Università
Ca'Foscari
Venezia

A Non-Repudiation Protocol

Group 7: Andrea Munarin, Francesco Perencin, Simone Jovon

Introduction

In this presentation:

1. A non-repudiation protocol
2. PEPA models
3. Derivation graphs
4. Markov chain and Performance analysis
5. PEPA Eclipse Plug-in

Protocols

General Definition

“The official procedure or system of rules governing affairs of state or diplomatic occasions.”

Computing Definition

“A set of rules governing the exchange or transmission of data between devices.”

Non-repudiation

"*Mallory buys a cell phone for $100, writes a paper cheque as payment, and signs the cheque with a pen. Later, she finds that she can't afford it, and claims that the cheque is a forgery. The signature guarantees that only Mallory could have signed the cheque, and so Mallory's bank must pay the cheque. This is non-repudiation; Mallory cannot repudiate the cheque.*"

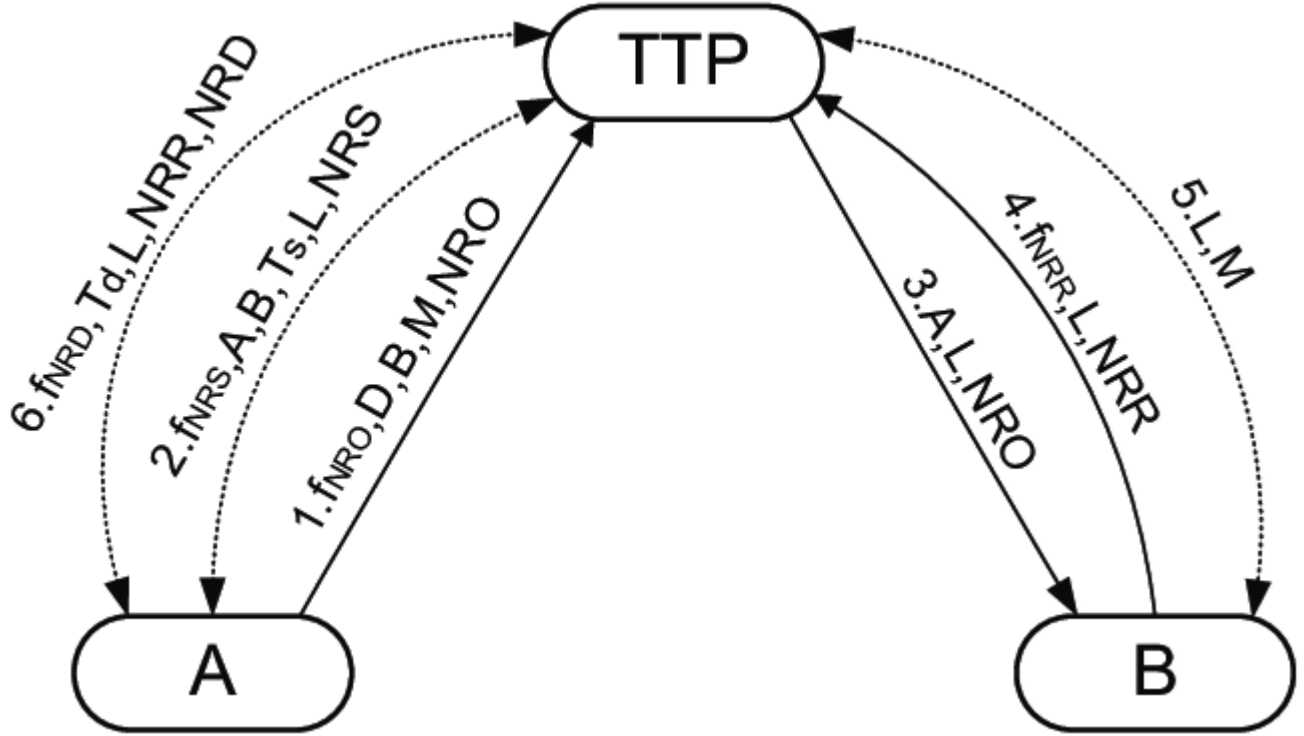
Zhou&Gollmann Model — Terminology 1

- ***M***: Message
- ***L***: a unique label chosen by TTP to identify the message M
- T_s: the time that TTP received A's submission
- T_d: the time that TTP delivered and available to B

Zhou&Gollmann Model — Terminology 2

- $NRO = sS_A(f_{NRO}, TTP, B, M)$
  - non-repudiation of origin for M
- $NRS = sS_D(f_{NRS}, A, B, T_s, L, NRO)$
  - non- repudiation of submission of M
- $NRR = sS_B(f_{NRR}, TTP, A, L, NRO)$
  - non-repudiation of receiving a message labelled L
- $NRD = sS_D(f_{NRD}, A, B, T_d, L, NRR)$
  - non-repudiation of delivery of M

