ECAI 2014
T. Schaub et al. (Eds.)


doi:10.3233/978-1-61499-419-0-973

# A Privacy-preserving Model for the Multi-agent Propositional Planning Problem

**Andrea Bonisoli** and **Alfonso E. Gerevini** and **Alessandro Saetti** and **Ivan Serina**[1]

## 1 Introduction

Over the last years, the planning community has formalized several models and approaches to multi-agent (MA) planning (e.g., [1, 2, 3]). One of the main motivations in MA planning is that some or all agents have private knowledge that cannot be communicated to other agents during the planning process and the plan execution.

The most known model for MA planning is MA-STRIPS [1]. In MA-STRIPS, the set of the executable actions is partitioned into $n$ sets $\{A_i\}_{i=1}^n$, such that $A_i$ is the set of actions the $i$-th agent is capable of executing. A proposition is considered *private* if it is required and affected only by the actions of a single agent. All other propositions are considered *public*. An action is private if all its preconditions and effects are private; the action is considered public, otherwise. An efficient approach [2] using MA-STRIPS is the multi-agent (distributed) formulation of $A^*$ (MA-$A^*$). In MA-$A^*$, no agent has complete knowledge of the search state, and hence during the $A^*$ search each agent sends a message to the other agents including a representation of the state under expansion, where, for sake of the agents' privacy, private propositions are encrypted.

The approach described in [2], which uses the MA-STRIPS formulation of MA planning, does not fully guarantee the privacy of the involved agents when: at least one public proposition is confidential (i.e., it should be kept hidden from some agent), or the identity/existence of at least one agent is confidential, and hence only certain authorized agents can communicate with her. E.g., consider four agents act: the retailer (`R`), the courier (`Co`), the retailer's supplier (`Su`), and the retailer's customer (`Cu`). Customer `Cu` needs to have goods `G` that are not currently in the retailer's shop (`Sh`). Retailer `R` sends a purchase order to its supplier `Su` for the shipment of a package `P` containing `G`. Express delivery courier `Co` moves package `P` from the supplier's factory (`F`) to the retailer's shop. Assume also that (`pack Su G P F`) is an action of agent `Su`; (`load Co P F`) is an action of agent `Co`; (`unpack Cu G P Sh`) is an action of agent `Cu`; (`in G P`) and (`loadable P`) are two (positive) effects of (`pack Su G P F`); (`loadable P`) is a precondition of (`load Co P F`); and, finally, (`in G P`) is a precondition of (`unpack Cu G P Sh`). Essentially, actions (`pack Su G P F`), (`load Co P F`), and (`unpack Cu G P Sh`) represent, respectively, that at factory `F` supplier `Su` packs goods `G` in package `P`, making package `P` loadable, courier `Co` loads package `P` from `F`, and, at shop `Sh`, customer `Cu` unpacks goods `G` from package `P`.

According to the approach described in [2], for this scenario propositions (`in G P`) and (`loadable P`) are public; hence, when agent supplier `Su` communicates the state obtained by executing its action (`pack Su G P F`) to agent courier `Co`, proposition (`in G P`) is not encrypted. The negative effect of this information exchange is that the privacy of the customer is violated, as it makes the courier know the content of package `P`. In order to preserve the privacy of the involved agents, the supplier should not communicate (`in G P`) to the courier. Moreover, while proposition (`in G P`) needs to be communicated to the retailer's customer so that the customer will be able to unpack goods `G` from package `P`, there should be no (direct) contact between the retailer's supplier and the retailer's customer.

In this abstract paper, we propose a model that preserves the privacy of the involved agents, and, discuss how the MA-$A^*$ search algorithm can be adapted to implement our model.

The model of MA planning that is most similar to the one we propose here is the model adopted by MAP-POP [3]. MAP-POP is a multi-agent planning system searching the space of partial-order plans by an $A^*$ POP algorithm. Each agent selects a (partial) plan $\pi$ from an open list, chooses an open (sub)goal $g$ from the selected plan, computes a set of plans refining $\pi$ to achieve $g$, sends the refined plans to every other agent, and receives the plans refined by other agents. Our model of MA planning avoids the global broadcasting and, by restricting message passing to certain agents, guarantees that the identity/existence of certain agents remains confidential.

