Peer-to-Peer 를 이용한 경매 모델

이영균[0], 공은배
충남대학교 컴퓨터공학과
{mazart,keb}@ce.cnu.ac.kr

Auctions and Mechanism Design on Peer-to-Peer Networking

Young-Kyun Lee[0], Eun-Bae Kong
Dept. of Computer Engineering, Chungnam National University

요 약

본 논문에서는 다자계산 이론과 Peer-to-Peer 네트워크 기술을 이용하여 안전하고 효율적인 경매 모델을 제안하고자 한다. 기존에 제안된 경매 모델의 경우 안전한 계산을 할 수 있었으나 메시지 전송에 있어 효율적인 작업을 할 수 없었다. 또한 경매의 규모가 커져감에 따라 부가적으로 들어가는 비용도 증가해야만 했다. 그러나 제안된 모델에서는 Peer-to-Peer 네트워크 기술을 이용함으로써 서버에 집중되는 네트워크 부하를 줄이고 또한 제안된 모델을 사용하는 다른 경매 그룹과 쉽게 연동 할 수 있어 경매 규모를 쉽게 확장을 할 수 있게 하였다.

1. 서론

최근 인터넷 기술의 발전으로 전자상거래를 통한 상업활동이 많아지게 되었다.

현재 사용되는 일반적인 모델은 상품 목록과 가격을 인터넷을 통해서 선전하고 구매자는 이를 보고 구매를 하는, 1 대 1 고정된 가격 상거래이다. 하지만 작은 거래에서 기업간의 큰 거래에 이르기까지 많은 수가 경매로 이루어진다. 즉, 고정된 가격을 가지고 거래가 이루어지는 것이 아니라 다자간의 가격 협상에 의해서 이루어 진다.

이미 국내외에서 eBay, Auction, Daum, Yahoo 등에서 경매를 통해 이러 서비스를 제공하고 있는데, 기존의 사이트들은 안전성과 Business 모델 측면에서 문제점을 안고 있다. Business 측면에서 볼 때, 이 사이트들에서 가장 많이 사용되는 경매 방식은 English Auction 인데 많은 통신 Overhead 가 있을뿐더러 책정되는 가격이 Vickery Auction 방식보다 더 낮은 경우가 많아 판매자에게 불이익을 초래하게 된다. 안전성 측면에서 볼 때 위의 경매를 포함한 기존의 많은 통신 프로토콜은 불안전한 채널과 정직한 호스트를 가정으로 설계되었다. 그러나, 인터넷 경매의 경우에는 서로 신뢰할 수 없는 불특정 다수가 프로토콜에 참여한다. 또, 프로토콜의 수행이 상대방의 통제하에 있는 컴퓨터에 의해서 수행이 되기 때문에 지시한대로 프로토콜이 성실히 수행되리란 보장도 없다. 즉, 자신의 통제밖에 있는 믿을 수 없는 컴퓨터가 해킹사고에 의해서건 그 소유자의 이익을 위해서건 프로토콜에서 벗어난 행동을 할 위험이 있다.

본 연구에서는 위에서 나온 문제점들을 보완할 수 있는 모델을 제안하고자 한다. 즉, 불안전한 채널과 부정직한 호스트의 현실에서 서로 신뢰할 수 없는 여러 프로세스들이 자신들의 비밀은 최대한 지키면서 그들의 비밀을 입력으로 이용하여 공통의 목표를 그들 스스로 안전하게 이루어내는 안전한 다자계산을 하는 방법과 경매* 규모가 커짐에 따라 네트워크를 효율적으로 이용할 수 있는 모델을 제안하고자 한다. 우선 2 장에서는 그간 경매에 사용된 기술들을 제시하고, 이들 모델이 경매 규모가 커짐에 따라 생기는 문제점을 보여주고, 3 장에서는 본 논문에서 제안하고자 하는 모델에 대해 설명을 할 것이다. 그리고 결론을 맺고자 한다.

2. 관련연구

일반적으로 인터넷 경매에 있어서 주요한 관점은 개인의 입찰가격 정보는 비밀을 유지하면서 경매 결과를 계산할 때에 얼마나 효과적으로 메시지 교환하느냐에 있다. 이 장에서는 이를 위해 제안된 몇 가지 모델들과 Peer-to-Peer(이하 P2P) 공유에 대한 설명하고자 한다.

