Compositional Analysis of Mobile Agents
using structural invariants of object nets

Michael Köhler * Heiko Rölke * Rüdiger Valk
University of Hamburg
1 Introduction

Mobility

Location and environment of a system.

How platforms can be protected against malicious agents.

How can integrity of platforms be achieved without having knowledge about the agents in advance?
How can integrity of platforms be achieved \textit{without} having knowledge about the agents in advance?

two approaches:

\begin{itemize}
  \item “proof-carrying code”
  \item “sandbox”
\end{itemize}
**Petri nets:**

- graphical and formal representation of systems
- formal analysis (here: invariants)

**Petri nets within Petri nets**

- locality and mobility

*this contribution: to extend the first to the second*
2. Object Systems

agent X at location A

agent X at location B

mobile computer X in security environment A

mobile computer X in security environment B

changing location and internal state

software agents

mobility
nets - within - nets

1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

changing location
and internal state

flexible manufacturing

Köhler/Rölke/Valk - Object Petri Nets and Mobile Agents - MOCA ’04
different cases of transition occurrence:
1. Introduction
2. Object Systems
3. Invariants
4. Mobility
5. Conclusion

transport
1. Introduction
2. Object Systems
3. Invariants
4. Mobility
5. Conclusion

autonomous action
interaction

object net marking has changed
Reference semantics

Creating distributed objects

Renew tool
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

\[
c := x; \\
a := \sqrt{\frac{5}{b \cdot c} + d \cdot e}
\]

\[
c := x \\
y_1 := b \cdot c \\
y_2 := d \cdot e \\
y_3 := \frac{5}{y_1} \\
y_4 := y_3 + y_2 \\
a := \sqrt{y_4}
\]
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

\begin{align*}
y_1 & := b \cdot c \\
y_2 & := d \cdot e \\
y_3 & := 5/y_1 \\
y_4 & := y_3 + y_2 \\
a & := \sqrt{y_4}
\end{align*}
process
history
value
semantics

see: LNCS 3098
Lectures on Concurrency and Petri Nets
2004
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion
creating distributed objects

distributed token value semantics

Köhler/Rölke/Valk - Object Petri Nets and Mobile Agents - MOCA’04
Definition 1. An object system, $OS = (N, \hat{N}, \rho)$, such that:

- The system-net $N = (P, T, \text{pre}, \text{post}, M_0)$ is a $P/T$-net with $|\cdot t|, |t^*| > 0$ for all $t \in T$.

- The object-net $\hat{N} = (\hat{P}, \hat{T}, \text{pre}, \text{post}, \hat{M}_0)$ is a $P/T$-net disjoint from the system-net: $(P \cup T) \cap (\hat{P} \cup \hat{T}) = \emptyset$.

- $\rho \subseteq T \times \hat{T}$ is the interaction relation.

\[(t2, t11) \in \rho\]
Definition 2. A marking of $OS$ is a multiset $M \in \mathcal{M}_v := MS(P \times MS(\hat{P}))$. 

\[
M = (p_1, 2'\hat{p}_{11} + 1'\hat{p}_{12}) + (p_1, 2'\hat{p}_{11} + 1'\hat{p}_{12}) \\
+ (p_3, 2'\hat{p}_{11}) + (p_3, 2'\hat{p}_{11}) \\
+ (p_3, 1'\hat{p}_{12})
\]
operations on markings:

\[ M = \sum_{i=1}^{n}(p_i, \hat{M}_i) \]

Abstraction from the token substructure:

\[ \Pi^1(\sum_{i=1}^{n}(p_i, \hat{M}_i)) = \sum_{i=1}^{n} p_i \]

Summation of the distributed markings:

\[ \Pi^2(\sum_{i=1}^{n}(p_i, \hat{M}_i)) = \sum_{i=1}^{n} \hat{M}_i \]

\[ M = (p_1, 2'\hat{p}_{11} + 1'\hat{p}_{12}) + (p_1, 2'\hat{p}_{11} + 1'\hat{p}_{12}) + (p_3, 2'\hat{p}_{11}) + (p_3, 2'\hat{p}_{11}) + (p_3, 1'\hat{p}_{12}) \]

\[ \Pi^1(M) = 2'p_1 + 3'p_3 \]

\[ \Pi^2(M) = 8'\hat{p}_{11} + 3'\hat{p}_{12} \]
**Definition 4.** Let $OS = (N, \tilde{N}, \rho)$ be an UEOS. Let $M, M' \in M_v$ be markings wrt. value semantics of $OS$. Then $M \xrightarrow{\tau} OS M'$ iff there exists $PRE, POST \in M_v$ such that $PRE \leq M$ and $M' = M - PRE + POST$, and the following holds:

\[
\begin{align*}
\tau = t \in T_\rho & \Rightarrow \Pi^1(PRE) = pre(t) \land \Pi^1(POST) = post(t) \land \\
\Pi^2(POST) & = \Pi^2(PRE) \land \\
\end{align*}
\]
such that \[ \text{PRE} \leq M \] and \[ M' = M - \text{PRE} + \text{POST} \], and the following holds:

