Logical Omniscience in the Semantics of BAN Logic

Mika Cohen, Mads Dam

LECS/ICT/KTH
Stockholm, Sweden

FCS'05, 2005-07-01

Logical omniscience problem

Combination knowledge - computation/cryptography problematic

- Difference between *feasibly computable* - and *logical* consequence

Wanted:

1. Agent knows all *feasibly computable* consequences of what it knows

Not wanted:

2. Agent knows all *logical* consequences of what it knows

Logical omniscience problem: Obtain (1) but avoid (2)

Logical omniscience problem in BAN

Example

- $\mathit{fresh}\ M \models \mathit{fresh}\ \{M\}_K$

Logical omniscience

- $\Box_a\ \mathit{fresh}\ M \models \Box_a\ \mathit{fresh}\ \{M\}_K$

But

- $\mathit{fresh}\ \{M\}_K$ **not** feasibly computable from $\mathit{fresh}\ M$

BAN

- Feasible cryptographic computation $\approx$ Dolev-Yao
- $\Box_a\ K\ \mathit{good\ for}\ a \cdot b,\ \Box_a\ \mathit{fresh}\ M \models \Box_a\ \mathit{fresh}\ \{M\}_K$
  - Typical BAN rule

Why is logical omniscience an issue for BAN?

BAN is a just proof system

- Deductive protocol verification

Can we bring semantical methods to BAN?

- Model checking
- Checking BAN extensions/variations
- Semantically based theorem provers (for BAN extensions)
- Knowledge programs

If semantics makes agents logically omniscient:

- Semantics is unfaithful to BAN
- Semantical methods are untrustworthy

Logical omniscience in all existing semantics for BAN-like logics

Objective

Solve the logical omniscience problem in the semantics of BAN

Requirements on our semantics

1. Knowledge is **not** closed under *logical* consequences
2. Knowledge is closed under *feasibly computable* consequences
3. Validates BAN

Why not require completeness w.r.t. BAN?

- BAN open ended, vaguely defined proof system
- "Add new proof rules as needed"

Completeness w.r.t. "conservative" extension desirable

- Return to this in conclusion

Existing semantics for BAN-like logics

Classical multi-agent system semantics

Canonical in computer science

- Fagin/Halpern/Moses/Vardi (95)

Applied to BAN

- Syverson (01), Decker (01), Halpern/Pucella/Meyden (03), Jacobs (04)

Classical semantics: Truth condition

Multi-agent system

- Set of system states $s, s', \ldots$
- $s|a$ is local state of a in s
  - "All data available to a at s"
  - Eg. local action trace

Agent knows a fact if her local state forces the fact

- $s \models \Box_a F \Leftrightarrow \forall s' : s|a = s'|a \Rightarrow s' \models F$

Classical semantics: Example

Example system

$$\bullet \xrightarrow{b\ sen\ M} \bullet \xrightarrow{a\ rec\ M} \bullet \qquad \begin{array}{l} \neg\Box_a\ b\ sent\ M \\ \Box_a\ a\ received\ M \end{array}$$

$$\bullet \xrightarrow{c\ sen\ M} \bullet \xrightarrow{a\ rec\ M} \bullet$$

Receive introspection

- $a\ received\ M \models \Box_a\ a\ received\ M$

Logical omniscience

Combination more problematic than logical omniscience alone

AT-style semantics

- Multi-agent system semantics adjusted for crypto communication
- **A**badi/**T**uttle 91
- Refinements/variations
  - Syverson/Oorschot (96), Wedel/Kessler (95)

AT-style semantics: Truth condition

Hides parts of local state to agent herself

- *Hide* replaces unopened cipher texts with $\bot$
- $\mathit{Hide}(\text{a receives } \{M\}_K) = \text{a receives} \bot$

Agent knows a fact if her local state *after hiding* forces the fact

- $s \models \Box_a F \Leftrightarrow \forall s' : \mathit{Hide}(s|a) = \mathit{Hide}(s'|a) \Rightarrow s' \models F$

AT-style semantics: Example

Example system

$$\bullet \xrightarrow{b\ sen\ \{M\}_K} \bullet \xrightarrow{a\ rec\ \{M\}_K} \bullet_s \quad \neg\Box_a\, a\ received\ \{M\}_K$$

$$\bullet \xrightarrow{c\ sen\ \{M'\}_{K'}} \bullet \xrightarrow{a\ rec\ \{M'\}_{K'}} \bullet_{s'}$$

$Hide(s|a) = Hide(s'|a) = \text{a rec} \perp$

Receive introspection broken

- $a\ received\ M \not\models \Box_a\, a\ received\ M$
- BAN invalidated

Logical omniscience

Kripke semantics

Standard frame work for modal logics

Agent knows a fact if fact holds at every obs. eq. state

- $s \models \Box_a F \Leftrightarrow \forall s' : s \equiv_a s' \Rightarrow s' \models F$
- $s \equiv_a s'$ iff s and s equivalent up to a:s power of observation

Classical multi-agent system semantics

- $s \equiv_a s' \Leftrightarrow s|a = s'|a$

AT semantics

- $s \equiv_a s' \Leftrightarrow \mathit{Hide}(s|a) = \mathit{Hide}(s'|a)$

Logical omniscience in Kripke

Assume

1 $\Delta \models F$
2 $s \models \Box_a \Delta$
3 $s \equiv_a s'$

$2 + 3 \Rightarrow$

4 $s' \models \Delta$

$1 + 4 \Rightarrow$

5 $s' \models F$

$3 + 5 \Rightarrow$

6 $s \models \Box_a F$

A generalization of Kripke

Epistemic equivalence indexed by renamings

Example system again

$\bullet \xrightarrow{b\ sen\ \{M\}_K} \bullet \xrightarrow{a\ rec\ \{M\}_K} \bullet_s$

