Rim Abid, Gwen Salaün, and Noël de Palma
gwen.salaun@inria.fr

This form is a summary description of the model entitled "Cloud Reconfiguration" 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

Distributed cloud applications are complex applications composed of a set of interconnected software components running on different virtual machines, hosted on remote physical servers. Deploying and reconfiguring this kind of applications are very complicated tasks especially when one or multiple virtual machines fail when achieving these tasks. Hence, there is a need for protocols that can dynamically reconfigure and manage running distributed applications. In [1], a novel protocol for reconfiguring distributed cloud applications is presented. This protocol is able to ensure communication between virtual machines and resolve dependencies by exchanging messages, (dis)connecting, and starting/stopping components in a specific order. The interaction between machines is assured via a publish-subscribe messaging system. Each machine reconfigures itself in a decentralized way. The protocol supports virtual machine failures, and the reconfiguration always terminates successfully even in the presence of a finite number of failures.

Due to the high degree of parallelism inherent to these applications, the protocol was formally specified using the LNT value-passing process calculus and analyzed using the model checking tools available in the CADP toolbox. This helped to detect several bugs and improve the protocol.

This collection of P/T nets was obtained from automatically-generated LNT specifications of the protocol. Each LNT specification reflects a given software architecture to be deployed, a given scenario (a list of addition/removal of virtual machines), and generates all possible executions of the protocol for this architecture. Each LNT specification was translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, a P/T net was obtained by stripping out all data-related information (variables, types, assignments, guards, etc.) from the interpreted Petri net, leading to a NUPN (Nested-Unit Petri Net) model translated to PNML using the CÆSAR.BDD tool.

Among a large family of LNT architectural models, we selected those leading to a NUPN with at least 10^{10} reachable states. Each NUPN is parameterized by two numbers N and P, where N is the number of virtual machines used for the reconfiguration, and P is a unique number characterizing the software architecture and the scenario. Notice that the NUPNs are independent from other parameters of the architecture (such as the number of components, and the number of bindings, i.e., communication links between components) because these parameters are encoded as LNT data values.

References

[1] Rim Abid, Gwen Salaün, and Noël De Palma. *Formal Design of Dynamic Reconfiguration Protocol for Cloud Applications.* Science of Computer Program.ming 117:1-16, 2016. Available from https://hal.inria.fr/hal-01246152/en.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(N, P)	N is the number of virtual machines and P characterizes the architecture and scenario	$\{3, 4\} \times \{1...20\}$

Rim Abid, Gwen Salaün, and Noël de Palma
gwen.salaun@inria.fr

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 3, P = 1$	2584	3094	6459	9	5–5–48
$N = 3, P = 2$	2585	3095	6463	9	5–5–48
$N = 3, P = 3$	2584	3094	6459	9	5–5–48
$N = 3, P = 4$	2584	3094	6459	9	5–5–48
$N = 3, P = 5$	2585	3095	6463	9	5–5–48
$N = 3, P = 6$	2584	3094	6459	9	5–5–48
$N = 3, P = 7$	2584	3094	6459	9	5–5–48
$N = 3, P = 8$	2585	3095	6463	9	5–5–48
$N = 3, P = 9$	2585	3095	6463	9	5–5–48
$N = 3, P = 10$	2585	3095	6463	9	5–5–48
$N = 3, P = 11$	2585	3095	6463	9	5–5–48
$N = 3, P = 12$	2585	3095	6463	9	5–5–48
$N = 3, P = 13$	2585	3095	6463	9	5–5–48
$N = 3, P = 14$	2585	3095	6463	9	5–5–48
$N = 3, P = 15$	2585	3095	6463	9	5–5–48
$N = 3, P = 16$	2585	3095	6463	9	5–5–48
$N = 3, P = 17$	2587	3099	6479	9	5–5–48
$N = 3, P = 18$	2587	3099	6479	9	5–5–48
$N = 3, P = 19$	2587	3099	6479	9	5–5–48
$N = 3, P = 20$	2587	3099	6479	9	5–5–48
$N = 4, P = 1$	3554	4263	8889	11	6–6–60
$N = 4, P = 2$	3554	4263	8889	11	6–6–60

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]

[a] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[b] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[c] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[d] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[e] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[f] from place 1 one cannot reach place 0.
[g] place 0 is a source place.
[h] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[i] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[j] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[k] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[l] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).
[m] stated by CÆSAR.BDD version 2.7 on all 22 instances (2 values of N × 20 values of P).

