다항함수를 이용한 효율적인 경매 모델

이연수°*, 오세영**, 공은배*
*충남대학교 컴퓨터공학과 **충남대학교 수학과
to2510@ce.cnu.ac.kr°, soh@cnu.ac.kr, keb@ce.cnu.ac.kr

A Polynomial Auction Protocol : PAP

Yeonsu Yi°, SeYoung Oh, and EunBae Kong
Dept. of {*Computer Engineering, **Mathematics}, ChungNam National University

요 약

경매 프로토콜의 우수성은 보안성, 효율성, 안정성의 측면에 있다. 기존에 제안된 경매 프로토콜은 보안을 강화함으로 인해 많은 계산량과 메시지 전송이 요구되어 높은 트래픽을 발생한다. 또한 경매의 규모가 커짐에 따라 Auctioneer의 부담이 가중 된다. 본 논문에서는 다항함수의 특성과 개인 정보 분할을 통해 기존의 보안성을 유지하면서도 효율성을 높인 경매 프로토콜 PAP를 제안하고자 한다. 효율성을 높이기 위해 곱연산을 피하고 xor연산을 이용하여 계산량을 줄이고, 안전성을 높이기 위해 다항함수(Polynomial)의 기본 성질을 이용해서 Bidder들의 정보를 분할한다. 제안한 경매 프로토콜은 계산량을 줄이면서도 Bidder들의 정보는 보호 된다.

1. 서 론

인터넷 시대가 시작되면서 오프라인상에서의 경제 활동이 인터넷상에서도 많은 사람들에게 관심을 끌고 있다. 현재 전자상거래는 판매자가 가격을 결정하고 제시된 가격으로 구매자가 구매의사를 결정하는 것에서 판매자가 거래에 직접 참여하여 구매자와 서로 가격을 흥정하는 거래로 옮겨지고 있다. 그 중 급성장하는 부분 중의 하나가 인터넷 경매이다.

인터넷 경매란 인터넷상에서 경쟁을 통해 원하는 물건을 구매하는 인터넷상에서의 경매를 의미한다. 시간을 절약하고 물품을 원하는 가격에 구매할 수 있는 장점 때문에 인터넷 경매에 관심이 높아지고 있다. 하지만 인터넷상에서 경매가 이뤄지다 보니 오프라인 상에서 필요하지 않은, 추가적인 보완점이 요구된다. 우선 인터넷상의 거래이므로 운영 서버는 안정적인 시스템을 갖춰야 하며 소비자가 믿고 신뢰할 수 있게 사이트를 운영해야 한다.

기존의 많은 경매 프로토콜은 불안전한 채널과 정직한 호스트를 가정하여 설계되었다. 하지만 자신의 통제 밖에서 낙찰자를 선정하는 것은 신뢰하기 어려운 문제이다. 또한 보안을 강화하다 보니 프로토콜의 많은 계산으로 효율성이 떨어지는 문제가 발생하게 된다. 따라서 실제상황과 같이 개인 정보에 대한 보안이 확실히 보장되고 한정된 자원으로 사람들이 신뢰할 수 있는 프로토콜을 구현하는 것은 인터넷 경매 활성화를 위한 큰 관심사이다.

본 연구에서는 위에서 언급한 문제점들을 보완하면서도 효율적인 측면을 고려한 모델을 제안한다. 즉, 불안전한 채널과 부정직한 호스트의 현실에서 정보 유출 없이 공통의 목표를 안전하게 이루어내는 다자계산 방법과 경매 규모가 커짐에 따라 네트워크를 효율적으로 이용할 수 있는 모델을 제안하고자 한다.

