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

I. Boureanu
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 reactively 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 2020s' ubiquitous systems, and are likely to be further endorsed and imposed.

So, being able to explicitly and naturally model data-sharing in multi-agent systems (MAS) is essential. However, the concurrent formalisms for MAS do not cater for explicit data-sharing between agents: neither at the syntactic nor at the semantic level. Such sharing can be nonetheless achieved e.g., via mechanisations based on duplicating agents' variables and the addition of synchronisation-driven actions. But, this is tedious and error-prone, and –above all– it is inefficient, yielding adding extra actions and generally duplication of agents' local variables.

To fill this gap, we put forward a formalism for the explicit expression of private data-sharing in MAS. That is, we encode syntactically and in a natural semantics "MAS with 1-to-1 private-channels": agent a and agent b have an explicit syntactic/semantic endowment to "see" some of each others' variables, without other agents partaking in this.

The Rising Power of Collusion. In the aforementioned setting of truly multi-party environments, collusions become a real threat (Samaila et al. 2017): corrupting two sensors instead of one is an easy way to maximise the effect of adversarially-injected reading to your smart car. Thus, studying strategic ability under collusions is of timely interest. So, on our "MAS with 1-to-1 private-channels", we 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.

2 Deciding A Fragment on ATL on "Gossiping" `vCGS`

In this section we provide a variant of `vCGS` with second-order visibility atoms that we prove to have decidable model checking problem w.r.t. a fragment of 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 $vis(vis(v, a), b)$, where $v \in AP$ is an atom and a, b are agents. The set* VA^2 *denotes the set of all* visibility atoms *$vis(vis(v, a), b)$, for all $v \in AP$ and $a, b \in Ag$. The set* $\mathsf{VA}^2_{a,b}$=$\{vis(vis(v, a), b) \in \mathsf{VA}^2 \mid v \in AP\}$ *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 $spec_a = \langle AP, V_a, GC_a\rangle$, where AP, V_a satisfy the same constraints as for agent specs, and GC_a is the set of* guarded commands*, which can be of* `init`-type *or* `update`-type *and are expressions of the form:*

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

where $v_i, u_j \in V_a$ for all $i \leq k_1, j \leq k_2$, the guard *φ is a boolean formula over AP, $a_j \in Ag \setminus \{a\}$ for all $j \leq k_2$ and $b_l, c_l \in Ag$ with $a \neq b_l \neq c_l \neq a$ for all $l \leq k_3$.*

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* $\Gamma = (spec_a)_{a \in Ag}$, *the* iCGS associated with Γ *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* $a \in Ag$, $Act_a = GC_a$.
- $S = \{s \subseteq AP \cup \mathsf{VA} \cup \mathsf{VA}^2 \mid$ *for every* $a \in Ag, v \in V_a, vis(v,a) \in s\}$ *is the* set of states. *Additionally from* $Vis(v,a)$*, which is defined as for* vCGS*, for* $s \in S$ *and* $a, b \in Ag$*, we define* $Vis(s,a,b) = \{v \in AP \mid vis(vis(v,a),b) \in s\}$.
- $S_0 \subseteq S$ *is the set of* initial states, *with* $s_0 \in S_0$ *iff for all* $v \in AP$*, we have* $v \in s_0$ *iff there exists* $\gamma_{own(v)} \in \mathtt{init}(Act_{own(v)})$ *with* $v := \mathtt{tt}$ *occurring in* $ass(\gamma_{own(v)})$*. Furthermore,* $vis(v,b) \in s_0$ *iff there exists* $\gamma_{own(v)} \in \mathtt{init}(Act_{own(v)})$ *with* $vis(v,b) := \mathtt{tt}$ *occurring in* $ass(\gamma_{own(v)})$*. Finally,* $vis(vis(v,b),a) \in s_0$ *iff there exists* $\gamma_b \in \mathtt{init}(Act_{own(v)})$ *with* $vis(vis(v,b),a) := \mathtt{tt}$ *occurring in* $ass(\gamma_b)$.
- *For every state* $s \in S$ *and agent* $a \in Ag$*, the protocol function* $P : S \times Ag \to 2^{\bigcup_{a \in Ag} Act_a}$*, returns the set* $P(s,a)$ *of commands* γ *such that* $s \models guard(\gamma)$ *and:*

$$atoms(guard(\gamma)) \subseteq Vis(s,a) \cup \bigcup \{Vis(s,b,a) \mid b \in Ag,$$
$$atoms(guard(\gamma)) \subseteq Vis(s,b,a) \cap Vis(s,b)\}$$

