Trust and Privacy in Grid Resource Auctions

Kris Bubendorfer, Ben Palmer and Ian Welch
School of Mathematics, Statistics and Computer Science
Victoria University of Wellington
Kelburn Parade
Wellington 6140
New Zealand
voice: +64 4 463 6484
fax: +64 4 463 5045
email: kris@mcs.vuw.ac.nz

Trust and Privacy in Grid Resource Auctions

I N T R O D U C T I O N

One of the vital components of any Grid computing infrastructure is the resource broker. A Grid resource broker is the arbiter for access to a Grid's computational resources and therefore its performance and functionality has a wide-ranging influence on the utilisation and performance of the Grid. Market based mechanisms, such as auctions, have often (Buyya, Abramson, Giddy, & Stockinger, 2002; K. Bubendorfer, Komisarczuk, Chard, & Desai, 2005; Chien, M., & W., 2005) been promoted as a solution for scalable resource economies because they are naturally decentralized, efficient and produce optimal allocations. Another advantage of such market-based mechanisms is that they are a natural fit with the principles of Utility computing (Eerola et al., 2003; Komisarczuk, Bubendorfer, & Chard, 2004) and efforts towards Grid commercialization (Dimitrakos et al., 2003; Graupner, Kotov, Andrzejak, & Trinks, 2003).

Ideally, we want to avoid relying on a single 'trusted' resource broker because it may not be trustworthy. For example, a broker holding a resource auction could examine the bids and reveal this information to others, or defraud participants by subverting the auction results. However, we can protect bid values by using a privacy preserving auction scheme. Fraud can be prevented by adding a verification protocol to the auction. The use of privacy preserving and verifiable auction protocols offers guarantees beyond those possible in real world auctions, making the electronic auctions as secure, or more secure, than their physical counterparts. The use of privacy preserving and verifiable auction protocols enables the construction of open and user centric Grid architectures. Indeed, it is possible to imagine such market oriented technologies underpinning peer based user-centric Grid communities, in which users can contribute and consume computing power on demand, purchase services and collectively provide the computing infrastructure.

In this chapter, we provide the background to understand privacy preserving and verifiable auction schemes and discuss the implications of adopting them on Grid architecture. We then evaluate a range of potential secure auction schemes and identify those that are most suitable to be adopted within for use in the Grid.

B A C K G R O U N D

Auctions are favored as an efficient solution to the challenge of distributed resource allocation in both economic (Buyya et al., 2002; K. Bubendorfer et al., 2005; Chien et al., 2005) and can also be successfully applied in noneconomic (Malone, Fikes, Grant, & Howard, 1988) resource allocation systems. There are four main types of auction protocol; the English, Dutch, Sealed-Bid, and what has since become known as the Vickrey auction protocol. The English auction is the conventional open outcry, ascending price, multiple bid protocol. The Dutch auction is an open outcry, descending price, single bid protocol. The Sealed-Bid, or tender, is a sealed single bid, best price (1st price)

protocol in which all bids are opened simultaneously. The Vickrey auction is similar to the Sealed-Bid auction, except that the winning bidder pays the amount of the second bid (2nd price). The second price bid mechanism results in a dominant strategy of truthful bidding in private value auctions, that is, bidding your true value will always give the best return regardless of other bidders strategies. It is worth noting that the revenue equivalence theorem states that all of the four main auction protocols return the same revenue in private value auctions (Vickrey, 1961), hence the selection of an auction protocol usually depends on implementation pragmatics such as messaging requirements.

When it comes to computational auctions however, it may not be possible to achieve QoS goals with a single representative good as the basis for resource allocations. Execution resources form an indivisible set, related and conditional upon the availability of each other. Game theorists term this as the combinatorial allocation problem (CAP) (Rothkopf, Pekec, & Harstad, 1995), in which a set of components have a synergistic value that exceeds the sum of the individual parts. Because of preferential combinations and possible substitutions, bidders have preferences not just for particular items, but for collections of items. The Generalised Vickrey Auction (GVA) (MacKie-Mason & Varian, 1994) extends the 2nd price Vickrey auction protocol to address the CAP.

