P2P 기반의 신뢰성 있는 e-Commerce시스템 설계

서선희*, 이경현**
*부경대학교 전산정보학과
**부경대학교 전자컴퓨터정보통신공학부
e-mail : sea312@empal.com*, khrhee@pknu.ac.kr**

Design of Trusted Peer-to-Peer e-Commerce System

Sun Hee Seo*, Kyung Hyune Rhee**
Department of Computer and Information Science, Pukyung National University
**Devision of Electronic, Computer & Telecommunication Engineering, Pukyung National University

요 약

P2P(Peer-to-Peer) 서비스는 기존의 서버/클라이언트 방식과는 달리 중앙서버를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 PC를 직접 연결 시켜 데이터 공유 및 교환 할 수 있게 해주는 기술과 그 기술을 응용해서 만든 새로운 서비스를 말한다. P2P 서비스를 전자상거래에 적용 시 상거래 서비스 이용자들은 중앙 서버 없이 직접 통신하면서 언제, 어디서나 제약 없이 개인별 상거래나 경매가 가능한 반면 별다른 안전 장치가 없어 피해가 우려된다. 본 논문에서는 P2P기반의 e-commerce에서 디지털 컨텐츠 판매에 대한 지불에 있어 좀 더 공정한 지불 프로토콜과, 피어들에 대한 신뢰성 보장을 위해 평판인증서(reputation certificate)를 사용하여 신뢰성 있는 e-commerce 시스템을 설계하고자 한다.

1. 서론

Peer-to-Peer(P2P) 네트워크 시스템이란 모든 사용자가 각각 서로 동등한 입장에서 정보를 공유하고 교환하는 체계이다. 인터넷 쇼핑몰을 중심으로 거래가 발생하는 기존의 전자상거래 방식과는 달리, P2P 기술을 전자상거래에 적용하는 경우 상거래 서비스 이용자들은 특정 중앙 서버에 의존하지 않고 개인별 상거래나 경매가 가능하다는 장점으로 인해 P2P 방식을 이용한 전자상거래 시스템 개발에 관한 연구가 급증하고 있다[1]. 그러나, 신뢰할 수 있는 관리 서버의 부재로 인해 P2P 네트워크는 신뢰성(reliability)이나 공정성(fairness) 같은 e-commerce 거래에 필요한 모든 서비스를 효과적으로 제공하지 못하고 있는 실정이다. 공정성은 e-commerce에서 중요한 보안 서비스로써 프로토콜의 종결 후, 교환에 참여했던 모든 개체들은 자신이 원하는 것을 받거나 혹은 어떤 개체도 원하는 것을 받지 못함을 보장하는 것을 말한다[2]. 또한, P2P 시스템에서는 사용자의 익명성 때문에 그들이 제공하는 자료들에 대한 신뢰성 또한 부족하다. 이에 본 논문에서는 디지털 컨텐츠의 판매와 지불에 있어 좀 더 공정한 지불과, 거래의 신뢰성을 보장하기 위한 P2P 기반의 e-commerce 시스템 설계에 대해 제안한다.

본 논문의 구성은 2장에서 관련연구로 P2P e-commerce 와 평판(reputation)에 대해 살펴보고, 3장에서 제안시스템 모델의 구성요소와 동작 방식에 대해 살펴보고, 4장에서 결론을 맺는다.

2.관련연구

2.1 P2P e-Commerce

디지털 경제의 본격적인 도입으로 초기 인터넷 기업들이 향유하던 거래비용의 감소와 선점효과 등 전

략적 우위를 가능하게 하는 많은 요소들이 이제 더 이상 의미를 갖기 어렵게 되었다. 디지털 경제의 속성은 컨텐츠의 디지털화를 통한 제작비용, 유통비용, 보관비용, 탐색비용, 복제비용 등의 절감과 이를 기업경영에 반영한 거래비용의 감소에 있다[3]. 하지만 이러한 거래 비용의 절감은 치열한 경쟁구조를 도입하게 되었고 온라인과 오프라인의 기업들은 엄청난 경쟁 환경 하에서 구체적인 대안을 찾지 못하고 있다. 또한 네트워크 효과와 수확 체증의 효과를 이용한 선점전략에 기초하여 기업의 독점적 이익을 보장해 줄 것으로 판단하고 엄청난 시스템 구축 및 마케팅비용을 수반한 투자는 수익성 모델을 요구하는 시장의 논리에 의거하여 주춤거리고 있는 실정이다[3]. 이러한 시점에서 인터넷 비즈니스의 새로운 모델로 등장하고 있는 P2P는 차세대 인터넷의 대안으로 상당한 의미를 갖는다. P2P는 원래 'Peer to Peer'의 약자로서, 개인 대 개인의 커뮤니케이션을 가능하게 해주는 다양한 기술의 총칭으로 일종의 분산컴퓨팅, 분산처리 기술방식을 일컫는다. 현재는 기술적인 측면보다는 소비자 각 개인이 중심이 되는 'Person to Person'의 개념으로 빠른 속도로 자리 매김하고 있다. 하지만 P2P의 본질적인 문제점인 거래의 신뢰성 보장에 대한 해결책이 아직까지 마련되지 않고 있으며, 결제, 배송 등 전자상거래 인프라 시스템이 제공되지 않아 실제적인 상거래 발생 가능성이 작다고 볼 수 있다.

