P2P 환경에서 신뢰성 있는 e-Commerce 모델

신정화* · 이경현*

Reliable e-Commerce Model on P2P Environment

Jung-Hwa Shin* · Kyung-Hyune Rhee*

본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

요 약

P2P(Peer-to-Peer)는 중앙서버 없이 개인간에 직접적인 연결을 통하여 디지털 자원(mp3, software, game, video 등)을 효과적으로 공유하는 방식으로 기존의 클라이언트/서버 방식과 달리 관련 프로그램만으로 디지털 자원에 대한 손쉬운 공유 및 교환이 가능하다. 본 논문에서는 이러한 P2P 기술을 서버가 중재자 역할을 하는 기존의 전자상거래 방식에 적용하여 구매자와 판매자가 직접적인 통신을 통하여 상거래를 수행할 수 있도록 한다. 또한, 특정 제품 구매시 해당 제품을 사용한 구매자들로부터 얻은 제품에 대한 신뢰값인 평판(reputation)을 참조하여 구매 제품에 대한 신뢰성을 향상시키고, 제품 교환과 지불이 정상적으로 수행될 수 있도록 보증 역할을 담당하는 ES(Escrow Server)를 사용하여 공정성(fairness)을 보장하는 P2P 방식의 새로운 e-Commerce 모델을 제안하고자 한다.

ABSTRACT

A P2P is a method that can share and exchange on digital resources through a direct connection on personnel without a central server. In this paper, we apply a P2P technology to a traditional electronic commerce method so that a seller and a customer can perform a commercial transaction through a direct communication. As such a result, we propose a new e-Commerce model on P2P environment to assure fairness in commercial transactions. To achieve our goal, we put an escrow server which is responsible for guarantee fair contents delivery and payment for the contents between a seller and a customer. When a customer buys content, he first obtains reputation values implicating reliability for the content and refers to these values to determine purchase. The proposed scheme, we can improve the reliability for the purchasing content and provide the fairness to both a seller and a customer simultaneously.

키워드

P2P(Peer-to-Peer), 공정성(Fairness), 평판(Reputation), 전자상거래(e-Commerce)

I. 서 론

인터넷 이용 환경과 기술의 발전으로 인터넷 이용자 수가 상당히 증가하고, 인터넷 사용을 위한 기반 시설의 구축과 개인용 컴퓨터 보급의 증가는 인터넷을 통한 각종 서비스의 이용과 활용 범위를

*부경대학교

접수일자 : 2004. 8. 3

확장시켰다. 이 중 전자상거래는 시, 공간적 제약을 받는 기존 상거래의 제한적인 영역을 대체하는 수단이 되고 있으며 특히, 인터넷을 통한 상거래 활동은 기존의 오프라인 상의 상거래가 단순히 온라인 작용을 넘어 빠르게 변화되고 있거나 여러 형태의 상거래 모델들이 결합하여 새로운 모델이 탄생하는 등 다양한 형태로 발전하고 있다. 전자상거래 비즈니스 모델들은 내용, 기능, 목적, 제공가치에 따라, 수익 형태에 따라, 기업 형태 유형에 따라, 거래 대상 유형이나, 거래 물품 유형 등에 따라 다양하게 분류할 수 있다[1][2].

기존의 전자상거래 방식은 클라이언트/서버 방식으로 사용자들은 특정 서버에 의존하여 상품 검색 및 구매 등의 상거래 활동을 수행하며, 정보의 공유 또한 제한적이다. 또한, 서버에 의존하여 상거래 작업을 수행하므로 거래에 관여하는 서버에 문제 발생시 더 이상 상거래를 유지하기 어려운 단점을 가진다. 클라이언트/서버 방식이 가진 이러한 문제점을 보완하기 위해 등장한 P2P(Peer-to-Peer) 방식은 서비스를 이용하는 각각의 컴퓨터들이 상황에 따라 서버 또는 클라이언트로 동작하면서 별도의 관리 서버 없이 직접적인 연결을 통해 서로의 자원에 대한 손쉬운 공유 및 교환이 가능하다[3].

이와 같은 P2P 기술을 전자상거래에 적용시 상거래 서비스 이용자들은 중앙 서버 없이 직접적인 통신을 통해 언제, 어디서나, 제약 없이 개인별 상거래나 경매 등의 작업이 가능하다.

