Illinois Center for Wireless Systems

ICWS Seminar Series

SECURE COMMUNICATION FOR DISTRIBUTED SYSTEMS

Professor Paul Cuff
Electrical Engineering
Princeton University

Monday, November 14, 2011
141 Coordinated Science Lab / 4:00 p.m.

Abstract: Distributed systems such as a power grid or data network can be vulnerable to malicious attackers due to the control signals and information that are communicated throughout the system. For example, Information and signals needed to control a power grid might be used by an adversary to overload and destabilize the grid. Similarly, an attacker might attempt to congest a data network. One important aspect of security in such a system is secrecy, addressed by cryptography, which is intended to render a communication signal meaningless to all but the intended recipient. This talk introduces a novel viewpoint and theoretical proof of secrecy, defined operationally in a way that is significant to distributed systems. Namely, we cast the system objective as a zero-sum game against an adversary and measure the secrecy performance of the system by the payoff it achieves against an optimal adversary.

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 no inexpensive way to exchange such long keys. In practice, proven secrecy is forsaken for less expensive encryption algorithms that are robust due to computational limitations. Information theorists have attempted to side-step the one-time-pad requirement by using channel noise to hide the message, or by rigorously analyzing partial secrecy, usually quantified by the equivocation (posterior entropy) of the information.

The work presented here considers a communication system designed specifically for the information being concealed and the possible uses of that information by an attacker. While the typical view of encryption is that the sensitive information is either successfully hidden or it is compromised, and that the secret key length and algorithm complexity make it harder to break the encryption, we find that the optimal communication signals in our framework will reveal a distorted version of the information in order to use the secret key resources most effectively on the most crucial aspects of the information. We also find that the full merits of perfect secrecy (for most specific systems) can be achieved with a smaller secret key rate than a one-time-pad.

Short Biography: Paul Cuff received the B.S. degree in electrical engineering from Brigham Young University in 2004 and the M.S and Ph.D. degrees in electrical engineering from Stanford University in 2006 and 2009. He was awarded the ISIT 2008 Student Paper Award for his work titled "Communication Requirements for Generating Correlated Random Variables" and was a recipient of the National Defense Science and Engineering Graduate Fellowship and the Numerical Technologies Fellowship.

ICWS Seminar series is supported by a grant from Rockwell Collins