

# 一种保护标价的多属性反向拍卖模型

纪美敬<sup>1,2</sup>, 罗永龙<sup>1,2</sup>, 周正珍<sup>1,2</sup>, 郭良敏<sup>1,2</sup>

(1. 安徽师范大学 计算机科学与技术系, 安徽 芜湖 241000;

2. 安徽师范大学 网络与信息安全技术研究中心, 安徽 芜湖 241000)

**摘要:**多属性反向拍卖作为一种电子采购方式已被广泛应用于电子商务中。在大多数拍卖模型中, 投标者的标价信息对于拍卖者来说完全公开, 在拍卖者和个别投标者共谋情况下, 会造成投标者之间的地位不平等, 给其他投标者造成经济损失。文中在逼近理想解评标方法和安全多方计算基础上, 提出一种保护标价的多属性反向拍卖模型, 该模型采用了安全逼近理想解协议, 实现标价保密和投标者地位公平, 抵御拍卖者与个别投标者的共谋。

**关键词:**拍卖; 安全逼近理想解协议; 保密

**中图分类号:** TP309

**文献标识码:** A

**文章编号:** 1673-629X(2012)06-0139-04

## A Multi-attribute Reverse Auction Model of Bid Price Protected

Ji Mei-jing<sup>1,2</sup>, Luo Yong-long<sup>1,2</sup>, Zhou Zheng-zhen<sup>1,2</sup>, Guo Liang-min<sup>1,2</sup>

(1. Department of Computer Science and Technology, Anhui Normal University, Wuhu 241000, China;

2. Engineering Technology Research Center of Network and Information Security,  
Anhui Normal University, Wuhu 241000, China)

**Abstract:** Reverse auction is widely used in electronic-commerce as an electronic-procurement method. However in the most auction models, the bid information of bidders is completely open to the auctioneer. It will result in inequalities between bidders and cause their losses in the case of complicity between the auctioneer and some bidders. Based on technique for order preference by similarity to ideal solution and secure multi-party computation, the bid price protected multi-attribute reverse auction model is presented. It makes use of a secure technique for order preference by similarity to ideal solution. This model realizes the security of bid-prices and the fairness of bidders, and withstands the complicity between auctioneer and bidder.

**Key words:** auction; STOPSIS; security

## 0 引言

在通常意义的拍卖中, 买卖双方仅根据价格确定物品的分配, 而在实际交易时, 往往会考虑物品更多的属性, 这种买卖双方价格在价格以外其他属性上进行多重谈判的拍卖模式称为多属性拍卖。多属性反向拍卖是买方利用网络广泛招标, 邀请合格的卖方投标, 在竞标过程中, 双方依据采购物品的多个属性共同谈判的拍卖模式。

Thiel<sup>[1]</sup>首次对多属性拍卖进行了详细的讨论, 指出如果卖方的偏好函数已知, 多属性拍卖问题最终将简化为单一属性的拍卖问题。Che<sup>[2]</sup>根据物品的价格

和数量两种属性, 给出了综合两种属性的评分标准, 并基于评分标准给出了一种最高叫价暗标拍卖模型和一种第二高叫价暗标拍卖模型。Bichler<sup>[3]</sup>对多属性拍卖进行了仿真实验, 结果表明多属性拍卖的效用优于单属性拍卖。金萍提出了一种暗标叫价多属性反向拍卖方法<sup>[4]</sup>, 实现了 Vickrey 拍卖从单属性到多属性的推广, 该方法继承了 Vickrey 拍卖的不足, 在递增叫价的多属性反向拍卖方法得到弥补<sup>[5]</sup>。Chen<sup>[6]</sup>利用 EWAA 算子和 LHA 算子设计出新的评标方法, 并基于新的评标方法和 Agent 技术给出了互动多属性反向拍卖系统。陈湘<sup>[7]</sup>设计 SVAMA 协议保证了标价的保密性, 但是该协议仅强调某个特殊属性。