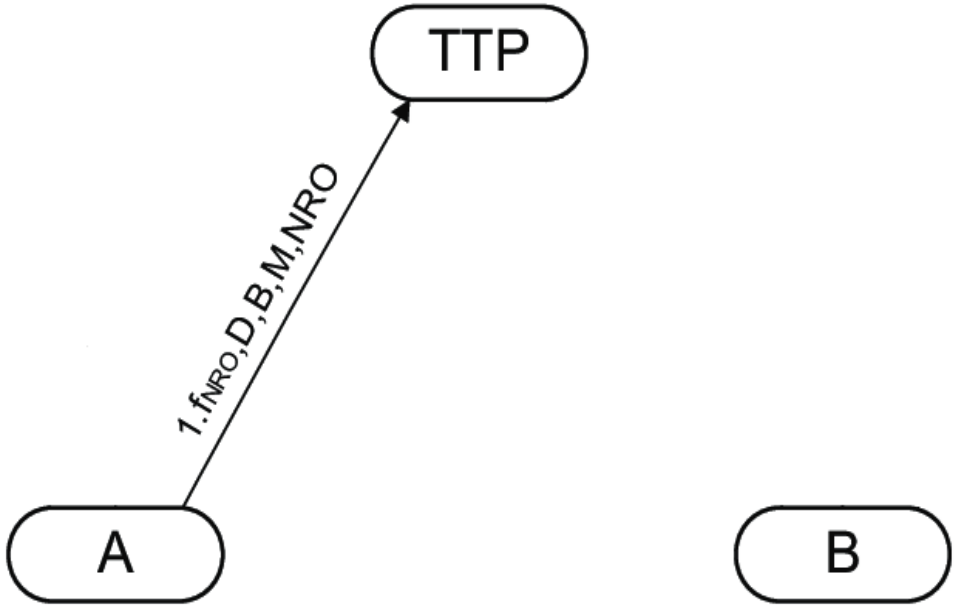
Zhou&Gollmann Model — Representation



Zhou&Gollmann Model — 1.request

A → TTP

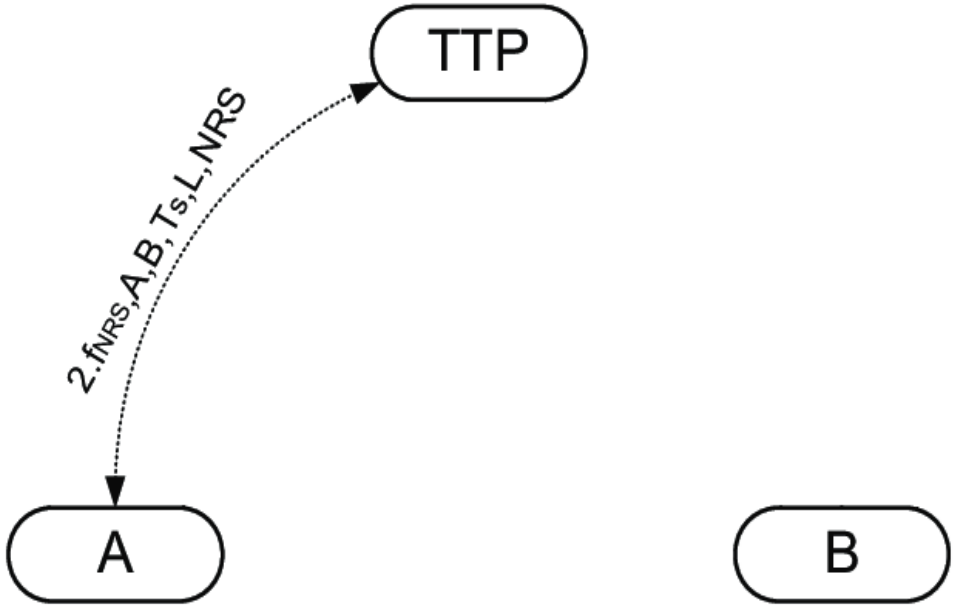
f_{NRO}, TTP, B, M, NRO



Zhou&Gollmann Model — 2.publish1&getByA1

A ↔ ***TTP***

f_{NRS}, *A*, *B*, T_S, *L*, *NRS*



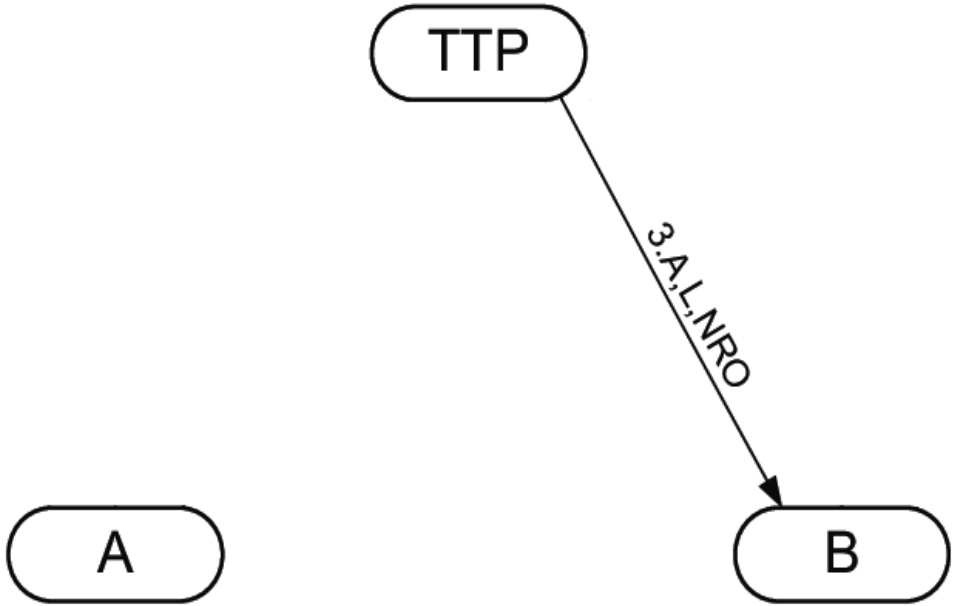
Zhou&Gollmann Model — 3.sendB

TTP → B

A, L, NRO

Andrea Munarin 14:06

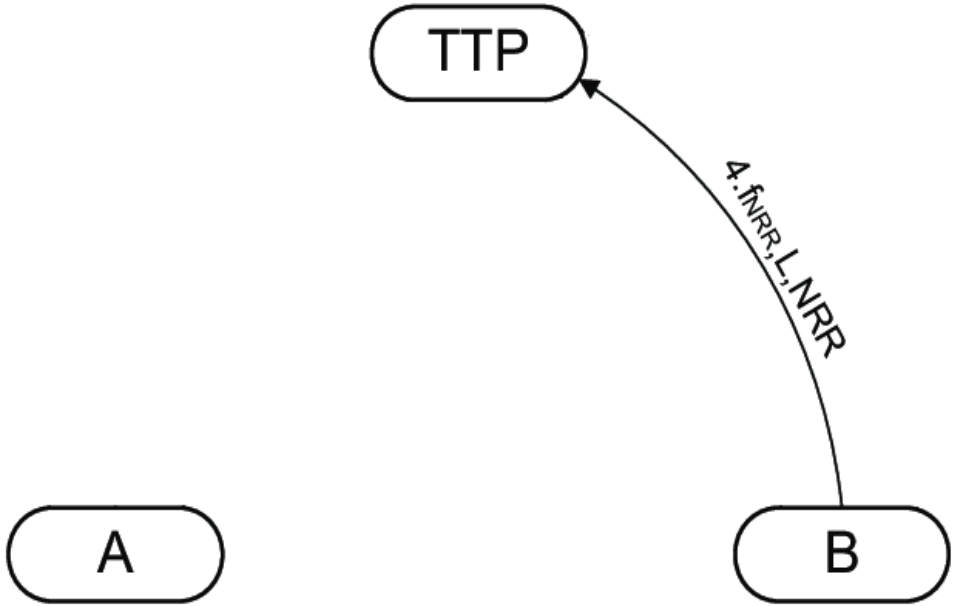
Is everything ok? 1



Zhou&Gollmann Model — 4.sendTTP

B → TTP

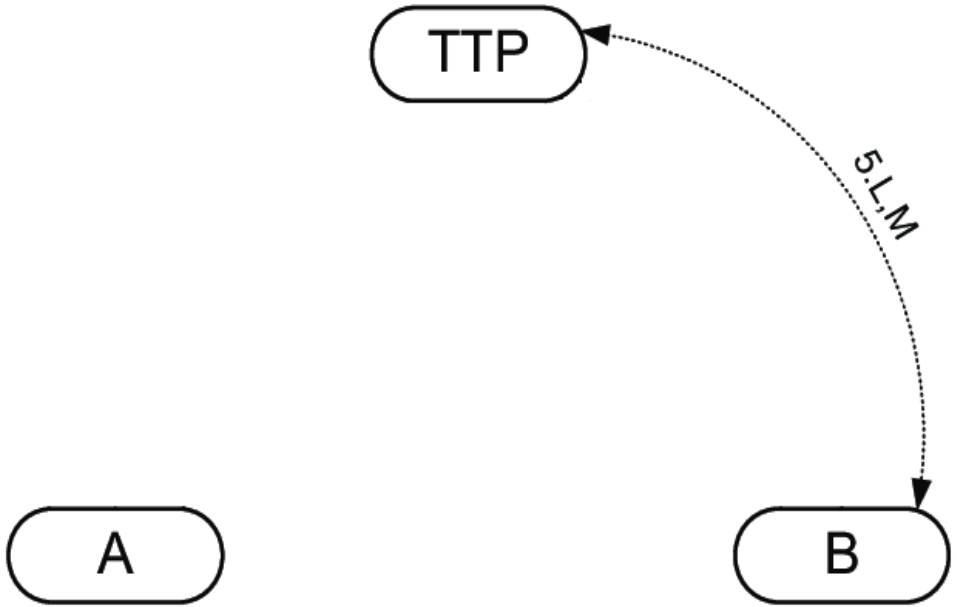
f_{NRR}, *L*, *NRR*



Zhou&Gollmann Model — 5.publish2&getByB

B ↔ ***TTP***

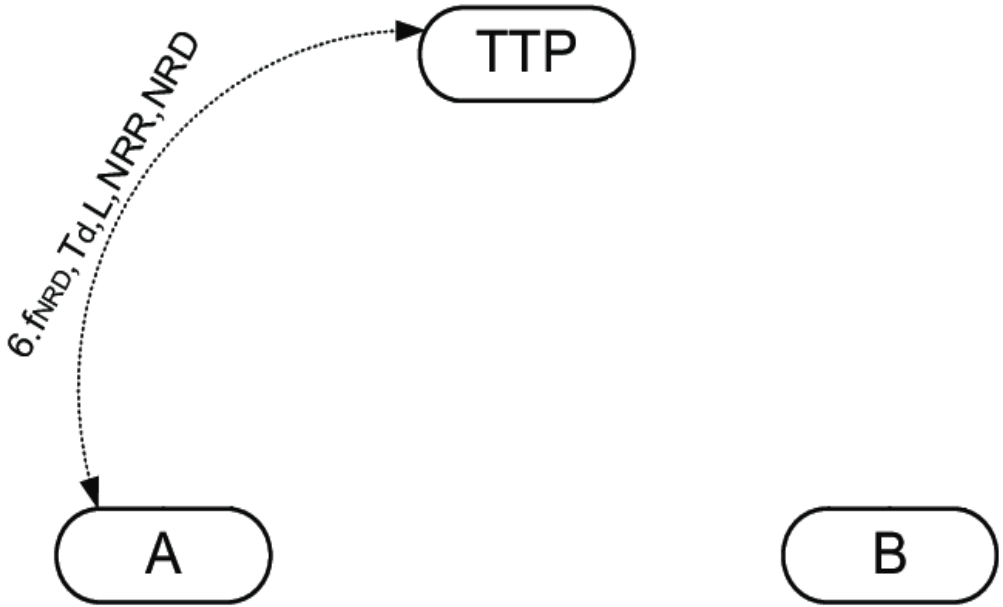
L, M



Zhou&Gollmann Model — 6.publish2&getByA2

A ↔ ***TTP***

f_{NRD}, T_d, L, NRR, NRD



Università
Ca'Foscari
