


**Opportunistic Encryption for Robust  
Wireless Security**


**R. Chandramouli ("Mouli")**  
mouli@stevens.edu

Multimedia System, Networking, and  
Communications (MSyNC) Laboratory,  
Department of Electrical and Computer Engineering,  
Stevens Institute of Technology

(joint work with C. Nanjunda, M. Haleem, and  
K.P. Subbalakshmi)



CHARLES V. SCHAEFER, Jr.  
SCHOOL OF ENGINEERING



**Wireless Link Properties**

- Wireless link states randomly vary with time and space.
  - Bursty errors (e.g., fading channels).
  - Random errors.
- Effect of link errors.
  - Bit flips.
  - Bit deletion and bit insertion

2

## Overview of Encryption Schemes

- Block cipher.
  - Fixed blocks of plaintext encrypted to same blocks of ciphertext using an encryption key.
- Stream cipher.
  - Block size equal to one bit.
- Symmetric key encryption.
  - Same key for encryption and decryption.
- Public key encryption.
  - Encryption and decryption keys are different.

3

## Avalanche Criterion

- Block ciphers satisfy avalanche criterion.
  - One input bit change causes (on an average) one half of output bits to be in error.
  - Removes statistical correlation between input and output bits.
  - Cryptanalysis is made harder (**security increases**).
- One bit error in received ciphertext block due to wireless link state implies:
  - Multiple bit errors in decrypted plaintext block (**throughput decreases**).

**Trade-off in security vs. wireless throughput**

4

## Popular Symmetric Block Cipher Modes

- **Electronic codebook mode (ECB).**
  - Every plaintext block is encrypted independently:  $c_i = E(K, p_i)$
  - One bit error in ciphertext block causes error propagation in decrypted plaintext block.
  - No loss of synchronization if integer multiples of blocks are lost.
    - Explicit re-synchronization is needed otherwise.
  - Identical plaintext is mapped to identical ciphertext

5

- **Cipher block chaining (CBC).**

- Before encryption plaintext block is XORed with previous ciphertext block:

$$c_i = E(K, p_i \oplus c_{i-1})$$

$$p_i = c_{i-1} \oplus D(K, c_i); c_0 : \text{initial value (IV)}$$

- An erroneous ciphertext block results in two plaintext blocks in error.
- If an integer number of blocks are in error then one additional plaintext block is in error before re-synchronization.
  - Explicit re-sync is needed otherwise.
- Identical plaintext is encrypted to non-identical ciphertext.

6

- **Cipher feedback mode (CFB).**
  - Operates on blocks of size  $j < b$  (plaintext block size).
  - Plaintext is XORed with output of an encryption algorithm.
  - Feedback to encryption algo. are previous ciphertexts.
  - An erroneous ciphertext block distorts corresponding decrypted plaintext block and following  $\lceil b/j \rceil$  blocks.
  - If number of lost bits is an integer multiple of  $j$  then  $\lceil b/j \rceil$  additional plaintext block are distorted before re-synchronization.
    - Explicit re-sync is needed otherwise.
- **Encryption is performed more often.**
  - Hardware throughput is low.
  - Higher power consumption—not desirable for low power mobile devices.

7

- **Output feedback mode (OFB).**
  - Operates on blocks of size  $j < b$  (plaintext block size).
  - Plaintext is XORed with output of an encryption algorithm.
  - Feedback to encryption algo. are previous outputs.
  - **One bit error in ciphertext causes single bit error in decrypted plaintext; no error propagation.**
  - If some bits are lost explicit re-synchronization needed.
- **Encryption is performed more often.**
  - Hardware throughput is low.
  - Higher power consumption—not desirable for low power mobile devices.

