

Opportunistic Encryption for Robust Wireless Security

by R. Chandramouli, ECE Dept., Stevens Institute of Technology

Date: October 13, 2005 (Thursday)
Time: 6:15 pm (refreshment starts at 6:00 pm)
Place: 202 ECEC, NJIT

About the Speaker

Dr. Chandramouli is an Associate Professor in the ECE department at Stevens Institute of Technology. His research in the areas of wireless networking and security, media security and forensics, and applied probability theory is funded by the NSF, U.S. Air Force, U.S. Army, and industry. He has given plenary talks at the Digital Forensics Research Workshop and Number Theory for Security Conference, among others.

He is an Associate Editor for the IEEE Transactions on Circuits and Systems for Video Technology and a Co-founder and Program Co-Chair of the IEEE International Workshop on Adaptive Wireless Networks. He is a recipient of the NSF CAREER award and IEEE Richard E. Merwin award. His recent paper on covert channel identification has been recognized as one of the top papers in IEEE ICIP (2004) by the IEEE Signal Processing Society.

About the Talk

Some of the very same properties that give ciphers their cryptographic strength also cause throughput reduction when operating in an interference prone wireless network. Therefore there is a fundamental trade-off between encryption based security and achievable throughput in secure wireless networks. This trade-off has not yet been explored in a comprehensive or systematic manner. In this talk, we present a mathematical framework to analyze this issue. Using mathematical optimization techniques we show that a method we call "opportunistic encryption" is able to exploit wireless channel opportunities to optimally trade-off security for throughput. The effect of an attacker will also be discussed. Numerical results for opportunistic AES encryption will be presented to illustrate this idea. It is observed that opportunistic encryption produces significant performance improvements compared to traditional fixed encryption.

This is joint work with C. Nanjunda, M. Haleem and K.P. Subbalakshmi.

Sponsors: IEEE Communications Society North Jersey Chapter
NJIT Department of Electrical and Computer Engineering