Information Theory and Secure Communications Architecture

J. Nicholas Laneman
Dept. of Electrical Engineering
University of Notre Dame

Abstract: In this talk, we overview communications architecture and present recent results for secure information transmission, in which messages are protected from an eavesdropper by exploiting some advantage between the transmitter and intended receiver. In Shannon's original work on secrecy, the advantage takes the form of a shared random sequence called a one-time pad, which now heavily influences the field of cryptography. In the wiretap channel model introduced by Wyner and extended by Csiszar and Korner, the advantage takes the form of a less noisy channel between the transmitter and intended receiver, which now heavily influences the field of physical-layer security. Although standard information-theoretic tools have successfully established the fundamental limits of secure communication limits over memoryless wiretap channels, elaborate models are difficult to analyze with these tools and, more importantly, the wiretap channel model has not been fully accepted by the cryptography community.

Our research focuses on the development of a general framework for information-theoretic security that is simple enough to be mathematically tractable yet powerful enough to be cryptographically relevant. The approach leverages information-spectrum methods, which center on properties of information viewed as a random variable instead of an expectation. We will present a general formula for secrecy capacity that applies to arbitrary channel models, including those that are not information stable, and holds for a variety of secrecy metrics, including those that are relevant in cryptography. We will point out how the coding theorem suggests a connection between secrecy and resolvability, i.e., the minimum number of bits required to simulate the output of a channel resulting from a random input, that may guide the design of coding schemes. Finally, we will apply the general result to secure communication over wireless fading channels with varying amounts of channel state information and over timing channels.

Joint work with Matthieu Bloch and Brian Dunn.

Friday, February 27, 2009
1:30-2:30 p.m.
Bryan Hall, room 305

Host: Joseph O’Sullivan

Short Bio: J. Nicholas Laneman is an Associate Professor of Electrical Engineering at the University of Notre Dame. He earned Ph.D. and M.S. degrees in Electrical Engineering from the Massachusetts Institute of Technology, Cambridge, MA, in 2002 and 1997, respectively, and B.S. degrees in Electrical Engineering and in Computer Science from Washington University, St. Louis, MO, in 1995. His current research interests are in communications architecture---a combination of information theory, signal processing for communications, network protocols, and hardware design---specifically for wireless systems. He received a PECASE and NSF CAREER Award in 2006, a ORAU Ralph E. Powe Junior Faculty Enhancement Award in 2003, and the MIT EECS Harold L. Hazen Teaching Award in 2001. He is a member of IEEE, ASEE, and Sigma Xi.