이에 본 논문에서는 기존 전자상거래 방식에 P2P 기술을 적용하여 관리자 없이 구매자와 판매자가 직접 상거래를 수행할 수 있고, 제품 구매시 이미 해당 제품을 구매한 구매자들로부터 얻은 판매자와 판매 제품에 대한 신뢰도를 나타내는 평판값을 참조하여 제품 구매를 결정할 수 있도록 함으로써 제품 구매에 있어 신뢰성을 향상시키고, 제품 교환과 지불시 문제가 발생할 경우 해결을 위해 별도의 보증 서버(ES : Escrow Server)를 사용하여 공정성을 보장하는 P2P 방식의 새로운 e-Commerce 모델을 제안하고자 한다. 제안 모델에서 상거래 대상은 디지털 컨텐츠이고, 컨텐츠 교환 및 지불에 있어 공정성 보장을 위해 구매자와 판매자 사이의 거래에 보증을 담당하는 보증 서버를 사용한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구로 전자상거래와 P2P 개요, 공정한 교환 프로토콜에 대해 살펴보고, 3장에서 P2P 방식을 이용한 전자상거래 방식에 대해서 설명하고, 필요한 요구사항을 살펴본다. 4장에서는 본 논문에서 제안하는 컨텐츠 판매와 지불에 있어 공정성과 판매 피어와 판매 컨텐츠에 대해 신뢰성이 보장되는 P2P 방식의 새로운 e-Commerce 모델의 동작 방식 및 특징을 설명하고, 5장에서 결론을 맺는다.

II. 관련연구

2.1 전자상거래 개요

전자상거래는 기업간 또는 기업과 소비자간의 상거래 활동을 통신 네트워크를 통해 수행하는 것으로 상품 및 서비스의 판매, 발주, 광고 등을 포함한 모든 경제 활동을 의미한다[4]. 전자상거래의 특징은 네트워크를 통해 공급자와 구매자를 직접 연결하므로 물리적인 판매 거점이 불필요하며, 기업 활동에 있어 시간과 공간의 제약이 사라져 기업은 24시간 내내 어디서나 상품 판매가 가능하다. 전자상거래의 목적은 상거래의 신속화와 효율화를 실현하고자 하는 것으로 인터넷 상에서 거래처의 선택을 비롯한 상품 구매, 가격 교섭, 계약 체결, 대금 결제 등 상거래에 관련된 모든 업무를 전자적으로 처리할 수 있는 환경을 만드는 것이다[4].

전자상거래의 유형에는 기업간 거래(B2B : Business to Business), 기업과 소비자간 거래(B2C : Business to Customer), 정부와 소비자간 거래(G2C : Government to Customer), 정부와 기업간 거래(G2C : Government to Customer), 기업내부 프로세스의 혁신을 통한 기업내 거래(B2E : Business to Eternal)가 있다. 반면, 모든 상거래가 인터넷을 통해 이루어지기 때문에 직접 거래 상대를 만나거나 물건을 눈으로 확인하지 못하는데 따른 여러 가지 문제점이 발생한다. 또한, 전자상거래는 대부분 신용카드의 사용을 통해 이루어지기 때문에 기업과 개인간의 거래에 있어 개인의 프라이버시 정보, 기업 비밀 등의 보호와 대금 결제의 신뢰성 보장이 무엇보다 중요하다. 그러므로, 전자상거래 등의 응용 서비스를 안전하게 제공하기 위해서 정보보호 서비스 요구 수준을 유지하면서 사용자에게 신뢰성을 보장해 주는 정보보호 기술이 필요하다. 전자상거래를 위해 필요한 보안 요구 사항으로 거래 메시지에 대한 기밀성 및 무결성, 거래 당사자에 대한 인증, 거래 요청 및 승낙에 대한 부인방지가 있다[4][5].

2.2 P2P(Peer-to-Peer) 개요

P2P는 사용 분야에 따라 다양하게 정의되고 있지만 일반적인 개념은 중앙 서버를 거치지 않고 정보를 찾는 사용자와 정보를 가진 사용자의 컴퓨터

를 직접 연결하여 서로의 자원을 공유할 수 있도록 해주는 기술과 그 기술을 응용하여 만든 서비스의 집합이라 할 수 있다[3][6]. 또한, P2P는 동등한 능력의 개인 대 개인을 의미하므로, 이용자 각각이 소유하고 있는 다양한 유형의 자원을 공유함으로써 이를 기반으로 이용자가 서로 원하는 정보를 검색 및 교환할 수 있어야 한다.

이와 같이 P2P에서는 서비스를 제공하기 위한 특정 서버의 개념이 없으며 서비스에 참여하는 각 피어가 서버와 클라이언트의 역할을 동시에 수행할 수 있다. 서비스에 참여하는 모든 피어들이 직접 연결되어 정보를 교환하므로 중앙 집중형의 서버에서 발생할 수 있는 병목 현상이나 단일지점오류를 피할 수 있고 확장성을 제공할 수 있다[3].

현재 국내의 소리바다[7]나 eDonkey[8]와 같은 파일 공유 서비스 등을 통해 P2P의 잠재력을 보여주고 있으며, 기존의 클라이언트/서버 모델의 수직적 구조의 분산 시스템 환경을 수평적 구조의 환경으로 변화시킬 수 있는 기술로 평가받고 있다. 또한, P2P는 저비용/고효율로 정보 확산에 편리하고, 파일 공유 뿐만 아니라 CPU나 디스크와 같은 컴퓨팅 자원의 공유, 온라인 협업, 전자거래 등으로 응용 분야가 확대되고 있다[9][10]. P2P 방식을 사용하여 제공될 수 있는 응용 서비스 분야로는 멀티미디어 파일 전송, 인터넷 쇼핑 및 경매 서비스, 인터넷 컨텐츠 검색과 제공, 협동 작업을 위한 업무용 도구 등과 같이 멀티미디어 환경에서 다양한 목적으로 사용될 수 있다. P2P 서비스는 구현 구조에 따라 순수 P2P(Pure P2P) 모델과 혼합형 P2P(Hybrid P2P) 모델로 구분할 수 있다[10].

