Biondi, Fabrizio; **Legay, Axel**; **Nielsen, Bo Friis**; **Wąsowski, Andrzej**
Maximizing entropy over Markov processes. (English) Zbl 1371.68175
J. Log. Algebr. Methods Program. 83, No. 5-6, 384-399 (2014).

Summary: The channel capacity of a deterministic system with confidential data is an upper bound on the amount of bits of data an attacker can learn from the system. We encode all possible attacks to a system using a probabilistic specification, an Interval Markov Chain. Then the channel capacity computation reduces to finding a model of a specification with highest entropy.

Entropy maximization for probabilistic process specifications has not been studied before, even though it is well known in Bayesian inference for discrete distributions. We give a characterization of global entropy of a process as a reward function, a polynomial algorithm to verify the existence of a system maximizing entropy among those respecting a specification, a procedure for the maximization of reward functions over Interval Markov Chains and its application to synthesize an implementation maximizing entropy.

We show how to use Interval Markov Chains to model abstractions of deterministic systems with confidential data, and use the above results to compute their channel capacity. These results are a foundation for ongoing work on computing channel capacity for abstractions of programs derived from code.

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)
68Q87 Probability in computer science (algorithm analysis, random structures, phase transitions, etc.)

Full Text: DOI

References:

[1] Goguen, J. A.; Meseguer, J., Security policies and security models, (IEEE Symposium on Security and Privacy, (1982)), 11-20

[2] Ryan, P.; McLean, J.; Millen, J.; Gligor, V., Non-interference, who needs it?, (14th IEEE Computer Security Foundations Workshop, Proceedings, (2001)), 237-238

[3] Malacaria, P., Assessing security threats of looping constructs, (Proceedings of the 34th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '07, New York, NY, USA, (2007), ACM), 225-235 · Zbl 1295.68089

[4] Clark, D.; Hunt, S.; Malacaria, P., A static analysis for quantifying information flow in a simple imperative language, J. Comput. Secur., 15, 3, 321-371, (2007)

[5] Shannon, C. E., A mathematical theory of communication, Bell Syst. Tech. J., 27, 379-423, (July 1948)

[6] Millen, J. K., Covert channel capacity, (IEEE Symposium on Security and Privacy, (1987)), 60-66

[7] Malacaria, P., Algebraic foundations for information theoretical, probabilistic and guessability measures of information flow, (2011)

[8] Biondi, F.; Legay, A.; Malacaria, P.; Wasowski, A., Quantifying information leakage of randomized protocols, (Giacobazzi, R.; Berdine, J.; Mastroeni, I., VMCAI, Lect. Notes Comput. Sci., vol. 7737, (2013), Springer), 68-87 · Zbl 1329.68188

[9] Jonsson, B.; Larsen, K. G., Specification and refinement of probabilistic processes, (LICS, (1991), IEEE Computer Society), 266-277

[10] Puterman, M. L., Markov decision processes: discrete stochastic dynamic programming, (April 1994), Wiley-Interscience

[11] Stoer, J.; Bulirsch, R.; Bartels, R.; Gautschi, W.; Witzgall, C., Introduction to numerical analysis, Texts Appl. Math., (2010), Springer

[12] Jaynes, E. T., Information theory and statistical mechanics, Phys. Rev. Online Arch. (Prola), 106, 4, 620-630, (May 1957)

[13] Clark, D.; Hunt, S.; Malacaria, P., Quantitative information flow, relations and polymorphic types, J. Log. Comput., 18, 2, 181-199, (2005), (Special Issue on Lambda-Calculus, Type Theory and Natural Language) · Zbl 1101.68560

[14] Smith, G., On the foundations of quantitative information flow, (de Alfaro, L., FOSSACS, Lect. Notes Comput. Sci., vol. 5504, (2009), Springer), 288-302 · Zbl 1234.68101

[15] Köpf, B.; Basin, D. A., An information-theoretic model for adaptive side-channel attacks, (Ning, P.; di Vimercati, S. D.C.; Syverson, P. F., ACM Conference on Computer and Communications Security, (2007), ACM), 286-296

