In Processes, We Believe!

Marrying Process Algebra and Epistemic Logic

Francien Dechesne and Mohammad Mousavi

TbILLC: Special Session on Logic, Information and Agency

Outline

Outline

Outline

Outline

Outline

Background of the research

VEMPS project (2006-2009)

using epistemic logic for verification of security protocols

Background of the research

VEMPS project (2006-2009)

using epistemic logic for verification of security protocols

TU Eindhoven & CWI Amsterdam:
Yanjing Wang, Jan van Eijck, Francien Dechesne,
Erik de Vink, Simona Orzan, Mohammad Mousavi

Background of the research

VEMPS project (2006-2009)

using epistemic logic for verification of security protocols

TU Eindhoven & CWI Amsterdam:
Yanjing Wang, Jan van Eijck, Francien Dechesne,
Erik de Vink, Simona Orzan, Mohammad Mousavi

(dynamic) epistemic logic
$\Updownarrow$
process algebra, formal semantics, verification of distributed processes, security

The prototypical example: Dining Cryptographers

Operational vs. Epistemic

The Gap

approach\spec	**Protocol**	**Goal**
Operational	Intuitive	Non-trivial; Difficult with Knowledge Properties
Epistemic	Laborious	Intuitive; combination of epistemic and temporal constructs

Operational Approach: basic process algebra

Simple PA: Syntax

$$\begin{array}{lcl} a & ::= & a[?,!](\overrightarrow{k}) \\ p, q & ::= & a \mid a; p \mid p + q \mid p \parallel q \end{array}$$

1. receive: $a?(\overrightarrow{k})$, send: $a!(\overrightarrow{k})$, individual actions or synchronizations: $a(\overrightarrow{k})$;

Operational Approach: basic process algebra

Simple PA: Syntax

$$\begin{array}{lcl} a & ::= & a[?,!](\overrightarrow{k}) \\ p, q & ::= & a \mid a; p \mid p + q \mid p \mid\mid q \end{array}$$

1. receive: $a?(\overrightarrow{k})$, send: $a!(\overrightarrow{k})$,
   individual actions or synchronizations: $a(\overrightarrow{k})$;
2. action prefixing: $a; q$

Operational Approach: basic process algebra

Simple PA: Syntax

$$\begin{array}{lcl} a & ::= & a[?,!](\overrightarrow{k}) \\ p, q & ::= & a \mid a; p \mid p + q \mid p \mid\mid q \end{array}$$

1. receive: $a?(\overrightarrow{k})$, send: $a!(\overrightarrow{k})$,
   individual actions or synchronizations: $a(\overrightarrow{k})$;
2. action prefixing: $a; q$
3. nondeterministic choice: $p + q$ (or $\sum_{i \in I} p_i$);

Operational Approach: basic process algebra

Simple PA: Syntax

$$\begin{array}{lcl} a & ::= & a[?,!](\overrightarrow{k}) \\ p, q & ::= & a \mid a; p \mid p + q \mid p \mid\mid q \end{array}$$

1. receive: $a?(\overrightarrow{k})$, send: $a!(\overrightarrow{k})$,
   individual actions or synchronizations: $a(\overrightarrow{k})$;
2. action prefixing: $a; q$
3. nondeterministic choice: $p + q$ (or $\sum_{i \in I} p_i$);
4. parallel composition: $p \mid\mid q$
   where send and receive synchronize.

Operational Approach: basic process algebra

Simple PA: Syntax

$$\begin{array}{lcl} a & ::= & a[?,!](\overrightarrow{k}) \\ p, q & ::= & a \mid a; p \mid p + q \mid p \mid\mid q \end{array}$$

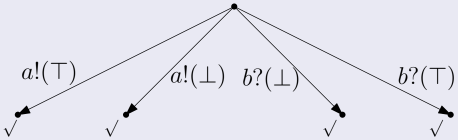
1. receive: $a?(\overrightarrow{k})$, send: $a!(\overrightarrow{k})$,
   individual actions or synchronizations: $a(\overrightarrow{k})$;
2. action prefixing: $a; q$
3. nondeterministic choice: $p + q$ (or $\sum_{i \in I} p_i$);
4. parallel composition: $p \mid\mid q$
   where send and receive synchronize.

Semantics:
labelled transition system generated by syntactic rules
(SOS: Structural Operational Semantics)

Operational Approach: basic process algebra

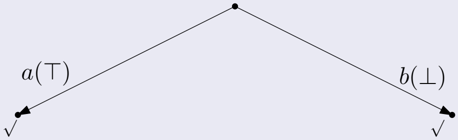
Simple PA: Intuitive Semantics

$$\sum_{i \in \{\top, \bot\}} (a!(i) + b?(i))$$



Simple PA: Intuitive Semantics

$$\sum_{i \in \{\top,\bot\}} (a!(i) + b?(i)) \,||\, (a?(\top) + b!(\bot))$$



Our approach

We try to bridge the gap by specifying *action visibilities* in the process algebraic protocol specification.
This creates the epistemic component in the behavior model.

