Privatizing Constraint Optimization

Rachel Greenstadt AAAI/Sigart Doctoral Consortium July 16, 2006

Problem: Privacy for DCOP

- Promise of DCOP
 - Coordination in optimal and automated ways
- Problems
 - Constraints may be personal and private
 - No evaluation of privacy in current systems
 - Current systems not designed for privacy

Approach

- Analyze existing DCOP algorithms
- Develop new metrics where appropriate
- Develop new algorithms with better privacy
- Analyze effect of continuous/dynamic DCOP on privacy

Example : Alice the Hairdresser

- Alice's concerns
 - Doesn't want
 clients to know
 how busy she is
 - Some clients
 preferred -- don't
 want others to
 know

- Customer concerns (Bob and Carol)
 - Alice gossips and they don't want their scheduling info spread around



Scheduling Domain: Entering the Mainstream









Scheduling Process

Public Information : Meetings/appts, participants

Scheduler → Meetings and Times

Private Information : Preferences

Centralized Models

- Central server optimizes subject to the constraints of individual preferences
- Privacy issues, unless trusted third party
- But are they trusted?
 - Your company's IT department
 - Google/Microsoft (Big Brother?)
 - Data retention

DCOP Model

- Distributed Constraint Optimization Problem
- Distribute the problem for privacy/efficiency/autonomy/scalability
- Many algorithms
 - DPOP (Dynamic Programming Optimization)
 - SynchBB (Synchronous Branch and Bound)
 - Adopt (Asynchonous Distributed Optimization)
 - OptAPO (Optimal Asynchronous Partial Overlay)
- Metrics are important to distinguish privacy properties of these algorithms

Analysis of Existing Algorithms

Research Questions :

- Which algorithms are best in given situation?
- Why do certain algorithms do better/worse?
- Approach:
 - Run experiments over many scheduling scenarios
 - Measure results with VPS metrics (AAMAS 05)

Results

- Distributed better than centralized
- ADOPT & DPOP better than SynchID & SynchBB
- Topology of agents has large impact on privacy
- Asynchrony improves privacy

Existing Metrics: Valuations of Possible States (VPS)

Possible states before optimizing $n = \{0, 1, 2, 3, 4, 5\}$

Possible states after optimizing $p = \{0,3,4\}$

Framework for quantitative metrics for privacy

- Assume agent A trying to infer private information about agent B
- The relationship between *n* and *p* can be used to measure privacy

Can we do better than centralized?





·Yes!

- DPOP and ADOPT performed best.
- All were better than centralized!

Critique of VPS Metrics (1)

No adversary/threat model

- Who is the adversary?
- What does the adversary do to gain information?
- What if he does something unexpected?

Critique of VPS Metrics (2)

- Aggregation of partial information obscures actual losses
 - Metrics aggregate pairwise results
 - E.g. average privacy loss of all pairs of agents
- Example:
 - All agents lose half their data
 - Half agents lose all their data
 - Result is the same!

New Metric : D|A



Consider only the Definitive harm D

 Adversary gains concrete information w/ probability 1

For a given Adversary A

> Stronger adversaries might gain more information

Private Information

	Valuation
Meeting AB	4
Meeting AC	1
Timeslot 0	2
Timeslot 1	4
Timeslot 2	0

	Valuation
Meeting AB	4
Timeslot 0	1
Timeslot 1	0
Timeslot 2	5

Alice's Private Data Bob's Private Data

	Valuation
Meeting AC	3
Timeslot 0	0
Timeslot 1	0
Timeslot 2	0

Carol's Private Data

For Alice, Bob, Carol

- How they value the meetings
- How they value their time
- 13 pieces total
- Corresponding to the 13 rows in the tables

How is information lost?



- Using DPOP algorithm
- Participants are organized into trees
- They send upward valuations for their subtrees

How is the Problem Solved?

