*Electrical & Computer Engineering*

# SEMINAR

**Louisiana State University**

# Design and Analysis of an ARQ Based Symmetric Key Generation Algorithm

*Yahya S. Khiabani*

**Department of Electrical and Computer Engineering**

**Louisiana State University**

**Abstract**—The main idea in this work is to design and analyze a symmetric key generation algorithm whereby we can strengthen wireless network security. Our main goal is generating a sequence of highly secure secret keys based on an ARQ based transmission mechanism that relies on the statistical independence of channel errors between the attacker and legitimate users. This leads to some information loss for the adversary which allows us to constantly extract keys by using universal Hashing techniques from communication process, about which we can make sure that adversary's knowledge remains negligible. More specifically, the key generation algorithm is analyzed and designed in a way that targeted security as well as the required throughput and synchronization goals for the transmission are achieved. Simulation results show that the designed algorithm achieves the desired requirements for both system security and throughput.

**Bio**—Yahya S. Khiabani received his B.S.E.E. and M.S.E.E degrees from University of Tabriz, Iran, in 2003 and 2007. He was admitted as a PHD student in Louisiana state university, ECE department, in 2009 and granted Economic Development Assistantship (EDA) to work on security algorithms in wireless networks under advisory of Dr. Shuangqing Wei. As a PHD student his research is focused on information theoretic based security and anti-eavesdropping algorithms in wireless networks including physical layer secrecy and cryptography.

**When:** Tuesday, **25 October 2011,** 13:30 - 14:30
**Where:** Room 145 EE Building
**Info:** `http://www.ece.lsu.edu/seminar`