De Wulf, Martin; **Doyen, Laurent**; **Markey, Nicolas**; **Raskin, Jean-François**
Robust safety of timed automata. (English) Zbl 1165.68392
Form. Methods Syst. Des. 33, No. 1-3, 45-84 (2008).

Summary: Timed automata are governed by an idealized semantics that assumes a perfectly precise behavior of the clocks. The traditional semantics is not robust because the slightest perturbation in the timing of actions may lead to completely different behaviors of the automaton. Following several recent works, we consider a relaxation of this semantics, in which guards on transitions are widened by $\Delta > 0$ and clocks can drift by $\epsilon > 0$. The relaxed semantics encompasses the imprecisions that are inevitably present in an implementation of a timed automaton, due to the finite precision of digital clocks.

We solve the safety verification problem for this robust semantics: given a timed automaton and a set of bad states, our algorithm decides if there exist positive values for the parameters Δ and ϵ such that the timed automaton never enters the bad states under the relaxed semantics.

MSC:

68Q45 Formal languages and automata

Keywords:

timed automaton; robustness; implementability; perturbation; drift

Software:

Uppaal

Full Text: DOI

References:

[1] Annichini A, Asarin E, Bouajjani A (2000) Symbolic techniques for parametric reasoning about counter and clock systems. In: Proc 12th int conf computer aided verification (CAV 2000), pp 419–434 · Zbl 0974.68523

[2] Asarin E, Bouajjani A (2001) Perturbed Turing machines and hybrid systems. In: Proc 16th annual symposium on logic in computer science (LICS). IEEE Comput Soc, Los Alamitos, pp 269–278

[3] Alur R, Courcoubetis C, Dill DL, Halbwachs N, Wong-Toi H (1992) An implementation of three algorithms for timing verification based on automata emptiness. In: Proc 13th IEEE real-time systems symposium. IEEE Comput Soc, Los Alamitos, pp 157–166

[4] Alur R, Dill DL (1994) A theory of timed automata. Theor Comput Sci 126(2):183–235 · Zbl 0803.68071 · doi:10.1016/0304-3975(94)90010-8

[5] Amnell T, Fersman E, Mokrushin L, Pettersson P, Yi W (2002) Times: A tool for modelling and implementation of embedded systems. In: Katoen J-P, Stevens P (eds) Proc 8th int conference tools and algorithms for the construction and analysis of systems (TACAS'02). Lecture notes in computer science, vol 2280. Springer, Berlin, pp 460–464 · Zbl 1043.68513

[6] Amnell T, Fersman E, Pettersson P, Sun H, Yi W (2003) Code synthesis for timed automata. Nord J Comput 9 · Zbl 1088.68625

[7] Alur R, Ivancic F, Kim J, Lee I, Sokolsky O (2003) Generating embedded software from hierarchical hybrid models. In: Proc 2003 conf languages, compilers, and tools for embedded systems (LCTES'03), pp 171–182

[8] Alur R, La Torre S, Madhusudan P (2005) Perturbed timed automata. In: Proc 8th int workshop hybrid systems: computation and control (HSCC'05). Lecture notes in computer science, vol 3414. Springer, Berlin, pp 70–85 · Zbl 1078.68070

[9] Asarin E, Maler O, Pnueli A, Sifakis J (1998) Controller synthesis for timed automata. In: Proc system structure and control. Elsevier, Amsterdam · Zbl 0933.94045

[10] Agrawal M, Thiagarajan PS (2004) Lazy rectangular hybrid automata. In: Proc of HSCC 04: Hybrid systems–computation and control. Lecture notes in computer science, vol 2993. Springer, Berlin, pp 1–15

[11] Altisen K, Tripakis S (2005) Implementation of timed automata: an issue of semantics or modeling? In: Proc 3rd int conf formal modelling and analysis of timed systems (FORMATS'05). Lecture notes in computer science. Springer, Berlin · Zbl 1175.68240

[12] Bouyer P, Chevalier F (2005) On conciseness of extensions of timed automata. J Autom Lang Comb 10(4):393–405 · Zbl

1146.68384

[13] Behrmann G, David A, Larsen KG, Håkansson J, Pettersson P, Yi W, Hendriks M (2006) Uppaal 4.0. In: QEST, pp 125–126

[14] Berthomieu B, Menasche M (1983) An enumerative approach for analyzing time Petri nets. In: Mason REA (ed) Information processing 83–Proceedings of the 9th IFIP world computer congress, September 1983. North-Holland/IFIP, pp 41–46

[15] Bouyer P, Markey N, Reynier P-A (2006) Robust model-checking of linear-time properties in timed automata. In: Correa JR, Hevia A, Kiwi M (eds) Proceedings of the 7th Latin American symposium on theoretical informatics (LATIN'06). Lecture Notes in Computer Science, vol 3887. Springer, Berlin, pp 238–249 · Zbl 1145.68464

[16] Bouyer P, Markey N, Reynier P-A (2008) Robust analysis of timed automata via channel machines. In: Amadio R (ed) Proceedings of the 11th international conference on foundations of software science and computation structures (FoSSaCS'08), Budapest, Hungary, March–April 2008. Lecture notes in computer science, vol 4962. Springer, Berlin, pp 157–171 · Zbl 1138.68431