(1) 순수 P2P

순수 P2P는 <그림 1>과 같이 피어들 간의 정보교환을 위해 중앙 서버에 의존하지 않고 동작하는 완전 분산형 모델이다. 관리 역할을 담당하는 중앙 서버가 없기 때문에 네트워크에 연결된 피어들을 스스로 동적으로 찾아야 하지만 서버에 지정된 규칙에 의해 실행되는 전통적인 서버/클라이언트 모델과는 달리 사용자들 자신이 나름대로의 규칙을 자율적으로 지정할 수 있고, 그들 자신의 네트워크 환경을 설정할 수도 있게 해준다. 반면, 순수 P2P는 필요한 정보의 검색을 위해 피어들 간에 질의를 보내는 작업이 중복해서 발생하므로 네트워크 트래픽의 과부하로 인해 전체 대역폭이 증가하여 네트워크 전체의 효율성과 피어 검색의 효율성을 저하시킬 수 있다. 순수 P2P 방식으로 Gnutella와 FreeNet이 있다[10].

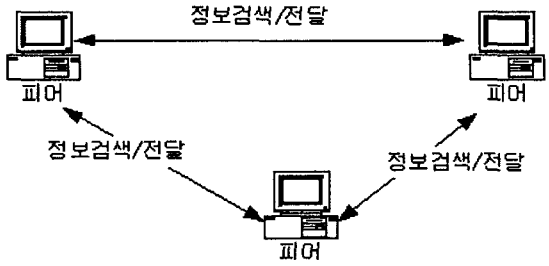

그림 1. 순수 P2P
Fig.1 Pure P2P

(2) 혼합형 P2P

현재 네트워크에 접속되어 있는 피어들의 식별정보나 공유자원/파일들의 목록과 같은 메타정보들을 관리하는 서버를 포함시킴으로써 피어들 간의 검색을 용이하게 하기 위한 모델이다. 서버가 관여하지만 검색을 위한 메타정보 이외의 자료들은 관리하지 않으며 실질적인 통신을 수립하고 필요한 정보를 교환하는 것은 피어들 자신의 몫이다. 중앙 서버는 전체 네트워크의 성능이나 연결 상태 파악, 검색에 있어 효율성을 제공하기 위한 인덱스 서버의 역할을 하거나, 트랜잭션, 과금, 인증 등을 처리하는 역할을 수행할 수 있으며, Napster와 국내의 소리바다 등이 혼합형 P2P 모델에 해당된다[10]. 혼합형 P2P의 동작 방식은 <그림 2>와 같다.

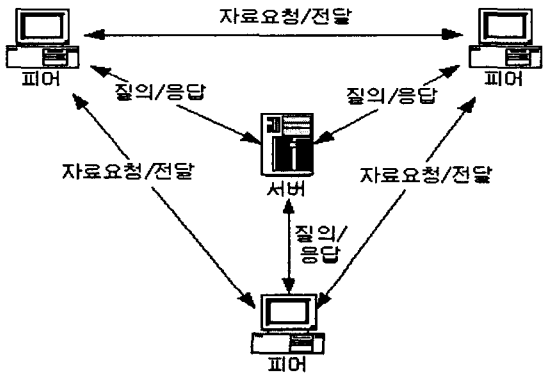

그림 2. 혼합형 P2P
Fig. 2 Hybrid P2P

2.3 공정한 교환 프로토콜

공정한 교환 프로토콜은 서비스를 이용하는 피어들 간에 원하는 컨텐츠와 컨텐츠에 대한 지불을 둘 다 얻거나 얻지 못함을 보장하는 것을 말한다. 교환에 있어 공정성을 보장하기 위해 완전한 신뢰

성을 기반으로 하는 TTP(Trusted Third Party)를 사용하고, TTP를 어떤 형태로 사용하는가에 따라 on-line 프로토콜과 optimistic 프로토콜로 구분한다[11][12][13].

(1) On-line 프로토콜

공정한 교환을 위해 항상 TTP가 개입하는 방법으로 TTP는 전송 정보의 공정성과 유효성을 보장한다. 반면, TTP가 항상 관여하게 됨으로써 사용자가 프로토콜을 사용하는 횟수에 비례하여 TTP의 계산량과 통신 비용 또한 증가한다.

(2) Optimistic 프로토콜

예외 상황, 즉 분쟁이 발생 했을 때만 TTP가 관여하여 분쟁을 해결하는 방법이다.

III. P2P 방식을 이용한 전자상거래

P2P 방식을 이용한 전자상거래는 기존의 클라이언트/서버 중심의 전자상거래와 달리 유통망을 간소화하여 온/오프라인 결합을 적극 유도하며, 최종 소비자와 공급자 사이의 유통을 최적화 시킴으로써 기존의 전자상거래가 가지고 있는 문제점을 해결하는 모델이 될 수 있다.