Venezia

PEPA Model

Initial Model — Client A

$$
\begin{aligned}
A_0 &\stackrel{\text{def}}{=} (request, r_{t1}).A_1 \\
A_1 &\stackrel{\text{def}}{=} (publish1, r_{p1}).A_2 \\
A_2 &\stackrel{\text{def}}{=} (getByA1, r_{ga1}).A_3 \\
A_3 &\stackrel{\text{def}}{=} (sendB, r_b).A_4 \\
A_4 &\stackrel{\text{def}}{=} (publish2, r_{p2}).A_5 \\
A_5 &\stackrel{\text{def}}{=} (getByA2, r_{ga2}).A_6 \\
A_6 &\stackrel{\text{def}}{=} (work, r_w).A_0
\end{aligned}
$$

Initial Model — Client B

$$
\begin{aligned}
B_0 &\stackrel{\text{def}}{=} (sendB, r_b).B_1 \\
B_1 &\stackrel{\text{def}}{=} (sendTTP, r_{t2}).B_2 \\
B_2 &\stackrel{\text{def}}{=} (publish2, r_{p2}).B_3 \\
B_3 &\stackrel{\text{def}}{=} (getByB, r_{gb}).B_4 \\
B_4 &\stackrel{\text{def}}{=} (work, r_w).B_0
\end{aligned}
$$

