In Favour of Posting

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

Combined Coding and Encryption and Its Applications to Network Coding

by

Dr. Haitham Rashwan

Lancaster University, United Kingdom

Date : 21 February 2012 (Tuesday)
Time : 11:00 am - 12:00 pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Network coding substantially increases network throughput. Random network coding is an effective technique for information dissemination in communication networks. Network coding security is designed against two types of attacks: Wiretapping and Byzantine attacks. The Wiretapping attack can tap some original packets, outgoing from the source to the destination with the purpose of recovering the message. The Byzantine attack can inject error packets; this type of attack has the potential to affect all packets gathered by an information receiver.

This talk will overview some of the recent progress on security of network coding. He proposes a new scheme for secure information packets over a random network coding channel. This scheme is based on combing both the GPT (Gabidulin-Paramonov-Tretiyakov) public key cryptosystem and the Silva-Koetter-Kschischang (SKK) codes in order to secure communications against both attacks. Moreover, he will address the performance of the system, transmitting the encrypted packets to the destination through wired communication networks by using different random network coding models. In addition, he will demonstrate a comparison between the proposed scheme and Silva-Koetter-Kschischang (SKK) codes. The proposed scheme is secure against Wiretapping and Byzantine attacks under some conditions which depend on Gabidulin (rank) code parameters.

Biography

Haitham Rashwan received the BEng degree in electronic engineering from DeMontfort University, UK in 2002, then the MSc degree in network communication and security from Loughborough University, UK in 2007, and the PhD degree in communication systems from Lancaster University, UK in 2011. From 2002-2006, he was a software engineer at Fine Media UK, UK. Since 2008, he has been at the School of Computing and Communication in Lancaster University, where he is currently a Research Associate. He was involved in several European and United Kingdom research projects in The Engineering and Physical Sciences Research Council (EPSRC) and Technology Strategy Board (TSB) programmes. Also he has lectured in an undergraduate course, acted as a teaching assistant for different undergraduate and MSc courses, acted as a reviewer for international conferences and participated in various academic and industrial events. His main research interests are Security of Network Coding, Applied Cryptography, Combined Coding and Encryption, Location Based Encryption, and Information Theory.

****ALL ARE WELCOME ****

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

S:\2012\sem0412_INC_Haitham Rashwan_WHY_210212