Secure Distributed Constraint Satisfaction: Reaching Agreement without Revealing Private Information

Makoto Yokoo[1], Koutarou Suzuki[2], and Katsutoshi Hirayama[3]

[1] NTT Communication Science Laboratories, NTT Corporation
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan
yokoo@cslab.kecl.ntt.co.jp
http://www.kecl.ntt.co.jp/csl/ccrg/members/yokoo/
[2] NTT Information Sharing Platform Laboratories, NTT Corporation
1-1 Hikari-no-oka, Yokosuka, Kanagawa 239-0847, Japan
koutarou@isl.ntt.co.jp
info.isl.ntt.co.jp/~koutarou/
[3] Kobe University of Mercantile Marine
5-1-1 Fukae-minami-machi, Higashinada-ku, Kobe 658-0022, Japan
hirayama@ti.kshosen.ac.jp
http://www-jo.ti.kshosen.ac.jp/~hirayama/

Abstract. This paper develops a secure distributed Constraint Satisfaction algorithm. A Distributed Constraint Satisfaction Problem (DisCSP) is a CSP in which variables and constraints are distributed among multiple agents. A major motivation for solving a DisCSP without gathering all information in one server is the concern about privacy/security. However, existing DisCSP algorithms leak some information during the search process and privacy/security issues are not dealt with formally. Our newly developed algorithm utilizes a public key encryption scheme. In this algorithm, multiple servers, which receive encrypted information from agents, cooperatively perform a search process that is equivalent to a standard chronological backtracking. This algorithm does not leak any private information, i.e., neither agents nor servers can obtain any additional information on the value assignment of variables that belong to other agents.

1 Introduction

A Distributed Constraint Satisfaction Problem (DisCSP) is a constraint satisfaction problem in which variables and constraints are distributed among multiple agents. Since various application problems in multi-agent systems can be formalized as DisCSPs, there have been many works on this topic in the last decade [5, 7, 10, 13, 14, 15].

One major motivation for solving a DisCSP without gathering all information in one server is the concern about privacy/security, i.e., the knowledge of the problem each agent has is private information and revealing such information

P. Van Hentenryck (Ed.): CP 2002, LNCS 2470, pp. 387–401, 2002.

to a server or other agents is not desirable. Consequently, we cannot gather all information in a single server and solve the problem by using centralized CSP techniques. In a DisCSP, a variable value can be considered as an action/plan that an agent will take. It is natural that an agent does not want to reveal information on possible plans or the final plan it will take to other agents.

For example, a problem of scheduling multiple meetings among multiple participants can be formalized as a DisCSP as follows. Each agent/participant has one variable that corresponds to each meeting. The domain of a variable is possible dates and time slots. There exist equality constraints among variables that represent the same meeting and belong to different agents (i.e., they must meet the same day/time). Also, there exist inequality constraints between multiple variables that belong to the same agent (i.e., a person cannot attend multiple meetings at the same time). Also, an agent has unary constraints on its variables (i.e., he/she has personal schedules that prevent him/her from attending a meeting). In this problem domain, it is clear that a person would not be happy to make such private information public.

However, existing DisCSP algorithms leak some information during the search process and privacy/security issues have not yet been dealt with formally. For example, in the asynchronous backtracking algorithm [14], each agent exchanges a tentative value assignment with each other. If the current assignment does not satisfy constraints, these agents change their assignments and perform backtracking in a certain order. During this search process, an agent can obtain some information on possible values of variables that belong to other agents. Also, an agent can learn the final value assignment of these variables.

When applying this algorithm to the meeting scheduling problem, we can assume each agent makes proposals on the date and time slot of the meeting and negotiates with other agents. The fact that an agent proposes a certain date reveals that he/she does not have any personal schedule on that date. If an agent declines a certain date, this means that he/she has a personal schedule or the date conflicts with some other meeting. Such private information is leaked during the search process.

On the other hand, in the research community on information security and cryptography, there have been many works on multi-party protocols, which deal with performing various computations based on private information of participants, while keeping the private information secret [4, 9]. However, as far as the authors are aware, there has been virtually no work on solving combinatorial optimization problems (including CSPs as a special case) by utilizing information security techniques, with the notable exception of the authors' recent works on secure dynamic programming [12, 16].

In this paper, we develop a secure DisCSP algorithm that utilizes information security techniques. As far as the authors are aware, this is the first research effort that combines the two growing research fields, i.e.. constraint satisfaction and information security.

In this paper, we say that an algorithm does not leak any private information if an agent cannot obtain any additional information on the value assignment of