8

## Trade-offs...

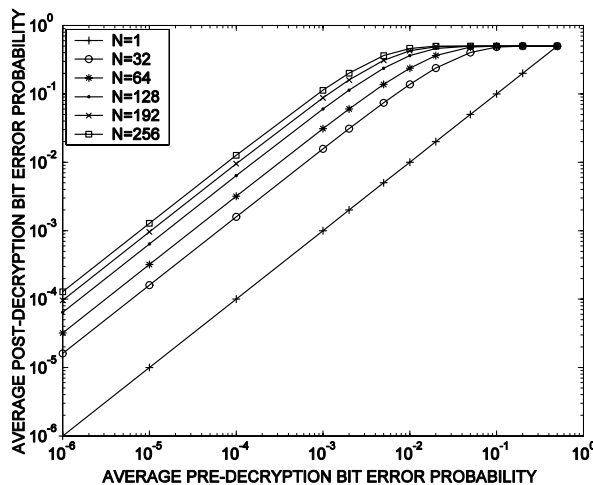
- High (hardware) throughput/low power consumption modes (ECB,CBC)
  - Bit error propagation after decryption.
  - Reduce network throughput.
- Low (hardware) throughput/high power consumption modes (1-CFB,OFB)
  - No bit error propagation.
  - Higher network throughput.

No single encryption mode is the clear winner.

9

## Error Propagation vs. Encryption Block Length

- $P_b$  : wireless link bit error rate
- $P_{b,post}$  : post decryption bit error rate
- $N$  : encryption block length

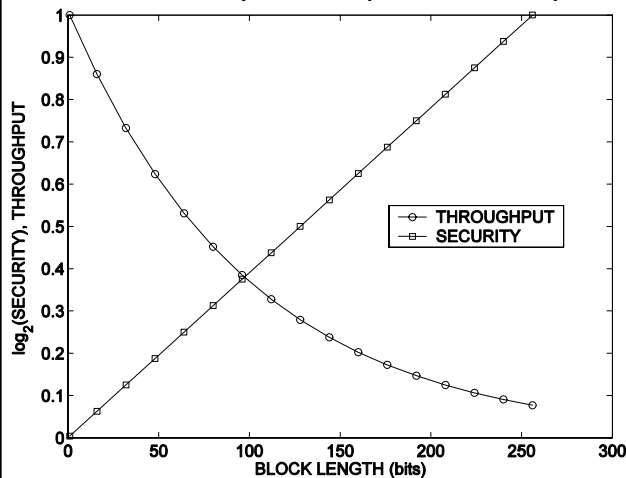


$$P_{b,post} \approx \frac{N}{2} P_b$$

10

## Throughput vs. Security Trade-off

- Throughput,  $D=R(1-NP_b)$ bits/sec;
- R: Transmission rate.
- Security level against brute force attack is  $\sim 2^N$



$P_b=10^{-2}$ .  
BPSK modulation,  
Rayleigh distributed,  
flat fading channel.

11

## Approaches to Error Control

- Forward error control (FEC) code.
  - FEC may fail due to error propagation effect.
- Reduce diffusion in encryption.
  - Reduced error propagation.
  - Reduced security.
- Interleaving.
  - Causes delay depending on interleaving depth.
- ARQ protocols.
  - Overhead, high delay bandwidth product...
- **Opportunistic encryption.**
  - Optimize encryption block size based on security and wireless link state conditions.
  - Optimally trade-off security for throughput.

12

## Scenarios

- Case 1: Exact wireless channel signal to noise ratio (SNR) known.
- Case 2: Only current average SNR and probability distribution of randomly time-varying SNR also known.
- Case 3: A Markov channel model is known for channel/link states.

13

## Security and Adversary Models

- $Q_N$ : Set of available encryption block lengths

$$S_i(N_i) = \frac{\log_2 N_i}{S_{\max}}, \quad S_{\max} = \log_2 \left( \max_{N_i \in Q_N} N_i \right)$$

**Average Security:**  $\bar{S} = \frac{1}{n} \sum_{i=1}^n S_i(N_i)$

$\Phi_i(N_i) = \Pr(\alpha \geq N_i)$  where  $\alpha$  is the "attacker success prob."

