안전한 전자 봉인입찰 경매 방법

김동호[0] 전중남 이건명
충북대학교 컴퓨터과학과, 첨단정보기술 연구센터
initself@aicore.chungbuk.ac.kr

Secure Electronic Sealed Bid Auction Method

Dong-Ho Kim Jung-Nam Jeon Keon-Myung Lee
Dept. of Computer Science, Chungbuk National University and AITrc

요 약

인터넷 사용이 급증하고 전자상거래의 발달과 동시에 전자 경매들이 인터넷 상에서 활발히 이루어 지고 있다. 그 중에서 아웃크라이(Out-Cry) 스타일의 경매들은 봉인입찰(Sealed Bid) 경매에 비해서 많이 행해지고 있다. 봉인입찰 경매들은 인터넷 상에서 수행되었을 때에 보안상의 문제점을 가지고 있다. 가장 치명적인 단점은 경매자(Auctioneer)에 대한 신뢰문제로 입찰자(Bidder)들은 경매자가 자신의 입찰정보를 알아내어 다른 입찰자를 도와주거나 더 많은 이익을 얻기 위해서 입찰 정보를 조작하지 않을까 걱정한다. 이런 문제를 해결하기 위해서 몇몇의 보안 프로토콜이 등장하였는데, 그것들은 신뢰할 수 있는 제삼자(Trusted Third Party)와 다수의 입찰 매니져(Bidding Manager)를 둠으로써 해결하고 있다. 첫 번째 방법에서는 경매자에 대한 절대적 신뢰를 전제로 하고 두 번째 방법에서는 경매자와는 별도의 다른 기관들이 요구되어 진다. 이 논문에서는 다른 기관 없이 인터넷 상에서 안전하게 행해질 수 있는 봉인입찰 경매 방법을 제시한다. 이 프로토콜은 Vickrey 경매와 FPSB 경매에서 모두 사용될 수 있고 다른 신뢰할 수 있는 제삼자의 도움 없이 입찰자와 경매자의 통신만으로 가능하기 때문에 비용이 절감된다.

1. 서 론

인터넷의 폭넓은 사용과 더불어 가상공간에서 많은 서비스들이 행해지고 있다. 그 중 가장 급속히 발전되는 분야가 생산자와 소비자가 상품을 팔고 사는 전자상거래이다. 계속해서 전자상거래 관련 새로운 기술이 등장하기는 하지만 아직도 해결해야 할 문제들이 산재해 있다. 그 중 보안문제는 전자상거래에서 가장 중요한 문제로 인식되고 있다. 이 논문에서는 인터넷 상에서 활발히 행해지는 전자상거래를 위한 경매의 보안에 관심을 둔다. 현재 많은 경매 사이트들이 생겨났고 서비스되고 있다.

많은 경매 서비스들은 기업대 기업(B-to-B)간, 기업대 고객(B-to-C)간 경매에서 영국식경매[3]와 같은 오픈크라이 스타일의 경매 서비스만을 제공하고 있다. 그 이유는 인터넷 상의 봉인입찰 경매에서는 경매자의 신뢰 문제가 등장되기 때문이다. 이것을 해결하기 위해서 일련의 보안 프로토콜은 경매자의 신뢰를 보장하는 프로토콜을 제시하였다[1][2]. 이런 방법들은 신뢰할 수 있는 제삼자와 다수의 입찰 매니져들이 비밀키를 부분적으로 소유함으로써 해결 할 수 있다.

이 논문에서는 위의 방법과는 다른 안전한 봉인입찰 경매 방법을 제시한다. 제시된 방법은 더 이상 다른 제삼자를 요구하지 않으며 따라서 경제적인 방법으로 구현될 수 있다. 이 논문은 다음과 같이 구성되어 있다. 2절에서는 경매 프로토콜들과 관련된 기술들을 알아보고, 3절에서는 봉인입찰 경매를 위한 제안된 프로토콜을 설명하고 4절에서는 제안된 프로토콜을 따르는 경매 시스템을 다중 에이전트 시스템으로 설계 후 5절에서 결론을 맺는다.

본 연구는 첨단 정보기술 연구센터(AITrc)를 통해서 과학재단 지원으로 수행된 것임.

2. 경매 프로토콜과 관련 기술들

2.1 경매 프로토콜

몇몇의 경매 프로토콜이 선보였는데, 그것들은 아웃크라이 스타일의 경매와 봉인입찰 경매로 크게 분류 할 수 있다. 아웃크라이 경매에서는 경매 가격이 공개되고 모든 입찰자들이 경매의 진행 상황을 알 수 있다. 이와는 반대로 봉인입찰 경매에서는 입찰자들의 입찰 정보는 경매 종료 시까지 비공개로 처리된다.

