Verifying Strategic Abilities in Multi-agent Systems with Private Data Sharing

Catalin Dima

Université Paris-Est Créteil

FMAI, Rennes, 3 Mai 2019

Joint work with:
Francesco Belardinelli, Imperial College London
Ioana Boureanu, University of Surrey
Vadim Malvone, Université d’Evry
FOCUS

Our contribution

- Explicit expression of temporary private data-sharing.
- Agents may change data visibility at their own will.
- Guarded commands for updating own variables and visibility.
- Strategic and coalition capacities through Alternating-time Temporal Logic with Imperfect Information:
  - Coalition power to achieve objectives by possibly sharing, temporarily, information, while still keeping some degree of privacy.
  - Privacy through epistemic subformulas.
- Generalization of Reactive Modules with dynamic visibility.
- Application to a security protocol.
Agents with Visibility-Control

Visibility atoms

Given an atom $v \in AP$ and agent $a \in Ag$, we denote with:

- $vis(v, a)$ as a visibility atom, expressing intuitively that the value of $v$ is visible to $a$.
- $VA$ as the set of all visibility atoms $vis(v, a)$.
- $VA_a = \{vis(v, a) \in VA \mid v \in AP\}$ as the set of atoms visible to agent $a$.
**Agents with Visibility-Control**

Visibility atoms

Given an atom $v \in AP$ and agent $a \in Ag$, we denote with:

- $vis(v, a)$ as a *visibility atom*, expressing intuitively that the value of $v$ is visible to $a$.
- $VA$ as the set of all *visibility atoms* $vis(v, a)$.
- $VA_a = \{vis(v, a) \in VA \mid v \in AP\}$ as the set of atoms visible to agent $a$.

Key aspect

- *At run time*, an agent $a$, who “controls” / “owns” atom $v$, can make it visible (resp., invisible) to agent $b$.
- That is, agent $a$ can change the truth value of atom $vis(v, b)$ at some point, and set it to true (resp., false).
Agents with Visibility-Control

Syntax

An agent specification \( a \) is a tuple \( \text{spec}_a = \langle \text{AP}, V_a, \text{GC}_a \rangle \), where:

- \( V_a \subseteq \text{AP} \) is the set of atoms controlled by agent \( a \);
- \( \text{GC}_a \) is a finite set of guarded commands:

\[
\gamma ::= \text{guard}(\gamma) \xrightarrow{} \text{ass}(\gamma)
\]

- \( \text{GC}_a = \text{init}_a \cup \text{update}_a \) : initialization actions \( \cup \) update commands, with \( \text{guard}(\gamma) = \top \) for each \( \gamma \in \text{init}_a \).
Agents with Visibility-Control

Guarded commands

\[ \gamma ::= \varphi \Rightarrow v_1 := t, \ldots, v_k := t, \]
\[ vis(v_{k+1}, a_1) := t, \ldots, vis(v_{k+m}, a_m) := t \]

where:

- \( \varphi \) is a boolean formula over \( AP \cup VA_a \);
- each \( v_i \) is a variable controlled by \( a \) (i.e. \( v_i \in V_a \));
- each \( a_i \) is an agent in \( Ag \) different from \( a \) (i.e. \( a_i \in Ag \setminus \{a\} \));
- \( t \in \{\top, \bot\} \).
Agents with Visibility-Control

Semantics

Given a set of agents specifications, an iCGS with propositional control for atom-visibility (νCGS) is $G=\langle AP, Ag, \{Act_a\}_{a \in Ag}, S, S_0, P, \tau, \{\sim a\}_{a \in Ag}, \pi \rangle$:

- For every $a \in Ag$, $Act_a = GC_a$.
- $S = \{s \subseteq AP \cup VA \mid \forall a \in Ag, v \in V_a, vis(v,a) \in s\}$ is the set of states.
Semantics for agents with visibility control

- $S_0 \subseteq S$ denotes the set of initial states, where $s_0 \in S_0$ iff there exist $(\gamma_a)_{a \in Ag}$ with $\gamma_a \in init_a$ for all $a$ such that
  1. for all $v \in AP$, $v \in s_0$ iff $v := \top$ occurs in $ass(\gamma_{own(v)})$;
  2. for all $vis(v, b) \in VA$, $vis(v, b) \in s_0$ iff $vis(v, b) := \top$ occurs in $ass(\gamma_{own(v)})$.

