

# Using Wormholes for Timely Data Delivery under DoS Attacks in Sensor Networks

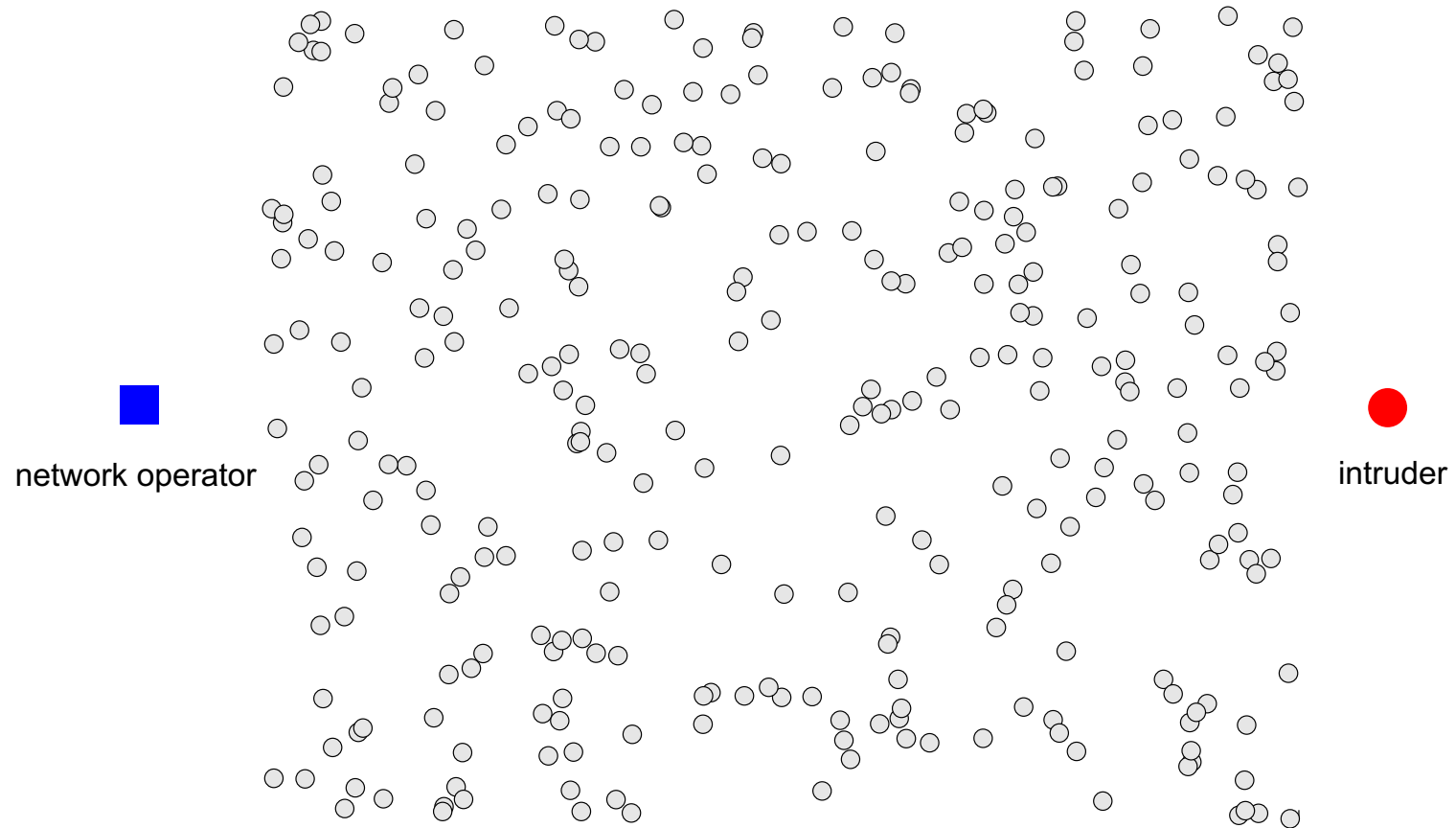
Mario Čagalj<sup>1</sup>      Srđan Čapkun<sup>2</sup>  
Jean-Pierre Hubaux<sup>1</sup>

<sup>1</sup>LCA-IC-EPFL

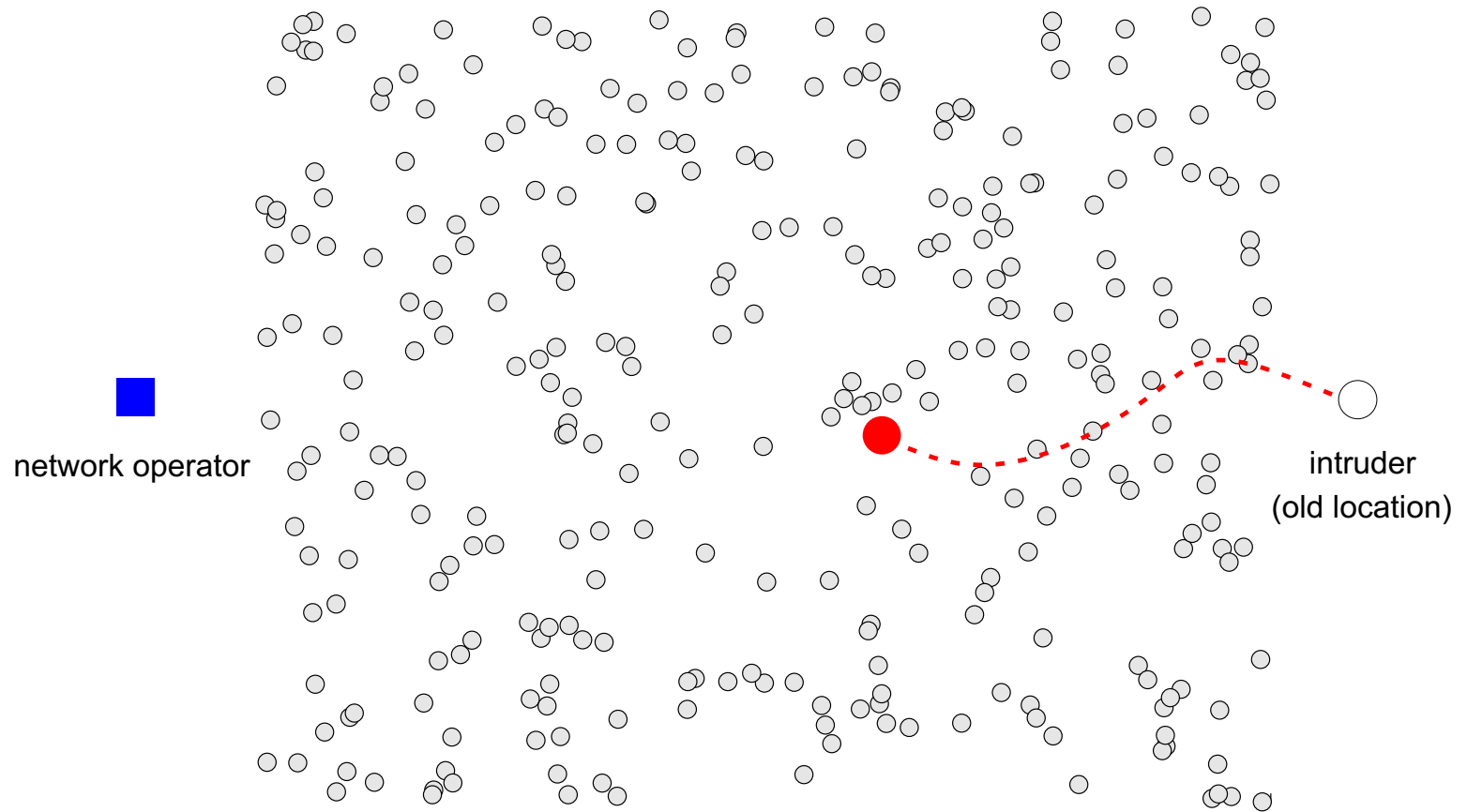
<sup>2</sup>Informatics and Mathematical Modelling Department  
Technical University of Denmark

