Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 27 (2005) 383–395

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

A new reverse auction agent system for m-commerce using mobile agents

Dong-Her Shih[a,*], Shin-Yi Huang[a], David C. Yen[b]

[a]*Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Touliu, Yunlin, Taiwan, R.O.C.*

[b]*Department of DSC and MIS, Miami University, Oxford, Ohio 45056, United States*

Available online 4 November 2004

Abstract

In order to get the goods, a buyer must search for the items through several auction sites in Internet. When the auction starts, the buyer needs to connect to these auction sites frequently so that he can monitor the bid states and re-bid. In this paper, we propose an automated negotiation model between two participants, for m-commerce, using collaborative mobile agents called mobile reverse auction agent system (MoRAAS), which mediates between the buyer and the sellers and executes bidding asynchronously and autonomously. This reduces the network load and offers more intelligent bidding. A new double encryption key chain technique and a new RVAP protocol are proposed to achieve unconditional bid privacy. Every losing bidder can control the privacy of their own bids while no trust is needed. Computational cost of our RVAP protocol is reduced by avoiding the costly verifiable encryption technique.

Keywords: Reverse Vickrey auction; Bid privacy; Mobile agent; M-commerce; Automated negotiation

1. Introduction

Though the technology of e-commerce has grown steadily, it is still difficult to implement the negotiation between a buyer and a seller online. The Internet auction agent system has been expanded as an alternative solution and the area of multi-agent systems [1] has achieved steadily growing interest in the past decade. Two key problems to be addressed in this area are automated resource allocation and task assignment among the individual agents. As a solution to these problems, it has become common practice to apply well-known results and insights from auction theory (e.g., Refs. [2,3]) and well-understood auction protocols like the English auction, the Dutch auction, and the Vickrey auction. Among the different protocols, the Vickrey auction [4] has received particular attention within the multi-agent community and has been applied in e-commerce. The Vickrey auction, in its original formulation, is used for selling goods or resource allocation. In task assignment scenarios, the

* Corresponding author. Tel.: +886 55342601; fax: +886 55312077.

E-mail addresses: shihdh@yuntech.edu.tw (D.-H. Shih), yendc@muohio.edu (D.C. Yen).

0920-5489/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2004.10.006

Vickrey auction works exactly the other way round (often referred to as reverse Vickrey auction): each bidder willing to execute a task makes a bid expressing the amount he wants to be paid for task execution, and the bidder submitting the lowest bid wins the auction; the winner receives an amount equaling the second lowest bid. In many auction sites, sellers take the lead in trades, while buyers have no authority except for estimating value. However, in the reverse auction, a buyer can display their desired goods, along with a desired price, or competitively identify potential sellers and sell their price until a sale is made. Thus, we usually concentrate on the use of the reverse Vickrey auction for task assignment scenarios.

Due to the growing number of cellular phones and PDAs, more and more people desire to perform activities using them. One of these activities is mobile commerce (m-commerce), where a user can buy a product or service no matter where he is. It is necessary to develop techniques and communication mechanisms for mobile commerce, which satisfy the requirements and the limitations of the mobile infrastructure.

This paper proposes an automated reverse auction agent system for mobile commerce (MoRAAS) using collaborative mobile agents based on our proposed RVAP (Reverse Vickrey Auction Protocol with bid privacy) for electronic commerce. The MoRAAS system mediates between the buyer and the seller and RVAP protocol executes bidding autonomously for the buyer. The RVAP auction is a novel protocol in which the sellers' bid agent can compete on price with bid privacy. The idea of encryption key chain is inherited and a new double encryption key chain technique is proposed, so that bid privacy for a losing bidder is achieved without any trust on other parties. Additionally, the new scheme is simpler as the third party T and the auctioneer A are removed.

2. Related works

Agent system and bid privacy of an auction are introduced in this section.

2.1. Auction agent system

Agents facilitate several auction types, including Dutch, English, Vickrey, and First-Price-Sealed-Bid auctions. At first-price open-cry English auction bidders win with and have to pay the amount of the highest bid. In descending price open-cry Dutch auctions, the auctioneer sells a single item at the first incoming bid. At a first-price sealed-bid auction, each bidder submits one bid in ignorance of all other bids and the highest bidder wins and pays the amount of his bid. Similarly, at second-price sealed-bid Vickrey auctions, the winning bidder pays the price of only the second highest bid. There are many auction sites have solutions that offer a convenience to the users. For example, eBay uses a reserve-price auction method. It allows the user to enter a reserve price. As long as the auction is open and the user's reserve price has not been reached, the agent bids the minimum amount necessary to become the highest bidder. However, this limits the user's choice of bidding strategy without bid privacy and may involve taking into account the effect of the 'winner's curse'. The winner's curse is the difference between the amount the winner paid and the next lower bid. If the bidder bids the perceived valuation of the item and wins, the bidder will know that he paid too much because others valued the item less. Sandholm and Huai [5] solve this problem with the agent allowing the user to coordinate bids across multiple auctions automatically and select a bidding strategy.

Nomad [5] and Magnet [6] are auction agents using a mobile agent mechanism. A mobile agent has the unique ability to transport itself from one system to another. This ability allows mobile agents to execute asynchronously and autonomously. Also, the mobile agents communicate with one another. Because of this ability, the auction agent using a mobile agent is smarter than the reserve auction agent. Thus, the agent tracks bids in multiple auction houses in order to look for the best deal and/or coordinates the user's bids in the different auctions.

2.2. Bid privacy of an auction

Bid privacy is a frequently desired property in auction schemes. It refers to the con?dentiality of losing bids to anybody even after the auction ends. Franklin and Reiter [7] were among the first to address electronic auction with bid privacy. They covered many basic problems, combined cryptographic primitives such as secret sharing, digital cash