Communication Interference in Mobile Boxed Ambients

FST&TCS 2002

joint with: M. Bugliesi, S. Crafa, M. Merro

Vladimiro Sassone

University of Sussex, MYTHS

Mobile Ambients

Both administrative domains and computational environments (Cardelli-Gordon)

- Subjective movements

$$n[\,\mathsf{in}\ m.P \mid Q\,] \mid m[\,R\,] \longrightarrow m[\,n[\,P \mid Q\,] \mid R\,]$$

$$m[\,n[\,\mathsf{out}\ m.P \mid Q\,] \mid R\,] \longrightarrow n[\,P \mid Q\,] \mid m[\,R\,]$$

- Process interaction

$$n[\,\langle M\rangle.P \mid (x).Q\,] \longrightarrow n[\,P \mid Q\{x := M\}\,],$$

- Boundary dissolver

$$\mathsf{open}\ n.P \mid n[\,Q\,] \longrightarrow P \mid Q.$$

Interferences in Mobile Ambients

- The inherent nondeterminism of movement may go wild: Grave Interferences.

$$k[\,n[\,\mathsf{in}\ m.P \mid \mathsf{out}\ k.R\,] \mid m[\,Q\,]\,]$$

Interferences in Mobile Ambients

- The inherent nondeterminism of movement may go wild: Grave Interferences.

$$k[\, n[\, \mathsf{in}\ m.P \mid \mathsf{out}\ k.R \,] \mid m[\, Q \,] \,]$$

- Introducing Safe Ambients (Levi-Sangiorgi)

$$n[\, \mathsf{in}\ m.P \mid Q \,] \mid m[\, \overline{\mathsf{in}}\ m.R \mid S \,] \longrightarrow m[\, n[\, P \mid Q \,] \mid R \mid S \,]$$

- Co-capabilities and single-threadedness rule out grave interferences

Interferences in Mobile Ambients

- The inherent nondeterminism of movement may go wild: Grave Interferences.

$$k[\,n[\,\mathsf{in}\ m.P \mid \mathsf{out}\ k.R\,] \mid m[\,Q\,]\,]$$

- Introducing Safe Ambients (Levi-Sangiorgi)

$$n[\,\mathsf{in}\ m.P \mid Q\,] \mid m[\,\overline{\mathsf{in}}\ m.R \mid S\,] \longrightarrow m[\,n[\,P \mid Q\,] \mid R \mid S\,]$$

- Co-capabilities and single-threadedness rule out grave interferences

- Safe Ambients with passwords have a conveniently treatable semantics. (Merro-Hennessy)

$$n[\,\mathsf{in}\ (m,k).P \mid Q\,] \mid m[\,\overline{\mathsf{in}}\ (m,k).R \mid S\,] \longrightarrow m[\,n[\,P \mid Q\,] \mid R \mid S\,]$$

≪ ⋘ ⋙ ≫

Mobile Boxed Ambients

- open's nature of ambient dissolver is a potential source of problems.

- Direct communication as alternative source of expressiveness: Mobile Boxed Ambients (Bugliesi et al.). Perform I/O on a subambient n's local channel (viz. $(x)^n$) as well as from the parent's local channel (viz. $(x)^\uparrow$)

$$(x)^n.P \mid n[\,\langle M\rangle.\,Q \mid R\,] \longrightarrow P\{x := M\} \mid n[\,Q \mid R\,]$$

$$\langle M\rangle.P \mid n[\,(x)^\uparrow.\,Q \mid R\,] \longrightarrow P \mid n[\,Q\{x := M\} \mid R\,].$$

Mobile Boxed Ambients

- open's nature of ambient dissolver is a potential source of problems.

- Direct communication as alternative source of expressiveness: Mobile Boxed Ambients (Bugliesi et al.). Perform I/O on a subambient n's local channel (viz. $(x)^n$) as well as from the parent's local channel (viz. $(x)^\uparrow$)

$$(x)^n.P \mid n[\,\langle M\rangle.\,Q \mid R\,] \longrightarrow P\{x := M\} \mid n[\,Q \mid R\,]$$

$$\langle M\rangle.P \mid n[\,(x)^\uparrow.\,Q \mid R\,] \longrightarrow P \mid n[\,Q\{x := M\} \mid R\,].$$

- But it is a great source of non-local nondeterminism and communication interference.

$$m[\,(x)^n.P \mid n[\,\langle M\rangle \mid (x).Q \mid k[\,(x)^\uparrow.R\,]\,]\,]$$

Mobile Boxed Ambients

- open's nature of ambient dissolver is a potential source of problems.

