ENEE 729E: Information-Theoretic Security for Wireless Communications

Introduction:
Information-theoretic physical-layer security has emerged in the past few years as a promising new approach to securing wireless communications. This field explores possibilities of providing security in the physical layer using techniques from information theory, communication theory and signal processing. This approach is a fundamental departure from the currently available cryptographic solutions in that the security it provides is unbreakable, provable and quantifiable (in bits/sec/hertz), and is effective even against computationally-unlimited adversaries. This approach exploits unique characteristics of the wireless medium, such as the inherent random fluctuations in the wireless channel, broadcast nature of wireless communications and overheard information, use of multiple antennas, carefully designed multi-user interactions (e.g., cooperative jamming and feedback), signal alignment, etc. In this course, we will cover security of single-user and multi-user (multiple-access, broadcast, interference and relay) wireless communication systems.

Tentative Course Outline:

- Shannon's secrecy system, and the one-time pad
- Wyner's wiretap channel
- Csiszar-Korner's generalization of the wiretap channel
- Gaussian wiretap channel
- Independent parallel wiretap channels
- Fading wiretap channel
- MIMO wiretap channel
- Multiple-access wiretap channel, and cooperative jamming
- Multi-receiver wiretap channel
- Broadcast channel with confidential messages
- Relay channel, and cooperative secrecy
- Interference channel with confidential messages

Prerequsites: ENEE620 and ENEE627.

Instructor: Sennur Ulukus, 2337 A. V. Williams Building, ulukus@umd.edu, (301) 405 4909.

Textbook: Lecture notes and research papers.

Grading: Class participation and course project.