2. 관련 연구와 모델 방법

경매 프로토콜에서 중요한 요구 조건 중 하나는 Bidder들의 개인 정보를 보호하면서 결과를 도출하는 것이다. 즉, 경매가 종료되더라도 경매 참가자 서로가 정보를 유추할 수 없어야 한다. 또한 경매 진행자도 개인 정보를 유출할 가능성이 있기 때문에 신뢰할 수 없다고 가정해야 한다. 이를 위해 Moni Naor가 제안한 프로토콜[2]에서는 신뢰할 수 있는 제3자를 두어 경매 진행자의 역할을 Auctioneer와 Auction Issuer로 분할하는 방식을 가지고 있다. 그러나 이 프로토콜은 몇 가지 보완해야 할 문제점이 있다. 우선 Auctioneer와 Issuer간의 서킷 전송량이 많아 실제 경매에 적용하기에 문제가 있고, 또한 이로 인해 프로토콜에 심각한 오버헤드를 초래할 수도 있다. 그리고 프로토콜 자체가 신뢰할 수 있는 제3자를 두어야 하는 문제점이 있다. 제3자(Auction Issuer)가 입찰가의 임의의 비트를 수정하는 경우에 Auction Issuer의 부정을 검출하기란 어려운 문제이다. [3]에서는 Naor가 제안한 프로토콜을 비트 단위로 암호화하는 GM암호화 기법을 사용하여 계산량을 상당히 감소하여 효율성을 높였다. 제3자를 신뢰하지 않아도 되는 장점이 있지만 Naor가 제안한 프로토콜과 마찬가지로 Auctioneer와 Auction Issuer의 결탁으로 쉽게 보안의 허점이 생길 수 있다.

경매 프로토콜에 있어서 낙찰자와 낙찰가를 결정하기 위해서는 경매 참여자의 정보가 필요하다. 따라서 경매 참가자는 자신의 정보를 공개해야 하며 이로 인해 다른 참가자들과 운영자들의 결탁으로 정보가 노출되는 것을 완벽히 막는 것은 불가능하다. 결국 자신 이외의 다른 사람이 내 정보를 알아내기 어렵게 만드는 것이 관건이다. 우선 다른 참가자들이 쉽게 알아볼 수 없게 암호화하는 것은 당연하다. 하지만 복잡한 암호화는 프로토콜의 수행에 많은 계산량을 초래한다. 또 정보를 공개해야하므로 암호화에 의존한 보안은 한계가 있다. 따라서 제안한 프로토콜에서는 개인 정보를 n개의 정보로 나누어 다른 Bidder들에게 분산하는 방법을 택하였다. n명의 Bidder들 사이에 비밀을 분산한다면 $(n-1)$명이 공모하지 않는 한 특정인의 개인정보를 알아내기란 어렵다.

기존 인터넷 경매 진행에서 낙찰자와 낙찰가를 알아내는 계산이 Auctioneer에게 집중되는 현상이 있다. 물건을 판매하고자하는 사람이 Auctioneer 역할을 하면 집중되는 부담을 줄일 수 있다. 여기에 계산량을 Bidder들이 나눠서 진행함으로써 효율성을 향상시키는 방법[1]을 제안 프로토콜 PAP에서 적용하였다.

본 논문의 구성은 다음과 같다. 먼저 3장에서는 제안 경매 프로토콜 PAP에 사용되는 기본적인 구성 요소들에 대해 기술하고 4장에서 새로운 경매 프로토콜 PAP를 제안한다. 다음으로 5장에서 제안 프로토콜 PAP를 분석하고 마지막으로 6장에서는 결론을 맺는다.

3. 모델 구성 요소

3.1 Peer to Peer Networking(P2P)

P2P 네트워크 모델은 이미 많은 곳에서 활용화되고 있다. P2P란 컴퓨터들 간의 직접적인 교환을 통한 컴퓨터 리소스의 공유를 말한다. 현재 나와 있는 P2P 모델에는 크게 세 가지 종류가 있다. 중앙 서버에 접속하여 리소스의 위치정보를 얻는 브로커 중재형, 개개인의 컴퓨터를 검색해서 리소스의 정보를 얻는 순수 P2P, 컴퓨터의 하드웨어 자원을 공유하는 Cycle Sharing(CPU Cycle Sharing)이다. 이중 제안된 경매 모델에 사용된 방식은 브로커 중재형 방식이다.

