Privacy Leakage of Search-based Multi-Agent Planning Algorithms

Abstract

Privacy-Preserving Multi-Agent Planning (PP-MAP) has recently gained the attention of the research community, resulting in a number of PP-MAP planners and theoretical works. Many such planners lack strong theoretical guarantees, thus in order to compare their abilities w.r.t. privacy, a versatile and practical metric is crucial. In this work, we propose such a metric, building on the existing theoretical work. We generalize and implement the approach in order to be applicable on real planning domains and provide an evaluation of state-of-the-art PP-MAP planners over the standard set of benchmarks. The evaluation shows that the proposed privacy leakage metric is able to provide comparison of PP-MAP planners and reveal important properties.

Introduction

Multi-agent planning (MAP) (Durfee 1999) comes in multiple flavors such as Dec-POMDPs (Oliehoek and Amato 2016) or Deterministic MAP (DMAP) (Brafman and Domshlak 2008; Torreño et al. 2017), each focusing on different aspects of MAP. One of the main rationales behind multi-agent planning is that the planning agents have a certain private knowledge necessary to solve the planning problem. The agents are not willing to share such information but they have to use it in order to be able to find a joint solution to the PP-MAP problem.

In recent years, a number of privacy preserving planning techniques have emerged, while in (Tožička, Štolba, and Komenda 2017) the authors have shown that for the most common MAP paradigms (including state-space search, such as MAFS (Nissim and Brafman 2014)) it is not possible to achieve complete (strong) privacy, efficiency, and completeness at the same time. This means that any practical privacy-preserving planner is essentially bound to leak some private information. In order to compare such planners in the context of privacy it is necessary to quantify such private information leakage.

In order to evaluate PP-MAP planners w.r.t. privacy, it is necessary to quantify private information leakage. A definition of privacy leakage metric has been addressed in two theoretical publications. The approach of (Van Der Krogt 2009) bases the leakage metric on the number of plans of an agent compatible with the communicated information, whereas the approach of (Štolba, Tožička, and Komenda 2017) (STK) uses the difference between the number of transition systems of the agent compatible with the information available to the adversary before and after the planning process. The former approach assumes the knowledge of the agent's problem and therefore can be used only by the agent itself. The latter is more general, as it is based purely on the knowledge available to the adversary. Both approaches were so far proposed only in theory.

Both mentioned works are theoretical and thus were never used to actually measure privacy leakage of a planning algorithm on a set of benchmarks. In this work, we fill this gap. We propose a generalized approach to privacy leakage quantification based on STK and implement it using an established MAP planning framework MAPlan (Fišer, Štolba, and Komenda 2015). We provide an evaluation of the MAFS (Nissim and Brafman 2014) and Secure-MAFS (Brafman 2015) planning algorithms on the CoDMAP (Štolba, Komenda, and Kovacs 2016) set of benchmarks and thoroughly compare the privacy properties of the mentioned algorithms.

Multi-Agent Planning

For a set of agents $\mathcal{A}$, a PP-MAP problem $\mathcal{M} = \{\Pi_i\}_{i=1}^{|\mathcal{A}|}$ is a set of agent problems, where for $\alpha_i \in \mathcal{A}$ agent problem is

$$\Pi_i = \left\langle \mathcal{V}_i = \mathcal{V}^{\mathsf{pub}} \cup \mathcal{V}^{\mathsf{priv}_i}, \mathcal{O}_i = \mathcal{O}^{\mathsf{pub}_i} \cup \mathcal{O}^{\mathsf{priv}_i}, s_I, s_\star \right\rangle,$$

where $\mathcal{V}_i$ is a set of variables s.t. each $V \in \mathcal{V}_i$ has a finite domain $\mathsf{dom}(V)$, $\mathcal{V}^{\mathsf{pub}}$ is the set of public variables (with all values public), common to all agents, and $\mathcal{V}^{\mathsf{priv}_i}$ is the set of variables private to α_i (with all values private), such that $\mathcal{V}^{\mathsf{pub}} \cap \mathcal{V}^{\mathsf{priv}_i} = \emptyset$ and $\mathcal{V}^{\mathsf{priv}_i} \cap \mathcal{V}^{\mathsf{priv}_j} = \emptyset$ for all $i \neq j$. A complete assignment over $\mathcal{V} = \mathcal{V}^{\mathsf{pub}} \cup \bigcup_{i=1}^{|\mathcal{A}|} \mathcal{V}^{\mathsf{priv}_i}$ is a *state*, partial assignment over $\mathcal{V}$ is a *partial state*.

The set $\mathcal{O}^i$ is a set of actions of α_i, $\mathcal{O}^{\mathsf{priv}_i}$ is a set of private actions and $\mathcal{O}^{\mathsf{pub}_i}$ is a set of public actions of α_i. The sets $\mathcal{O}^{\mathsf{pub}_i}$, $\mathcal{O}^{\mathsf{priv}_j}$ are pairwise disjoint for all i, j. An action is defined as $a = \langle \mathsf{pre}(a), \mathsf{eff}(a) \rangle$, where $\mathsf{pre}(a)$ and $\mathsf{eff}(a)$ are partial states over $\mathcal{V}_i$ representing the precondition and the effect respectively. An action a is public if

$\mathsf{vars}(\mathsf{pre}(a)) \cap \mathcal{V}^{\mathsf{pub}} \neq \emptyset$ or $\mathsf{vars}(\mathsf{eff}(a)) \cap \mathcal{V}^{\mathsf{pub}} \neq \emptyset$, otherwise a is private. A public action may also have private preconditions or effects.

We use $s[V]$ to denote the value of V in the (partial) state s, $s[\mathcal{V}']$ to denote the state s restricted to $\mathcal{V}' \subseteq \mathcal{V}_i$, and $\mathsf{vars}(s)$ to denote the set of variables with value defined in s. The state s_I is the initial state and $s_\star$ is a partial state representing the goal condition, i.e., s is a goal state iff $s_\star = s[\mathsf{vars}(s_\star)]$.

An action a is applicable in a state s if $s[\mathsf{vars}(\mathsf{pre}(a))] = \mathsf{pre}(a)$ and the application of a in s, denoted as $s' = a \circ s$ results in a state s' s.t. $s'[V] = \mathsf{eff}(a)[V]$ if $V \in \mathsf{vars}(\mathsf{eff}(a))$ and $s'[V] = s[V]$ otherwise.

