University of Utah
ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT ECE

Dr. Paul Cuff

Information Sciences & Systems
Electrical Engineering, Princeton University

August 27 – MEB 3235 – 1:00 p.m.

"Information Theory for Secrecy and Control"

ABSTRACT:

This talk introduces a couple of novel viewpoints and results for control and secrecy in distributed systems.

Information theory provides fundamental limits for perfect secrecy. In particular, perfect theoretical secrecy of communication sent over a public channel can only be achieved by use of a secret key known only to the transmitter and receiver, and the length of the secret key must be as long as the message being sent. This statement is discouraging because there is not an inexpensive way to exchange such long keys. An attempt to side-step this requirement is to use channel noise to hide the message and to analyze partial secrecy. The typical approach is to measure partial secrecy using "equivocation," which is defined as the conditional entropy of the information given everything the eavesdropper intercepts. While equivocation has some desired properties of secrecy, this talk outlines a measurement of partial secrecy in terms of how well the eavesdropper can reconstruct the information. The particular assumptions made are motivated by distributed systems. One interesting discovery is that, up to a point, reduction in secret key costs nothing in terms of information leaked to the eavesdropper from this viewpoint.

It is possible to embed digital information in control signals. The idea of embedding digital information in apparently unrelated signals is found in digital watermarking and steganography. There, the purpose is to attach a label to a signal or hide information, unobservable to the casual observer. In this work we present some basic questions and a few answers for embedding information in a related control signal or action sequence. A nice illustration of this type of setting is the game of bridge, where the bids made and cards played affect not only the outcome of the game but also the information conveyed to the partner. In this talk we illustrate the results using simple games as well as communication settings.

The public is invited