

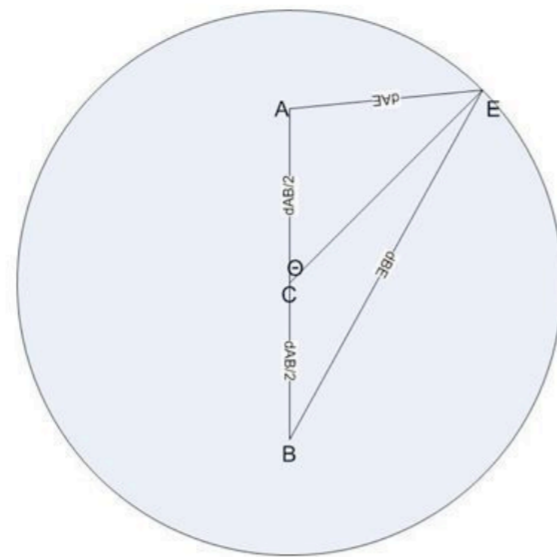
# Randomization for Security In Half-Duplex Two-Way Gaussian Channels

Aly El Gamal, Moustafa Youssef, and Hesham El Gamal



## System Model

- BPSK Encoding
- Free space path loss model
- Hard Decision Decoding
- Noise effect is ignored at Eve
- **Energy-based detection at Eve**



**In BAN, Eve can't exist inside the circle**

## Randomized Feedback in One-Way Channels

- **Challenge:**
  - Eve can identify jammed symbols by measuring the received power level
- **Solution:**
  - Randomized transmit power

**Randomized Scheduling in Two-Way Channels**

## The TDM Protocol

$$R_s \geq 0.5 \max_{\beta, f_1, f_2} (\min_{\theta, \mathcal{C}} ([R_M - R_E]^+))$$

$$R_M = (1 - \beta) \left( 1 - H \left( 1 - \phi \left( \sqrt{\frac{\rho_{min}}{d_{AB}^\alpha}} \right) \right) \right)$$

$$R_E = (1 - \beta(1 - P_m) - (1 - \beta)P_f) \left( 1 - H \left( \frac{\beta P_m P_{e|m}}{1 - \beta(1 - P_m) - (1 - \beta)P_f} \right) \right)$$

**The randomized power levels limit the ability of Eve to distinguish jammed from un-jammed symbols**

## Randomized Scheduling and Power Allocation

- Each legitimate node chooses to transmit a data symbol with a defined probability of transmission independent of the other node
- Any given time interval can be
  - Silence Interval: Both transmitters are inactive
  - Only Alice's transmitter is active
  - Only Bob's transmitter is active
  - Concurrent Transmission: Both transmitters are active

**The optimal scheme must strike a balance between wasting transmission opportunities and confusing Eve**

## Achievable Secrecy Rate

$$R_{sec} \geq \max_{P_t, f} (\min_{\theta, \mathcal{C}} ([R_M - \max(R_{EA}, R_{EB})]^+))$$

$$R_M = P_t (1 - P_t) \left( 1 - H \left( 1 - \phi \left( \sqrt{\frac{\rho_{min}}{d_{AB}^\alpha}} \right) \right) \right)$$

$$R_{EA} = D_A \left( 1 - H \left( \frac{P_e^{(EA)}}{D_A} \right) \right)$$

$$R_{EB} = D_B \left( 1 - H \left( \frac{P_e^{(EB)}}{D_B} \right) \right)$$

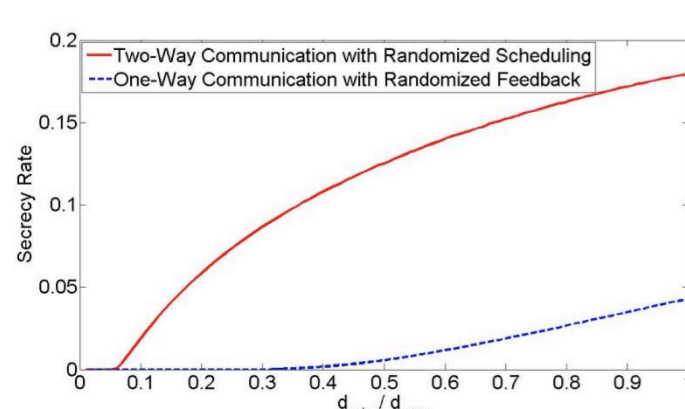
$D_A, D_B$  represent the portion of symbols classified by Eve as being transmitted by Alice or Bob respectively

**The ability of Eve to distinguish state 2 and 3 is limited for a large radius**

## TinyOS Implementation

- Using Berkeley's telosb nodes
- The CSMA/CA is removed from the radio stack to allow for concurrent transmission
- TinyOS 2.x allows access to the CC2420 RSSI register during reception of a packet
- The eavesdropper base its energy detector on the RSSI measurements at the **symbol** level
- The eavesdropper has the advantage of training its classifier on the same configuration in which it will run
- Discrete transmit power levels

## Numerical Results



**Experiment 1**      **Experiment 2**

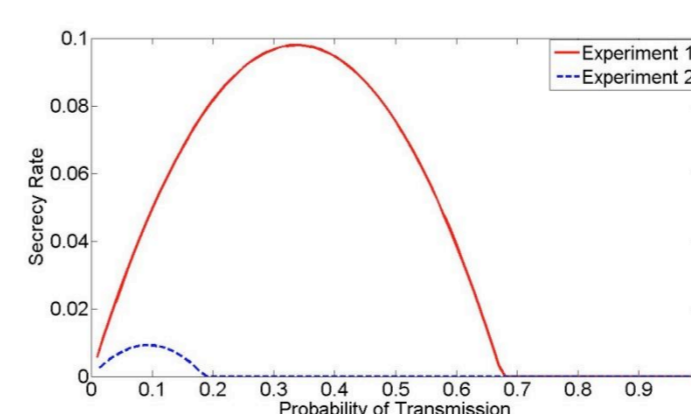
$d_{AB} = 1 \text{ ft}$        $d_{AB} = 19 \text{ ft}$

$d_{AE} = 20 \text{ ft}$        $d_{AE} = 1 \text{ ft}$

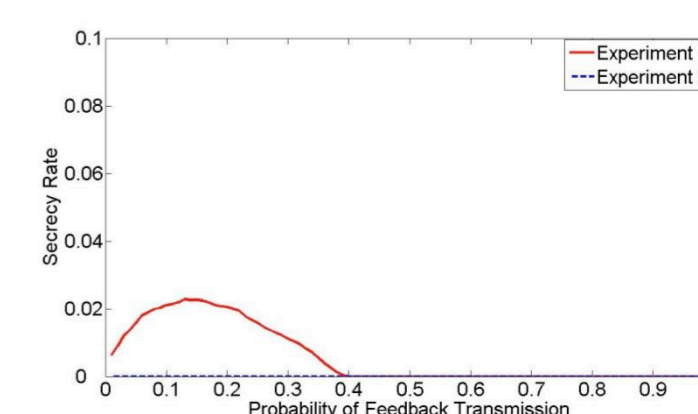
$d_{BE} = 20 \text{ ft}$        $d_{BE} = 20 \text{ ft}$

**Indoor Environments  
with few scatterers**

## Experimental Results



Two-Way Protocol



TDM Protocol