Lanotte, Ruggero; **Maggiolo-Schettini, Andrea**; **Troina, Angelo**
Weak bisimulation for probabilistic timed automata. (English) Zbl 1208.68160
Theor. Comput. Sci. 411, No. 50, 4291-4322 (2010).

Summary: We are interested in describing timed systems that exhibit probabilistic behaviour. To this purpose, we consider a model of probabilistic timed automata and introduce a concept of weak bisimulation for these automata, together with an algorithm to decide it. The weak bisimulation relation is shown to be preserved when either time, or probability is abstracted away. As an application, we use weak bisimulation for probabilistic timed automata to model and analyze a timing attack on the dining cryptographers protocol.

MSC:

68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)
68Q45 Formal languages and automata

Keywords:

probabilistic timed automata; weak bisimulation

Full Text: DOI

References:

[1] Aldini, A.; Bravetti, M.; Gorrieri, R., A process-algebraic approach for the analysis of probabilistic non-interference, Journal of computer security, 12, 191-245, (2004)

[2] Alur, R.; Courcoubetis, C.; Dill, D.L., Verifying automata specifications of probabilistic real-time systems, (), 28-44

[3] Alur, R.; Dill, D.L., A theory of timed automata, Theoretical computer science, 126, 183-235, (1994) · Zbl 0803.68071

[4] Andersen, J.H.; Kristoffersen, K.J.; Larsen, K.G.; Niedermann, J., Automatic synthesis of real time systems, (), 535-546 · Zbl 1412.68136

[5] Andersen, H.H.; Mendler, M., An asynchronous process algebra with multiple clocks, ()

[6] Asarin, E.; Maler, O.; Pnueli, A., On discretization of delays in timed automata and digital circuits, (), 470-484 · Zbl 0933.94045

[7] Baier, C.; Hermanns, H., Weak bisimulation for fully probabilistic processes, (), 119-130

[8] C. Baier, On algorithmic verification methods for probabilistic systems, Habilitation Thesis, Univ. Mannheim, 1998.

[9] Bellman, R.E., Dynamic programming, (1957), Princeton University Press

[10] Bernardo, M.; Gorrieri, R., A tutorial on EMPA: a theory of concurrent processes with nondeterminism, priorities, probabilities and time, Theoretical computer science, 202, 1-54, (1998) · Zbl 0902.68075

[11] Beauquier, D., On probabilistic timed automata, Theoretical computer science, 292, 65-84, (2003) · Zbl 1064.68063

[12] Bouyer, P., Forward analysis of updatable timed automata, Formal methods in system design, 24, 281-320, (2004) · Zbl 1073.68041

[13] van Breugel, F.; Worrel, J., Towards quantitative verification of probabilistic systems (extended abstract), (), 421-432 · Zbl 0986.68093

[14] Brumley, D.; Boneh, D., Remote timing attacks are practical, The international journal of computer and telecommunications networking, 48, 701-716, (2005)

[15] Cattani, S.; Segala, R., Decision algorithm for probabilistic bisimulation, (), 371-385 · Zbl 1012.68127

[16] Chatzikokolakis, K.; Norman, G.; Parker, D., Bisimulation for demonic schedulers, (), 318-332 · Zbl 1234.68293

[17] Chatzikokolakis, K.; Palamidessi, C., Probable innocence revisited, Theoretical computer science, 367, 123-138, (2006) · Zbl 1153.94451

[18] Chatzikokolakis, K.; Palamidessi, C., Making random choices invisible to the scheduler, (), 42-58 · Zbl 1151.68517

[19] Chaum, D., The dining cryptographers problem: unconditional sender and recipient untraceability, Journal of cryptology, 1, 65-75, (1988) · Zbl 0654.94012

[20] Cerans, K., Decidability of bisimulation equivalences for parallel timer processes, (), 302-315

[21] D'Argenio, P.R.; Hermanns, H.; Katoen, J.-P., On generative parallel composition, (), 30-54

[22] Desharnais, J.; Gupta, V.; Jagadeesan, R.; Panangaden, P., The metric analogue of weak bisimulation for probabilistic processes, ()

[23] Desharnis, J.; Gupta, V.; Jagadeesan, R.; Panangaden, P., Metrics for labelled Markov processes, Theoretical computer science, 318, 323-354, (2004) · Zbl 1068.68093

[24] Focardi, R.; Gorrieri, R., A classification of security properties, Journal of computer security, 3, 5-33, (1995)

[25] Halmos, P.R., Measure theory, (1950), Springer-Verlag · Zbl 0117.10502

[26] Henzinger, T.A.; Nicollin, X.; Sifakis, J.; Yovine, S., Symbolic model checking for real-time systems, Information and computation, 111, 193-244, (1994) · Zbl 0806.68080

[27] Hermanns, H.; Herzog, U.; Mertsiotakis, V., Stochastic process algebras — between lotos and Markov chains, Computer networks and ISDN systems, 30, 901-924, (1998)

[28] Hermanns, H.; Stegle, M., Bisimulation algorithms for stochastic process algebras and their BDD-based implementation, (), 244-264

[29] Hillston, J., A compositional approach to performance modelling, (1996), Cambridge University Press

[30] Howard, H., Dynamic programming and Markov processes, (1960), MIT Press · Zbl 0091.16001

[31] H.E. Jensen, H. Gregersen, Formal design of reliable real time systems, Master's Thesis, Aalborg University, 1995.

