Antoine Toullalan, Fabrice Kordon
Fabrice.Kordon@lip6.fr

*This form is a summary description of the model entitled "MultiCrashLeafsetExtension" 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 the extension of a LeafSet in a pastry [2] DHT (Distributed Hash Table) where nodes store data among leafset: each value is stored on a "master" node surrounded by $\frac{S}{2}$ nodes on its right and $\frac{S}{2}$ on its left ; each of them managing copies [1].

When a node in the leafset crashes, another one in the leafset detects its absence processes to the leafset extension so that the number of copies in the DHT remains constant (then, the value may be decided at a majority of $\frac{S}{2}+1$ identical copies). The model focuses on the protocol that extend the leafset when a ode is down only.

We consider the following modeling hypotheses:

- the maximum number of crashes is specified in the model,
- the crash is handled by the node which first detects the fault,
- the leafset is extended to the right or to the left, according to the position of the crashed node in the leafset,
- if the master node crashes, then the closest node to the right or to the lefts is selected to be the new master (depending on the side where the node having detected the crash is),
- when a Node manages a crash, no crash can happen until the crash is handled.

## References

1. S. Legtchenko, S. Monnet, P. Sens, and G. Muller. Churn-resilient replication strategy for peer-to- peer distributed hash-tables. In R. Guerraoui and F. Petit, editors, Stabilization, Safety, and Security of Distributed Systems, 11th International Symposium, SSS 2009, Lyon, France, November 3-6, 2009. Proceedings, volume 5873 of Lecture Notes in Computer Science, pages 485–499. Springer, 2009

2. A. I. T. Rowstron and P. Druschel. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. In R. Guerraoui, editor, Middleware 2001, IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, Germany, November 12-16, 2001, Proceedings, volume 2218 of Lecture Notes in Computer Science, pages 329–350. Springer, 2001.

## Scaling parameter

| **Parameter name** | **Parameter description** | **Chosen parameter values** |
|---|---|---|
| $S, C$ | $S$ is the size of the leafset, $C$ is the number of possible crashes | $(16,2)$, $(16,3)$, $(16,4)$, $(16,5)$, $(16,6)$, $(16,7)$, $(16,8)$, $(24,2)$, $(24,3)$, $(24,4)$, $(24,5)$, $(24,6)$, $(24,7)$, $(24,8)$, $(24,9)$, $(24,10)$, $(24,11)$, $(24,12)$, $(32,2)$, $(32,3)$, $(32,4)$, $(32,5)$, $(32,6)$, $(32,7)$, $(32,8)$, $(32,9)$, $(32,10)$, $(32,11)$, $(32,12)$ |

Antoine Toullalan, Fabrice Kordon
Fabrice.Kordon@lip6.fr

## Size of the model

| Parameter | Number of places | Number of transitions | Number of arcs |
|---|---|---|---|
| (16, 2) | 2 952 | 42 55 | 17 902 |
| (16, 3) | 3 606 | 5 141 | 20 838 |
| (16, 4) | 4 260 | 6 027 | 23 774 |
| (16, 5) | 4 914 | 6 913 | 26 710 |
| (16, 6) | 5 568 | 7 799 | 29 646 |
| (16, 7) | 6 222 | 8 685 | 32 582 |
| (16, 8) | 6 876 | 9 571 | 35 518 |
| (24, 2) | 7 032 | 10 855 | 46 214 |
| (24, 3) | 8 390 | 12 757 | 52 526 |
| (24, 4) | 9 748 | 14 659 | 58 838 |
| (24, 5) | 11 106 | 16 561 | 65 150 |
| (24, 6) | 12 464 | 18 463 | 71 462 |
| (24, 7) | 13 822 | 20 365 | 77 774 |
| (24, 8) | 15 180 | 22 267 | 84 086 |
| (24, 9) | 16 538 | 24 169 | 90 398 |
| (24, 10) | 17 896 | 26 071 | 96 710 |
| (24, 11) | 19 254 | 27 973 | 103 022 |
| (24, 12) | 20 612 | 29 875 | 109 334 |
| (32, 2) | 13 544 | 21 807 | 93 598 |
| (32, 3) | 15 862 | 25 109 | 104 566 |
| (32, 4) | 18 180 | 28 411 | 115 534 |
| (32, 5) | 20 498 | 31 713 | 126 502 |
| (32, 6) | 22 816 | 35 015 | 137 470 |
| (32, 7) | 25 134 | 38 317 | 148 438 |
| (32, 8) | 27 452 | 41 619 | 159 406 |
| (32, 9) | 29 770 | 44 921 | 170 374 |
| (32, 10) | 32 088 | 48 223 | 181 342 |
| (32, 11) | 34 406 | 51 525 | 192 310 |
| (32, 12) | 36 724 | 54 827 | 203 278 |

## 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)

(a) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(b) transitions “Node0Crash” and “Node1Crash” share a common input place “CrashReservoir”, but only the former transition has input place “Node0IsActive”.
(c) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(d) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(e) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(f) from place “CrashReservoir” one cannot reach place “Node0NotifyThatHeIsActive”.
(g) there exist 4 source places, e.g., place “CrashReservoir”.
(h) at least place “Lx0IsActiveInTheLeafSet”; confirmed by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(i) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).

