SCALABLE DISTRIBUTED COMPUTING WITH BYZANTINE FAULTS

VALERIE KING, STEVEN LONERGAN, JARED SAIA

Abstract. We address the problem of designing distributed algorithms for large scale networks that are robust to Byzantine faults, where it is not feasible for any processor to broadcast to every other processor. We ask how many bits of communication are needed per processor to compute such fundamental problems as leader election and Byzantine agreement. In this talk we show that $\tilde{O}(n^{1/2})$ bits per processor suffice with high probability, even if there is a fraction of nearly a third corrupt processors who can send an unlimited number of messages. This result is in the full information synchronous model, and only in the case where the malicious processors are chosen at the start.

To the authors' best knowledge, there have been no protocols to compute Byzantine agreement without some processor sending $O(n)$ message to every other processor, even if private channels or cryptography are assumed, unless the number of bits of communication are limited for corrupt processors.