[17] Clarke E, Grumberg O, Peled D (1999) Model checking. MIT Press, Cambridge

[18] Chaochen Z, Hoare CAR, Ravn AP (1991) A calculus of durations. Inf Process Lett 40(5):269–276 · Zbl 0743.68097 · doi:10.1016/0020-0190(91)90122-X

[19] Cassez F, Henzinger TA, Raskin J-F (2002) A comparison of control problems for timed and hybrid systems. In: Proc 5th int workshop hybrid systems: computation and control (HSCC'02). Lecture notes in computer science, vol 2289. Springer, Berlin, pp 134–148 · Zbl 1044.93518

[20] Chaochen Z, Hansen MR, Sestoft P (1993) Decidability and undecidability results for duration calculus. In: In proc of STACS 93: symposium on theoretical aspects of computer science. Lecture notes in computer science, vol 665. Springer, Berlin, pp 58–68 · Zbl 0811.68115

[21] Courcoubetis C, Yannakakis M (1991) Minimum and maximum delay problems in real-time systems. In: Proc 3rd int workshop computer aided verification (CAV'91). Lecture notes in computer science, vol 575. Springer, Berlin, pp 399–409 · Zbl 0777.68045

[22] De Wulf M, Doyen L, Markey N, Raskin J-F (2004) Robustness and implementability of timed automata. In: Lakhnech Y, Yovine S (eds) Proceedings of the joint conferences formal modelling and analysis of timed systems (FORMATS'04) and formal techniques in real-time and fault-tolerant systems (FTRTFT'04), Grenoble, France, September 2004. Lecture notes in computer science, vol 3253. Springer, Berlin, pp 118–133

[23] De Wulf M, Doyen L, Raskin J-F (2005) Almost ASAP semantics: from timed models to timed implementations. Form Asp Comput 17(3):319–341 · Zbl 1101.68670 · doi:10.1007/s00165-005-0067-8

[24] Dierks H (1999) Specification and verification of polling real-time systems. PhD thesis, University of Oldenburg · Zbl 0953.68087

[25] Dierks H (2001) PLC-automata: a new class of implementable real-time automata. Theor Comput Sci 253(1):61–93 · Zbl 0954.68085 · doi:10.1016/S0304-3975(00)00089-X

[26] Dill D (1990) Timing assumptions and verification of finite-state concurrent systems. In: Proc 1st int workshop automatic verification methods for finite state systems (CAV'89). Lecture notes in computer science, vol 407. Springer, Berlin, pp 197–212

[27] Dima C (2007) Dynamical properties of timed automata revisited. In: Proc of FORMATS 07: formal modeling and analysis of timed systems. Lecture notes in computer science, vol 4763. Springer, Berlin, pp 130–146 · Zbl 1142.68040

[28] Daws C, Kordy P (2006) Symbolic robustness analysis of timed automata. In: Proc of FORMATS 06: formal modeling and analysis of timed systems. Lecture notes in computer science, vol 4202. Springer, Berlin, pp 143–155 · Zbl 1141.68429

[29] Fränzle M (1999) Analysis of hybrid systems: an ounce of realism can save an infinity of states. In: CSL. Lecture notes in computer science, vol 1683. Springer, Berlin, pp 126–140 · Zbl 0944.68119

[30] Gupta V, Henzinger TA, Jagadeesan R (1997) Robust timed automata. In: Maler O (ed) Proc int workshop hybrid and real-time systems (HART'97). Lecture notes in computer science, vol 1201. Springer, Berlin, pp 331–345

[31] Henzinger TA, Kirsch CM, Sanvido MA, Pree W (2003) From control models to real-time code using giotto. IEEE Control Syst Mag 23(1):50–64 · doi:10.1109/MCS.2003.1172829

[32] Henzinger TA, Nicollin X, Sifakis J, Yovine S (1992) Symbolic model checking for real-time systems. In: Proc 7th annual symposium logic in computer science (LICS'92). IEEE Comput Soc, Los Alamitos, pp 394–406 · Zbl 0806.68080

[33] Hune T, Romijn J, Stoelinga M, Vaandrager FW (2001) Linear parametric model checking of timed automata. In: Proc 7th int conf tools and algorithms for construction and analysis of systems (TACAS'01), pp 189–203 · Zbl 0978.68094

[34] Milner R (1980) A calculus of communicating systems. Lecture notes in computer science, vol 92. Springer, Berlin · Zbl 0452.68027

[35] Maler O, Pnueli A, Sifakis J (1995) On the synthesis of discrete controllers for timed systems (an extended abstract). In: STACS, pp 229–242 · Zbl 1379.68227

[36] Puri A (1998) Dynamical properties of timed automata. In: Proc 5th int symposium formal techniques in real-time and fault-tolerant systems (FTRTFT'98). Lecture notes in computer science, vol 1486. Springer, Berlin, pp 210–227

[37] Puri A (2000) Dynamical properties of timed automata. Discrete Event Dyn Syst 10(1–2):87–113 · Zbl 0986.93042 · doi:10.1023/A:1008387132377

[38] Swaminathan M, Fränzle M (2007) A symbolic decision procedure for robust safety of timed systems. In: Proceedings of the 14th international symposium on temporal representation and reasoning (TIME'07). IEEE Comput Soc, Los Alamitos, p 192

[39] Yovine S (1996) Model checking timed automata. In: European educational forum: school on embedded systems, pp 114–152