2.1 순수 다자 계산

경매를 암호학적인 관점에서 보면 안전한 다자간의 계산에 있다. 다자간의 계산을 위한 프로토콜은 많은 곳에서 제안되어 있다. [3, 6]에서 제시된 프로토콜은 n 개의 파티로 이루어진 그룹에서 각 파티에 비밀 값 a_i 에 대해서 $F(a_1, a_2, ..., a_n)$를 계산하는 것을 말한다. 프로토콜이 끝난 후에는 각 파티들은 $F(a_1, a_2, ..., a_n)$의 결과값 이외에는 어떠한 정보를 추가로 얻을 수 없다. 이를 경매에 적용을 하면 각각의 파티들은 입찰자가 되는 것이고, 함수 F 는 Auctioneer 가 되는 것이다. 이러한 모델의 경우 각 파티들의 상호 작용을 통해 이루어지는 것이므로 많은 양의 네트워크 리소스 소비와 Party 들간의 비밀스런 통신이 보장되어야 한다.

2.2 분산 Auctioneer 서버 방식

다음으로 제시된 모델은 몇몇 Auctioneer 서버들 사이에서의 복잡한 연산을 통해 각 파티들의 입찰정보의 비밀을 유지하는 것이다. [2, 4] 모델은 안전한 계산을 위해서는 최소한 4 개 이상의 서버가 필요하다. 또한 각 서버들 사이의 여러 라운드의 메시지 교환이 필요하다. 다음으로 제시된 모델은 Cachin[7]에 의해 제시된 모델로 2 개의 Auction Servers 를

통해서 경매를 진행하는 것이다. 이 모델에서 파티는 단 한 개의 Server 와 연결이 되며, 서버의 확장을 통해서 비밀을 유지시킨다. [2, 4]의 시스템의 경우 서버들 사이의 많은 양의 메시지 교환이 필요로 한다. 또한 이들 모델의 경우 믿을 수 있는 Auctioneer 의 서버가 필요하다. [5]

2.3 P2P Networking

P2P[8] 네트워크 모델은 이미 많은 곳에서 활용화되고 있다. P2P 란 컴퓨터들간의 직접적인 교환을 통한 컴퓨터 리소스의 공유를 말한다. 현재 나와 있는 P2P 모델에는 크게 세 가지 종류가 있다. - 브로커 중재형 공유, 순수 P2P 공유 방식, Cycle Sharing(CPU Cycle Sharing)

이 세 가지 방식 중 제안된 경매 모델에 사용된 방식은 브로커 중재형 방식이다. 이는 경매의 규모가 커져감에 따라 경매에 대한 정보를 검색하고, 관리하기 위해서 이들 정보를 유지하는데 있어 브로커를 사용하기 위해서다. 이는 MP3 음악 파일을 공유하는 소리바다, Napster 에서도 사용이 되고 있다.

본 논문에서는 개인의 기밀성을 유지하기 위해서 Auctioneer 와 Auction Issuer 사이는 Moni Naor[1]에서 제안된 프로토콜을 사용할 것이고, 네트워크의 효율성을 높이기 위해서 P2P 네트워크 위에서 동작하는 2 개의 구성요소로 이루어진 경매 모델을 제안할 것이다.

3. P2P Networking 상에서의 경매 모델

이번 장에서는 제안 하고자 하는 프로토콜에 대한 설명을 하고자 한다. 우선 전체적인 구성요소 및 관계를 설명한 후 프로토콜의 동작을 제시하고자 한다.

