http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (8): 1221-1227, 2009
ISSN 1812-5638

First-Price Sealed Auction Model with Increased Fairness for Resource Allocation in Grids

M. Mirzayi and M.R. Khayyambashi
University of Isfahan, Hezarjerib Street, Isfahan, Iran

Abstract: The goal of grid computing is to achieve all kinds of resources sharing between organizations. Auctioning models are a source of solutions to the challenge of resource allocation in grid. Auction models can guarantee the interest of participants in the grid with fairness and efficiency. In this study, we modify the bidding stage using Signcryption model and a new definition of grid auction fairness is presented that is based on communication network measurement. First-price sealed auction (FPA) is used for resource management using new methods. SimGrid simulation framework is used which support auction protocols and evaluate results from users' perspective as well as from resources' perspective. The results showed that the new model has a good behavior in grid environment and security and fairness increase in auction model with this method.

Key words: Grid computing, resource management, auction model, parallel signing and encryption, fairness

INTRODUCTION

Computational grids are emerging as a new paradigm for solving large-scale problems in engineering and commerce (Abramson *et al*., 2000; Buyya *et al*., 2001). Resources in the grid context belong to different control organizations with different interest. More importantly, both resources and end-users are geographically distributed. In managing such complex environments, traditional approaches cannot be employed (Buyya *et al*., 2002). Most of the related work in grid computing is resource management and scheduling. Economic approaches are suitable for grids because of their decentralized structure and the use of incentives for resource owners to contribute resources (Grosu and Das, 2004). So, one problem is how to allocate resources for achieving the goal of high efficient utilization of resources.

Auctioning models are one of the economic approaches to the challenge of resource allocation in grid because they provide a decentralized structure and respect the autonomy of resource owners. In the auction model each service provider and user acts independently and they agree privately on the selling price. The auction models can guarantee the interest of participants in the grid with fairness and efficiency. So, the concept of fairness in auction models has to be enriched. Gomoluch and Schroeder (2003) and Abramson *et al*. (2002) present Economic-based resource management systems in Grid. Economic models help resource provider to manage and evaluate resource allocations to user communities. Buyya *et al*. (2002) provides economic models and system architecture for resource management in Grid environments. It also presented a computational economy-driven grid system. In Wolski *et al*. (2001) problems of resource allocation in grids under auctions models have been investigated. There are several works investigate auction models for resource management in grid computing environment.

Grosu and Das (2004) presented an analysis of first-price auction, Vickrey auction and Double auction. It analyses these protocols for using in resource allocation. In a grid environment, the communication requirements of some auction models may become a bottleneck. Thus, it is important to analyze communication complexity of different auction protocols when applied to grid environments. Assunção and Buyya (2006) presented an investigation on the communication requirements of four auction models for resource allocation. Many investigations have been done about auction requirements such as fairness, data security and different implementations have been proposed. A centralized internet auction protocol proposed that consider problems about fairness and security in an auction system (Liaw *et al*., 2006). Wu *et al*. (2008) have been mentioned some problems of Liaw *et al*. (2006) and it have proposed a new protocol for solving these problems. Juang *et al*. (2005) includes a first-price sealed-bid auction protocol that performs security and fairness. Achieving fairness of auctions conducted over the

Corresponding Author: Mansooreh Mirzayi, University of Isfahan, Hezarjerib Street, Isfahan, Iran
Tel: +989132721443, +983712221718 Fax: +983712222018, +983117932670

internet using a single auction server is a challenging problem by Peng *et al.* (1998), since differing message transmission delays experienced by bidders can clearly compromise an auction's fairness. Ezhilehelvan and Morgan (2001) proposed distributed system architecture for internet auction that provides fairness requirement. In most of the mentioned protocols, it should be considered that no solution has been proposed to choose the winner when there is more than one maximum bid. If more than one bidder have proposed the same maximum bid, it uses random numeric and weighted selection method for determining winner (Ezhilchelvan and Morgen, 2001).

For security reasons and in order to maintain fairness, in the sealed-bid auction protocol, all bids are encrypted in transmission. In this study, a new model for encryption/decryption in bidding stage and a method for determining final winner in an auction model are presented which increase fairness. At the reminder, latency time and resource utilization of an auction protocol in grid environments, namely first-price sealed-bid (FPA) is investigated.