在这些多属性拍卖方法中, 买卖双方重点考虑的是收益问题, 考虑标价信息保密性的较少。如果投标者(卖方)的标价信息对于拍卖者(买方)来说是完全公开的, 拍卖者一旦和其中一个投标者共谋, 就会造成投标者之间的地位不平等, 同时也给其他投标者造成

收稿日期: 2011-11-12; 修回日期: 2012-02-17

基金项目: 安徽高校省级自然科学研究重点项目(KJ2010A133); 安徽省高等学校青年人才基金项目(2011SQRL026); 安徽省高校省级科学研究项目(KJ2011Z142)

作者简介: 纪美敬(1986-), 女, 安徽宿州人, 硕士研究生, 研究方向为信息安全、可信计算。

巨大的经济损失。因此,保护标价信息是多属性反向拍卖的重要研究方向。

TOPSIS<sup>[8]</sup>法即逼近理想解的排序方法,是求解多属性决策问题的一个典型方法。其基本思想是:首先,构建问题的理想解和负理想解,然后在众多方案中找到一个方案使其离理想解最近,离负理想解最远。该方法对标价个数、属性个数及属性值的分布无特殊限制,灵活,实用。文中在逼近理想解(TOPSIS)评标方法和安全多方计算已有工作<sup>[9-12]</sup>的基础上,提出了一种保护标价信息的多属性反向拍卖模型。

## 1 保护标价的多属性反向拍卖模型

### 1.1 基本定义和协议

定义1(加权点的欧几里德距离公式)向量  $X = (x_1, x_2, \dots, x_n)$  和  $Y = (y_1, y_2, \dots, y_n)$  表示两个  $n$  维数据,权值向量  $W = (w_1, w_2, \dots, w_n)$ ,  $w_i (i \in [1, n])$  表示第  $i$  个分量的权值,则加权点间的欧几里德距离公式为:

$$d(X, Y) = \sqrt{(w_1 x_1 - w_1 y_1)^2 + \dots + (w_n x_n - w_n y_n)^2} \quad (1)$$

该公式是欧几里德公式的扩展。

定义2(标价保密性)在拍卖过程中,拍卖者根据掌握的信息不能推出投标者的标价。

协议1(点积协议)<sup>[9]</sup> Alice 有一个私有变量  $X = (x_1, x_2, \dots, x_n)$ , Bob 有一个私有变量  $Y = (y_1, y_2, \dots, y_n)$ , Alice 需要得到  $u = X \cdot Y + v = \sum_{i=1}^n x_i y_i + v$ ,  $v$  仅仅被 Bob 知道。

协议2(安全多方排序协议)<sup>[10]</sup> 有  $n$  个参与方,每一方都拥有一个秘密输入,他们希望在不泄露自己秘密输入信息的前提下,得到其输入按一定的顺序在这  $n$  个秘密输入中所处的位置的问题。

### 1.2 模型描述

文中讨论以买方为主的多属性反向拍卖模型,规定通信信道是物理安全的,在半诚实模型下进行。多属性反向拍卖模型用元组  $M = \langle B, S, A, W, \text{STOPSIS} \rangle$  表示,其中:

$B$  表示唯一买方(拍卖者),仅购买一件物品; $S$  表示卖方(投标者)的集合,假设集合中  $n$  个卖方,  $S = \{S_1, S_2, \dots, S_n\}$ ;

$A$  表示属性空间,  $A = A_1 \times A_2 \times \dots \times A_m$ , 拍卖物品包含  $m$  个属性  $a_1, a_2, \dots, a_m$ , 其取值范围分别是  $A_1, A_2, \dots, A_m$ , 为便于描述文中将属性分为两类:定量属性和定性属性;

$W$  是权值向量,  $W = (w_1, w_2, \dots, w_m)$ ,  $w_i (i \in [1, m])$  表示第  $i$  个属性的权值。