NCCR MICS / September 22, 2005

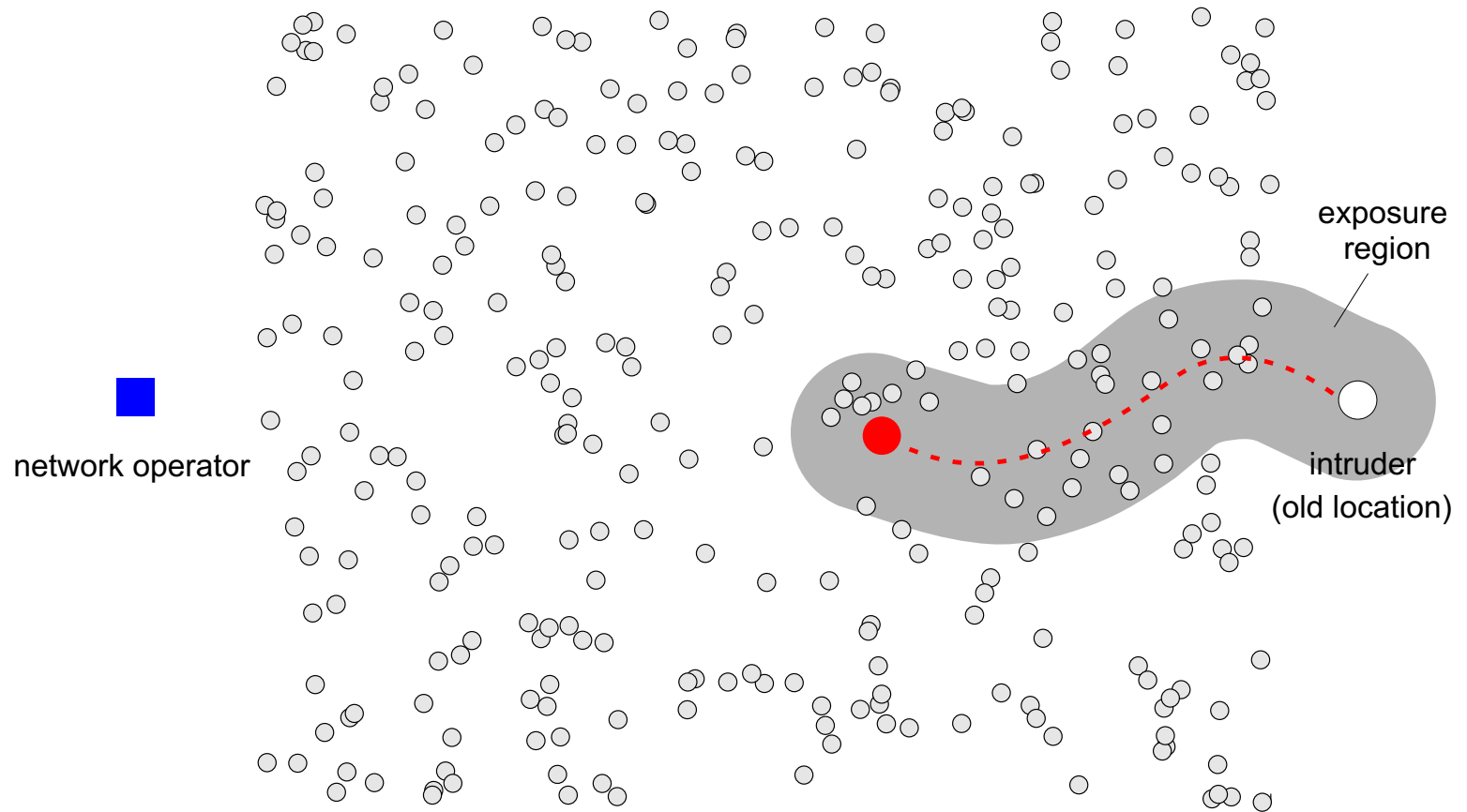
# Motivation



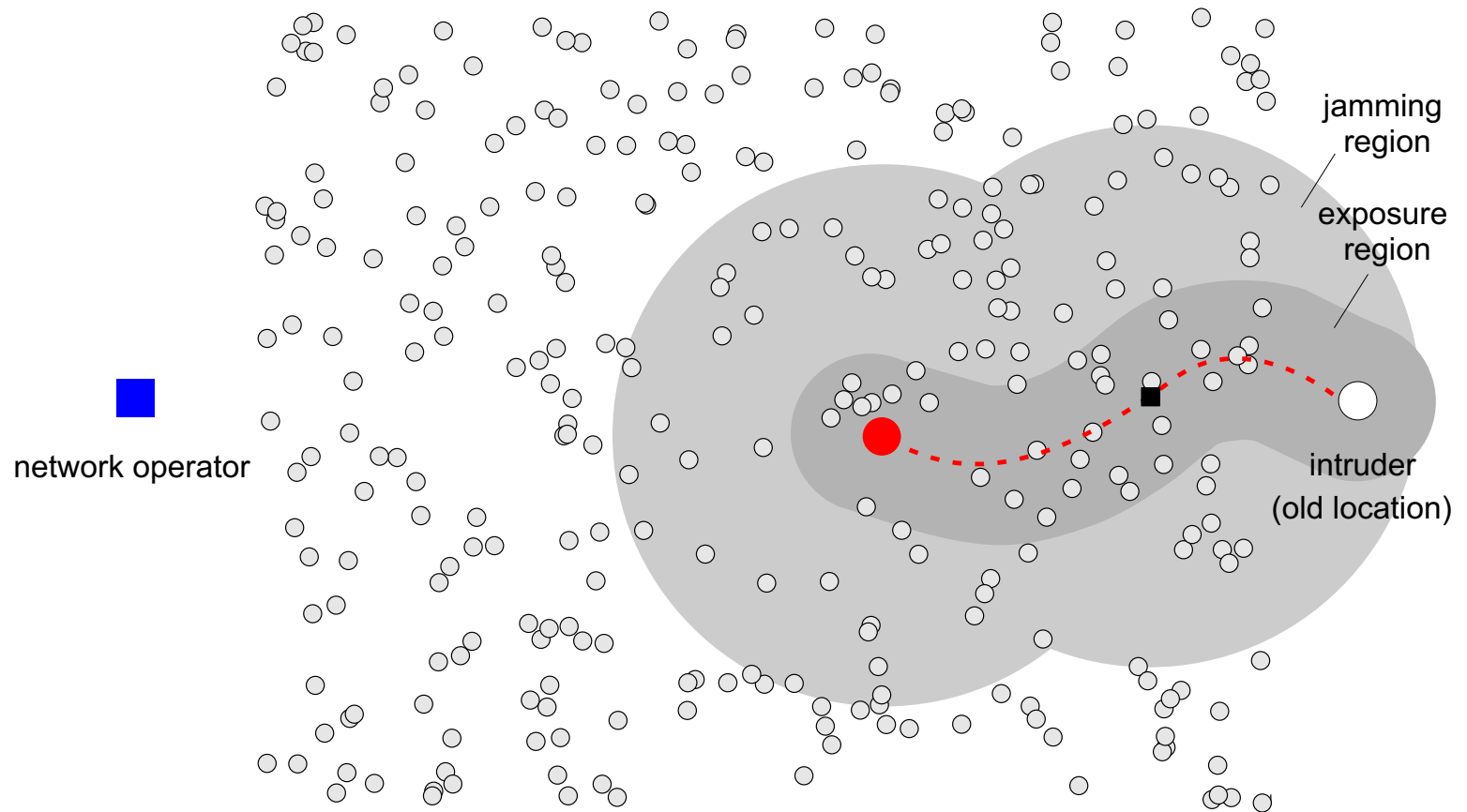
# Motivation



# Motivation

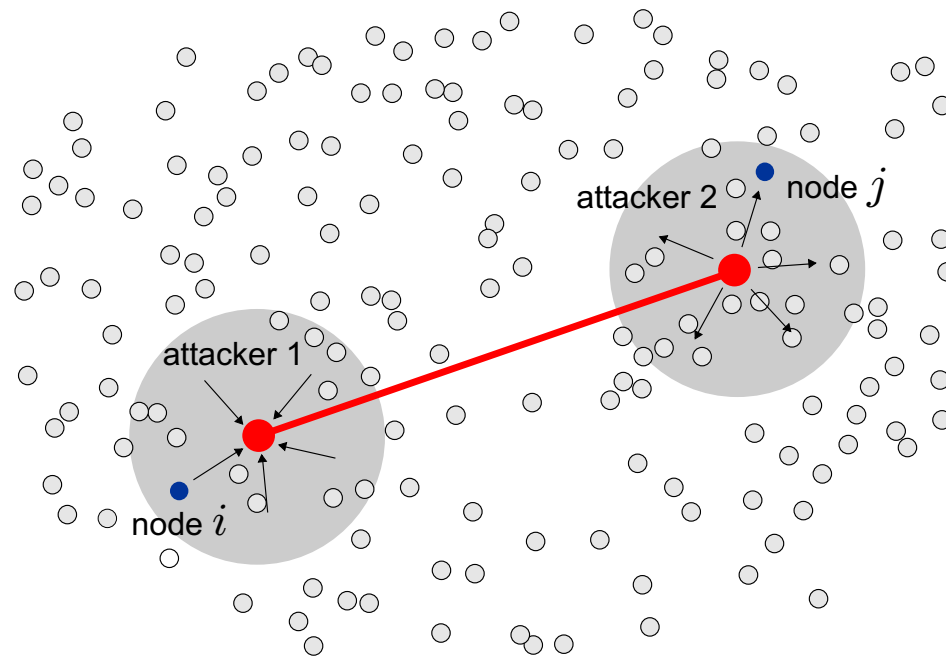


# Motivation



# Wormhole Attacks (Hu, Perrig and Johnson)

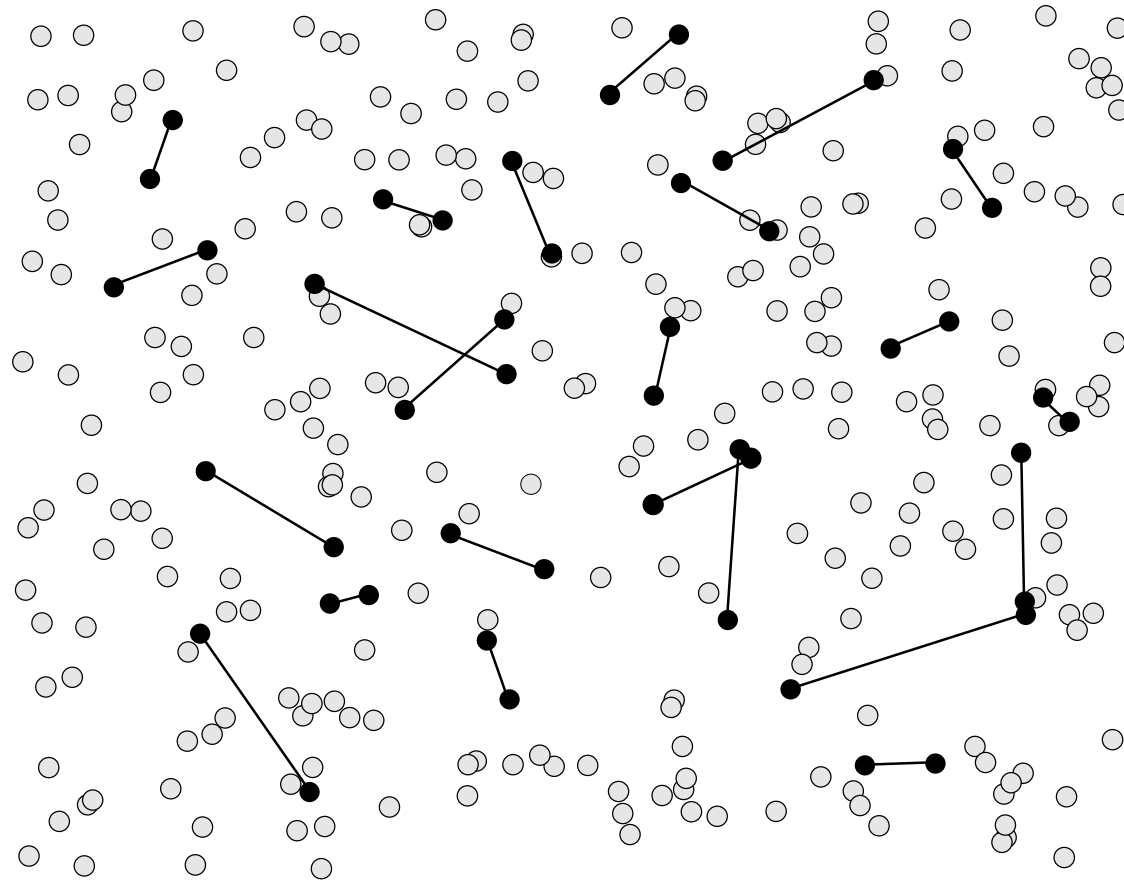
- Attacker's goal is to disrupt routing information by creating shortcuts in the network



