A study of several privacy-preserving multiparty negotiation problems with applications to supply chain management

Thesis Summary

Sumit Chakraborty (FP/04/2000)

Indian Institute of Management Calcutta, 2006

Supervisor : Professor Asim Kumar Pal

Negotiation is a means for a group of decision-making agents to reach mutually beneficial agreement through exchange of strategic information. But, the decision makers are often reluctant to share their private information with others. The primary contribution of this thesis is to study various scenarios of multi-party negotiation in the areas of supply chain management, e-markets and auctions in order to suggest appropriate privacy models for these problems and finally to develop privacy-preserving coordination mechanisms and/or protocols for these situations by applying the concept of secure multi-party computation to the underlying problem, which is more often than not an optimization problem in a distributed setting where parties are connected over an insecure medium such as internet. Specifically, four problems have been tackled in the thesis:

1. Collaborative supply chain planning
2. Discriminatory price negotiation in an e-market
3. Combinatorial reverse auction and 1-n-p negotiation protocol
4. Multi-objective group decision making and group buying

The sharing of information is important for efficient supply chain planning. But, the partners of a supply chain are often reluctant to share their strategic information. On the other hand, the lack of information exchange gives rise to information asymmetry and causes problems related to capacity utilization, inventory control, transportation, distribution and customer service. Thus, sharing or exchange of information yet maintaining the privacy is an important issue. Collaborative supply chain is an active example of a networked system of a large number of partners each having its own strategic goal. This scenario is quite common in the current era of globalization and technological and strategic collaboration of different firms across the globe. These partners are engaged in execution of a joint plan ranging over a variety of operations. Privacy is a critical yet complex issue for collaborative supply chain planning, particularly when each partner has its own strategic interest. Maintaining privacy in non-trivial transactions like joint optimization in an electronic environment is still a challenge to the security community.

The first chapter (Introduction) gives the general motivation of the negotiation scenarios and problems studied in the thesis, and attempts to outline the existing as well the proposed approaches for the solution.

In chapter 2, the collaborative supply chain-planning problem has been analyzed in great detail from a veriety of angles. The issues that have been addressed are :

- Global planning domain based solution vs. local planning domain based solution.
- Compensation based negotiation vs. negotiation without compensation.
- Synchronization of bidding (serial vs. parallel)
- Linear vs. nonlinear plans
- Local vs. global optimization
- Complexity of the supply chain (2-tier and multi-tier).

Dudek (2004) has given a mathematical programming based iterative solution procedure (generating alternative plans in each iteration) which basically works with local planning domain based plans and compensation negotiation, but finally achieves only a local minimum solution (for the total supply chain cost). The algorithm even for only 2 party (single buyer and single supplier) is very time consuming, as it has to conduct a negotiation for compensation amount in every iteration of plan generation. In addition, there is also disclosure of cost effects (i.e. change of costs over the previous plan). Dudek has also outlined for single buyer multiple suppliers and multiple buyers single supplier cases based on a similar principle. We have tried to reduce the disclosure and total negotiation time for various scenarios of CSCP (including multi-tier) as already mentioned.

To develop the coordination mechanisms, we have used secure multi-party computation (SMC) concepts and in the process we have proposed some SMC protocols which are useful for general problem beyond this thesis: (a) secure linear programming algorithm extending the concept given by Du (2001), (b) private comparison protocol and (c) secure summation protocol.

Price negotiation is a common phenomenon in e-markets (e.g. auction) and an important aspect of supply chain management. In chapter 3, a *discriminatory price negotiation* problem has been studied wherein a supplier wants to supply to a number of interested buyers according to its capacity. Different buyers pay different unit prices to the supplier. Each buyer has a different demand function indicating its price-quantity choices. The supplier wishes to optimize its own parameter (e.g. revenue) subject to a capacity allocation model while determining individual supplies. Here, the privacy will involve the demand function of each buyer and the optimization function of the supplier and for each buyer individual supplies (price and quantity) to other buyers.

