Towards a Tree of Channels

Xudong GUAN, INRIA Sophia-Antipolis

Introduction

Starting points: Dπ, $lsd\pi$, npict

- process/resource distribution - FLAT
- migration + local communication

How about HIERARCHICAL localities?

- administrative domains and firewalls
- hierarchical security policy
- hierarchical failure semantics
- models: ambients, seal, DJoin-M-kell, LAπ, MR

A Secret-Passing Example

In π:

$$\mathtt{n}(x)p \mid (\nu\, \mathtt{a})(\mathtt{n}\langle \mathtt{a} \rangle \mid q) \longrightarrow (\nu\, \mathtt{a})(p\{x := \mathtt{a}\} \mid q)$$

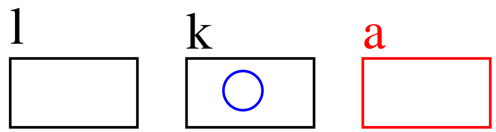
(one global location)

In Dπ:

$$\mathtt{l}[\mathtt{n}(x)p] \mid (\nu\, \mathtt{a})(\mathtt{k}[\mathbf{go}\ \mathtt{l}.\mathtt{n}\langle \mathtt{a} \rangle] \mid \mathtt{a}[q])$$

$$\longrightarrow^{*} (\nu\, \mathtt{a})(\mathtt{l}[p\{x := \mathtt{a}\}] \mid \mathtt{a}[q])$$

flat locations

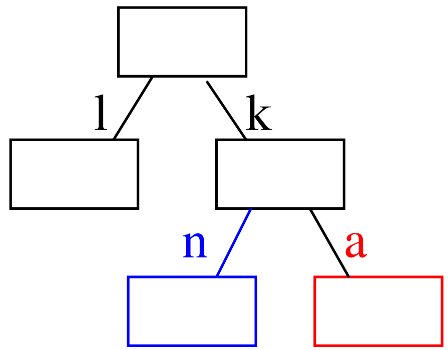


In mobile ambients:

$$\mathtt{l}[\mathbf{open}\ \mathtt{n}.(x)p] \mid \mathtt{k}[(\nu\, \mathtt{a})(\mathtt{n}[\mathbf{out}\ \mathtt{k}.\mathbf{in}\ \mathtt{l}.\langle \mathbf{out}\ \mathtt{l}.\mathbf{in}\ \mathtt{k}.\mathbf{in}\ \mathtt{a} \rangle] \mid \mathtt{a}[q])]$$

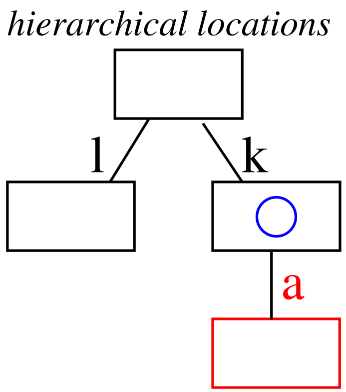
$$\longrightarrow^{*} (\nu\, \mathtt{a})(\mathtt{l}[p\{x := \mathbf{out}\ \mathtt{l}.\mathbf{in}\ \mathtt{k}.\mathbf{in}\ \mathtt{a}\}] \mid \mathtt{k}[\mathtt{a}[q]])$$

hierarchical locations



A Secret-Passing Example - cont.

In our model — Tπ:



$$\mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\, \mathtt{a})(\uparrow.\mathtt{l}\, \langle \mathtt{a} \rangle \mid \mathtt{a}[q])]$$