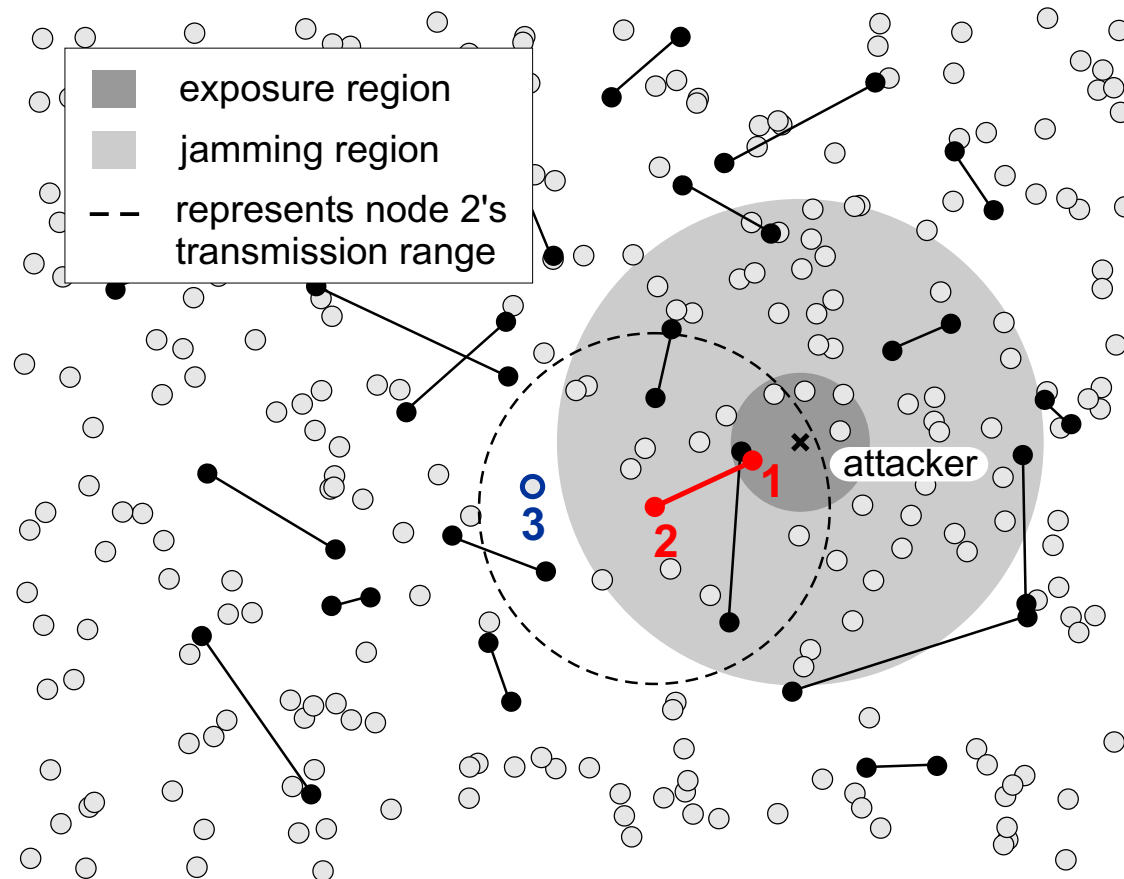
# Wormholes as a Defense Mechanism

- **Main idea:** form wormholes (links resistant to jamming) from the exposure region to the region not affected by jamming
- We study three approaches to realize wormholes
  - **Pairs of sensor nodes connected through wire**
  - **Coordinated frequency-hopping pairs**
  - Uncoordinated channel-hopping

# Wormholes via Wired Sensor Pairs - Hybrid Sensor Network



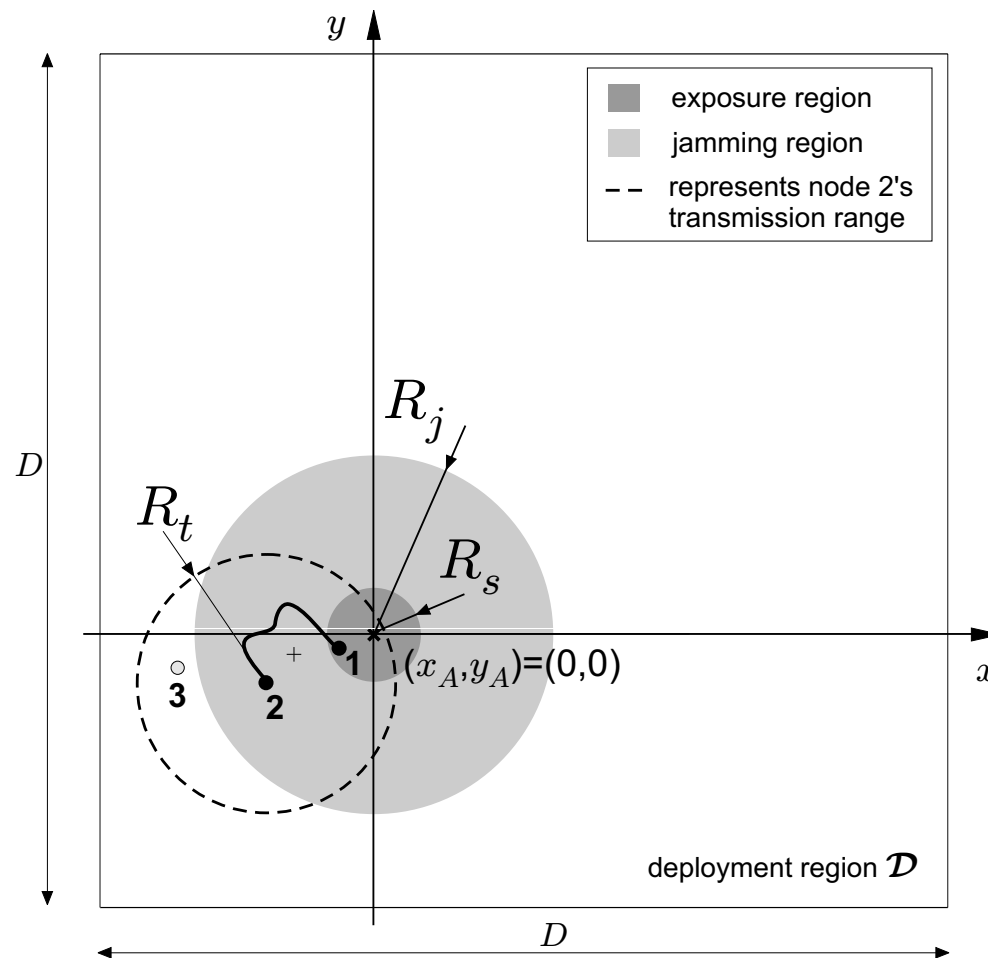
# Wormholes via Wired Sensor Pairs - Hybrid Sensor Network



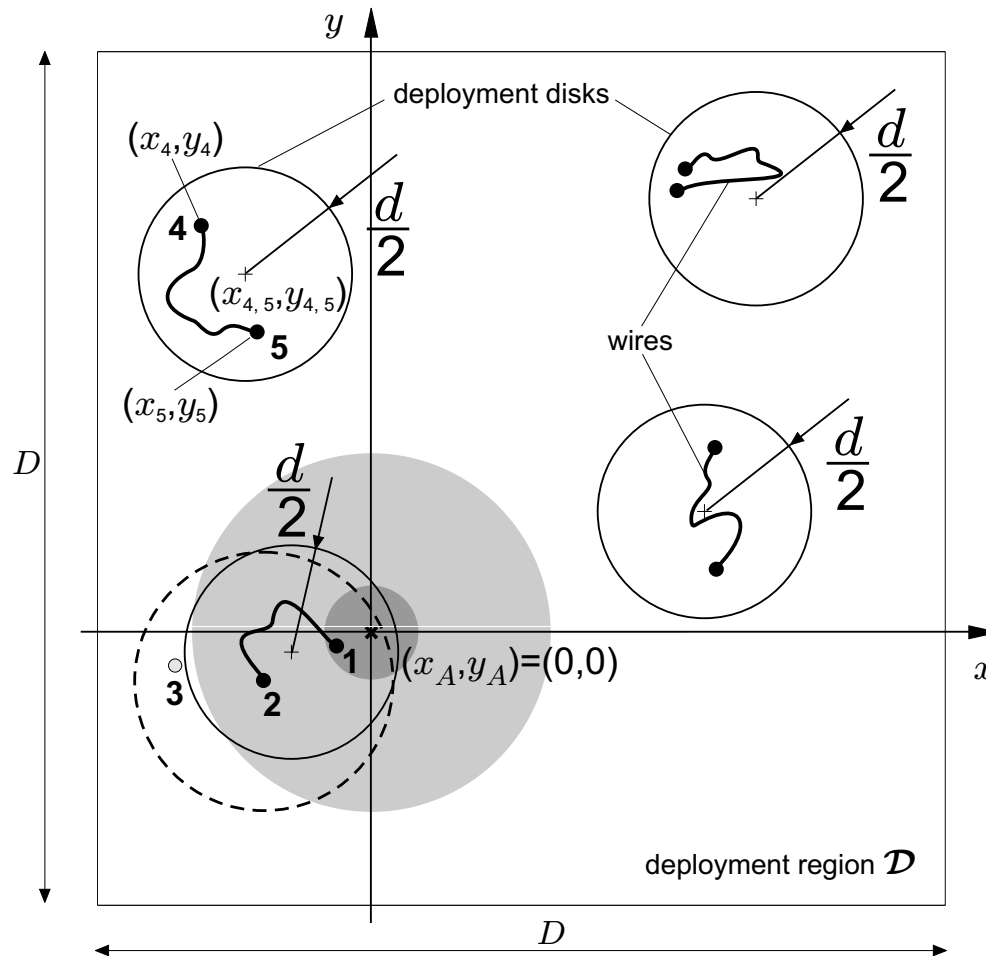
# Analysis of Wired Sensor Pairs

- Assumptions:
  - Deployment region  $\mathcal{D}$  is a  $D \times D$  square
  - Both regular nodes ( $n$ ) and connected pairs ( $K$ ) deployed independently and uniformly at random
  - Attacker is ignorant of the locations of connected pairs
- Calculate  $P[\text{at least one wormhole} | (x_A, y_A)]$ , where  $(x_A, y_A)$  is the location of the attacker