P2P 방식에서 상거래 행위는 클라이언트/서버 방식의 전자상거래와 달리 구매자가 구매의사가 있는 제품의 사양을 적어 서버로 보내면 서버는 등록되어 있는 판매자 목록 중 구매자의 요구 사항에 맞는 물품을 제공할 수 있는 판매자 목록을 구매자에게 알려준다. 서버로부터 받은 정보를 이용하여 구매자는 각 판매자에게 직접 견적서를 요청하고, 여러 판매자들로부터 받은 견적서 중 적합한 하나를 선택하여 거래가 이루어지게 된다. 이때, 서버는 최종 거래에 대한 정보만 확보할 뿐 판매자와 구매자간의 거래에는 개입하지 않는다[2]. 그리고, 구매자는 제품 구매를 위해 들이는 웹 서핑 시간이나 검색 시간을 줄일 수 있으며, 중간 브로커를 거치지 않고 판매자와 직접적인 연결을 통한 거래가 가능하기 때문에 수수료가 들지 않으며, 특정 지역이나 특정 업종을 지정할 수 있는 장점을 가진다. 이와 같이 P2P를 이용한 전자상거래와 기존의 전자상거래에서의 차이는 현격한 비용 절감 효과에 있으며 서비스 이용자에 의한, 이용자를 위한 상거래 방식이다.

P2P 방식의 비용 절감은 서버를 중심으로 하는 서비스와 달리 컨텐츠의 저장과 관리 부담을 개별 사용자에게 분산시키므로 저장과 컴퓨터 시스템에 대한 비용을 절감할 수 있고, 사용자 트래픽 역시 중앙 서버로 집중하지 않고 사용자 회선으로 분산되기 때문에 회선 비용 또한 절감할 수 있다[2]. 현재 P2P 방식을 이용하여 전자상거래 서비스를 제공하는 곳으로 오픈포유[15]가 유명하며 이외에도 쇼핑바다[16]나 산업기자재 판매를 위한 파텍21[17] 등이 있다. 이 서비스들의 경우 대부분 매매보호를 위한 서비스는 제공하지만, 실제 P2P 방식을 이용한 전자상거래 구현시 다음과 같은 여러 가지 요구 사항을 필요로 한다.

- 공정성(Fairness) : 구매자와 판매자가 서로 원하는 제품과 지불을 제대로 받을 수 있도록 보장해야 한다.
- 인증(Authentication) : 구매자와 판매자는 상호간의 정보 전달에 있어 자신이 원하는 상대가 맞는지 상대방의 신원을 확인할 수 있어야 한다.
- 기밀성(Confidentiality) : 구매자와 판매자간에 주고받는 거래 메시지가 허가되지 않은 제3자에게 노출되는 것으로부터 보호되어야 한다.
- 무결성(Integrity) : 구매자와 판매자간에 주고받는 거래 메시지가 제 3자에 의해 위, 변조되지 않아야 한다.
- 부인방지(Non-Repudiation)

-송신부인방지(Non-Repudiation of Origin) : 거래 종료 후 구매자는 자신이 보낸 거래 요청 메시지에 대하여 부인할 수 없어야 한다.

-수신부인방지(Non-Repudiation of Receipt) : 거래 종료 후 판매자는 구매자로부터 받은 구매 요청 메시지에 대하여 부인할 수 없어야 한다.

- 적시성(Timeliness) : 유한한 시간 내에 공정성을 잃지 않고, 프로토콜이 종료되어야 한다.

IV. P2P 방식을 이용한 새로운 e-Commerce 모델

본 논문에서 제안하는 모델은 P2P 서비스 방식 중 "혼합형 P2P 서비스"를 기반으로 하고, P2P 방식의 전자 상거래에 필요한 여러 가지 보안 요구사항을 고려하여 설계하였다.

4.1 제안 모델

P2P 방식의 전자상거래가 활성화되기 위해 무엇보다 중요한 요소는 거래에 대한 공정성 보장과 판

매자와 판매 컨텐츠에 대한 신뢰이다. 이에 본 논문에서는 보증 서버(ES : Escrow Server)를 사용하여 거래 당사자들 간에 컨텐츠 판매와 지불에 대해 공정성을 보장하고, 판매자와 판매 컨텐츠에 대한 신뢰도를 나타내는 평판 값을 이용하여 구매에 대한 신뢰성을 보장할 수 있는 P2P 방식의 새로운 e-Commerce 모델을 제안하고자 한다.