Rim Abid, Gwen Salaün, and Noël de Palma
gwen.salaun@inria.fr

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]
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* ..... ?
quasi-live — *for every transition t, there exists a reachable marking in which t can fire* ..... ? [p]
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
$N = 3, P = 1$	$\geq$ 6.04469e+10 [q]	?	1 [r]	$\leq$ 5 [s]
$N = 3, P = 2$	$\geq$ 7.59421e+10 [t]	?	1 [u]	$\leq$ 5 [v]
$N = 3, P = 3$	$\geq$ 4.59885e+10 [w]	?	1 [x]	$\leq$ 5 [y]
$N = 3, P = 4$	$\geq$ 7.75114e+10 [z]	?	1 [aa]	$\leq$ 5 [ab]
$N = 3, P = 5$	$\geq$ 6.54918e+10 [ac]	?	1 [ad]	$\leq$ 5 [ae]
$N = 3, P = 6$	$\geq$ 5.3956e+10 [af]	?	1 [ag]	$\leq$ 5 [ah]
$N = 3, P = 7$	$\geq$ 5.51052e+10 [ai]	?	1 [aj]	$\leq$ 5 [ak]
$N = 3, P = 8$	$\geq$ 8.84278e+10 [al]	?	1 [am]	$\leq$ 5 [an]
$N = 3, P = 9$	$\geq$ 3.28481e+10 [ao]	?	1 [ap]	$\leq$ 5 [aq]
$N = 3, P = 10$	$\geq$ 6.41154e+10 [ar]	?	1 [as]	$\leq$ 5 [at]
$N = 3, P = 11$	$\geq$ 5.53567e+10 [au]	?	1 [av]	$\leq$ 5 [aw]
$N = 3, P = 12$	$\geq$ 8.93633e+10 [ax]	?	1 [ay]	$\leq$ 5 [az]
$N = 3, P = 13$	$\geq$ 7.59421e+10 [ba]	?	1 [bb]	$\leq$ 5 [bc]
$N = 3, P = 14$	$\geq$ 5.53566e+10 [bd]	?	1 [be]	$\leq$ 5 [bf]
$N = 3, P = 15$	$\geq$ 6.54918e+10 [bg]	?	1 [bh]	$\leq$ 5 [bi]
$N = 3, P = 16$	$\geq$ 6.54918e+10 [bj]	?	1 [bk]	$\leq$ 5 [bl]
$N = 3, P = 17$	$\geq$ 6.68417e+10 [bm]	?	1 [bn]	$\leq$ 5 [bo]
$N = 3, P = 18$	$\geq$ 7.34346e+10 [bp]	?	1 [bq]	$\leq$ 5 [br]
$N = 3, P = 19$	$\geq$ 6.54961e+10 [bs]	?	1 [bt]	$\leq$ 5 [bu]
$N = 3, P = 20$	$\geq$ 4.21669e+10 [bv]	?	1 [bw]	$\leq$ 5 [bx]
$N = 4, P = 1$	$\geq$ 1.07608e+12 [by]	?	1 [bz]	$\leq$ 6 [ca]
$N = 4, P = 2$	$\geq$ 9.62807e+11 [cb]	?	1 [cc]	$\leq$ 6 [cd]

[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] safe by construction – stated by the CÆSAR compiler.
[p] stated by CÆSAR.BDD version 2.7 to be true on 1 instance(s) out of 22, and unknown on the remaining 21 instance(s).
[q] stated by CÆSAR.BDD version 2.7.
[r] stated by the CÆSAR compiler.
[s] upper bound given by the number of leaf units.
[t] stated by CÆSAR.BDD version 2.7.
[u] stated by the CÆSAR compiler.
[v] upper bound given by the number of leaf units.
[w] stated by CÆSAR.BDD version 2.7.
[x] stated by the CÆSAR compiler.
[y] upper bound given by the number of leaf units.
[z] stated by CÆSAR.BDD version 2.7.
[aa] stated by the CÆSAR compiler.
[ab] upper bound given by the number of leaf units.
[ac] stated by CÆSAR.BDD version 2.7.
[ad] stated by the CÆSAR compiler.
[ae] upper bound given by the number of leaf units.
[af] stated by CÆSAR.BDD version 2.7.

Rim Abid, Gwen Salaün, and Noël de Palma
gwen.salaun@inria.fr

(ag) stated by the CÆSAR compiler.
(ah) upper bound given by the number of leaf units.
(ai) stated by CÆSAR.BDD version 2.7.
(aj) stated by the CÆSAR compiler.
(ak) upper bound given by the number of leaf units.
(al) stated by CÆSAR.BDD version 2.7.
(am) stated by the CÆSAR compiler.
(an) upper bound given by the number of leaf units.
(ao) stated by CÆSAR.BDD version 2.7.
(ap) stated by the CÆSAR compiler.
(aq) upper bound given by the number of leaf units.
(ar) stated by CÆSAR.BDD version 2.7.
(as) stated by the CÆSAR compiler.
(at) upper bound given by the number of leaf units.
(au) stated by CÆSAR.BDD version 2.7.
(av) stated by the CÆSAR compiler.
(aw) upper bound given by the number of leaf units.
(ax) stated by CÆSAR.BDD version 2.7.
(ay) stated by the CÆSAR compiler.
(az) upper bound given by the number of leaf units.
(ba) stated by CÆSAR.BDD version 2.7.
(bb) stated by the CÆSAR compiler.
(bc) upper bound given by the number of leaf units.
(bd) stated by CÆSAR.BDD version 2.7.
(be) stated by the CÆSAR compiler.
(bf) upper bound given by the number of leaf units.
(bg) stated by CÆSAR.BDD version 2.7.
(bh) stated by the CÆSAR compiler.
(bi) upper bound given by the number of leaf units.
(bj) stated by CÆSAR.BDD version 2.7.
(bk) stated by the CÆSAR compiler.
(bl) upper bound given by the number of leaf units.
(bm) stated by CÆSAR.BDD version 2.7.
(bn) stated by the CÆSAR compiler.
(bo) upper bound given by the number of leaf units.
(bp) stated by CÆSAR.BDD version 2.7.
(bq) stated by the CÆSAR compiler.
(br) upper bound given by the number of leaf units.
(bs) stated by CÆSAR.BDD version 2.7.
(bt) stated by the CÆSAR compiler.
(bu) upper bound given by the number of leaf units.
(bv) stated by CÆSAR.BDD version 2.7.
(bw) stated by the CÆSAR compiler.
(bx) upper bound given by the number of leaf units.
(by) stated by CÆSAR.BDD version 2.7.
(bz) stated by the CÆSAR compiler.
(ca) upper bound given by the number of leaf units.
(cb) stated by CÆSAR.BDD version 2.7.
(cc) stated by the CÆSAR compiler.
(cd) upper bound given by the number of leaf units.