Our approach

We try to bridge the gap by specifying *action visibilities* in the process algebraic protocol specification.
This creates the epistemic component in the behavior model.

Structural Operational Semantics: derived formally from PA-term syntax through set of rules.

(Reference: "Operational and Epistemic approaches to protocol analysis: Bridging the Gap", LPAR 2007. Cf. `http://www.win.tue.nl/~mousavi/pai.htm`)

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations
- To be able to capture different views of what happens

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations
- To be able to capture different views of what happens
- SOS-rules generate an *Annotated* LTS

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations
- To be able to capture different views of what happens
- SOS-rules generate an *Annotated* LTS
- which can be decomposed into LTS and Kripke model.

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations
- To be able to capture different views of what happens
- SOS-rules generate an *Annotated* LTS
- which can be decomposed into LTS and Kripke model.
- On these ALTSs we can check properties in our epistemic temporal language.

Bridging the gap: our proposal

- We extend actions in a simple process algebra with identity-annotations
- To be able to capture different views of what happens
- SOS-rules generate an *Annotated* LTS
- which can be decomposed into LTS and Kripke model.
- On these ALTSs we can check properties in our epistemic temporal language.
- (Spoiler) these ALTSs are like Interpreted Systems

Decorated actions:

$(J)\alpha$: action α is perceived as α by $i \in J$ and as $\rho(\alpha)$ by others.

Process Algebraic Framework with epistemics

Decorated actions:

$(J)\alpha$: action α is perceived as α by $i \in J$ and as $\rho(\alpha)$ by others.

where

- $J \subseteq Id$: the intended audience of a
- $\rho : A \rightarrow A \cup \{\tau\}$ a public appearance function
- τ: the invisible action

Process Algebraic Framework with epistemics

Decorated actions:

$(J)\alpha$: action α is perceived as α by $i \in J$ and as $\rho(\alpha)$ by others.

where

- $J \subseteq Id$: the intended audience of a
- $\rho : A \rightarrow A \cup \{\tau\}$ a public appearance function
- τ: the invisible action

Simple PA with views: Syntax

$$\begin{array}{lcl} d & ::= & (J)a[?,!](\overrightarrow{k}) \\ p, q & ::= & d \mid d;p \mid p+q \mid p \mid\mid q \end{array}$$

Process Algebraic Framework with epistemics

Decorated actions:

$(J)\alpha$: action α is perceived as α by $i \in J$ and as $\rho(\alpha)$ by others.

where

- $J \subseteq Id$: the intended audience of a
- $\rho : A \rightarrow A \cup \{\tau\}$ a public appearance function
- τ: the invisible action

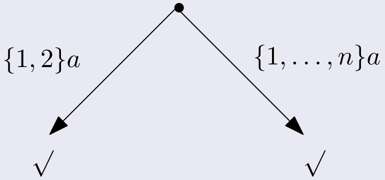
Simple PA with views: Syntax

$$\begin{array}{lcr} d & ::= & (J)a[?,!](\overrightarrow{k}) \\ p, q & ::= & d \mid d; p \mid p + q \mid p \mid\mid q \end{array}$$

($\Rightarrow \rho$ is now part of the protocol specification!)

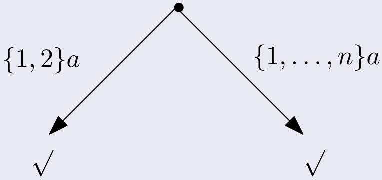
Simple PA with views: example

$$(\{2\}b! + (\{1,\ldots,n\})a) \mid\mid (\{1\})b?$$



Simple PA with views: example

$$(\{2\}b! + (\{1,\ldots,n\})a) \mid\mid (\{1\})b?$$



Suppose $\rho(b) = c$. Then in the left branch, $\{3,\ldots,n\}$ see c.

Formal semantics: operational part (Summarized)

$$(\mathbf{a})\,\frac{}{(d,\pi)\overset{d}{\Rightarrow}\surd_{\pi\frown d}}$$

$$(\mathbf{s0})\,\frac{(x_0,\pi)\overset{d}{\Rightarrow}(y_0,\pi')}{(x_0;x_1,\pi)\overset{d}{\Rightarrow}(y_0;x_1,\pi')} \qquad (\mathbf{s1})\,\frac{(x_0,\pi)\overset{d}{\Rightarrow}\surd_{\pi'}}{(x_0;x_1,\pi)\overset{d}{\Rightarrow}(x_1,\pi')}$$