文中采用安全逼近理想解协议(STOPSIS 协议)做为评标方法。

该模型可以实现标价保密和投标者地位公平,抵御拍卖者与投标者间的共谋。

## 2 安全逼近理想解协议

### 2.1 协议思想

安全逼近理想解协议(STOPSIS 协议)是在 TOPSIS 评标方法的基础上,利用安全多方排序协议并结合文中提出的加权点的欧几里德距离协议(SEDMAWPP 协议)和安全除法协议(SDP 协议)计算出标价到理想解、负理想解的相对接近度,从而确定中标者,实现标价保密性。流程如图1所示。

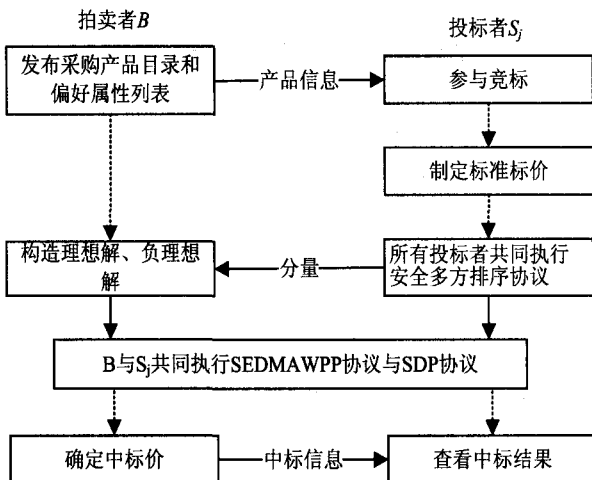


图1 STOPSIS 协议流程图

### 2.2 协议描述

安全逼近理想解协议——STOPSIS 协议分为公布购买信息、本地标价、求出理想解和负理想解、确定中标价4个步骤。

Step1: 公布购买信息。

拍卖者在拍卖网站上发布采购产品目录,公开偏好属性列表  $a = (a_1, a_2, \dots, a_m)$ 。

Step2: 本地标价。

每个投标者  $S_j$  对自己的产品进行标价,得到相应的实际标价向量  $X_j = (x_{1j}, x_{2j}, \dots, x_{mj})$ , 然后利用两极比例法<sup>[8]</sup>对定性属性值进行量化,再利用安全多方排序协议和比例转化法<sup>[8]</sup>对属性值进行归一化处理<sup>[8]</sup>, 最后得到标准标价向量  $X_j = (x_{1j}, x_{2j}, \dots, x_{mj})$ 。

Step3: 求出理想解和负理想解。

For( $i = 1, \dots, m$ )// 对每个属性  $a_i$  都进行如下操作

{  $n$  个投标者使用安全多方排序协议,可以找到  $X_i^+, X_i^-$ 。其中:

$$X_i^+ = \begin{cases} \max(X_{ij}), \text{效益型属性值} \\ \min(X_{ij}), \text{成本型属性值} \end{cases} \quad (2)$$

$$X_i^- = \begin{cases} \max(X_{ij}), \text{成本型属性值} \\ \min(X_{ij}), \text{效益型属性值} \end{cases}$$

并把  $X_i^+$ ,  $X_i^-$  发送给拍卖者。

拍卖者构造理想解  $X^+ = (X_1^+, X_2^+, \dots, X_m^+)$  和负理想解  $X^- = (X_1^-, X_2^-, \dots, X_m^-)$ 。

Step4: 确定中标价。

Protocol SEDMAWPP (Secure Euclid - Distance Measure Among Weighted Points Protocol)

{ 输入: Alice 输入  $X = (x_1, x_2, \dots, x_n)$ ,  $W = (w_1, w_2, \dots, w_n)$ , Bob 输入  $Y = (y_1, y_2, \dots, y_n)$ 。

输出: Alice 得到  $U = \sum_{i=1}^n w_i^2 (x_i - y_i)^2 + v$ , 其中  $v = v_1 + v_2$ , 且  $v_1, v_2$  仅 Bob 知道。

