Self Reordering for security in Generalized English Auctions (GEA)

Marius-Călin Silaghi[*]
Florida Institute of Technology (FIT)
Melbourne, Florida USA
msilaghi@cs.fit.edu

Boi V. Faltings
Swiss Federal Institute of Technology (EPFL)
Lausanne, Switzerland
Boi.Faltings@epfl.ch

ABSTRACT

Distributed approaches to negotiation have special privacy properties as main advantage over existing centralized/cryptographic techniques: The problem of an agent only has to be revealed according to the needs of the negotiation. After a negotiation has closed, the agents know how much they have communicated and therefore they know an acceptable upper-bound on their privacy loss due to the search.

In this article we first introduce Generalized English Auctions, a large class of negotiations that can be addressed naturally by distributed algorithms. It is then shown how a security problem found in existing protocols can be solved by enabling a certain dynamic reordering schema. We have introduced a technique allowing to add dynamic reordering to existing asynchronous complete search algorithms that have polynomial space requirements. Several recent developments of this technique are shortly mentioned.

Categories and Subject Descriptors

I.2.11 [**Computer Methodologies**]: Artificial Intelligence—*Distributed Artificial Intelligence*

General Terms

Security,Verification,Algorithms

1. PROBLEM AND APPROACH

The auctions enabled by our approach to Generalized English Auctions are a kind of multi-unit combinatorial exchanges where the final solution has to get the agreement of a predefined (sub)set of agents (the *initiators*). We therefore call such auction problems *Multi-Unit Supervised Combinatorial Exchanges (MUSCEWDP)*.

Definition 1. *MUSCEWDPs are Multi-Unit Combinatorial Exchanges winner determination problems where the solution needs the agreement of a predefined set of agents.*

First we cast MUSCEWDPs into a practical framework based on CSPs. The problem of an agent is a Negotiation Valued Constraint Satisfaction Problem (NVCSP). The NVCSP of A_u can be perceived as a Valued CSP that can be strictly monotonically relaxed: $c_1(u)$,...,$c_{n_u}(u)$. Variables can model transactions. The domain of each variable contains a value F meaning *unchanged* and *indifferent*. The value of a tuple t in $c_k(u)$ is $price^t_k(u)$. (Requested) prices monotonically descend. A formal definition is given in [1].

Definition 2. *A Dynamic DisCSP (DyDisCSP) is defined by:*

- *A set of agents* A_1,...,A_n. $A_k, k \in [1, h], n \geq h \geq 1$, *are* h *agents called* initiators.
- *Each agent* A_j *owns a NVCSP,* $NVCSP_j$.
- *Each agent* A_j *is interested in a set of public variables V(j).*

Given a valuation v for all the public variables, $S(v)$ is the set of agents owning a variable instantiated in v to something else than F. By convention, the *initiators* also always belong to $S(v)$. Intuitively, $S(v)$ is the set of agents that have to agree on the valuation v, in order for v to be a solution.

Definition 3 (Acceptable valuation). *A valuation* v *is acceptable if each agent* A_i *in* $S(v)$ *proposes a feasible tuple for the projection of* v *on V(i).*

Intuitively, a *stable valuation* is minimal in the sense that it corresponds to an agreement of the agents in $S(v)$, and by eliminating any subset of transactions, no agreement can be obtained with the *initiators* on the remaining valuation [1].

Definition 4. *An agent* A_i *is* active *either if* A_i *is an initiator, or recursively, if an agent that is active proposes a valid instantiation outside* F *of a public variable of* A_i.

Definition 5 (Solution). *A solution of a DyDisCSP is a stable acceptable valuation* v *of all the public variables.*

Definition 6 (Optimal Solution). *Given the set* Γ *of all solutions of a DyDisCSP, and the set*

$$\mathcal{A} = \{b |\ b = \operatorname*{argmin}_{a\in\Gamma}(\sum_{A_i\in S(a), i>h} price^a_{k_i}(i))\},$$

[*] This work was performed while the first author was working at EPFL.

AAMAS'02, July 15-19, 2002, Bologna, Italy.

a solution v is optimal when $v \in \mathcal{A}$, v is pareto-optimal for $S(v)$ over $\mathcal{A}$ (given preferences, see details in [1]), and no agent A_i, $i>0$, wants to reveal a constraint c_j, $j>k_i$.

The feasibility condition is $\sum_{A_i \in S(v)} price^v_{k_i}(i) \leq 0$.

The feasibility condition verifies that the solution leads to a positive balance. The *initiators* gain.

1.1 Generalized English Auctions

The Generalized English Auction (GEA) is a technique for solving MUSCEWDPs/DyDisCSPs. A GEA consists of series of rounds where each round starts when an agent relaxes its constraints. The relaxation is followed by a search process that defines a winner given the current relaxation state of the DyDisCSPs. The GEA ends when no agent wants any longer to start a new round by relaxing its constraints.

1.2 Estimated Social Welfare (ESW)

Declared-pareto-optimal solution is a pareto optimal solution computed for the problems declared by the agents.