**Average vulnerability:**  $\Phi = \frac{1}{n} \sum_{i=1}^n \Pr(\alpha \geq N_i)$

14

## Case 1: Exact Channel SNR Known (I)

- Channel SNR at  $i$ th time slot:  $\gamma_i$

Throughput (of  $i$ th time slot):  $D_i(\gamma_i, N_i) = R_i(1 - N_i P_b(\gamma_i))$

Required Security:  $S_{req} = \frac{1}{n} \sum_{i=1}^n S_i(N_i)$

The Lagrangian of the problem:

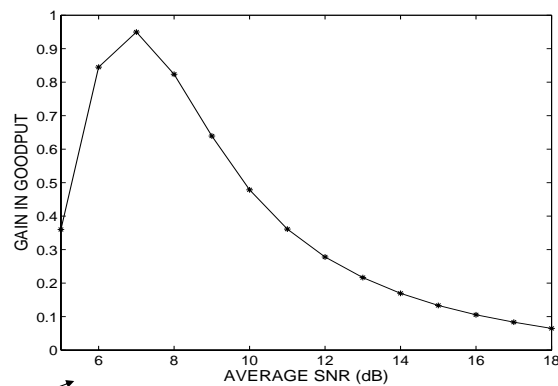
$$C^{(n)} = \frac{1}{nR_{\max}} \sum_{i=1}^n D_i(\gamma_i, N_i) + \frac{\lambda}{n} \sum_{i=1}^n S_i(N_i)$$

Optimum encryption block length:

$$N_i = \frac{\left( \prod_{i=1}^n [R_i P_b(\gamma_i)] \right)^{\frac{1}{n}}}{R_i P_b(\gamma_i)} e^{(S_{\max} S_{req}) \log_e 2}$$

15

## Goodput Gain



Performance with fixed rate (BPSK)

16

## Case 1: Exact Channel SNR Known (II)

$\Phi_i(N_i) = \Pr(\alpha \geq N_i)$  where  $\alpha$  is the "attacker success prob."

Allowable vulnerability level of the message,  $\Phi = \frac{1}{n} \sum_{i=1}^n \Pr(\alpha \geq N_i)$

$\Phi_{\max} > \Phi_i > \Phi_{\min}$ , for all  $i$

### 1. Exponential

$$\Pr(\alpha \geq N_i) = e^{-kN_i}$$

Optimum solution

resembles

"Water-filling" algorithm

### 2. Uniform

$$\Pr(\alpha \geq N_i) = \frac{N_{\max} - N_i}{N_{\max} - N_{\min}}$$

Optimum solution is found

Using *fractional knapsack* algorithm

17

**Exponential distribution:**  $\Pr(\alpha \geq N_i) = e^{-kN_i}$

Throughput (of  $i$ th time slot):  $D_i(\gamma_i, N_i) = R(1 - N_i P_b(\gamma_i))$

The Lagrangian of the problem:

$$C = \frac{R}{n} \sum_{i=1}^n \left( 1 + \frac{1}{k} \ln \Phi_i P_i \right) + v \left( \frac{1}{n} \sum_{i=1}^n \Pr(\alpha \geq N_i) - \Phi \right) + \sum_{i=1}^n \lambda_i (\Phi_i - \Phi_{\min}) + \sum_{i=1}^n \mu_i (\Phi_{\max} - \Phi_i)$$

Karush Kuhn Tucker Conditions :

$$\frac{\partial C}{\partial \Phi_i} = 0 \Rightarrow \Phi_i = - \frac{R P_i}{k(v + \lambda_i - \mu_i)}$$

$\lambda_i (\Phi_i - \Phi_{\min}) = 0, \mu_i (\Phi_{\max} - \Phi_i) = 0$  (complementary slackness)