Initial Model — TTP

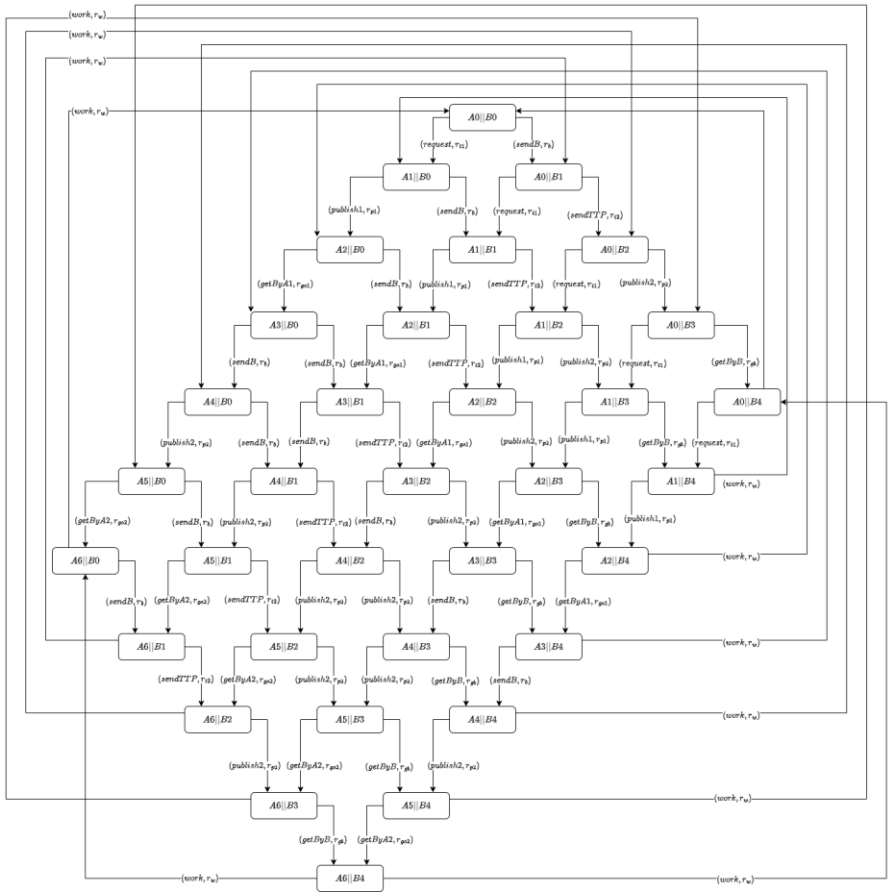
$$TTP \stackrel{\text{def}}{=} (publish1, r_{p1}).TTP + (publish2, r_{p2}).TTP + (sendB, r_b).TTP$$

Initial Model — System

$$System \stackrel{\text{def}}{=} TTP \underset{\mathcal{L}}{\bowtie} (A_0 || B_0)$$

$$\mathcal{L} = \{publish1, publish2, sendB\}$$

Derivation Graph A||B



Università
Ca'Foscari
Venezia

Simplified Model

Simplified Model — Clients AB

$$
\begin{aligned}
AB_0 &\stackrel{\text{def}}{=} (request, r_{t1}).AB_1 \\
AB_1 &\stackrel{\text{def}}{=} (publish1, r_{p1}).AB_2 \\
AB_2 &\stackrel{\text{def}}{=} (getByA1, r_{ga1}).AB_3 \\
AB_3 &\stackrel{\text{def}}{=} (sendB, r_b).AB_4 \\
AB_4 &\stackrel{\text{def}}{=} (sendTTP, r_{t2}).AB_5 \\
AB_5 &\stackrel{\text{def}}{=} (publish2, r_{p2}).AB_6 \\
AB_6 &\stackrel{\text{def}}{=} (getByA2, r_{ga2}).AB_7 + (getByB, r_{gb}).AB_8 \\
AB_7 &\stackrel{\text{def}}{=} (getByB, r_{gb}).AB_9 \\
AB_8 &\stackrel{\text{def}}{=} (getByA2, r_{ga2}).AB_9 \\
AB_9 &\stackrel{\text{def}}{=} (work, r_w).AB_0
\end{aligned}
$$

Simplified Model — TTP

$$TTP \stackrel{\text{def}}{=} (publish1, r_{p1}).TTP + (publish2, r_{p2}).TTP + (sendB, r_b).TTP$$

Simplified Model — System

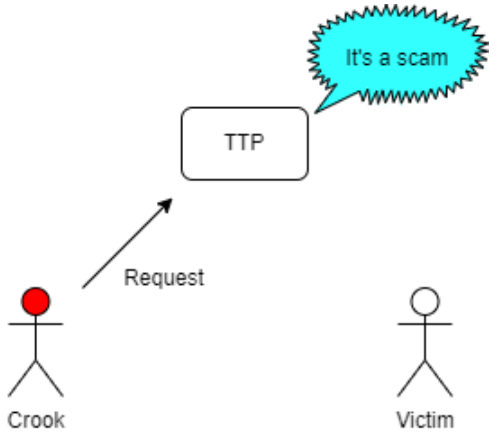
$$System \stackrel{\text{def}}{=} TTP \underset{\mathcal{L}}{\bowtie} AB_0$$

$$\mathcal{L} = \{publish1, publish2, sendB\}$$

Improved System — Verification

Non-Repudation Protocol might be used by unofficial entities:

- User can sign fake contract
- TTP must verify the authenticity of contract
- If scam is recognized, the procedure has to be stopped



Improved System — Clients AB

$$
\begin{aligned}
AB_0 &\stackrel{\text{def}}{=} (request, r_{t1}).AB_1 \\
AB_1 &\stackrel{\text{def}}{=} (verify, T).AB_2 \\
AB_2 &\stackrel{\text{def}}{=} (publish1, T).AB_3 \\
AB_3 &\stackrel{\text{def}}{=} (getByA1, r_{ga1}).AB_4 \\
AB_4 &\stackrel{\text{def}}{=} (sendB, T).AB_5 \\
AB_5 &\stackrel{\text{def}}{=} (sendTTP, r_{t2}).AB_6 \\
AB_6 &\stackrel{\text{def}}{=} (publish2, T).AB_7 \\
AB_7 &\stackrel{\text{def}}{=} (getByA2, r_{ga2}).AB_{8.1} + (getByB, r_{gb}).AB_{8.2} \\
AB_{8.1} &\stackrel{\text{def}}{=} (getByB, r_{gb}).AB_9 \\
AB_{8.2} &\stackrel{\text{def}}{=} (getByA2, r_{ga2}).AB_9 \\
AB_9 &\stackrel{\text{def}}{=} (work, r_w).AB_0
\end{aligned}
$$

Improved System — TTP

$$TTP \stackrel{\text{def}}{=} (verify, r_v).TTP' + (publish2, r_{p2}).TTP + (sendB, r_b).TTP$$
$$TTP' \stackrel{\text{def}}{=} (publish1, r_{p1}).TTP$$

