Bérard, Béatrice; **Kouchnarenko, Olga**; **Mullins, John**; **Sassolas, Mathieu**
Opacity for linear constraint Markov chains. (English) Zbl 1384.93137
Discrete Event Dyn. Syst. 28, No. 1, 83-108 (2018).

Summary: On a partially observed system, a secret φ is opaque if an observer cannot ascertain that its trace belongs to φ. We consider specifications given as Constraint Markov Chains (CMC), which are underspecified Markov chains where probabilities on edges are required to belong to some set. The nondeterminism is resolved by a scheduler, and opacity on this model is defined as a worst case measure over all implementations obtained by scheduling. This measures the information obtained by a passive observer when the system is controlled by the smartest scheduler in coalition with the observer. When restricting to the subclass of linear CMC, we compute (or approximate) this measure and prove that refinement of a specification can only improve opacity.

MSC:

93E03 Stochastic systems in control theory (general)
60H10 Stochastic ordinary differential equations (aspects of stochastic analysis)
93C05 Linear systems in control theory

Keywords:

opacity; Markov models; specification; refinement

Full Text: DOI

References:

[1] Alur R, Černý P, Zdancewic S (2006) Preserving secrecy under refinement. In: Proc. ICALP'06, LNCS, vol 4052. Springer, pp 107-118 · Zbl 1133.94307

[2] Baier C, Katoen JP (2008) Principles of model checking (representation and mind series). The MIT Press · Zbl 1361.68117

[3] Baier, C; Katoen, JP; Hermanns, H; Wolf, V, Comparative branching-time semantics for Markov chains, Inf Comput, 200, 149-214, (2005) · Zbl 1101.68053

[4] Benedikt M, Lenhardt R, Worrell J (2013) LTL model checking of interval Markov chains. In: Proc. TACAS'13, LNCS, vol 7795. Springer, pp 32-46 · Zbl 1381.68147

[5] Bérard B, Mullins J, Sassolas M (2010) Quantifying opacity. In: Ciardo G, Segala R (eds) Proc. QEST'10. IEEE Computer Society, pp 263-272 · Zbl 1361.68117

[6] Bérard, B; Chatterjee, K; Sznajder, N, Probabilistic opacity for Markov decision processes, Inf Process Lett, 115, 52-59, (2015) · Zbl 1366.68213

[7] Bérard, B; Mullins, J; Sassolas, M, Quantifying opacity, Math Struct Comput Sci, 25, 361-403, (2015) · Zbl 1361.68117

[8] Bérard B, Kouchnarenko O, Mullins J, Sassolas M (2016) Preserving opacity on interval Markov chains under simulation. In: Cassandras CG, Giua A, Li Z (eds) Proceedings of 13th international workshop on discrete event systems, WODES'16. IEEE, pp 319-324 · Zbl 1360.68570

[9] Bhargava M, Palamidessi C (2005) Probabilistic anonymity. In: Abadi M, de Alfaro L (eds) Proc. CONCUR'05, LNCS, vol 3653, pp 171-185 · Zbl 1134.68426

[10] Billingsley P (1995) Probability and measure, 3rd edn. Wiley · Zbl 0822.60002

[11] Biondi, F; Legay, A; Nielsen, BF; Wąsowski, A, Maximizing entropy over Markov processes, J Logic Algebr Methods Programm, 83, 384-399, (2014) · Zbl 1371.68175

[12] Bryans, JW; Koutny, M; Mazaré, L; Ryan, PYA, Opacity generalised to transition systems, Int J Inf Secur, 7, 421-435, (2008)

[13] Caillaud, B; Delahaye, B; Larsen, KG; Legay, A; Pedersen, ML; Wasowski, A, Constraint Markov chains, Theor Comput Sci, 412, 4373-4404, (2011) · Zbl 1223.68070

[14] Chatterjee K, Henzinger T, Sen K (2008) Model-checking omega-regular properties of interval Markov chains. In Amadio RM (ed) Proc. FoSSaCS'08, pp 302-317 · Zbl 1138.68441

[15] Chaum, D, The dining cryptographers problem: unconditional sender and recipient untraceability, J Cryptol, 1, 65-75, (1988) · Zbl 0654.94012

[16] Clarkson, MR; Schneider, FB, Hyperproperties, J Comput Secur, 18, 1157-1210, (2010)

[17] Delahaye B (2015) Consistency for parametric interval Markov chains. In: André É, Frehse G (eds) Proc SynCoP'15, OASICS, vol 44. Schloss Dagstuhl - LZI, pp 17-32

[18] Jonsson B, Larsen KG (1991) Specification and refinement of probabilistic processes. In: Proceedings LICS'91. IEEE Computer Society, , pp 266-277

[19] Mazaré L. (2005) Decidability of opacity with non-atomic keys. In: Proceedings FAST'04, international federation for information processing, vol 173. Springer, pp 71-84

[20] Piterman N (2007) From nondeterministic Büchi and Streett automata to deterministic parity automata. Logic Methods Comput Sci 3(3) · Zbl 1125.68067

[21] Roos C, Terlaky T, Vial JP (1997) Theory and algorithms for linear optimization. An interior point approach. John Wiley \& Sons Ltd, Wiley-Interscience · Zbl 0954.65041

[22] Saboori, A; Hadjicostis, CN, Current-state opacity formulations in probabilistic finite automata, IEEE Trans Autom Control, 59, 120-133, (2014) · Zbl 1360.68570

[23] Segala R (1995) Modeling and verification of randomized distributed real-time systems. Ph.D. thesis, MIT Department of Electrical Engineering and Computer Science

[24] Sen K, Viswanathan M, Agha G (2006) Model-checking Markov chains in the presence of uncertainties. In: Hermanns H, Palsberg J (eds) Proceedings of 12th international conference on tools and algorithms for the construction and analysis of systems, TACAS'06, LNCS, vol 3920. Springer, pp 394-410 · Zbl 1180.68179

[25] Vardi MY (1985) Automatic verification of probabilistic concurrent finite-state programs. In: Proceedings 26th annual symposium on foundations of computer science (FOCS'85). IEEE Computer Society, pp 327-338 · Zbl 1371.68175