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/](https://perso.telecom-paristech.fr/kuznetso/)  
[petr.kuznetsov@telecom-paris.fr](mailto:petr.kuznetsov@telecom-paris.fr)  
Télécom Paris, Institut Polytechnique de Paris

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

**References**