18

Case I:  $\lambda_i = 0, \mu_i = 0 \Rightarrow \Phi_{\max} > \Phi_i = -\frac{RP_i}{kV} > \Phi_{\min}$

Case II:  $\lambda_i = 0, \mu_i \neq 0 \Rightarrow \Phi_i = \Phi_{\max} = -\frac{RP_i}{k(v + \lambda_i)} \Rightarrow \lambda_i = -\frac{RP_i}{k\Phi_{\max}} - v$

Case III:  $\lambda_i \neq 0, \mu_i = 0 \Rightarrow \Phi_i = \Phi_{\min} = -\frac{RP_i}{k(v + \mu_i)} \Rightarrow \mu_i = -\frac{RP_i}{k\Phi_{\min}} - v$

The solution should satisfy:

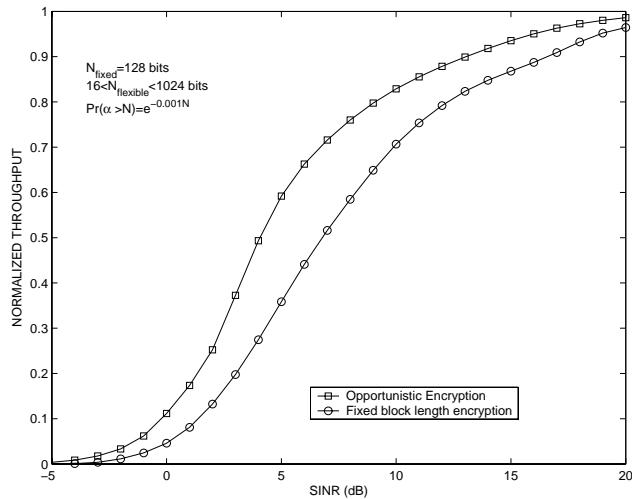
$$\sum_{i=1}^{n'} \max(\Phi_{\min}, \alpha P_i) \wedge \min(\Phi_{\max}, \alpha P_i) = \Phi \text{ where } \alpha = -\frac{R}{kV}$$

The solution involves iterations to identify the best set of channels associated with each of the above three cases. In each iteration  $\alpha$  satisfies

$$n_1 \Phi_{\min} + n_2 \Phi_{\max} + \sum_{i \in s} \alpha P_i = n\Phi \text{ where}$$

$s$  is the set of time slots with  $\Phi_{\min} < \Phi_i < \Phi_{\max}$

## Throughput Gain

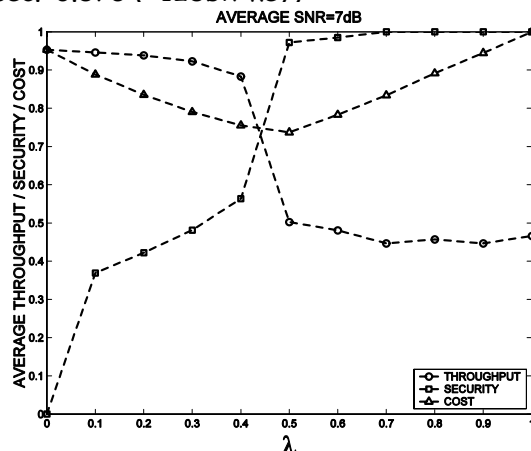


- Uniform distribution:  $\Pr(\alpha \geq N_i) = \frac{N_{\max} - N_i}{N_{\max} - N_{\min}}$
- Throughput maximization subject to vulnerability constraint.
  - Re-formulate as fractional knapsack problem.
- Outline of optimal solution:
  - Sort the channel SNR's in decreasing order.
  - Allocate minimum block lengths so that  $\Phi_{\min}$  is achieved.
  - Allocate block lengths to the ordered channels corresponding to  $(\Phi_{\max} - \Phi_{\min})$
  - Stop when it cannot be done anymore.