전형적인 아웃크라이 스타일의 경매에는 영국식 경매(English Auction)와 네덜란드식 경매(Dutch Auction)가 있다. 영국식 경매에서는 입찰자들이 입찰 가격을 올려감으로써, 더 이상 높은 가격을 제시하지 않으면 경매는 끝나게 되고 가장 높은 가격을 제시한 입찰자가 그 가격으로 낙찰되는 방법이다. 네덜란드식 경매에서는 경매자가 입찰자가 응찰할 때까지 계속적으로 가격을 낮추어 가고 그 가격에서 낙찰 받게 되는 방법이다. 이 방법은 실시간으로 처리되는 물품에 대하여 효과적으로 처리할 수 있는 경매 방법이다. 인터넷 상에서 행해지는 대부분의 경매 사이트들은 간결함과 대중성 때문에 대부분 영국식 경매를 제공하고 네덜란드식 경매는 일부의 사이트들이 제공하고 있다. 그 이유는 네덜란드식 경매가 인터넷에서 수행될 때 실시간으로 처리되어야 하는 특성으로 인터넷 접속 품질과 연관성이 있기 때문이다.

한편, 봉인입찰 경매에서는 대표적으로 FPSB(First

Price Sealed Bid) 경매와 Vickrey(Second Price Sealed Bid) 경매가 있다. FPSB 경매에서는 각 입찰자들이 서로 비공개로 가격을 제시하고 그 중 가장 높을 가격을 제시한 입찰자에게 낙찰된다. Vickrey 경매에서는 각 입찰자들이 비공개로 가격을 제시하고 가장 높은 가격을 제시한 입찰자가 두 번째 높은 가격을 제시한 입찰자의 가격으로 낙찰되는 방법이다.

오프라인(Off-Line) 봉인입찰 경매에서는 입찰자는 입찰가격을 적어 봉인하고 도장을 찍어 경매자에게 전달한다. 따라서 입찰자는 나중에 자신의 봉인을 확인, 공개여부를 검사할 수 있으므로 입찰 종료까지의 보안을 확신할 수 있다. 하지만 봉인입찰이 인터넷상에서 수행되어지면 전자적으로 처리되기 때문에 어려운 문제가 발생된다. 만일 경매자가 입찰자의 가격을 알게되면 다른 입찰자에게 노출하거나 이익을 더 많이 내기 위해 입찰가격을 조작할 수 있는 보안상 문제점이 발생된다.

2.2 관련연구

인터넷 상에서 봉인입찰 경매를 지원하기 위해 몇몇의 프로토콜들이 개발되었다[1][2]. 그것들은 다음과 같이 두 가지로 분류될 수 있다. 하나는 믿을 수 있는 제삼자로 하여금 경매를 수행하도록 하는 방법이고 다른 하나는 신뢰하지 못하는 경매자를 미리 가정하고 경매를 실행하는 방법이다.

첫 번째 접근방법에서 경매자는 신뢰할 수 있는 서트파티로 인식되고 입찰자는 자신의 입찰정보를 경매자의 공개키로 암호화하여 경매자와 Contract Signing 프로토콜과 Certified Mail[5]을 사용하여 입찰정보를 전송한다. Contract Signing 프로토콜과 Certified Mail을 사용하면 입찰자는 자신의 입찰정보가 입찰 마감시간 안에 적절히 전송되었다는 것을 증명 받을 수 있다. 또한 입찰자는 자신의 입찰 정보가 경매 종료 시까지 노출되지 않는다고 기대하게 된다. 이런 방법의 경매에서 입찰자는 경매자를 무조건적으로 신뢰하게 되는데 이런 가정하에서는 중요한 봉인입찰 경매는 이루어지기 곤란하다.

다른 하나는 경매자의 신뢰를 확신하지 못하다고 가정하는 프로토콜로 경매자와 더불어 다수의 입찰 매니져를 두는 방법이다[1]. 입찰 매니져는 경매자가 경매자 종료될 때까지 입찰자들의 입찰정보를 알지 못하도록 보장한다. 입찰자들은 자신의 비밀키로 입찰정보를 암호화한다. 그리고 키정보를 각각의 입찰 매니져에게 나누어 전달한다[8]. 입찰이 종료되면 입찰 매니져는 자신이 소유하고 있는 부분키를 경매자에게 전달, 경매자는 그 비밀키를 이용해 입찰 정보를 알아낸다. 이런 프로토콜들은 경매자의 부적절한 행동을 방해해 경매가 공정하게 행해질 수 있도록 도움을 준다. 하지만 이런 프로토콜들은 다수의 입찰 매니져를 요구하게 되고, 시스템 구현 시 부가적인 비용이 따르게 되므로 작은 비즈니스 어플리케이션에는 부적절하게 된다.