1: Alice 构造向量  $A_1 = (w_1^2, w_2^2, \dots, w_n^2)$ 。

2: Bob 构造向量  $B_1 = (y_1^2, y_2^2, \dots, y_n^2)$ 。

3: Alice 和 Bob 执行点积协议 SPP( $A_1, B_1$ ), Alice 得到  $U_1 = \sum_{i=1}^n w_i^2 y_i^2 + v_1$ 。

4: Bob 构造向量  $B_2 = (-2y_1, -2y_2, \dots, -2y_n)$ 。

5: Alice 构造向量  $A_2 = (w_1^2 x_1, w_2^2 x_2, \dots, w_n^2 x_n)$ 。

6: Alice 和 Bob 执行点积协议 SPP( $A_2, B_2$ ), Alice 得到  $U_2 = -2 \sum_{i=1}^n w_i^2 x_i y_i + v_2$ 。

7: Alice 计算  $U = \sum_{i=1}^n w_i^2 x_i^2 + U_1 + U_2$ 。

{ //end Protocol

图2 加权点的欧几里德距离协议

Step4.1: 拍卖者和投标者  $S_j$  使用图2所示的 SEDMAWPP 协议计算出  $U_j^+$  和  $U_j^-$ , 其中:

$$\begin{cases} U_j^+ = \sum_{i=1}^m (w_i X_{ij} - w_i X_i^+)^2 + v_j^+ \\ U_j^- = \sum_{i=1}^m (w_i X_{ij} - w_i X_i^-)^2 + v_j^- \end{cases} \quad (3)$$

Step4.2: 拍卖者和投标者  $S_j$  使用图3所示的 SDP 协议, 拍卖者计算出  $S_j$  的标价到理想解的距离  $S_j^+$  和负理想解的距离  $S_j^-$  的比  $k$ , 其中,

$$S_j^+ = \sqrt{U_j^+ - v_j^+}, S_j^- = \sqrt{U_j^- - v_j^-}, \frac{S_j^+}{S_j^-} = k \quad (4)$$

Step4.3: 拍卖者利用公式  $C_j = \frac{S_j^-}{S_j^+ + S_j^-} = \frac{1}{1+k}$  计算出标价到理想解、负理想解的相对接近度。

Step4.4: 拍卖者把  $C_j$  按由大到小的顺序排列标价, 排在最前面的标价最优, 即为中标价。

### 3 性能分析

根据评标方法 STOPSIS 协议来分析模型的性能。

#### 3.1 正确性

在 STOPSIS 协议的 Step3 中, 利用安全多方排序协议, 求出理想解  $X^+ = (X_1^+, \dots, X_m^+)$  和负理想解  $X^- = (X_1^-, \dots, X_m^-)$ 。安全多方排序协议的正确性已在文献[10]证明。在 Step4.1 利用 SEDMAWPP 协议得到:

Protocol SDP (Secure Division Protocol)

{ 输入: Alice 输入  $x_1, x_2$ , Bob 输入  $y_1, y_2$ 。输出: Alice 得到  $D = (x_1 - y_1)/(x_2 - y_2)$ 。

1: Bob 随机产生数  $\beta$ 。

2: Alice 和 Bob 执行点积协议 SPP( $x_1, \beta$ ), Alice 得到  $d_1 = \beta x_1 + v_1$ ,  $v_1 = -\beta y_1$  仅 Bob 知道。

3: Alice 和 Bob 执行点积协议 SPP( $x_2, \beta$ ), Alice 得到  $d_2 = \beta x_2 + v_2$ ,  $v_2 = -\beta y_2$  仅 Bob 知道。

4: Alice 计算  $D = d_1/d_2$ 。

{ //end Protocol

图3 安全除法协议

$$\begin{aligned} U_j^+ &= \sum_{i=1}^m (w_i X_i^+)^2 + U_1 + U_2 \\ &= \sum_{i=1}^m ((w_i X_i^+)^2 + (w_i X_{ij})^2 - 2(w_i)^2 X_i^+ X_{ij}) + v_1 + v_2 \\ v_2 &= \sum_{i=1}^m (w_i X_i^+ - w_i X_{ij})^2 + v_j^+, \end{aligned}$$