The public projection of a (partial) state s is $s^\triangleright = s[\mathcal{V}^{\mathsf{pub}}]$. The public projection of an action $a \in \mathcal{O}^{\mathsf{pub}}$ is $a^\triangleright = \langle \mathsf{pre}(a)^\triangleright, \mathsf{eff}(a)^\triangleright \rangle$. The public projection of Π_i is

$$\Pi_i^\triangleright = \left\langle \mathcal{V}^{\mathsf{pub}}, \mathcal{O}_i^\triangleright = \{a^\triangleright | a \in \mathcal{O}^{\mathsf{pub}_i}\}, s_I^\triangleright, s_\star^\triangleright \right\rangle$$

The solution to Π_i is a sequence $\pi_i = (a_1, ..., a_k)$ of actions from $\mathcal{O}_i \cup \bigcup_{j \neq i} \mathcal{O}_j^\triangleright$, s.t. a_1 is applicable in $s_I = s_0$ and for each $1 \leq i \leq k$, a_i is applicable in s_{i-1} and $s_i = a_i \circ s_{i-1}$ and s_k is a goal state. We define $\pi^\triangleright = (a_1^\triangleright, ..., a_k^\triangleright)$ with all private actions omitted to be the public projection of π. The global solution to $\mathcal{M}$ is a set of plans $\{\pi_i\}_i^{|\mathcal{A}|}$ such that each π_i is a local solution to Π_i and all π_i agree on the public actions, formally $\pi_i^\triangleright = \pi_j^\triangleright$ for all i, j.

Privacy Leakage

Let us first state a number of assumptions we place on the agents and their interaction, as is usual in the Secure Multiparty Computation literature.

Semi-honest agents. The agents adhere to the algorithm and the communication protocol but try to infer as much private knowledge as possible.

Knowledge of the algorithm. The adversary knows the planning algorithm of the agent, but we do not assume any particular heuristic and thus the adversary does not exploit any information gained from the heuristic computation except for the heuristic value itself.

FIFO communication. Each communication channel between a pair of agents is first-in, first-out, i.e., the messages are received in the order they were sent.

Publicly known bounds. We assume that there are publicly known bounds on the size of the agent's problem, in particular, $|\mathcal{V}^{\mathsf{priv}}| \leq p$ and $|\mathsf{dom}(V)| \leq d$ for all $V \in \mathcal{V}^{\mathsf{priv}}$.

Colluding adversaries. We refer to the agent trying to hide information as agent $\alpha = \alpha_i$ for some i (the agent). We model all other agents as a single agent (the adversary), which is common in Secure Multiparty Computation, as all the agents can collude and combine their knowledge in order to infer more private information. We omit the index i when referring to the agent in a clear context.

We adopt (and later generalize) the leakage metric of STK, which is itself based on (Smith 2009), as follows. First, it is important to understand what information is the adversary given and what additional information it obtains through the planning process. The a priori information is a tuple $I_{\mathsf{apriori}} = \langle \Pi^\triangleright, \pi^\triangleright, p, b \rangle$ where $\Pi^\triangleright$ is the public projection of the problem and $\pi^\triangleright$ of the solution plan, p and b are the publicly known bounds on the number of private variables and on the size of private variable domains respectively.

The information obtained by the adversary is a sequence of messages exchanged between the agents $M = (m_1, ..., m_k)$. The posterior information, that is, the additional information available to the adversary after the execution of the planning process, is a tuple $I_{\mathsf{post}} = \langle \Pi^\triangleright, \pi^\triangleright, p, b, M \rangle$.

Based on STK in order to quantify the information, we associate the a priori information I_{apriori} with a random variable H representing the uncertainty of the adversary about the agent's input of the planning algorithm (i.e., the problem Π_α and the respective transition system $\mathcal{T}(\Pi_\alpha)$. We denote t_{apriori} the number of transition systems compatible with I_{apriori}. Assuming uniform distribution of the inputs the probability of any particular transition system being the input of α is $1/t_{\mathsf{apriori}}$. Converting to an information measure ((Smith 2009) uses min-entropy) yields $\log \frac{1}{P(H)} = \log t_{\mathsf{apriori}}$, where $\log$ represents base-2 logarithm.

Similarly, we associate the public output, i.e., the communicated messages with a random variable L representing the new observed data. The conditional probability $P(H|L)$ then corresponds to the probability of a transition system being the hidden input with respect to all available information I_{post}. The respective information measure is then conditional min-entropy $\log \frac{1}{P(H|L)} = \log t_{\mathsf{post}}$

The final information leakage is computed as

$$\log t_{\mathsf{apriori}} - \log t_{\mathsf{post}}$$

where t_{apriori} is the number of transition systems compatible with I_{apriori} and t_{post} is the number of transition systems compatible with I_{post}.

By observing that each action contributes to the number of possible transition systems independently, we can focus on the number of transition systems represented by each individual action t^a and compute the number of transition system as

$$t = \prod_{a^\triangleright \in \mathcal{O}^\triangleright} t^a \tag{1}$$

For a single variable with domain size d, the projected action $a^\triangleright \in \mathcal{O}^\triangleright$ represents any possible subset of d^2 transitions, that is at most $2^{d^2} - 1$ possibilities. The transition system where $a^\triangleright$ is applicable in no value(s) of a variable is not possible as we assume that $a^\triangleright$ represents a non-empty transition system. All possible combinations of p independent private variables result in $t^a = (2^{d^2} - 1)^p$ possibilities. Transition systems with multiple effects are possible because multiple actions can be represented by a single projected action.

Let us now define and generalize sources of private information leakage based on the properties of actions, originally introduced by STK. A single projected action $a^\triangleright \in \mathcal{O}^\triangleright$ represents all actions $a_k \in \mathcal{O}^{\mathsf{pub}}$ such that $a_k[\mathcal{V}^{\mathsf{pub}}] = a^\triangleright$, as in Figure 1. We define the set $\mathcal{O}_a^\triangleright = \{a' \in \mathcal{O}^{\mathsf{pub}} | a^\triangleright = a'^\triangleright\}$

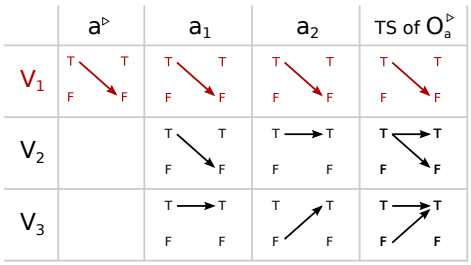

Figure 1: Example of public projection and related transition systems. $\mathcal{V}^{\mathsf{pub}} = \{V_1\}, \mathcal{V}^{\mathsf{priv}} = \{V_2, V_3\}$, all variables are binary. Left, $a^{\triangleright}$ shows the public transition system, $a_1, a_2 \in \mathcal{O}^{\triangleright}_a$ are the actions with equal public projections and their individual transition systems. Right $a^{\triangleright}$ shows the full transition system composed of transition systems of both a_1 and a_2.

as the set of actions for which $a^{\triangleright}$ is the public projection. We define properties of $a^{\triangleright}$ as follows.