The discriminatory price negotiation protocol proposed in the thesis takes care of these existing capacity allocation models: linear allocation, proportional allocation and allocation for the maximization of revenue. The works by Atallah et al. (2003,2004) and Sandholm and Suri (2001,2002) form the basis of this work. Sandholm and Suri (2001) have given an auction protocol for this problem. But, they have not considered the privacy issue. Atallah et. al. (2003,2004) have solved the problem for a fixed demand situation, wherein he used the services of an intermediary called proxy (or distributor) to keep a distance between the buyers and the supplier.

To develop the price negotiation protocol, we have used secure multi-party computation (SMC) concepts and in the process we have proposed some SMC protocols which are useful for general problem beyond this thesis: a) joint function evaluation with or without a mediator and b) two protocols to compute the sum of values from the parties having no interconnection – one using homomorphic encryption and the other using mixnet.

In chapter 4, a *combinatorial reverse auction* problem has been studied wherein a buyer negotiates with n suppliers to procure p (types of) items within a given time frame. Here the buyer will procure one item from one supplier only, but a supplier may supply more than one items to the buyer. Suppliers submit their bids. The objective is to label the bids as winning or losing so as to minimize the buyer's cost with the constraint that the buyer obtains all items (in required quantity). We have described a privacy model for combinatorial reverse auction and have proposed a *1-n-p* negotiation protocol. Following m-n negotiation protocol (Aknine et al, 2004) the negotiation process has two distinct phases – *Pre-bid* and *Final bid*. During pre-bid suppliers singly or jointly bid for a combination of items, i.e. in each round a supplier can choose to merge with other suppliers to form a new subgroup or split with the current subgroup to

change its bids. Pre-bid phase consists of a number of rounds or cycles of bidding. The objective of each pre-bid cycle is to find the minimum cost bid for all subgroups. At the end of this phase the winners get *preaccepted* and the losers get *prerejected*. In final bid phase (which has only one round of bidding) the suppliers submit their final bids irrespective of being preaccepted or prerejected in pre-bid. Finally, the buyer finds the optimum combinations of the final bids.

The privacy requirements considered are: a) Pre-bid: subgroup formation (forward and backward privacy), and anonymity of the winner in each pre-bid cycle. b) Final bid: anonymity of the losers and traceability of the winners. A privacy preserving 1-n-p negotiation protocol has been developed for the purpose. A couple of SMC protocols, which are also useful for general problems beyond this thesis, have been proposed: key management protocol for secure group communication and minimum protocol (without any interaction among the parties).

In chapter 5, we have studied a stochastic linear multi-objective group decision making (MOGDM) problem. A group of DMAs are involved in a negotiation process and each of them provides the limits of variations of the coefficients of objective functions and constraints in interval form. The basic objective of MOGDM is to find out a commonly acceptable solution combining the preferences of all DMAs. Xanthopulos et al. (2000) gave a computing framework with three distinct stages: 1. A mediator (MA) transforms the stochastic problem into a deterministic problem (using the median values of each interval parameter – both upper and lower limits). 2. MA guides each DMA through an interactive search process and finds a set of alternative solutions. 3. The commonly agreed solution for the group is found by aggregating individual solutions based on complete or incomplete preferential information.

The privacy restrictions considered are: a) Stage 1: MA should not know the interval parameters of the DMAs. The median values will not be disclosed to the DMAs. The deterministic problem will be known only to MA. b) Stage 2: During the interactive search process MA should not learn the preferential information of the individual DMAs, nor should it learn anything about the set of solutions of the DMAs. c) Stage 3: While aggregating individual choices, no DMA would learn anything about others' solutions, nor MA will learn anything about the commonly agreed solution.

A privacy preserving MOGDM protocol has been designed for the above framework. Light Beam Search (Jaskiewicz et al., 1999) has been used for the interactive search procedure. Moreover, this protocol has been demonstrated on a group buying problem (Anand et al, 2003). To develop this protocol a few SMC tools, which are also useful for general problems beyond the thesis, have been proposed: median protocol, light beam search protocol and private preference matching protocol.

The final chapter concludes by indicating some open problems.

Keywords **:** privacy, negotiation, coordination mechanism, multi-objective group decision making, secure multi-party computation, secure group communication, supply chain, combinatorial reverse auction, pricing, multi-objective group decision making.