AUCTION ALLOCATION MODELS

The auction model supports negotiation between a service provider and many consumers and reduces negotiation to a single value. The main players in a grid auction are (Grosu and Das, 2004; Gomoluch and Schroeder, 2003):

- **Grid service providers (GSPs): Providing the traditional role of producers:** They contribute their resources to the grid and collect the bids from users. They also determine the winning users which are the users that send jobs for execution.
- **User broker (UB): Representing consumers in an auction:** Consumers interact with their own brokers for managing their computations on the grid. The User Broker is responsible for auction (resource) discovery, auction analysis and selection, submitting, managing and monitoring the execution of jobs on the user's behalf and providing the user with a uniform view of grid resources.
- **Grid trading services (GTS):** The GSPs running software systems along with grid trading services to enable resource trading and execution of consumer requests directed through GRBs. The GTS can act as auctioneer if an auction-based model is used in deciding the service access price or an external auctioneer service can be used

Buyya *et al.* (2001) provides detailed information on the role played by GSPs, UBs and GTSs and compares them to actual Grid components and implementations. The steps involved in the auction process are:

- A GSP announces their services
- Brokers offer their bids
- Step 2 goes on until no one is willing to bid a higher price or the auctioneer stops auction
- The GSP offers the service to the winner
- The consumer uses the resource

FIRST PRICE AUCTION PROTOCOL (FPA)

In our implementation of the first-price sealed auction, bidders are not aware of each other's offers. The bidder who bids the highest wins the auction and pays exactly the amount he bids. This type of auction is implemented in single round or multi rounds. We use a multi round sealed-bid auction for allocating resource in grid. In the first round, UBs submit their bids during the time which is determined by GTS. When the first deadline expires, auction is terminated and the winner is determined or the bids become public and a new deadline is determined. Figure 1 shows this scenario.

At the end of the synchronization phase, all the UBs know the current best bid. Summarizing, in the worst case it takes startup time plus the whole duration of the collection and synchronization phase to identify and diffuse the current best bid (Fig. 2). The duration of a synch phase depends on the communication network latency. This auction protocol can be divided into three stages:

Cycle:
1. UBj, j=1,2,…,m sends bid b_j to GSP_i
2. for j=1to m
   GSP_i receives bid b_j

3. After GSP_i collects all the bids $\{b_1,b_2,\ldots,b_m\}$, it dose the following:
   3.1 Determines the U_w and makes it public for all UBs:
   $w=\{i|b_i=\max\{b_1,b_2,\ldots,b_m\}\}$
If GSPi TERMINATE break cycle
End cycle

4.1 Notifies the winner,UB_w
4.2 Send reject messages to the user brokers UB_i, I?w

5. UB_w sends the job to GSP_i executes it
6. UB_w sends the payment b_w to GSP_i

Fig. 1: FPA Protocol (multi round)

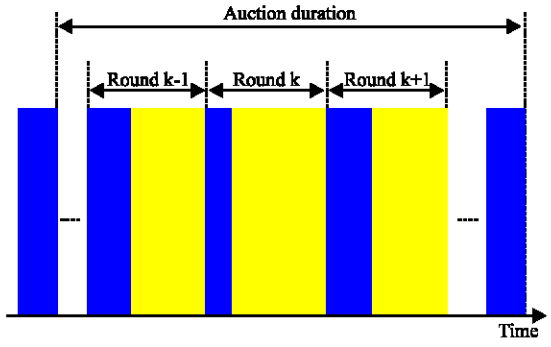

Fig. 2: Time scan of FPA model

- The bidding stage
- The determining winner stage
- The payment and the using of the resource stage

In this study we concentrate on the bidding and determining winner stages.

THE BIDDING STAGE

In the bidding stage, the GTS starts the auction and accepts bids from UBs in the current round before the set deadline is expired. For security reasons and in order to maintain fairness, in the sealed-bid auction protocol, all bids are encrypted in transmission. When it's the bidding deadline, GTS can open all bids and decide the winner. Subramanian (1998) proposed a multi-bidding auction scheme which used public key cryptosystem. In the following, we will explain the details of the bidding stage in grid resource allocation based on Subramanian' s scheme.