제안 모델에서 서비스 참여를 원하는 피어들은 먼저 인덱스 서버에 등록을 하고 거래시 사용하기 위한 인증서를 발급 받고, 컨텐츠 판매를 원하는 피어들은 판매하고자 하는 컨텐츠에 대한 설명 및 가격 정보 등을 인덱스 서버에 등록한다. 인덱스 서버는 서비스에 참여하는 피어들이 등록한 ID, 판매 컨텐츠 목록, 판매 피어의 평판 값, 판매 컨텐츠 자체에 대한 평판 값을 저장하고 있다. 상거래가 일어나기 전 컨텐츠 구매를 원하는 피어들은 인덱스 서버로 구매하고자 하는 컨텐츠에 관한 정보를 전송하고, 인덱스 서버는 구매 피어의 요구 사항에 맞는 컨텐츠를 가진 판매 피어 목록과 판매 피어의 신뢰도를 나타내는 평판 값과 각 판매 피어의 컨텐츠에 대한 신뢰도를 나타내는 평판 값을 함께 구매 피어로 전송한다. 구매 피어는 인덱스 서버로부터 받은 목록 중 평판 값을 참조하여 몇몇 판매 피어에게 견적 요구를 의뢰하여 확인하고, 그 중 특정 하나의 피어로 구매 요청을 하여 구매 의사를 결정하게 된다. 피어들 간에 주고받는 모든 메시지는 안전하고 기밀성이 보장되는 채널을 통해 전송되는 것으로 가정한다.

판매 피어와 판매 컨텐츠에 대한 평판 값은 서비스 이용을 위해 처음 등록시 기본값으로 설정되고, 컨텐츠 구매에 대한 거래가 완료된 후 구매자가 인덱스 서버에 전송하는 값에 따라 업데이트된다. 컨텐츠에 대한 평판 값 뿐만 아니라 판매 피어에 대한 평판 값을 참조함으로써 구매자는 동일한 컨텐츠를 판매하는 여러 피어들이 해당 컨텐츠에 대해 동일한 평판 값을 가질 경우 판매 피어에 대한 평판 값을 참조하여 좀 더 높은 신뢰도를 가지는 피어를 선택할 수 있다.

또한, 본 논문에서는 컨텐츠 교환과 지불에 있어 판매 피어와 구매 피어 상호간에 공정성 보장을 위해 별도의 보증 서버(ES : Escrow Server)를 사용하고, 이 서버 역시 신뢰된 서버로 가정한다. 구매 피어와 판매 피어는 ES를 통해 원하는 컨텐츠와 지불을 제대로 받을 수 있게 된다.

제안 모델은 상황에 따라 3가지 프로토콜로 동작한다.

(1) Main Protocol : 컨텐츠 판매와 지불이 정상적으로 이루어질 경우 동작하는 프로토콜
(2) Resolve Protocol : 구매 피어가 지불을 하고도 해당 컨텐츠를 받지 못할 경우 동작하는 프로토콜
(3) Abort Protocol : 판매 피어가 판매한 컨텐츠에 대한 지불을 받지 못할 경우 동작하는 프로토콜

4.2 제안 모델의 표기법 및 동작 방식

4.2.1 표기법

본 논문에서 사용되는 표기법은 다음과 같다.

- IS(Index Server) : 상거래 서비스에 참여하는 피어들이 등록한 피어 ID, 판매 컨텐츠에 대한 설명, 판매 가격 그리고 피어의 신뢰도를 나타내는 평판 값, 피어들이 판매하는 컨텐츠에 대한 신뢰도를 나타내는 평판 값을 관리한다. IS가 관리하는 정보의 형태는 다음과 같다.

$$< P_i, desc_{P_i}, amount_{P_i}, (R_{P_i}, R_{C_{P_i}}) >$$

  - P_i : 피어의 ID
  - $desc_{P_i}$: P_i가 판매하고자 하는 컨텐츠에 대한 설명
  - $amount_{P_i}$: P_i가 판매하고자 하는 컨텐츠에 대한 가격
  - $(R_{P_i}, R_{C_{P_i}})$: P_i에 대한 신뢰도와 P_i의 컨텐츠에 대한 신뢰도를 나타내는 평판 값

- ES(Escrow Server) : 구매 피어와 판매 피어 사이에 컨텐츠 판매과 지불에 있어 분쟁이 발생할 경우 해결을 위해 사용되는 보증서버이다.

- A : 구매 피어의 식별자

- B : 판매 피어의 식별자

- C_i : 판매 컨텐츠

- m_i : 구매 요청/응답 메시지

- Pay_A : 구매 피어의 지불 정보

- $revokeinfo = Sig_{PK_A}(Pay_A)$: 구매 피어가 지불을 하고도 자신이 원하는 컨텐츠를 받지

못할 경우 동작하는 "resolve protocol"에서 분쟁 해결을 위해 ES가 이용하는 정보로 구매 피어가 지불한 지불 정보를 판매 피어가 이용할 수 없도록 하는 정보이다.

- $aftoken = Sig_{PK_{ES}}(cancel, Pay_A)$: "resolve protocol"에서 분쟁 해결을 위해 ES가 생성하는 정보로 구매 피어가 지불을 하고도 컨텐츠를 제대로 받지 못한 경우 자신의 지불 정보를 판매 피어가 이용할 수 없도록 했지만 이미 판매 피어가 사용한 경우 법적 증거로 사용할 수 있도록 하는 정보이다.