Definition 1. Let $a^{\triangleright} \in \mathcal{O}^{\triangleright}$, we say $a^{\triangleright}$ is

Init-applicable (ia) if for all $V \in \mathcal{V}^{\mathsf{priv}}$ there exists $a \in \mathcal{O}^{\triangleright}_a$, $\mathsf{pre}(a)[V] = s_I[V]$.

Not-init-applicable (nia) if for all $V \in \mathcal{V}^{\mathsf{priv}}$ there is no $a \in \mathcal{O}^{\triangleright}_a$ such that $\mathsf{pre}(a)[V] = s_I[V]$.

Privately-independent (pi) if there exist $V \in \mathcal{V}^{\mathsf{priv}}$ and $a \in \mathcal{O}^{\triangleright}_a$ such that $V \notin \mathsf{vars}(\mathsf{pre}(a))$, or for all values $v \in \mathsf{dom}(V)$ there is some $a' \in \mathcal{O}^{\triangleright}_a$ such that $v = \mathsf{pre}(a')[V]$.

Privately-dependent (pd) if there exist $V \in \mathcal{V}^{\mathsf{priv}}$ and $a \in \mathcal{O}^{\triangleright}_a$ such that $V \in \mathsf{vars}(\mathsf{pre}(a))$ and there exists some value $v \in \mathsf{dom}(V)$ such that $v \neq \mathsf{pre}(a')[V]$ for all $a' \in \mathcal{O}^{\triangleright}_a$.

Privately-nondeterministic (pn) if there exist $V \in \mathcal{V}^{\mathsf{priv}}$ and $a, a' \in \mathcal{O}^{\triangleright}_a$ such that $V \in \mathsf{vars}(\mathsf{eff}(a)) \wedge V \in \mathsf{vars}(\mathsf{eff}(a'))$ and $\mathsf{eff}(a)[V] \neq \mathsf{eff}(a')[V]$.

Informally, an action is init-applicable in V if it is applicable in the initial state (where the value of V is not known but fixed to some v_0). An action is privately-independent in V if it is applicable on a state regardless of the value of V, privately-dependent if it is applicable only for some values of V and not applicable for some other values of V. Finally, an action is privately-nondeterministic if its application can result in two different values of V.

According to Definition 1, the example action in Figure 1 is ia, pd, pn in V_2 and ia, pi in V_3. WLOG we can assume that $s_I[V_2] = T$ and $s_I[V_3] = T$. Moreover, $a^{\triangleright}$ is pi in V_3 because $\mathsf{pre}(a_1)[V_3] = T$ and $\mathsf{pre}(a_2)[V_3] = F$, pd in V_2 because $\mathsf{pre}(a_1)[V_2] = T$ and $\mathsf{pre}(a_2)[V_2] \neq F$. Finally, $a^{\triangleright}$ is pn in V_3 because $\mathsf{eff}(a_1)[V_3] \neq \mathsf{eff}(a_2)[V_3]$.

Leakage of Search-Based Algorithms

MAFS is an adaptation of classical heuristic forward-search to the multi-agent setting. Each agent $\alpha_i \in \mathcal{A}$ expands its search space defined over the variables in $\mathcal{V}_i$. The agent α_i expands a state s using all applicable actions in $\mathcal{O}_i$. If s is expanded using $a \in \mathcal{O}^{\mathsf{priv}_i}$, the resulting state $s' = a \circ s$ is added only to the open list of agent α_i as it has changed only in private variables $\mathcal{V}^{\mathsf{priv}_i}$. If s is expanded using $a \in \mathcal{O}^{\mathsf{pub}_i}$, the resulting state $s' = a \circ s$ is sent to (all) other agents, as it may influence their search. In order to keep information private, only the public projection $s'^{\triangleright}$ is sent to other agents. Nevertheless, in order to be able to reconstruct the private parts of received states, each agent α_i must include some reference to the i-parent state, defined as follows.

Definition 2. Let s, s', s'' be states defined over $\mathcal{V}_i$ in the search space of agent $\alpha_i \in \mathcal{A}$ such that $s' = a_0 \circ s$ where $a_0 \in \mathcal{O}^{\mathsf{pub}_i}$ and s'' is the result of application of a sequence $(a_1, ..., a_k)$ on s', where for all $a_2, ..., a_{k-1} \notin \mathcal{O}_i$. We say, that s' is the ***i*-parent** of s''.

Informally, the i-parent of s'' is the last state s' expanded by α_i on the path leading to s''. In order to reconstruct the private part $s''[\mathcal{V}^{\mathsf{priv}_i}]$ of the state s'', the agent α_i needs to know the i-parent state s' (or, at least, its private part). Let S^i be the state space of agent α_i, we define $\delta_i : S^i \to \mathbb{N}$ as the function assigning an agent-specific identifier (id) to each state $s \in S^i$. The $\delta_i(s)$ for each agent is sent as part of each state message $m = \langle s^{\triangleright}, \delta_1(s), ..., \delta_n(s) \rangle$ where $s^{\triangleright}$ is a public projection of the sent or received state and $\delta_1, ..., \delta_n$ are the id functions representing $s[\mathcal{V}^{\mathsf{priv}_i}]$ for each $i \in 1, ..., n$. In order to be complete, it must hold $\delta_i(s) \neq \delta_i(s')$ if $s[\mathcal{V}^{\mathsf{priv}_i}] \neq s'[\mathcal{V}^{\mathsf{priv}_i}]$ for each agent, otherwise the agent would not be able to reconstruct the correct private part.

The message m might also contain the global heuristic value h or projected heuristic value $h^{\triangleright}$ computed by the sending agent and the g value determining the cost for getting from s_I to s. The projected heuristic is $h^{\triangleright}$ is computed by each agent α_i on Π_i separately, thus the computation itself leaks no information and the resulting value depends only on the problem of agent α_i. In contrast, the global heuristic is computed in a distributed way with all agents participating. We assume that the global heuristic is privacy-preserving, such as MA-Pot (Štolba, Fišer, and Komenda 2016), and therefore the computation itself leaks no private information as well.