본 논문에서 이러한 문제점 해결의 방안으로 거래에 대한 판매자의 신뢰성문제를 해결하기 위해 평판인증서을 이용하고, 신뢰성 있는 보증서버를 두어 공정한 지불과 배송이 가능하도록 한다.

2.1.1 e-Commerce요구사항

e-commerce 서비스를 제공하기 위한 요구 사항은 다음과 같다[4].

- 공정성(Fairness) : 구매자와 판매자간에 정보를 전달 할 때 자신이 원하는 정보를 둘 다 가질 수 있거나 가지지 못함을 보장 할 수 있어야 한다.
- 신뢰성(Trustiness) : 전자상거래에 참여하는 피어들에 대한 신뢰성을 제공할 수 있어야 한다.
- 인증(Authentication) : 구매자와 판매자간에 정보를 전달 할 때 자신이 원하는 상대인지를 확인할 수 있어야 한다.
- 기밀성(Confidentiality) : 구매자와 판매자간에 주고받는 정보는 불법적인 사용자에 의해 변조되어서는 안 된다.
- 부인방지(Non-Repudiation) : 구매자와 판매자는 서로 간에 보낸 메시지에 대해 부인할 수 없어야 한다.

2.2 평판(Reputation)

소리바다나 Napster, eDonkey 등의 P2P프로그램에서 어떤 노래를 찾고자 할 때 우리는 아무 정보 없이 파일 제공자가 제공하는 정보만으로 그 파일에 대한 모든 것을 판단한다. 그 파일이 실제로는 바이러스나 웜 등을 포장해 놓은 것일 수도 있고 매우 질이 낮은 것일 수도 있지만 실제 사용자들은 그것을 판단할 수 있는 어떠한 정보도 가지고 있지 않은 것이다. 이러한 문제점들에 대한 일차적인 해결 방안으로 사용자들의 경험에 의한 의견이나 소문 등을 생각할 수 있으며 실제로 이것은 여러 인터넷 사이트에서 사용되고 있다. 특히나 eBay나 옥션 등에서 거래를 할 때 판매자와 구매자에 대한 평가가 거래에 대한 큰 판단기준이 되고 있다. 반면 그러한 의견이나 소문들의 신뢰도 혹은 위조 가능성이 문제가 될 수 있다. 이러한 문제점에 대한 해결 방안으로 몇 가지의 방법이 제시되고 있는데, 그 중 평판에 기반한 시스템이 가장 주목할 만하다[5].

3.제안 시스템

제안 시스템은 전자상거래에 참여하는 피어에 대한 신뢰성과 거래에 대한 공정성을 보장하기 위해, 판매자와 구매자의 거래에 직접 관여하지는 않지만 P2P 기반의 가상의 상거래 공간을 제공하는 마켓매니저(MM:Market Manager)를 가정하며, 마켓 매니저는 공정한 거래를 위한 매매보증(Escrow) 서버와 거래에 대한 피어들의 신뢰도를 평가하기 위해 평판관리 서버를 운영한다. 또한 판매와 지불의 공정성을 위해 조건 암호기법[6]을 이용하여 구매자가 올바른 지불 단계를 수행하지 않으면 디지털 컨텐츠를 획득하지 못하도록 한다.

3.1 시스템 구성요소

- RMS(Reputation Manager Server) : 서비스에 참여하는 피어들의 평판 값을 받아 RC(Reputation Certificate)를 발행한다.
- ES(Escrow Server) : 개인 간 거래에서의 지불 문제를 해결하기 위해 신뢰성 있는 ES를 두어 중개 역할을 하게 한다.

