Carnegie Mellon University
CyLab

www.cylab.cmu.edu

Designing Secure and Reliable Wireless Sensor Networks

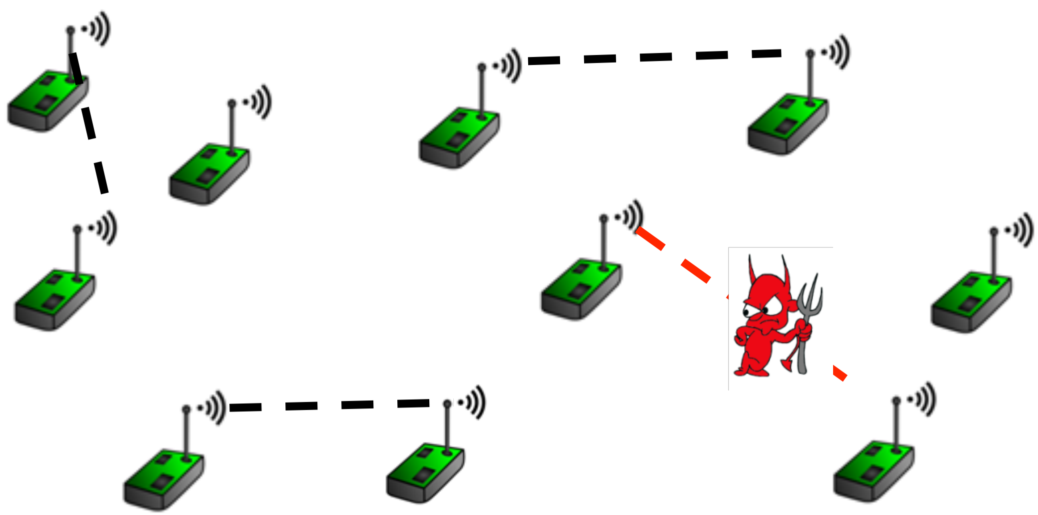
Osman Yağan

Assistant Research Professor, ECE

Joint work with J. Zhao, V. Gligor, and F. Yavuz

Wireless Sensor Networks

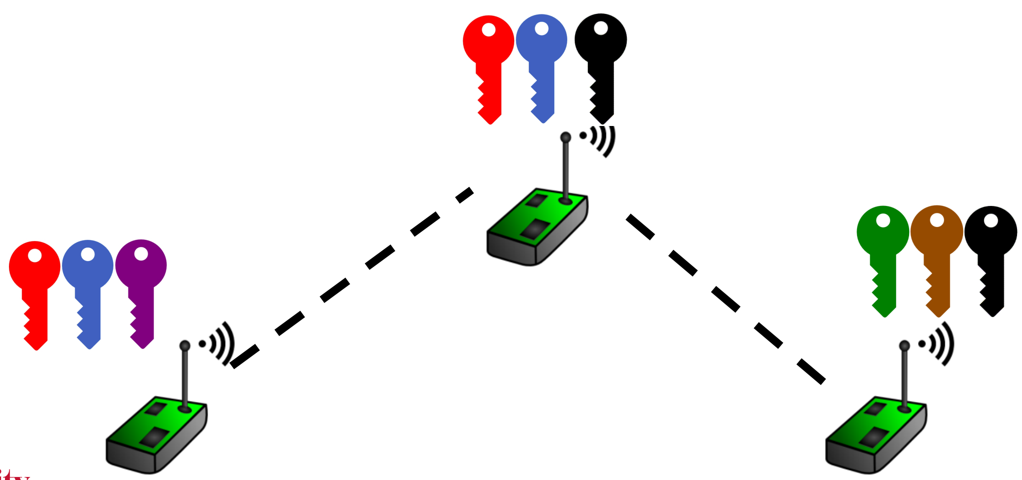
- Distributed collection of sensors: low-cost, resource-constrained, and often deployed in a **hostile environment**
- Wireless communications
  - Monitored **and** modified by an adversary
  - Cryptographic protection is needed
  - Proposed method: **Random** key predistribution (since topology is often unknown before deployment)



Random key predistribution

1. The Eschenauer–Gligor (EG) scheme [ACM CCS '02]

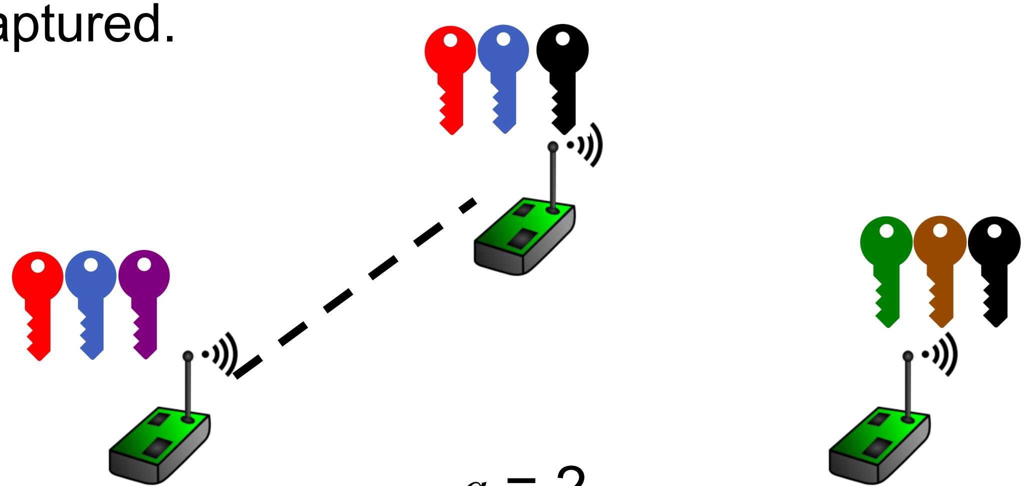
- For a network with ***n*** sensors:
  - A large pool of ***P*** cryptographic keys
  - For each sensor, sample ***K*** keys uniformly at random
  - Example values: ***n*** = 10^4 , ***P*** = 10^5 , and ***K*** = 10^2
- Two sensors can **securely** communicate over an existing wireless link if they have **at least one common key**



A simple extension of the EG scheme

2. The q-composite scheme [Chan–Perrig–Song IEEE S&P ‘03]

- Same initial construction with the EG scheme;
- For any two sensors, secure communication over an existing wireless link if they share at least ***q*** keys (***q>1***)
- **Advantage:** Improved resilience against node capture attacks when ***few*** sensors are captured → Worse than EG if a large number sensors are captured.