- Initialization actions are **not chosen by the agent**!
Semantics

- 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 update commands $\gamma$ such that:
  - $atoms(guard(\gamma)) \subseteq Vis(s, a)$;
  - $s \models guard(\gamma)$.
Semantics

- The transition function \( \tau : S \times Act_1 \times \ldots \times Act_{|Ag|} \rightarrow S \) is such that a transition \( \tau(s, (\gamma_1, \ldots, \gamma_n)) = s' \) holds iff:
  - For every \( a \in Ag \), \( \gamma_a \in P(s, a) \).
  - For every \( v \in AP \) and \( own(v) \in Ag \):
    - \( v \in s' \) if either \( v := \top \in ass(\gamma_{own(v)}) \) or \( v \in s \).
    - \( v \not\in s' \) if either \( v := \bot \in ass(\gamma_{own(v)}) \) or \( v \not\in s \).
    - \( vis(v, a) \in s' \) if either \( vis(v, a) := \top \in ass(\gamma_{own(v)}) \) or \( vis(v, a) \in s \).
    - \( vis(v, a) \not\in s' \) if either \( vis(v, a) := \bot \in ass(\gamma_{own(v)}) \) or \( vis(v, a) \not\in s \).
Visibly Concurrent Game Structures

Semantics

• The indistinguishability relation: \( s \sim_a s' \) iff \( \text{Vis}(s, a) = \text{Vis}(s', a) \) and for every \( v \in \text{Vis}(s, a) = \text{Vis}(s', a), \) \( v \in s \) iff \( v \in s' \).

• The labeling function \( \pi : S \rightarrow 2^{AP \cup VA} \) is the identity, i.e., each state is named with the atoms belonging to it.
A QUEST

• Model security protocols as a multi-agent systems.
• Formalize security properties in temporal epistemic logics:
  • Anonymity = absence of knowledge.
  • Authentication = mutual knowledge.
  • Coercion-freeness = absence of a strategy (with imperfect information) for the attacker to achieve a goal.
  • etc.
• Adapt multi-agent models to case studies in security.
A TERRORIST FRAUD CASE STUDY

Distance-bounding security protocols

1. A card (called prover) demonstrates to a card-reader (called verifier) that it is physically situated no further than a distance-bound, which a parameter of the protocol.

2. Via exchanges, the prover also authenticates himself to the verifier.

3. In terrorist-fraud (TF) attacks, a prover $P^*$, who is malicious and far away from the honest verifier $V$, colludes with an adversary $A$ (who is close to $V$) such that the coalition makes the verifier $V$ believe that $P^*$ is close to $V$ and acting legitimately.

4. A valid terrorist-fraud attack is one where $P^*$ helps $A$ in such a way that $A$ can pass the protocol on $P^*$’s behalf only once (no card transmission!).
The Hancke and Khun Protocol

Verifier
secret: $x$

Prover
secret: $x$

**Initialization Phase**

pick $N_V$

$N_V$ →

pick $N_P$

← $N_P$

$a_1 \| a_2 = f_x(N_P, N_V)$

**Distance Bounding Phase**

for $i = 1$ to $n$

pick $c_i \in \{1, 2\}$

start $timer_i$

$c_i$ →

stop $timer_i$

$r_i$ ←

check responses

check timers

$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \end{cases}$

Out$_V$

Terrorist fraud attack

• dishonest far-away $P$ colludes with the attacker $A$.

• $P$ gives $A$ the values $a_1$ and $a_2$ only once.

• In the timed phase, $A$ will be able to answer correctly.