**Transport:**
\[
\tau = t \in T_{\rho} \Rightarrow \Pi^1(\text{PRE}) = \text{pre}(t) \land \Pi^1(\text{POST}) = \text{post}(t) \land \\
\Pi^2(\text{POST}) = \Pi^2(\text{PRE}) \land
\]

**Interaction:**
\[
\tau = (t, \hat{t}) \in \rho \Rightarrow \Pi^1(\text{PRE}) = \text{pre}(t) \land \Pi^1(\text{POST}) = \text{post}(t) \land \\
\Pi^2(\text{PRE}) \geq \text{pre}(\hat{t}) \land \\
\Pi^2(\text{POST}) = \Pi^2(\text{PRE}) - \text{pre}(\hat{t}) + \text{post}(\hat{t}) \land
\]

Simulation
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion
3. Place-Invariants

**Proposition 1.** Let OS be an Eos as in Def. 1.

1. The abstract behaviour – determined by the projection \( \Pi^1 \) – on the system level of an Eos corresponds to the behaviour of the system-net viewed as a P/T-net:

\[
\text{M} \xrightarrow{t \in \text{OS}} \text{M}' \text{ implies } \Pi^1(\text{M}) \xrightarrow{t \in N} \Pi^1(\text{M}'), \text{ and } \Pi^1(\text{M}') \text{ is uniquely determined.}
\]
3. The behaviour of the distributed object-net is determined by $\Pi^2$ and is a sub-behaviour of the object-net viewed as a P/T-net:

$$M \xrightarrow{\text{OS}} M' \text{ implies } \Pi^2(M) \xrightarrow{\hat{t}} \Pi^2(M'), \text{ and } \Pi^2(M') \text{ is uniquely determined.}$$

5. Synchronisation is an action composed of two sub-actions:

$$M \xrightarrow{(t, \hat{t})\text{ OS}} M' \text{ implies }$$

$$\Pi^1(M) \xrightarrow{t} \Pi^1(M') \text{ as well as } \Pi^2(M) \xrightarrow{\hat{t}} \Pi^2(M').$$

Furthermore, $\Pi^1(M')$ and $\Pi^2(M')$ are uniquely determined.
A \(P\)-invariant \(i \in \mathbb{Z}^{|P|}, i \neq 0\) is a vector that fulfils \(i' \cdot \Delta = 0\). Then every reachable marking \(M\) fulfils the linear equation \(i \cdot M = i \cdot M_0\).

**Proposition 2.** Let \(OS = (N, \hat{N}, \rho)\) be an Eos as in Def. 1 and let \(i \in \mathbb{Z}^{|P|}\) be an invariant of the system-net and \(\hat{i} \in \mathbb{Z}^{|\hat{P}|}\) one of the object-net. Then for all reachable marking \(M \in \mathcal{M}_v\) it holds:

\[
i \cdot \Pi^1(M) = i \cdot \Pi^1(M_0) \quad \text{and} \quad \hat{i} \cdot \Pi^2(M) = \hat{i} \cdot \Pi^2(M_0)
\]
\[
\forall e \in D \quad \forall u \in D \\
T : e \mapsto u \\
v \mapsto \delta \\
\delta : x \mapsto y + 1 \\
\delta : z \mapsto x + \\
\text{MOCA-Module 31} \\
\]
4. Mobility

- Spontaneous Move: Neither the agent nor its environment initiate the transport. The movement can take place, but it is not enforced. No coupling of the environment and the agent is needed.
- Subjective Move: The agent itself initiates the movement, so agent and environment have to be coupled. This is described by the channel `move`, which has to be enabled in the agent. The movement takes places if the environment is able to execute it.
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

– Objective Move: The environment initiates the movement of the agent. The agent is forced to be transported. The initiative of the environment is modelled by the place travel ticket.
– Consensual move: Both the environment and the agent come to an agreement on the movement. This is modelled by a combination of the channel move, which has to be enabled in the agent, and the external condition modelled by the travel ticket.
\[ \Delta = \begin{array}{cccc}
\text{pool} & \text{pool} & \text{pub} & \text{pool} \\
-1 & 1 & -1 & 1 \\
\text{public} & 1 & -1 & \\
\text{semaphor} & -1 & 1 & -n \\
\text{private} & -1 & 1 & n \\
\end{array} \]

Solving the equation \( \mathbf{i} \cdot \Delta = \mathbf{0} \) we obtain \( \mathbf{i}'_1 = (0, 1, 1, n) \) and \( \mathbf{i}'_2 = (1, 0, -1, 0) \) as invariants of the system-net. Using

\[ M(\text{public}) + M(\text{pool}) + n \cdot M(\text{private}) = n \]