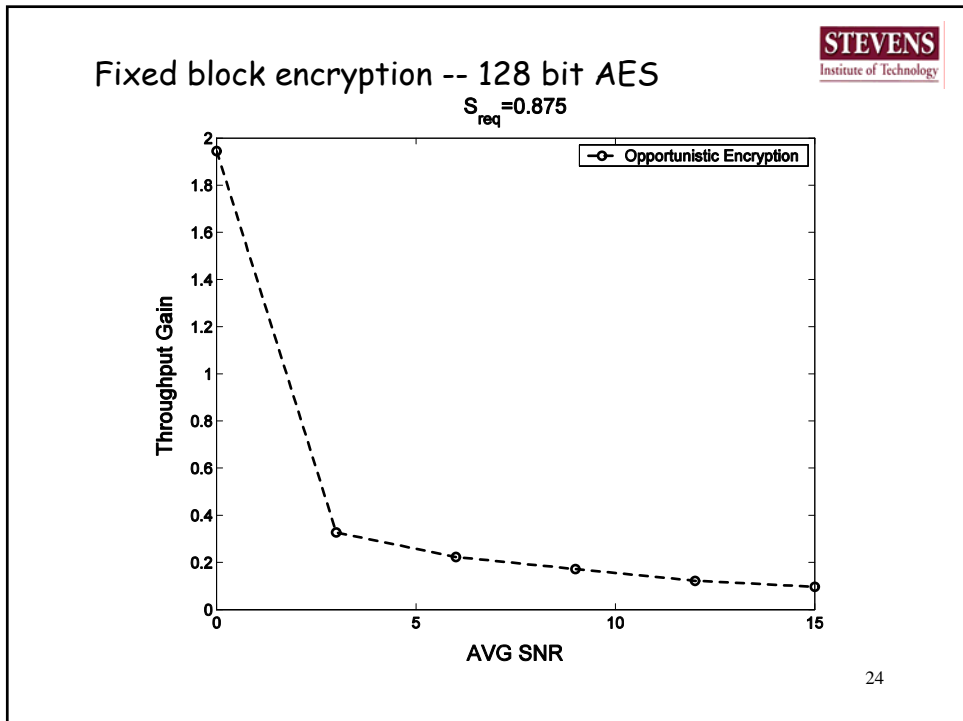
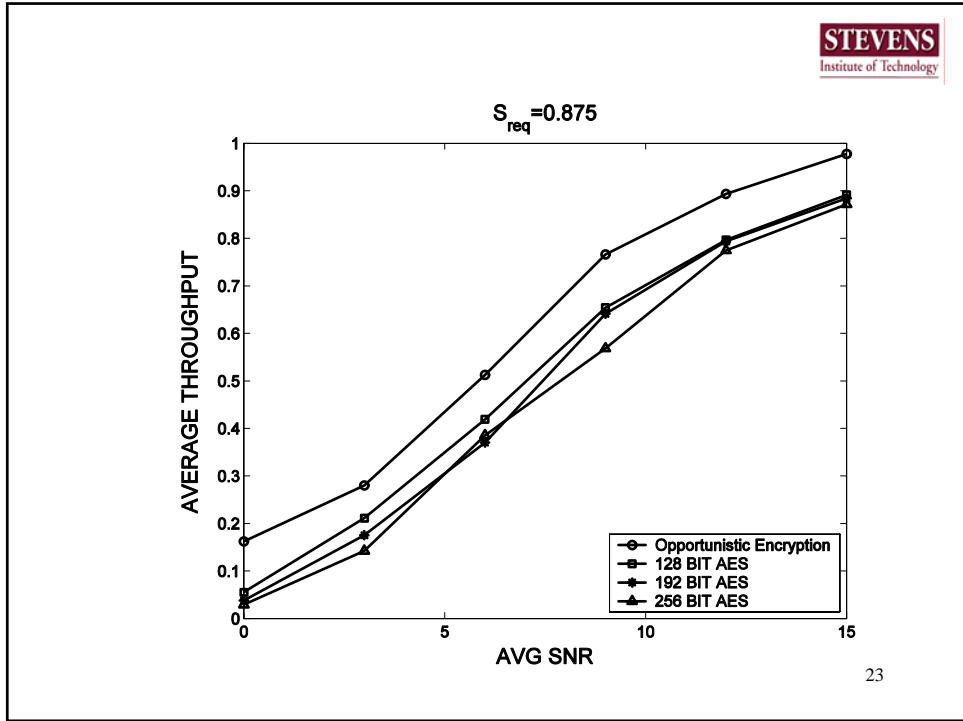
21