## 2 Privacy-preserving Multi-agent Planning

A *privacy-preserving multi-agent planning problem* for a set of agents $\Sigma = \{\alpha_i\}_{i=1}^n$ is a tuple $\langle \{A_i\}_{i=1}^n, \{F_i\}_{i=1}^n, \{I_i\}_{i=1}^n, \{G_i\}_{i=i}^n, \{M_i\}_{i=1}^n \rangle$ where:

- $A_i$ is the set of actions agent $\alpha_i$ is capable of executing, and such that for every pair of agents $\alpha_i$ and $\alpha_j$, $A_i \cap A_j = \emptyset$;
- $F_i$ is the set of relevant facts for agent $\alpha_i$;
- $I_i \subseteq F_i$ is the portion of the initial state relevant for $\alpha_i$;
- $G_i \subseteq F_i$ is the set of goals for agent $\alpha_i$;
- $M_i \subseteq F_i \times \Sigma$ is the set of messages agent $\alpha_i$ can send to the other agents.

Facts and actions are literals and pair $\langle Pre, Eff \rangle$, respectively, where *Pre* is a set of positive literals and *Eff* is a set of positive or negative literals. Let $X+/X-$ denote the positive/negative literals in set $X$, respectively. Let $\mathcal{MG}$ be the graph induced by $\{M_i\}_{i=1}^n$, where nodes represent agents, and edges represent possible information exchanges between agents; i.e., an

[1] Università degli Studi di Brescia, email:{name.surname}@unibs.it

edge from node $\alpha_i$ to node $\alpha_j$ labelled $p$ represents the agent $\alpha_i$'s capability of sending $p$ to agent $\alpha_j$. In order to have well-defined sets $\{M_i\}_{i=1}^n$, $\forall \alpha_i, \alpha_j \in \Sigma$, $\forall p$ s.t. $p \in F_i$ and $p \in F_j$, there should be a path in $\mathcal{MG}$ from the node representing $\alpha_i$ to the node representing $\alpha_j$ formed by edges labelled $p$, if $p \in I_i$, or $\exists a \in A_i \cdot p \in \mathit{Eff}{+}(a)$, or $\exists a \in A_i \cdot p \in \mathit{Eff}{-}(a)$.

A plan for a multi-agent planning problem is a set $\{\pi_i\}_{i=1}^n$ of $n$ single-agent plans. Each single agent plan is a sequence of happenings. Each happening of agent $\alpha_i$ consists of a (possibly empty) set of actions of $\alpha_i$, and a (possibly empty) set of exogenous events. Exogenous events are facts that become true/false because of the execution of actions of other agents; in this sense, these events cannot be controlled by agent $\alpha_i$. Formally, $\pi_i = \langle h_i^1, \ldots, h_i^l \rangle$, $h_i^j = \langle A_i^j, E_i^j \rangle$, $A_i^j \subseteq A_i$, $E_i^j \subseteq \bigcup_k F_k$, for $i = 1 \ldots n$, $j = 1 \ldots l$, $k \in \{1, \ldots, i-1, i+1 \ldots, n\}$.

The execution of plan $\pi_i$ generates a state trajectory, $\langle s_i^0, s_i^1, \ldots, s_i^l \rangle$, and a sequence of messages, $\langle m_i^1, \ldots, m_i^l \rangle$, where $s_i^0 = I_i$ and $s_i^j$ and $m_i^j$ are defined as follows, for $j = 1 \ldots l$ and $k = 1 \ldots i-1, i+1 \ldots n$:

$$s_i^j = s_i^{j-1} \cup \bigcup_{a \in A_i^j} \mathit{Eff}{+}(a) \cup E{+}_i^j \setminus \bigcup_{a \in A_i^j} \mathit{Eff}{-}(a) \setminus E{-}_i^j,$$