The adversary agent cannot observe the global search tree as it includes private actions of the agent and when receiving a state, the adversary has no information about the action applied by the agent. The adversary can easily encode the id of the i-parent state in the communication by setting $\delta_i(s)$ to a unique id of the state s. When the adversary receives $m = \langle s^{\triangleright}, \delta_1(s), ..., \delta_n(s) \rangle$ the information in $\delta_i(s)$ encodes exactly the i-parent.

Another crucial information the adversary needs to determine is whether two states s, s' such that $s^{\triangleright} = s'^{\triangleright}$ received from the agent are in fact two different states.

Definition 3. Let s, s' be two states. We say that s, s' are **publicly equivalent but different** (PEBD) if $s^{\triangleright} = s'^{\triangleright} \wedge s \neq s'$. We use $s \triangleq s'$ to denote PEBD states s, s'.

As proposed by STK, the PEBD states can be determined based on g and h values and the sets of successor states. Let α_i be the agent and all other agents the colluding adversaries.

Proposition 4. *(STK, generalized for $|\mathcal{A}| > 2$) Let s, s' be states s.t. $s^{\triangleright} = s'^{\triangleright}$. Let h, g be the heuristic function and*

g the cost function. If $s[V^{\mathsf{priv}_j}] = s[V^{\mathsf{priv}_j}]$ *for all* $j \neq i$ *and* $h(s) \neq h(s') \vee g(s) \neq g(s')$ *then* $s \triangleq s'$.

We introduce a new proposition which is applicable when the agents use a projected heuristic computation.

Proposition 5. *Let* s, s' *be states s.t.* $s^{\triangleright} = s'^{\triangleright}$. *Let* $h^{\triangleright}$ *be a projected heuristic function computed by the agent* α_i. *If* $h^{\triangleright}(s) \neq h^{\triangleright}(s')$ *then* $s \triangleq s'$.

Proof. Trivial as $h^{\triangleright}$ depends only on Π_i and therefore if $h^{\triangleright}(s) \neq h^{\triangleright}(s')$ it must hold that $s[\mathcal{V}_i] \neq s'[\mathcal{V}_i]$. □

Finally, for each transition in the reconstructed search tree, the adversary needs to determine the actions possibly responsible for the transition. Let s, s' be two states such that s is the i-parent of s'. We define $\mathcal{O}^{\mathsf{com}} \subseteq \mathcal{O}^{\triangleright}$ as the set of all actions compatible with the public projections $s^{\triangleright}, s'^{\triangleright}$, formally for all $a^{\triangleright} \in \mathcal{O}^{\mathsf{com}}$ holds $\mathsf{pre}(a^{\triangleright})[V] = s^{\triangleright}[V]$ for all $V \in \mathsf{vars}(\mathsf{pre}(a^{\triangleright}))$ and $\mathsf{eff}(a^{\triangleright})[V] = s'^{\triangleright}[V]$ for all $V \in \mathsf{vars}(\mathsf{eff}(a^{\triangleright}))$.

Based on all the above information, the colluding adversary agents build the reconstructed search tree structure. Let α_i be the agent and all other agents the colluding adversaries. The reconstructed search tree is formally defined as follows.

Definition 6. The search tree is defined as a tuple $\mathsf{ST} = \langle S_{\mathsf{rec}}, S_{\mathsf{sen}}, S_I, ip, ipa, E_{\mathsf{rec}}, E_{\mathsf{sen}}, h, g \rangle$ where

- $S_{\mathsf{rec}}, S_{\mathsf{sen}}$ is the set of public states $s^{\triangleright}$ received from the agent α_i and sent to the agent α_i respectively.
- S_I is the set of public states $s^{\triangleright}$ such that s is reachable from s_I without using actions of the agent α_i.
- $ip : S_{\mathsf{rec}} \cup \{s_I^{\triangleright}\} \to S_{\mathsf{sen}}$ assigns to each received state $s^{\triangleright}$ its i-parent $s'^{\triangleright}$.
- $ipa : \mathcal{O}^{\triangleright} \to 2^{S_{\mathsf{rec}}}$ assigns to each action $a^{\triangleright} \in \mathcal{O}^{\triangleright}$ of the agent the set of received states such that $a^{\triangleright}$ is possibly responsible for the transition.
- $E_{\mathsf{rec}} \subseteq S_{\mathsf{rec}} \times S_{\mathsf{rec}}$ and $E_{\mathsf{sen}} \subseteq S_{\mathsf{sen}} \times S_{\mathsf{sen}}$ are partial PEBD relations on received and sent states respectively, based on I_{post} and the above propositions.
- h, g are the heuristic and cost functions for each state. Alternatively $h^{\triangleright}$ represents the projected heuristic function received from the agent.

Note that the search tree can be reliably reconstructed only up to the last state for which all successors were received. Based on the reconstructed search tree and Definition 1 the adversary constructs a function

$$\varpi : 2^{\mathcal{O}^{\triangleright}} \to 2^{\{\mathsf{ia},\mathsf{nia},\mathsf{pi},\mathsf{pd},\mathsf{pn}\}} \tag{2}$$

which assigns a set of properties to a set of actions, such that for at least one of the actions all the properties hold.

Detecting the Sources of leakage

Let us now focus on how to determine the properties defined in Definition 1 based on the reconstructed search tree in Definition 6. We use s for $s^{\triangleright}$ in the following algorithm descriptions to simplify the notation.

Init-applicable Let $a^{\triangleright} \in \mathcal{O}^{\triangleright}$ such that there exists $s \in ipa(a^{\triangleright})$ for which $s_I = ip(s)$. Then $a^{\triangleright}$ is init-applicable. If there is no such $s \in ipa(a^{\triangleright})$, $a^{\triangleright}$ is not-init-applicable.