- P_i : 컨텐츠 거래에 참여하는 판매피어, 구매피어
- RD(Reputation Data) : 구매피어가 RMS에게 보내는 판매피어에 대한 평판 정보
- RC(Reputation Cerificate) : 평판 값을 수렴하여 RMS가 발행하는 평판인증서

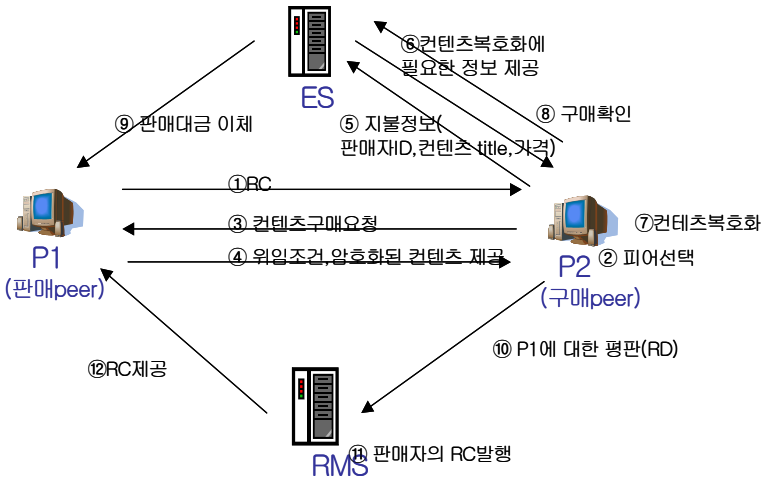
- RC(Reputation Cerificate) 형식

판매 PeerID	Rating	Time stamp	유효기간	RMS Signature

- RD(Reputation Data) 형식

Target PeerID	Voting PeerID	Rating	Time stamp	Voter Signature

3.2 P2P 기반 상거래 모델



<그림 1> 제안시스템 모델

제안모델은 크게 가입단계, 거래/지불단계, 평판단계로 나뉘어 동작한다.

❖ 표기법

- $*$: 모든 피어
- q : 충분히 큰 소수
- x : 판매피어의 ElGamal 타입 개인키, $x \in Z_q$
- y : 판매피어의 ElGamal 타입 공개키, $y = g^x$
- P_1 : 판매피어(Seller)
- P_2 : 구매피어(Buyer)
- MM : 마켓 매니저
- PU_X : 피어 X의 공개키
- PK_X : 피어 X의 개인키
- $Cert_X$: 공개키 PU_X에 대한 인증서
- $E_{PU}(\cdot)$: 공개키를 이용한 암호화
- $D_{PK}(\cdot)$: 개인키를 이용한 복호화
- $Sig_{PK}(\cdot)$: 전자서명 생성
- $Ver_{PU}(\cdot)$: 전자서명 검증
- $Enc_K(\cdot)$: 비밀키를 이용한 암호화
- $Dec_K(\cdot)$: 비밀키를 이용한 복호화
- K_{XY} : 피어 X와 피어 Y의 공유키

(가) 가입

① 각 피어 P_i는 시스템에 가입한다.

② MM은 RMS에 P_i의 기본 평판 값을 등록한다.

③ P_i의 공개키 PU_i에 대한 인증서 $Cert_i$와 평판에 대한 RC_i를 피어에게 발급한다.

(나) 거래/지불단계

① $P_1 \rightarrow *$ (Advertise) :

판매(Seller) 피어 P_1는 자신의 컨텐츠에 대한 정보 m_1, $Sig_{PK_{P_1}}(m_1)$를 P2P 네트워크로 발송한다. 이때 자신의 평판에 대한 RC도 포함한다.

$m_1 = \{ P_1, Cert_{P_1} item\_info, RC_{P_1} \}$,

$Sig_{PK_{P_1}}(m_1)$

② $P_2 \rightarrow P_1$ (구매요청) :

구매(Buyer) 피어 P_2는 P2P상에서 자신이 원하는 컨텐츠를 검색하고, RC의 평판에 따라 적당한 판매 피어를 선택하고, 선택한 판매피어에게 m_2, $Sig_{PK_{P_2}}(m_2)$를 전송한다.

$m_2 = \{ item\_info, P_1, P_2, C = E_{PU_{P_1}}(K_{12}) \}$,

$Sig_{PK_{P_2}}(m_2)$

③ $P_1 \rightarrow P_2$:

P_1는 컨텐츠 전송을 위한 키(K)를 생성하고 위임 조건(ϕ)을 명시하여 다음을 계산한 후, m_3, $Sig_{PK_{P_1}}(m_3)$를 전송한다.

ϕ = {거래정보(구매피어, 판매피어, 컨텐츠 정보, 가격, 날짜 등}, $Sig_{PK_{P_1}}(\phi)$

임의의 난수 $r \in Z_q$를 선택하고 다음을 계산한다.

