North Jersey
Communications
Chapter

A New Look at Wireless Security: Error Correcting Ciphers

by K.P. Subbalakshmi, ECE Dept., Stevens Institute of Technology

Date: February 23, 2006 (Thursday)
Time: 6:15 pm (refreshment starts at 6:00 pm)
Place: 202 ECEC, NJIT

About the Speaker

Dr. K.P. Subbalakshmi (Suba) is an Assistant Professor in the Dept. of E.C.E at Stevens Institute of Technology. Her research interests lie in the areas of information and communication security (encryption, steganography etc), joint source channel coding with applications to sensor networks, multiple description coding and QoS issues in multimedia networking. Her research is funded by the NSA, NSF, US Army, AFRL, NJCST and the Industry.

She is the chair of the IEEE COMSOC Special Interest Group on Security, Multimedia Communications Technical Committee. She is the program chair of the IEEE GLOBECOM Symposium on Information and Wireless Security, 2006. She has chaired and organized several special sessions in conferences and serves on the technical program committees of several international conferences.

Further details of her research can be found at http://www.ece.stevens-tech.edu/~suba

About the Talk

Securing wireless link using encryption has become possible with the advent of strong ciphers and wireless standards. But the very property that makes a cipher stronger (diffusion) is also a reason for making it highly sensitive to bit errors caused by noisy wireless links. Even a single bit error in the encrypted data block will cause about half of the decrypted bits to be in error---causing a significant reduction in throughput, higher battery power consumption etc. Hence error resilience and encryption often work at cross purposes leading to some fundamental trade-offs. Traditionally, encryption and forward error correcting coding (FEC) have been treated separately which does not take this trade-off into consideration.

However, a single joint encryption-error correction paradigm may be less expensive and more efficient than the traditional approach. There are several theoretical and practical challenges in the joint design of encryption and error correction. Recently, we addressed these issues by designing the first class of codes, called high diffusion codes (HD codes) that can be used in the diffusion layer of a cipher. We first identified two criteria that these codes must satisfy: (a) for optimal error resilience and (b) for optimal diffusion (security). Mathematical properties of the code were explored and algorithms were developed for constructing such codes. A theoretical cipher was constructed using this code at the diffusion layer. Simulation results show that the HD-cipher in the GF(8) space performs better in terms of error correction capability over a traditional concatenated system.

This talk will present the fundamental ideas behind HD codes and discuss the construction of the codes and the cipher.

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

For more information contact Nirwan Ansari (973) 596-3670, or check **http://web.njit.edu/~ieeenj/comm.html** for latest updates. Directions to NJIT can be found at: **http://www.njit.edu/University/Directions.html**.