# Geometry Used in the Analysis



# Geometry Used in the Analysis



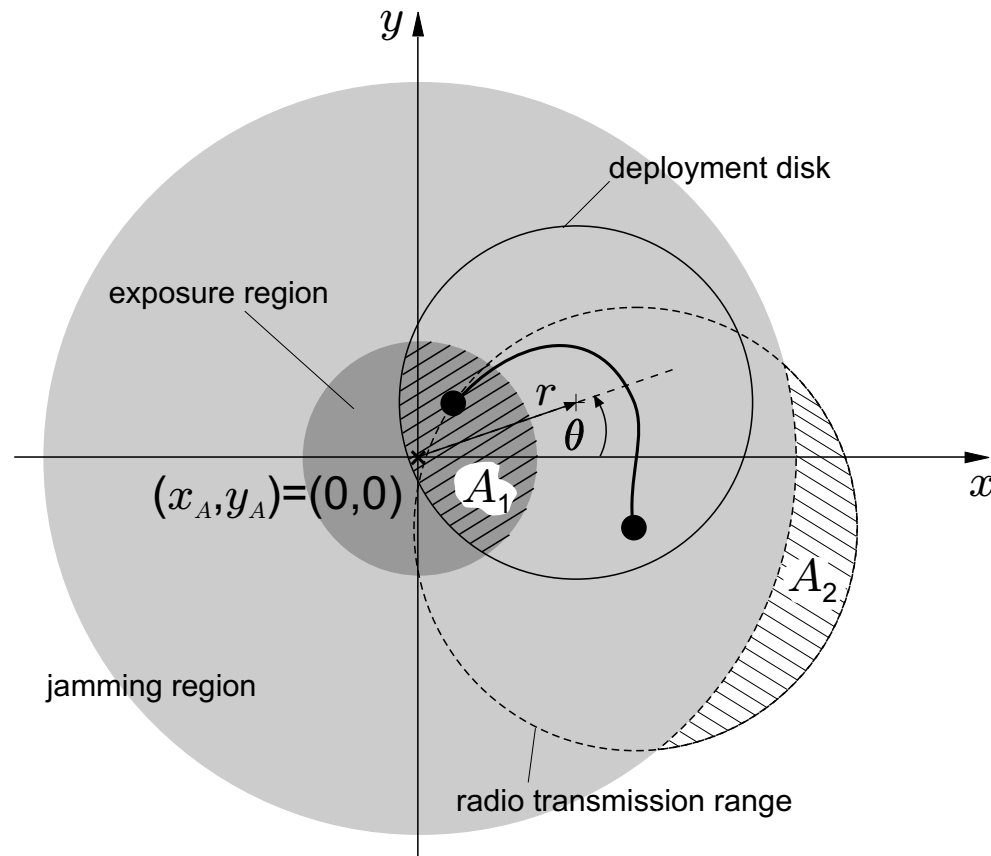
## Analysis contd.

- Define  $S \equiv \{\text{a given connected pair forms a wormhole from the exposure region around } (x_A, y_A) \text{ to the area not affected by jamming}\}$
- Let  $p_s = P[S]$ , then, by the independence assumption:

$$P[\text{at least one wormhole} | (x_A, y_A)] \approx 1 - e^{-Kp_s}$$

$$\text{Critical number of wired pairs} \approx \frac{\ln(1 - p_w)}{p_s}$$

# Calculation of probability $P[S]$ (1/2)



## Calculation of probability $P[S]$ (2/2)

$$\begin{aligned} P[S] &= \iint_{(x,y) \in \mathcal{D}} P[S | \mathbf{P}_{k,l} = (x, y)] f_{\mathbf{P}_{k,l}}(x, y) dx dy \\ &= \frac{1}{D^2} \iint_{\substack{r \in [\underline{r}, R_s + \frac{d}{2}] \\ \theta \in [0, 2\pi]}} P[S | \mathbf{P}_{k,l} = (r \cos \theta, r \sin \theta)] r dr d\theta , \end{aligned}$$

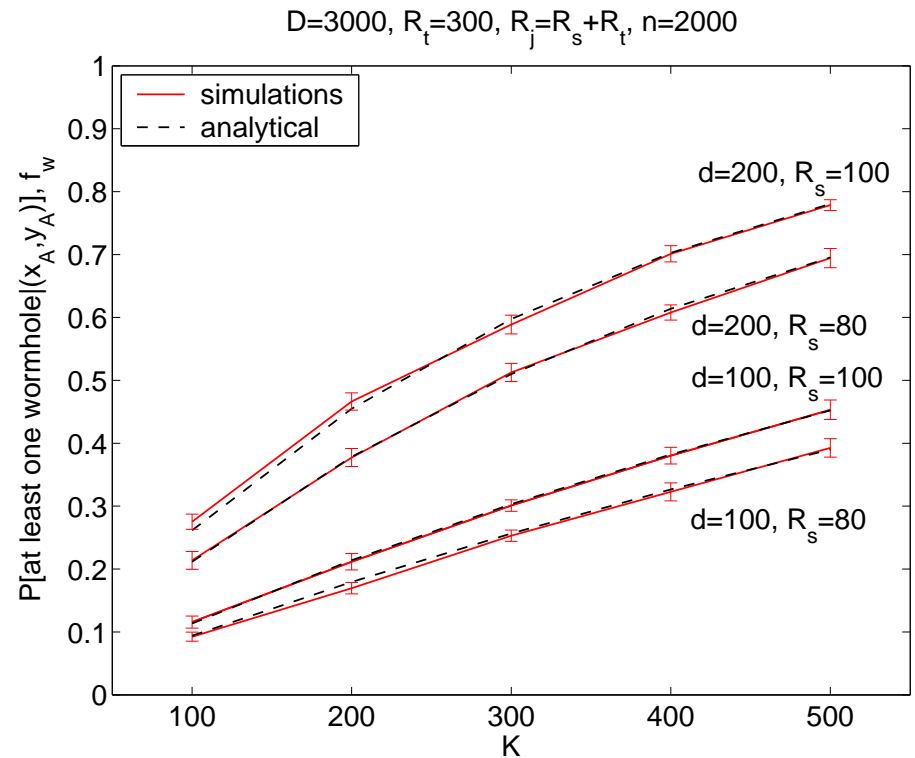
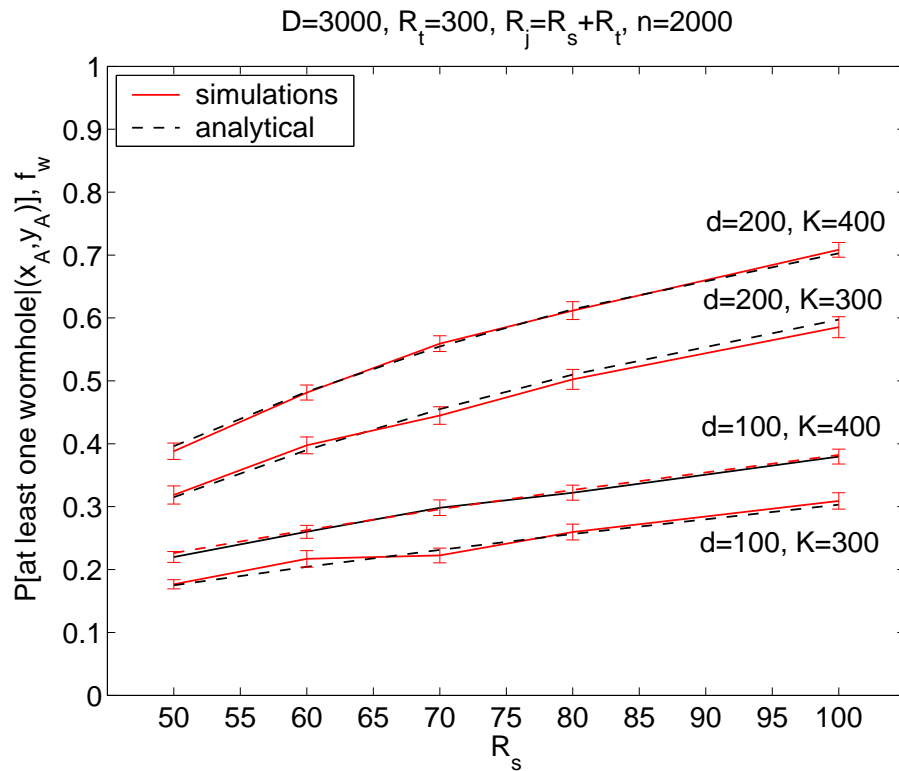
where:

$$P[S | \mathbf{P}_{k,l} = (r, \theta)] \approx \frac{32 |A_1(r)|}{(d^2 \pi)^2} \iint_{(x,y) \in \bar{A}_1(r, \theta)} \left( 1 - e^{-\frac{n |A_2(x,y)|}{D^2}} \right) dx dy$$