- $Sig_{PK_{P_i}}(m)$: 메시지 m을 피어의 개인키로 서명한 값

- $E_k(m)$: 메시지 m을 대칭키 k로 암호화한 값

- $E_{pub_{P_i}}(m)$: 메시지 m을 피어의 공개키로 암호화한 값

4.2.2 제안 모델의 동작 방식

제안 모델은 컨텐츠 판매와 지불이 문제없이 정상적으로 이루어질 경우 동작하는 "main protocol", 구매 피어가 지불을 하고도 구매 의사를 밝힌 컨텐츠를 제대로 받지 못할 경우 동작하는 "resolve protocol", 판매 피어가 구매 피어로부터 판매 컨텐츠에 대하여 올바른 지불을 받지 못할 경우 동작하는 "abort protocol"로 나누어져 동작한다. 제안 모델의 전체적인 동작 방식은 아래 그림과 같다.

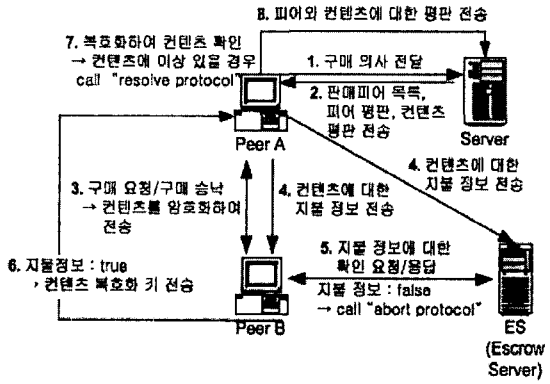

그림 3. 제안모델의 동작 방식
Fig. 3 The Operation of Proposal Model

(1) Main Protocol

1. $A \rightarrow IS$: $Send(desc_C)$

구매 피어(A)는 구매 하고자 하는 컨텐츠에 관한 정보를 인덱스 서버(IS)로 전송한다.

2. $IS \rightarrow A$:

$Send(B_1, B_2, \ldots, B_n, (R_{B_1}, R_{C_{B_1}}), (R_{B_2}, R_{C_{B_2}}), \ldots, (R_{B_n}, R_{C_{B_n}}))$

인덱스 서버는 구매 피어의 요청에 맞는 컨텐츠를 가진 판매 피어 ID와 각 판매 피어의 평판 값, 판매 컨텐츠에 대한 평판 값을 구매 피어에게 전송한다.

3. 구매 피어는 서버로부터 받은 판매 피어들에 대한 평판 값과 판매 컨텐츠에 대한 평판 값을 참조하여 구매를 원하는 피어(B_1)를 선택한다.

4. $A \rightarrow B_1$:

$m_1 = Sig_{PK_A}(A, B_1, desc_{C_{B_1}}, amount_{C_{B_1}}, ES)$

구매 피어(A)는 구매를 위해 선택한 판매 피어(B_1)로 구매와 관련된 메시지를 자신의 개인키를 사용하여 서명한 후 전송한다.

5. $B_1 \rightarrow A$: $m_2 = Sig_{PK_{B_1}}(m_1, E_k(C_{B_1}))$

판매 피어는 구매 피어가 보낸 메시지를 검증하여 확인하고, 구매자에게 해당 컨텐츠를 전송하기 전 구매자가 자신이 구매한 컨텐츠에 대한 비용을 지불한 후 컨텐츠를 사용할 수 있도록 하기 위해 컨텐츠를 암호화하여 암호화된 결과와 구매자로부터 받은 구매 메시지를 자신의 개인키로 서명하여 구매 피어에게 전송한다. 이때, 암호화에 사용하는 키는 구매 발생시마다 랜덤하게 생성하여 사용한다.

6. $A \rightarrow B_1, A \rightarrow ES : m_3 = Sig_{PK_A}(Pay_A)$

구매 피어는 판매 피어로부터 받은 구매 메시지에 대한 응답을 검증하고, 암호화된 컨텐츠를 복호화할 수 있는 키를 얻기 위해 구매 컨텐츠에 대한 지불 정보를 판매 피어와 ES(Escrow Server)에게 전송한다. 지불 정보를 판매 피어 뿐만 아니라 ES에게도 전송하는 이유는 구매 피어가 해당 컨텐츠에 대해 잘못된 지불을 할 경우 ES가 개입하여 해결해 주기 위해서이다. 이때, 구매 피어가 지불정보를 전송하고도 일정 시간 이내에 판매 피어로부터 구매 컨텐츠를 복호화 할 수 있는 키를 받지 못

할 경우 "resolve protocol"을 수행한다.

7. $B_1 \rightarrow ES : Pay_A$

$ES \rightarrow B_1 : compare(A(Pay_A), B_1(Pay_A))$

판매 피어는 구매 피어로부터 받은 지불 정보에 대한 정당성 확인을 위해 ES에 지불 정보를 전송하여 확인을 의뢰한다. ES는 구매 피어로부터 받은 지불 정보와 판매 피어로부터 받은 지불 정보를 비교하여 결과를 판매 피어에게 알려준다.

