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 \( k = \text{hash}(S) \) for the corresponding root node in the DHT) to perform a service. Once S has finished, S contact C (key \( k' = \text{hash}(A + S) \) 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 \( L = 32 \)
References


Scaling parameter

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter description</th>
<th>Chosen parameter values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L$</td>
<td>Size of the leaf sets for S and C</td>
<td>2, 6, 10, 18, 22, 28, 32</td>
</tr>
</tbody>
</table>

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

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

Structural properties

- **free choice** — all (different) transitions with a shared input place have no other input place ........................................... X (a)
- **state machine** — every transition has exactly one input place and exactly one output place ......................................................... X (b)
- **marked graph** — every place has exactly one input transition and exactly one output transition ............................................. X (c)
- **connected** — there is a undirected path between every two nodes (places or transitions) ......................................................... X (d)
- **strongly connected** — there is a directed path between every two nodes (places or transitions) ..................................................... X (e)
- **source place(s)** — one or more places have no input transitions ........................................................................................................... X (f)
- **sink place(s)** — one or more places have no output transitions ........................................................................................................ X (g)
- **source transition(s)** — one or more transitions have no input places ............................................................................................ X (h)
- **sink transition(s)** — one or more transitions have no output places ............................................................................................. X (i)
- **loop-free** — no transition has an input place that is also an output place .................................................................................... X (j)
- **conservative** — for each transition, the number of input arcs equals the number of output arcs ................................................. X (k)
- **subconservative** — for each transition, the number of input arcs equals or exceeds the number of output arcs .......................... X (l)

(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 1.7 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) 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.

(g) from place “c1” one cannot reach place “malicious reservoir”.

(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).
Behavioural properties

safe — in every reachable marking, there is no more than one token on a place .............................................. X (m)
deadlock — there exists a reachable marking from which no transition can be fired ......................................... √ (n)
reversible — from every reachable marking, there is a transition path going back to the initial marking ................. X (o)
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 ............ X (p)

Size of the marking graphs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Number of reachable markings</th>
<th>Number of transition firings</th>
<th>Max. number of tokens per place</th>
<th>Max. number of tokens per marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>L = 2</td>
<td>1 029 ( \in [8, 86] ) (q)</td>
<td>?</td>
<td>1</td>
<td>( \in [8, 86] ) (r)</td>
</tr>
<tr>
<td>L = 6</td>
<td>( 2,272 \times 10^6 ) (q)</td>
<td>?</td>
<td>?</td>
<td>≥ 18</td>
</tr>
<tr>
<td>L = 10</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>≥ 29</td>
</tr>
<tr>
<td>L = 18</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>≥ 49</td>
</tr>
<tr>
<td>L = 22</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>≥ 60</td>
</tr>
<tr>
<td>L = 28</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>≥ 75</td>
</tr>
<tr>
<td>L = 32</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>≥ 86</td>
</tr>
</tbody>
</table>

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 formulae are stated below:

\[
F_{ok} : |SstopOK| = L \land |CstopOK| = L \quad (1)
F_{abort} : |SstopAbort| > 0 \lor |CstopAbort| > 0 \quad (2)
P : AF(F_{ok} \lor F_{abort}) \quad (3)
\]

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).

\( (m) \) only safe for \( L = 1 \); for \( L > 2 \), the unfolded nets put several tokens in the same initial marking places.

\( (n) \) 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).

\( (o) \) 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).

\( (p) \) the net has at least one transition and its marking graph has deadlocks.

\( (q) \) computed by alpina, ITS-Tools, marcie, neco, and pnxdd at MCC’2013; confirmed by CÆSAR.BDD version 1.8.

\( (r) \) lower and upper bounds given by the number of initial tokens and the number of places.

\( (s) \) computed by ITS-Tools and marcie at MCC’2013.