3.1 프로토콜 구성 요소

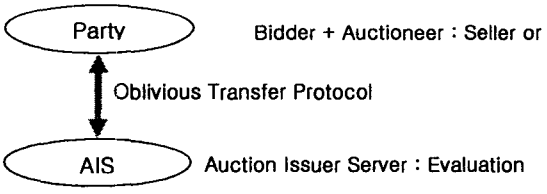

그림 1. 프로토콜 구성 요소

프로토콜을 이루는 구성요소는 그림 1 에서 보듯이 Party 와 Auction Issuer Server(이하 AIS) 2 가지로 이루어져 있다. 우선 Party 는 경매의 입찰자 및 실제 상품을 파는 Seller 역할을 한다. 즉 Party 는 Seller 의 역할과 입찰자의 역할, 두 가지를 동시에 할 수 있다. 이는 어느 누구든 물건을 팔거나 살 수 있기 때문이다. 이는 [1]에서 제시한 Bidder 와 Auctioneer 의 역할을 동시에 하는 것이다. AIS 는 [1]에서 제시한 AI 와 같이 경매의 결과를 계산할 수 있는 모듈을 탑재하고 있다. 즉 [1]에서의 AI 와 같은 역할을 하는 것이다. 이와 같이 2 개의 구성요소로 모델을 변경한 이유는 [1]에서 제시한 모델에서는 각각의 경매에 대한 Auctioneer 를 선정하고 이곳과 통신을 하게 되는데 Auctioneer 의 역할을 할 수 있는 서버의 수는 한정이 되어 있기 때문에 경매할 품목이 늘어나고 각각의 Bidder 들이 여러 개의 경매에 동시에 참여하게 될 경우 Auctioneer 에 대한 네트워크 부하가 증가하게 되기 때문이다. 그렇기 때문에 Auctioneer 역할을 하는 모듈을 각 파티에 탑재시켜서 Bidder 들의 증가에 따른 이를 담당할 수 있는 Auctioneer 를 P2P 네트워크를 통해서 분산시킨 것이다.

AIS 의 경우 Party 의 경매 정보를 관리하는 동시에 Party 들에게 검색할 수 있는 환경을 제공한다. 또한 다른 경매 그룹과 P2P 연결을 통해서 그 쪽의 경매 정보 또한 AIS 에 업데이트 된다.

3.2 구성 요소들 간의 관계

구성 요소들 간의 관계는 모두 P2P 네트워크상에서 통신이 이루어지며, Party 와 AIS 는 Oblivious Transfer Protocol[1]에 의해 통신한다. 또한 Party 와 AIS 는 Garbled Circuit Technique Attributed to Yao[3, 6]를 사용하여서 다자간의 계산을 안전하고 효과적으로 계산한다.

다른 경매그룹과의 관계는 AIS 간의 P2P 경매 정보 공유를 통해서 두 그룹간의 정보 교환이 이루어지며 서로의 AIS 경매 정보의 내용이 갱신되는 것이다. 이는 서로 인접한 AIS 사이에 이루어지므로 새로운 경매가 발생이 되었을 경우에 경매 내용을 주고 받는 것이다.

Party 와 Party 사이의 관계는 두 가지 관점에서 볼 수 있는데 우선 입찰자와 판매자 사이에는 P2P 공유가 이루어지며 입찰자 사이에는 아무 관계를 형성하지 않는다. 후자의 경우 입찰자 서로간의 공유를 통해서 이루어지는 단합을 막기 위한 것이다. 전자의 경우 판매자가 Auctioneer 역할을 수행함으로 [1]에 제시된 모델에서의 Auctioneer 의 부하를 막고자 하는 것이다.

경매 모델이 2 개의 구성요소로 이루어질 경우 판매자와 AIS 가 서로 단합을 할 경우에 모든 입찰정보를 알 수 있는데 이러한 문제는 메시지의 내용 변경을 통해서 해결을 하였다.

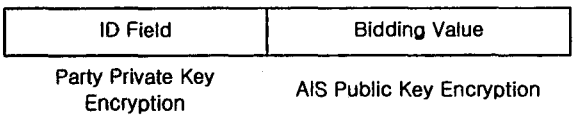

그림 2. 메시지 형식

그림 2 에서와 같이 각각의 파티들은 메시지를 2 개의 키로 암호화하는데 우선 자신의 ID 번호를 자신만이 알고 있는 Key 로서 암호화한다. 이는 다른 Party 는 물론 AIS 도 알 수가 없다. 다른 하나는 AIS 의 공개키로써 입찰 가격을 암호화하는데 이는 경매의 결과를 알기 위해서 입찰가격을 알아야 하기 때문이다. 이렇게 두 개의 키로 암호화 할 경우 누가 어느 가격에 입찰을 했는지는 AIS 와 판매자가 협력을 해도 알 수가 없다.