[16] Köpf, B.; Mauborgne, L.; Ochoa, M., Automatic quantification of cache side-channels, (Madhusudan, P.; Seshia, S. A., CAV,

Lect. Notes Comput. Sci., vol. 7358, (2012), Springer), 564-580

[17] Yasuoka, H.; Terauchi, T., Quantitative information flow - verification hardness and possibilities, (CSF, (2010), IEEE Computer Society), 15-27

[18] Alvim, M. S.; Chatzikokolakis, K.; Palamidessi, C.; Smith, G., Measuring information leakage using generalized gain functions, (Chong, S., CSF, (2012), IEEE), 265-279

[19] Landauer, J.; Redmond, T., A lattice of information, (CSFW, (1993)), 65-70

[20] Aldini, A.; Pierro, A. D., Estimating the maximum information leakage, Int. J. Inf. Secur., 7, 3, 219-242, (2008)

[21] Giacobazzi, R.; Mastroeni, I., Abstract non-interference: parameterizing non-interference by abstract interpretation, (Jones, N. D.; Leroy, X., POPL, (2004), ACM), 186-197 · Zbl 1325.68043

[22] Mastroeni, I.; Giacobazzi, R., An abstract interpretation-based model for safety semantics, Int. J. Comput. Math., 88, 4, 665-694, (2011) · Zbl 1215.68125

[23] Chatzikokolakis, K.; Palamidessi, C.; Panangaden, P., Anonymity protocols as noisy channels, Inf. Comput., 206, 2-4, 378-401, (2008) · Zbl 1147.68394

[24] Bhargava, M.; Palamidessi, C., Probabilistic anonymity, (Abadi, M.; de Alfaro, L., CONCUR, Lect. Notes Comput. Sci., vol. 3653, (2005), Springer), 171-185 · Zbl 1134.68426

[25] Chen, H.; Malacaria, P., Quantifying maximal loss of anonymity in protocols, (Li, W.; Susilo, W.; Tupakula, U. K.; Safavi-Naini, R.; Varadharajan, V., ASIACCS, (2009), ACM), 206-217

[26] Malacaria, P.; Chen, H., Lagrange multipliers and maximum information leakage in different observational models, (PLAS '08, New York, USA, (2008), ACM), 135-146

[27] Cover, T. M.; Thomas, J. A., Elements of information theory, (2006), Wiley · Zbl 1140.94001

[28] Tarjan, R. E., Depth-first search and linear graph algorithms, SIAM J. Comput., 1, 2, 146-160, (1972) · Zbl 0251.05107

[29] Chatterjee, K.; Sen, K.; Henzinger, T. A., Model-checking omega-regular properties of interval Markov chains, (Amadio, R. M., FoSSaCS, Lect. Notes Comput. Sci., vol. 4962, (2008), Springer), 302-317 · Zbl 1138.68441

[30] Kozine, I.; Utkin, L. V., Interval-valued finite Markov chains, Reliab. Comput., 8, 2, 97-113, (2002) · Zbl 1001.65007

[31] Girardin, V., Entropy maximization for Markov and semi-Markov processes, Methodol. Comput. Appl. Probab., 6, 109-127, (2004) · Zbl 1043.60080

[32] de Alfaro, L., Formal verification of probabilistic systems, (1997), PhD thesis, Stanford

[33] de Alfaro, L., Temporal logics for the specification of performance and reliability, (Reischuk, R.; Morvan, M., STACS, Lect. Notes Comput. Sci., vol. 1200, (1997), Springer), 165-176

[34] Caillaud, B.; Delahaye, B.; Larsen, K. G.; Legay, A.; Pedersen, M. L.; Wasowski, A., Constraint Markov chains, Theor. Comput. Sci., 412, 34, 4373-4404, (2011) · Zbl 1223.68070

[35] Delahaye, B.; Katoen, J. P.; Larsen, K. G.; Legay, A.; Pedersen, M. L.; Sher, F.; Wasowski, A., Abstract probabilistic automata, (Jhala, R.; Schmidt, D. A., VMCAI, Lect. Notes Comput. Sci., vol. 6538, (2011), Springer), 324-339 · Zbl 1317.68095