The protocol notions which are necessary are defined as follows:

- g and 1/g are public and private keys of GTS, respectively
- UB's public keys and private keys are b and 1/b, respectively
- e encryption key and 1/e decryption key.
- X→Y:[message]$^{1/x}$ means that X signs the message with X's private key and sends it to Y. Therefore, Y can verify that the message is from X
- X→Y:[message]^{y} means that X encrypts the message with Y's public key and sends it to Y. Therefore, only Y can decrypt the message with his private key 1/y

The bidding stage is specified as follows:

UB→GTS: [M1, b, payment^{e}, [price]$^{1/b}$]^{g}: UB bids on the resource. The information of the bid includes the message M1,UB's public key, the encrypted payment with key e and the signed price offered by B. Then GTS can use the public key b to confirm that the price is offered by UB.

GTS→UB: [[payment^{e}]$^{1/g}$, [price]$^{1/b}$]^{b}: After receiving the bid, GTS acknowledges the receipt of the bid. The acknowledgement includes the encryption of the payment signed by GTS's private key 1/g and the price signed by UB's private key 1/b. and it is secured with UB's public key b.

GTS→everybody: [resource description, maximum price offered]$^{1/g}$: When a round of bidding is cut off, GTS collects all the bids in this round and publishes the maximum bid. This stage repeated until no bidder wishes to make a higher bid. As mentioned before, in this scheme the encryption and signature algorithm is used that consider both public and private keys for each sender or receiver. When a message is encrypted with one of the keys (public or private), it is decrypted by another one. By using this method, not only privacy of message will be preserved, also it can authenticate sender. Signing and public key encryption is a common tool which provides message privacy and authentication. O'Mahony *et al.* (1997) and Schneier (1996) evaluated a number of encryption and signature algorithms, it shows public key algorithm is much slower than other encryption algorithms.

In a grid environment, there are resources with different capabilities and a set of users, each with a set of jobs, wish to use these resources. Each job has a deadline and an allowed maximum budget. So, it is important to define resource allocation policies that allocate resources to the jobs regarding their deadline. Bidding stage in grid auction protocols is one of the applications that can use parallel signing and encryption. This method is proposed by Pieprzyk and Pointcheval (2003) and its security and correctness had been proved. Signcryption is security model which uses parallel signing and encryption for generating encrypted and sign message. This model has defined by 3 following algorithms:

Gen: The key generation algorithm which, for a security parameter k, outputs a Pair of keys (SDK; VEK). SDK is the user's sign/decrypt key, which is kept secret and VEK is the user's verify/encrypt key, which is made public for all other users.

SigEnc: The encryption and signing algorithm which, for a message m, the public key of the receiver VEK_R and the private key of the sender SDK_S, produces a signed and cipher text c = SignEnc $_{SDK\,S,VEK\,R}$ (m).

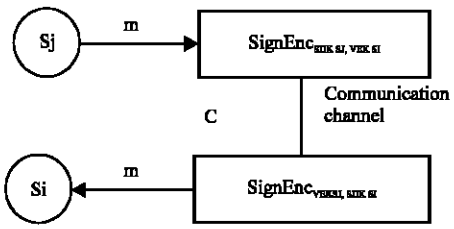

Fig. 3: Parallel signing and encryption method

VerDec: The decryption and verifying algorithm which, for a signed-ciphertext c,the private key SDK_R of the receiver and the public key VEK_S of the sender,Recovers the message m = =VerDec $_{VEK\,S,SDK\,R}$(C).

Thus, following stages (Fig. 3) should be done in sending a message from a sender (Sj) to a receiver (S_i):

At the following, we investigate Subramanian's auction protocol for resource allocation in grid and propose a new scheme using Signcryption model. This scheme decrease the time of encryption/decryption computations to enhance efficiency, thus it is suitable for applying in grid auction protocols. We modify the bidding stage using Signcryption model.

UB→GTS: [M1, VEK_b, payment^e, price]^{SDK_b,VEK_g}: The information of the bid includes the message M1, UB's verify/encrypt key, the encrypted payment with key e and the sigened price offered by B. GTS can use the SDK_g,VEK_b keys and VerDec algorithm to Recovers the message.