3. 안전한 봉인입찰 경매 프로토콜

이 절에서는 경매자와 더불어 다수의 입찰자들 간의 봉인 입찰 경매를 가능하게 하는 방법을 제시한다. 기본 아이디어는 다음과 같다.

입찰자는 자신의 입찰정보와 경매 종료후의 비밀키를 검증할 수 있는 키 정보를 자신의 비밀키로 암호화 하여 경매자에게 전달한다. 경매 종료후 입찰자는 경매자에게 비밀키를 전달하게 되고, 경매자는 키를 검증 후 입찰자들의 입찰정보를 해독해 낙찰자를 결정한다. 제안된 방법은 FPSB 경매와 Vickrey 경매 모두에서 사용될 수 있다.

3.1 안전한 봉인입찰 경매 프로토콜

제안된 전자 경매 시스템은 경매자 서버와 다수의 입찰자 클라이언트들로 구성된다. 경매자 서버는 경매를 열고 경매 시작을 알리며 입찰을 받아들이고 경매를 종료한다. 입찰자 클라이언트들은 사용자의 입찰정보를 받아들여 경매자 서버와 정해진 프로토콜로 경매에 참여한다.

[그림 1]은 경매자 서버와 입찰 클라이언트간의 제안된 경매 프로토콜의 도식화를 나타낸다. 경매자를 신뢰할 수 없을 경우에는 다음과 같은 보안문제가 발생한다. 경매자는 다른 입찰자를 도와주기 위해서 현재 입찰정보를 노출시키거나 Vickrey 경매에는 많은 이익을 내기위해 정보를 조작한다. 이런 문제점은 경매자에게 경매 종료 시까지 입찰정보를 노출시키지 않음으로써 해결할 수 있다.

다른 문제점으로는 입찰자의 신뢰성 문제를 생각해 볼 수 있다. 이런 경우는 입찰가격을 제출한 입찰자들이 자신의 생각을 바꾸는 경우로서, 자신의 입찰정보를 무효화시키기 위해서 잘못된 비밀키를 전달할 수 있다. 이런 경우를 방지하기 위해서 3.2절에서 제시한 비밀키 보장기술을 사용한다.

또한, 경매과정이 전자적으로 처리되기 때문에 경매자가 제출된 입찰정보를 가지고 낙찰자를 선택할 때 문제가 발생할 수 있다. 이것을 해결하기 위해 감독기술이 요구되게 되고 제안된 프로토콜에서는 경우에 따라서 입찰이 끝났을 때 경매자는 입찰자에게 모든 입찰정보를 보내주고 입찰자들에게 자신의 입찰정보와 또한 낙찰 정보를 알 수 있는 방법을 제시한다.

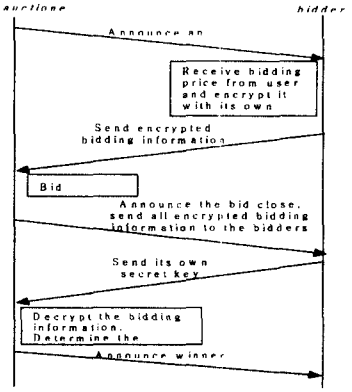

그림 1. 제안한 경매 프로토콜의 도식도

FPSB 경매에서는 낙찰자의 비밀키를 모든 입찰자들에게 부여, 낙찰여부를 검증할 수 있게 하고 Vickrey 경매에서는 낙찰자에게 모든 비밀키를 전달하게 하여 낙찰여부를 검증시키는 기능도 필요로 한다.

3.2 비밀키 관리

입찰자들이 자신의 입찰정보를 무효화시키기 위해서 잘못된 비밀키를 전송하는 것을 막기 위해서는 Blind Signature를 기반으로 한 방법이 요구된다. Blind Signature의 특성[8] 때문에 경매자은 그가 서명한 내용에 대해서는 모르게 된다.

입찰자가 처음 경매에 참여했을 때 입찰자는 자신의 비밀키에 전자서명을 Blind Signature를 이용, 경매자에게서 받고 입찰 시 입찰가격과 비밀키에 대한 전자서명을 자신의 비밀키로 암호화하여 경매자에게 전달한다. 입찰 종료 후 입찰자는 비밀키와 전자서명을 보내게 되고 경매자는 미리 전달된 입찰정보를 비밀키로 해독 후, 입찰정보에 포함되어 있는 전자서명과 보내온 전자서명을 비교, 비밀키가 타당한지 검증하게 된다.

3.3 메시지전송의 시간제약 문제

제안된 프로토콜에서는 다수의 메시지 전송이 경매자 서버와 입찰 클라이언트들에게서 일어난다.

