In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Institute of Network Coding
and
Department of Information Engineering
Seminar

Secure Compute-and-Forward Using Nested Lattice Codes

by

Prof. Navin Kashyap

Indian Institute of Science, Bangalore

Date : 17 February 2014 (Monday)
Time : 2:30 - 3:30 pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

The wireless two-way relay model is a key primitive or building block in physical-layer network coding schemes. In this model, a relay helps two users to exchange their messages, which are assumed to lie in some finite Abelian group G. The compute-and-forward strategy has two phases - a multiple-access (MAC) phase and a broadcast phase. In the MAC phase, the two users transmit real-valued signals (satisfying some power constraint) that encode their respective messages, and the relay receives the superposition (real-valued sum) of the two signals with some Gaussian noise added. From the received signal, the relay computes the sum, in the group G, of the users' messages, and in the ensuing broadcast phase, it forwards the computed sum to the two users. Nazer and Gastpar (2011) showed that the two users can reliably exchange their messages at any rate up to (1/2)*log(1/2 + SNR) using nested lattice codes.

In this talk, we impose an additional security requirement: the relay is untrusted, so it should get little or no information about each individual user's message beyond what is obtainable from the sum it can compute. We devise novel coding schemes involving nested lattice codes and randomization by well-chosen probability distributions on the lattice points. The choice of probability distribution determines the strength of the security guarantee. We show that we can have reliable and perfectly secure exchange of messages at any rate up to rate (1/2)*log(SNR) - log(2e) using our coding scheme. If we relax perfect security to strong information-theoretic security, then rates up to (1/2)*log(1/2 + SNR) - (1/2)*log(2e) are achievable.

This is joint work with Shashank Vatedka and Andrew Thangaraj.

Biography

Navin Kashyap received the B.Tech. degree in Electrical Engineering from the Indian Institute of Technology, Bombay, in 1995, the M.S. degree in Electrical Engineering from the University of Missouri-Rolla in 1997, and the M.S. degree in Mathematics and the Ph.D. degree in Electrical Engineering from the University of Michigan, Ann Arbor, in 2001. During the period 2002-2003, he held a postdoctoral appointment (2002-2003) at the University of California San Diego. From 2004 until 2010, he was on the faculty of the Department of Mathematics and Statistics at Queen's University, Canada, where he still retains an appointment as an Adjunct Professor. Since January 2011, he has been an Associate Professor in the Department of Electrical Communication Engineering at the Indian Institute of Science, Bangalore. His research interests lie primarily in the application of combinatorial and probabilistic methods in information and coding theory.

**** All ARE WELCOME ****

Host: Professor Sidharth Jaggi (Tel: 3943-4326, Email: sid@ie.cuhk.edu.hk)
Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8388)

S:\2014\sem0414_INC_Navin Kashyap_SID_170214