Privately-independent Among all transitions in ST a particular action is responsible for, we need to find those where the transitions originate in two PEBD states. We use the following algorithm:

1. Let $\mathcal{O}_s^{\triangleright} = \emptyset$ for each $s \in S_{\mathsf{rec}}$ denote the subset of actions responsible for the transition from $ip(s)$ to s identified to be privately-independent.
2. For each $a^{\triangleright} \in \mathcal{O}^{\triangleright}$ and for each $s_1, s_2 \in ipa(a^{\triangleright})$ such that $s_1 \neq s_2$
   (a) $s_1' = ip(s_1), s_2' = ip(s_2)$
   (b) If $(s_1', s_2') \in E_{\mathsf{sen}}$, add the action $a^{\triangleright}$ to both $\mathcal{O}_{s_1}^{\triangleright}, \mathcal{O}_{s_2}^{\triangleright}$.
3. For each $s \in S_{\mathsf{rec}}$, at least one action $a^{\triangleright} \in \mathcal{O}_s^{\triangleright}$ is privately-independent.

Privately-dependent For each transition from s to s' in ST a particular action $a^{\triangleright} \in \mathcal{O}^{\triangleright}$ is responsible for, we need to determine whether $a^{\triangleright}$ is responsible also for all transition from states s'' such that $(s, s'') \in E_{\mathsf{sen}}$. We use the following algorithm:

1. Let $\mathcal{O}_s^{\triangleright} = \emptyset$ for each $s \in S_{\mathsf{rec}}$ denote the subset of actions responsible for the transition from $ip(s)$ to s identified to be privately-dependent.
2. For each $a^{\triangleright} \in \mathcal{O}^{\triangleright}$, for each $s_1 \in ipa(a^{\triangleright})$ and for each PBED state s_2 s.t. $(ip(s_1), s_2) \in E_{\mathsf{sen}}$
   (a) If there is no $s_3 \in ipa(a^{\triangleright})$ such that $ip(s_3) = s_2$, add action $a^{\triangleright}$ to $\mathcal{O}_{s_1}^{\triangleright}$.
3. For each $s \in S_{\mathsf{rec}}$, at least one action of $a^{\triangleright} \in \mathcal{O}_s^{\triangleright}$ is privately-dependent.

Privately-nondeterministic Among all transitions in ST a particular action is responsible for, we need to find those where the transitions originate in the same state, but results in two PEBD states. We use the following algorithm:

1. Let $\mathcal{O}_s^{\triangleright} = \emptyset$ for each $s \in S_{\mathsf{sen}}$ denote the subset of actions responsible for the transition from $ip(s)$ to s identified to be privately-nondeterministic.
2. For each $a^{\triangleright} \in \mathcal{O}^{\triangleright}$ and for each $s_1, s_2 \in ipa(a^{\triangleright})$ such that $(s_1, s_2) \in E_{\mathsf{rec}}$ and $s' = ip(s_1) = ip(s_2)$,
   (a) add action $a^{\triangleright}$ to $\mathcal{O}_{s'}^{\triangleright}$.
3. For each $s \in S_{\mathsf{sen}}$, at least one action of $a^{\triangleright} \in \mathcal{O}_s^{\triangleright}$ is privately-nondeterministic.

Computing the Privacy Leakage

The next step is to use the reconstructed search tree to compute the actual number of transition systems compatible with the received messages and, eventually, to compute the leakage estimate. Based on Equation 1 we first compute the number of transition systems represented by a combination of the properties from Definition 1. As by ϖ the properties are assigned to, we construct a linear program (LP) in order to best utilize the obtained knowledge.

Transition Systems of an Action

In contrast to STK, we introduce a novel general approach to compute the number of transition systems represented by a given set $X \in 2^{\{\mathsf{ia},\mathsf{nia},\mathsf{pi},\mathsf{pd},\mathsf{pn}\}}$ of properties. To do so, we introduce a number of first-order logic formulas which describe the properties of actions related to privacy leakage. For each $V \in \mathcal{V}^{\mathsf{priv}}$, and each $v \in \mathsf{dom}(V)$, we define the first order logic propositions $\mathsf{pre}_{V=v}$ and $\mathsf{eff}_{V=v}$. The semantics of $\mathsf{pre}_{V=v} = \mathsf{true}$ is that for some $a \in \mathcal{O}_a^{\triangleright}$, $\mathsf{pre}(a)[V] = v$ and of $\mathsf{pre}_{V=v} = \mathsf{false}$ is that for all $a \in \mathcal{O}_a^{\triangleright}$, $\mathsf{pre}(a)[V] \neq v$, analogously $\mathsf{eff}_{V=v}$ for effects.

Subsequently, we can express the properties defined in Definition 1 using the following formulas. Let $a^{\triangleright} \in \mathcal{O}^{\triangleright}$, $V \in \mathcal{V}^{\mathsf{priv}}$, and $v_0 \in \mathsf{dom}(V)$ is some fixed value of V, then

$$\mathsf{ia} = \bigwedge_{V \in \mathcal{V}^{\mathsf{priv}}} \mathsf{pre}_{V=v_0}$$

$$\mathsf{nia} = \bigvee_{V \in \mathcal{V}^{\mathsf{priv}}} \neg\mathsf{pre}_{V=v_0}$$

$$\mathsf{pi} = \bigvee_{V \in \mathcal{V}^{\mathsf{priv}}} \Big(\bigwedge_{v \in \mathsf{dom}(V)} \mathsf{pre}_{V=v} \Big)$$

$$\mathsf{pd} = \bigvee_{V \in \mathcal{V}^{\mathsf{priv}}} \Big(\bigvee_{v \in \mathsf{dom}(V)} \mathsf{pre}_{V=v} \wedge \bigvee_{v \in \mathsf{dom}(V)} \neg\mathsf{pre}_{V=v} \Big)$$

$$\mathsf{pn} = \bigvee_{V \in \mathcal{V}^{\mathsf{priv}}} \Big(\bigvee_{v \neq v' \in \mathsf{dom}(V)} (\mathsf{eff}_{V=v} \wedge \mathsf{eff}_{V=v'}) \Big)$$

Combinations of properties can be obtained by conjunction, e.g., $\mathsf{ia} \wedge \mathsf{pi}$ for init-applicable and privately-independent.

The next step is to compute the number of possible transition systems t^X w.r.t. the set of properties X. Let $\bar{\lambda}_X = \bigwedge_{x \in X} x$ denote the conjunction of the formulas respective to the properties in X. Let M be the set of all models of the formula $\bar{\lambda}_X$. For each $V \in \mathcal{V}^{\mathsf{priv}}$ and $v \in V$, the model $m \in M$ either assigns $\mathsf{pre}_{V=v} = \mathsf{true}$, $\mathsf{pre}_{V=v} = \mathsf{false}$, or $\mathsf{pre}_{V=v}$ is not in $\bar{\lambda}_X$ and therefore m assigns no value to $\mathsf{pre}_{V=v}$. The same holds for $\mathsf{eff}_{V=v}$. For each variable $V \in \mathcal{V}^{\mathsf{priv}}$, we define the set $P_V^+ = \{\mathsf{pre}_{V=v} | v \in \mathsf{dom}(V), \mathsf{pre}_{V=v} = \mathsf{true}\}$ of positive propositions and P_V^{free} the set of unassigned propositions (analogously E_V^+ , and E_V^{free} for effects). Let $p^{\mathsf{free}} = |P_V^{\mathsf{free}}|, p^+ = |P_V^+|$ and e^{free}, e^+ analogously.

