In Favour of Posting

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

Reliable Deniable and Hidable Communication

by

Dr. Mayank Bakshi

Postdoctoral Fellow, Institute of Network Coding

The Chinese University of Hong Kong

Date : 15 January 2014 (Wednesday)
Time : 11:00 am - 12:00 pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

In this talk, we explore the fundamental information theoretic limits of communication in the presence of an eavesdropper when even the knowledge that there is communication taking place is of critical importance. One example of such scenario could be a whistleblower (say, Alice) wanting to communicate deniably to the outside world (say, Bob) knowing that even a suspicion of communication by the eavesdropper (say, Willie) could have dire consequences. Under this communication scenario, three things are desirable - (a) the message be reliably decoded by Bob, (b) the communication be deniable to Willie, i.e., the active distribution of codewords doesn't look too different from an innocent communication, and (c) the message be secure from Willie.

We consider two potential tricks that Alice has at her disposal - pretending innocence and hiding in noise. To showcase the power of the first trick, we consider a simple network of parallel links. Bob gets to see the output of all the links, but Willie only sees an unknown subset of them. Alice is given a fixed innocent distribution and has to design the codebook such that the active distribution mimics the innocent distribution on the subset observed by Willie. We calculate the capacity under this setting and show that by exploiting the fact that Bob gets to see more links than Willie, Alice can talk both deniably and hidably to Bob at a positive rate.

In our second setting, we showcase how Alice could also exploit channel noise as a resource. As an example, we consider Alice transmitting over a Binary Symmetric Channel such that the noise to Bob is smaller than the noise to Willie and the innocent transmission status for Alice is all 0's. By exploiting the statistical nature of the noise, we show that Alice can still communicate deniably and hidably with Bob, though at a sublinear rate of O(1/sqrt(n)).

In the last part of this talk, I briefly mention a new secrecy metric that we call "Super-strong secrecy" that naturally arises out of our formulation of the deniability problem. Although, this metric may be strictly stronger than the commonly considered information-theoretic notion of strong secrecy, it turns out that for the class of weakly symmetric channels, there is no penalty in rate by demanding this stronger secrecy metric.

Joint work with Pak Hou Che, Swanand Kadhe, Prof Sidharth Jaggi, Prof Alex Sprintson, and Prof Chung Chan.

Biography

Dr Mayank Bakshi is a postdoctoral fellow at the Chinese University of Hong Kong. He finished his PhD in Electrical Engineering from California Institute of Technology in 2011. Prior to that, he finished his Master and Bachelor degree at Indian Institute of Technology Kanpur in 2005 and 2003 respectively. His research focuses on Network Coding, Network Security, and Sparse Recovery.

**** All ARE WELCOME ****

Host: Professor Raymond W.H. Yeung (Tel: 3943-8375, Email: whyeung@ie.cuhk.edu.hk)
Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8388)

S:\2014\sem0114_INC_Mayank Bakshi_WHY_150114