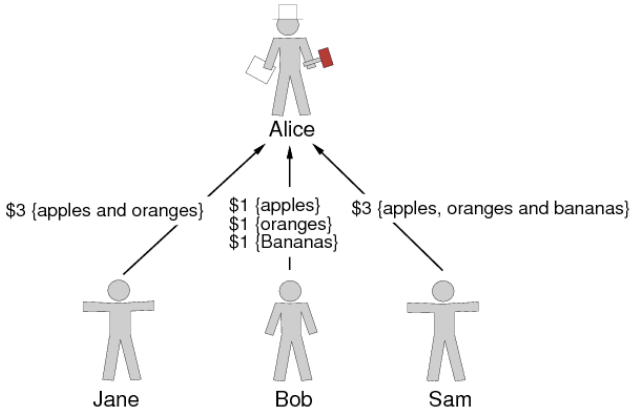

Figure 1: A combinatorial auction.

Figure 1 illustrates a combinatorial auction in which Alice is the auctioneer, Jane wants apples only if she can also have oranges, Bob wants all of the goods but does not need all of them and Sam needs all of the goods together. The highest revenue of $4 is generated by allocating the apples and oranges to Jane, the bananas to Bob and nothing to Sam. For a combinatorial 2nd price auction the price paid by the winner, is their bid less a discount equal to their contribution to the revenue from the auction. This discount is simply calculated by removing the winner from the auction and re-computing the result, the difference in revenues is the '2nd price' discount. The difference between the two values is the winner's discount. Solving a single GVA auction is *NP*-hard (Rothkopf, Pekec, & Harstad, 1995), and for this reason there are a number of optimised variations (Nisan & Ronen, 2000; Parkes, 2001), and approximations (Lehmann, Oallaghan, & Shoham, 2002) that reduce the computation time.

MAIN FOCUS

All auction protocols have known problems when deployed into an electronic market. An exhaustive analysis of these protocol considerations is detailed in (Sandholm, 1996), however, it is worth detailing a few examples. Both the English and Vickrey auctions suffer from self-enforced bidder collusion. All auctions reveal some information, for example, the Dutch auction reveals the winner and their bid, the English auction will reveal the valuations of all bidders (except the winner, who has not yet reached their maximum valuation), and the Vickrey auction will reveal the winner and the price of the second bid but not the bidder of the second price or the price bid by the winner. A compromised or corrupt auctioneer may reveal all the bid values in the case of both sealed bid auctions; and in the Vickrey auction, may misrepresent the amount the winner must pay. In addition, the values of past bids can be collected and either used in future auctions, or passed on to colluding bidders – "*Even if current information can be safeguarded, records of past behavior can be extremely valuable, since historical data can be used to estimate willingness to pay.*" (Varian, 1995).

Trust and Auctioneers in the Grid Economy

If a Grid economy relies on a 'trusted' auctioneer, we have to satisfy to all users as to who owns, controls or audits the auctioneer, where it is placed, and how the auction data is secured. However, a 'trusted' auctioneer does not mean that the auctioneer is trustworthy. Suppose Alice is running a sealed bid auction for her own (and others delegated) resources. The auction is implemented as a webservice and hosted by Sam. Users Bob and Jane *trust* Alice and submit bids to her auction as shown in Figure 2.

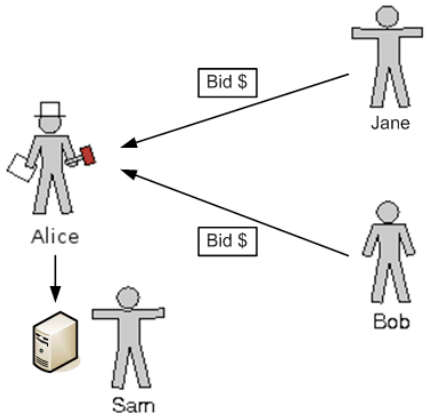

Figure 2: A Resource Auction.

There are many potential problems with this auction. Sam or Alice can examine the bids and potentially reveal this information to others - many bidders would prefer their bids to remain private. Alice could also refuse to count certain bids in the auction, while Sam could filter bids preventing Alice from including them in the auction. Alice could easily

defraud the organizations that have delegated resources to her. Alice could: choose a winner regardless of the bid values to *favor* certain users, choose the winner correctly but report a reduced price and pocket the difference herself, or award the most profitable bids to her own resources. A large amount of trust is placed in Alice with no way of determining if she has correctly executed the auction, in effect Alice is acting as a black box allocator.

