THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Everlasting Security in
Wireless Communications Networks
by
Professor Dennis Goeckel
Electrical and Computer Engineering Department
University of Massachusetts at Amherst
USA

Date : **27 August, 2014 (Wednesday)**
Time : **11:00am – 12:00noon**
Venue : **Room 833 Ho Sin Hang Engineering Building**
The Chinese University of Hong Kong

Abstract

Security is one of the most prominent concerns of contemporary wireless communication systems, as evidenced by the recent surge in traditional cryptographic and emerging information-theoretic approaches for such. In this talk, we consider everlasting secrecy, which we define as preventing the interception of any signal that can be stored and eventually decrypted by an interested and determined eavesdropper. Of particular interest here is the challenging scenario where the eavesdroppers can be both arbitrarily close to system nodes and of unknown location. After reviewing recent efforts of other groups, we focus on our novel approaches for information-theoretic secrecy for both one-way communication in single links and arbitrary communication patterns in large networks. In particular, for one-way communication in single links, we exploit the fact that nonlinear operators are not necessarily commutative and describe a collection of approaches that force the eavesdropper into a different ordering of two nonlinear operations than the desired recipient, hence enabling information-theoretic secrecy. For asymptotically large networks, we demonstrate how to combine network coding and physical layer approaches to keep all system messages secure from eavesdroppers of unknown location. Our perspective on future directions in the area concludes the talk.

Biography

Dennis Goeckel received his PhD from the University of Michigan in 1996. Since 1996, he has been with the Electrical and Computer Engineering Department at the UMass-Amherst, where he is currently a Professor. Prof. Goeckel has been a Lilly Teaching Fellow and received the University of Massachusetts Distinguished Teaching Award in 2007. His research interests are in physical-layer communications and networking, and he currently serves as an Associate Editor for the IEEE/ACM Transactions on Networking (IEEE/ACM ToN). Prof. Goeckel is an NSF CAREER Award winner and IEEE Fellow.

** ALL ARE WELCOME **

Host: Professor Sidharth Jaggi (Tel: 3943-4326, Email: sjaggi@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)