$$m_i^j = \bigcup_k sm{+}_{i \to k}^j(n-1) \cup \bigcup_k sm{-}_{i \to k}^j(n-1), \text{ with}$$

$$sm{+}_{i \to k}^j(\tau) = \Big\{ \langle p, \alpha_k \rangle | \langle p, \alpha_k \rangle \in M_i, p \in \bigcup_{a \in A_i^j} \mathit{Eff}{+}(a) \cup rm{+}_i^j(\tau-1) \Big\}$$

$$sm{-}_{i \to k}^j(\tau) = \Big\{ \langle \neg p, \alpha_k \rangle | \langle p, \alpha_k \rangle \in M_i, p \in \bigcup_{a \in A_i^j} \mathit{Eff}{-}(a) \cup rm{-}_i^j(\tau-1) \Big\}$$

$$rm{+}_i^j(\tau) = \Big\{ p \mid \langle p, \alpha_i \rangle \in \bigcup_k sm{+}_{k \to i}^j(\tau) \Big\},$$

$$rm{-}_i^j(\tau) = \Big\{ p \mid \langle \neg p, \alpha_i \rangle \in \bigcup_k sm{-}_{k \to i}^j(\tau) \Big\},$$

$$rm{+}_i^j(0) = rm{-}_i^j(0) = \emptyset.$$

We say that the single-agent plan $\pi_i$ is *consistent* if the following conditions hold for $j = 1 \ldots l$ and $\tau = 1 \ldots n-1$:

(1) $E{+}_i^j = \bigcup_\tau rm{+}_i^j(\tau)$, $E{-}_i^j = \bigcup_\tau rm{-}_i^j(\tau)$;
(2) $\forall a, b \in A_i^j \cdot \mathit{Pre}(a) \cap \mathit{Eff}{-}(b) = \mathit{Pre}(b) \cap \mathit{Eff}{-}(a) = \emptyset$;
(3) $\forall a, b \in A_i^j \cdot \mathit{Eff}{+}(a) \cap \mathit{Eff}{-}(b) = \mathit{Eff}{+}(b) \cap \mathit{Eff}{-}(a) = \emptyset$;
(4) $\forall a \in A_i^j, \forall e \in E{-}_i^j(\tau) \cdot \mathit{Pre}(a) \cap e = \emptyset = \mathit{Eff}{+}(a) \cap e = \emptyset$.

Basically, (1) asserts that at planning step $j$ all the exogenous events for agent $\alpha_i$ are the positive/negative literals $\alpha_i$ receives during the information exchange; (2) and (3) assert that at planning step $j$ agent $\alpha_i$ executes no pair of mutually exclusive actions; finally, (4) asserts that at planning step $j$ agent $\alpha_i$ executes no action that is mutex with some action executed by other agents.

Let $\langle s_i^0, s_i^1, \ldots, s_i^l \rangle$ be the state trajectory generated by single-agent plan $\pi_i$. Plan $\pi_i$ is executable if $\mathit{Pre}(a) \subseteq s_i^{j-1}$, $\forall a \in A_i^j, j = 1 \ldots l$. Plan $\pi_i$ is valid for agent $\alpha_i$ if it is executable, consistent, and achieves the goals of agent $\alpha_i$, i.e., $G_i \subseteq s_i^l$. A multi-agent plan $\{\pi_i\}_{i=1}^n$ is a solution of the multi-agent privacy-preserving planning task if single-agent plan $\pi_i$ is valid for agent $\alpha_i$, for $i = 1 \ldots n$.