其中  $v_j^+ = v_1 + v_2$ 。

同理得到:

$$U_j^- = \sum_{i=1}^m (w_i X_i^- - w_i X_{ij})^2 + v_j^-$$

在 Step4.2 利用 SDP 得到:

$$D = \frac{d_1}{d_2} = \frac{\beta U_j^+ - \beta v_j^+}{\beta U_j^- - \beta v_j^-} = \frac{U_j^+ - v_j^+}{U_j^- - v_j^-}$$

那么:

$$C_j = \frac{1}{1+k} = \frac{1}{1 + \frac{d_1}{d_2}} = \frac{1}{1 + \frac{\sqrt{U_j^+ - v_j^+}}{\sqrt{U_j^- - v_j^-}}}$$

$$= \frac{\sqrt{\sum_{i=1}^m (w_i X_i^- - w_i X_{ij})^2}}{\sqrt{\sum_{i=1}^m (w_i X_i^+ - w_i X_{ij})^2} + \sqrt{\sum_{i=1}^m (w_i X_i^- - w_i X_{ij})^2}}$$

故该模型是正确的。

#### 3.2 保密性

在 STOPSIS 协议的 Step4.1 中, 利用 SEDMAWPP 协议拍卖者得到  $U_j^+$ 、 $U_j^-$ , 但是  $U_j^+$ 、 $U_j^-$  是和随机数  $v_j^+$ 、 $v_j^-$  相关的, 拍卖者不能简单地猜出投标者的标价  $X_j(X_{1j}, X_{2j}, \dots, X_{mj})$ 。

在 Step4.2, 利用 SDP 协议拍卖者可以计算  $S_j$  的

标价到理想解的距离  $S_j^+$  和负理想解的距离  $S_j^-$  的比  $k$ , 但是不能推出  $S_j^+$ ,  $S_j^-$  具体值。

结合公式 3, 公式 4 拍卖者可以得到公式 5。

$$\begin{aligned}(S_j^+)^2 &= \sum_{i=1}^m (w_i X_i^+ - w_i X_{ij})^2 \\(S_j^-)^2 &= \sum_{i=1}^m (w_i X_i^- - w_i X_{ij})^2 \\ \frac{S_j^+}{S_j^-} &= k\end{aligned}\quad (5)$$

但是拍卖者根据公式 5 不能推出  $WX_j(w_1 X_{1j}, w_2 X_{2j}, \dots, w_m X_{mj})$  的具体值。

以  $m=2$  为例,  $WX_j(w_1 X_{1j}, w_2 X_{2j})$  是圆 1(以  $o_1$  为圆心,  $r_1$  为半径)和圆 2(以  $o_2$  为圆心, 以  $r_2$  为半径)的交点, 其中  $r_1 = S_j^+$ ,  $r_2 = S_j^-$ ,  $o_1 = WX^+(w_1 X_1^+, w_2 X_2^+)$ ,  $o_2 = WX^-(w_1 X_1^-, w_2 X_2^-)$ ,  $\frac{r_1}{r_2} = k$ ,  $|o_1 o_2| = m$ 。  $o_1, o_2$ ,

$WX_j$  可以构成三角形, 由三角形的性质得:

$$\frac{m}{1-k^2} > \sum_{i=1}^2 (w_i X_i^+ - w_i X_{ij})^2 \geq \frac{m}{1+k^2} \quad (6)$$

由于  $r_1, r_2$  不确定, 满足公式 6 的  $WX_j$  有无数个, 如图 4 所示, 拍卖者并不能确定的  $WX_j$  具体位置。

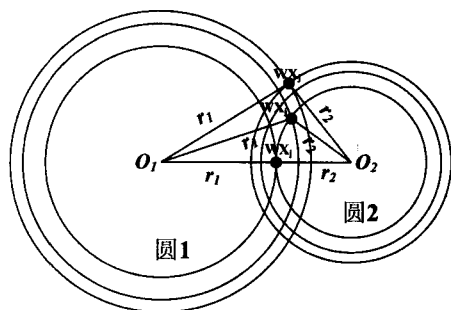


图 4 圆 1 和圆 2 的相交关系

综上, 在该模型中投标者的标价是保密的。在拍卖者与个别投标者共谋的情况下, 拍卖者也不可能向其提供其他投标者标价, 能够抵御拍卖者与投标者间的共谋, 投标者之间是公平的。