If $p^+ = 0$ and $e^+ = 0$, $t^{\emptyset} = (2^{d^2} - 1)^p$ as by STK. Otherwise, let us first fix a subset of $k' \leq p^{\mathsf{free}}$ propositions to be $\mathsf{pre}^a_{V=v} = \mathsf{true}$ and a subset of $l' \leq e^{\mathsf{free}}$ propositions to be $\mathsf{eff}^a_{V=v} = \mathsf{true}$, all other free propositions are fixed to be false.

This way we arrive at a fixed number of true preconditions and true effects, in particular $k = p^+ + k'$ and $l = e^+ + l'$. The number of possible transition systems for such configuration is equal to the number of bipartite graphs with partitions of size k and l such that each of the nodes has a degree ≥ 1 (all nodes are connected). There is $(2^k - 1)^l$ of all bipartite graphs and $(2^{k-j} - 1)^l$ bipartite graphs which do not use j particular fixed nodes. We can use this number in the inclusion-exclusion principle and arrive at

$$ts(k, l) = \sum_{j=0}^{k} (-1)^k \binom{k}{j} (2^{k-j} - 1)^l$$

Moreover, we care not only about the number of true preconditions and effects, but also about their identity, therefore we need to consider all possible choices of k' and l' propositions. The final number of transition systems for action for which the set X of properties holds is

$$t^X = \sum_{k'=0}^{k'=p^{\mathsf{free}}} \sum_{l'=0}^{l'=e^{\mathsf{free}}} \binom{p^{\mathsf{free}}}{k'} \binom{e^{\mathsf{free}}}{l'} ts(p^+ + k', e^+ + l')$$

In order to exclude the empty transition system, if $p^+ = 0$ then k' starts from 1 instead of 0 and if $e^+ = 0$ then l' starts from 1 instead of 0.

Total Number of Transition Systems

For each $a^{\triangleright} \in \mathcal{O}^{\triangleright}$, let the number of transition systems represented by $a^{\triangleright}$ before the algorithm is executed be denoted by $\tau_{\mathsf{apriori}}(a^{\triangleright})$ and the number of transition systems represented by $a^{\triangleright}$ after the algorithm is executed be denoted by $\tau_{\mathsf{post}}(a^{\triangleright})$. In this section, we focus on the computation of $\tau_{\mathsf{post}}(a^{\triangleright})$, the computation of $\tau_{\mathsf{apriori}}(a^{\triangleright})$ is analogous.

Let $\mathcal{O}^X \subseteq \mathcal{O}^{\triangleright}$ denote a set of actions for which the set X of properties holds, as deduced from the search tree reconstruction. We know that for at least one $a^{\triangleright} \in \mathcal{O}^X$, X holds, but we do not know which one is it. Now consider an action $a^{\triangleright}$ such that $a^{\triangleright} \in \mathcal{O}^X$ and $a^{\triangleright} \in \mathcal{O}^{X'}$ where $X \neq X'$, how do we best (optimally) determine the number of transition systems $\tau_{\mathsf{post}}(a^{\triangleright})$ in the presence of such information?

We pose the problem as a combinatorial optimization problem and solve it using LP. In order to formulate an LP, we define an LP variable $\bar{a}$ for each action $a^{\triangleright} \in \mathcal{O}^{\triangleright}$. The variable $\bar{a}$ represents the logarithm of $\tau_{\mathsf{post}}(a^{\triangleright})$ ($\bar{a} = \log \tau_{\mathsf{post}}(a^{\triangleright})$). Logarithm can be applied to both sides of an inequality as we use logarithm with base > 1. This way, we can use a sum variant of Equation 1, $\sum_{a^{\triangleright} \in \mathcal{O}^{\triangleright}} \tau_{\mathsf{post}}(a^{\triangleright})$. Each LP variable $\bar{a}$ is bounded by $1 \leq \bar{a} \leq \log t^{\emptyset}$. We formulate the following objective function to be maximized:

$$\mathsf{Maximize} \sum_{a^{\triangleright} \in \mathcal{O}^{\triangleright}} \bar{a}$$

resulting in the logarithm of Equation 1. For each $\mathcal{O}^X \subseteq \mathcal{O}^{\triangleright}$ we formulate a disjunctive constraint:

$$\bigvee_{a^{\triangleright} \in \mathcal{O}^{X'}} (\bar{a} \leq \log t^X)$$

For example if there is a set of actions $\{a_1^{\triangleright}, a_2^{\triangleright}, a_3^{\triangleright}\}$ and we know that at least one of the actions is privately-independent the disjunctive constraint is:

$$\bar{a_1} \leq \log t^{\{\mathsf{pi}\}} \vee \bar{a_2} \leq \log t^{\{\mathsf{pi}\}} \vee \bar{a_3} \leq \log t^{\{\mathsf{pi}\}}$$

Such a disjunctive formulation can either be directly solved by a branch-and-bound algorithm or transformed to mixed-integer linear program (MILP) by using the Big-M reformulation. In order to do so, for each constraint in the disjunction we define a binary variable, e.g., $y_1, y_2, y_3 \in \{0, 1\}$,

and enforce that only one of them holds true by

$$y_1 + y_2 + y_3 = 1$$

Then we define a large enough constant M and reformulate the above disjunction as

$$\bar{a_1} \leq \log t^{\{\mathsf{pi}\}} + M(1 - y_1)$$
$$\bar{a_2} \leq \log t^{\{\mathsf{pi}\}} + M(1 - y_2)$$
$$\bar{a_3} \leq \log t^{\{\mathsf{pi}\}} + M(1 - y_3)$$

which significantly expands all but one of the bounds, thus rendering them ineffective. Such transformation then allows to use a standard solver with MILP capabilities, such as the IBM CPLEX.

