Towards the Verification of Strategic Ability in MAS with Private Data-Sharing

I. Bourceanu  
University of Surrey  
UK

C. Dima  
Université Paris-Est Creteil  
France

F. Belardinelli and V. Malvone  
Université d’Evry  
France

1 Introduction

The Increasing Importance of Private Information Sharing. The 5th-generation of networks is set to be one of the important ICT developments into the 2020s. In this way, smart buildings, cities and cars will be in constant connectivity, transferring data back and forth, sometimes on private channels. These private communications should lead to interlocutors reactively controlling and influencing subsequent information-flow and parts of the system. Already, your UK’s Hive heating-control system privately gets a reading from the smart-thermostat sensors and, based on the privately-attained measurements, Hive reactsively changes the temperature settings in your house. At the same time, the private nature of Internet-of-Things communications is to be safeguarded at all costs (Samaila et al. 2017). In a nutshell, private communications will be at the core in the private nature of Internet-of-Things communications.

The 5th-generation of networks is set to be one of the perfect recall. We then identify an expressive fragment of Temporal Logic (ATL). We show that the problem is generally undecidable for ATL with imperfect information and perfect recall. We then identify an expressive fragment of ATL and a reasonable specialisation of the syntax/semantics for “MAS with 1-to-1 private-channels” for which the problem is decidable; the said specialisation of our “MAS with private-channels” explicitly models the ability to “gossip”: agent $a$ has a shorthand to gossip with agent $b$ about the variables that $c$ and $d$ had “confined” in $a$ and $b$, respectively.

2 Deciding A Fragment on ATL on “Gossiping” $\text{vCGS}$

In this section we provide a variant of $\text{vCGS}$ with second-order visibility atoms that we prove to have decidable model checking problem w.r.t. a fragment of $\text{ATL}^*$. Most importantly, the result applies to our security scenarios.

Definition 1 (Gossip Atoms) A second-level visibility atom or gossip atom is any atomic proposition written $\text{vis}(\text{vis}(v, a), b)$, where $v \in \text{AP}$ is an atom and $a, b$ are agents. The set $\text{VA}^2$ denotes the set of all visibility atoms $\text{vis}(\text{vis}(v, a), b)$, for all $v \in \text{AP}$ and $a, b \in \text{Ag}$. The set $\text{VA}^2_{a,b} = \{ \text{vis}(\text{vis}(v, a), b) \in \text{VA}^2 \mid v \in \text{AP}\}$ denotes the set of atoms visible to some agent $b$ via some agent $a$.

Intuitively, a gossip atom is a means, for an agent, of communicating all data he receives from another agent to a third party, by making that data visible.

Definition 2 (Gossip Agents: Syntax) A gossip agent spec is a tuple $\text{spec}_a = (\text{AP}, V_a, \text{GC}_a)$, where $\text{AP}, V_a$ satisfy the same constraints as for agent specs, and $\text{GC}_a$ is the set of guarded commands, which can be of $\text{init-type}$ or $\text{update-type}$ and are expressions of the form:

$$\gamma ::= \varphi \mapsto \bigwedge_{i \leq k_1} v_i := t_i, \bigwedge_{j \leq k_2} \text{vis}(u_j, a_j) := t_j, \bigwedge_{l \leq k_3} \text{vis}(w_l, b_l), c_l = t_l$$

where $v_i, u_j \in V_a$ for all $i \leq k_1, j \leq k_2$, the guard $\varphi$ is a boolean formula over $\text{AP}, a_j \in \text{Ag} \setminus \{a\}$ for all $j \leq k_2$ and $b_l, c_l \in \text{Ag}$ with $a \neq b_l \neq c_l \neq a$ for all $l \leq k_3$. First study the model checking problem for Alternating-time Temporal Logic (ATL). We show that the problem is generally undecidable for ATL with imperfect information and perfect recall. We then identify an expressive fragment of ATL and a reasonable specialisation of the syntax/semantics for “MAS with 1-to-1 private-channels” for which the problem is decidable; the said specialisation of our “MAS with private-channels” explicitly models the ability to “gossip”: agent $a$ has a shorthand to gossip with agent $b$ about the variables that $c$ and $d$ had “confined” in $a$ and $b$, respectively.
The semantics of a gossip agent spec extends the semantics of an agent spec with specific rules for taking into account the second-level visibility atoms.