### 3.3 复杂性

(1) 轮复杂度: 在安全多方排序协议中, 拍卖者之间需要  $mn$  轮通信, 在执行 SEDMAWPP 协议和 SDP 协议时拍卖者与投标者中需要  $4mn$  轮通信, 故整个模型的轮复杂度为  $O(mn)$ 。

(2) 计算复杂度: 模型的重要计算代价是确定中标价阶段的  $2mn^2$  次加解密运算, 故整个模型的计算复杂度是  $O(mn^2)$ 。

## 4 结束语

文中在安全多方计算的基础上, 提出了 SEDMAWPP 协议和 SDP 协议, 并将它们引入到 TOPSIS 评标方法中, 设计出了一种保护标价的多属性反向拍卖模型, 实现了标价保密性、投标者地位公平性, 能抵御拍卖者与个别投标者共谋, 且方法简单、易实现。文中提出的 SEDMAWPP 协议可以被广泛地应用在信息匹配、空间几何计算、图像处理等领域。

### 参考文献:

- [1] Thiel S. Some Evidence on the Winner's Curse[J]. American Economic Review, 1998, 78(5): 884-895.
- [2] Che Y K. Design competition through multi dimensional auction[J]. RAND Journal Economics, 1993, 24(4): 668-680.
- [3] Bichler M. An experimental analysis of multi-attribute auctions[J]. Decision Support System, 2000, 29(3): 249-268.
- [4] 金 萍, 石纯一. 一种暗标叫价的多属性拍卖方法[J]. 计算机学报, 2006, 29(1): 145-152.
- [5] 金 萍, 石纯一. 一种递增叫价的多属性拍卖方法[J]. 计算机研究与发展, 2006, 43(7): 1135-1141.
- [6] Chen Peiyu, Zhao Wenmei. The Design of Interactive Multi-attribute Reverse Auction System[C]//2009 Chinese Control and Decision Conference (CCDC 2009). [s. l.]: [s. n.], 2009: 4036-4040.
- [7] 陈 湘, 胡山立. 一种安全的多属性拍卖模型[J]. 计算机研究与发展, 2007, 44(4): 680-685.
- [8] 徐玖平, 吴 巍. 多属性决策的理论与方法[M]. 北京: 清华大学出版社, 2007.
- [9] 罗永龙, 黄刘生, 徐维江, 等. 一个保护私有信息的多边形相交判定协议[J]. 电子学报, 2007, 35(4): 685-691.
- [10] 肖 倩, 罗守山, 陈 萍, 等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报, 2008(4): 709-714.
- [11] 张彩云, 罗永龙, 石 磊. 一个点与矩形区域包含关系的安全判定协议[J]. 计算机技术与发展, 2009, 19(9): 140-142.
- [12] 赵晓孔, 罗永龙, 程 超, 等. 一种基于反馈的信任生成算法[J]. 计算机技术与发展, 2010, 20(12): 166-169.

(上接第 129 页)

- [10] Wang Hong, Jiang Junna. Image Processing Based on Fuzzy Cellular Automata Model[C]//Fourth International Conference on Innovative Computing, Information and Control. [s. l.]: [s. n.], 2009: 954-957.

- [11] Yan P, Xianyan Y. Integral image compression based on optical characteristic[J]. Computer Vision, IET, 2011, 5(3): 164-168.
- [12] 王学玲, 王国宇, 聂占堂. 基于元胞自动机的毫米波图像边缘检测[J]. 微计算机信息, 2007(8): 288-290.