

Security-Resource Trade-offs in Wireless Networks



K.P. Subbalakshmi, <http://www.ece.stevens-tech.edu/~suba>

GOAL

Guaranteeing security in wireless networks is challenging due to: *highly error prone links, high variability in the error rates in these links, often limited bandwidth and finally the limited battery power of the end devices.* A holistic approach must be taken to address the fundamental trade-offs in wireless security: between power consumption, error resilience, security and throughput

Approach and Impact

New approach

- **Link State Adaptive Encryption**
 - Combining error resilience and encryption
 - Stochastic models for post-decryption bit errors
- **Power Aware Encryption**
 - Joint authentication-encryption algorithms
 - Power consumption models for existing encryption algorithms
 - Stochastic dynamic programming optimization of power-security

Research Impact

- Analysis and algorithms for power, bandwidth and SNR constrained wireless and sensor network security

Some Results and Publications:

- Encryption and Error Resilience
 - High-Diffusion Cipher
 - A joint encryption-error correction paradigm in a block cipher
 - Currently as resilient as AES against linear and differential cryptanalysis
 - Other tests underway
 - Chetan Nanjunda Mathur, Karthik Narayan, and K. P. Subbalakshmi, "[On the Design of Error Correcting Ciphers](#)," EURASIP Journal on Wireless Communications and Networking, *Special Issue on Wireless Network Security*, To Appear 2007.
 - Chetan N. Mathur and K. P. Subbalakshmi, "[Energy Efficient Wireless Encryption](#)", IEEE GLOBECOM 2006, Symposium on Network and Information Systems Security, November 2006.