- Direct communication as alternative source of expressiveness: Mobile Boxed Ambients (Bugliesi et al.). Perform I/O on a subambient n's local channel (viz. $(x)^n$) as well as from the parent's local channel (viz. $(x)^\uparrow$)

$$(x)^n.P \mid n[\,\langle M \rangle.\,Q \mid R\,] \longrightarrow P\{x := M\} \mid n[\,Q \mid R\,]$$

$$\langle M \rangle.P \mid n[\,(x)^\uparrow.\,Q \mid R\,] \longrightarrow P \mid n[\,Q\{x := M\} \mid R\,].$$

- But it is a great source of non-local nondeterminism and communication interference.

$$m[\,(x)^n.P \mid n[\,\langle M \rangle \mid (x).Q \mid k[\,(x)^\uparrow.R\,]\,]\,]$$

Introducing NBA: Communication

NBA: a fresh foundation based on: each ambient comes equipped with two mutually non-interfering channels, for local and upward communications.

$$(x)^n.P \mid n[\langle M\rangle^{\hat{}}.Q \mid R] \longrightarrow P\{x := M\} \mid n[Q \mid R]$$

$$\langle M\rangle^n.P \mid n[(x)^{\hat{}}.Q \mid R] \longrightarrow P \mid n[Q\{x := M\} \mid R]$$

≪ ⋘ ⋙ ≫

Introducing NBA: Communication

NBA: a fresh foundation based on: each ambient comes equipped with two mutually non-interfering channels, for local and upward communications.

$$(x)^n.P \mid n[\langle M\rangle^{\hat{}}.Q \mid R] \longrightarrow P\{x := M\} \mid n[Q \mid R]$$

$$\langle M\rangle^n.P \mid n[(x)^{\hat{}}.Q \mid R] \longrightarrow P \mid n[Q\{x := M\} \mid R]$$

Introducing NBA: Communication

NBA: a fresh foundation based on: each ambient comes equipped with two mutually non-interfering channels, for local and upward communications.

$$(x)^n.P \mid n[\langle M\rangle^{\hat{}}.Q \mid R] \longrightarrow P\{x := M\} \mid n[Q \mid R]$$

$$\langle M\rangle^n.P \mid n[(x)^{\hat{}}.Q \mid R] \longrightarrow P \mid n[Q\{x := M\} \mid R]$$

- Good algebraic laws; simple type system;
- Expressiveness??

Introducing NBA: Communication

NBA: a fresh foundation based on: each ambient comes equipped with two mutually non-interfering channels, for local and upward communications.

$$(x)^n.P \mid n[\langle M\rangle^{\hat{}}.Q \mid R] \longrightarrow P\{x := M\} \mid n[Q \mid R]$$

$$\langle M\rangle^n.P \mid n[(x)^{\hat{}}.Q \mid R] \longrightarrow P \mid n[Q\{x := M\} \mid R]$$

- Good algebraic laws; simple type system;
- Expressiveness??
- Hmm, rather poor: $n[P]$ cannot, for instance, communicate with children it doesn't know statically. It can never learn about incoming ambients, and will never be able to talk to them.

Introducing NBA: Mobility

- Essentially, our idea is to introduce co-actions of the form $\overline{\mathsf{enter}}(x)$ which have the effect of binding the variable x.

- Such a purely binding mechanism does not provide a way control of access, but only to registers it. As a (realistic) access protocol where newly arrived agents must register themselves to be granted access to local resources.

Introducing NBA: Mobility

- Essentially, our idea is to introduce co-actions of the form $\overline{\mathsf{enter}}(x)$ which have the effect of binding the variable x.

- Such a purely binding mechanism does not provide a way control of access, but only to registers it. As a (realistic) access protocol where newly arrived agents must register themselves to be granted access to local resources.

- Need a finer mechanism of access control:

$$a[\,\mathsf{enter}\langle b, k\rangle.P_1 \mid P_2\,] \mid b[\,\overline{\mathsf{enter}}(x, k).Q_1 \mid Q_2\,] \longrightarrow b[\,a[\,P_1 \mid P_2\,] \mid Q_1\{x := a\} \mid Q_2\,]$$

This represent an access protocol where the credentials of incoming processes (k in the rule above) are controlled, as a preliminary step to the registration protocol.

Introducing NBA: Mobility

- Essentially, our idea is to introduce co-actions of the form $\overline{\text{enter}}(x)$ which have the effect of binding the variable x.

- Such a purely binding mechanism does not provide a way control of access, but only to registers it. As a (realistic) access protocol where newly arrived agents must register themselves to be granted access to local resources.

- Need a finer mechanism of access control:

$$a[\,\text{enter}\langle b, k\rangle.P_1 \mid P_2\,] \mid b[\,\overline{\text{enter}}(x, k).Q_1 \mid Q_2\,] \longrightarrow b[\,a[\,P_1 \mid P_2\,] \mid Q_1\{x := a\} \mid Q_2\,]$$

This represent an access protocol where the credentials of incoming processes (k in the rule above) are controlled, as a preliminary step to the registration protocol.