Timeslot 0	Timeslot 1	Timeslot 2	Bob's Valuation
-	-	-	0
AB	-	-	3
-	AB	-	4
-	-	AB	-1

Bob builds a table with his utility for scheduling the meeting (AB) in each timeslot

- Bob's valuation is V(AB) V(timeslot)
- Row 2 is $V(AB) T_0$ or 4 1 = 3
- He sends the table to Alice and she optimizes
- We count as lost any data which the adversary determines with probability 1 (only one state remaining)

Results



	Valuation	
Meeting AB	4	
Meeting AC	1	
Timeslot 0	2	
Timeslot 1	4	
Timeslot 2	0	

	Valuation
Meeting AB	4
Timeslot 0	1
Timeslot 1	0
Timeslot 2	5

(a) Alice's Private Information

(b) Bob's private information

	Valuation
Meeting AC	3
Timeslot 0	0
Timeslot 1	0
Timeslot 2	0

(c) Carol's private information

- Bob and Carol lose all their information to Alice
- 8 pieces of personal information
- Out of 13 total pieces (Alice's 5 valuations are not revealed)
- So privacy loss is 8/13

New Example: Chain Topology



Only Carol loses her information

Privacy loss is 4/13

Metric in VPS Framework

$$\bigvee_{i} (\mathbb{P}_{i}(S_{i})) = \sum_{x=1}^{|s_{i}|} I_{\sum_{j \neq i} \sum_{t \in S(t_{x})} I_{\mathbb{P}_{i}^{j}(t)=1}}$$

 $\langle \alpha \rangle \rangle$

$$\frac{\sum_{\forall i} \mathbb{V}_i(\mathbb{P}_i(S_i))}{\sum_{\forall i} |s_i|}$$

- This function sums up all pieces of personal information known by any other participant j about participant i
- We then add up the results for each participant and divide by the total amount of personal data

A for Adversary:

But we still don't have a threat model

- Adversary could take many actions
 - 1. View messages sent to a single participant in the course of algorithm
 - 2. Run "StalkerPro" to do sophisticated inference
 - 3. Use outside domain knowledge
 - 4. Collude with other participants
 - 5. Actively manipulate the message stream
- Each action has a cost

A for Adversary

- If we can linearize this cost in risk/resources, we can get at the two dimensional plane
- Linearization can be hard to do
- But, it is important to do so to resolve the harm of partial information

D|A Conclusions

- Previous metrics don't capture intuitive notions of privacy loss
- Or contextualize it in a threat model
- Proposed D|A metric
 - Good for broad notions of privacy
 - Helping us design new algorithms
 - Still needs work on A side

Current and Future work: New algorithms

Approach :

- Use analysis to identify key features of algorithms for privacy
 - Topology
 - Asynchrony
- Design algorithms around these features
- Import ideas from anonymity and trust management literature

Current and Future Work: Dynamic DCOP

- Scheduling is inherently dynamic
 - New events constantly arise
- Expectation: more privacy loss
- Research Goals
 - quantify privacy loss in dynamic DCOP
 - evaluate privacy impact of different approaches

Goals of Dissertation

- Develop techniques to evaluate privacy in DCOP
- Understand how well existing algorithms protect privacy
- Quantify design tradeoffs between privacy, efficiency and optimality
- Design algorithms with more privacy than status quo

Example Results



See poster, DCR paper, or AAAI paper for additional results

Example : Alice's Schedule

Alice's Schedule

08:00 - 08:30 : Pay traffic ticket 09:00 - 11:00 : Workgroup meeting 12:00 - 13:30 : Lunch with clients 14:00 - 14:30 : Call lawyer about divorce settlement

15:00 - 17:30 : Job interview 17:30 - 18:00 : Pick up kids from after school program 19:00 - 19:30 : Pick up babysitter 20:00 - 00:00 : Hot date!

Alice has a busy schedule and would like to optimize it but she doesn't want all parties to know about all her time conflicts

DA in DPOP



Leaf nodes lose all their information 9/25 meeting valuations 35/70 timeslot valuations 45% privacy loss No single node can cletermine the internal nodes' valuations for certain



Trees with greater depth and less breadth produce more privacy and less efficiency

Nodes near the bottom of the tree lost more privacy than nodes at the top.

Asvnchronv



- Asynchrony improves privacy iff message origin is unknown
- Use anonymity techniques to hide message origins better
 - Without sacrificing too much efficiency?