**Definition 3 (Gossip Agents: Semantics)** Given a gossip agent spec \( \Gamma = (\text{spec}_a)_{a \in Ag} \), the iCGS associated with \( \Gamma \) is \( G(\Gamma) = \langle Ag,\{Act_a\}_{a \in Ag},S,S_0,P,\tau,\{\sim_a\}_{a \in Ag},\pi \rangle \) where:

- For every \( a \in Ag \), \( Act_a = GC_a \).
- \( S = \{ s \subseteq AP \cup VA \cup VA^2 \mid \text{for every} \ a \in Ag, v \in V_a, vis(v,a) \in s \} \) is the set of states.
- \( S_0 \subseteq S \) is the set of initial states, with \( s_0 \in S_0 \) iff there exists \( \gamma_{\text{own}(v)} \in \text{init}(Act_{\text{own}(v)}) \) with \( v := \tau \) occurring in \( \text{ass}(\gamma_{\text{own}(v)}) \). Furthermore, \( vis(v,b) \in s_0 \) iff there exists \( \gamma_{\text{own}(v)} \in \text{init}(Act_{\text{own}(v)}) \) with \( vis(v,b) := \tau \) occurring in \( \text{ass}(\gamma_{\text{own}(v)}) \). Finally, \( vis(v,b),a \in s_0 \) iff there exists \( \gamma_b \in \text{init}(Act_{\text{own}(v)}) \) with \( vis(v,b,a) := tt \) occurring in \( \text{ass}(\gamma_b) \).
- For every state \( s \in S \) and agent \( a \in Ag \), the protocol function \( P : S \times Ag \rightarrow 2^{\bigcup_{a \in Ag}Act_a} \), returns the set \( P(s,a) \) of commands \( \gamma \) such that \( s \models \text{guard}(\gamma) \) and:

\[
\text{atoms}(\text{guard}(\gamma)) \subseteq Vis(s,a) \cup \bigcup_{ \gamma \in \text{ass}(s) } \{ Vis(v,b,a) \mid b \in Ag, \text{atoms}(\text{guard}(\gamma)) \subseteq Vis(s,b,a) \cap Vis(s,b) \}
\]

- The transition function \( \tau : S \times Act_1 \times \ldots \times Act_{\left|Ag\right|} \rightarrow S \) is such that a transition \( \tau(s,(\gamma_1,\ldots,\gamma_n)) = s' \) holds iff:
  - for every \( a \in Ag \), \( \gamma_a \in P(s,a) \);
  - The conditions for \( v \in s' \) and \( vis(v,b), a \in s' \) are the same as in the case of the vCGS associated to an agent spec.
  - \( vis(v,b), a \in s' \) if either \( ass(\gamma_a) \) contains an assignment of the type \( vis(v,b), a \) := \( tt \) or \( vis(v,b) \in s \).
  - Similarly, \( vis(v,b), a \notin s' \) if either \( ass(\gamma_a) \) contains an assignment of the type \( vis(v,b), a \) := \( ff \) or \( vis(v,b) \notin s \).

- The indistinguishability relation is defined as: \( s \sim_a s' \) iff \( Vis(s,a) = Vis(s',a) \), for every \( b \neq a \), \( Vis(s,b,a) = Vis(s',b,a) \), and for every \( v \in Vis(s,a) \cup \bigcup_{b \neq a} Vis(s,b,a) \), \( v \in s \) iff \( v \in s' \).

