Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Research Seminar

Some Recent Results On The Use Of Network Coding In Dynamic Clouds

Muriel Médard
MIT

12-1pm Friday 26th June 2015

Abstract: As distributed storage and highly dynamic mobile networks become more widely used in combination, they contend with challenges, three of which we consider in this talk. The first one comes from highly dynamic environments, where we must seek to make best use of locally available storage and network resources in way that maintains data integrity. We show that using a random linear network coding (RLNC) distributed storage system greatly increases durability of data in a dynamic decentralized environment. The second problem we consider is the risk posed to data stored at nodes that are untrusted. We show that coding alone can play a role akin to encryption, with coded portions of data in trusted nodes acting as keys for coded data in untrusted ones. In general, we may interpret keys as representing the size of the list over which an adversary would need to generate guesses in order to recover the plaintext, leading to a natural connection among list decoding, RLNC and secrecy. Under such a model, we show that algebraic block maximum distance separable (MDS) codes can be constructed so that lists satisfy certain secrecy criteria, which we define to generalize common perfect secrecy and weak secrecy notions. The third type of difficulty concerns the risk of passwords' being guessed over some nodes storing data, as illustrated by recent cloud attacks. In this domain, the use of guesswork as a metric shows that the dominant effect on vulnerability is not necessarily from a single node, but that it varies in time according to the number of guesses issued. We also introduce the notion of inscrutability, as the growth rate of the average number of probes that an attacker has to make, one at a time, using his best strategy, until he can correctly guess one or more secret strings from multiple randomly chosen strings

Short Bio: Muriel Médard is the Cecil H. Green Professor of Electrical Engineering and Computer Science at Massachusetts Institute of Technology (MIT) where she leads the Network Coding and Reliably Communications Group. She is an IEEE Fellow and a US National Academy of Engineering Gilbreth Lecturer. She serves as Editor-in-Chief of the IEEE Journal on Selected Areas in Communications.

Venue: Seminar Room, Dunlop-Oriel House/CTVR.

Further Details: Doug Leith (doug.leith@tcd.ie)

CONNECT
Networks of the Future