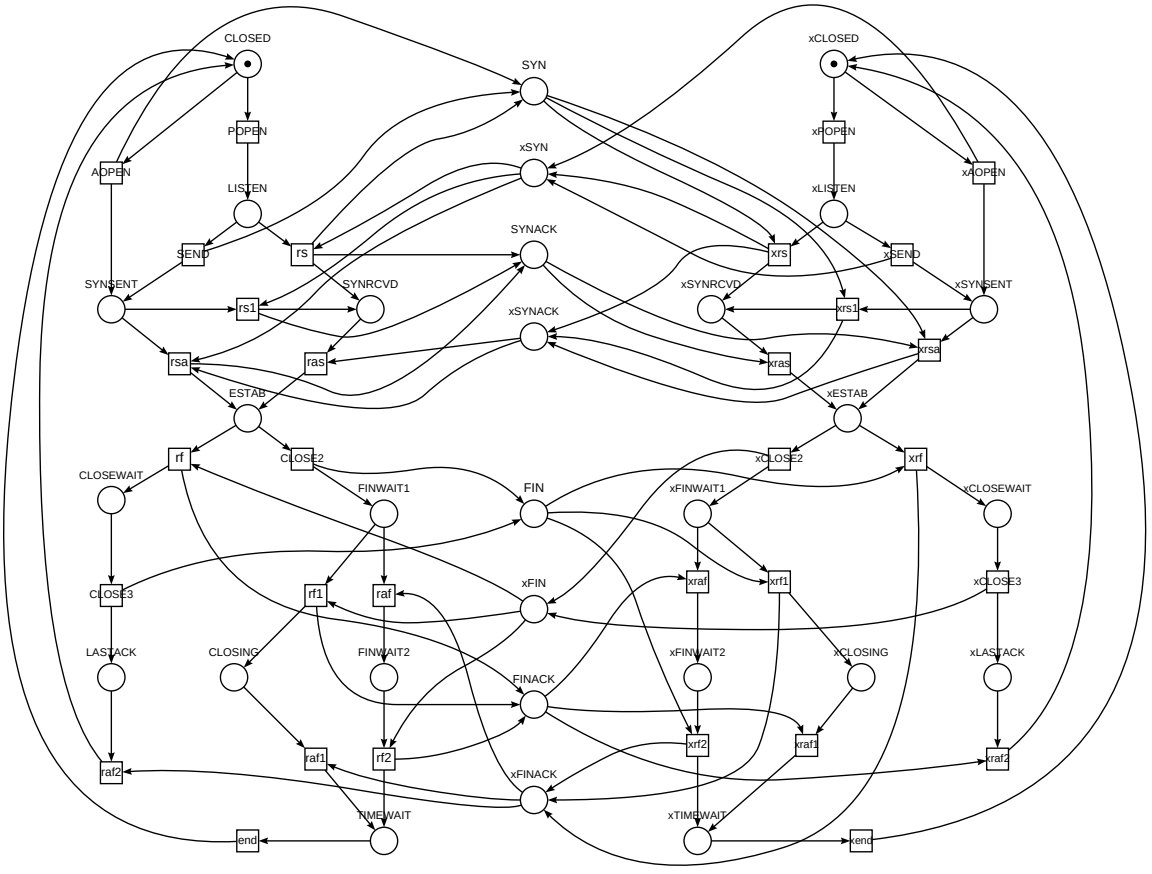
Dmitry Zaitsev
daze@acm.org

This form is a summary description of the model entitled "TCPcondis" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.

Description

TCPcondis stands for "TCP connection and disconnection". The model describes connection and disconnection procedures of Transmission Control Protocol according to RFC 793. Two communicating systems (symmetric) occupy the left and right parts of the model while its central part represents flags of TCP header. A three way handshake is modeled based on the Transmission Control Protocol Functional Specification.



Graphical representation for $N = 1$

References

[1] Zaitsev D.A. Clans of Petri Nets: Verification of protocols and performance evaluation of networks, LAP LAMBERT Academic Publishing, 2013, 292 p.

[2] Zaitsev D.A. Petri Nets for Modeling and Computing. Videolecture. USA: IGI-Global, August 2015, 2 hrs 25 mins.

