P2P 방식을 이용한 새로운 e-Commerce 모델

위성균°, 이경현
부경대학교 전자컴퓨터정보통신공학부
wskyun@dreamwiz.com°, khrhee@pknu.ac.kr

The New e-Commerce Model using P2P System

Sung-Kyun Wee° Kyung-Hyune Rhee
Department of Computer and Information Science, Pukyong National University°
Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University

요 약

P2P 서비스는 서버를 거치지 않고 네트워크에 연결된 컴퓨터간의 직접적인 교환에 의해 자원과 서비스를 공유할 수 있는 방식으로 기존의 클라이언트/서버 방식과 달리 관련 프로그램만으로 자원에 대한 공유 및 교환이 가능하다. 이러한 P2P의 특징을 이용하여 서버가 중재자 역할을 하는 전자상거래 방식에 P2P 기술을 적용하여 구매자와 판매자의 직접적인 통신에 의해 상거래가 가능한 새로운 모델을 제안하고자 한다. 제안 모델은 구매자와 판매자간의 디지털 컨텐츠 교환과 지불에 대해 공정성을 보장해 주고, 컨텐츠를 사용한 구매자들로부터 받은 평판(reputation)값을 통하여 판매자가 제공하는 컨텐츠에 대한 신뢰성 또한 보장할 수 있다.

1. 서 론

인터넷의 급속한 발전과 확산으로 인터넷 이용자 수가 증가하고, 인터넷 이용을 위한 기반 환경의 확충 및 개인용 컴퓨터의 이용 증가로 인터넷을 통한 각종 서비스 이용 및 활용 범위가 점차적으로 증가하고 있다. 그 중 인터넷을 통한 상거래 활동이 점차적으로 증가하면서 기존의 오프라인 상의 상거래가 단순히 온라인 적용을 넘어 급속한 속도로 변형 또는 이식되거나 여러 형태의 상거래 모델들이 결합하여 새로운 모델이 탄생하는 등 다양한 형태로 발전하고 있다[1].

현재 전자상거래는 클라이언트/서버 방식으로 동작하므로 사용자들은 특정 서버에 의존하여 상거래 활동을 수행하며, 정보의 공유 영역 또한 제한적이며, 해당 서버에 문제가 생길 경우 더 이상 상거래를 유지하기 어려운 단점이 있다. 이와 같이 클라이언트/서버 방식이 가지고 있는 문제점을 해결하기 위해 등장한 P2P 기술은 서비스에 참여하는 각각의 컴퓨터들이 서버인 동시에 클라이언트로 동작하면서 중앙 서버 없이 직접 연결을 통해 서로의 자원에 대한 공유 및 교환을 할 수 있다[2]. 이러한, P2P 기술을 전자상거래에 적용 시 상거래 서비스 이용자들은 중앙 서버 없이 직접 통신하면서 언제, 어디서나, 제약 없이 개인별 상거래나 경매가 가능하여 P2P 거래가 급증하고 있지만 정작 별다른 거래 안전장치가 없어 피해가 우려된다. 이에 본 논문에서는 P2P 방식을 이용한 새로운 e-Commerce 모델을 제안하고자 한다. 제안 모델에서 상거래 대상은 디지털 컨텐츠이고, 컨텐츠 교환 및 지불시 거래 당사자들간의 공정성(fairness)을 보장해 주고, 구매한 컨텐츠를 이용한 피어 들로부터 받은 해당 컨텐츠에 대한 평판값을 기반으로 컨텐츠 구매에 대한 신뢰성을 향상시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구로 전자상거래와 P2P의 개요에 대해 살펴보고, 3장에서 P2P 방식을 이용한 전자상거래에 대해 설명하고, 구현에 있어 필요한 고려사항을 살펴본다. 4장에서는 본 논문에서 제안하는 새로운 P2P e-Commerce 모델의 동작 방식을 설명하고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 전자상거래 개요

전자상거래는 인터넷이 보편화되기 이전에도 기업간 문서를 전자적 방식으로 교환하거나, PC통신의 홈쇼핑·홈뱅킹 등 다양한 형태로 존재해 왔으나, 인터넷이 대중화되면서 전자상거래는 인터넷상에서의 거래와 관련지어 생각하게 되었다.

현재 전자상거래는 컴퓨터통신망을 통해 이루어지는 상품 및 서비스의 판매, 발주, 광고 등을 포함한 모든 경제 활동을 의미하는 것으로 인터넷상에서 기업과 소비자가 상품 및 서비스를 거래하는 것도 전자상거래에 포함된다. 전자상거래의 목적은 상거래의 신속화와 효율화를 실현하고자 하는 것으로 인터넷상에서 거래처의 선택을 비롯한 상품 구매, 가격 교섭, 계약 체결, 대금 결제 등 상거래에 관련된 모든 업무를 전자적으로 처리할 수 있는 환경을 만드는 것이다[1].