Handling Complexity

Although general enough, the described computation of leakage is not tractable for practical use on realistically large problems, such as the CoDMAP benchmarks. The most demanding operations are the finding of PEBD states and determining the number of transition systems t^X based on the set X of properties.

The PEBD states computation is $O(|S_{\mathsf{rec}}|^2)$, i.e., quadratic in the number of received states, as we need to test each state against each other state. Moreover, the number of received states can be up to the number of states expanded by the agent α, as in the case where all actions are public, every expanded state is also sent to all other agents.

The computation of t^X is even worse as we need to find all models of the formula $\bar{\lambda}_X$. Let $\mathsf{vars}(\bar{\lambda}_X)$ denote the number of propositional variables in $\bar{\lambda}_X$, then finding all valuations of $\bar{\lambda}_X$ is $O(2^{\mathsf{vars}(\bar{\lambda}_X)})$ and $\mathsf{vars}(\bar{\lambda}_X)$ can be as large as $p \cdot d$, therefore the complexity is $O(2^{pd})$. That said, the values are problem-independent and thus can be pre-computed just once and stored in a table. Still, the complexity is forbidding for larger values of p and d.

In order to be able to run the analysis on the actual CoDMAP domains, we need to simplify the privacy leakage estimate computation. First, notice that the full set E_{rec} of PEBD states over the received states is used only in the computation of privately-dependent actions. Therefore, we remove the computation of privately-dependent actions from the analysis and thus we can skip the pre-computation of all PEBD states. Instead, we test the states on PEBD equivalence only when needed.

The computation of t^X is a bigger challenge. We use the pre-computed values for small values of p and d which are stored in the form of $\log t^X$. Notice, that for $t^{\emptyset} = (2^d - 1)^p$ the value $\log t^{\emptyset} = p(2^d - 1)$ can be easily computed for any (positive) p, d. We use this value to extrapolate also for all other X as $\log t^X = k_X p(2^d - 1)$ where k is a X-dependent constant extrapolated from the exactly computed values.

Evaluation

We demonstrate the ability of the proposed leakage quantification metric to be used to compare privacy-preserving planners. In order to compare various planners on various domains we do not compare the absolute value of the leakage (that is, the leaked bits of information), but a ratio of the leakage of the particular algorithm to the ground truth leakage. The ground truth leakage is computed the same way as the leakage of the algorithm, but with action properties derived directly from the private information of the agent. Similarly, the upper bounds on $p = |\mathcal{V}^{\mathsf{priv}}|$ and d are computed directly from the private problem description, where $d = \max_{V \in \mathcal{V}^{\mathsf{priv}}} |\mathsf{dom}(V)|$.

Implementation

We have modified the MAPlan planner to a) print out sent and received states, b) enable the ϵ-MAFS search. The leakage analysis was implemented in Python using SymPy[1] and PuLP[2]. The upper bounds on $p = |\mathcal{V}^{\mathsf{priv}}|$ and d necessary for the computation are computed directly from the private problem description, where $d = \max_{V \in \mathcal{V}^{\mathsf{priv}}} |\mathsf{dom}(V)|$. We have used the pre-computed values of $\log t^X$ for small values of p, d and simplified extrapolations for large values, as described in the previous section.

We have evaluated the following planner configurations:

MAFS Plain MAFS as implemented in MAPlan, using A* search and MA-LM-Cut distributed heuristic (Štolba, Fišer, and Komenda 2015) **(dist)** and projected LM-Cut heuristic (Helmert and Domshlak 2009) **(proj)**.

Secure-MAFS As Secure-MAFS is not implemented in MAPlan, we have simulated its execution post-hoc by removing the states which would not be sent. We evaluate variants with the distributed **(dist)** and projected **(proj)** LM-Cut heuristic.

We have set the planning memory limit to 512MB and time limit to 15 minutes. Note that it is not necessary for the planner to find a plan in order to perform the leakage evaluation (only the final plan $\pi^{\triangleright}$ cannot be used in that case). As the leakage evaluation runtime and memory consumption is relatively high w.r.t. the number of received states, such limits are reasonable.

Benchmarks

The evaluation is based on the planning domains used in the CoDMAP (Komenda, Stolba, and Kovacs 2016) competition. Moreover, we have implemented a domain named UAVs which was used by STK as a running example. The simplest problem is shown in Figure 3. The planning task is to visit the locations while refueling at a base where the UAV operator and base are agents and the private information is the visited location and state of supplies respectively. We have constructed 5 problems with increasing number of locations and UAVs.

Comparison of the Search Algorithms

Table 1 shows an IPC-score-like evaluation of the leakage ratio, where the leakage ratio is summed over all problems in the domain for each planner configuration. The table clearly

[1] http://www.sympy.org

[2] https://pythonhosted.org/PuLP/

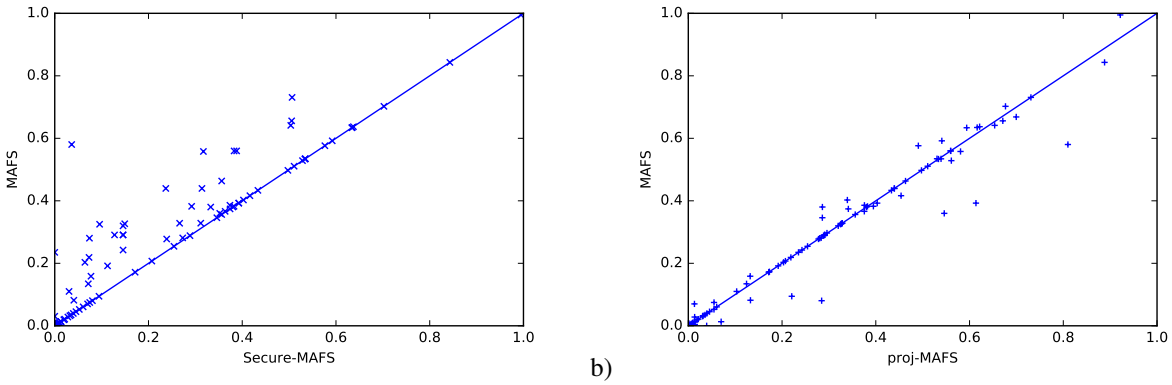

Figure 2: Detailed leakage ratio comparison, MAFS vs. Secure-MAFS (a) and MAFS vs. MAFS with projected heuristic (b).