## Case 2: Average Channel SNR Known

- Define cost function:  $C(\gamma, N) = (1 - \lambda)D(\gamma, N) + \lambda S(N)$
- Rijndael cipher;  $N = \{128, 160, 192, 224, 246\}$
- Average SNR = 7dB.
- Min. sec. = 0.875 (~128bit key)



22



### Case 3: Finite State Markov Channel Model

- Channel SNR is quantized to finite set of states.
- Channel jumps from one state to another as a Markov process.
- Each state corresponds to a range of bit error rates.
- State transition probabilities are functions of various physical layer parameters.

25

### A Markov Decision Process (MDP) Model (I)

- Define state of the MDP as:  $\{(c_s, b_t), s = 1 \dots r; t = 1 \dots q\}$
- r-number of channel states.
- q-capacity of receiver buffer.
- Assume ACK/NAK sent to transmitter.
- $Q_n$ : set of available encryption block lengths (action set).  $|Q_n| = k$ .
- Buffer occupancy:  $b_t = \sum_{a=1}^k m_a N_a$   
where  $m_a$  blocks of lengths  $N_a$  were successfully transmitted.

26

## A Markov Decision Process (MDP) **STEVENS** Institute of Technology

### Model (II)

- MDP state transition probability:

$$P_{ij}(a) = P(c(n+1) = c_{s_j}, b(n+1) = b_{t_j} \mid c(n) = c_{s_i}, b(n) = b_{t_i}, a)$$

- Reward function of MDP:

$$r(i, a) = b_i + N_a(1 - P_{bl,a}(c_{s_i}))$$

- Bellman's equation (dynamic program):

$$v_{\alpha,T}(i) = \max_a \{r(i, a) + \alpha \sum_j P_{ij}(a) v_{\alpha,T-1}(j)\}$$

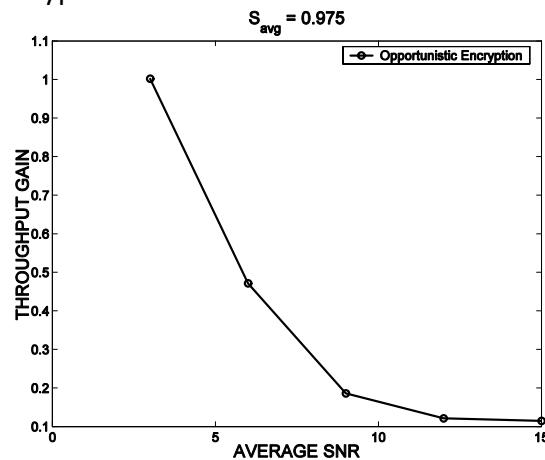
$v_{\alpha,T}(\cdot)$ : Optimum function value T steps into future

$0 < \alpha < 1$ : discount factor

27

## Throughput Gain **STEVENS** Institute of Technology

- $N_a = \{128, 160, 192, 224, 256\}$
- $r = 8$  (no. of channel states)
- $T = 1000$ ;  $\alpha = 0.5$
- Fixed encryption uses 224 bit block



28

## Conclusions

- Link state adaptive encryption (opportunistic encryption) results in significant throughput increase for a wide range of channel SNR.
- Opportunistic encryption performs well with varying degrees of side information about the channel conditions.
- Provides a framework to model security vs. throughput trade-off.