We can prevent Alice or Sam from learning and potentially revealing private information by hiding the bid values in such a way that *still permits Alice to correctly compute the outcome of the auction*. This type of auction is privacy preserving, where the bid values are hidden by encryption or obfuscation. Figure 3 shows Alice holding a privacy preserving sealed bid auction.

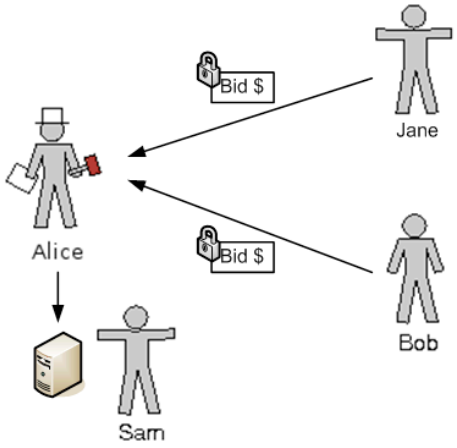

Figure 3: A Privacy Preserving Resource Auction.

In such a privacy-preserving auction, Alice cannot manipulate or misrepresent the bid values (to take a cut). Alice also cannot preferentially favor her resources as the actual values are hidden until the winner and the resource allocation is determined, at which time, only the winning bid value(s) are revealed. However, while a privacy-preserving auction offers significantly better guarantees, we still do not know if all of the bids were counted, and we also do not know if the auction protocol was computed correctly.

The trustworthiness of a privacy-preserving auction can be further enhanced with the addition of a verification scheme. A verifiable privacy-preserving auction is shown in Figure 4. A verification scheme allows bidders and other third parties to verify offline that the auction was executed correctly and that all bids were considered in the result.

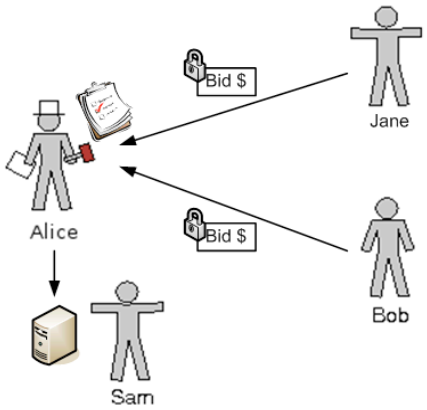

Figure 4: A Verifiable Privacy Preserving Resource Auction.

The verification gives bidders confidence that their bids have been counted and that the auction result has been computed correctly. A nice property is that the owners of any resources delegated to Alice can also verify the auction to make sure they are getting the correct amount of money from Alice. The combination of verification and privacy preservation eliminates the need to trust Alice.

Techniques for Implementing Privacy Preserving and Verifiable Auctions

A number of techniques are used to implement privacy preserving auction protocols and verification schemes. The cryptographic techniques most often used to implement privacy-preserving auctions are summarized below:

- **Homomorphic encryption:** is used to encrypt the bid values while still allowing operations to be performed on them (Yokoo & Suzuki, 2002; Brandt, 2006).
- **Polynomial secret sharing:** is used to spread the bid values over several auctioneers (Kikuchi, 2002) while still allowing bid comparisons. The values of bids are hidden in the degree of a polynomial.
- **Garbled circuit**: uses a circuit composed of virtual Boolean gates to conduct the auction (Cachin, 1999; Naor, Pinkas, & Sumner, 1999). This circuit is created and garbled by an auction issuer and sent to an auctioneer to execute. The garbling of the circuit prevents the auctioneer from discovering any bid values while still allowing the circuit to compute the auction result.

Verification for use with auction protocols has been most often implemented using one of the following techniques:

- **zero knowledge proofs:** to prove the auction was correctly executed while revealing no other information (Brandt, 2006).
- **Range proofs:** have also been used to prove that an encrypted value is the largest in a set of encrypted values (Lipmaa, Asokan, & Niemi, 2002).
- **Cut and choose verification:** is used in the garbled circuits protocol (Naor et al., 1999) where x copies of a garbled circuit are constructed for the auction and x-1

randomly chosen copies are opened before the auction to check they have been correctly constructed.