Antoine Toullalan, Fabrice Kordon
Fabrice.Kordon@lip6.fr

**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* ..... ?
**dead transition(s)** — *one or more transitions cannot fire from any reachable marking* ..... ✗
**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* ..... ✗ [q]
**live** — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ✗ [r]

(j) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(k) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(l) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(m) stated by CÆSAR.BDD version 3.5 on all 29 instances (see all aforementioned parameter values).
(n) the definition of Nested-Unit Petri Nets (NUPN) is available from `http://mcc.lip6.fr/nupn.php`
(o) By construction, initial marking of place CrashReservoir $> 1$.
(p) Stated by PROD on Mai 2021 which is not a surprise, the protocol blocks in several situations corresponding to final configurations.
(q) By construction, since the model ends.
(r) By construction, since the model ends.

Antoine Toullalan, Fabrice Kordon
Fabrice.Kordon@lip6.fr


## 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 |
|---|---|---|---|---|
| (16, 2) | 33 708 (s) | 38 129 (t) | ? | ≥ 44 (u) |
| (16, 3) | 268 068 (v) | 303 607 (w) | ? | ≥ 47 (x) |
| (16, 4) | 1 341 616 (y) | 1 520 155 (z) | ? | ≥ 50 (aa) |
| (16, 5) | ? | ? | ? | ≥ 53 (ab) |
| (16, 6) | ? | ? | ? | ≥ 56 (ac) |
| (16, 7) | ? | ? | ? | ≥ 59 (ad) |
| (16, 8) | ? | ? | ? | ≥ 62 (ae) |
| (24, 2) | 108 020 (af) | 122 621 (ag) | ? | ≥ 60 (ah) |
| (24, 3) | ? | ? | ? | ≥ 63 (ai) |
| (24, 4) | ? | ? | ? | ≥ 66 (aj) |
| (24, 5) | ? | ? | ? | ≥ 69 (ak) |
| (24, 6) | ? | ? | ? | ≥ 72 (al) |
| (24, 7) | ? | ? | ? | ≥ 75 (am) |
| (24, 8) | ? | ? | ? | ≥ 78 (an) |
| (24, 9) | ? | ? | ? | ≥ 81 (ao) |
| (24, 10) | ? | ? | ? | ≥ 84 (ap) |
| (24, 11) | ? | ? | ? | ≥ 87 (aq) |
| (24, 12) | ? | ? | ? | ≥ 90 (ar) |
| (32, 2) | 249 308 (as) | 283 497 (at) | ? | ≥ 76 (au) |
| (32, 3) | ? | ? | ? | ≥ 79 (av) |
| (32, 4) | ? | ? | ? | ≥ 82 (aw) |
| (32, 5) | ? | ? | ? | ≥ 85 (ax) |
| (32, 6) | ? | ? | ? | ≥ 88 (ay) |
| (32, 7) | ? | ? | ? | ≥ 91 (az) |
| (32, 8) | ? | ? | ? | ≥ 94 (ba) |
| (32, 9) | ? | ? | ? | ≥ 97 (bb) |
| (32, 10) | ? | ? | ? | ≥ 100 (bc) |
| (32, 11) | ? | ? | ? | ≥ 103 (bd) |
| (32, 12) | ? | ? | ? | ≥ 106 (be) |

(s) Stated by PROD on May 2021.
(t) Stated by PROD on May 2021.
(u) lower bound given by the number of initial tokens.
(v) Stated by PROD on May 2021.
(w) Stated by PROD on May 2021.
(x) lower bound given by the number of initial tokens.
(y) Stated by PROD on May 2021.
(z) Stated by PROD on May 2021.
(aa) lower bound given by the number of initial tokens.
(ab) lower bound given by the number of initial tokens.
(ac) lower bound given by the number of initial tokens.
(ad) lower bound given by the number of initial tokens.
(ae) lower bound given by the number of initial tokens.
(af) Stated by PROD on May 2021.
(ag) Stated by PROD on May 2021.
(ah) lower bound given by the number of initial tokens.
(ai) lower bound given by the number of initial tokens.
(aj) lower bound given by the number of initial tokens.
(ak) lower bound given by the number of initial tokens.
(al) lower bound given by the number of initial tokens.
(am) lower bound given by the number of initial tokens.
(an) lower bound given by the number of initial tokens.
(ao) lower bound given by the number of initial tokens.
(ap) lower bound given by the number of initial tokens.
(aq) lower bound given by the number of initial tokens.
(ar) lower bound given by the number of initial tokens.

(as) Stated by PROD on May 2021.
(at) Stated by PROD on May 2021.
(au) lower bound given by the number of initial tokens.
(av) lower bound given by the number of initial tokens.
(aw) lower bound given by the number of initial tokens.
(ax) lower bound given by the number of initial tokens.
(ay) lower bound given by the number of initial tokens.
(az) lower bound given by the number of initial tokens.
(ba) lower bound given by the number of initial tokens.
(bb) lower bound given by the number of initial tokens.
(bc) lower bound given by the number of initial tokens.
(bd) lower bound given by the number of initial tokens.
(be) lower bound given by the number of initial tokens.