NBA: Syntax

Names: a,b,. . . n,x,y,. . . $\in \mathbf{N}$

Locations:

η	$::=$	a	nested names
	$\mid$	$\hat{\hat{}}$	enclosing ambient
	$\mid$	$\star$	local

Messages:

M, N	$::=$	a	name
	$\mid$	$\mathsf{enter}\langle M, N\rangle$	may enter
	$\mid$	$\mathsf{exit}\langle M, N\rangle$	may exit
	$\mid$	$M.N$	path

Processes:

P	$::=$	$\mathbf{0}$	nil process
	$\mid$	$P_1 \mid P_2$	composition
	$\mid$	$(\boldsymbol{\nu} n)P$	restriction
	$\mid$	$!\pi.P$	replication
	$\mid$	$M[P]$	ambient
	$\mid$	$\pi.P$	prefixing

Prefixes:

π	$::=$	M	messages
	$\mid$	$(x_1, \ldots, x_k)^\eta$	input
	$\mid$	$\langle M_1, \ldots, M_k\rangle^\eta$	output
	$\mid$	$\overline{\mathsf{enter}}(x, M)$	allow enter
	$\mid$	$\overline{\mathsf{exit}}(x, M)$	allow exit

NBA: Reduction Semantics

mobility

$$n[\mathsf{enter}\langle m,k\rangle.P_1 \mid P_2] \mid m[\overline{\mathsf{enter}}(x,k).Q_1 \mid Q_2] \longrightarrow m[n[P_1 \mid P_2] \mid Q_1\{x := n\} \mid Q_2]$$

$$n[m[\mathsf{exit}\langle n,k\rangle.P_1 \mid P_2] \mid Q] \mid \overline{\mathsf{exit}}(x,k).R \longrightarrow m[P_1 \mid P_2] \mid n[Q] \mid R\{x := m\}$$

communication

$$(\tilde{x}).P \mid \langle\tilde{M}\rangle.Q \longrightarrow P\{\tilde{x} := \tilde{M}\} \mid Q$$

$$(\tilde{x})^n.P \mid n[\langle\tilde{M}\rangle^{\hat{}}.Q \mid R] \longrightarrow P\{\tilde{x} := \tilde{M}\} \mid n[Q \mid R]$$

$$\langle\tilde{M}\rangle^n.P \mid n[(\tilde{x})^{\hat{}}.Q \mid R] \longrightarrow P \mid n[Q\{\tilde{x} := \tilde{M}\} \mid R]$$

structural congruence

$$P \equiv Q \qquad Q \longrightarrow R \qquad R \equiv S \text{ implies } P \longrightarrow S$$

≪ ⋘ ⋙ ≫

NBA: Behavioural Equivalence

- Barbs

$$P \downarrow_n \text{ iff } P \equiv (\nu \vec{m})(n[\overline{\mathsf{enter}}(x,k).Q \mid R] \mid S), \qquad \text{for } \{n,k\} \cap \{\vec{m}\} = \emptyset.$$

$$P \Downarrow_n \text{ iff } P \Longrightarrow P' \text{ and } P' \downarrow_n .$$

≪ ⋘ ⋙ ≫

NBA: Behavioural Equivalence

- Barbs

$$P\downarrow_n \text{ iff } P \equiv (\nu\vec{m})(n[\overline{\mathsf{enter}}(x,k).Q \mid R] \mid S), \quad \text{for } \{n,k\} \cap \{\vec{m}\} = \emptyset.$$

$$P\Downarrow_n \text{ iff } P \Longrightarrow P' \text{ and } P'\downarrow_n .$$

- A relation $\mathscr{R}$ is reduction closed if

$$P\mathscr{R}Q \text{ and } P \rightarrow P' \text{ implies } Q \Rightarrow Q' \text{ with } P'\mathscr{R}Q';$$

it is barb preserving if $P\mathscr{R}Q$ and $P\downarrow_n$ implies $Q\Downarrow_n$.

- Reduction barbed congruence, written $\cong$, is the largest congruence relation over processes which is reduction closed and barb preserving.

- Note: We could equivalently observe $\langle\cdot\rangle\hat{}$.

≪ ⋘ ⋙ ≫

The rest of the talk

- Two small examples
- A few equational laws
- LTS characterization of reduction barbed bisimulation congruence.
- A type system
- An encoding of BA into NBA: BA $\lesssim$ NBA + Guarded Choice

A one-to-one communication server

- Let $\mathsf{w}(k)$ be a bidirectional forwarder for any pair of incoming ambients.

$$\mathsf{w}(k) \triangleq \mathsf{w}[\ \overline{\mathsf{enter}}(x,k).\overline{\mathsf{enter}}(y,k).(!(z)^x.\langle z\rangle^y \mid !(z)^y.\langle z\rangle^x)\ ]$$

An agent can be defined as: $A(a,k,P,Q) \triangleq a[\mathsf{enter}\langle \mathsf{w}, k\rangle.P \mid \mathsf{exit}\langle \mathsf{w}, k\rangle.Q]$ and a communication server as:

$$\mathsf{o2o}(k) \quad = \quad (\boldsymbol{\nu} r)\ (\ r[\langle\,\rangle^{\hat{}}\,] \mid !\,(\,)^r.(\mathsf{w}(k) \mid \overline{\mathsf{exit}}(\_,k).\overline{\mathsf{exit}}(\_,k).r[\langle\,\rangle^{\hat{}}\,])\ )$$

A one-to-one communication server

- Let w(k) be a bidirectional forwarder for any pair of incoming ambients.