[그림 1]은 그들의 전송과정을 보여 주는데 몇몇의 메시지들은 경매 종료 시까지 도착해야 되는 시간제약 사항이 발생된다. 입찰 클라이언트들이 경매자 서버에게 입찰정보를 전달하면 경매자 서버는 현재시간과 비교해 종료시간 이전인지 확인하고 Contract Signing 프로토콜을 사용[7], 입찰정보를 교환한다. 입찰 클라이언트가 자신의 비밀키 정보를 보낼 때에도 정해진 마감시간 이전에 제공되어야 하고 그 때에도 전송시간 타당성을 검사하는 기능의 Contract Signing 프로토콜을 사용한다.

제안된 방법에서는 경매자 서버와 입찰 클라이언트 사이에 안전한 통신의 성립을 가정하고 입찰 클라이언트는 경매자 서버에게 항상 대기하고 있어야 한다는 것을 전제로 하고 있다.

4. 안전한 봉인입찰 경매를 위한 다중 에이전트 시스템

제안된 경매방법은 경매 서버와 입찰 클라이언트 사이의 많은 메시지 전송이 요구된다. 또한 경매과정은 경매자와 입찰자의 많은 참여 없이 자동적으로 행해져야 하고 경매 서버와 입찰 클라이언트는 사용자를 대신해 사용자가 제시한 경매가격과 다른 메시지를 처리함으로써 경매에 참여한다. 이런 경매 시스템은 다중 에이전트 시스템으로 구현할 경우 많은 이득이 따른다. 따라서 경매자 서버와 각 입찰 클라이언트를 에이전트로 제각기 구현 할 수 있다.

각 에이전트는 상대방을 찾고 메시지를 교환할 통신 프로토콜과 암호화 기능을 가지고 있어야 한다. 경매과정에서 경매자 서버 에이전트는 입찰정보를 받고, 입찰을 종료하고 비밀키를 받아 낙찰자를 결정하는 등 중요한 역할을 수행한다. 또한 입찰 에이전트는 항상 수행가능한 데몬 프로그램처럼 동작하는데 사용자로부터 입찰가격을 건네 받아 비밀키를 생성하고 경매 서버 에이전트로부터 전자서명을 교부받아서 암호화된 입찰정보를 전달한다. 그리고 경매 서버 에이전트의 경매 종료를 인식하고 비밀키를 전달하고 낙찰여부를 전달받고 이에 대한 검증을 하게 된다.

5. 결론

이 논문은 경매자와 입찰자외의 다른 입찰 매니져 없는 안전한 봉인입찰 경매 프로토콜로 경매자가 비합법적인 행동을 하지 못하게 하는 환경을 제시한다. 대신에 다른 입찰 매니져를 사용하는 경매보다 경매자와 입찰자들 간에 많은 통신을 요구로 한다. 기본 아이디어는 경매자가 경매 종료 시까지 입찰자의 입찰정보를 볼 수 없게 하는 것인데, 이렇게 하기 위해서 입찰자는 자신의 비밀키를 이용해 입찰정보를 암호화 하여 전달 경매자로 하여금 경매 조작을 방지한다. 이런 방법으로 봉인입찰 경매에서 경매자의 신뢰성 문제를 극복한다.

또한 입찰자가 방해할 목적으로 비밀키를 잘 못 보내는 것을 방지하기 위해서 자신의 비밀키에 대한 전자서명을 받아내어 입찰 정보와 함께 제출하게 한다. 이렇게 제출된 정보는 경매자에 의해 검증되고 확인된다. 제안된 프로토콜은 다중 에이전트로 설계되어 경매과정에서 일어나는 입찰자와 경매자의 통신을 책임지게 된다.

6. 참고 문헌

[1] M. K. Franklin, M.K. Reiter, Fair exchange with a semi-trusted third party, *Proc. of the 4th ACM Conf. on Computer and Communication Security*, pp.1-6, 1997.

[2] A. Asokan, V. Shoup, M. Waidner, Asynchronous protocols for optimistic fair exchange, *Proc. of the IEEE Symp. On Research in Security and Privacy*, pp.86-99, 1998.

[3] T. W. Sandholm, Distributed Relation Decision Making, in *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence* (G. Weiss, eds.), The MIT Press, pp.259-298, 1999.

[4] P. Garcia, E. Gimenez, L. Godo, J. A. Rodriguez-Aguilar, Bidding Strategies for Trading Agents in Auction-based Tournaments, in *Agent Mediated Electronic Commerce*(P. Noriega, C. Sierra, eds), pp.151-165, Springer, 1999.

[5] D. Gollmann, *Computer Security*, John Wiley & Sons, 1999.

[6] W. Stallings, *Cryptography and Network Security: Principle and Practice*, Prentice-Hall, 1999.

[7] C. P. Pfleeger, *Security in Computing*, Prentice-Hall, 1997.

[8] T. Okamoto, H. Yamamoto, *Modern Cryptography*, Industry Books, 1997