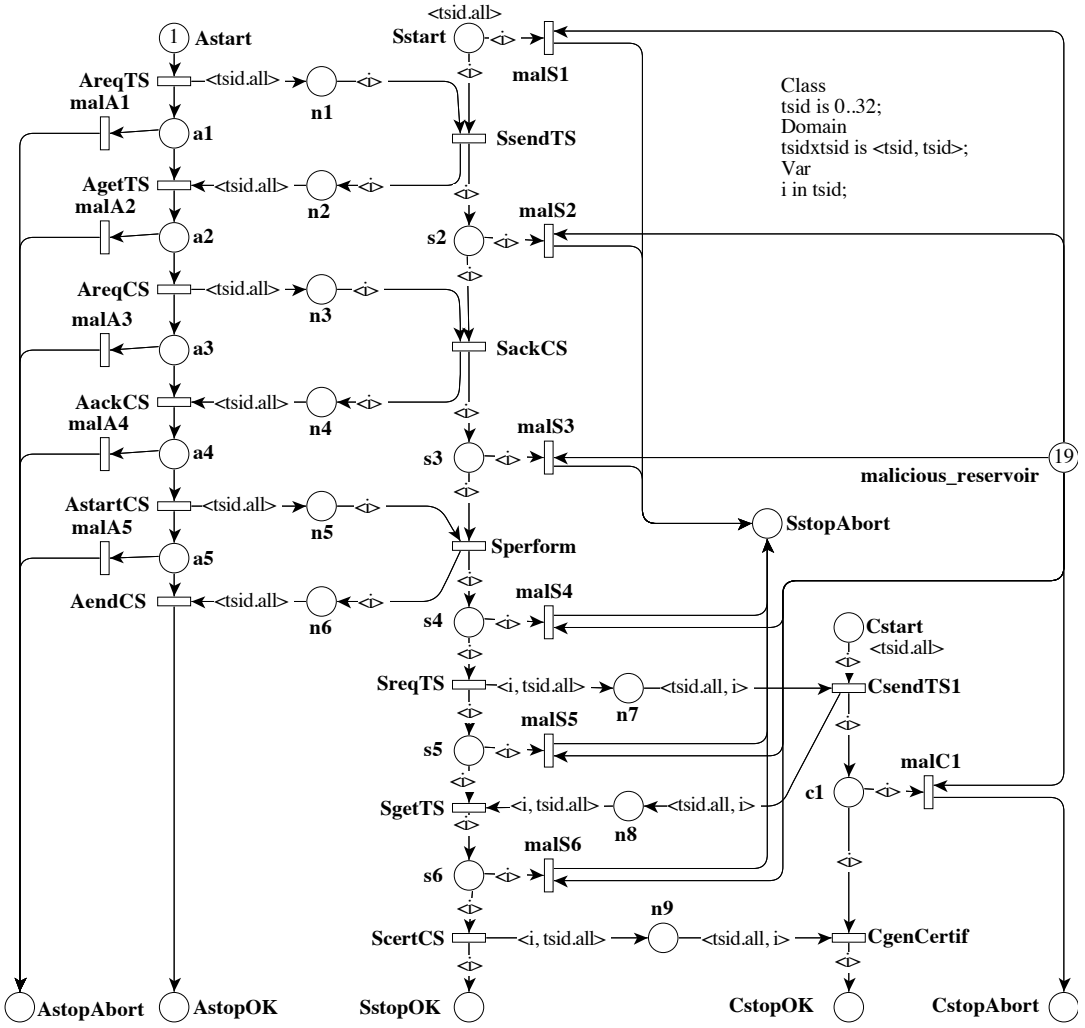
Fabrice Kordon
Fabrice.Kordon@lip6.fr

This form is a summary description of the model entitled "Quasi Certification Protocol over a DHT" 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

This Petri net models a quasi certification protocol on top of a DHT. In this protocol, an Actor A contact a server S (key $k = hash(S)$ for the corresponding root node in the DHT) to perform a service. Once S has finished, S contact C (key $k' = hash(A + S)$ for the corresponding root node in the DHT) that will certify that A did a service S at a timestamp t. To get this certificate, any X contact C for his answer.