$$\mathsf{w}(k) \triangleq \mathsf{w}[\ \overline{\mathsf{enter}}(x,k).\overline{\mathsf{enter}}(y,k).(!(z)^x.\langle z\rangle^y \mid !(z)^y.\langle z\rangle^x)\ ]$$

An agent can be defined as: $A(a,k,P,Q) \triangleq a[\mathsf{enter}\langle \mathsf{w},k\rangle.P \mid \mathsf{exit}\langle \mathsf{w},k\rangle.Q]$ and a communication server as:

$$\mathsf{o2o}(k) \quad = \quad (\boldsymbol{\nu} r)\ (\ r[\langle\,\rangle^{\hat{}}\,] \mid !\,(\,)^r.(\mathsf{w}(k) \mid \overline{\mathsf{exit}}(\_,k).\overline{\mathsf{exit}}(\_,k).r[\langle\,\rangle^{\hat{}}\,])\ )$$

- It can be proved that:

$$(\boldsymbol{\nu} k)(\ \mathsf{o2o}(k) \mid A(k,a_1,\langle M\rangle^{\hat{}}.P_1,Q_1) \mid A(k,a_2,(x)^{\hat{}}.P_2\{x\},Q_2) \mid \Pi_{i\in I}A(K,a_i,R_i,S_i)\ )$$

$$\Longrightarrow \cong\ (\boldsymbol{\nu} k)(\ \mathsf{o2o}(k) \mid a_1[P_1 \mid Q_1] \mid a_2[P_1\{x := M\} \mid Q_2] \mid \Pi_{i\in I}A(K,a_i,R_i,S_i)\ )$$

that is, once two agents engage in communication no other agent knowing the key k can interfere with their completing the exchange.

A print server

- The following process assigns a progressive number to incoming jobs.

$$\mathsf{enqueue}_k \triangleq (\boldsymbol{\nu} c)\ (\ c[\langle 1 \rangle\hat{}\ ] \mid !(n)^c.\overline{\mathsf{enter}}(x, k).\langle n \rangle^x.c[\langle n+1 \rangle\hat{}\ ])$$

≪ ⋘ ⋙ ≫

A print server

- The following process assigns a progressive number to incoming jobs.

$$\mathsf{enqueue}_k \triangleq (\boldsymbol{\nu} c)\ (\ c[\langle 1\rangle^{\hat{}}\ ] \mid !(n)^c.\overline{\mathsf{enter}}(x,k).\langle n\rangle^x.c[\langle n+1\rangle^{\hat{}}\ ])$$

- We can turn it into a print server (which consumes such numbers).

$$\mathsf{prtsrv}(k) \triangleq k[\ \mathsf{enqueue}_k \mid \mathsf{print}\ ]$$

$$\mathsf{print} \triangleq (\boldsymbol{\nu} c)\ (\ c[\langle 1\rangle^{\hat{}}\ ] \mid !(n)^c.\overline{\mathsf{exit}}(x,n).(data)^x.(P\{data\} \mid c[\langle n+1\rangle^{\hat{}}\ ])$$

- A client then acts as:

$$\mathsf{job}(M,k) \triangleq (\boldsymbol{\nu} p)p[\ \mathsf{enter}\langle k,k\rangle.(n)^{\hat{}}.(\boldsymbol{\nu} q)q[\mathsf{exit}\langle p,n\rangle.\langle M\rangle^{\hat{}}\ ]\ ]$$

It enters the server prtsrv(k) (using enqueue), it is assigned a number that it uses as a password to carry job M to print (which eventually will bind it to $data$ in P. (Dynamic name discovery and passwords are fundamental here.)

≪ ⋘ ⋙ ≫

Some Equational Laws

Garbage Collection laws

- $l[\ (\tilde{x}_i)^n.P \mid (\tilde{x}).Q \mid \langle\tilde{M}\rangle^m.R\ ] \ \cong\ \mathbf{0}$
- $l[\ (\tilde{x})^n.P \mid \langle\tilde{M}\rangle.P \mid \langle\tilde{M}\rangle^m.P\ ] \ \cong\ \mathbf{0}$

≪ ⋘ ⋙ ≫

UNIVERSITY OF SUSSEX

Some Equational Laws

Garbage Collection laws

- $l[\ (\tilde{x}_i)^n.P \mid (\tilde{x}).Q \mid \langle\tilde{M}\rangle^m.R\ ] \ \cong\ \mathbf{0}$
- $l[\ (\tilde{x})^n.P \mid \langle\tilde{M}\rangle.P \mid \langle\tilde{M}\rangle^m.P\ ] \ \cong\ \mathbf{0}$