Improved System — System

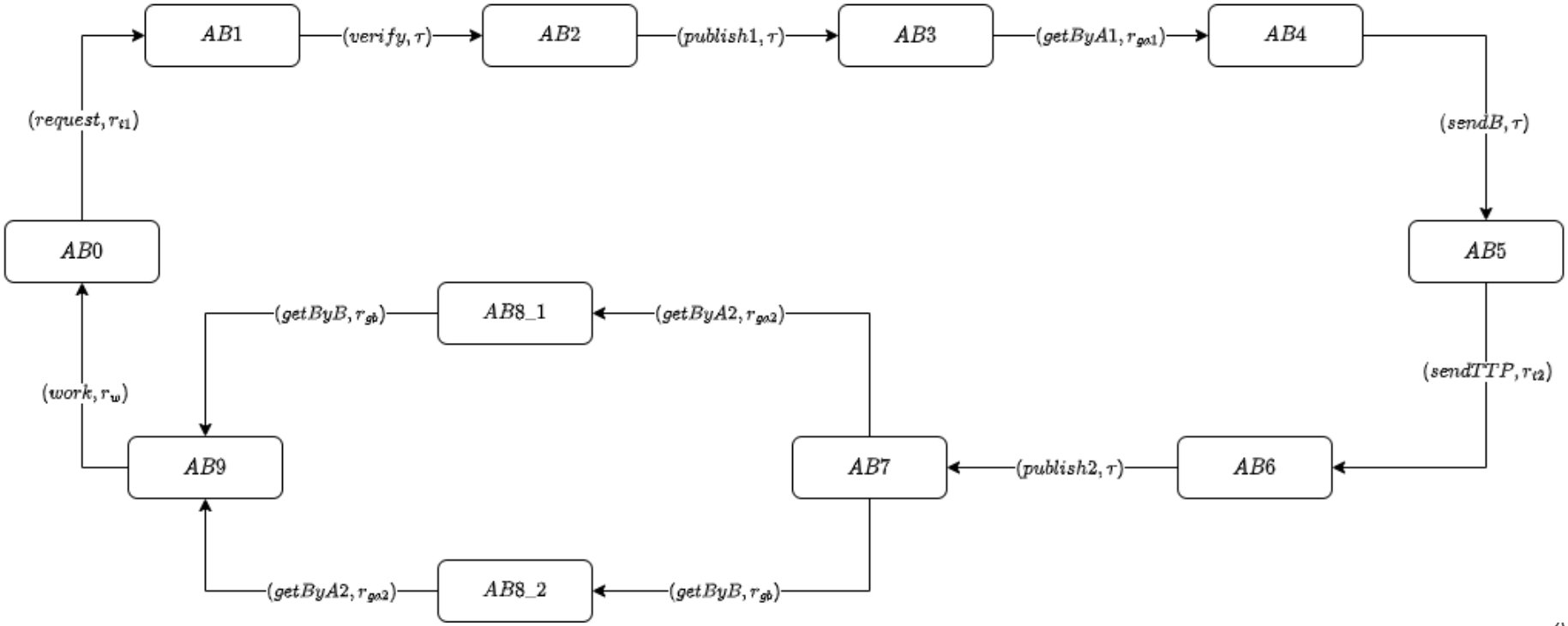
$$System \stackrel{\text{def}}{=} TTP \underset{\mathcal{L}}{\bowtie} AB_0$$