• This valid TF-strategy makes $A$ pass the protocol every time without being in the possession of the card ($N_P$).
THE HANCKE AND KHUN PROTOCOL

Verifier
secret: \( x \)

Prover
secret: \( x \)

**Initialization phase**
- pick \( N_V \)
- \( N_V \rightarrow N_P \)
- \( N_P \leftarrow N_V \)
- \( a_1 \parallel a_2 = f_x(N_P, N_V) \)

**Distance bounding phase**
- for \( i = 1 \) to \( n \)
  - pick \( c_i \in \{1, 2\} \)
  - start \( \text{timer}_i \)
  - stop \( \text{timer}_i \)
  - check responses
  - check timers

\( r_i = \begin{cases} 
  a_{1,i} & \text{if } c_i = 1 \\
  a_{2,i} & \text{if } c_i = 2 
\end{cases} \)

**Terrorist fraud attack**
- dishonest far-away \( P \) colludes with the attacker \( A \).
- \( P \) gives \( A \) the values \( a_1 \) and \( a_2 \) only once.
- In the timed phase, \( A \) will be able to answer correctly.
- This valid TF-strategy makes \( A \) pass the protocol every time without being in the possession of the card \( (N_P) \).
Uniform strategies

- A uniform memoryfull strategy for $a \in Ag$ is a function $f_a : S_0 \cdot S^* \rightarrow Act_a$ such that for all $h, h' \in S_0 \cdot S^*$:
  1. $f_a(h) \in P(\text{last}(h), a)$;
  2. if $h \sim_a h'$ then $f_a(h) = f_a(h')$.

  where, $h \sim_a h'$ iff $|h| = |h'|$ and for every $i \leq |h|$, $h_i \sim_a h'_i$.

- A joint strategy for coalition $A \subseteq Ag$ is a tuple of uniform strategies $(f_a)_{a \in A}$.
MODEL-CHECKING STRATEGIC PROPERTIES

Alternating-time temporal logic

State ($\varphi$) and path ($\psi$) formulas in $ATL^*$ are:

$$
\varphi ::= q \mid \neg \varphi \mid \varphi \land \varphi \mid \langle\langle A \rangle\rangle \psi
$$

$$
\psi ::= \varphi \mid \neg \psi \mid \psi \land \psi \mid X \psi \mid (\psi U \psi)
$$

where $q \in AP$ and $A \subseteq Ag$.

Formulas in $ATL$ restrict the use of LTL operators inside the coalition operators:

$$
\psi ::= \langle\langle A \rangle\rangle X \varphi \mid \langle\langle A \rangle\rangle \varphi U \varphi \mid \langle\langle A \rangle\rangle \varphi R \varphi
$$

$[[A]]$ is the dual of $\langle\langle A \rangle\rangle$. 
SATISFACTION OF FORMULAS

Interpretation of $ATL^*$ formulas on iCGS

The satisfaction relation $\models$ for an iCGS $G$, path $p$, index $i \in \mathbb{N}$ and $ATL^*$ formula $\phi$ is defined as follows:

$$(G, p, i) \models \langle A \rangle \psi \iff \text{for some uniform joint strategy } F_A,$$

$$\text{for all } p' \in out(p_{\leq i}, F_A), (G, p', i) \models \psi$$

where, $out(h, F_{\Gamma})$ is the set of all paths $p$ starting from history $h$ and compatible with joint strategy $F_{\Gamma}$.

- A subjective interpretation of $ATL^*$ can be given by choosing $out_{subj}(h, F_{\Gamma})$ as the set of all paths $p$ starting from some history $h' \sim^E_A h$ and compatible with joint strategy $F_{\Gamma}$. 
There exists a collusion between the far-away prover $p$ and the attacker $a$ such that session $i$ is finished successfully, yet whatever the attacker $a$ did, she cannot pass session $i + 1$ without the collusion of the prover:

$$\langle\langle\text{prover, attacker}\rangle\rangle F(\text{successful\_help\_once} \Rightarrow [[\text{attacker}]] G \text{help\_useless\_after})$$
MODEL-CHECKING

- The model checking problem for $ATL$ on vCGS is undecidable (corollary of the result for CGS).
- The model-checking problem for $ATL$ when all coalitions have distributed knowledge is decidable.
The model checking problem for \textit{ATL} on vCGS is undecidable (corollary of the result for CGS).