Architectural Implications for the Grid

The use of privacy preserving and verifiable auction protocols has many advantages for architecting on demand Grid or utility computing systems. As there is no longer any need to trust an auctioneer acting as a resource broker or scheduler, we can build new Grid architectures. The absence of trust enables Grid allocation architectures that are user-centric, peer oriented, open and dynamic. From this flexibility we should also see improvements in reliability, availability and accessibility. Resource auctions can be executed safely using *any* computing resources contributed by *any* provider, and as such, as the size of the Grid increases, additional untrustworthy computing resources can be deployed or redeployed dynamically to meet any subsequent growth in the number of resource auctions. Verifiable auctions remove the need to treat either a trusted auctioneer or privacy preserving protocol as a black box, and provide an audit trail by which incorrect allocations and pricing can be detected. Using this approach, virtual organization can safely auction delegated resources without having to trust any of the individual members of the virtual organization. If a member of a virtual organization, was found to be committing fraud or simply incorrectly programmed, then detection of this behavior would allow the virtual organization to suspend or perhaps redeploy the resources contributed by that member. The results from the verification process could also be used to feed into reputation service.

A U C T I O N T A X O N O M Y

We have constructed a feature centric taxonomy of secure sealed bid auction schemes and note those that also include verification. The taxonomy provides a framework in which to compare the features of secure auction protocols, and serves to identify those which are suitable to be deployed within a Grid economy. We consider the following attributes of secure auction protocols:

- **Price Flexibility** Permits sufficient range and combinations of prices to be generated by the bidders. Some schemes restrict this in different ways i.e., by defining a finite range and granularity of bid values to reduce encryption costs.
- **Verifiability** allows the result of an auction to be checked
    - **Group:** only allows parties that were taking part in the auction to verify the auction process.
    - **Public:** allows any third party to verify the auction process regardless of whether they were taking part in the auction.
- **Type Flexibility:** The scheme supports multiple types of auction:
    - **Single:** supports more than one winner determination scheme, e.g. 1^{st} price, 2^{nd} price, and $(M + 1)^{st}$ price for multiples of the single good.
    - **Combinatorial**: supports auctions where combinations of goods can be bid for.

- **Bid Privacy:** to provide privacy in auctions, the bids are encrypted. The information to decrypt these bids is distributed in two main ways:
    - **Trust Model** bids are encrypted. The information to decrypt these bids is then distributed amongst some number of parties:
        - **Threshold** trust is shared among a set of *n* hosts. Unless a certain number (a quorum) of this set of hosts are corrupt, the privacy of the scheme is preserved.
            - **t,n** The (t,n) if less than t auctioneers of the *n* are subverted and colluding, then the auction is secure.
            - **n,n** The (n,n) unless all *n* of the auctioneers are subverted and colluding, the auction is secure.
        - **Two Party** trust is distributed between two separate parties who must not collude to ensure that the auction is secure.
    - **Level**: when bid privacy is provided, it can provide different levels of privacy. These levels of privacy are grouped as follows:
        - **0:** only the winning bidder and the price they paid are revealed.
        - **1:** in addition to the information leakage of level 0, one other piece of information is revealed. For example, apart from the information revealed by level 0, the fourth highest bid could also be revealed.
        - **m:** (only applicable to combinatorial auctions): in addition to the information revealed at level 0, all maximum bids for any combination of goods is revealed.
        - **s:** in addition to the information leakage of level 0, it is also possible to recover bid statistics. For example, the maximum bid, the average bid, and the standard deviation of bids.
        - ***:** all of the bid values are available to the auctioneer after the auction.
- **Bid Anonymity:** if the bidder is kept anonymous, then the value of their bid cannot be associated with them.

Table 1 identifies which attributes and features are implemented by the surveyed privacy preserving and/or verifiable auction schemes.

Mechanism Evaluation for the Grid Context

We have three main requirements from our discussion of architectural implications for the Grid: (1) we should be able to avoid having to trust a single auctioneer; (2) we should be able to verify that the auction was conducted correctly; and, (3) we should be able to provide strong bid privacy.

We want a scheme that avoids trusting a single auctioneer because this represents a single point of failure. Ideally, the auctions should be capable of being run by a dynamic set of auctioneers who cooperate. This provides reliability, availability and accessibility. In terms of our taxonomy, only bid privacy schemes using threshold trust meet this requirement. All the schemes except for Garbled Circuits (Juels & Szydlo, 2003; Naor et