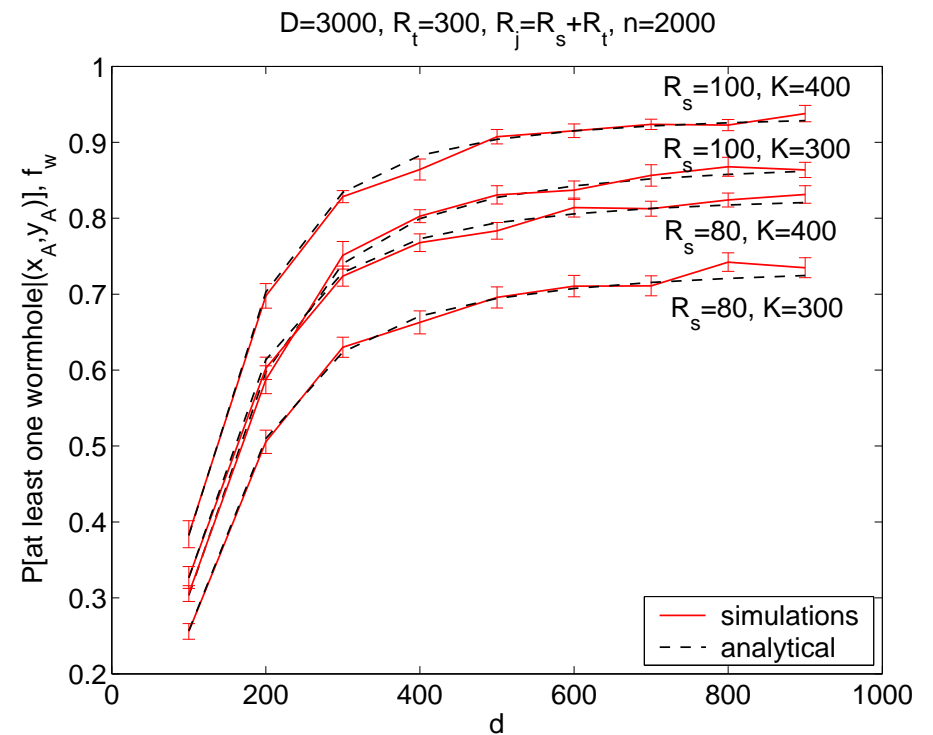
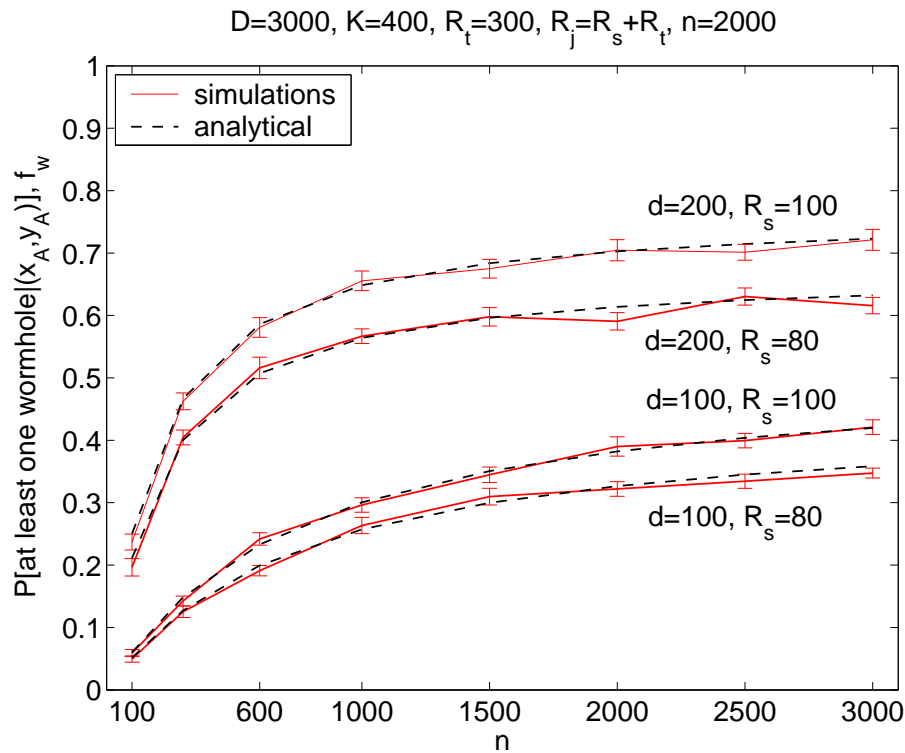
# Simulations: methodology

- Evaluate  $P[\text{at least one wormhole} | (x_A, y_A)]$ , assuming  $R_j = R_s + R_t$ 
  - For each different value of  $K, R_s, n$  and  $d$ , generate a random topology with  $n$  regular nodes and  $K$  pairs
  - Throw randomly  $N = 500$  jamming regions (disk of radius  $R_j$ ) in  $\mathcal{D}$
  - Count the number  $n_W \leq N$  of jamming regions for which there is at least one wormhole  $\Rightarrow$  relative frequency  $f_W(N) = n_W/N$
- We average the results obtained from 20 experiments and present them with 95% confidence interval

# Simulations: results (1/2)



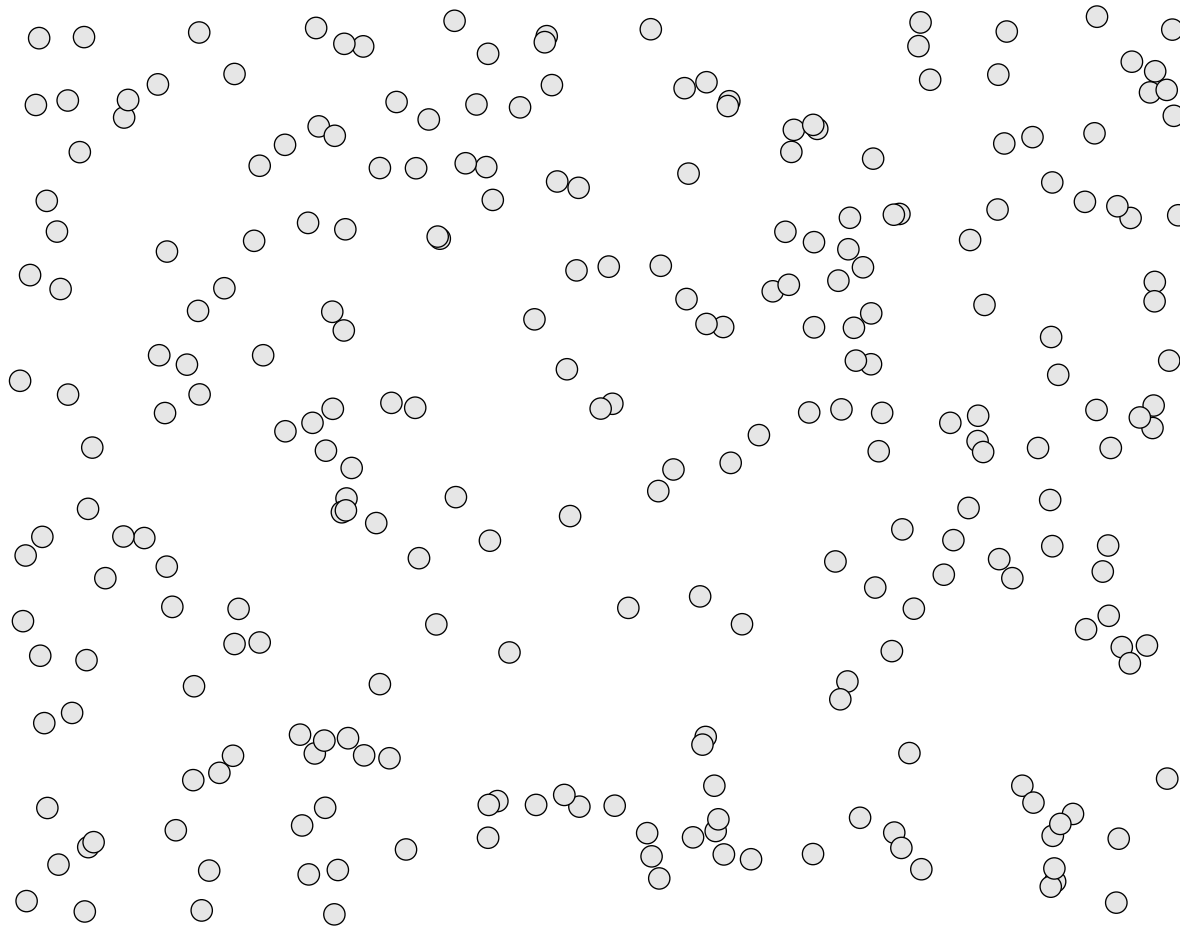
# Simulations: results (2/2)