The model-checking problem for \textit{ATL} when all coalitions have distributed knowledge is decidable.

Distributed knowledge achievable through public announcements.

Decidable cases must avoid information forks [Finkbeiner \\& Schewe]:

1. No two variables \(v_1, v_2 \in \bigcup b \not \in A V b\) with \(v_1 \not \in \text{Vis}(s, a_1) \setminus \text{Vis}(s, a_2)\) and \(v_2 \not \in \text{Vis}(S, a_1) \setminus \text{Vis}(S, a_2)\) for some \(s \in S, a_1, a_2 \in A\).

2. And agents may choose their initial state! (contrary to vCGS init actions!)
Model-Checking

- The model checking problem for $ATL$ on vCGS is undecidable (corollary of the result for CGS).
- The model-checking problem for $ATL$ when all coalitions have distributed knowledge is decidable.
- Distributed knowledge achievable through public announcements.
- Decidable cases must avoid information forks [Finkbeiner & Schewe]:
  1. No two variables $v_1, v_2 \in \bigcup_{b \notin A} V_b$ with $v_1 \in Vis(s, a_1) \setminus Vis(s, a_2)$ and $v_2 \in Vis(s, a_2) \setminus Vis(S, a_1)$ for some $s \in S, a_1, a_2 \in A$.
  2. And agents may choose their initial state! (contrary to vCGS init actions!)
A vCGS with broadcast within coalition $A$ (or $A$-cast) is such that, for all $a \in Ag$, $v \in V_a$ and $\gamma_a \in Act_a$:

(†$^A$) If $vis(v, b) ::= \top$ appears in $asg(\gamma_a)$ for some $b \in Ag \setminus \{a\}$, then also $vis(v, c) ::= \top$ is in $asg(\gamma_a)$ for every $c \in A \setminus \{a\}$.

- If $vis(v, c) ::= \bot$ appears in $asg(\gamma_a)$ for some $c \in A \setminus \{a\}$, then also $vis(v, b) ::= \bot$ is in $asg(\gamma_a)$ for every $b \in Ag \setminus \{a\}$.

- Agents have no obligation to reveal any of their atoms.
- If they choose to disclose some atoms, then coalition $A$ has to be informed.
- Individual indistinguishability for some agent $a \in A$ does not imply distributed knowledge among all agents in $A$.
- Generalized form of systems without information forks: information forks are allowed only at initial states (due to init actions, not because of A-cast visibility!).
Decidability for $A$-cast vCGS

Lemma 1

Given a joint strategy $F_A$ on some $A$-cast vCGS and two histories $h_1, h_2$ with $h_1 \sim_A^C h_2$, $h_1[1] = h_2[1]$, and $h_i \in \text{out}(h_1[1], \sigma_A)$ for $i = 1, 2$. Then $h_1 \sim_A^D h_2$ and also $F_a(h_1) = F_a(h_2)$ for all $a \in A$.

- This lemma does not imply that common knowledge and distributed knowledge coincide.
- There may still exist histories $h_1$ and $h_2$ with $h_1 \sim_A^C h_2$ but $h_1 \not\sim_A^D h_2$ – due to $h_1[1] \neq h_2[1]$. 
Decidability for A-cast vCGS

Theorem

The model checking problem for A-cast vCGS and A-formulas is decidable.

Proof idea:

- By Lemma 1, it suffices to remember the initial and final state for each history compatible with a joint A-strategy.
- Build a turn-based game with perfect information in which the protagonist simulates each winning strategy for coalition A on subsets of $S_0 \times S$ encoding information sets.
- Construction available for ATL with the subjective semantics – hence simple reachability or safety objectives.
CONCLUSIONS AND DIRECTIONS OF STUDY

• Agents with visibility control.
• Information forks can be allowed at initial states, without harming decidability of model-checking ATL.
• Generalizations of Lemma 1?
• Generalization for ATL*?
• Generalization for Strategy Logic?