Communication laws

- $l[\ \langle\tilde{M}_0\rangle^{\hat{}} \mid \langle\tilde{M}_1\rangle^{\hat{}}\ ] \ \cong\ l[\langle\tilde{M}_0\rangle^{\hat{}}\ ] \mid l[\langle\tilde{M}_1\rangle^{\hat{}}\ ]$
- $l[(\tilde{x}).P \mid \langle\tilde{M}\rangle.Q] \ \cong\ l[P\{\tilde{x} := \tilde{M}\} \mid Q]$
- $(\boldsymbol{\nu} l)(\ (\tilde{x})^l.P \mid l[\langle\tilde{M}\rangle^{\hat{}}.Q]\ ) \ \cong\ (\boldsymbol{\nu} l)(\ P\{\tilde{x} := \tilde{M}\} \mid l[Q]\ )$
- $m[(\tilde{x})^l.P \mid l[\langle\tilde{M}\rangle^{\hat{}}.Q]] \ \cong\ m[P\{\tilde{x} := \tilde{M}\} \mid l[Q]]$

Some Equational Laws

Garbage Collection laws

- $l[\ (\tilde{x}_i)^n.P \mid (\tilde{x}).Q \mid \langle\tilde{M}\rangle^m.R\ ] \ \cong\ \mathbf{0}$
- $l[\ (\tilde{x})^n.P \mid \langle\tilde{M}\rangle.P \mid \langle\tilde{M}\rangle^m.P\ ] \ \cong\ \mathbf{0}$

Communication laws

- $l[\ \langle\tilde{M}_0\rangle^{\hat{}} \mid \langle\tilde{M}_1\rangle^{\hat{}}\ ] \ \cong\ l[\langle\tilde{M}_0\rangle^{\hat{}}\ ] \mid l[\langle\tilde{M}_1\rangle^{\hat{}}\ ]$
- $l[(\tilde{x}).P \mid \langle\tilde{M}\rangle.Q] \ \cong\ l[P\{\tilde{x} := \tilde{M}\} \mid Q]$
- $(\boldsymbol{\nu} l)(\ (\tilde{x})^l.P \mid l[\langle\tilde{M}\rangle^{\hat{}}.Q]\ ) \ \cong\ (\boldsymbol{\nu} l)(\ P\{\tilde{x} := \tilde{M}\} \mid l[Q]\ )$
- $m[(\tilde{x})^l.P \mid l[\langle\tilde{M}\rangle^{\hat{}}.Q]] \ \cong\ m[P\{\tilde{x} := \tilde{M}\} \mid l[Q]]$

Mobility laws

- $(\boldsymbol{\nu} p)(m[\mathsf{enter}\langle n,p\rangle.P] \mid n[\overline{\mathsf{enter}}(x,p).Q]) \ \cong\ (\boldsymbol{\nu} p)(n[Q\{x := m\} \mid m[P]])$
- $l[m[\mathsf{enter}\langle n,p\rangle.P] \mid n[\overline{\mathsf{enter}}(x,p).Q]] \ \cong\ l[n[Q\{x := m\} \mid m[P]]]$

An LTS for NBA

Concretions: $(\boldsymbol{\nu}\tilde{p})\langle P\rangle Q$ and $(\boldsymbol{\nu}\tilde{p})\langle M\rangle Q$

(Amb Co-enter)

$$\frac{P \xrightarrow{\overline{\mathsf{enter}}(n,k)} P'}{m[P] \xrightarrow{m\ \overline{\mathsf{enter}}(n,k)} (\boldsymbol{\nu})\langle P'\rangle \mathbf{0}}$$

(Co-enter HO)

$$\frac{P \xrightarrow{m\ \overline{\mathsf{enter}}(n,k)} (\boldsymbol{\nu}\tilde{p})\langle P_1\rangle P_2 \quad \tilde{p}\cap \mathrm{fn}(Q)=\emptyset}{P \xrightarrow{m\ \overline{\mathsf{enter}}(n,k)Q} (\boldsymbol{\nu}\tilde{p})(m[n[Q] \mid P_1] \mid P_2)}$$

(Exit)

$$\frac{P \xrightarrow{\mathsf{exit}\langle n,k\rangle} (\boldsymbol{\nu}\tilde{p})\langle m[P_1]\rangle P_2}{n[P] \xrightarrow{\mathsf{exit}\langle k\rangle} (\boldsymbol{\nu}\tilde{p})\langle m\rangle(m[P_1] \mid n[P_2])}$$

(τ-Exit)

$$\frac{P \xrightarrow{\mathsf{exit}\langle k\rangle} (\boldsymbol{\nu}\tilde{p})\langle m\rangle P' \quad Q \xrightarrow{\overline{\mathsf{exit}}(m,k)} Q'}{P \mid Q \xrightarrow{\tau} (\boldsymbol{\nu}\tilde{p})(P' \mid Q')}$$

(Exit HO)

$$\frac{P \xrightarrow{\mathsf{exit}\langle n,k\rangle} (\boldsymbol{\nu}\tilde{p})\langle m[P_1]\rangle P_2 \quad x\in \mathrm{fn}(R) \quad \tilde{p}\cap \mathrm{fn}(Q|R)=\emptyset}{P \xrightarrow{\mathsf{exit}\langle n,k\rangle QR} (\boldsymbol{\nu}\tilde{p})(m[P_1] \mid n[P_2 \mid Q] \mid R\{x:=m\})}$$

