CCIT Report #688 February 2008

Brahms: Byzantine Resilient Random Membership Sampling

Edward Bortnikov* Maxim Gurevich* Idit Keidar* Gabriel Kliot†
Alexander Shraer*

Abstract

We present Brahms, an algorithm for sampling random nodes in a large dynamic system prone to Byzantine failures. Brahms stores small membership views at each node, and yet overcomes Byzantine failures of a linear portion of the system. Brahms is composed of two components. The first one is a Byzantine-resistant gossip-based membership protocol. The second one uses a novel memory-efficient approach for uniform sampling from a possibly biased stream of ids that traverse the node. We evaluate Brahms using rigorous analysis, backed by extensive simulations, which show that our theoretical model captures the protocol's essentials. We show that, with high probability, an attacker cannot create a partition between correct nodes. We further prove that each node's sample converges to a uniform one over time. To our knowledge, no such properties were proven for gossip-based membership in the past.

Keywords: random sampling, gossip, membership, Byzantine failures.

[1]Department of Electrical Engineering, The Technion – Israel Institute of Technology.
Email: {ebortnik@techunix, gmax@techunix, idish@ee, shralex@techunix}.technion.ac.il.
[2]Department of Computer Science, The Technion – Israel Institute of Technology.
Email: gabik@cs.technion.ac.il.