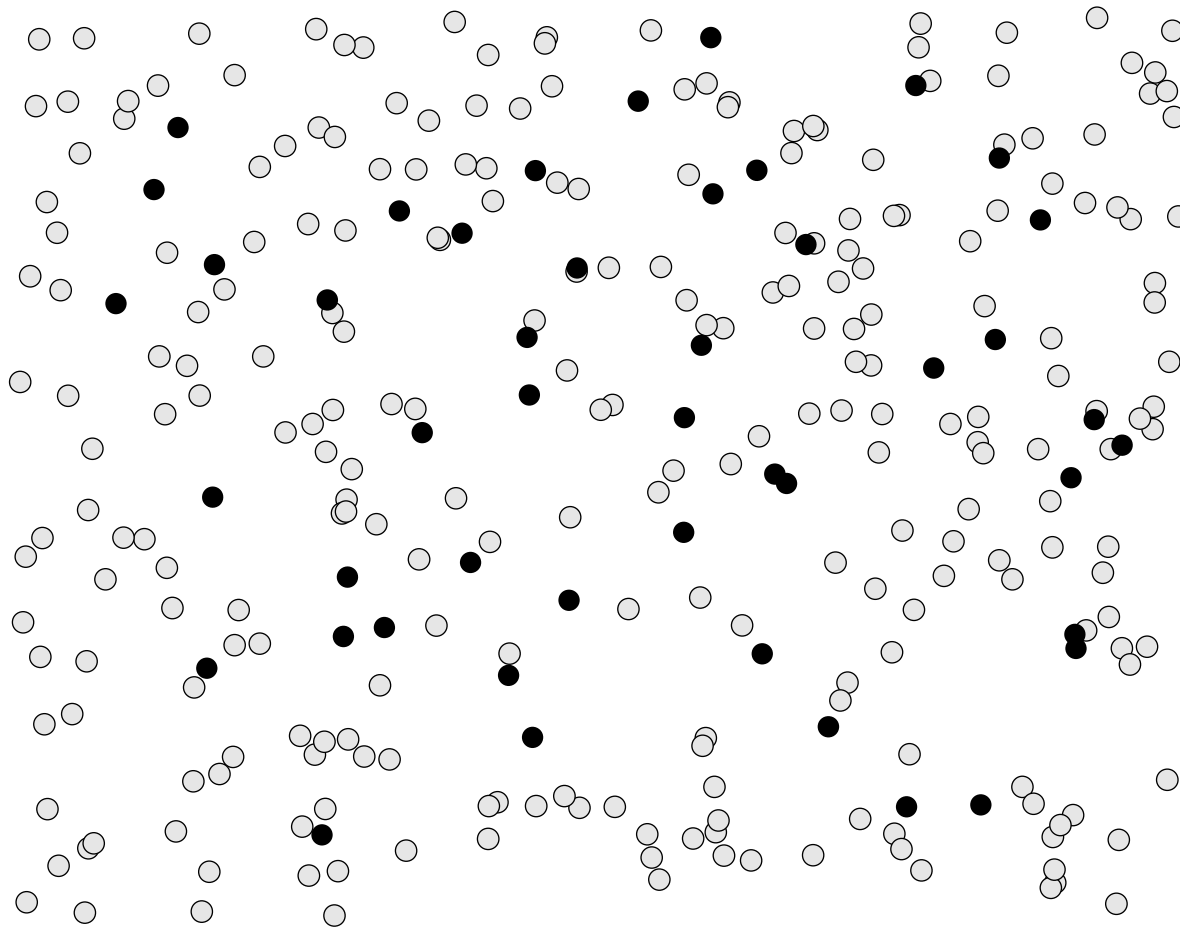
# Wormholes via Coordinated Frequency-Hopping (FH) Pairs

- Wired Sensor Pairs may be suboptimal
- Coordinated FH Pairs is an alternative approach
  - Deploy a certain number of FH enabled nodes (e.g., Bluetooth)
  - FH enabled nodes create FH pairs through wireless links resistant to jamming
  - FH node restricted to be member of at most one FH pair - to reduce the synchronization overhead
  - We do not propose multihop communication over multiple FH enabled nodes

