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

Dudek (2004) has given a mathematical progr

change its bids. Pre-bid phase consists of a number of rounds or cycles of b

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.