Model: Smart Home Automation
Type: P/T Net
Origin: Industrial (Nokia Bell Labs)

since
MCC 2020

Ajay Krishna and Hubert Garavel
ajay.muroor-nadumane@inria.fr

This form is a summary description of the model entitled "Smart Home Automation" 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.

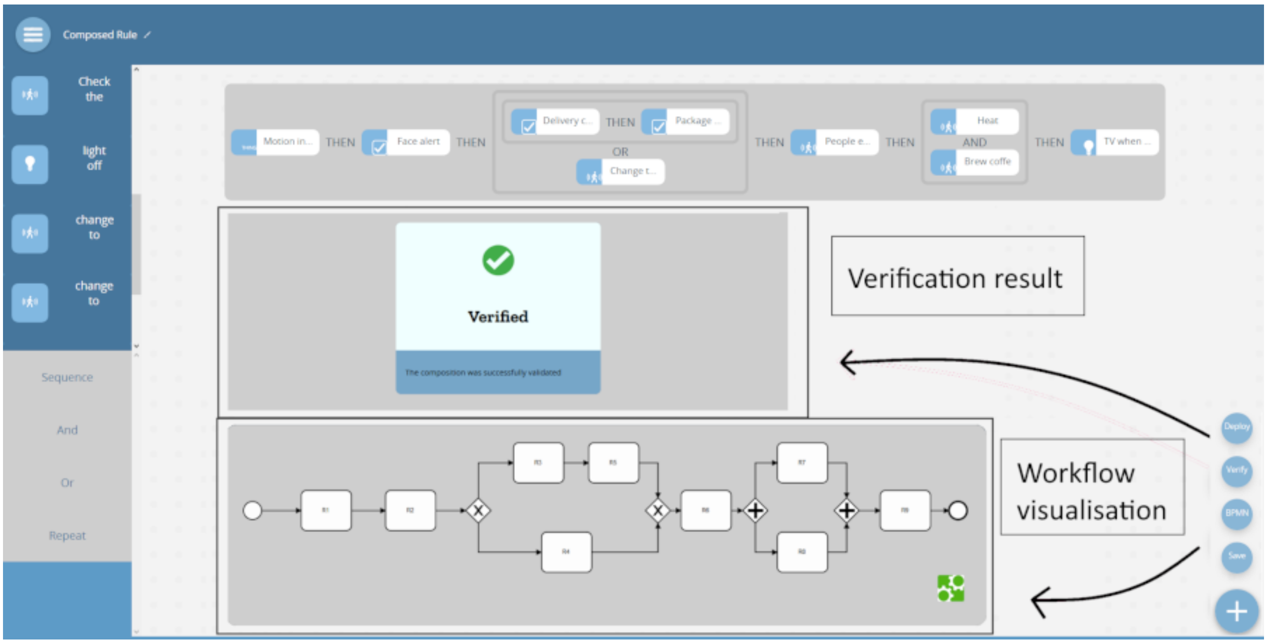
Description

Among the Internet of Things (IoT), which gathers everyday objects that communicate together using Internet, smart homes are a fast-growing area. Smart home automation is often programmed using Event-Condition-Action rules of the following form: "IF *event* THEN *action*". For instance, the rule "IF *thermostat(temperature < 19)* THEN *heater(turn_on=true)*" involves two connected objects *thermostat* and *heater*; checking whether the thermostat is below 19 degrees is the event condition, and turning on the heater is the action.

The present MCC model was obtained as part of the efforts to build a formal analysis framework for smart home automation [1]. Each instance of this model was produced from one smart home automation scenario specified using a composition of Event-Condition-Action rules. The events and actions associated to the objects, and the model of objects are based on the Web of Things (WoT) Thing Description, a standardization effort led by W3C and partners to make objects interoperable.

The instances were specified in LNT language, a modern successor of LOTOS. Each LNT specification was translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. From each LOTOS specification, 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.

Most of these NUPNs have been generated *before* applying all the structural and data-flow optimizations of the CÆSAR compiler for LOTOS; all but three of the NUPNs obtained *after* these optimizations have been discarded, because they were too small, thus not challenging enough for the MCC.



Analysis framework for smart home automation

References

Ajay Krishna, Michel Le Pallec, Alejandro Martinez, Radu Mateescu, and Gwen Salaün. *MOZART: Design and Deployment of Advanced IoT Applications*. In Companion Proceedings of the Web Conference 2020 (WWW '20), Taipei, Taiwan, ACM, New York, USA, pp. 163–166, April 2020. DOI: https://doi.org/10.1145/3366424.3383532

Ajay Krishna and Hubert Garavel
ajay.muroor-nadumane@inria.fr

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	N is the number of the instance (instances are sorted by increasing numbers of places)	$1 \cdots 19$

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 1$	38	113	321	21	4–18–33
$N = 2$	41	127	359	23	4–20–36
$N = 3$	45	145	405	25	4–22–39
$N = 4$	139	159	361	13	5–7–32
$N = 5$	213	245	557	19	7–10–49
$N = 6$	219	254	581	17	7–9–46
$N = 7$	251	290	658	19	8–10–52
$N = 8$	252	291	664	21	8–11–55
$N = 9$	253	293	664	19	8–10–52
$N = 10$	273	308	699	23	8–13–61
$N = 11$	290	315	722	27	8–15–69
$N = 12$	376	399	909	33	9–19–85
$N = 13$	385	407	935	35	9–21–89
$N = 14$	422	448	1026	37	10–22–95
$N = 15$	427	451	1038	39	10–24–101
$N = 16$	499	533	1222	45	12–27–118
$N = 17$	571	617	1410	49	14–29–130
$N = 18$	653	706	1618	57	16–34–153
$N = 19$	741	809	1844	61	18–36–166

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)]

[(a)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(b)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(c)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(d)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(e)] stated by CÆSAR.BDD version 3.3 to be true on 10 instance(s) out of 19, and false on the remaining 9 instance(s).
[(f)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(g)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(h)] stated by CÆSAR.BDD version 3.3 to be true on 11 instance(s) out of 19, and false on the remaining 8 instance(s).
[(i)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(j)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
[(k)] stated by CÆSAR.BDD version 3.3 to be true on 16 instance(s) out of 19, and false on the remaining 3 instance(s).
[(l)] stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).