제안 모델에서의 Auctioneer 의 역할은 많이 축소를 시키고 단지 Party 들의 입력들을 AIS 에게 P2P 네트워크와 Proxy OT Protocol 를 사용하여서 전달해주는 역할만 한다.

3.3 프로토콜의 동작

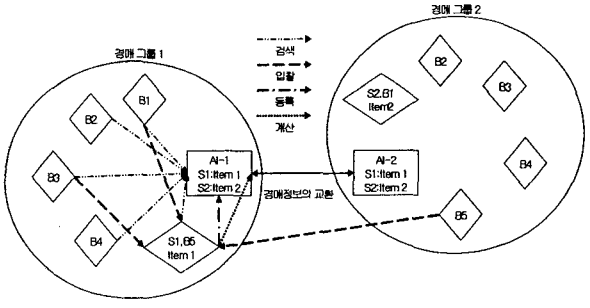

그림 3. 프로토콜의 동작

그림 3 에서는 B5 가 판매자가 되는 경우 하나만 보여 주지만 B1 에서 B4 까지 모두가 판매자가 될 수 있다.

제안된 프로토콜의 동작은 5 단계로 이루어져 있으며 이들 각각의 단계를 살펴 보면 다음과 같다. - 본 논문에서는 AIS 에 각각의 Party 들이 등록하는 과정은 생략한다

3.3.1 상품 등록 단계

Party 중 물건을 경매에 붙이고자 하는 사람이 있을 경우 B5(S1)은 AIS(AI-1)에 상품 정보와 자신의 ID 를 AIS 에 등록한다. 이때 AIS(AI-1)에서는 다른 경매그룹의 AIS(AI-2)에 이를 알려 주고 정보를 보내는 동시에 AI-2 에 정보 갱신 유무를 확인 후에 AIS(AI-1)의 정보를 갱신한다. 이 과정 중에 꼭 필요한 정보는 B5(S1)의 ID 정보, IP, Port Number 정보와 상품 정보 및 경매 정보가 필요하다. IP 와 Port Number 를 알아야 하는 이유는 P2P 네트워크를 이용하기 위해서이다.
또한 AIS 에서는 경매 결과 계산을 Garbled Circuit 구성을 한다.[1]

3.3.2 경매 검색 단계

자신이 구매하고자 하는 상품이 있을 때에는 AIS 서버를 이용하여 상품을 검색한다. 즉 Party(B1~B5)는 AIS(AI-1)서버를 이용하여 상품을 검색한다. AIS(AI-1)에는 연결된 모든 경매 그룹의 경매 내용을 사용하여서 검색을 한다.

3.3.3 입찰 단계

원하는 상품을 찾았을 경우 해당 상품의 판매자 정보를 알아 내고 그곳에 접속을 하여서 입찰 가격을 보내준다. 이때 입찰 정보를 보낼 때에는 전에도 설명했듯이 자신의 ID 는 자신의 비밀키를 이용하여 암호화 하고, 입찰 가격을 AIS 의 공개키를 사용하여서 암호화한 후에 보낸다.

이때 판매자(B5(S1))는 경매 마감 시간이 되었을 경우 입찰자와의 P2P 네트워킹을 끝내고, AIS 와의 OT Protocol 을 준비를 한다.

3.3.4 계산 단계

이 단계에서는 [1]에서 제안된 모델의 Auctioneer 와 Auction Issuer 간의 OT Protocol 를 바탕으로 이루어 지며 계산의 결과는 B5 에 저장이 된다. 이때 경매에서 승자는 판매자, AIS 모두 알 수가 없는 상태이다. 그렇기 때문에 이를 알기 위해서 Party 들의 승인이 필요하다. 이를 위해서 경매 결과 메시지를 작성하게 되는데 메시지 각 필드의 값은 다음과 같이 구성된다. 입찰된 가격과 승자의 암호화된 ID 와 암호화된 ID 를 판매자의 비밀키로 다시 암호화 시킨 ID 로 넣는다. 마지막 승자의 암호화된 ID 를 다시 암호화하는 이유는 인증에 쓰이기 때문이다.