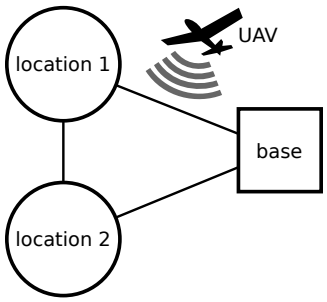

Figure 3: The UAV domain.

search	MAFS		Secure-MAFS	
heuristic	dist.	proj.	dist.	proj.
blocksworld	*5.18*	**4.85**	*5.18*	**4.85**
depot	**0.08**	*0.13*	**0.08**	*0.13*
driverlog	0.17	0.17	0.17	0.17
elevators	3.37	*3.40*	**3.35**	3.38
logistics	5.82	*6.14*	**5.44**	5.75
rovers	*3.76*	3.72	2.78	**2.76**
satellites	*3.10*	*3.10*	**1.96**	**1.96**
sokoban	**0.05**	*0.06*	**0.05**	*0.06*
woodwork.	0.00	0.00	0.00	0.00
taxi	0.00	0.00	0.00	0.00
wireless	0.19	0.19	0.19	0.19
zenotravel	3.04	*3.16*	**1.87**	2.03
uav	2.92	*3.14*	**2.30**	2.52
sum	27.69	*28.04*	**23.38**	23.78

Table 1: Comparison of search algorithms. Minimal leakage in bold, maximal in italics.

shows that the use of Secure-MAFS decreases privacy leakage, which has already been suggested by STK, but here, we present a quantified result. Moreover, the results show that the use of projected heuristic significantly increases privacy leakage in some domains as Proposition 5 can be used to discern PEBD states. For comparison, the Figure 4 shows the absolute values of leaked private information in bits averaged per domain for each planner configuration.

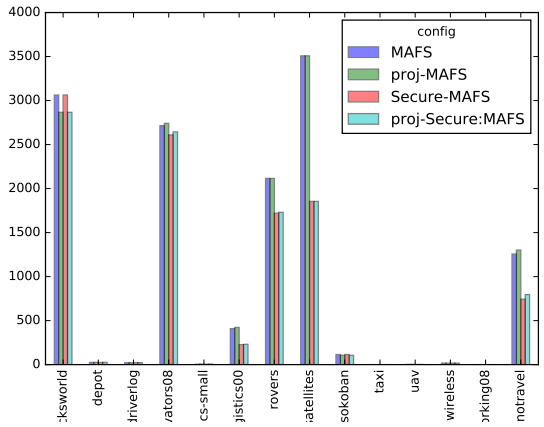

Figure 4: Absolute values of privacy leakage in bits of information averaged per domain.

Figure 2 provides a more detailed comparison of the leakage ratios per problem. Again, in some problems, the proposed privacy leakage metric was able to show that Secure-MAFS (above) leaks less private information and MAFS with projected heuristic (below) leaks more private information.

Conclusion

In this work, we have proposed a generalization of the privacy leakage quantification approach of (Štolba, Tožička, and Komenda 2017) to arbitrary numbers of private variables and sizes of private domains. As the original work was only theoretical, we have proposed a number of algorithms and computational techniques to arrive at the privacy leakage metric for actual MAP planners and domains.

In order to be tractable on real benchmark problems, we have proposed an approximation of the leakage quantification metric. This enabled us to evaluate the MAFS and Secure-MAFS algorithms on the CoDMAP domains using

distributed and projected heuristics. In addition to confirming the known fact that Secure-MAFS leaks less information than MAFS, we were also able to show a novel result stating that the MAFS algorithm actually leaks more private information when using the projected heuristic then when using the distributed one (assuming that the distributed computation is secure).

References

Brafman, R. I., and Domshlak, C. 2008. From one to many: Planning for loosely coupled multi-agent systems. In *Proceedings of the 18th International Conference on Automated Planning and Scheduling (ICAPS'08)*, 28–35.

Brafman, R. I. 2015. A privacy preserving algorithm for multi-agent planning and search. In *Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence, IJCAI*, 1530–1536.

Durfee, E. H. 1999. Distributed problem solving and planning. In Weiß, G., ed., *A Modern Approach to Distributed Artificial Intelligence*. San Francisco, CA: The MIT Press. chapter 3.

Fišer, D.; Štolba, M.; and Komenda, A. 2015. MAPlan. In *Proceedings of the Competition of Distributed and Multi-Agent Planners (CoDMAP-15)*, 8–10.

Helmert, M., and Domshlak, C. 2009. Landmarks, critical paths and abstractions: What's the difference anyway? In *Proceedings of the 19th International Conference on Automated Planning and Scheduling (ICAPS)*, 162–169.

Komenda, A.; Stolba, M.; and Kovacs, D. L. 2016. The international competition of distributed and multiagent planners (CoDMAP). *AI Magazine* 37(3):109–115.

Nissim, R., and Brafman, R. I. 2014. Distributed heuristic forward search for multi-agent planning. *Journal of Artificial Intelligence Research* 51:293–332.

Oliehoek, F. A., and Amato, C. 2016. *A concise introduction to decentralized POMDPs*. Springer.

Smith, G. 2009. On the foundations of quantitative information flow. In *Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures*, 288–302.

Štolba, M.; Fišer, D.; and Komenda, A. 2015. Admissible landmark heuristic for multi-agent planning. In *Proceedings of the 25th International Conference on Automated Planning and Scheduling (ICAPS)*, 211–219.

Štolba, M.; Fišer, D.; and Komenda, A. 2016. Potential heuristics for multi-agent planning. In *Proceedings of the 26th International Conference on Automated Planning and Scheduling, ICAPS'16*, 308–316.

Štolba, M.; Komenda, A.; and Kovacs, D. 2016. Competition of distributed and multiagent planners (CoDMAP). In *Proceedings of the AAAI Conference on Artificial Intelligence*, 4343–4345.

Štolba, M.; Tožička, J.; and Komenda, A. 2017. Quantifying privacy leakage in multi-agent planning. *Transactions on Internet Technology (TOIT)*.

Torreño, A.; Onaindia, E.; Komenda, A.; and Štolba, M. 2017. Cooperative multi-agent planning: a survey. *ACM Computing Surveys (CSUR)* 50(6):84.

Tožička, J.; Štolba, M.; and Komenda, A. 2017. The limits of strong privacy preserving multi-agent planning. In *Proceedings of the 27th International Conference on Automated Planning and Scheduling, ICAPS'17*.

Van Der Krogt, R. 2009. Quantifying privacy in multiagent planning. *Multiagent and Grid Systems* 5(4):451–469.