$$\mathcal{L} = \{verify, publish1, publish2, sendB\}$$

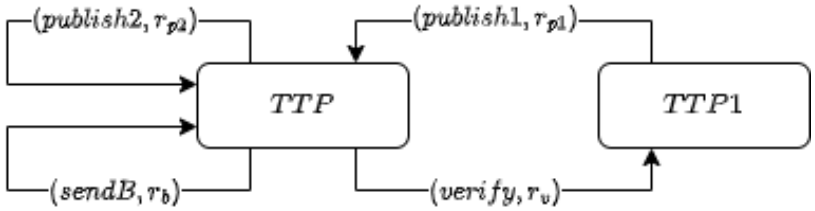
Università
Ca'Foscari
Venezia

Derivation Graphs

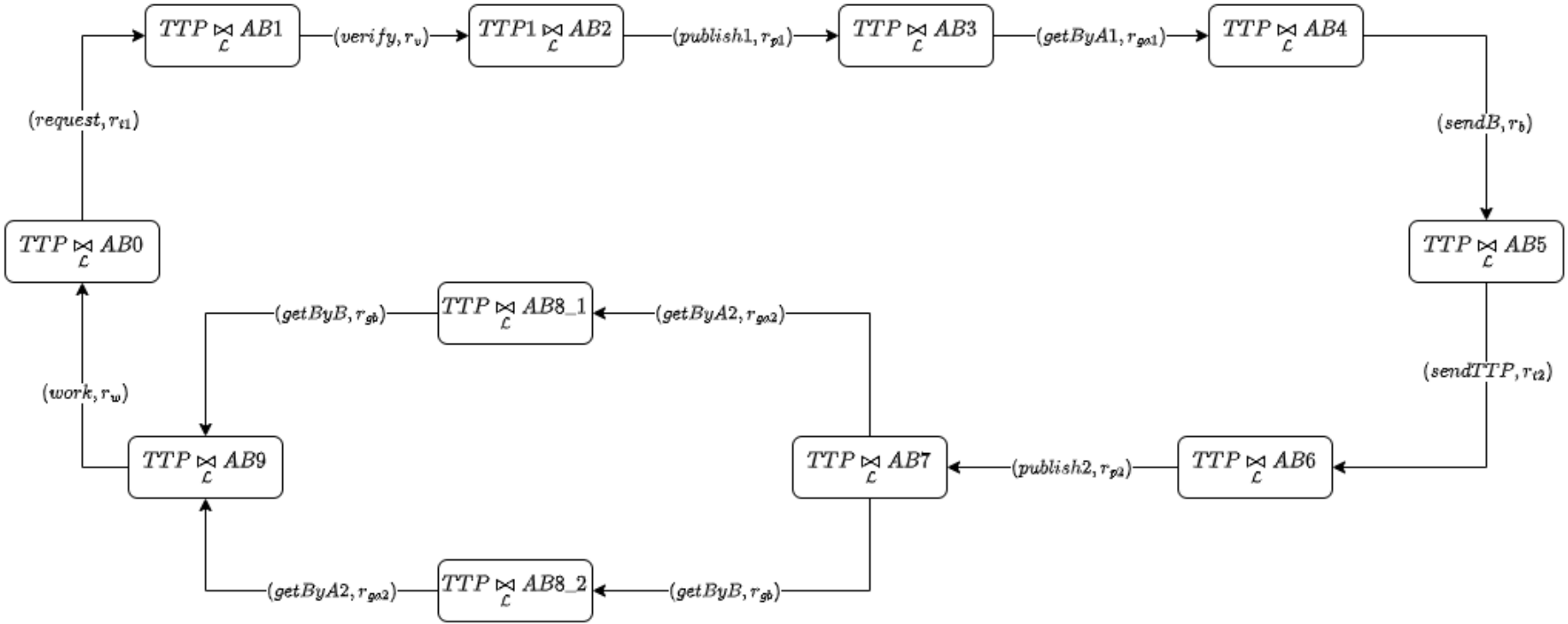
Clients AB


AB1
(verify, τ)
AB2
(publish1, τ)
AB3
(getByA1, r_ga1)
AB4
(request, r_t1)
(sendB, τ)
AB0
AB5
(getByB, r_gb)
AB8_1
(getByA2, r_ga2)
(work, r_w)
(sendTTP, r_t2)
AB9
AB7
(publish2, τ)
AB6
(getByA2, r_ga2)
AB8_2
(getByB, r_gb)

TTP



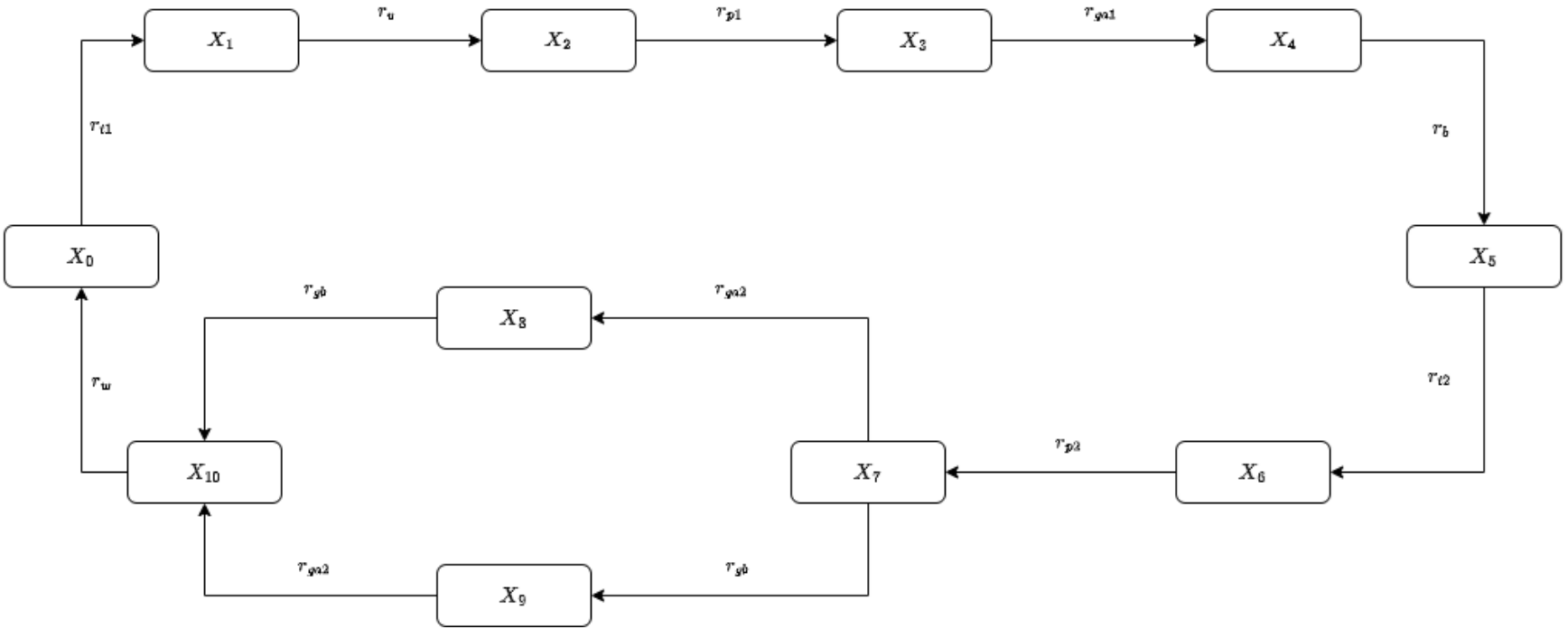
System


$TTP \bowtie_{\mathcal{L}} AB1$
$(verify, r_v)$
$TTP1 \bowtie_{\mathcal{L}} AB2$
$(publish1, r_{p1})$
$TTP \bowtie_{\mathcal{L}} AB3$
$(getByA1, r_{gA1})$
$TTP \bowtie_{\mathcal{L}} AB4$
$(request, r_{t1})$
$(sendB, r_b)$
$TTP \bowtie_{\mathcal{L}} AB0$
$TTP \bowtie_{\mathcal{L}} AB5$
$(getByB, r_{gb})$
$TTP \bowtie_{\mathcal{L}} AB8\_1$
$(getByA2, r_{gA2})$
$(work, r_w)$
$(sendTTP, r_{t2})$
$TTP \bowtie_{\mathcal{L}} AB9$
$TTP \bowtie_{\mathcal{L}} AB7$
$(publish2, r_{p2})$
$TTP \bowtie_{\mathcal{L}} AB6$
$(getByA2, r_{gA2})$
$TTP \bowtie_{\mathcal{L}} AB8\_2$
$(getByB, r_{gb})$

Università
Ca'Foscari
Venezia

Markov Chains and Performance analysis

Underlying Markov chain



Infinitesimal generator matrix

$$A = \begin{pmatrix}
-rt1 & rt1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -rv & rv & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -rp1 & rp1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -rga1 & rga1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -rb & rb & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -rt2 & rt2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -rp2 & rp2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -(rga2 + rgb) & rga2 & rgb & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -rgb & 0 & rgb \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -rga2 & rga2 \\
rw & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -rw
\end{pmatrix}$$