The main difference with existing models to multi-agent planning, like [3], is related to sets $\{M_i\}_{i=1}^n$ and the purpose for which agents use them. Essentially, $M_i$ determines the messages agent $\alpha_i$ can generate during the execution of its plan, that can be sent to other agents without loss of privacy. E.g., for the MA scenario described above, $\langle (\mathtt{in\,G\,P}), \mathtt{R} \rangle \in M_{\mathtt{Su}}$, and $\langle (\mathtt{in\,G\,P}), \mathtt{Cu} \rangle \in M_{\mathtt{R}}$. Therefore, when agent supplier `Su` packs goods `G` into package `P`, `Su` communicates that `G` is in `P` to agent retailer `R`; when `R` receives this communication, `R` sends it to agent customer `Cu`, so that courier `Co` has no access to message $(\mathtt{in\,G\,P})$, and there is no direct contact between the retailer's seller and the retailer's customer.

In the rest of the paper, we describe how MA-$A^*$ [2] can be adapted to handle our problem model. Briefly, in MA-$A^*$ each agent considers a separate search space, since each agent maintains its own open list and, when an agent expands a state $s$ from its open list, the agent uses its own actions. The open search states that are relevant to different agents are shared, i.e., when $s$ is expanded each agent sends to the others a representation of $s$ obtained by encrypting private propositions. In order to preserve the privacy according with $\{M_i\}_{i=1}^n$, each agent $\alpha_i$ generates its own key that will be used to encrypt every proposition in $F_i$ except those that $\alpha_i$ sends to or receives from other agents. Agents that are capable to communicate proposition $p$ initially exchange a (shared) key to encrypt $p$.

At the beginning, each agent $\alpha_i$ constructs its own (partially encrypted) description $I_i'$ of the initial global state of the MA scenario. Initially, $\alpha_i$ sets $I_i'$ to $I_i$. For each agent $\alpha_k$ $\alpha_i$ is capable to communicate with, $\alpha_i$ encrypts the portion of $I_i'$ formed by all propositions $p \in F_i$ such that $\langle p, \alpha_k \rangle \notin M_i$. Specifically, $\alpha_i$ encrypts $p$ by using the encryption key of $p$, if it exists; while $\alpha_i$ encrypts $p$ by using its own encryption key, otherwise. Then, $\alpha_i$ sends the resulting state to $\alpha_k$. When agent $\alpha_i$ receives a description of the initial state, $\alpha_i$ decrypts the portion of the state formed by the (encrypted) propositions in $F_i$ and computes the union between the resulting state and $I_i'$. If such a state $I_i''$ is different from $I_i'$, agent $\alpha_i$ sets $I_i'$ to $I_i''$, and, for each agent $\alpha_k$ $\alpha_i$ is capable to communicate with, $\alpha_i$ sends the description of $I_i'$ to $\alpha_k$ as described before. This procedure is repeated until, for every agent $\alpha_i$, $I_i'$ does not change anymore. Similarly, subsequently each agent constructs its own (partially encrypted) description $G_i'$ of the initial global set of goals of the MA scenario.

Then, each agents $\alpha_i$ performs the MA-$A^*$ procedure from initial state $I_i'$ to achieve the goals $G_i'$. The important difference w.r.t. the procedure described in [2] concerns the information exchange among agents. Agents send messages only to agents they can communicate with, instead of sending broadcast messages. The exchanged messages still include (partially encrypted) description of the world state, but the encrypted propositions of these messages are different. Specifically, when agent $\alpha_i$ expands a state, for every other agent $\alpha_k$ $\alpha_i$ can communicate with, agent $\alpha_i$ encrypts the portion of the state formed by every proposition $p$ such that $\langle p, \alpha_k \rangle \notin M_i$ by using the encryption key of $p$, if exists, or its own encryption key, otherwise. Then, $\alpha_i$ sends the resulting state to $\alpha_k$.

## REFERENCES

[1] Ronen I. Brafman and Carmel Domshlak, 'From one to many: Planning for loosely coupled multi-agent systems', in *Proc. of the 18th ICAPS*, (2008).
[2] Raz Nissim and Ronen I. Brafman, 'Multi-agent A* for parallel and distributed systems', in *Proc. of the 11th AAMAS*, (2012).
[3] Alejandro Torreño, Eva Onaindia, and Óscar Sapena, 'An approach to multi-agent planning with incomplete information', in *Proc. of the 20th ECAI*, (2012).