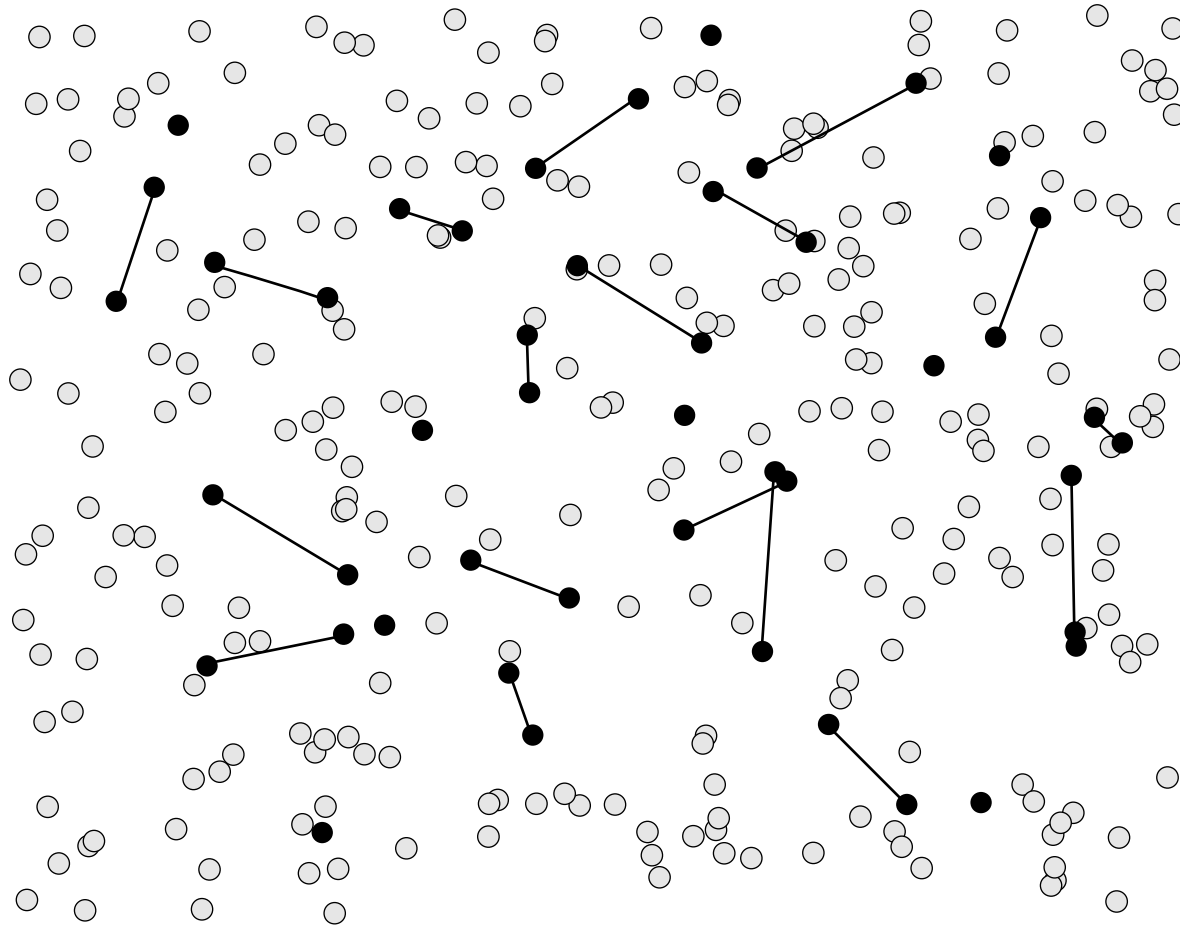
# Opportunistic FH Pairing



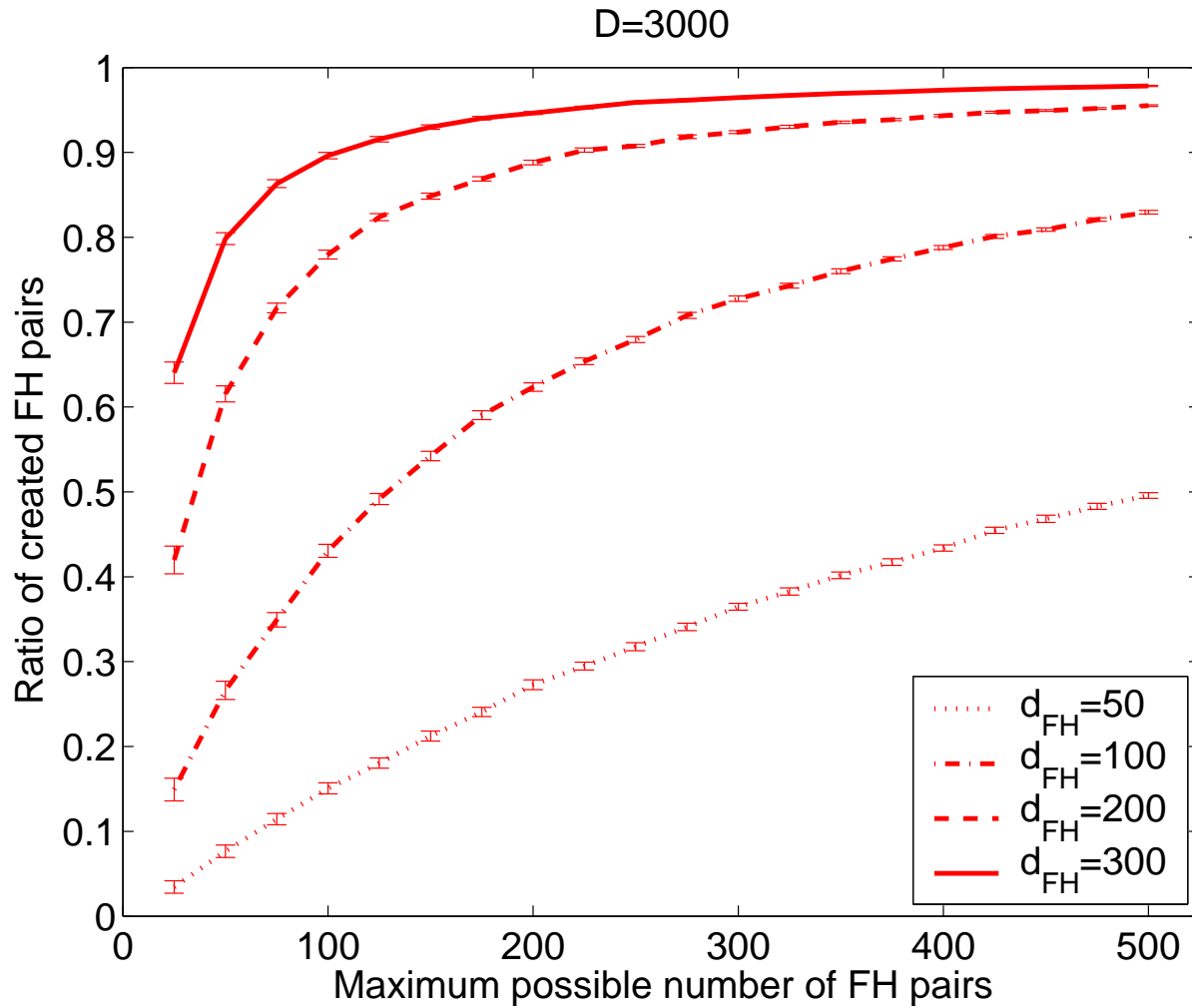
# Opportunistic FH Pairing



# Opportunistic FH Pairing



# Ratio of Created FH Pairs



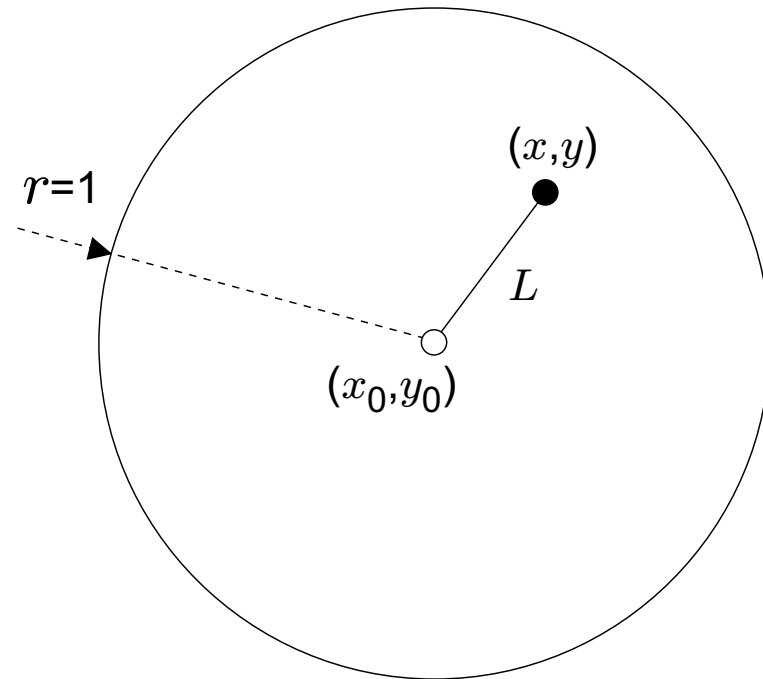
# Modelling Opportunistic FH Pairing Process - Hypothesis

- Picking a random point from the unit disk

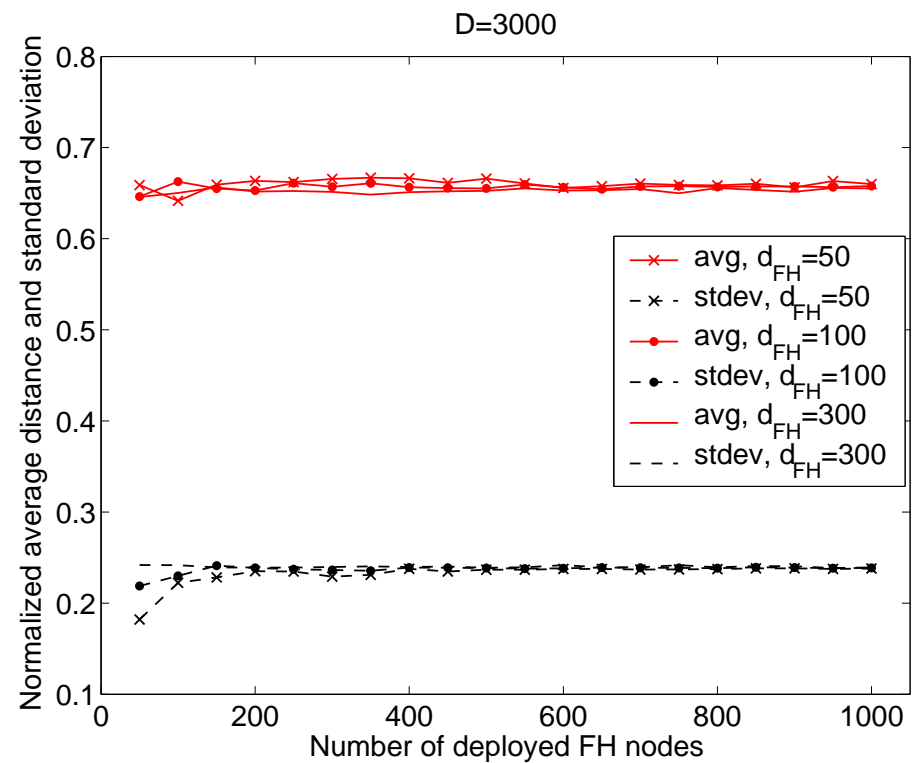
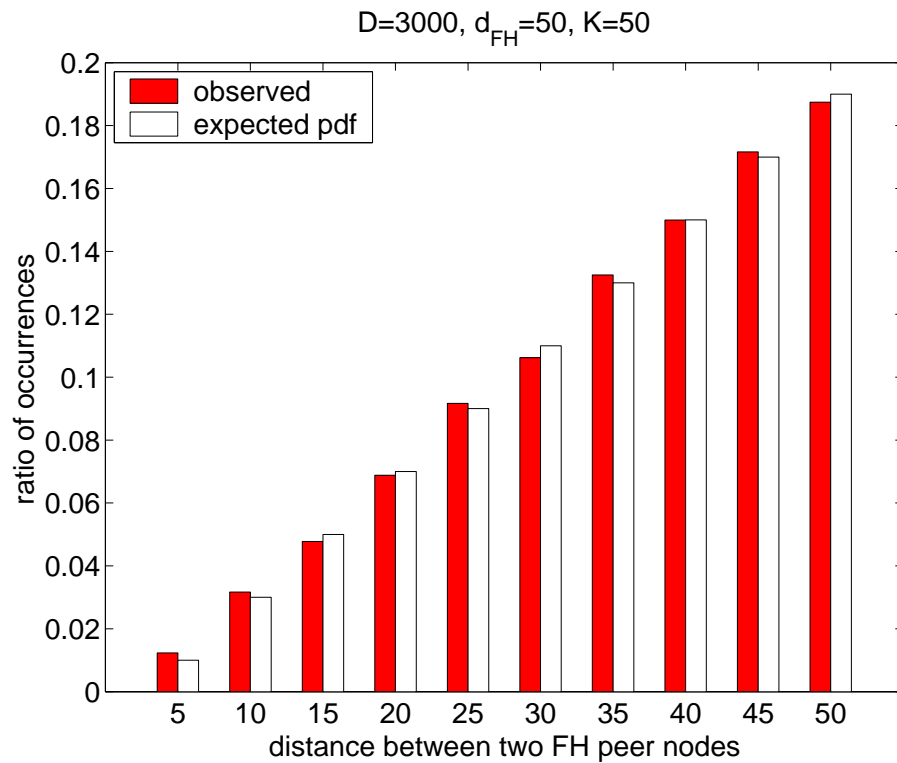
$$f_L(x) = \frac{2x\pi}{r^2\pi} = 2x$$

$$E[L] = \int_0^1 x f_L(x) \approx 0.66\bar{6}$$

$$STD[L] \approx 0.2357$$



# Modelling Opportunistic FH Pairing Process - Hypothesis Validation



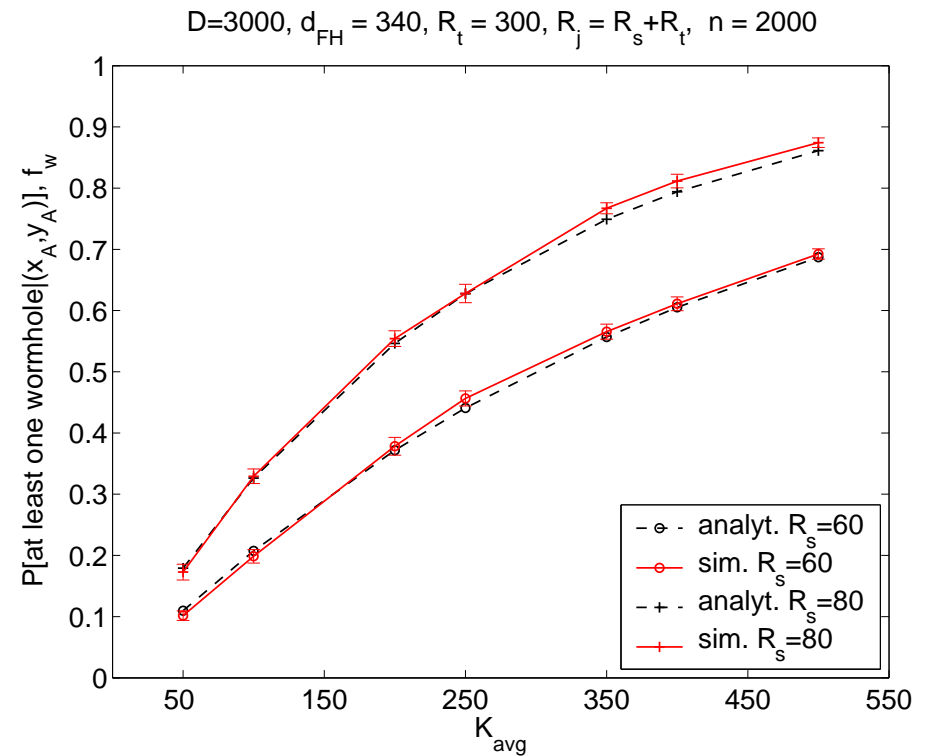
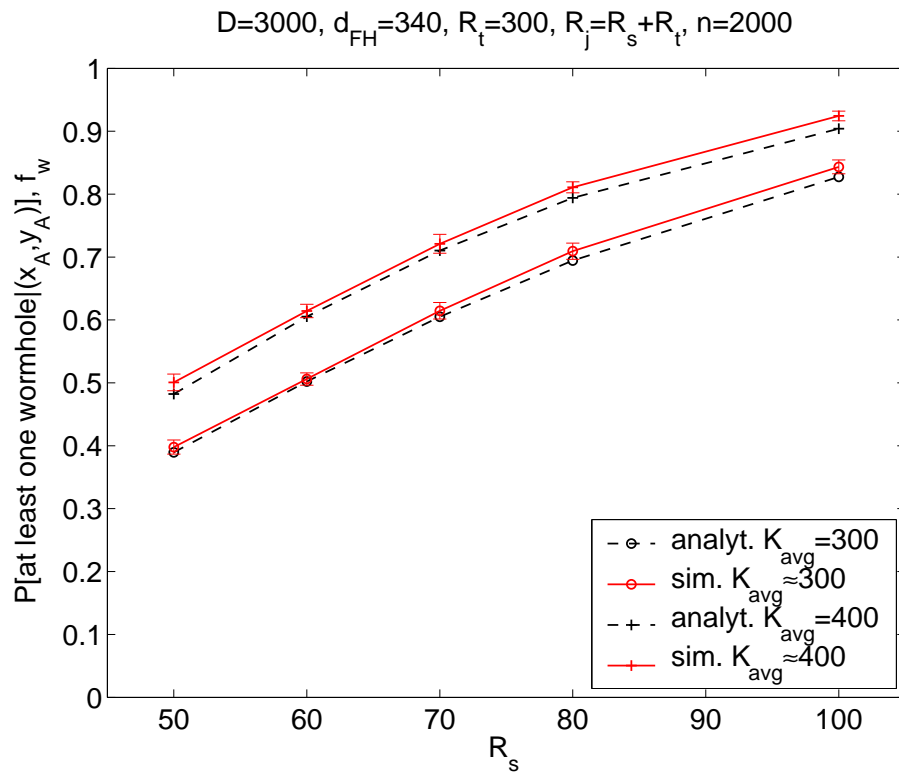
# $P[\text{at least one wormhole} | (x_A, y_A)]$ with FH Pairs