경매의 규모(동시에 진행 중인 경매의 수, 또는 경매 참여자수)가 커짐에 따라 경매에 대한 정보(물품검색, 참가자의 키값, 참가자의 위치정보 등)도 많아지고 그것을 검색하고 관리, 유지하는 것 또한 커다란 문제이다. 이것을 해결하기 위해 P2P Networking을 적용시킨다. 우선 크게 3부분 즉, 물품공개서버(webserver 이하 WS), 물품판매희망자(Auctioneer), 물품구매희망자(Bidder)로 나눈다. WS는 Auctioneer가 판매하길 희망하는 물품을 공지하고 Auctioneer와 Bidder들의 신분을 확인하는 역할을 한다. Auctioneer는 물품에 대한 정보와 경매 참가자들의 정보를 제공하는 브로커 역할을 한다. Bidder들은 원하는 물품을 WS에서 검색하고 Auctioneer에게 경매 참여의사를 밝히고 실질적인 경매 진행 계산을 수행한다. Bidder는 브로커를 통해 다른 Bidder들의 위치정보를 얻고 직접 다른 Bidder들에게 필요한 정보를 얻는다.

3.2 다항함수

n개의 서로 다른 양의 정수해 b_k, $k=1,\cdots,n$를 갖고 최고차항의 계수가 1인 다항함수는 $f(x)=\prod_{k=1}^{n}(x-b_k)$ 형태를 갖는다. 적용되는 경매 프로토콜에서는 $i<j$일 때 $b_i<b_j$ 임을 가정한다. 모든 b_i가 다항함수 $f(x)$의 해이므로 $b_i\neq b_j$ (단, $i\neq j$)이면 $b_i-1<k<b_i<h<b_i+1$인 k, h에 대해 $f(k)\cdot f(h)<0$이다. 즉, $f(x)$는 b_i좌우에서 부호가 바뀌게 된다. 역으로 생각하면 중간값 정리[1]에 의해 폐구간 $[k, h]$에서 연속이고 $f(k)\cdot f(h)<0$ 이면 $f(p)=0$인 p가 $[k, h]$에 존재한다. $f(x)$는 정수의 해 만을 가지므로 p가 정수가 되며 구간 $[k, h]$에 정수는 유일하므로 $p=b_i$임을 알 수 있다.

4. 다항함수를 이용한 경매 프로토콜 (Polynomial Auction Protocol : PAP)

4.1 적용 방법

3장에서 설명한 함수 f에 경매를 적용하면 입찰가는 자연수에 해당하는 수로 함수의 해, b_i가 된다. 경매에 참가한 Bidder i는 임의의 x에 대해서 $(x-b_i)$를 계산할 수 있다. 좌표평면위에서 Bidder들의 입찰가를 해로 갖는 최고차항의 계수가 1인 다항함수를 생각하자. 이 함수의 해들 중 값 $b_i=\max\{b_1, b_2, b_3, \cdots, b_n\}$보다 큰 h에 대해서는 $f(h)>0$이 된다. 그리고 b_i와 $b_j=\max\{b_1, b_2, \cdots, b_{i-1}, b_{i+1}, \cdots, b_n\}$값 사이의 k에 대해서 $f(k)<0$이다. 여기서 각 Bidder들은 bidding 가능한 연속되는 두 정수 사이의 값을 자신이 입찰한 값과 순차적으로 대소를 비교하여 양과 음의 값을 얻어 낸다. 예를 들어 Bidder k가 b_k값을 bidding하면 *max bidding value*(이하 *mbv*)에서 bidding한 부분까지 bit 1을 갖고 나머지 bit는 0을 갖는 h-bit의 값 즉, $111\cdots10\cdots0$을 얻을 것이다. h의 크기는 bidding 범위를 나타낸다.

4.2 경매 프로토콜 PAP

경매 프로토콜 즉, Polynomial Auction Protocol(PAP)은 총 5 단계 즉, 등록, 검색, 입찰, 계산, 낙찰단계로 이루어진다.

4.2.1. [**등록단계**]

1. 물건을 경매에 붙이고자 하는 사람(Auctioneer)은 자신의 *ID*를 쇼핑몰(WS)에 등록한다.
2. Auctioneer는 경매 물품과 *mbv*, 경매단위 *d*, 경매 진행 시간 등을 WS에 등록하고 서명을 위한 알고리즘 $sign_{Auctioneer}$에 대한 생성키, 검증키 ($s\_sk_{Auctioneer}$, $s\_pk_{Auctioneer}$)와 암호화 알고리즘 E에 대한 비밀키, 공개키($sk_{Auctioneer}$, $pk_{Auctioneer}$), 해쉬함수 H를 생성한다.
3. WS는 경매 정보를 공표한다.