2.2 P2P(Peer-to-Peer) 개요

P2P 기술은 고성능 중앙서버나 광대역 네트워크 없이도 정보를 찾는 사람과 정보를 가진 사람의 컴퓨터 간에 직접적인 연결을 통해 다양한 정보를 공유할 수 있도록 하는 기술과 기술을 응용하여 제공되는 서비스들의 집합을 의미한다. P2P 기술은 저비용/고효율로 정보 확산에 편리하고, 파일 공유 뿐만 아니라 CPU나 디스크와 같은

컴퓨팅 자원의 공유, 온라인 협업, 전자거래 등으로 응용 분야가 확대되고 있다[3].

P2P 기술을 이용한 서비스 형태는 비슷한 성능을 가진 컴퓨터끼리 연결되어 동작하는 순수 P2P 방식과 컴퓨터간 상호 작용을 원활히 해주기 위한 서버가 개입되어 있는 혼합형 P2P 방식이 있다[3]. P2P 서비스 이용에 있어 장점은 특정 서버에 문제가 발생하더라도 모든 사용자에게 서비스가 중단되는 경우는 발생하지 않으며, 또한 네트워크에 연결되어 있는 여러 사용자들이 가진 정보에 대하여 손쉬운 공유가 가능하다. 한편, 피어 프로그램의 유지 보수 부담이 있고, 시스템 운영의 안정성과 신뢰도 문제, 그리고 개방되고 분산되어 있는 만큼 P2P 작업을 수행하는 사용자들의 책임성이 요구된다. 또한, P2P서비스를 이용하는 참여자가 항상 온라인 상태로 유지되어야 하고, 악의적인 소프트웨어의 손쉬운 분배로 인하여 보안 문제를 야기 시키는 단점이 있다[4].

3. P2P 방식을 이용한 전자상거래

P2P 방식의 전자상거래는 기존의 인터넷 환경에서 일어나는 상거래와 달리 구매자가 구매 의사가 있는 제품을 밝히면 서비스에 가입된 모든 제공자들에게 주문 내용이 실시간으로 전달이 되고, 해당 제품의 제공자는 견적을 구매자에게 보내며, 구매자는 여러 제공자들로부터 받은 견적 가운데 가장 유리한 업체를 선택하여 직접 연락을 취하는 형태로 이루어진다. 이 경우 구매자는 제품 구매를 위해 들이는 웹 서핑 시간이나 검색 시간을 줄일 수 있고, 중간 브로커를 거치지 않고 제공자와 직접적인 연결을 통하여 거래가 가능하기 때문에 수수료가 들지 않으며, 특정 지역이나 특정 업종을 지정할 수 있는 장점을 가진다[5]. P2P 방식을 이용한 전자상거래는 실제 구현에 있어 다음과 같은 요구 사항을 필요로 한다.

- 공정성 : 구매자와 판매자간에 서로가 원하는 정보를 모두 다 가질 수 있거나 둘 다 가지지 못함을 보장할 수 있어야 한다.
- 인증 : 구매자와 판매자는 상호간에 정보를 전달할 때 자신이 원하는 상대인지를 확인할 수 있어야 한다.
- 기밀성 : 구매자와 판매자간에 주고 받는 정보는 허가되지 않은 제3자로부터 보호되어야 한다.
- 무결성 : 구매자와 판매자간에 주고 받는 정보는 불법적인 사용자에 의해 변조되어서는 안된다.
- 부인방지 : 구매자와 판매자는 서로간에 보낸 메시지에 대해 부인할 수 없어야 한다.

4. P2P 방식을 이용한 새로운 e-Commerce 모델

본 논문에서 제안하는 e-Commerce 모델은 P2P 서비스 방식 중 중앙 서버가 존재하는 하이브리드 방식을 기반으로 한다. 서비스에 참여하는 모든 피어들은 인증된 피어이고, 서비스에 참여하는 개체들간에 주고 받는 모든 메시지는 안전하고 기밀성이 보장되는 채널을 통해 전송되는 것으로 가정한다. 중앙 서버는 서비스에 참여하는 피어들이 등록한 판매하고자 하는 컨텐츠에 대한 목록과 컨텐츠에 대한 신뢰도를 나타내는 평판값(trust)을 저장하고 있다. 컨텐츠 구매를 원하는 피어들은 중앙 서버가 제공하는 평판값을 참조하여 구매를 원하는 대상 피어를 결정할 수 있다. 또한, 본 논문에서는 컨텐츠 교환과 지불에 있어 판매 피어와 구매 피어 상호간에 공정성을 보장해 주기 위해 보증 서버(ES : Escrow Server)를 사용하고, 이 서버는 신뢰된 서버로 가정한다. 판매 피어는 구매 피어로부터 컨텐츠 요청이 있을 경우 먼저 보증 서버에게 해당 컨텐츠를 전송한 후 구매 피어에게 전송하고, 구매 피어는 컨텐츠의 정당성 확인을 위해 판매 피어에게 받은 컨텐츠와 구매에 대한 지불 정보를 보증 서버로 전송한다. 보증 서버는 판매 피어로부터 받은 컨텐츠와 구매 피어로부터 받은 컨텐츠를 비교하여 일치할 경우 구매 피어에게 올바른 컨텐츠임을 알리고, 판매 피어에게 구매 피어로부터 받은 지불 정보를 전송한다. 본 논문에서 사용되는 표기법과 동작 방식은 다음과 같다.