- Random point picking model  $\Rightarrow$  created FH pairs are independent
- For  $n_{FH}$  deployed FH enabled nodes and FH radio range  $d_{FH}$  we have:

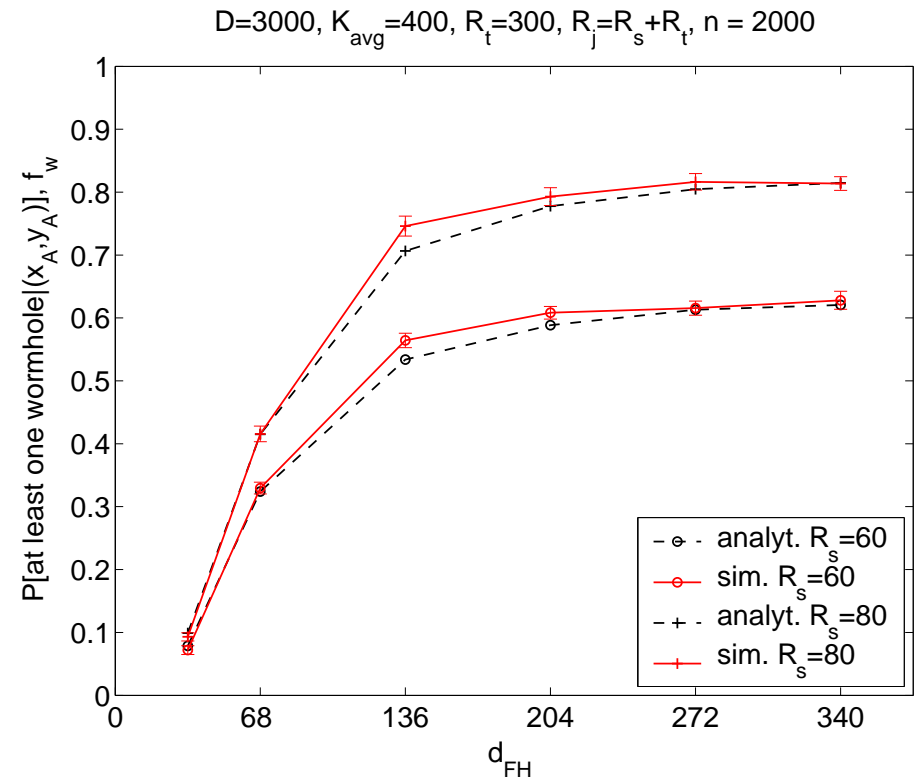
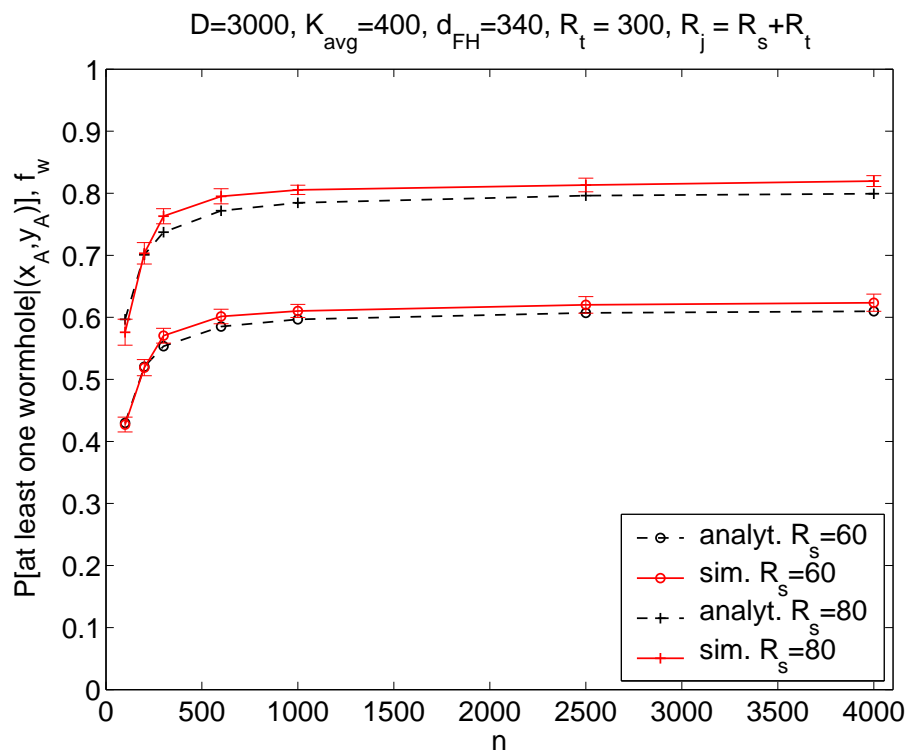
$$P[\text{at least one wormhole} | (x_A, y_A)] \approx 1 - e^{-K_{FH} \times p_s^{FH}}$$

- $K_{FH} = f(d_{FH})$  is the number of realized FH pairs out of  $2 \times n_{FH}$
- $p_s^{FH}$  is the probability that a given FH pair forms a wormhole

# Simulations and Model Validation (1/2)



# Simulations and Model Validation (2/2)



# Conclusion and Future Work

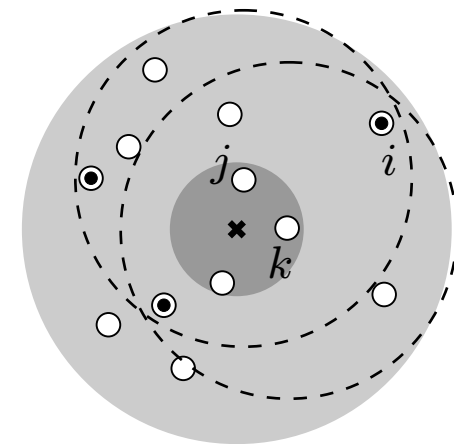
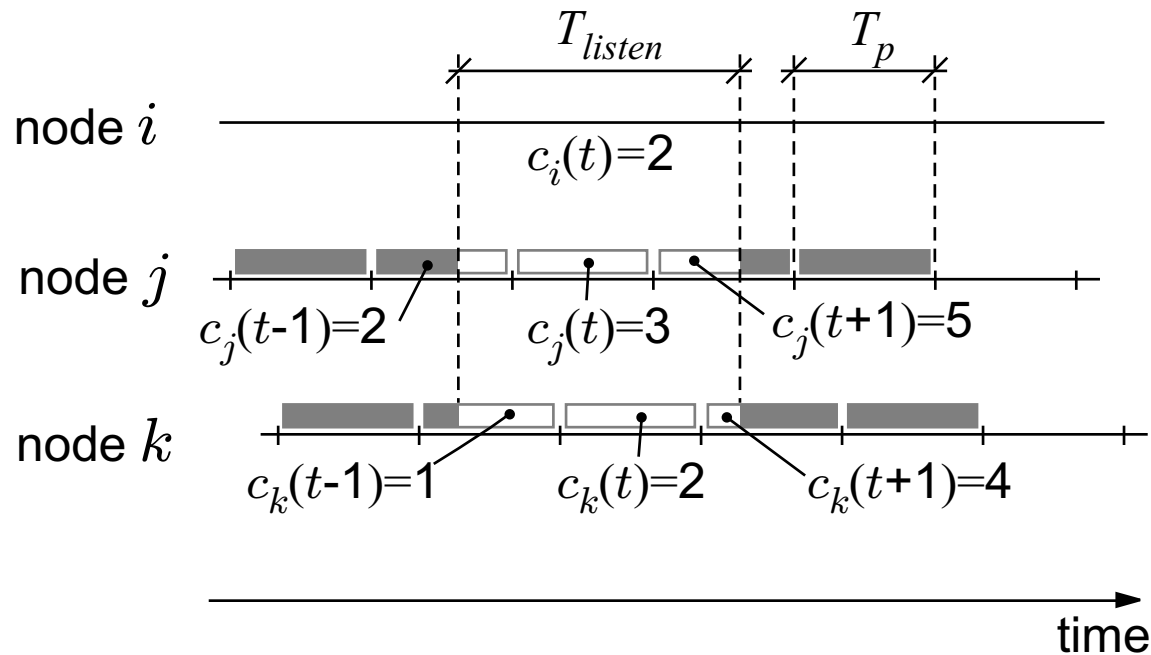
- Security should be taken seriously into account if want more than mere temperature and humidity readings
- DoS attacks present a serious threat  $\Rightarrow$  coverage paradox
- We show that wormholes can be used to thwart some DoS attacks
- We propose three wormhole defense mechanisms and quantify the probability of success for each
- Many interesting open problems (e.g., hybrid solutions, implementation)



# Wormholes via Uncoordinated Channel-Hopping (CH)

- Sensors are capable of hopping between orthogonal radio channels
- Entire packet is transmitted on a single channel
- Network is augmented with a set of specialized relaying-only nodes
- No synchronization between nodes is assumed
- Many advantages (flexibility, no coordination, etc.)

# Uncoordinated CH: Rationale



- regular nodes
- ⦿ relaying-only nodes

# Uncoordinated CH: Rationale contd.