This service relies on numerous algorithms scheduled by means of a protocol. Reliability over the DHT is ensured by replication over *"leaf sets"* of size L (we assume it is the same value for S and C). The Petri net in the Figure models this protocol where A, S and C interact. The objective is to certify that either one actor behave maliciously (i.e. does not respect the protocol) and then no certification is issued or, if all is OK, one certificate is appropriately emitted.



Graphical representation for $L = 32$

Fabrice Kordon
Fabrice.Kordon@lip6.fr

References

The QuasiCertification service is presented in: X. Bonnaire, R. Cortés, F. Kordon, O. Marin. *A Scalable Architecture for Highly Reliable Certification.* Proceedings TrustCom 2013.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
L	Size of the leaf sets for S and C	2, 6, 10, 18, 22, 28, 32

Size of the colored net model

number of places: 30
number of transitions: 26
number of arcs: 77

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
$L = 2$	86	56	223
$L = 6$	270	116	659
$L = 10$	550	176	1287
$L = 18$	1398	296	3119
$L = 22$	1966	356	4323
$L = 28$	2998	446	6489
$L = 32$	3806	506	8173

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 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[b] stated by CÆSAR.BDD version 2.6 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[c] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[d] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[e] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[f] from place "c1_0" one cannot reach place "malicious_reservoir".
[g] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32); at least "Astart" is a source place.
[h] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32); at least "AstopOK" is a sink place.
[i] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[j] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[k] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[l] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).
[m] stated by CÆSAR.BDD version 1.7 on all 7 instances (2, 6, 10, 18, 22, 28, and 32).

Fabrice Kordon
Fabrice.Kordon@lip6.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* ..... ✓ [p]
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* ..... ? [q]
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ✗ [r]

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
$L = 2$	1 029 [s]	3084 [t]	1 [u]	20 [v]
$L = 6$	2.272×10^6 [w]	1.6008E+7 [x]	1 [y]	20 [z]
$L = 10$	?	?	?	≥ 29
$L = 18$	?	?	?	≥ 49
$L = 22$	?	?	?	≥ 60
$L = 28$	?	?	?	≥ 75
$L = 32$	?	?	?	≥ 86

Other properties

P is the main property to be verified on this model. It states that, from the initial configuration of the system, all executions lead to F_{ok} or to F_{abort}.

F_{ok} corresponds to a state where a certificate has been issued. F_{abort} corresponds to the situations where something went wrong: no certificate gets emitted.

The corresponding formulæ are stated below:

$$F_{ok}: \quad |SstopOK| = L \wedge |CstopOK| = L \tag{1}$$
$$F_{abort}: \quad |SstopAbort| > 0 \vee |CstopAbort| > 0 \tag{2}$$
$$P: \quad AF(F_{ok} \vee F_{abort})) \tag{3}$$

It is expressed there in CTL but could also be expressed in LTL.

P has been proved to be true up to $L = 32$ using ITS-Tool (not as an surprise model).

[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] only safe for $L = 1$; for $L > 2$, the unfolded nets put several tokens in the same initial marking places.
[p] stated by CÆSAR.BDD version 2.0 to be true on 1 instance(s) out of 7, and unknown on the remaining 6 instance(s); confirmed at MCC'2014 by Helena on all colored instances, and by Lola and Tapaal on all P/T instances.
[q] stated by CÆSAR.BDD version 2.0 to be true on 2 instance(s) out of 7, and unknown on the remaining 5 instance(s).
[r] the net has at least one transition and its marking graph has deadlocks.
[s] computed at MCC'2013 by Alpina, ITS-Tools, Marcie, Neco, and PNXDD; confirmed by CÆSAR.BDD version 1.8; computed at MCC'2014 by GreatSPN, Marcie, PNMC, PNXDD, Stratagem, and Tapaal.
[t] computed at MCC'2014 by Marcie.
[u] computed at MCC'2014 by GreatSPN, Marcie, PNMC, and Tapaal.
[v] computed at MCC'2014 by GreatSPN, Marcie, PNMC, and Tapaal.
[w] computed at MCC'2013 by ITS-Tools and Marcie; confirmed at MCC'2014 by GreatSPN, Marcie, PNMC, PNXDD, and Tapaal.
[x] computed at MCC'2014 by Marcie.
[y] computed at MCC'2014 by GreatSPN, Marcie, PNMC, and Tapaal.
[z] computed at MCC'2014 by GreatSPN, Marcie, PNMC, and Tapaal.