4.1 표기법

- CS(Central Server) : 서비스에 참여하는 피어의 ID와 피어들이 등록한 컨텐츠 목록, 피어들의 신뢰값을 저장하는 서버
- $desc_{P_i}$: 피어들이 등록한 컨텐츠 정보
- P_i : 컨텐츠 판매 피어 또는 구매 피어 식별자
- ES(Escrow Server) : 컨텐츠 교환 및 지불에 있어 공정성 보장을 위해 사용되는 서버
- C : 교환 대상 컨텐츠 (이미지, 오디오 등)
- K : 컨텐츠 암호화를 위해 랜덤하게 생성된 대칭키
- $E_K(C)$: 컨텐츠 C에 대해 대칭키를 사용한 암호화
- $H(E_K(C))$: 암호화된 컨텐츠에 대해 암호학적 해쉬 함수 처리를 수행
- pay_{P_i} : 구매 피어가 제공하는 지불 정보

4.2 동작 방식

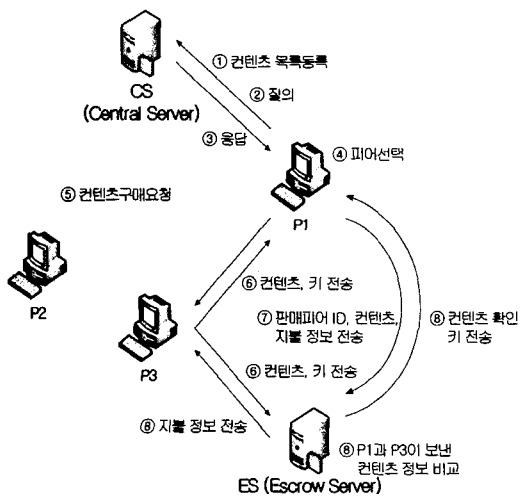

그림 1 . 제안 모델의 동작방식

① P1 → CS : Register ($ID, desc_{P_1}$)

서비스에 참여하는 피어들은 자신이 가진 컨텐츠 중 판매하고

자 하는 컨텐츠 목록을 CS에 등록한다. CS가 관리하는 피어들에 대한 정보는 다음과 같다.

$<P_1, desc_{P_1}, trust>$

- P_1 : 컨텐츠 목록을 등록한 피어의 ID
- $desc_{P_1}$: P1이 등록한 컨텐츠 정보
- trust : P1의 평판을 나타내는 값으로 서비스 이용을 위해 처음 로그인한 피어들의 trust 값은 0으로 초기화되고, 컨텐츠를 구매한 피어들이 컨텐츠 확인 후 서버에게 trust 값을 전송한다. trust 값은 컨텐츠 구매를 원하는 피어들이 해당 컨텐츠에 대한 신뢰도를 참조하도록 하기 위해 사용된다.

② P1 → CS : $Query(desc)$
P1은 컨텐츠 구매를 위해 필요로 하는 컨텐츠에 대한 질의를 CS에 전송한다.

③ CS → P1 : Response(P_i, trust)
CS는 P1이 요청한 컨텐츠를 가지고 있는 피어 ID와 해당 피어가 제공하는 컨텐츠에 대한 신뢰값을 함께 전송한다.

④ P1 : Select
P1은 CS로부터 받은 목록 중 컨텐츠에 대한 신뢰값을 나타내는 "trust" 값을 참조하여 하나의 피어(P3)를 선택한다.

⑤ P1 → P3 : Request(Content)
선택한 피어(P3)에게 컨텐츠 구매 의사를 알린다.

⑥ P3 → ES : Send(P3, P1, $H(E_K(C)), K$)
P3 → P1 : Send($E_K(C)$)
P3은 P1의 요청에 따라 컨텐츠를 판매하기 전 컨텐츠 교환과 지불에 대한 공정성을 보장 받기 위해 먼저 판매할 컨텐츠를 암호화하여 해쉬한 값과, 컨텐츠 복호화에 필요한 키를 ES에게 전송한 다음 암호화된 컨텐츠를 P1에게 전송한다.