Transpose infinitesimal generator matrix

$$A = \begin{pmatrix}
-rt1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & rw \\
rt1 & -rv & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & rv & -rp1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & rp1 & -rga1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & rga1 & -rb & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & rb & -rt2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & rt2 & -rp2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & rp2 & -(rga2 + rgb) & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & rga2 & -rgb & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & rgb & 0 & -rga2 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Global balance equations

$$
\begin{cases}
-\pi(X_0)\cdot r_{t1} + \pi(X_{10})\cdot r_w = 0 \\
\pi(X_0)\cdot r_{t1} - \pi(X_1)\cdot r_v = 0 \\
\pi(X_1)\cdot r_v - \pi(X_2)\cdot r_{p1} = 0 \\
\pi(X_2)\cdot r_{p1} - \pi(X_3)\cdot r_{ga1} = 0 \\
\pi(X_3)\cdot r_{ga1} - \pi(X_4)\cdot r_b = 0 \\
\pi(X_4)\cdot r_b - \pi(X_5)\cdot r_{t2} = 0 \\
\pi(X_5)\cdot r_{t2} - \pi(X_6)\cdot r_{p2} = 0 \\
\pi(X_6)\cdot r_{p2} - \pi(X_7)\cdot (r_{ga2} + r_{gb}) = 0 \\
\pi(X_7)\cdot r_{ga2} - \pi(X_8)\cdot r_{gb} = 0 \\
\pi(X_7)\cdot r_{gb} - \pi(X_9)\cdot r_{ga2} = 0 \\
\pi(X_8)\cdot r_{gb} + \pi(X_9)\cdot r_{ga2} - \pi(X_{10})\cdot r_w = 0 \\
\pi(X_0)+\pi(X_1)+\pi(X_2)+\pi(X_3)+\pi(X_4)+\pi(X_5)+\pi(X_6)+\pi(X_7)+\pi(X_8)+\pi(X_9)+\pi(X_{10}) = 1
\end{cases}
$$

Steady state distribution

$$R = r_w(r_{t1}r_v(r_{p1}r_{ga1}r_br_{t2}(r_{p2}(r_{ga2}^2 + r_{gb}r_{ga2} + r_{gb}^2) + r_{gb}r_{ga2}^2 + r_{gb}^2r_{ga2}) + r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2r_{ga2})) + r_{t2}r_{p2}(r_{gb}r_{ga2}^2+r_{gb}^2r_{ga2}))+r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2+r_{gb}^2r_{ga2}))+r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2+r_{gb}^2r_{ga2}))+r_{p1}r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2+ r_{gb}^2r_{ga2})) + r_vr_{p1}r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2r_{ga2})) + r_{t1}r_vr_{p1}r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2r_{ga2})$$

$$\pi(X_0) = \frac{r_wr_vr_{p1}r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2+r_{gb}^2r_{ga2})}{R}$$

$$\pi(X_1) = \frac{r_{t1}r_wr_{p1}r_{ga1}r_br_{t2}r_{p2}(r_{gb}r_{ga2}^2+r_{gb}^2r_{ga2})}{R}$$

Steady state probabilities

$$\pi(X_2) = \frac{r_{t1}r_w r_v r_{ga1} r_b r_{t2} r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

$$\pi(X_3) = \frac{r_{t1}r_w r_v r_{p1} r_b r_{t2} r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

$$\pi(X_4) = \frac{r_{t1}r_w r_v r_{p1} r_{ga1} r_{t2} r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

$$\pi(X_5) = \frac{r_{t1}r_w r_v r_{p1} r_{ga1} r_b r_{p2}(r_{gb}r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

$$\pi(X_6) = \frac{r_{t1}r_w r_v r_{p1} r_{ga1} r_b r_{t2}(r_{gb}r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

$$\pi(X_7) = \frac{r_{t1}r_w r_v r_{p1} r_{ga1} r_b r_{t2} r_{p2} r_{ga2} r_{gb}}{R}$$

Steady state probabilities

$$\pi(X_8) = \frac{r_{t1} r_w r_v r_{p1} r_{ga1} r_b r_{t2} r_{p2} r_{ga2}^2}{R}$$

$$\pi(X_9) = \frac{r_{t1} r_w r_v r_{p1} r_{ga1} r_b r_{t2} r_{p2} r_{gb}^2}{R}$$

$$\pi(X_{10}) = \frac{r_{t1} r_v r_{p1} r_{ga1} r_b r_{t2} r_{p2} (r_{gb} r_{ga2}^2 + r_{gb}^2 r_{ga2})}{R}$$

Utilisation

$$U_{AB} = \pi(X_0) + \pi(X_1) + \pi(X_2) + \pi(X_3) + \pi(X_4) + \pi(X_5) + \pi(X_6) + \\ \pi(X_7) + \pi(X_8) + \pi(X_9) + \pi(X_{10})$$

$$U_{TTP} = \pi(X_1) + \pi(X_2) + \pi(X_4) + \pi(X_6)$$

Throughput

$$
\begin{aligned}
T_{request} &= r_{t1} \cdot \pi(X_0) \\
T_{verify} &= r_v \cdot \pi(X_1) \\
T_{publish1} &= r_{p1} \cdot \pi(X_2) \\
T_{getByA1} &= r_{ga1} \cdot \pi(X_3) \\
T_{sendB} &= r_b \cdot \pi(X_4) \\
T_{sendTTP} &= r_{t2} \cdot \pi(X_5) \\
T_{publish2} &= r_{p2} \cdot \pi(X_6) \\
T_{getByA2} &= r_{ga2} \cdot \pi(X_7) + r_{ga2} \cdot \pi(X_9) \\
T_{getByB} &= r_{gb} \cdot \pi(X_7) + r_{gb} \cdot \pi(X_8) \\
T_{work} &= r_w \cdot \pi(X_{10})
\end{aligned}
$$