Therefore \( M(\text{private}) > 0 \) implies \( M(\text{private}) = 1 \) and \( M(\text{public}) = M(\text{pool}) = 0 \) which is the desired property.
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

---

agent-nets in pool:

- Public
- Private
- Semaphor
- Flag 1
- Flag 2
- Ready for Public
- Ready for Private

---

Köhler/Rölke/Valk - Object Petri Nets and Mobile Agents - MOCA '04
In the following the system net $N$ is analysed using invariants. The incidence matrix is given as:

$$
\Delta = \begin{pmatrix}
\text{pool} \rightarrow \text{pub} & \text{pub} \rightarrow \text{pool} & \text{pool} \rightarrow \text{prv} & \text{prv} \rightarrow \text{pool} \\
\text{ready public} & -1 & 1 & \\
\text{public} & 1 & -1 & \\
\text{ready private} & & -1 & 1 \\
\text{private} & & 1 & -1 \\
\text{flag}_1 & -1 & & 1 \\
\text{flag}_2 & 1 & & -1
\end{pmatrix}
$$

The incidence matrix is used to analyze the system net $N$. The $\Delta$ matrix shows the changes in the system states.

The system net $N$ is analyzed using invariants, and the incidence matrix is given as follows:

$$
\Delta = \begin{pmatrix}
\text{pool} \rightarrow \text{pub} & \text{pub} \rightarrow \text{pool} & \text{pool} \rightarrow \text{prv} & \text{prv} \rightarrow \text{pool} \\
\text{ready public} & -1 & 1 & \\
\text{public} & 1 & -1 & \\
\text{ready private} & & -1 & 1 \\
\text{private} & & 1 & -1 \\
\text{flag}_1 & -1 & & 1 \\
\text{flag}_2 & 1 & & -1
\end{pmatrix}
$$

In the system net, there is a condition:

$$\hat{M}(\text{public}) + \hat{M}(\text{private}) \leq 1$$

So, the agent proves that it does not attempt to enter the private and the public place at the same time.
\[3 \cdot \text{no money} + 1 \cdot \text{money} + 1 \cdot \text{public} + 1 \cdot \text{flowers} + 2 \cdot \text{jewels} = 3\]

\[1 \cdot \text{no flowers} + 1 \cdot \text{flowers} = 1\]

\[1 \cdot \text{no jewels} + 1 \cdot \text{jewels} = 1\]
\[3 \cdot \text{no money} + 1 \cdot \text{money} + 1 \cdot \text{public} + 1 \cdot \text{flowers} + 2 \cdot \text{jewels} = 3\]

\[1 \cdot \text{no flowers} + 1 \cdot \text{flowers} = 1\]

\[1 \cdot \text{no jewels} + 1 \cdot \text{jewels} = 1\]
\[3 \cdot \text{no money} + 1 \cdot \text{money} + 1 \cdot \text{public} + 1 \cdot \text{flowers} + 2 \cdot \text{jewels} = 3\]

\[1 \cdot \text{no flowers} + 1 \cdot \text{flowers} = 1\]
\[1 \cdot \text{no jewels} + 1 \cdot \text{jewels} = 1\]
3 \cdot \text{no money} + 1 \cdot \text{money} + 1 \cdot \text{public} + 1 \cdot \text{flowers} + 2 \cdot \text{jewels} = 3

1 \cdot \text{no flowers} + 1 \cdot \text{flowers} = 1
1 \cdot \text{no jewels} + 1 \cdot \text{jewels} = 1
3 · no money + 1 · money + 1 · public + 1 · flowers + 2 · jewels = 3

1 · no flowers + 1 · flowers = 1
1 · no jewels + 1 · jewels = 1
Which amount of money have 2 agents in public1 and one in public4?

Simulation

\[3 \cdot \text{no money} + 1 \cdot \text{money} + 1 \cdot \text{public} + 1 \cdot \text{flowers} + 2 \cdot \text{jewels} = 3\]
move pool -> public

semaphor

x:buy_flowers()
x:buy_jewels()

move pool -> private

pool

4

private

move

private ... -> pool

x

x

xx

x:toprivate() x:topublic()

xx

public1

public2

public3

public4

#flowers

flowers#

jewels#

#jewels

move

public -> pool

agent[3]
move pool -> public

semaphor

x:buy_flowers()

x:buy_jewels()

move pool -> private

pool

3 3

private move

private ... -> pool

x

x

xx

x:toprivate() x:topublic()

x

xx

public1 public2

public3 public4

#flowers flowers#

#jewels jewels#

move

pool -> public

semaphor

x:buy_flowers()

x:buy_jewels()
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion
1. Introduction

2. Object Systems

3. Invariants

4. Mobility

5. Conclusion

UHamburg

Köhler/Rößke/Valk-Object Petri Nets and Mobile Agents - MOCA’04

Page 49
5. Conclusions

- Object systems support locality/mobility

- They provide a formal basis for distribution of objects

- We presented a new and simple formalism

- The concept of place-invariants is extended