4.2.2. [**검색단계**]

4. 구매자들은 WS에서 자신이 원하는 물품을 검색하고 자신의 *ID*와 위치 정보를 Auctioneer에게 등록함으로써 경매 참여 의사를 밝힌다.
5. 경매 참여 의사를 밝힌 Bidder i는 서명을 위한 알고리즘 $sign_i$에 대한 생성키, 검증키(s_sk_i, s_pk_i)와 암호화 알고리즘 E에 대한 비밀키, 공개키(sk_i, pk_i)를 생성한다.

4.2.3. [**입찰단계**]

6. Bidder i는 bidding 값 $b_i\leq mbv$을 선정 후 C_i값을 아래와 같이 계산한다.

$$h=\frac{mbv}{d};$$

for $k=1,\cdots,h$ {

$$c_k=\begin{cases}1 & \text{if } mbv-k\cdot d+0.5>b_i\\ 0 & else\end{cases}$$

}

$$C_i=c_1||c_2||c_3||\cdots||c_h;$$

|| : bit를 연결한 2진수를 의미한다.

7. Bidder i는 random 수 r_i를 생성[2]하고 Auctioneer로부터 $pk_{Auctioneer}$키를 얻는다.
8. Bidder i는 $H(b_i\oplus r_i)$, $H(r_i)$ $sign_i(s\_sk_i, H(b_i\oplus r_i))$, $sign_i(s_sk_i, H(r_i))$값을 Auctioneer에게 전달한다.
9. Auctioneer는 Bidder i의 $H(b_i\oplus r_i)$, $H(r_i)$정보를 서명 검증하고 4단계에서 받은 *ID*에 매칭한다.

4.2.4. [**계산단계**]

10. Bidder i는 h-bit 크기의 $n-1$개의 random 수 $\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{ii-1}, \alpha_{ii+1}, \cdots, \alpha_{in}$값을 결정한 후 아래 알고리즘을 통해 α_{ii}값을 결정한다.

1) 중간값정리: 폐구간 $[a, b]$에서 연속인 함수 f에 대하여 $f(a)$와 $f(b)$사이의 값을 k라고하면 $f(x)=k$를 만족하는 x가 개구간 (a, b)사이에 적어도 한 개 존재한다.

2) 난수 값은 충분히 큰 수이므로 같을 경우는 없다고 봐도 무방하다.

$a_{ii} = a_{i1}$;
for $j = 2, \cdots, n$ {
  if$(j \neq i)$ $a_{ii} = \neg(a_{ii} \oplus a_{ij})$;
}
$a_{ii} = C_i \oplus \neg a_{ii}$;

11. Bidder i는 *Auctioneer*를 통해 Bidder j의 위치 정보를 얻고 Bidder j에게 pk_j를 얻는다.(p2p-브로커 중재형)
12. Bidder i는 $E_{pk_j}(sign_i(s_sk_i, a_{ij}), a_{ij})$값을 Bidder j에게 전달.(단, $i \neq j$)
13. Bidder i는 Bidder j에게 받은 값을 자신의 sk_i를 통해 복호화하여 a_{ji}값을 얻고 Bidder j의 검증키 s_pk_j를 통해 검증한다.
14. Bidder i는 a_{ii}와 13단계에서 얻은 a_{ji}들 즉, $a_{1i}, a_{2i}, \cdots, a_{i-1i}, a_{i+1i}, \cdots, a_{ni}$값들을 아래와 같이 연산해서 β_i값을 계산한다.

$\beta_i = a_{1i}$;
for $j = 2, \cdots, n$ {
  $\beta_i = \neg(\beta_i \oplus a_{ji})$;
}

15. Bidder i는 계산된 $E_{pk_{Auctioneer}}(\beta_i)$값을 Auctioneer에게 전송한다.
16. Auctioneer는 전송되어온 β_i값들을 이용하여 β를 아래와 같이 연산한다.(β값의 bit의 변화는 다항함수의 해 즉, bidding값을 표현한다.)

$\beta = \beta_1$;
for $j = 2, \cdots, n$ {
  $\beta = \neg(\beta \oplus \beta_j)$;
}

17. Auctioneer는 16단계에서 얻은 β를 이용하여 낙찰 예정가 즉, β가 나타내는 값 중 두 번째로 큰 값 η를 공표한다.

4.2.5. [**낙찰단계**]

18. 공표된 값 보다 큰 값을 bidding 한 입찰자(candidate)는 $E_{pk_{Auctioneer}}(r_{candidate})$를 Auctioneer에게 전송한다.
19. Auctioneer는 β를 통해 얻은 가장 큰 값 이상의 값들과 전송되어온 $r_{candidate}$값을 연산하여 낙찰가와 낙찰자를 찾는다.