A Characterisation of Reduction Bisimulation

- Thm. If $P \xrightarrow{\tau} P'$ then $P \longrightarrow P'$. If $P \longrightarrow P'$ then $P \xrightarrow{\tau}\equiv P'$.
- Bisimilarity. A symmetric relation $\mathscr{R}$ is a bisimulation if

$$P \mathrel{\mathscr{R}} Q \quad \text{and} \quad P \xrightarrow{\alpha} P' \quad \text{implies} \quad \exists Q \stackrel{\hat{\alpha}}{\Longrightarrow} Q' \quad \text{with} \quad P' \mathrel{\mathscr{R}} Q'.$$

- $P \approx Q$ if $P \mathrel{\mathscr{R}} Q$ for some bisimulation $\mathscr{R}$.
- The closure under substitutions of $\approx$ is denoted by $\approx_c$.
- Thm. If $P \approx_c Q$ then $P \cong Q$ and viceversa.

A Type System for NBA

- Types

Message Types	W	$::=$	$\mathsf{N}[E]$	ambient/password
		$\mid$	$\mathsf{C}[E]$	capability
Exchange Types	E, F	$::=$	shh	no exchange
		$\mid$	$W_1 \ldots W_k$	tuples $(k \geq 0)$
Process Types	T	$::=$	$[E, F]$	composite exchange

$\mathsf{N}[E]$ types both ambients and passwords; shh is the silent type; $\mathsf{N}[\mathsf{shh}]$ is an ambient with no upward exchanges or a password that reveal the visitor's name.

A Type System for NBA

- Types

Message Types	W	$::=$	$\mathsf{N}[E]$	ambient/password
		$\mid$	$\mathsf{C}[E]$	capability
Exchange Types	E, F	$::=$	shh	no exchange
		$\mid$	$W_1 \ldots W_k$	tuples $(k \geq 0)$
Process Types	T	$::=$	$[E, F]$	composite exchange

$\mathsf{N}[E]$ types both ambients and passwords; shh is the silent type; $\mathsf{N}[\mathsf{shh}]$ is an ambient with no upward exchanges or a password that reveal the visitor's name.

- Type Environments

(Env Empty)

$$\frac{}{\varnothing \vdash \diamond}$$

(Env name)

$$\frac{\Gamma \vdash \diamond \quad a \notin \mathrm{Dom}(\Gamma)}{\Gamma, a : W \vdash \diamond}$$

Typing Rules

Messages

(Projection)

$$\frac{\Gamma, a : W, \Gamma' \vdash \diamond}{\Gamma, a : W, \Gamma' \vdash a : W}$$

(Path)

$$\frac{\Gamma \vdash M_1 : \mathsf{C}[E_1] \quad \Gamma \vdash M_2 : \mathsf{C}[E_2]}{\Gamma \vdash M_1.M_2 : \mathsf{C}[E_1 \sqcup E_2]}$$

(Enter)

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash N : \mathsf{N}[F] \quad (F \leqslant G)}{\Gamma \vdash \mathsf{enter}\langle M, N\rangle : \mathsf{C}[G]}$$

(Exit)

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash N : \mathsf{N}[F] \quad (F \leqslant G)}{\Gamma \vdash \mathsf{exit}\langle M, N\rangle : \mathsf{C}[G]}$$

Typing Rules

- Messages

(Projection)

$$\frac{\Gamma, a : W, \Gamma' \vdash \diamond}{\Gamma, a : W, \Gamma' \vdash a : W}$$

(Path)

$$\frac{\Gamma \vdash M_1 : \mathsf{C}[E_1] \quad \Gamma \vdash M_2 : \mathsf{C}[E_2]}{\Gamma \vdash M_1.M_2 : \mathsf{C}[E_1 \sqcup E_2]}$$

(Enter)

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash N : \mathsf{N}[F] \quad (F \leqslant G)}{\Gamma \vdash \mathsf{enter}\langle M, N\rangle : \mathsf{C}[G]}$$

(Exit)

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash N : \mathsf{N}[F] \quad (F \leqslant G)}{\Gamma \vdash \mathsf{exit}\langle M, N\rangle : \mathsf{C}[G]}$$

- Processes

(Par)

$$\frac{\Gamma \vdash P : [E, F] \quad \Gamma \vdash Q : [E, F]}{\Gamma \vdash P \mid Q : [E, F]}$$

(Repl)

$$\frac{\Gamma \vdash P : [E, F]}{\Gamma \vdash !P : [E, F]}$$

(Dead)

$$\frac{\Gamma \vdash \diamond}{\Gamma \vdash \mathbf{0} : [E, F]}$$

(New)

$$\frac{\Gamma, n : \mathsf{N}[G] \vdash P : [E, F]}{\Gamma \vdash (\boldsymbol{\nu} n{:}\mathsf{N}[G])P : [E, F]}$$

Typing Rules: II

- Processes: mobility

(Amb)

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash P : [F, E]}{\Gamma \vdash M[P] : [G, H]}$$

(Prefix)

$$\frac{\Gamma \vdash M : \mathsf{C}[F] \quad \Gamma \vdash P : [E, G] \quad (F \leqslant G)}{\Gamma \vdash M.P : [E, G]}$$

