Byzantine-tolerant Uniform Node Sampling Service

Emmanuelle Anceaume[1] and Yann Busnel[2]

[1] CNRS / IRISA, Campus de beaulieu, Rennes (France)
emmanuelle.anceaume@irisa.fr
[2] IMT Atlantique, Rennes (France)
yann.busnel@imt-atlantique.fr

Abstract. We consider the problem of achieving uniform node sampling in large scale systems in presence of Byzantine nodes. The uniform node sampling service offers to applications using it a single simple primitive that returns, upon invocation, the identifier of a random node that belongs to the system. We first propose an omniscient strategy that processes on the fly an unbounded and arbitrarily biased input stream made of node identifiers exchanged within the system, and outputs a stream that preserves the uniformity property. Informally, uniformity states that any node in the system should have the same probability to appear in the sample of any correct node of the system. We show through a Markov chain analysis that this property holds despite any arbitrary bias introduced by the adversary. We then propose a strategy based on a sketch data structure that is capable of approximating the omniscient strategy without requiring any prior knowledge on the composition of the input stream. We show through both theoretical analysis and extensive simulations that this "knowledge-free" strategy accurately approximates the omniscient one. We evaluate the resilience of the knowledge-free strategy by studying two representative attacks (flooding and targeted attacks). We quantify the minimum number of identifiers that Byzantine nodes must insert in the input stream to prevent uniformity. Finally, we propose a new construction that processes each input stream with sketches put in series that allows to both increase the accuracy of a single sketch and decrease the time to converge to a uniform output stream. To our knowledge, such a work has never been proposed before.

This work has been partially founded by the French ANR project SocioPlug (ANR-13-INFR-0003) and by the DeSceNt project granted by the Labex Comin-Labs excellence laboratory (ANR-10-LABX-07-01).
A shorter preliminary version of this paper entitled "Uniform Node Sampling Service Robust against Collusions of Malicious Nodes" appeared in the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)

Keywords: Data stream, Byzantine nodes, Uniform sampling, Markov chains, Randomized approximation algorithm