$h = \frac{mbv - \eta}{d}$;
for $i = 0, \cdots, N_{candidate}$ {
  for $k = 0, \cdots, h$ {
    $can = H((\eta + k*d) \oplus r_i)$;
    if$(ID == can)$ (ID, k)를 저장
  }
}
저장된값중 $ID_{k_{max}}$를찾음

20. Auctioneer는 낙찰가를 공표하고 낙찰확인 메시지를 *winner*에게 전송한다.

5. PAP 분석

bidding 값은 정수이므로 정수 부분에서 양응을 판단할 수 없는 0이 나타날 수 있으므로 실수 부분에서 부호를 판단하기 위해 입찰단계 6에서 0.5의 값을 택하였다. 계산단계 16에서 Auctioneer는 β값의 bit가 변한 곳을 통해 낙찰가를 알 수 있다. 물론 Auctioneer는 누가 어떤 값을 bidding했는지는 알 수 없다. 하지만 선택한 낙찰가보다 큰 값에서 중복 bidding의 경우가 있었다면 β값만을 통해 낙찰가를 알아낼 수 없다. 따라서 추가적으로 택한 낙찰가보다 더 큰 값의 bidding 여부를 판단해야 한다. 18단계에서 후보자들의 난수 값을 얻어 19단계를 통해 biding값의 중복여부를 확인하고 낙찰자와 낙찰가를 결정한다.

계산단계 17에서 η를 두 번째 큰 값을 선택한 것은 Vickrey Auction[3]을 수행하기 위함이다. 하지만 η를 가장 큰 값으로 택하게 되면 English Auction[4]을 수행할 수 있다.

기존에 경매 프로토콜에서는 경매규모가 커짐에 따라 Auctioneer가 수행해야 하는 계산량이 증가하고 경매에 참가자의 키 관리가 어려워진다. 하지만 제안 경매 프로토콜 PAP는 경매규모가 커지더라도 Bidder들이 직접 분산하여 계산을 하고 P2P 네트워킹 기법을 적용하여 Auctioneer가 직접 키 관리를 하지 않고 P2P의 브로커 역할만 하여 Bidder가 Bidder에게 직접 키를 전송받게 된다. 따라서 기존 경매 프로토콜보다 Auctioneer의 역할 부담이 크게 감소되므로 보다 효율적인 프로토콜이 된다.

6. 결론

본 논문에서는 다항함수의 성질과 정보를 분할하는 방법을 이용하여 Auctioneer와 Bidder들 사이에 효율적이고 안전한 경매 프로토콜 PAP를 제안하였다. PAP에서는 참가한 Bidder들 사이에서 자신을 제외한 모든 참가자가 공모하지 않는 한 어떤 개체들도 다른 특정 개체들의 정보를 얻거나 유추할 수 없으며, 경매의 결과는 정확하다는 것이 보장된다. 곱연산과 같은 계산량이 큰 연산은 지양하고 xor연산을 사용함으로써 실행 속도를 증가시켰다. 그리고 P2P 네트워킹을 적용하여 Auctioneer가 참가한 Bidder들의 정보를 가지고 있지 않아도 되므로 Auctioneer의 역할을 축소시켜 누구라도 손쉽게 Auctioneer의 역할을 수행 가능하게 하여 각 물품에 대한 경매를 판매자가 직접 진행하도록 하였다. 향후 중복값에 대해 더 효율적으로 개선하고자 한다.

7. 참 고 문 헌

[1] Felix Brandt, "Secure and Private Auctions without Auctioneers" 2002.

[2] 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.

[3] 신상욱, 류희수. "효율적인 sealed-bid 경매 프로토콜", 정보보호학회 논문지 제12편 제 6호, December 2002.

3) 가장 높은 가격을 매긴 사람에게, 두 번째 높은 가격으로 낙찰하는 방식
4) 가장 높은 가격을 매긴 사람이 제시한 가격에 낙찰하는 방식