Ajay Krishna and Hubert Garavel
ajay.muroor-nadumane@inria.fr

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* .... ? [(r)]
reversible — *from every reachable marking, there is a transition path going back to the initial marking* .... ? [(s)]
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* .... ? [(t)]

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
$N = 1$	43201 [(u)]	?	1	18
$N = 2$	86401 [(v)]	?	1	20
$N = 3$	259201 [(w)]	?	1	22
$N = 4$	5.30768e+06 [(x)]	?	1	∈ [6, 7] [(y)]
$N = 5$	1.97063e+10 [(z)]	?	1	∈ [8, 10] [(aa)]
$N = 6$	1.50828e+10 [(ab)]	?	1	∈ [8, 9] [(ac)]
$N = 7$	3.41149e+11 [(ad)]	?	1	∈ [9, 10] [(ae)]
$N = 8$	8.06569e+11 [(af)]	?	1	∈ [9, 11] [(ag)]
$N = 9$	3.94082e+11 [(ah)]	?	1	∈ [9, 10] [(ai)]
$N = 10$	4.30089e+11 [(aj)]	?	1	∈ [9, 13] [(ak)]
$N = 11$	1.91042e+12 [(al)]	?	1	∈ [9, 15] [(am)]
$N = 12$	1.12986e+14 [(an)]	?	1	∈ [10, 19] [(ao)]
$N = 13$	1.12986e+14 [(ap)]	?	1	∈ [10, 21] [(aq)]
$N = 14$	≥ 2.37036e+15 [(ar)]	?	1 [(as)]	∈ [11, 22] [(at)]
$N = 15$	≥ 2.30393e+15 [(au)]	?	1 [(av)]	∈ [11, 24] [(aw)]
$N = 16$	≥ 5.85388e+17 [(ax)]	?	1 [(ay)]	∈ [13, 27] [(az)]
$N = 17$	≥ 3.6238e+19 [(ba)]	?	1 [(bb)]	∈ [15, 29] [(bc)]
$N = 18$	≥ 2.04925e+22 [(bd)]	?	1 [(be)]	∈ [17, 34] [(bf)]
$N = 19$	≥ 2.49735e+24 [(bg)]	?	1 [(bh)]	∈ [19, 36] [(bi)]

(m) stated by CÆSAR.BDD version 3.3 on all 19 instances (19 values of N).
(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 3.3 to be true on 16 instance(s) out of 19, and false on the remaining 3 instance(s).
(q) stated by CÆSAR.BDD version 3.3 to be true on 16 instance(s) out of 19, and false on the remaining 3 instance(s).
(r) stated by CÆSAR.BDD version 3.3 to be true on 10 instance(s) out of 19, false on the remaining 3 instance(s), and unknown on the remaining 6 instance(s).
(s) stated by CÆSAR.BDD version 3.3 to be false on 10 instance(s) out of 19, and unknown on the remaining 9 instance(s).
(t) stated by CÆSAR.BDD version 3.3 to be false on 16 instance(s) out of 19, and unknown on the remaining 3 instance(s).
(u) stated by CÆSAR.BDD version 3.3.
(v) stated by CÆSAR.BDD version 3.3.
(w) stated by CÆSAR.BDD version 3.3.
(x) stated by CÆSAR.BDD version 3.3.
(y) upper bound given by the number of leaf units.
(z) stated by CÆSAR.BDD version 3.3.
(aa) upper bound given by the number of leaf units.
(ab) stated by CÆSAR.BDD version 3.3.
(ac) upper bound given by the number of leaf units.
(ad) stated by CÆSAR.BDD version 3.3.
(ae) upper bound given by the number of leaf units.
(af) stated by CÆSAR.BDD version 3.3.

(ag) upper bound given by the number of leaf units.
(ah) stated by CÆSAR.BDD version 3.3.
(ai) upper bound given by the number of leaf units.
(aj) stated by CÆSAR.BDD version 3.3.
(ak) upper bound given by the number of leaf units.
(al) stated by CÆSAR.BDD version 3.3.
(am) upper bound given by the number of leaf units.
(an) stated by CÆSAR.BDD version 3.3.
(ao) upper bound given by the number of leaf units.
(ap) stated by CÆSAR.BDD version 3.3.
(aq) upper bound given by the number of leaf units.
(ar) stated by CÆSAR.BDD version 3.3.
(as) stated by the CÆSAR compiler.
(at) upper bound given by the number of leaf units.
(au) stated by CÆSAR.BDD version 3.3.
(av) stated by the CÆSAR compiler.
(aw) upper bound given by the number of leaf units.
(ax) stated by CÆSAR.BDD version 3.3.
(ay) stated by the CÆSAR compiler.
(az) upper bound given by the number of leaf units.
(ba) stated by CÆSAR.BDD version 3.3.
(bb) stated by the CÆSAR compiler.
(bc) upper bound given by the number of leaf units.
(bd) stated by CÆSAR.BDD version 3.3.
(be) stated by the CÆSAR compiler.
(bf) upper bound given by the number of leaf units.
(bg) stated by CÆSAR.BDD version 3.3.
(bh) stated by the CÆSAR compiler.
(bi) upper bound given by the number of leaf units.