(Co-enter)

$$\frac{\Gamma \vdash M : \mathsf{N}[\tilde{W}] \quad \Gamma, x : \mathsf{N}[\tilde{W}] \vdash P : [E, F]}{\Gamma \vdash \overline{\mathsf{enter}}(x, M).P : [E, F]}$$

(Co-exit)

$$\frac{\Gamma \vdash M : \mathsf{N}[\tilde{W}] \quad \Gamma, x : \mathsf{N}[\tilde{W}] \vdash P : [E, F]}{\Gamma \vdash \overline{\mathsf{exit}}(x, M).P : [E, F]}$$

(Co-enter-silent)

$$\frac{\Gamma \vdash M : \mathsf{N}[\mathsf{shh}] \quad \Gamma \vdash P : [E, F] \quad (x \notin \mathrm{fv}(P))}{\Gamma \vdash \overline{\mathsf{enter}}(x, M).P : [E, F]}$$

(Co-exit-silent)

$$\frac{\Gamma \vdash M : \mathsf{N}[\mathsf{shh}] \quad \Gamma \vdash P : [E, F] \quad (x \notin \mathrm{fv}(P))}{\Gamma \vdash \overline{\mathsf{exit}}(x, M).P : [E, F]}$$

Typing Rules: II

- Processes: I/O

(Input)

$$\frac{\Gamma, \tilde{x}{:}\tilde{W} \vdash P : [\tilde{W}, E]}{\Gamma \vdash (\tilde{x}{:}\tilde{W}).P : [\tilde{W}, E]}$$

(Input $\hat{}$)

$$\frac{\Gamma, \tilde{x}{:}\tilde{W} \vdash P : [E, \tilde{W}]}{\Gamma \vdash (\tilde{x}{:}\tilde{W})^{\hat{}}.P : [E, \tilde{W}]}$$

(Input M)

$$\frac{\Gamma \vdash M : \mathsf{N}[\tilde{W}] \quad \Gamma, \tilde{x}{:}\tilde{W} \vdash P : [G, H]}{\Gamma \vdash (\tilde{x}{:}\tilde{W})^{M}.P : [G, H]}$$

(Output)

$$\frac{\Gamma \vdash \tilde{M} : \tilde{W} \quad \Gamma \vdash P : [\tilde{W}, E]}{\Gamma \vdash \langle \tilde{M} \rangle.P : [\tilde{W}, E]}$$

(Output $\hat{}$)

$$\frac{\Gamma \vdash \tilde{M} : \tilde{W} \quad \Gamma \vdash P : [E, \tilde{W}]}{\Gamma \vdash \langle \tilde{M} \rangle^{\hat{}}.P : [E, \tilde{W}]}$$

(Output N)

$$\frac{\Gamma \vdash N : \mathsf{N}[\tilde{W}] \quad \Gamma \vdash \tilde{M} : \tilde{W} \quad \Gamma \vdash P : [G, H]}{\Gamma \vdash \langle \tilde{M} \rangle^{N}.P : [G, H]}$$

- Subject Reduction. If $\Gamma \vdash P : T$ and $P \longrightarrow Q$, then $\Gamma \vdash Q : T$.

Encoding: BA in NBA

We can encode BA into NBA enriched with a focused form of nondeterminism.

$$
\begin{array}{lcll}
\{\!|\, P \,|\!\}_n & = & \overline{\mathsf{cross}} \mid \langle\!\langle\, P \,\rangle\!\rangle_n & \\
\langle\!\langle\, m[P] \,\rangle\!\rangle_n & = & m[\{\!|\, P \,|\!\}_m] & \\
\langle\!\langle\, (x)^a P \,\rangle\!\rangle_n & = & (x)^a \langle\!\langle\, P \,\rangle\!\rangle_n & \\
\langle\!\langle\, (x) P \,\rangle\!\rangle_n & = & (x) \langle\!\langle\, P \,\rangle\!\rangle_n + (x)^{\hat{}} \langle\!\langle\, P \,\rangle\!\rangle_n + \overline{\mathsf{exit}}(y, \mathsf{pw})(x)^y \langle\!\langle\, P \,\rangle\!\rangle_n & y \notin \mathrm{fn}(P) \\
\langle\!\langle\, (x)^{\uparrow} P \,\rangle\!\rangle_n & = & (\boldsymbol{\nu} p) p[\mathsf{exit}\langle n, \mathsf{pr}\rangle.(x)^{\hat{}}.\mathsf{enter}\langle n, p\rangle.\langle x\rangle^{\hat{}}\,] \mid \overline{\mathsf{enter}}(y, p)(x)^y \langle\!\langle\, P \,\rangle\!\rangle_n & p, y \notin \mathrm{fn}(P) \\
\langle\!\langle\, \langle M\rangle^a P \,\rangle\!\rangle_n & = & \langle M\rangle^a \langle\!\langle\, P \,\rangle\!\rangle_n & \\
\langle\!\langle\, \langle M\rangle P \,\rangle\!\rangle_n & = & \langle M\rangle \langle\!\langle\, P \,\rangle\!\rangle_n + \langle M\rangle^{\hat{}} \langle\!\langle\, P \,\rangle\!\rangle_n + \overline{\mathsf{exit}}(y, \mathsf{pr})\langle M\rangle^y \langle\!\langle\, P \,\rangle\!\rangle_n & y \notin \mathrm{fn}(P) \\
\langle\!\langle\, \langle M\rangle^{\uparrow} P \,\rangle\!\rangle_n & = & (\boldsymbol{\nu} p) p[\mathsf{exit}\langle n, \mathsf{pw}\rangle.\langle M\rangle^{\hat{}}.\mathsf{enter}\langle n, p\rangle.\langle \cdot\rangle^{\hat{}}\,] \mid \overline{\mathsf{enter}}(y, p)(\_)^y \langle\!\langle\, P \,\rangle\!\rangle_n & p, y \notin \mathrm{fn}(P)
\end{array}
$$

