



THE CHINESE UNIVERSITY OF HONG KONG
Institute of Network Coding
and
Department of Information Engineering
Seminar



Group Secret Key Agreement over State-Dependent Wireless Broadcast Channels

by

Prof. Mahdi Jafari Siavoshani
Sharif University of Technology, Iran

Date : 27 August 2014 (Wednesday)
Time : 2:30 - 3:30pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

In this talk, we consider a group of m trusted and authenticated nodes that aim to create a shared secret key K over a wireless channel in the presence of an eavesdropper Eve. We assume that there exists a state dependent wireless broadcast channel from one of the honest nodes to the rest of them including Eve. All of the trusted nodes can also discuss over a cost-free, noiseless and unlimited rate public channel which is also overheard by Eve. For this setup, we develop an information-theoretically secure secret key agreement protocol. We show the optimality of this protocol for "packet erasure" and "linear deterministic" wireless broadcast channels. For "state-dependent Gaussian" wireless broadcast channels, we derive the achievable secret key generation rate for the devised scheme and show the optimality of this protocol for the regime of "high-SNR and large-dynamic range over the channel states" in the degrees of freedom sense.

Biography

Mahdi Jafari Siavoshani received his PhD from Swiss Federal Institute of Technology (EPFL) in 2012. He is currently an assistant professor of the Computer Engineering Department at Sharif University of Technology, Iran.

He is interested in various fundamental problems that arise in communication networks. His research interests mainly focus on understanding the fundamental limits of such networks as well as the design of new techniques and algorithms that are suitable for practical implementation. He is also interested in the connection of communication and computer sciences.

**** ALL ARE WELCOME ****

Host: Professor Raymond W.H. Yeung (Tel: 3943-8375, Email: whyeung@ie.cuhk.edu.hk)
Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8388)