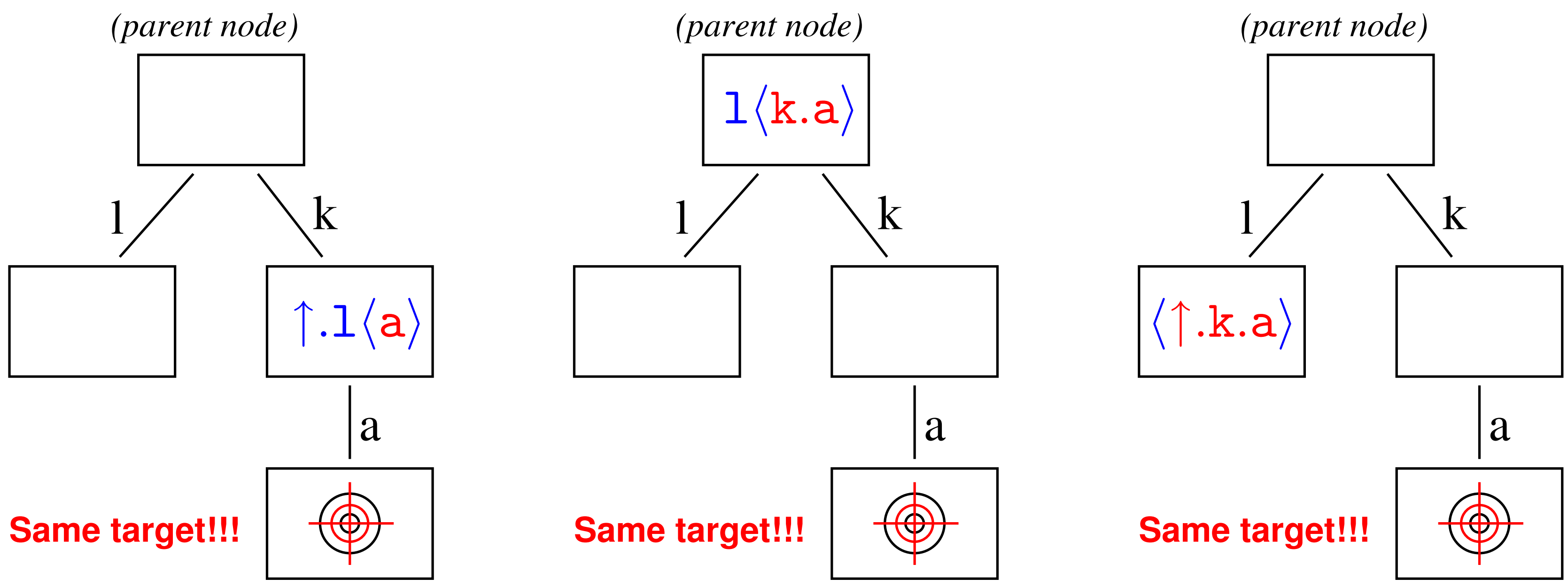
$\longrightarrow \quad (\nu\, \mathtt{k.a})(\mathtt{l}[(x)p] \mid \mathtt{l}\langle \mathtt{k.a} \rangle \mid \mathtt{k}[\mathtt{a}[q]])$ *migration — upward*

$\longrightarrow \quad (\nu\, \mathtt{k.a})(\mathtt{l}[(x)p \mid \langle \uparrow.\mathtt{k.a} \rangle] \mid \mathtt{k}[\mathtt{a}[q]])$ *migration — downward*

$\longrightarrow \quad (\nu\, \mathtt{k.a})(\mathtt{l}[p\{x := \uparrow.\mathtt{k.a}\}] \mid \mathtt{k}[\mathtt{a}[q]])$ *local anony. comm.*

Address Translation during Migration

$$\mathtt{k}[\uparrow.\mathtt{l}\ \langle \mathtt{a} \rangle] \quad \longrightarrow \quad \mathtt{l}\ \langle \mathtt{k.a} \rangle \quad \longrightarrow \quad \mathtt{l}[\langle \uparrow.\mathtt{k.a} \rangle]$$



Formalization

Syntax of Tπ

Strings:

$$
\begin{array}{rcll}
s, t & ::= & \varepsilon & \text{empty} \\
 & | & \mathtt{a}.s & \text{concatenation}
\end{array}
$$

Addresses:

$$
\begin{array}{rcll}
g, h & ::= & s & \text{string} \\
 & | & \uparrow.g & \text{up one level}
\end{array}
$$

Values:

$$
\begin{array}{rcll}
u, v & ::= & g & \text{address} \\
 & | & x & \text{variable}
\end{array}
$$

Processes:

$$
\begin{array}{rcll}
P, Q & ::= & \mathbf{0} & \text{empty} \\
 & | & P \mid P' & \text{parallel composition} \\
 & | & !\,P & \text{replication} \\
 & | & \mathtt{a}[P] & \text{location} \\
 & | & (\nu\, s)P & \text{restriction, } s \neq \varepsilon \\
 & | & u\,\chi & \text{mobile agents}
\end{array}
$$

