In Favour of Posting

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

Secure Multiplex Coding and Its Application to Secure Network Coding

by

Prof. Ryutaroh Matsumoto
Department of Communications and Integrated Systems
Tokyo Institute of Technology

Date : 23 March 2011 (Wednesday)
Time : 11:00 am - 12:00 pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

In the coding for wiretap channels and the secure network coding, traditionally the transmitter has to include random bits statistically independent of the secret message that should be hidden from the eavesdropper. The inclusion of random bits decreases the information rate. In order to get rid of the loss of information rate, Yamamoto et al. proposed the secure multiplex coding for wiretap channel in ITW 2005, in which there are multiple independent secret messages and one secret message serves as random bits for another secret message, thereby there is no loss of information rate. We improve Yamamoto et al.'s result in three ways over memoryless broadcast channels: (1) They only evaluated mutual information between one secret message and the eavesdroppers information. We evaluate the mutual information of arbitrary collection of secret message, and clarifies the set of achievable rate tuples with specified maximum amount of mutual information between each collection of secret messages and the eavesdropper's information. (2) We tighten the evaluation of mutual information by Yamamoto et al. with finite code length. (3) Our coding scheme can support a common message destined for both legitimate receiver and eavesdropper, as done in the broadcast channel with confidential messages considered by Csiszar and Korner.

In the latter half of this talk, we apply the above idea to the secure network coding, and obtain improvements to the weakly secure network coding proposed by Bhattad and Narayanan in NetCod 2005 and the universal weakly secure network coding proposed by Silva and Kschischang in ITW 2009.

This is a joint work with Masahito Hayashi (Tohoku University and National University of Singapore).

Remark: This is a consolidated talk of two papers arXiv:1101.4036 and arXiv:1102.3002.

Biography

Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Japan, in 1996, 1998 and 2001 respectively. He was an Assistant Professor from 2001 to 2004, and has been an Associate Professor since 2004 in the Department of Communications and Integrated Systems of Tokyo Institute of Technology. His research interest includes error-correcting codes, quantum information theory, and communication theory. Dr. Matsumoto received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He received the Best Paper Awards from IEICE in 2001 and 2008.

****ALL ARE WELCOME ****

Host: Professor Raymond W.H. Yeung (Tel: 2609-8375, Email: whyeung@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8388)