Stochastic Accountability in Distributed Systems

January 21, 2022

There are two major ways to deal with failures in distributed computing:

Fault-tolerance: we anticipate failures by investing into replication and synchronization, so that the system's correctness is not affected by faulty components.

Accountability: we detect failures *a posteriori* and raise undeniable evidences against faulty components.

Accountability in computing has been proposed for generic distributed systems [5, 4] as a mechanism to detect deviations of system nodes from the algorithms they are assigned with. It has been shown that a large class of deviations of a given process from a given deterministic algorithm can be detected by maintaining a set of *witnesses* that keep track of all *observable* actions of the process and check them against the algorithm [6].

The generic approach can be, however, very expensive in practice. In this project, instead of heading for detecting all observable failures [5, 4], we intend to explore the potential of stochastic accountability in generic distributed systems, already addressed in the networking context [7]. The approach is to randomly sample a subset of events in an execution with the goal to detect faulty behavior. As a first step, we intend to focus on gossip-based broadcast algorithms [2] and cryptocurrencies [3, 1] where a malicious source may "equivocate" in order to make correct processes disagree on the messages they deliver.

Contact

Petr Kuznetsov
https://perso.telecom-paristech.fr/kuznetso/
petr.kuznetsov@telecom-paris.fr
Télécom Paris, Institut Polytechnique de Paris

Stefan Schmid
https://www.univie.ac.at/ct/stefan/
stefan.schmid@tu-berlin.de
Technical University of Berlin

References

[1] D. Collins, R. Guerraoui, J. Komatovic, P. Kuznetsov, M. Monti, M. Pavlovic, Y. A. Pignolet, D. Seredinschi, A. Tonkikh, and A. Xygkis. Online payments by merely broadcasting messages.

In *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2020, Valencia, Spain, June 29 - July 2, 2020*, pages 26–38. IEEE, 2020.

[2] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. Scalable byzantine reliable broadcast. In J. Suomela, editor, *33rd International Symposium on Distributed Computing, DISC 2019, October 14-18, 2019, Budapest, Hungary*, volume 146 of *LIPIcs*, pages 22:1–22:16.

[3] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. The consensus number of a cryptocurrency. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019, Toronto, ON, Canada, July 29 - August 2, 2019.*, pages 307–316, 2019.

[4] A. Haeberlen and P. Kuznetsov. The Fault Detection Problem. In *Proceedings of the 13th International Conference on Principles of Distributed Systems (OPODIS'09)*, Dec. 2009.

[5] A. Haeberlen, P. Kuznetsov, and P. Druschel. The case for byzantine fault detection. In *Proceedings of the Second Workshop on Hot Topics in System Dependability (HotDep'06)*, Nov 2006.

[6] A. Haeberlen, P. Kuznetsov, and P. Druschel. PeerReview: Practical accountability for distributed systems. In *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP'07)*, Oct 2007.

[7] K. Thimmaraju, L. Schiff, and S. Schmid. Preacher: Network policy checker for adversarial environments. *IEEE/ACM Trans. Netw.*, 29(5):2087–2100, 2021.