$c_1 = g^r,\ c_2 = (y)^r \cdot K$

임의적으로 $v \in M$를 선택하고 다음을 계산한다.

$u_1 = E_{PU_{ES}}(v),\ u_2 = x - H(\phi, v)$

$m_3 = \{ c_1,\ c_2,\ \phi,\ Enc_{K_{12}}(u_1, u_2),$

$Enc_K(item)\},\ Sig_{PK_{P_1}}(m_3)$

④ $P_2 \rightarrow ES$:

구매피어는 ES를 통해 지불정보를 제공한다.

$m_4 = \{\ c_1,\ u_1,\ \phi,\ E_{PU_{ES}}(pay\_info)\}$,

$Sig_{PK_{P_2}}(m_4),\ Cert_{P_2}$

⑤ $ES \rightarrow P_2$:

ES는 ϕ를 검증하고, 명시된 조건에 따라 대금 및 복호화에 필요한 정보를 계산한 후 m_5, $Sig_{PK_{ES}}(m_5)$ 제공한다.

$v = D_{PK_{ES}}(u_1),\ c_B = c_1^{H(\phi, v)}$

$m_5 = E_{PU_{P_2}}(c_B),\ Sig_{PK_{ES}}(m_5)$

⑥ 구매피어는 컨텐츠 복호화 키를 계산하여 컨텐cm를 복호한다.

$K = c_2 \cdot c_1^{-u_2} \cdot c_B^{-1}$

$item = Dec_K(Enc_K(item))$

(다) 평판단계

① $P_2 \rightarrow RMS$:

구매피어는 구매한 컨텐츠에 대한 평판을 RMS에게 제공한다.

$RD = < m_6 = \{ P_1,\ P_2,$ rating, $T\},$

$Sig_{PK_{P_2}}(m_6) >$

② RMS는 수집된 평판값들을 취합하고 평가하여 새로운 RC를 발급한다.

3.3 제안 시스템의 특징

본 논문에서 제안한 P2P방식의 e-commerce시스템에서는 구매피어와 판매피어 간의 상거래에 대한 신뢰성과 공정성을 위해 지불중개 서버인 ES와 평판관리서버인 RMS를 두었다. 조건 암호기법을 이용하여 구매자가 ES를 통해 컨텐츠 구입에 대한 올바른 지불정보를 제공하는 경우에만 판매자에 의해 암호화된 컨텐츠를 복호화할 수 있으며, 평판 관리 서버를 통해 구매자가 판매 피어에 대한 신뢰성을 평가할 수 있도록 하였다. 제안 방식에서 ES가 복호화에 필요한 정보를 제공하지만 ES에게 주어지는 정보만으로는 ES가 암호화된 컨텐츠를 획득할 수는 없으므로 판매자는 올바른 가격을 지불한 정당한 구매자만이 컨텐츠를 획득할 수 있음을 확신 할 수 있다. 평판에 있어서 reputation voting의 위조방지를 위해 평판 값을 보낼 때, 구매피어의 서명을 포함하고, voting의 임의적인 삭제, 추가와 악의적인 사용자들(임의의 제3자)에 의한 평판 조작은 RMS에서 평판 값을 수렴하여 평판 인증서를 발행하게 하므로 신뢰성을 보장할 수 있는 '평판' 정보가 되도록 하였다.

4.결론

본 논문에서는 P2P e-commerce의 원활한 발전을 위해 지불 중개 서버를 두어 지불에 관계된 문제를 해결하고자 하였으며, 판매자에 대한 신뢰성 문제를 해결하고자 평판 인증서를 사용하였다.

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 것이다.

참고문헌

[1] Diogo R.ferreira, J.J.Pinto Ferreria, "Building an e-marketplace on a Peer-to-Peer infrastructure", International Journal Computer Integrated Manufacturing, 2004.

[2] Petros Daras, Despoina Palaka, Venetia Giagourta, "A novel Peer-to-Peer payment", IEEE, 2003.

[3] 김희락, "P2P 결제서비스의 현황과 전망", 대은경제리뷰, 2001.

[4] Ji Won Jung, "A Fair and Reliable e-Commerce Model InP2P Network", master's thesis Pukyung Nat'l Unvi., 2004.

[5] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani De Vimercati, "Choosing Reputable Servents in a P2P Network", WWW2002, 2002.

[6] Y. Watanabe, M. Numao, "Conditional Cryptographic Delegation for P2P Data Sharing", In Proceedings of International Security Conference(ISC 2002), LNCS 2433, pp.309-321, 2002.