GTS→UB: [[payment^e], price]^{SDK_g,VEK_b}: GTS acknowledges the receipt of the bid using SigEnc algorithm and UB can use the SDK_b,VEK_g keys and VerDec algorithm to Recovers the message.

GTS→everybody: [resource description, maximum price offered]$^{1/g}$: We investigate these methods by simulation in grid environment.

USING RESPONSE TIME TO DETERMINE WINNER

Determining winner is an important part in FPA protocol. The information which GSP uses is the bids and number of UBs who have proposed these bids and by this information selects winner. If only one UB suggested the highest bid, it is the specified winner. As mentioned, in FPA protocols bidders don't know the bid values of other bidders so, equal maximum bids are possible. If more than one UB have placed the highest bid which of them is final winner?

Numeric random and weighted selection method is used in (Ezhilchelvan and Margan, 2001) for determining final winner in equal conditions. This method preserves fairness between bidders in an auction, but it doesn't consider time of submitted bids. On the other hand, the time of submitting a bid doesn't have any effect in determining final winner. It would be possible to propose a more fairness algorithm using the time. Our proposed solution is registering response time in the GSP which can be used as a measure for determining final winner. For computing response time, it is necessary to consider the effect of communication network parameters. One of these parameters is link delay that it used in (Wang *et al*., 2007) for analyzing network fairness.

For determining response time, these signs are used:

- **T0:** Is the moment when GSP publishes the commodity information
- **Ti:** (I = 1, 2, 3,...) Represents the moment UBi receives the information
- **Ti':** Represents the moment UBi sends bid request
- **Ti":** represents the moment when GSP receives UB i' feedback

Thus the subjective respond time of each UB should be Ti'-September 8, 2009Ti, which is denoted by Response i. We can see that Ti"-T0 = Response i + RTTi, where RTTi denotes the round trip time of data package transferring. So, response i is:

$$\text{Response I} = \text{Ti5"-T0-RTTi} \quad (1)$$

Considering these parameters, we proposed a suitable solution for increasing fairness in FPA grid auction model. In this solution, each GSP estimates RTT value for all UBi, with this value and (1) computes response time for each of them. Some methods for estimating RTT are presented in (Karn and Patridge, 1991). By this solution, probability of equal conditions (the same highest bid and the same response time) will be decreased in each GSP for FPA protocol.

SIMULATION ENVIRONMENT AND EXPERIMENTAL RESULTS

FPA allocation mechanism is investigated with proposed methods for bidding stage and determining final

winner presented in this study. The SimGrid simulation framework introduced by Casanova (2002) is used. Some parameters are selected for evaluation of the methods. The parameters are the latency time for encryption/decryption and determining final winner and resource utilization.For comparing two structures, S is supposed as the number of resource each with 1000 MIPS (million instructions per second) processing capacity. The topology of resource interconnections has been considering a fully-connected topology (one network link for each pair of computing resources). Although, the fully-connected model fails to model realistic distributed computing environments but it is simple for implementation and makes it possible to use the results for a wide range of environments.

The maximum acceptable latency of any single message is set to 2 sec. The limit of auction rounds for multi round Sealed-Bid auction is set to 20. To evaluate new method in bidding and determining winner we compare Subramanian's scheme (shown as sub FPA) with Signcryption model (shown as improved FPA).

At best, one would expect that parallel encryption and sign will consume roughly the same time as the most time-consuming operation (either signing or encryption, for the joint encryption and signing and either verifying or decrypting, for the joint decryption and verifying).

- Time (parallel encrypt and sign) ≅ max {time (encrypt), time (sign)}
- Time (parallel decrypt and verify) ≅ max {time (decrypt), time (verify)}

Signcryption method can concurrently encrypt and sign (decrypt and verify), so, it has more performance than sequential public key algorithm and the lower time order.

For evaluation the new method for fair winner determination, it is necessary to consider the time which is required by GSP to determine best bids. This time includes selecting of the highest bid with the lowest response time. Figure 4 shows the required time for winner determination based on usual method and the proposed method.

Winner determination based on user response time requires more time than usual way. But this increasing in latency time can be considerable in combination with parallel Signcryption method.