$\bullet \xrightarrow{c\ sen\ \{M'\}_{K'}} \bullet \xrightarrow{a\ rec\ \{M'\}_{K'}} \bullet_{s'}$

$\{M\}_K$ at s corresponds for a to $\{M'\}_{K'}$ at s'

- Observable properties of $\{M\}_K$ at s
  =
  Observable properties of $\{M'\}_{K'}$ at s'

We make $\equiv_a$ keep track of message correspondences

- Index $\equiv_a$ by renaming r of messages

$s \equiv_a^r s'$

- s and s' observationally equivalent for a
- M at s corresponds for a to $r(M)$ at s', for all M

Requirements for $s \equiv_a^r s'$

r should respect local state

- $r(s|a) = s'|a$

r should respect keys used

- $K \textit{ used by a at } s \Rightarrow r(\{M\}_K) = \{r(M)\}_{r(K)}$

  $\vdots$

We return later to "*K used by a at s*"

New truth condition for knowledge

Agent knows message satisfies property if corresponding messages at obs. eq. states satisfy property

- $s \models \Box_a F(M) \Leftrightarrow \forall s' : \forall r : s \equiv_a^r s' \Rightarrow s' \models F(r(M))$

Example system

$$\bullet \xrightarrow{b\ sen\ \{M\}_K} \bullet \xrightarrow{a\ rec\ \{M\}_K} \bullet\ \Box_a\ a\ received\ \{M\}_K$$

$$\bullet \xrightarrow{c\ sen\ \{M'\}_{K'}} \bullet \xrightarrow{a\ rec\ \{M'\}_{K'}} \bullet$$

Receive introspection restored

Agents do **not** know all *logical* consequences

1. $\Delta \models F$

   $s \models \Box_a \Delta$

   $s \equiv_a^r s'$

   $\Rightarrow$

   $s' \models r(\Delta)$

   $\Rightarrow \cdots$

   (1) is irrelevant!

   $r(\Delta) \models r(F)$ needed to obtain $s \models \Box_a F$

Agents know all *feasibly computable* consequences

"feasibly computable consequence" vague

- No existing attempt to make precise for BAN-like logics

Our proposal

- $\Delta \models F \Rightarrow \text{a uses} \, \text{Keys}(\Delta, F), \; \Box_a \Delta \models \Box_a F$

Example

- $\mathit{fresh}\ x \models \mathit{fresh}\ \{x\}_y \Rightarrow a\ \mathit{uses}\ \text{y}, \; \Box_a\, \mathit{fresh}\ x \models \Box_a\, \mathit{fresh}\ \{x\}_y$
- Univ. subst. $\Rightarrow a\ \mathit{uses}\ K, \; \Box_a\, \mathit{fresh}\ M \models \Box_a\, \mathit{fresh}\ \{M\}_K$

Abstraction of BAN rules

BAN validated

Soundness lemma 1: Keys known are used

- $\Box_a K\ good\ a \cdot b \models a\ uses\ K$
- Implicit in BAN
- Depends on definition of *keys used*

Customary definition: Keys used are the keys extracted

- Received and initially possessed messages closed under un-pairing and decryption
- Lemma (1) fails in some models

New definition: Keys used are the keys known

- $s \models a\ uses\ K \Leftrightarrow \exists$ predicate $p :\ s \models \Box_a\ p(K)$
- (1) immediate

Keys used are the keys known (Details)

Cannot define *a uses* by $\Box_a$ directly

- $\Box_a$ defined by $\equiv_a^r$ defined by *a uses*

Can define *a uses* and $\Box_a$ through mutual recursion

We select least definition of *a uses* satisfying

- $s \models a \; uses \; K \Leftrightarrow \exists$ predicate $p : \; s \models \Box_a \, p(K)$

Always exists

Recent work: If predicates only apply to existing messages:

- New definition eq. to customary
- BAN predicates need slight modification

S5 axioms

- T $\Box_a F \models F$
  - $s \equiv_a^{\iota} s$ ("Reflexivity")
- 4 $\Box_a F \models \Box_a \Box_a F$
  - $s \equiv_a^{r} s', \quad s' \equiv_a^{r'} s'' \Rightarrow s \equiv_a^{r' \circ r} s''$ ("Transitivity")
- 5 $\neg \Box_a F \models \Box_a \neg \Box_a F$
  - $s \equiv_a^{r} s' \Rightarrow s' \equiv_a^{r^{-1}} s$ ("Symmetry")

Other related work

- Counterpart semantics
  - Lewis (68)
  - Not computationally grounded
  - Agents are logically omniscient
- Resource bounded knowledge
  - Fagin/Halpern/Moses/Vardi (95)
  - None attempted for BAN
  - Breaks radically with Kripke semantics

Conclusion

Summary

Kripke semantics

1 Agent knows all *logical* consequences of what she knows

Intended in BAN:

2 Agent knows all *feasibly computable* consequences of what she knows

Mismatch makes Kripke semantics of limited use for BAN

We propose a generalization of Kripke

- Epistemic equivalence relation keeps track of message correspondences
- Avoids (1)
- Achieves (2)
- Validates BAN

Application: Semantically based methods

- Model checking

⋮

Current work

Completeness

- For multi-agent models
- For message passing systems and fixed vocabulary

Semantics for first-order extension

- Useful when data is complex, partly hidden
- Translation of BAN related logics

Thanks!