Abstract:

In this thesis we investigate the secure network coding problem. We are interested in both passive and active attacks in network coding.

The first part of this thesis focuses on passive attacks in network coding. A passive attacker can either eavesdrop from a network link between two nodes (“outside”) or by controlling a network node itself (“inside”). We revisit a secret sharing approach to secure network codes against an outside wiretapper. We propose an efficient link protection scheme to prevent an inside wiretapper from obtaining more meaningful (decoded or decodable) information about the original message than what can be disclosed at the node it controls.

The second part of this thesis is dedicated to the investigation of active attacks (pollution attacks) in network coding. We present some special authentication codes (A-codes) as information-theoretic authentication schemes to mitigate pollution attacks in network coding. We derive some bounds on parameters associated with these special A-codes, and show some efficient constructions of these A-codes.

Date: 13th May 2013 (Monday)
Time: 10.30am – 12.00pm
Venue: MAS Executive Classroom 1 (MAS-03-06)
Supervisor: Associate Professor Wang Huaxiong