where $\overline{\mathsf{cross}} = !\overline{\mathsf{enter}}(x, \mathsf{mv}) \mid !\overline{\mathsf{exit}}(x, \mathsf{mv})$, in $n = \mathsf{enter}\langle n, \mathsf{mv}\rangle$, and out $n = \mathsf{exit}\langle n, \mathsf{mv}\rangle$.

≪ ⋘ ⋙ ≫

Encoding: BA in NBA

We can encode BA into NBA enriched with a focused form of nondeterminism.

$$\{\!\mid P \mid\!\}_n = \overline{\mathsf{cross}} \mid \langle\!\langle P \rangle\!\rangle_n$$

$$\langle\!\langle m[P] \rangle\!\rangle_n = m[\{\!\mid P \mid\!\}_m]$$

$$\langle\!\langle (x)^a P \rangle\!\rangle_n = (x)^a \langle\!\langle P \rangle\!\rangle_n$$

$$\langle\!\langle (x) P \rangle\!\rangle_n = (x) \langle\!\langle P \rangle\!\rangle_n + (x)^{\hat{}} \langle\!\langle P \rangle\!\rangle_n + \overline{\mathsf{exit}}(y, \mathsf{pw})(x)^y \langle\!\langle P \rangle\!\rangle_n \qquad y \notin \mathrm{fn}(P)$$

$$\langle\!\langle (x)^{\uparrow} P \rangle\!\rangle_n = (\boldsymbol{\nu} p) p[\mathsf{exit}\langle n, \mathsf{pr}\rangle.(x)^{\hat{}}.\mathsf{enter}\langle n, p\rangle.\langle x\rangle^{\hat{}}\,] \mid \overline{\mathsf{enter}}(y, p)(x)^y \langle\!\langle P \rangle\!\rangle_n \qquad p, y \notin \mathrm{fn}(P)$$

$$\langle\!\langle \langle M\rangle^a P \rangle\!\rangle_n = \langle M\rangle^a \langle\!\langle P \rangle\!\rangle_n$$

$$\langle\!\langle \langle M\rangle P \rangle\!\rangle_n = \langle M\rangle \langle\!\langle P \rangle\!\rangle_n + \langle M\rangle^{\hat{}} \langle\!\langle P \rangle\!\rangle_n + \overline{\mathsf{exit}}(y, \mathsf{pr})\langle M\rangle^y \langle\!\langle P \rangle\!\rangle_n \qquad y \notin \mathrm{fn}(P)$$

$$\langle\!\langle \langle M\rangle^{\uparrow} P \rangle\!\rangle_n = (\boldsymbol{\nu} p) p[\mathsf{exit}\langle n, \mathsf{pw}\rangle.\langle M\rangle^{\hat{}}.\mathsf{enter}\langle n, p\rangle.\langle \cdot\rangle^{\hat{}}\,] \mid \overline{\mathsf{enter}}(y, p)(\_)^y \langle\!\langle P \rangle\!\rangle_n \qquad p, y \notin \mathrm{fn}(P)$$

where $\overline{\mathsf{cross}} = !\overline{\mathsf{enter}}(x, \mathsf{mv}) \mid !\overline{\mathsf{exit}}(x, \mathsf{mv})$, in n = $\mathsf{enter}\langle n, \mathsf{mv}\rangle$, and out n = $\mathsf{exit}\langle n, \mathsf{mv}\rangle$.

Thm. If $P \xrightarrow{\tau} P'$ then $\{\!\mid P \mid\!\} \xrightarrow{\tau} \gtrsim \{\!\mid P' \mid\!\}$.

If $\{\!\mid P \mid\!\} \xrightarrow{\tau} Q$, then $\exists P \xrightarrow{\tau} P'$ with $Q \gtrsim \{\!\mid P' \mid\!\}$.

If P and Q are single-threaded, then $\{\!\mid P \mid\!\}_n \cong \{\!\mid Q \mid\!\}_n$ implies $P \cong Q$.

≪ ⋘ ⋙ ≫

Conclusion and Future Work

- Type inference.
- Information flow analysis.
- Comparison with Seal calculus.
- Implementation.
- Logics.