3.3.5 결과 발표 단계

경매 결과 메시지가 완성이 되면 메시지를 공유 폴더에 두어서 입찰에 참여한 모든 Party 들이 결과를 볼 수 있도록 한다. 이때 승자는 자신의 암호화된 아이디를 알고 있기 때문에 승자 자신은 자신이 낙찰되었다는 것을 알 수 있다. 낙찰을 확인한 승자는 자신의 ID 와 판매자의 비밀키로 암호화된 ID 를 자신의 키로 복호화해서 다시 판매자에게 보낸다. 그러면 판매자는 자신의 키를 이용하여 낙찰자가 복호화한 암호화된 ID 를 풀어서 승자의 ID 와 비교 함으로써 결과를 알 수 있다.

경매의 결과가 모두 확인이 되었을 경우 판매자는 낙찰자의 정보를 AIS 에 보내서 경매가 종료되었음을 알려준다. 이때 AIS 에서는 자신이 가지고 있는 정보를 갱신함과 동시에 다른 경매 그룹의 AIS 서버에게도 알려주고 다른 그룹의 AIS 서버의 정보갱신이 확인됨과 동시에 프로토콜이 종료된다.

제안된 프로토콜은 기존의 모델 중 뛰어난 [1]에서 제안한 모델과 비교하여 보면 다음과 같은 장점이 있다. 우선 이전의 모델에서는 경매의 수나 입찰자의 수가 증가하다 보면 Auctioneer 에서 병목 현상이 생기는데 제안 모델에서는 각각의 Party 로 이들 모듈을 분산시킴으로써 보다 효율적으로 네트워크 리소스를 사용할 수 있다. 두번째로는 다른 경매 그룹과 쉽게 연동을 시킬 수 있어서 경매 규모를 쉽게 확장시킬 수 있다. 세번째로는 뛰어난 안전성을 유지할 수 있다. 마지막으로 구성요소를 줄임으로써 모델을 더욱 간편화 할 수 있다.

4. 결론

본 논문에서는 P2P 네트워크 모델 위에서 Party 와 Auction Issuer Server 2 개의 구성요소로 이루어진 모델을 통해서 [1]에서 제안된 모델과 같은 안전성은 유지하는 동시에 다른 경매 그룹과의 자연스런 연결을 통해 경매의 규모의 확장을 쉽게 할 수 있으며 또한 경매 정보에 대한 효율적인 검색을 할 수 있게 하였다. 또한 여러 경매가 동시에 일어날 경우에 생기는 네트워크 부하를 줄일 수 있게 되었다. 앞으로 각각의 경매 그룹들 사이의 Auction Issuer Server 들 사이의 경매 처리에 대한 부하 분배 및 경매 처리 모듈의 분배를 통해서 보다 효율적이고 보다 안전한 모델을 만들 수 있을 것이다.

5. 참고문헌

[1] Moni Naor, Benny Pinkas, and Reuben Sumner. "Privacy Preserving Auctions and Mechanism Design" Proceedings of the 1st ACM conf. on Electronic Commerce, Denver, Colorado, November 1999.

[2] M. K. Franklin and M. K. Reiter, "The Desing and Implementation of a Secure Auction Server", IEEE Tran. on Software Engineering, 22(5), pp. 302-312, 1996

[3] O. Goldreich, M. Micali and A. Wigderson, "How to play any mental game", Proc. 19th ACM Symp. on Theory of Computing, 1987, pp.218-229

[4] M. harkavy, J. D. Tygar and H. Kikuchi, "Electronic Auctions with private bids", 3rd USENIX Workshop on Electronic Commerce, pp. 61-73, 1999

[5] M. Kumar and S. I. Feldman, "Internat Auctions", 3rd USENIX Workshop on Electronic Commerce, 1999

[6] A.C. Yao, "How to Generate and Exchange secrets", Proc. of the 27th IEEE Symp. on Foundations of Computer Science, 1986, pp. 162-167

[7] C. Cachin, "Efficient private bidding and auctions with an oblivious third party", to appear, Proc. 6th ACM Conf. on Computer and Communications Security, 1999

[8] Parameswaran, M., Susarla, A., Whinston, A.B. "P2P networking: an information sharing alternative", Computer , Volume: 34 Issue: 7 , July 2001 Page(s): 31 -38