Università
Ca'Foscari
Venezia

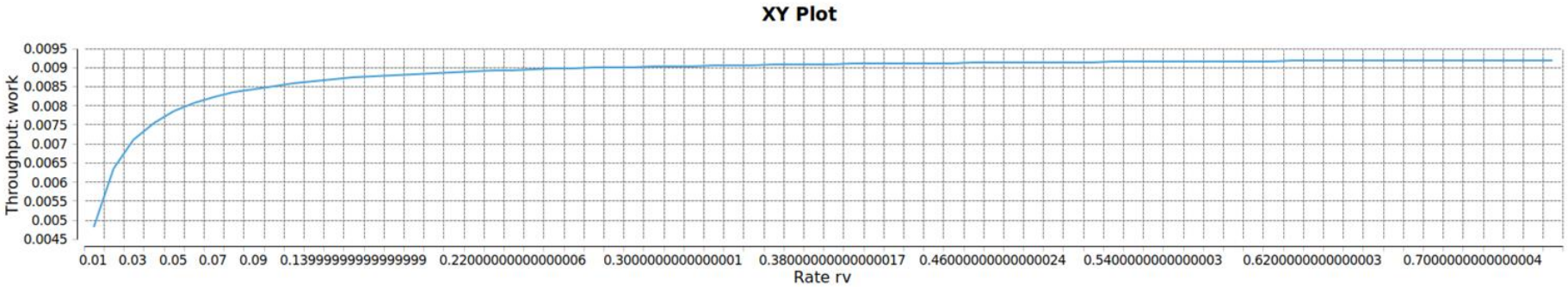
PEPA Eclipse Plug-in

Pepa Model

model.pepa

```
rb = 1.0;
rga1 = 1.0;
rga2 = 1.0;
rgb = 1.0;
rp1 = 1.0;
rp2 = 1.0;
rt1 = 1.0;
rt2 = 1.0;
rw = 0.01;
rv = 0.05;
AB0 = (request, rt1).AB1;
AB1 = (verify, infty).AB2;
AB2 = (publish1, infty).AB3;
AB3 = (getByA1, rga1).AB4;
AB4 = (sendB, infty).AB5;
AB5 = (sendTTP, rt2).AB6;
AB6 = (publish2, infty).AB7;
AB7 = (getByA2, rga2).AB8_1 + (getByB, rgb).AB8_2;
AB8_1 = (getByB, rgb).AB9;
AB8_2 = (getByA2, rga2).AB9;
AB9 = (work, rw).AB0;
TTP = (verify, rv).TTP1 +(publish2, rp2).TTP + (sendB, rb).TTP;
TTP1 = (publish1, rp1).TTP;
TTP <verify, publish1,publish2,sendB> AB0
```

Experimentation



Throughput Variation

Our model

Utilisation | Throughput | Population

Action	Throughput
getByA1	0.007843137254901955
getByA2	0.007843137254901954
getByB	0.007843137254901954
publish1	0.007843137254901954
publish2	0.007843137254901952
request	0.007843137254901962
sendB	0.007843137254901954
sendTTP	0.00784313725490196
verify	0.007843137254901959
work	0.007843137254901962

Original model

Utilisation | Throughput | Population

Action	Throughput
getByA1	0.00930232558139535
getByA2	0.00930232558139535
getByB	0.00930232558139535
publish1	0.00930232558139535
publish2	0.00930232558139535
request	0.00930232558139535
sendB	0.00930232558139535
sendTTP	0.00930232558139535
work	0.00930232558139535

Utilisation

Steady state probabilities

1	TTP	AB0	0.007843137254901962
2	TTP	AB1	0.15686274509803919
3	TTP1	AB2	0.007843137254901954
4	TTP	AB3	0.007843137254901955
5	TTP	AB4	0.007843137254901954
6	TTP	AB5	0.00784313725490196
7	TTP	AB6	0.007843137254901952
8	TTP	AB7	0.003921568627450977
9	TTP	AB8_1	0.003921568627450977
10	TTP	AB8_2	0.003921568627450977
11	TTP	AB9	0.7843137254901962

Utilisation

$$U_{AB} = 1$$

$$\begin{aligned} U_{TTP} \sim & \, 0.156862755 + 0.007843137 \\ & + 0.007843137 + 0.007843137 \\ & = 0,180392166 \end{aligned}$$

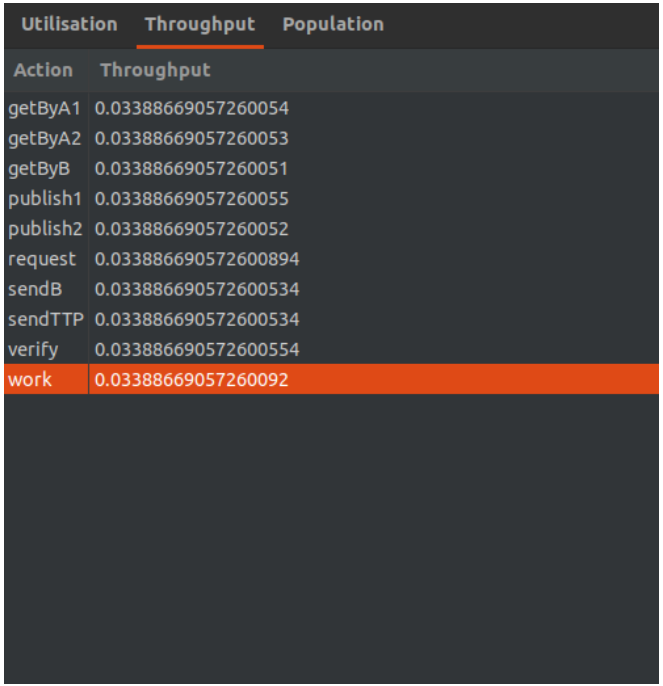
More clients

model.pepa | model2.pepa

```
rb = 1.0;
rga1 = 1.0;
rga2 = 1.0;
rgb = 1.0;
rp1 = 1.0;
rp2 = 1.0;
rt1 = 1.0;
rt2 = 1.0;
rw = 0.01;
rv = 0.05;
AB0 = (request, rt1).AB1;
AB1 = (verify, rv).AB2;
AB2 = (publish1, rp2).AB3;
AB3 = (getByA1, rga1).AB4;
AB4 = (sendB, rb).AB5;
AB5 = (sendTTP, rt2).AB6;
AB6 = (publish2, rp2).AB7;
AB7 = (getByA2, rga2).AB8_1 + (getByB, rgb).AB8_2;
AB8_1 = (getByB, rgb).AB9;
AB8_2 = (getByA2, rga2).AB9;
AB9 = (work, rw).AB0;
TTP = (verify, rv).TTP1 +(publish2, rp2).TTP + (sendB, rb).TTP;
TTP1 = (publish1, rp1).TTP;
TTP[1] <verify, publish1,publish2,sendB> AB0[5]
```

Throughput

Total throughput



Utilisation | Throughput | Population

Action	Throughput
getByA1	0.03388669057260054
getByA2	0.03388669057260053
getByB	0.03388669057260051
publish1	0.03388669057260055
publish2	0.03388669057260052
request	0.033886690572600894
sendB	0.033886690572600534
sendTTP	0.033886690572600534
verify	0.033886690572600554
work	0.03388669057260092

Throughput of multi-client

$$T_{work} = \frac{0.03388669057260092}{5} = 0.006777338114520184$$

Throughput of single-client

$$T_{work} = 0.007843137254901962$$