Computer Science
Seminar

Breaking the $O(n^2)$ bit barrier: Scalable Byzantine Agreement with an Adaptive adversary

Jared Saia
University of New Mexico

Abstract: We present an algorithm for Byzantine agreement that is scalable in the sense that each processor sends only soft-O($sqrt(n)$) bits, where n is the total number of processors. Our algorithm succeeds with high probability against an adaptive adversary, which can take over processors at any time during the protocol, up to the point of taking over arbitrarily close to a 1/3 fraction. Moreover, our algorithm works in the presence of flooding: processors controlled by the adversary can send out any number of messages. We assume the existence of private channels between all pairs of processors but make no other cryptographic assumptions. Finally, our algorithm has latency that is polylogarithmic in n. To the best of our knowledge, ours is the first algorithm to solve Byzantine agreement against an adaptive adversary, while requiring o(n^2) total bits of communication.

Jared Saia obtained his PhD from the University of Washington and is now an Associate Professor at the University of New Mexico. His broad research interests are in theory and algorithms with strong interests in distributed algorithms, game theory, security, and spectral methods. A current interest is determining how large groups can function effectively when there is no leader. He is the recipient of several awards including the NSF CAREER Award, the UNM Junior Faculty Research Excellence Award, and several best paper awards.

Tuesday, October 19, 2010, 4:00 pm
Mathematics and Science Center: W201

The paper describing these results won the best paper award at PODC 2010.

Mathematics and Computer Science
Emory University