- \( \pi : S \rightarrow 2^{AP \cup VA \cup VA^2} \) is the identity function.

We now introduce some notions that will be use in the proof of our main result.

**Definition 4 (Synchronization)** A gossip agent spec \( \Gamma = (\text{spec}_a)_{a \in Ag} \) with \( \text{spec}_a = (AP,V_a,GC_a) \) is said to have synchronization steps if for each agent \( a \in Ag \), there exists some variable \( \text{turn}_a \in V_a \), such that \( \text{turn}_a \notin S_0 \) for any initial state \( s_0 \in S_0 \) and \( GC_a \) has two types of commands:

1. Update commands, of type \( \gamma := \text{turn}_a \rightarrow \text{turn}_a = ff \), \( \bigwedge v_i = t_i \) with \( t_i \in \{tt, ff\} \).

2. Synchronization commands, of type \( \gamma := \lnot \text{turn}_a \rightarrow \text{turn}_a = tt \land \bigwedge vis(v_i,a_i) = t_i \land \bigwedge vis(v_j,b_j) = c_j \) with \( t_i, t_j \in \{tt, ff\} \).

Additionally, the set of synchronization commands for each agent \( a \) contains, for sets \( V_1, V_2 \subseteq V_a \) of variables and sets \( B_1, B_2 \subseteq Ag \) of agents, one command of the following form:

\[
\delta_a(V_1,V_2,B_1,B_2,B_3) := \lnot \text{turn}_a \rightarrow \text{turn}_a = tt \land \bigwedge v \in V_1 \land b \in B_1 \land v \in V_2 \land b \not\in B_2 \land v \in V_2 \land b \in B_3 \land \bigwedge vis(v,b,c) = tt
\]

The increasing fragment of \( ATL^* \) is the set of formulas \( \varphi \) which has the property that nested coalitions must be increasing. Formally, a formula \( \varphi \) is in \( ATL^* \) iff for each subformula \( (\langle A \rangle) \varphi \) of \( \varphi \) and subformula \( (\langle B \rangle) \chi \) of \( \psi \) we have that \( A \subseteq B \). Additionally, we require that no nexttime operator occurs in formulas. We denote this fragment as \( ATL^*_\chi \). We also say that formula \( \varphi \) utilizes only coalitions which include a set \( A \) of agents if any subformula \( (\langle B \rangle) \psi \) of \( \varphi \) has \( B \subseteq A \).

We adapt here the semantics of \( ATL^*_\chi \) with distributed knowledge (Guelev, Dima, and Enea 2011; Jiang, Zhang, and Perrussel 2015). First, given an agent spec \( \Gamma = (\text{spec}_a)_{a \in Ag} \), consider some command \( \gamma_a \in GC_a \), \( \gamma_a = \phi \rightleftharpoons up \), \( vis \) with \( up \) the part consisting of variable updates and \( vis \) consisting of visibility updates (including gossip updates). We denote \( \gamma_a^{up} \) the command \( \phi \rightleftharpoons up \), that is, the command obtained from \( \gamma \) by purging any visibility updates. For a given set of visibility atoms \( W \subseteq VA \cup VA^2 \), we denote \( \Gamma'(VA, VA^2) \) the agent spec which results by replacing each command \( \gamma_a \) with \( \gamma_a^{up} \) and the init commands are commands which set the visibility of all atoms from \( W \) to \( tt \) and of all atoms not in \( W \) to \( ff \).

Given a formula \( \varphi = (\langle A \rangle) \psi \) with \( \psi \) not containing any coalition operator and a state \( s \in S \), we denote \( s \models_D \varphi \) if

\[
\Gamma'(VA, VA^2)_{a \in A, a,b \in A} = \bigcup_{a \in A} VA_{a,b} \models_D (\langle A \rangle) \psi \models \varphi
\]

**Theorem 1** The model-checking problem for the class of agent specifications with synchronization steps and formulas in \( ATL^*_\chi \) is decidable.

**References**