[3] Zaitsev D.A. Verification of protocol TCP via decomposition of Petri net model into functional subnets. Proceedings of the Poster session of 12th Annual Meeting of the IEEE and ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, October 5-7, 2004, Volendam, Netherlands, p. 73-75.

Dmitry Zaitsev
daze@acm.org

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	Number of communicating processes on each side ($CLOSED = xCLOSED = N$).	5, 10, 15, 20, 25, 30, 35, 40, 50

Size of the model

Although the model is parameterized, its size does not depend on parameter values.

number of places:	30
number of transitions:	32
number of arcs:	108

Structural properties

ordinary — *all arcs have multiplicity one* ..... ✔
simple free choice — *all transitions sharing a common input place have no other input place* ..... ✘ [a]
extended free choice — *all transitions sharing a common input place have the same input places* ..... ✘ [b]
state machine — *every transition has exactly one input place and exactly one output place* ..... ✘ [c]
marked graph — *every place has exactly one input transition and exactly one output transition* ..... ✘ [d]
connected — *there is an undirected path between every two nodes (places or transitions)* ..... ✔ [e]
strongly connected — *there is a directed path between every two nodes (places or transitions)* ..... ✔ [f]
source place(s) — *one or more places have no input transitions* ..... ✘ [g]
sink place(s) — *one or more places have no output transitions* ..... ✘ [h]
source transition(s) — *one or more transitions have no input places* ..... ✘ [i]
sink transitions(s) — *one or more transitions have no output places* ..... ✘ [j]
loop-free — *no transition has an input place that is also an output place* ..... ✔ [k]
conservative — *for each transition, the number of input arcs equals the number of output arcs* ..... ✘ [l]
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ..... ✘ [m]
nested units — *places are structured into hierarchically nested sequential units* [n] ..... ✘

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* ..... ✘ [o]
dead place(s) — *one or more places have no token in any reachable marking* ..... ✘ [p]
dead transition(s) — *one or more transitions cannot fire from any reachable marking* ..... ✘ [q]
deadlock — *there exists a reachable marking from which no transition can be fired* ..... ✘
reversible — *from every reachable marking, there is a transition path going back to the initial marking* ..... ✔

[a] 34 arcs are not simple free choice, e.g., the arc from place "ESTAB" (which has 2 outgoing transitions) to transition "rf" (which has 2 input places).
[b] transitions "rf" and "CLOSE2" share a common input place "ESTAB", but only the former transition has input place "xFIN".
[c] 28 transitions are not of a state machine, e.g., transition "AOPEN".
[d] 22 places are not of a marked graph, e.g., place "CLOSED".
[e] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[f] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[g] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[h] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[i] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[j] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[k] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[l] 20 transitions are not conservative, e.g., transition "AOPEN".
[m] 10 transitions are not subconservative, e.g., transition "AOPEN".
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[p] stated by CÆSAR.BDD version 3.3 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).
[q] stated by CÆSAR.BDD version 2.6 on all 9 instances (5, 10, 15, 20, 25, 30, 35, 40, and 50).

Dmitry Zaitsev
daze@acm.org

live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ✔

Size of the marking graphs

Parameter	Number of reachable markings	Number of transition firings	Max. number of tokens per place	Max. number of tokens per marking
$N = 5$	2985834	24899392	5	20
$N = 10$	?	?	?	≥ 20 [r]
$N = 15$	?	?	?	≥ 30 [s]
$N = 20$	?	?	?	≥ 40 [t]
$N = 25$	?	?	?	≥ 50 [u]
$N = 30$	?	?	?	≥ 60 [v]
$N = 35$	?	?	?	≥ 70 [w]
$N = 40$	?	?	?	≥ 80 [x]
$N = 50$	?	?	?	≥ 100 [y]

Other properties

The model is a safe Petri net when $N = 1$. It was modelled with Tina http://www.laas.fr/tina

[r] lower bound given by the number of initial tokens.
[s] lower bound given by the number of initial tokens.
[t] lower bound given by the number of initial tokens.
[u] lower bound given by the number of initial tokens.
[v] lower bound given by the number of initial tokens.
[w] lower bound given by the number of initial tokens.
[x] lower bound given by the number of initial tokens.
[y] lower bound given by the number of initial tokens.