8. $B_1 \rightarrow A : m_A = E_{pub_A}(k)$

ES에 요청한 결과, 구매 피어로 부터 받은 지불 정보가 올바를 경우 판매 피어는 구매 피어가 암호화된 컨텐츠를 사용할 수 있도록 복호에 필요한 키를 구매 피어의 공개키로 암호화하여 전송한다. 만약 구매 피어로부터 받은 지불 정보가 올바르지 않다면, "abort protocol"을 수행한다.

9. $A = check(C_{B_1}, desc_{C_{B_1}})$

구매 피어는 판매 피어로부터 받은 키를 이용하여 컨텐츠를 복호화하고, 서버에 등록된 설명과 동일한 컨텐츠인지 확인하여 다를 경우 ES에게 문제를 제기하는 "resolve protocol"을 수행한다.

10. 구매 피어는 구매 컨텐츠에 대한 확인이 끝나면 판매 피어에게 최종 대금 결제를 수행하고, 판매 피어에 대한 평판과 판매 피어의 컨텐츠에 대한 평판을 인덱스 서버로 전송한다. 인덱스 서버는 해당 판매 피어에 대한 평판 값과 컨텐츠에 대한 평판 값을 업데이트하고, 다음 거래시 구매 피어들이 참조할 수 있도록 한다.

(2) Abort Protocol

판매 피어가 구매 피어로부터 받은 지불 정보에 문제가 있을 경우 ES에 요청시 해결을 위해 동작하는 프로토콜이다.

1. $B_1 \rightarrow ES : request(cancel)$

판매 피어는 구매 피어로부터 받은 지불 정보에 문제가 있을 경우 ES에 의뢰하여 구매 피어와의 거래 중지를 요청한다.

2. $ES \rightarrow A, B_1 : Cancel$

ES는 구매 피어와 판매 피어에게 거래 중지 메시지를 보내게 되고, 두 피어 사이의 거래는 중단된다. 구매 피어는 판매 피어로부터 구매를 원하는 컨텐츠를 받긴 했지만 암호화되어 있기 때문에 사용할 수 없게 된다.

(3) Resolve Protocol

구매 피어가 자신이 구매한 컨텐츠에 대해 지불을 하고도 해당 컨텐츠를 복호화 할 수 있는 키를 제대로 받지 못하거나 복호화한 컨텐츠가 서버에 등록된 설명과 다른 컨텐츠일 경우 동작하는 프로토콜이다.

1. $A \rightarrow ES : revokeinfo = Sig_A(Pay_A)$

구매 피어는 문제 해결 요청을 위해 "revokeinfo" 정보를 생성하여 ES에게 전송한다.

2. ES는 구매 피어가 보낸 "revokeinfo" 정보가 유효하고 "abort protocol"이 실행 중이 아니라면 판매 피어가 정확한 복호화 키를 주지 않은 것으로 판단하여 구매 피어가 준 지불 정보를 사용할 수 없도록 한다. 그리고, 판매 피어가 이미 지불 정보를 사용하였다면 구매 피어에게 "afftoken"을 발행하여 분쟁 발생시 대응할 수 있도록 한다.

3. 구매 피어는 판매 피어와 판매 컨텐츠에 대한 평판을 서버로 전송한다.

4.3 제안 모델의 분석

제안 모델에서는 다음과 같은 보안 서비스를 제공한다.

(1) 공정성

판매자와 구매자는 지불에 대한 정확한 컨텐츠가 아니거나 해당 컨텐츠에 대한 지불이 제대로 일어나지 않을 경우 ES에게 해결을 요청한다. 이때, ES는 판매자와 구매자 사이에 직접적으로 개입하는 것은 아니지만 문제 발생시 해결을 도와줄 수 있다. 이를 통해 구매자와 판매자는 거래에 대한 공정성을 보장 받을 수 있다.

(2) 인증

상거래에 참여하는 피어들은 컨텐츠에 대한 판매나 구매를 위해 먼저 서버에 로그인을 한다. 로그인시 피어들에 대한 인증이 이루어지고, 거래를 위한 메시지를 주고 받을 때 피어 개개인의 개인키로 전송 메시지에 서명함으로써 피어들에 대한 인증 또한 가능하다.

(3) 기밀성
구매자와 판매자간에 교환되는 컨텐츠는 암호화되어 전송되므로 기밀성을 보장받을 수 있다.

(4) 부인방지
판매자와 구매자가 상호 교환하는 메시지는 개인키로 서명하여 사용되기 때문에 거래 종료 후, 구매자와 판매자는 자신에 보낸 메시지에 대해 부인할 수 없다.

V. 결론 및 향후 과제

본 논문에서는 서버 중심으로 동작하는 기존의 전자상거래 방식에 중앙 서버 없이 서비스 이용자들간의 직접적인 통신을 통하여 구매 및 판매가 가능한 P2P 방식을 적용한 새로운 e-Commerce 모델을 제안하였다. 제안 모델은 ES(Escorw Server)를 통하여 컨텐츠 교환과 지불에 있어 공정성을 보장해 줄 수 있고, 피어에 대한 평판 값을 참조하여 거래를 원하는 피어에 대한 신뢰도를 높일 수 있으며, 컨텐츠 자체에 대한 평판 값을 참조하여 안전하고 정확한 컨텐츠 구매가 가능한 이점을 가진다. 또한, 제안 모델에서는 전자상거래에서 필요한 공정성, 기밀성, 인증, 부인방지 등과 같은 보안 서비스를 제공하고 있다.

