?," 2004 IEEE International Symposium on Cluster Computing and the Grid, pp.440-448, 2004.

[13] Krishna Kant, Ravi Iyer, Vijay Tewari, "A Framework for Classifying Peer-to-Peer Technologies," pp.368-375, CCGRID 2002.

[14] 조남수, 김우환, 윤효진, 이인석, 천정희, 김태성, 진승헌, 추경균, "P2P 환경의 자기 평판 관리 시스템", 정보보호학회논문지, 제14권 제2호, pp.35-45, 2004. 4.

[15] Natalia Stakhanova, Sergio Ferrero, Johnny Wong, Ying Cai, "A reputation-based trust management in peer-to-peer network systems," In Proceedings of 17th International Conference on Parallel and Distributed Computing Systems, PDCS-2004.

신 정 화

e-mail : shinjh@mail1.pknu.ac.kr

1997년 한국방송통신대학교 컴퓨터과학과(이학사)

2000년 부경대학교 전산정보학과(이학석사)

2001년~현재 부경대학교 전자계산학과 박사과정

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

신 원

e-mail : shinweon@tit.ac.kr

1996년 부경대학교 전자계산학과(이학사)

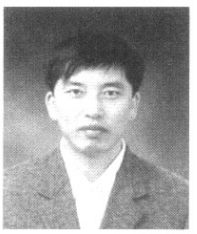
1998년 부경대학교 전자계산학과(이학석사)

2001년 부경대학교 전자계산학과(이학박사)

2002년~2005년 (주)안철수연구소 선임연구원

2005년~현재 동명정보대학교 정보보호학과 전임강사

관심분야 : 소프트웨어 보안, 악성코드, 이동에이전트 보안, 암호학 응용



이 경 현

e-mail : khrhee@pknu.ac.kr

1982년 경북대학교 수학교육과(학사)

1985년 한국과학기술원 응용수학과(석사)

1992년 한국과학기술원 수학과(박사)

1982년~1993년 3월 한국전자통신연구소 선임연구원

1993년 3월~현재 부경대학교 전자컴퓨터 정보통신공학부 교수

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

관심분야 : 암호이론, 멀티미디어 정보보호, 네트워크 보안, 암호 프로토콜