The University of New South Wales

Faculty of Engineering
School of Electrical Engineering & Telecom

Invited Talk

A Unified Framework for Key Agreement over Wireless Fading Channels

Lifeng Lai

Assistant Professor
Systems Engineering Department
University of Arkansas, Little Rock, USA

Date: 11 October 2010, Monday
Time: 3:00 p.m. – 4:00 p.m.
Venue: G3, Electrical Engineering Building

Abstract

In this talk, we will discuss how to generate information theoretically secure keys using wireless fading channels. First, a key agreement framework that unifies existing source and channel models for key agreement over wireless fading channels is presented. It is shown that, in general, to fully exploit the resources provided by time varying channel gains, one needs to combine both the channel model and the source model. Asymptotic analyses suggest that in the long coherence time regime, the channel model is asymptotically optimal. On the other hand, in the high signal to noise ratio regime, the source model is asymptotically optimal. Second, the framework is extended to the scenario with an active attacker whose goal is to minimize the key rate that can be generated using our protocol. The attacker's optimal attack strategy is identified. The key rate under this attack model is then characterized.

This is a joint work with Professor Yingbin Liang of Syracuse University and H. Vincent Poor of Princeton University.

Biography

Dr. Lifeng Lai received the B.E. and M. E. degrees in Information Science and Electrical Engineering from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the PhD degree in Electrical and Computer Engineering from the The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at the Department of Electrical Engineering, Princeton University from Sept. 2007 to Aug. 2009. He is now an assistant professor at University of Arkansas, Little Rock. He was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. His current research interest includes Wireless Network Security, Statistic Analysis in Cognitive Radio Networks, Biometric Security Systems and Cooperative Communications. He co-authored a paper that received the Best Paper Award from IEEE Global Communications Conference, 2008.

* * * * * **ALL ARE WELCOME** * * * * * **For ENQUIRIES:** Dr. Wei Zhang (Ph: 9385 4033)