Parallel dynamic logic with communication

L. Aszalós P. Balbiani

Institut de recherche en informatique de Toulouse
LILaC group

Purpose

- Verification of cryptographic protocols
  - messages
  - actions
  - agents
- Modal logic for formal verification

Problem

Communication in open networks

Alice (A) and Bob (B) want to exchange messages,
but Intruder (I) controls the communication lines.

Objectives

Alice sends the message m to Bob.

Confidentiality: A knows that only B can understand m.
Authenticy: B knows that only A could create m.
Integrity of data: m is not altered.

Intruder

Can spy, divert, record, replay, modify messages.
Cannot decrypt messages without keys.

Cryptography

We can protect our messages with encription:

$$\begin{array}{ll} \text{plaintext} & \\ \quad\downarrow & encryption \\ \text{ciphertext} & \\ \quad\downarrow & decryption \\ \text{plaintext} & \end{array}$$

- With *symmetric key encryption* we use the same key to encrypt and decrypt messages: $E(k_{AB}, E(k_{AB}, m)) = m$.
- With *public key encryption* we have pairs of keys: $k_A(k_A^{-1}(m)) = m$ and $k_A^{-1}(k_A(m)) = m$. k_A is the *public key* and k_A^{-1} is the *private key*.

Attacks

Needham-Schroeder public key protocol

Message 1. $A \to B$: $k_B(N_A, A)$
Message 2. $B \to A$: $k_A(N_A, N_B)$
Message 3. $A \to B$: $k_B(N_B)$

Attack

1.	$A \to I$:	$k_I(N_A, A)$
1'.	$I(A) \to B$:	$k_B(N_A, A)$
2'.	$B \to I(A)$:	$k_A(N_A, N_B)$
2.	$I \to A$:	$k_A(N_A, N_B)$
3.	$A \to I$:	$k_I(N_B)$
3'.	$I(A) \to B$:	$k_B(N_B)$

Basic modal logic

$$A = p_k \mid \neg A \mid A \vee B \mid \Box A$$

Model $\mathcal{M} = \langle W, R, V \rangle$

W set of possible words

V is a valuation
$\{p_1, p_2, \ldots\} \times W \to \{0, 1\}$

R is a relation
$R \subseteq W \times W$

$s \models_{\mathcal{M}} \Box A$ iff for all t, if sRt then $t \models_{\mathcal{M}} A$.

Logic of actions

Actions:

$$\lambda \mid \pi_k \mid A? \mid (\alpha;\beta) \mid (\alpha \cup \beta)$$

$$A = p_k \mid \neg A \mid A \vee B \mid [\alpha]A$$

Model $\mathcal{M} = \langle W, R, V \rangle$

$R_\alpha \subseteq W \times W$

$R_{\alpha\cup\beta} = R_\alpha \cup R_\beta$, $R_{\alpha;\beta} = R_\alpha \circ R_\beta$

$s \models_{\mathcal{M}} [\alpha]A$ iff for all t, if $sR_\alpha t$ then $t \models_{\mathcal{M}} A$.

Parallel actions

$$\alpha = \lambda \mid \pi_k \mid A? \mid (\alpha; \beta) \mid (\alpha \cup \beta) \mid \mathtt{send}(m) \mid \mathtt{rec}(m)$$

$$A = p_k \mid \neg A \mid A \vee B \mid [\alpha \,\|\, \beta]A$$

model $\mathcal{M} = (W_1, W_2, R_1, R_2, V)$

- W_1 and W_2 are nonempty sets of local states,
- R_1 and R_2 are families of binary relations
  $R_1(\pi) \subseteq W_1 \times W_1$ and
  $R_2(\pi) \subseteq W_2 \times W_2$, for all atomic programs π,
- V is a valuation on $W_1 \times W_2$,
  $V(p_j) \subseteq W_1 \times W_2$, for all propositional variables p_j.

Communication

Actions

$\texttt{send}(m)$ and $\texttt{rec}(m)$

- No lost messages.
- The messages are received in the same order as they are sent.

It is possible that agent 2 does not read yet some messages sent by agent 1 and vice versa.