Anonymous communication:

$$
\begin{array}{rcll}
\chi & ::= & \langle \tilde{u} \rangle & \text{polyadic output} \\
 & | & (\tilde{x})p & \text{polyadic input}
\end{array}
$$

Threads: p, q processes without locations

Binding Rules

A restriction binds addresses pointing to the restricted location:

$$\mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\,\mathtt{a})(\uparrow.\mathtt{l}\,\langle\mathtt{a}\rangle \mid \mathtt{a}[q])]$$

$$\longrightarrow \quad (\nu\,\mathtt{k.a})(\mathtt{l}[(x)p] \mid \mathtt{l}\langle\mathtt{k.a}\rangle \mid \mathtt{k}[\mathtt{a}[q]]) \qquad \textit{migration — upward}$$

$$\longrightarrow \quad (\nu\,\mathtt{k.a})(\mathtt{l}[(x)p \mid \langle\uparrow.\mathtt{k.a}\rangle] \mid \mathtt{k}[\mathtt{a}[q]]) \qquad \textit{migration — downward}$$

$$\longrightarrow \quad (\nu\,\mathtt{k.a})(\mathtt{l}[p\{x := \uparrow.\mathtt{k.a}\}] \mid \mathtt{k}[\mathtt{a}[q]]) \qquad \textit{local anony. comm.}$$

Structural Rules

SPLIT	$\mathtt{a}[P \mid Q] \equiv \mathtt{a}[P] \mid \mathtt{a}[Q]$	
GARB	$\mathtt{a}[\mathbf{0}] \equiv \mathbf{0}$	
RES-LOC	$\mathtt{a}[(\nu\, s)P] \equiv (\nu\, \mathtt{a}.s)\mathtt{a}[P]$,	if $fa(P)/_{\uparrow.\mathtt{a}.s} = \emptyset$

Reduction Rules - I

COMM $(\tilde{x})p \mid \langle \tilde{u} \rangle \longrightarrow p\{\tilde{x} := \tilde{u}\}$

R-CTX $P \longrightarrow Q \Longrightarrow P \mid R \longrightarrow Q \mid R$

$P \longrightarrow Q \Longrightarrow (\nu\, s)P \longrightarrow (\nu\, s)Q$

$P \longrightarrow Q \Longrightarrow \mathtt{a}[P] \longrightarrow \mathtt{a}[Q]$

R-STRUCT $P \equiv P',\ P' \longrightarrow P'',\ P'' \equiv P''' \quad \Longrightarrow \quad P \longrightarrow P'''$

Reduction Rules - II

Migration rules and address translation:

Up	$\mathtt{a}[\uparrow.g\,\chi] \longrightarrow g\,(\mathtt{a} \oplus \chi)$	$\mathtt{a} \oplus \uparrow.g$	$\triangleq$	g	
		$\mathtt{a} \oplus g$	$\triangleq$	$\mathtt{a}.g$	otherwise

e.g. $\mathtt{k}[\uparrow.\mathtt{l}\langle \mathtt{a},\ \uparrow.\mathtt{l}.\mathtt{b}\rangle] \longrightarrow \mathtt{l}(\mathtt{k} \oplus \langle \mathtt{a},\ \uparrow.\mathtt{l}.\mathtt{b}\rangle) = \mathtt{l}\langle \mathtt{k}.\mathtt{a},\ \mathtt{l}.\mathtt{b}\rangle$

Dn	$\mathtt{a}.g\,\chi \longrightarrow \mathtt{a}[\,g\ ({}^{\mathtt{a}}\!\uparrow \oplus \chi)]$	${}^{\mathtt{a}}\!\uparrow \oplus \mathtt{a}.t$	$\triangleq$	t	
		${}^{\mathtt{a}}\!\uparrow \oplus g$	$\triangleq$	$\uparrow.g$	otherwise

e.g. $\mathtt{l}\langle \mathtt{k}.\mathtt{a},\ \mathtt{l}.\mathtt{b}\rangle \longrightarrow \mathtt{l}[{}^{\mathtt{l}}\!\uparrow \oplus \langle \mathtt{k}.\mathtt{a},\ \mathtt{l}.\mathtt{b}\rangle] = \mathtt{l}[\langle \uparrow.\mathtt{k}.\mathtt{a},\ \mathtt{b}\rangle]$

Important: bound addresses in χ are **not** translated.

