Introduction to the course

Information Theoretic Security

Somayeh Salimi

September 19, 2013

Communication Theory Lab
ACCESS Linnaeus Center
School of Electrical Engineering
KTH Royal Institute of Technology
Stockholm, Sweden

General Info

- Ph.D. level course
- 8 credits
- Prerequisite: the basic course on information theory

General Description

Information Theoretic Security:

- focuses on secure communications from an information theoretic perspective.
- exploits different concepts and tools of information theory and coding theory to provide security without any need to shared key or other assumptions in conventional cryptography
- uses the concepts and tools in the area to formulate the problem and solve them

Content of the course

- Session 1- Recapitulation of Information Theory Basics
  - AEP
  - strong typicality
- Session 2- An introduction to security
  - main security services
  - Shannon's secrecy systems
  - security primitives: symmetric encryption, public key cryptography, hash functions
  - Security in the layered architecture
  - integration of physical layer security with upper layers security
- Session 3- Wiretap channel
  - basic wiretap channel and secrecy capacity
  - achievability and converse proofs
  - secrecy capacity for some special cases
  - the basic wiretap channel with a shared key

Content of the course

- Sessions 4,5- Secret key agreement
  - source and channel models of secret key agreement with a q-round public channel
  - weak and strong secret key
  - extension of the basic key agreement scheme
  - key agreement through a generalized MAC
- Sessions 6,7- secure source coding
  - distributed
  - lossless
  - lossy
- Session 8- one advanced topic on information theoretic security context

Content of the course

- Session 9- Secure network coding
  - network coding active and passive attacks
  - notion of strong security and weak security
  - computationally bounded and unbounded wiretapper
  - secure multicast capacity and the required field size

Requirements for final grade

- Homework
  - should be done in an individual base
  - every homework should be handed in
  - minimum number of points must be achieved for each homework along with the sum of all achieved points
  - The problem assignments are weekly or biweekly where the due is in two weeks.
- Final presentation
  - some topics or papers are suggested for the final presentation.
  - the students can suggest other paper related to information theoretic security but it should be adjusted with the teacher
  - each student should review the paper and present it in a 30-min talk points
  - The deadline of the final presentations is three weeks after the last lecture.

Course Schedule

- Lecture#1: Sep. 19, 1:00-3:00 PM
- Lecture#2: Sep. 26, 1:00-3:00 PM
- Lecture#3: Oct. 3, 2:00-5:00 PM
- Lecture#4: Oct. 10, 1:00-3:00 PM
- Lecture#5: Oct. 17, 2:00-5:00 PM
- Lecture#6: Oct. 24, 9:00-12:00 AM
- Lecture#7: Oct. 31, 2:00-5:00 PM
- Lecture#8: Nov. 7, 2:00-5:00 PM
- Lecture#9: Nov. 14, 2:00-5:00 PM

Course literature

- “Information Theoretic Security,”Y. Liang, H. V. Poor and S. Shamai, Now publishers Inc. 2009: ISBN-10: 1601982402.
- “Network Information Theory,”A. El Gamal and Y. -H. Kim, Cambridge 2011:ISBN 9781107008731 (Lecture notes is available under http://arxiv.org/abs/1001.3404)
- “Physical-Layer Security: From Information Theory to Security Engineering,”M. Bloch, J. Barros, Cambridge 2011: ISBN-10: 0521516501.