Global state

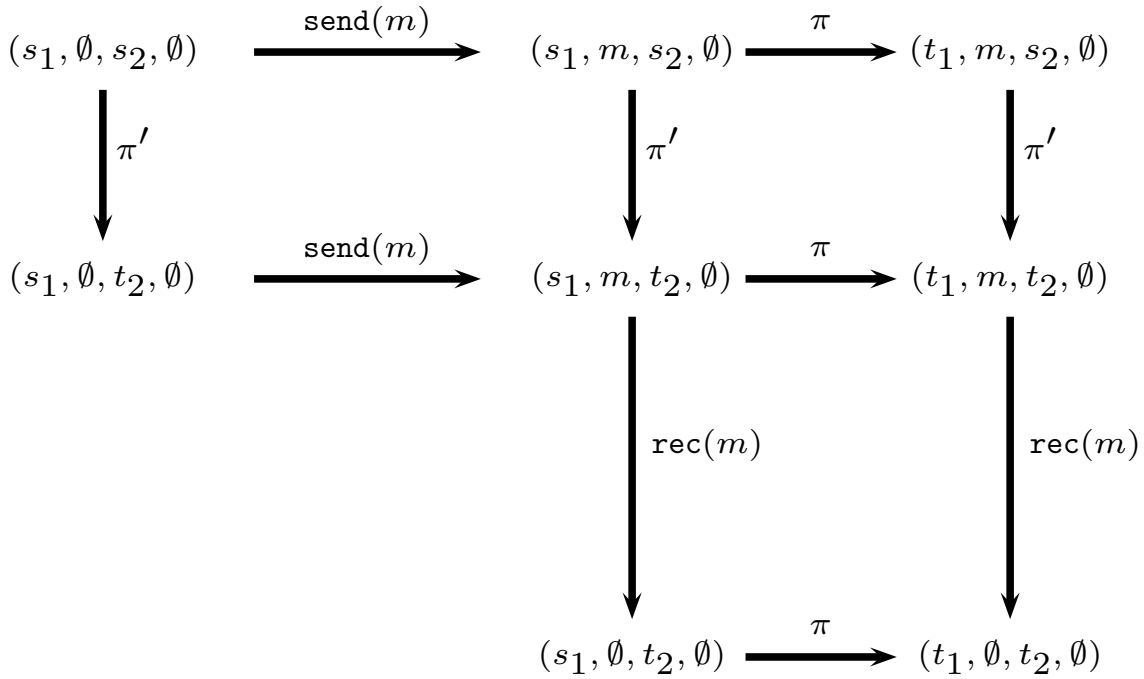
(s_1, c_1, s_2, c_2), where

- $s_1 \in W_1$ is the current local state of the first agent,
- c_1 is the list of all the messages sent by the first agent but laid unread by the second agent,
- $s_2 \in W_2$ is the current local state of the first agent
- c_2 is the list of all the messages sent by the second agent but laid unread by the first agent.

Truth relation

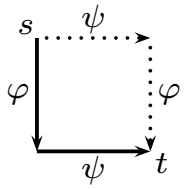
- $(s_1, c_1, s_2, c_2) \models_{\mathcal{M}} p$ iff $(s_1, s_2) \in V(p)$.
- $(s_1, c_1, s_2, c_2) \models_{\mathcal{M}} [\alpha \parallel \beta] A$ iff for all (t_1, d_1, t_2, d_2), if $(s_1, c_1, s_2, c_2) R_{\alpha \parallel \beta} (t_1, d_1, t_2, d_2)$ then $(t_1, d_1, t_2, d_2) \models_{\mathcal{M}} A$.

$$\alpha = \mathtt{send}(m); \pi \quad \beta = \pi'; \mathtt{rec}(m)$$



Properties

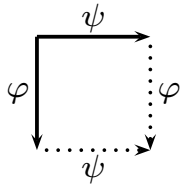
Commutativity properties



$$[\varphi \,\|\, \lambda][\lambda \,\|\, \psi]A \leftrightarrow [\lambda \,\|\, \psi][\varphi \,\|\, \lambda]A$$

	π_j	$B?$	$\mathtt{send}(m)$	$\mathtt{rec}(m)$
π_i	•		•	•
$A?$		•		
$\mathtt{send}(m)$	•		•	
$\mathtt{rec}(m)$	•			•

Confluence properties



$$\langle\varphi \,\|\, \lambda\rangle[\lambda \,\|\, \psi]A \rightarrow [\lambda \,\|\, \psi]\langle\varphi \,\|\, \lambda\rangle A$$

	π_j	$B?$	$\mathtt{send}(m)$	$\mathtt{rec}(m)$
π_i	•		•	•
$A?$		•		
$\mathtt{send}(m)$	•		•	•
$\mathtt{rec}(m)$	•		•	•

Conclusion

Results

- Tableau method (sound, complete)
- Axiomatization of a fragment (sound, complete)
- Decidability in nonelementary time

Open problems

- axiomatization of the full language
- cryptography, epistemic modalities