DEFINITION 7. *The* Solution Cost *is given by the sum of the prices asked by the agents to the initiators for agreeing on the alternatives composing the solution.*

DEFINITION 8 (ESTIMATED SOCIAL WELFARE). *An estimated social welfare solution (ESW) is a declared-pareto-optimal solution with minimal Solution Cost.*

Guaranteeing that a solution is ESW is possible with complete search techniques.

DEFINITION 9. *A problem with equivalent solutions is a problem where the difference between the quality (value) of its solutions is equal to the difference between the cost or the respective solutions (the solutions are equally good).*

It is worth mentioning that for problems with equivalent solutions an ESW gives the best possible estimation of the real Social Welfare. This is the case of a bandwidth allocation problem where any two paths in the network are equally good as long as it has the required bandwidth and QoS.

1.3 Security problem in ABT/AAS

The problem is that a solution of a DyDisCSP does not need to be an acceptable solution for all the agents, as long as some of them are not **active** in the solution and do not gain anything. Asynchronous backtracking (ABT) and Asynchronous Aggregation Search (AAS) are asynchronous complete search algorithms for satisfying all agents [1]. In ABT and AAS, both **ok?** and **nogood** messages transport some kind of nogoods. These are the nogoods entailed by the view, respectively the explicit nogoods. In order to allow the agents detect messages that are potentially harmful for the quality of the computed DyDisCSP solution, we introduce the notions of legal nogood and legal assignment.

We want to prevent the agents from disturbing the search by generating illegal messages. A message (containing a nogood $\neg N$) is illegal if it is generated by an agent that can be inactive in some valuation that extends a partial valuation found in the Cartesian-product defined by N.

1.4 Veri£able distributed search

We requests agents to build messages in such a way that their lawfulness can be proved.

DEFINITION 10 (LEGAL EXPLICIT NOGOOD). *Any legal explicit nogood generated by an agent A_i, where A_i is not an* initiator, *must contain at least one* assignment *of a variable v from $V(i)$ such that v does not contain F.*

DEFINITION 11. *Each assignment I_i generated by an agent A_i that is not* initiator *needs a* justification. *The* justification *of the assignment I_i consists of a pair (v,h) built from an assignment $\langle v, s, h \rangle$ that activates A_i.*

DEFINITION 12 (LEGAL ASSIGNMENT). *An assignment is legal if its justification is valid and the variable in the justification does not contain F in its instantiation. By convention, any assignment generated by an initiator is legal.*

2. DYNAMIC REORDERING IN ABT/AAS

A complete algorithm that respects the aforementioned security requirements can be built once dynamic reordering can be performed in ABT or AAS. The optimal solution can be extracted with some Branch and Bound approach. Several powerful optimization algorithms exist [1].

A technique for dynamic reordering in protocols like ABT and AAS is detailed in [1]. It allows for many reordering heuristics. The dynamic reordering technique consists of defining a set of reordering roles/offices. For n agents $(A_1,...,A_n)$, up to $n-1$ reordering offices are useful $(R^0,...,R^{n-2})$. A strict total order is defined on offices. The offices can be occupied by agents or by communities.

Given its currently known ordering state o, the current holder, $H^k(o)$, of an office R^k may propose an ordering o' that changes the holder of any office $R^t, t \geq k$. o' can also change the current order on the agents that have a priority lower than $A^k(o)$. $A^t(o)$ denotes the identity of the agent that has the position t in the ordering o. Heuristic data based on assignments of $A^k(o)$ can be sent in finite time to any $H^t(o), t \geq k$. $H^k(o)$ is constrained to decide its proposals in a finite time after receiving the last such heuristic data.

The decision o' taken by $H^k(o)$ in the frame of an office R^k has to be broadcasted to all agents $A^t(o), t>k$, and eventually to any $H^t(o'), t \geq k$. The decision can be included in messages under the most general form: $\langle H^k(o') \leftarrow R^k, ..., H^{n-2}(o') \leftarrow R^{n-2}; A^1(o'), ..., A^n(o'); h(o') \rangle$. $h(o')$ is the history of o' built as defined for instantiations in AAS, and formalized as *signatures* or *traces* in [1].

3. SECURE, FAIR, EFFICIENT

For the security of the search, we need to dynamically involve on low positions in search only agents that are known to be active. This can be easily obtained in ABTR or AASR using the reordering heuristics obtained using the rules of SAS presented in [1].

With reordering based on voting, conventions like $H^k(o) \equiv \{A^t(o) | t>k\}$ can enhance fairness. Conventions like $H^k(o) \equiv \{A^t(o) | t \leq k\}$ can enhance privacy [1].

Some efficiency gains are obtained with the reordering convention $H^k(o) \equiv A^{k+1}(o)$, and $H^k(o)$ generates o' such that $A^{k+1}(o') \equiv A_t$ where A_t is the agent sending the first received valid nogood by $A^{k+1}(o)$ [1].

4. REFERENCES

[1] Marius-Călin Silaghi. *Polynomial-Space Asynchronous Search*. PhD thesis, Swiss Federal Institute of Technology (EPFL), CH-1015 Ecublens, 2002. submitted.