$$(\mathbf{n0})\,\frac{(x_0,\pi)\overset{d}{\Rightarrow}(y_0,\pi')}{(x_0+x_1,\pi)\overset{d}{\Rightarrow}(y_0,\pi')} \qquad (\mathbf{p0})\,\frac{(x_0,\pi)\overset{d}{\Rightarrow}(y_0,\pi')}{(x_0\parallel x_1,\pi)\overset{d}{\Rightarrow}(y_0\parallel x_1,\pi')}$$

$$(\mathbf{p4})\,\frac{(x_0,\pi)\overset{(\mathrm{J})?a}{\Rightarrow}(y_0,\pi') \quad (x_1,\pi)\overset{(\mathrm{J}')!a}{\Rightarrow}(y_1,\pi'')}{(x_0\parallel x_1,\pi)\overset{(\mathrm{J}\cup\mathrm{J}')a}{\Rightarrow}(y_0\parallel y_1,\pi\frown(\mathrm{J}\cup\mathrm{J}')a)}$$

Formal semantics: epistemic part (Summarized)

$$\frac{}{\pi \stackrel{i}{=} \pi} \qquad \frac{i \in J}{\pi \frown J(a) \stackrel{i}{=} \pi \frown J(a)} \qquad \frac{\pi \stackrel{i}{=} \pi' \quad i \notin J \quad \rho(a) = \rho(b)}{\pi \frown J(a) \stackrel{i}{=} \pi' \frown J(b)}$$

$$\frac{\pi \stackrel{i}{\cdots} \pi' \quad i \notin J \quad \rho(a) = \tau}{\pi \frown J(a) \stackrel{i}{=} \pi} \qquad \frac{\pi \stackrel{i}{\cdots} \pi' \quad i \notin J \quad \rho(a) = \tau}{\pi \stackrel{i}{=} \pi' \frown J(a)}$$

Seminal book:

Fagin, Halpern, Moses, and Vardi. *Reasoning About Knowledge.* MIT Press, 1995.

Interpreted Systems as semantics for epistemic temporal logic.

Seminal book:

Fagin, Halpern, Moses, and Vardi. *Reasoning About Knowledge.* MIT Press, 1995.

Interpreted Systems as semantics for epistemic temporal logic.

Transition systems with rich states:

- global state is n-tuple of local states
- indistinguishability relations between global states generated on the basis of local state for each agent.

Interpreted Systems: framework

- Agents $\mathcal{I} = \{1, \ldots, n\}$
- Local states L_i, global states:$L = \prod_{i=1}^{n} L_i$
- Run r: a sequence of global states
- Protocol R: set of runs
- Valuation function $\nu : L \rightarrow \Phi$
- Indistinguishability $\overrightarrow{l} \overset{i}{\approx} \overrightarrow{l'}$ iff $l_i = l'_i$

Interpreted system: (R, ν)

Our focus: protocol component (not valuation)

Interpreted Systems: framework

- Agents $\mathcal{I} = \{1, \ldots, n\}$
- Local states L_i, global states:$L = \prod_{i=1}^{n} L_i$
- Run r: a sequence of global states
- Protocol R: set of runs (note: given, not generated)
- Valuation function $\nu : L \rightarrow \Phi$
- Indistinguishability $\overrightarrow{l} \overset{i}{\approx} \overrightarrow{l'}$ iff $l_i = l'_i$

Interpreted system: (R, ν)

Our focus: protocol component (not valuation)

Motivation

Work in progress!

Motivation

Work in progress!

We want to

- Link the process algebra specs to ISs
- Allow to transform results from one to the other:
  - PA as a syntax for generating ISs
  - exploited analysis tools available for IS
  - characterize semantic properties of classes of PA specs

Trace: sequence of decorated actions.

$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$[\![0]\!]_{aux} \quad \doteq \quad \langle\rangle$$

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$
\begin{array}{lcl}
[\![0]\!]_{aux} & \doteq & \langle\rangle \\
[\![d; p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux}
\end{array}
$$

IS for PA

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$
\begin{array}{lcl}
[\![0]\!]_{aux} & \doteq & \langle\rangle \\
[\![d; p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux} \\
[\![p + q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \cup [\![q]\!]_{aux}
\end{array}
$$

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$\begin{array}{lcl} [\![0]\!]_{aux} & \doteq & \langle\rangle \\ [\![d; p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux} \\ [\![p + q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \cup [\![q]\!]_{aux} \\ [\![p \mid\mid q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \mid\mid_{tr} [\![q]\!]_{aux} \end{array}$$

where $\mid\mid_{tr}$ auxiliary function

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$
\begin{array}{lcl}
[\![0]\!]_{aux} & \doteq & \langle\rangle \\
[\![d;p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux} \\
[\![p+q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \cup [\![q]\!]_{aux} \\
[\![p \mid\mid q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \mid\mid_{tr} [\![q]\!]_{aux}
\end{array}
$$

where $||_{tr}$ auxiliary function

$$
P \mid\mid_{tr} \emptyset \quad \doteq \quad \emptyset \mid\mid_{tr} P \qquad \doteq \quad P
$$