Dynamic Creation of Locations

Before passing the secret ...

$$
\begin{array}{lll}
 & \mathtt{l}[(x)p] \mid \mathtt{k}[\langle\uparrow.\mathtt{l}\rangle] \mid \mathtt{k}\,(x)(\nu\,\mathtt{a})(x\,\langle\mathtt{a}\rangle \mid \mathtt{a}\langle\varepsilon\rangle) & \\
\longrightarrow & \mathtt{l}[(x)p] \mid \mathtt{k}[\langle\uparrow.\mathtt{l}\rangle \mid (x)(\nu\,\mathtt{a})(x\,\langle\mathtt{a}\rangle \mid \mathtt{a}\langle\uparrow\rangle)] & \textsc{Dn+Split} \\
\longrightarrow & \mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\,\mathtt{a})(\uparrow.\mathtt{l}\,\langle\mathtt{a}\rangle \mid \mathtt{a}\langle\uparrow\rangle)] & \textsc{Comm} \\
\longrightarrow & \mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\,\mathtt{a})(\uparrow.\mathtt{l}\,\langle\mathtt{a}\rangle \mid \mathtt{a}[\langle\uparrow.\uparrow\rangle])] & \textsc{Dn} \\
 & & \\
= & \mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\,\mathtt{a})(\uparrow.\mathtt{l}\,\langle\mathtt{a}\rangle \mid \mathtt{a}[q])] & \text{let } q = \langle\uparrow.\uparrow\rangle \\
\longrightarrow & (\nu\,\mathtt{k.a})(\mathtt{l}[(x)p] \mid \mathtt{l}\langle\mathtt{k.a}\rangle \mid \mathtt{k}[\mathtt{a}[q]]) & \textsc{Up} \\
\longrightarrow & (\nu\,\mathtt{k.a})(\mathtt{l}[(x)p \mid \langle\uparrow.\mathtt{k.a}\rangle] \mid \mathtt{k}[\mathtt{a}[q]]) & \textsc{Dn} \\
\longrightarrow & (\nu\,\mathtt{k.a})(\mathtt{l}[p\{x := \uparrow.\mathtt{k.a}\}] \mid \mathtt{k}[\mathtt{a}[q]]) & \textsc{Comm}
\end{array}
$$

Migrating Arbitrary Processes

Packing processes to threads $\langle\!\langle P \rangle\!\rangle_\varepsilon$:

$$\begin{aligned}
\langle\!\langle \mathbf{0} \rangle\!\rangle_s &\triangleq \mathbf{0} & \langle\!\langle \mathtt{a}[P] \rangle\!\rangle_s &\triangleq \langle\!\langle P \rangle\!\rangle_{s.\mathtt{a}} \\
\langle\!\langle P \mid Q \rangle\!\rangle_s &\triangleq \langle\!\langle P \rangle\!\rangle_s \mid \langle\!\langle Q \rangle\!\rangle_s & \langle\!\langle (\nu\, t) P \rangle\!\rangle_s &\triangleq (\nu\, s.t) \langle\!\langle P \rangle\!\rangle_s \\
\langle\!\langle\, !\, P \rangle\!\rangle_s &\triangleq\ !\, \langle\!\langle P \rangle\!\rangle_s & \langle\!\langle u\, \chi \rangle\!\rangle_s &\triangleq (s \oplus u)\, (s \oplus \chi)
\end{aligned}$$

e.g. $\langle\!\langle \mathtt{l}[(x)p] \mid \mathtt{k}[(\nu\, \mathtt{a})(\uparrow.\mathtt{l}\, \langle \mathtt{a} \rangle \mid \mathtt{a}[q])] \rangle\!\rangle_\varepsilon = \mathtt{l}(x)p' \mid (\nu\, \mathtt{k.a})(\mathtt{l}\langle \mathtt{k.a} \rangle \mid q')$

Migration:

$$u(x)P \triangleq u(x)\langle\!\langle P \rangle\!\rangle_\varepsilon$$

Correspondance (conjecture):

$$P \simeq \langle\!\langle P \rangle\!\rangle_\varepsilon$$

Summary of the Talk

Goal:

- To support hierarchy in distributed π-calculi.

Some highlights:

- flat model — fixed-tree model — mobile-tree model
- easy navigation by address translation