As Fig. 5 shows, it presents the latency time in using the bidding models and the proposed method for determining final winner user in FPA protocol. It takes the

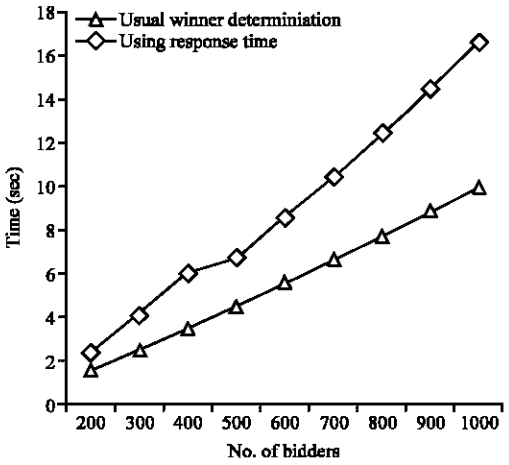

Fig. 4: Required time for winner determination based on user response time

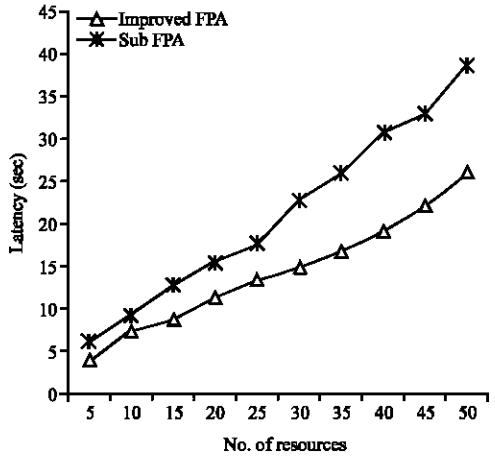

Fig. 5: Latency time

duration of a bidding cycle and synchronization cycle plus the pace at which the GSPs compute the current best bid. In the worst case, FPA with Signcryption model needs lower latency time than Subramanian's scheme.

The percentage of resource utilization has been measured to investigate proposed method from resource's perspective. Resource utilization for a resource is defined as the ratio of the total execution time at the resource to the total simulation time (Grosu and Das, 2004). Figure 6 shows the amount of resource utilization improved FPA and sub FPA protocols. Both auctions present similar performance in some cases and in the most cases improved FPA is better than sub FPA. So, FPA protocol based Signcryption method and using response time has acceptable resource utilization in comparison with other model.

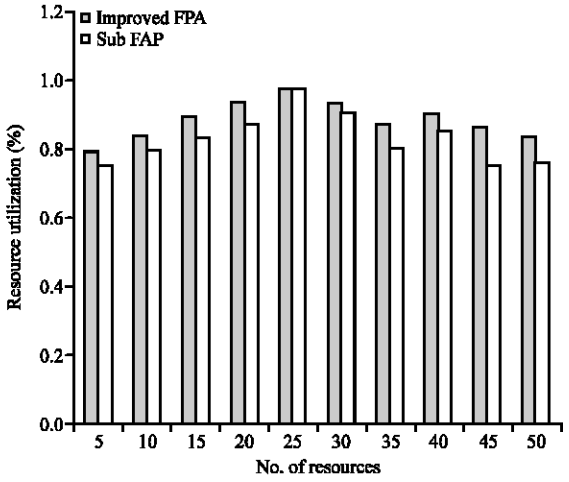

Fig. 6: Resource utilization

CONCLUSION

In this study, Subramanian bidding auction scheme which used public key cryptosystem is used for bidding stage in grid auction protocol. In the following we have explained the details of the bidding stage in grid resource allocation based on Signcryption model. Then one method for increasing fairness in a FPA auction model is proposed. Considering an average value for transmission delay, a suitable solution is used for computing user response time and then determining winner user based on the lowest response time for allocating resource in grid computing. The two auction allocation models are presented and these protocols are simulated using the SimGrid simulation framework. Some parameters are considered for evaluation of the methods. The parameters are latency time and resource utilization. FPA using Signcryption model presents an acceptable performance from the user's perspective and from the resource's perspective.

REFERENCES

Abramson, D., J. Giddy and L. Kotler, 2000. High performance parametric modeling with Nimrod/G: Killer application for the global grid?. Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS 2000), Cancun, Mexico, May 1-5, IEEE Computer Society Press: Los Alamitos, CA, pp: 520-528.