⑦ P1 → ES :
Send(P1, P3, $H'(E_K(C)), pay\_info_{P1}$)
P1은 컨텐츠에 대한 정당성 확인과 지불을 위해 P3으로부터 받은 암호화된 컨텐츠에 해쉬한 값, 컨텐츠 판매 피어의 ID, 지불 정보를 ES에게 전송한다.

⑧ ES : Compare ($H(E_k(C))$, $H'(E_k(C))$)
ES는 P3으로부터 받은 $H(E_k(C))$값과 P1으로부터 받은 $H'(E_k(C))$값을 비교하여 해쉬값이 동일할 경우 P3으로부터 올바른 컨텐츠 전달이 이루어진 것으로 보고 컨텐츠를 복호화할 수 있는 키를 P1에게 전송하고, P1이 보낸 지불 정보를 확인하여 유효하면 P3에게 컨텐츠에 대한 지불 정보 pay_{P1}를 전송한다. 만약 P3과 P1으로부터 받은 해쉬값이 동일하지 않을 경우 AS는 컨텐츠 교환이 제대로 수행되지 않은 것으로 판단하여 P1에게 통보하고 작업은 종료된다. 지불의 경우에도 동일하다. 이와 같이 AS는 판매 피어와 구매 피어간의 컨텐츠 교환 및 지불에 있어 어느 한 피어가 컨텐츠를 받고 지불을 하지 않거나 반대의 경우가 발생하는 것에 대해 중재자 역할을 수행하며 피어간의 공정성을 보장해 준다.

⑨ P1 → ES : Send(P_3, trust)
P1은 구매한 컨텐츠를 사용한 후 컨텐츠의 정확성 여부에 따라 ES에게 해당 컨텐츠에 대한 신뢰도에 해당하는 "trust" 값을 전송한다.

⑩ ES : Update(trust)
ES는 컨텐츠를 구매한 피어 들로부터 받은 "trust" 값을 이용하여 각 피어들이 제공한 컨텐츠에 대한 신뢰도 값을 갱신하고 새로운 컨텐츠 교환이 발생할 경우 항상 최신의 신뢰도 값을 참조할 수 있도록 제공해 준다.

제안 모델은 P2P 전자상거래에 필요한 요구 사항 중 AS를 통하여 피어간의 컨텐츠 교환 및 지불에 있어 공정성을 보장하고, 피어간에 교환하는 컨텐츠에 대해 암호화와 해쉬를 통해 교 기밀성 및 무결성을 보장할 수 있다.

5. 결론

본 논문에서는 서버가 개입되어 동작하는 기존의 전자상거래 방식에 서버 없이 서비스 이용자들간의 직접적인 통신에 의해 구매 및 판매가 가능한 P2P 서비스를 적용한 새로운 e-Commerce 모델을 제안하였다. 제안 모델은 컨텐츠 교환과 지불에 있어 공정성을 보장해 줄 수 있고 또한, 피어들이 제공한 컨텐츠에 대한 평판값을 참조하여 신뢰성 보장과 안전하고 정확한 컨텐츠 구매가 가능한 이점을 가진다. P2P 기술의 계속적인 발전으로 파일 공유 분야로 제한되었던 P2P 기술의 응용 분야가 점점 다양해지면서 응용 분야에 따라 필요한 보안 요구 사항에 대한 연구와 P2P 기술의 표준화와 관련된 추가적인 연구가 필요할 것으로 판단된다.

[참고문헌]

[1] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영 공저, "전자상거래 보안 기술", 1999
[2] DIOGO R.FERREIRA, J.J.PINTO FERREIRA, "Building an e-marketplace on a peer-to-peer infrastructure", INT.J.COMPUTER INTEGRATED MANUFACTUREING, APRIL-MAY 2004, VOL.17, NO.3, 254-264
[3] Krishna Kant, Ravi Iyer, "A Framework for Classifying Peer-to-Peer Technologies", CCGRID'02, 2002
[4] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani di, "Choosing Reputable Servents in a P2P Network", WWW2002, 2002
[5] 정유진, "P2P의 현황 및 전망", 지급결제와 정보기술, 2001
[6] Bill Horne, Benny Pinkas, Tomas Sander, "Escrow Services and Incentives in Peer-to-Peer Networks", EC'01, 2001
[7] SAI HO KWOK, KARL R. LANG AND KAR YAN TAM, "Peer-to-Peer Technology Business and Service Models:Risks and Opportunities", Electronic Markets,