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$
\begin{array}{lcl}
[\![0]\!]_{aux} & \doteq & \langle\rangle \\
[\![d;p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux} \\
[\![p+q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \cup [\![q]\!]_{aux} \\
[\![p \mid\mid q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \mid\mid_{tr} [\![q]\!]_{aux}
\end{array}
$$

where $\mid\mid_{tr}$ auxiliary function

$$
\{\langle\rangle\} \uplus P \mid\mid_{tr} Q \quad \doteq \quad P \mid\mid_{tr} \{\langle\rangle\} \uplus Q \qquad \doteq \quad (P \mid\mid_{tr} Q)
$$

Trace: sequence of decorated actions.
$[\![-]\!]_{aux}$: *CCSi* process $\mapsto$ set of traces.

$$
\begin{array}{lcl}
[\![0]\!]_{aux} & \doteq & \langle\rangle \\
[\![d;p]\!]_{aux} & \doteq & d \frown [\![p]\!]_{aux} \\
[\![p+q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \cup [\![q]\!]_{aux} \\
[\![p \mid\mid q]\!]_{aux} & \doteq & [\![p]\!]_{aux} \mid\mid_{tr} [\![q]\!]_{aux}
\end{array}
$$

where $\mid\mid_{tr}$ auxiliary function

$$
\begin{array}{l}
\{(\mathtt{J})\alpha \frown tr\} \uplus P \mid\mid_{tr} \{(\mathtt{J}')\alpha' \frown tr'\} \uplus Q \quad \doteq \\
\qquad (\mathtt{J})\alpha \frown (\{tr\} \uplus P \mid\mid_{tr} \{(\mathtt{J}')\alpha' \frown tr'\} \uplus Q) \cup \\
\qquad (\mathtt{J}')\alpha' \frown (\{(\mathtt{J})\alpha \frown tr'\} \uplus \{tr\} \uplus P \mid\mid_{tr} Q) \cup \\
\qquad \bigcup \{(\mathtt{J} \cup \mathtt{J}')a \frown (\{tr\} \uplus P \mid\mid_{tr} \{tr'\} \cup Q) \mid (\mathtt{J}')a \frown tr' \in Q \\
\qquad\quad (\alpha = a? \wedge \alpha' = a!) \vee (\alpha = a! \wedge \alpha' = a?)\}
\end{array}
$$

IS for PA

$$[\![p]\!]_{tr} = \{tr \mid tr \in [\![p]\!]_{aux} \wedge closed(tr)\}$$

(‘$closed(tr)$: tr contains no send or receive actions)

Formal Results

Comparing operational and IS-semantics:

- There is a one-one correspondence between local states of the protocol in IS semantics and local trace projections in operational semantics

Formal Results

Comparing operational and IS-semantics:

- There is a one-one correspondence between local states of the protocol in IS semantics and local trace projections in operational semantics

Consider finite initialized and prefix-closed (fipc) ISs. Characterizing the class of ISs generated:

- If $|A| = 1$: for each fipc interpreted system R, there is a process algebraic description p such that $[\![p]\!]_{tr} = R$.
- For $|A| \geq 2$ and at least 2 agents: there exist fipc ISs that cannot be generated by any process algebraic specification.

Towards Characterization

Cf. embedding of DEL in ISs (van Benthem et al):

- Perfect Recall: by construction
- Synchronicity: depends on properties ρ
- Uniform No Miracles: ??

Future work: relate different ρ-types to structural properties of epistemic relations in ISs.
(E.g. with additional parameters distinguishing more groups of agents.)

Final conclusions

We propose to include epistemic elements in operational specification.

Final conclusions

We propose to include epistemic elements in operational specification.

A connection to interpreted systems helps to open the tools developed for multi-agent systems.

Final conclusions

We propose to include epistemic elements in operational specification.

A connection to interpreted systems helps to open the tools developed for multi-agent systems.

On the theoretical level, it will be interesting to characterize the class of ISs generated by our framework. (Like van Benthem et al. 2010 did for DEL.)

Final conclusions

We propose to include epistemic elements in operational specification.

A connection to interpreted systems helps to open the tools developed for multi-agent systems.

On the theoretical level, it will be interesting to characterize the class of ISs generated by our framework. (Like van Benthem et al. 2010 did for DEL.)

Any questions?

Final conclusions

We propose to include epistemic elements in operational specification.

A connection to interpreted systems helps to open the tools developed for multi-agent systems.

On the theoretical level, it will be interesting to characterize the class of ISs generated by our framework. (Like van Benthem et al. 2010 did for DEL.)

Thank You!!!