- *The* transition function $\tau : S \times Act_1 \times \ldots \times Act_{|Ag|} \to S$ *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* $vis(v,b) \in s'$ *are the same as in the case of the* vCGS *associated to an agent spec.*
  - $vis(vis(v,a),b) \in s'$ *if either* $ass(\gamma_a)$ *contains an assignment of the type* $vis(vis(v,a),b) := \mathtt{tt}$ *or* $vis(vis(v,a),v) \in s$.
  - *Similarly,* $vis(vis(v,a),b) \notin s'$ *if either* $ass(\gamma_a)$ *contains an assignment of the type* $vis(vis(v,a),b) := \mathrm{ff}$ *or* $vis(vis(v,a),v) \notin s$.
- *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* $v \in s'$.
- $\pi : S \to 2^{AP \cup \mathsf{VA} \cup \mathsf{VA}^2}$ *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* $\Gamma = (spec_a)_{a \in Ag}$ *with* $spec_a = (AP, V_a, GC_a)$ *is said to have* synchronization steps *if for each agent* $a \in Ag$*, there exists some variable* $turn_a \in V_a$ *such that* $turn_a \notin s_0$ *for any initial state* $s_0 \in S_0$ *and* GC_a *has two types of commands:*

1. *Update commands, of type* $\gamma ::= turn_a \rightsquigarrow turn_a = \mathrm{ff}, \bigwedge v_i = t_i$ *with* $t_i \in \{\mathtt{tt}, \mathrm{ff}\}$.
2. *Synchronization commands, of type* $\gamma ::= \neg turn_a \rightsquigarrow turn_a = \mathtt{tt} \wedge \bigwedge vis(v_i,a_i) = t_i \wedge \bigwedge vis(vis(u_j,b_j),c_j) = t_j$ *with* $t_i, t_j \in \{\mathtt{tt}, \mathrm{ff}\}$.

Additionnally, 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:*

$$\delta_a(V_1,V_2,B_1,B_2,B_3) ::= \neg turn_a \rightsquigarrow$$
$$turn_a = \mathtt{tt}, \bigwedge_{v \in V_1} \bigwedge_{b \in B_1} vis(v,b) = \mathtt{tt},$$
$$\bigwedge_{v \in V_2} \bigwedge_{b \in B_2} \bigwedge_{c \in B_3} vis(vis(v,b),c) = \mathtt{tt}$$

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

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

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

$$(\Gamma'(\bigcup_{a \in A} \mathsf{VA} \cup \bigcup_{a,b \in A} \mathsf{VA}^2_{a,b}, s \cup \bigcup_{a \in A} \mathsf{VA} \cup \bigcup_{a,b \in A} \mathsf{VA}^2_{a,b}) \models \varphi$$

Theorem 1 *The model-checking problem for the class of agent specifications with synchronization steps and formulas in* $ATL^*_{\nearrow}$ *is decidable.*

References

Guelev, D. P.; Dima, C.; and Enea, C. 2011. An alternating-time temporal logic with knowledge, perfect recall and past: axiomatisation and model-checking. *Journal of Applied Non-Classical Logics* 21(1):93–131.

Jiang, G.; Zhang, D.; and Perrussel, L. 2015. Knowledge sharing in coalitions. In *AI 2015*, volume 9457 of *LNCS*, 249–262.

Samaila, M. G.; Neto, M.; Fernandes, D. A. B.; Freire, M. M.; and Inácio, P. R. M. 2017. Security challenges of the internet of things. In Batalla, J. M.; Mastorakis, G.; Mavromoustakis, C. X.; and Pallis, E., eds., *Beyond the Internet of Things: Everything Interconnected.* Cham: Springer International Publishing. 53–82.