[32] H.E. Jensen, Model checking probabilistic real time systems, in: Proc. of the 7th Nordic Work. on Progr. Theory, Institute of Technology, 1996, pp. 247-261.

[33] Kanellakis, P.C.; Smolka, S.A., CCS expressions, finite state processes, and three problems of equivalence, Information and computation, 86, 43-68, (1990) · Zbl 0705.68063

[34] Kocher, P.C., Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems, (), 104-113 · Zbl 1329.94070

[35] Kwiatkowska, M.; Norman, G.; Segala, R.; Sproston, J., Automatic verification of real-time systems with discrete probability distribution, Theoretical computer science, 282, 101-150, (2002) · Zbl 1050.68094

[36] Kwiatkowska, M.; Norman, G.; Sproston, J., Symbolic model checking for probabilistic timed automata, (), 293-308 · Zbl 1109.68517

[37] R. Lanotte, D. Beauquier, A decidable probability logic for timed probabilistic systems, CoRR, cs.LO/0411100, 2004. · Zbl 1198.68169

[38] Lanotte, R.; Maggiolo-Schettini, A.; Troina, A., Weak bisimulation for probabilistic timed automata and applications to security, (), 34-43

[39] Lanotte, R.; Maggiolo-Schettini, A.; Troina, A., A classification of time and/or probability dependent security properties, (), 177-193

[40] Lanotte, R.; Maggiolo-Schettini, A.; Troina, A., Reachability results for timed automata with unbounded data structures, Acta informatica, 47, 279-311, (2010) · Zbl 1214.68199

[41] Lanotte, R.; Maggiolo-Schettini, A.; Milazzo, P.; Troina, A., Design and verification of long-running transactions in a timed framework, Science of computer programming, 73, 76-94, (2008) · Zbl 1170.68024

[42] Lanotte, R.; Maggiolo-Schettini, A.; Troina, A., Time and probability-based information flow analysis, IEEE transactions on software engineering, 36, 719-734, (2010)

[43] Larsen, K.G.; Skou, A., Bisimulation through probabilistic testing, Information and computation, 94, 1-28, (1991) · Zbl 0756.68035

[44] Larsen, K.G.; Wang, Y., Time abstracted bisimulation: implicit specifications and decidability, Information and computation, 134, 75-101, (1997) · Zbl 0887.68068

[45] Lynch, N.A.; Vaandrager, F.W., Forward and backward simulations, II: timing-based systems, Information and computation, 128, 1-25, (1996) · Zbl 0856.68103

[46] Milner, R., Communication and concurrency, (1989), Prentice Hall · Zbl 0683.68008

[47] Nicollin, X.; Sifakis, J.; Yovine, S., From ATP to timed graphs and hybrid systems, Acta informatica, 30, 181-202, (1993) · Zbl 0790.68067

[48] Paige, R.; Tarjan, R.E., Three partition refinement algorithms, SIAM journal on computing, 16, 973-989, (1987) · Zbl 0654.68072

[49] Philippou, A.; Lee, I.; Sokolsky, O., Weak bisimulation for probabilistic systems, (), 334-349 · Zbl 0999.68146

[50] PRISM Model Checker. Web site: http://www.cs.bham.ac.uk/dxp/prism.

[51] Reiter, M.K.; Rubin, A.D., Crowds: anonimity for web transactions, ACM transactions on information and system security, 1, 66-92, (1998)

[52] Ryan, P.; Schneider, S., Process algebra and non-interference, (), 214-227

[53] R. Segala, Modeling and verification of randomized distributed real-time systems, Ph.D. Thesis, MIT, Laboratory for Computer Science, 1995.

[54] Sokolova, A.; de Vink, E.P., Probabilistic automata: system types, parallel composition and comparison, (), 1-43 · Zbl 1203.68089

[55] Sproston, J.; Troina, A., Simulation and bisimulation for probabilistic timed automata, (), 213-227 · Zbl 1290.68081

[56] M. Stoelinga, Alea jacta est: verification of probabilistic, real-time and parametric systems, Ph.D. Thesis, University of

Nijmegen, the Netherlands, 2002.

[57] Wang, Y., Real-time behaviour of asynchronous agents, ()