Abramson, D., R. Buyya and J. Giddy, 2002. A computational economy for grid computing and its implementation in the nimrod-G resource broker. Future Gener. Comput. Syst., 18: 1061-1074.

Assunção, M. and R. Buyya, 2006. An Evaluation of communication demand of auction protocols in grid environment. Proceedings of the World Scientific GECON 2006, May 16, Singapore, pp: 24-33.

Buyya, R., D. Abramson and J. Giddy, 2001. A case for economy grid architecture for service-oriented grid computing. Proceedings of the International Parallel and Distributed Processing Symposium: 10th IEEE International Heterogeneous Computing Workshop, April 2001, IEEE Computer Society Press, San Francisco, CA. pp: 1-15.

Buyya, R., D. Abramson, J. Giddy and H. Stockinger, 2002. Economic models for resource allocation and scheduling in grid computing. Concurrency Comput. Practice Experience, 14: 1507-1542.

Casanova, H., 2002. Simgrid: A toolkit for the simulation of application scheduling. Proceedings of the IEEE/ACM International Symposium on Cluster Computing and the Grid, May 15-18, Brisbane, Australia, pp: 430-437.

Ezhilchelvan, P. and G. Morgan, 2001. A dependable distributed auction system: architecture and an implementation framework. Proceedings of the 5th International Symposium, Mar. 26-28, University of New Castle, pp: 3-10.

Gomoluch, J. and M. Schroeder, 2003. Market-based resource allocation for grid computing: A model and simulation. Proceedings of the 1st International Workshop on Middleware for Grid Computing, (IWMGC'03), London, UK., pp: 211-218.

Grosu, D. and A. Das, 2004. Auction-based resource allocation protocols in grids. Proceedings of the 16th IASTED International Conference on Parallel and Distributed Computing and Systems, November 2004, Cambridge, MA, USA., pp: 20-27.

Juang, W.S., H.T. Liaw, P.C. Lin and C.K. Lin, 2005. The design of a secure and fair sealed-bid auction service. Mathemat. Comput. Model., 41: 973-985.

Karn, P. and C. Partridge, 1991. Improving round-trip time estimates in reliable transport protocols. ACM Trans. Comput. Syst., 9: 364-373.

Liaw, H.T., W.S. Juang and C.K. Lin, 2006. An electronic online bidding auction protocol with both security and efficiency. Applied Mathemat. Comput., 174: 1487-1497.

O'Mahony, D., M. Pierce and H. Tewari, 1997. Electronic Payment Systems. 2nd Edn., Artech House, USA., ISBN-10: 1580532683.

Peng, C., J.M. Pulidod, K.J., Lin and D. Blough, 1998. The design of an Internet based real time auction system. Proceedings of the IEEE Workshop on Dependable and Real Time e-Commerce Systems (DARE-98), Denver.

Pieprzyk J. and D. Pointcheval, 2003. Parallel Authentication and Public-Key Encryption. In: Information Security and Privacy, Safavi-Naini, S. and J. Seberry (Eds.). Springer-Verlag, Heidelberg, ISBN: 978-3-540-40515-3, pp: 383-401.

Schneier, B., 1996. Applied Cryptography. 2nd Edn., Wiley, New York, ISBN: 0-471-11709-9.

Subramanian, S., 1998. Design and verification of a secure electronic auction protocol. Proceedings of the IEEE 17th Symposium on Reliable Distributed System, Oct. 20-23, West Lafayette, IN, USA., pp: 204-210.

Wang, X., X. Zhang, S. Yang and X. Xue, 2007. Design of a fairness guarantee mechanism based on network measurement. Proceedings of the 10th IEEE High Assurance Systems Engineering Symposium, Nov. 14-16, Plano, TX, Hase, pp: 425-426.

Wolski, R., J.S. Plank, J. Brevik and T. Bryan, 2001. Analyzing market-based resource allocation strategies for the computational grid. Int. J. High Perfor. Comp. Appli., 15: 258-281.

Wu, C., C. Chang and I.C. Lin, 2008. New sealed-bid electronic auction with fairness, security and efficiency. J. Comput. Sci. Technol., 23: 253-264.