P2P 기술의 발전으로 파일 공유로 제한되었던 P2P 기술의 응용 분야가 점점 다양해지면서 디지털 컨텐츠의 유통 뿐만 아니라 네트워크를 통한 협업 시스템이나 분산 컴퓨팅에까지 적용 가능하다. 그러나, 이러한 P2P의 가능성이 구체화되고 상용화되기 위해서는 해결해야할 몇 가지 문제점들이 있으며, P2P 기반의 상거래 모델이 수익 창출에 성공할 수 있을지의 여부는 많은 시간과 시행 착오를 거쳐야 알 수 있을 것으로 예상된다. 또한, P2P의 적용 분야에 따라 필요한 보안 요구 사항에 대한 연구와 P2P 기술의 표준화와 관련된 추가적인 연구와 피어와 컨텐츠에 대한 신뢰도를 위해 이용하는 평판 값의 관리에 대한 연구가 지속적으로 필요할 것으로 판단된다.

참고문헌

[1] DIOGO R.FERREIRA, J.J.PINTO FERRERIA, "Building an e-marketplace on a peer-to-peer infrastrucuture", INT.J.COMPUTER INTEGRATED MANUFACTUREING, APRIL-MAY 2004, VOL.17, No.3, 254-264
[2] 서수석, 임규홍, 이종호, "P2P의 전자상거래 응용 및 발전방향에 관한 연구", 한국경영정보학회 춘계학술대회 논문집, 2002
[3] "세상을 바꾸는 힘의 중심 P2P", 프로그램 세계, 2002, 7월호
[4] 이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영 공저, "전자상거래 보안 기술", 생능출판사, 1999
[5] 소프트포럼, "B2B 전자상거래 보안"
[6] Dejan S. Milojicic, Vana Kalogeraki, Rajan Lukose, Kiran Nagaraja, Jim Pruyne, Bruno Richard, Sami Rollins, Zhichen Xu, "Peer-to-Peer Computing", HP TechReport HPL-2002-57, 2002. http://www.hpl.hp.com/techreports/2002/HPL-2002-57.pdf
[7] 소리바다, http://www.soribada.com
[8] eDonkey, http:/www.edonkey2000.com
[9] "차세대 인터넷 P2P", 전현성 외 4인 역, O'REILLY, 한빛미디어
[10] Krishna Kant, Ravi Iyer, "A Framework for classifying Peer-to-Peer Technologies", CCGRID'02, 2002
[11] Holger Vogt, "Asynchronous Optimistic Fair Exchange Base don Revocable Items", Financial Cryptography, 2003
[12] N.Asokan, "Fairness in electronic commerce", PhD thesis, University of Waterloo, Canada, May 1998
[13] N. Asokan, M. Schunter and M.waidner, "Optimistic protocols for fair exchange", 4th ACM Conference on Computer and communications Security, 1997
[14] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani di, "Choosing Reputable Servents in a P2P Network", WWW2002, 2002
[15] 오픈포유, "http://www.open4u.co.kr"
[16] 쇼핑바다, "http://www.shoppingbada.co.kr"
[17] 파텍21, "http://www.partec21.com"
[18] Bill Horne, Benny PInkas, Tomas sander, "Escrow Services and Incentives in Peer-to-Peer Networks", EC'01, 2001
[19] SAI HO KWOK, KARL R. LANG AND KAR YAN TAM, "Peer-to-Peer Technology

Business and Service Models : Risks and Opportunities", Electronic Markets, 2002

저자소개

신정화(Jung-Hwa Shin)

1997년 한국방송통신대학교 전자계산학과(이학사)
2000년 부경대학교 대학원 전산정보학과(이학석사)
2001년~현재 부경대학교 대학원 전자계산학과 박사과정
※관심분야 : 암호이론, 네트워크 보안, 이동 에이전트, XML 보안, Peer-to-Peer 보안

이경현(Kyung-Hyune Rhee)

1982년 경북대학교 수학교육과(학사)
1985년 한국과학기술원 응용수학과(이학석사)
1992년 한국과학기술원 수학과(이학박사)
1985년~1993년 한국전자통신연구소 선임 연구원
1995년~1996년 Univ. of Adelaide 응용수학과, Australia 방문교수
1999년 Univ. of Tokyo, 객원 연구원
2001년~2002년 Univ. of California at Irvine, USA, Visiting Scholar
2002년~2003년 Intergovernmental Organization, Colombo Plan Staff College, Manila, Philippines Chair of Division of Information & Communication Technology
1993년~현재 부경대학교 전자컴퓨터정보통신공학부 정교수
1997년~현재 한국멀티미디어학회 학술이사
2001년~현재 한국정보보호학회 논문지 편집위원
※관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론