$q = 2$

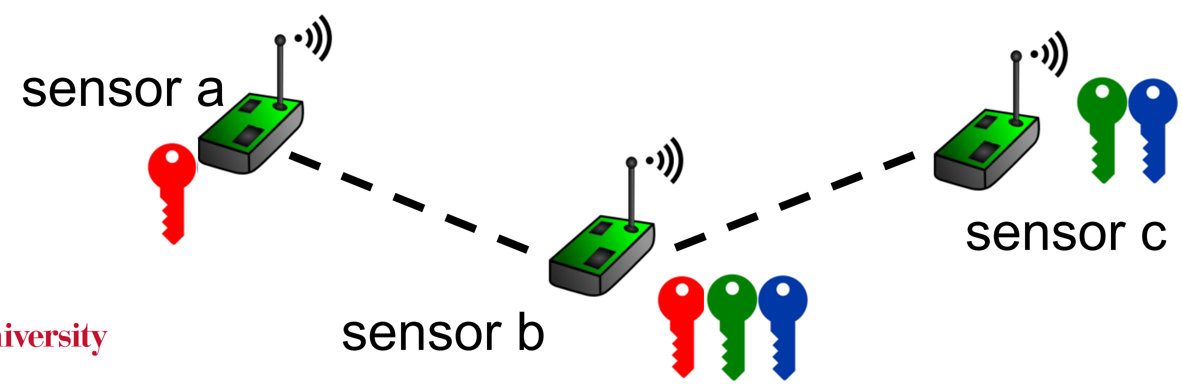
Carnegie Mellon University
CyLab

An alternative method

3. The pairwise scheme [Chan–Perrig–Song IEEE S&P ’03]

- Each sensor is paired (offline) with ***K*** distinct **nodes** which are randomly selected from amongst all other nodes.
- For each sensor and any sensor paired to it, a unique (pairwise) key is generated and assigned only to those two nodes.
- **Advantage:** Node-to-node authentication and quorum-based key revocation are possible without requiring a trusted third party.

With ***K***=*1*, *S_a={b}*, *S_b={c}*, and *S_c={b}* where *S_i* is the set of nodes selected by node *i*:



The Main Question

Given the **RANDOMNESS** involved in

- Distribution of cryptographic keys
- Physical location of sensors, due to random deployment (& **mobility)**

How do we ensure that the network has **end-to-end connectivity** that is **reliable** against

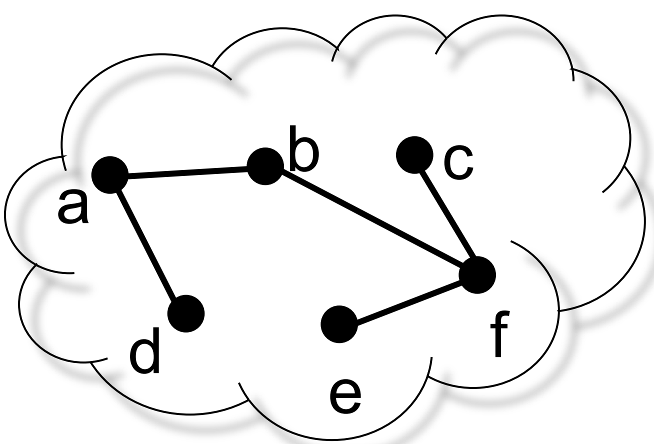
i) Sensor failures due to adversarial attacks, battery depletion, product malfunctioning; and

ii) Link failures due to sensor mobility, environmental conditions, product malfunctioning?

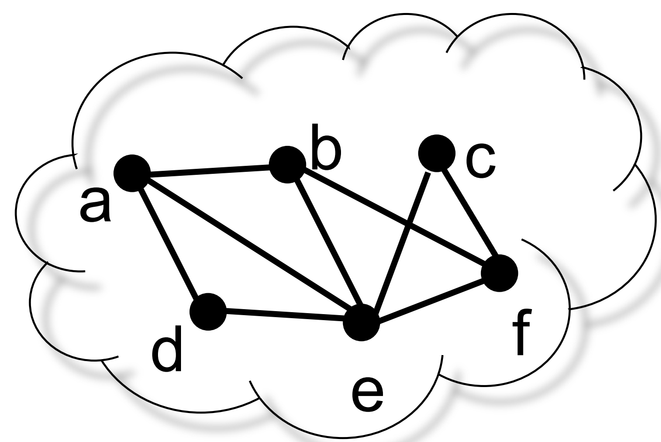
A Reliability Metric: k-connectivity

- Connectivity
  - At least 1 path between any two nodes
- *k*-Connectivity
  - At least *k* mutually disjoint paths between any two nodes
  - Equivalent definition: **Remains connected despite the removal**

  –**of any (*k*−1) nodes or edges**
  - Addtl. advantages: multi-path routing, achieving consensus, etc.



Connected



2-Connected

Our Goal

For a desired level of reliability specified by the parameter *k*,

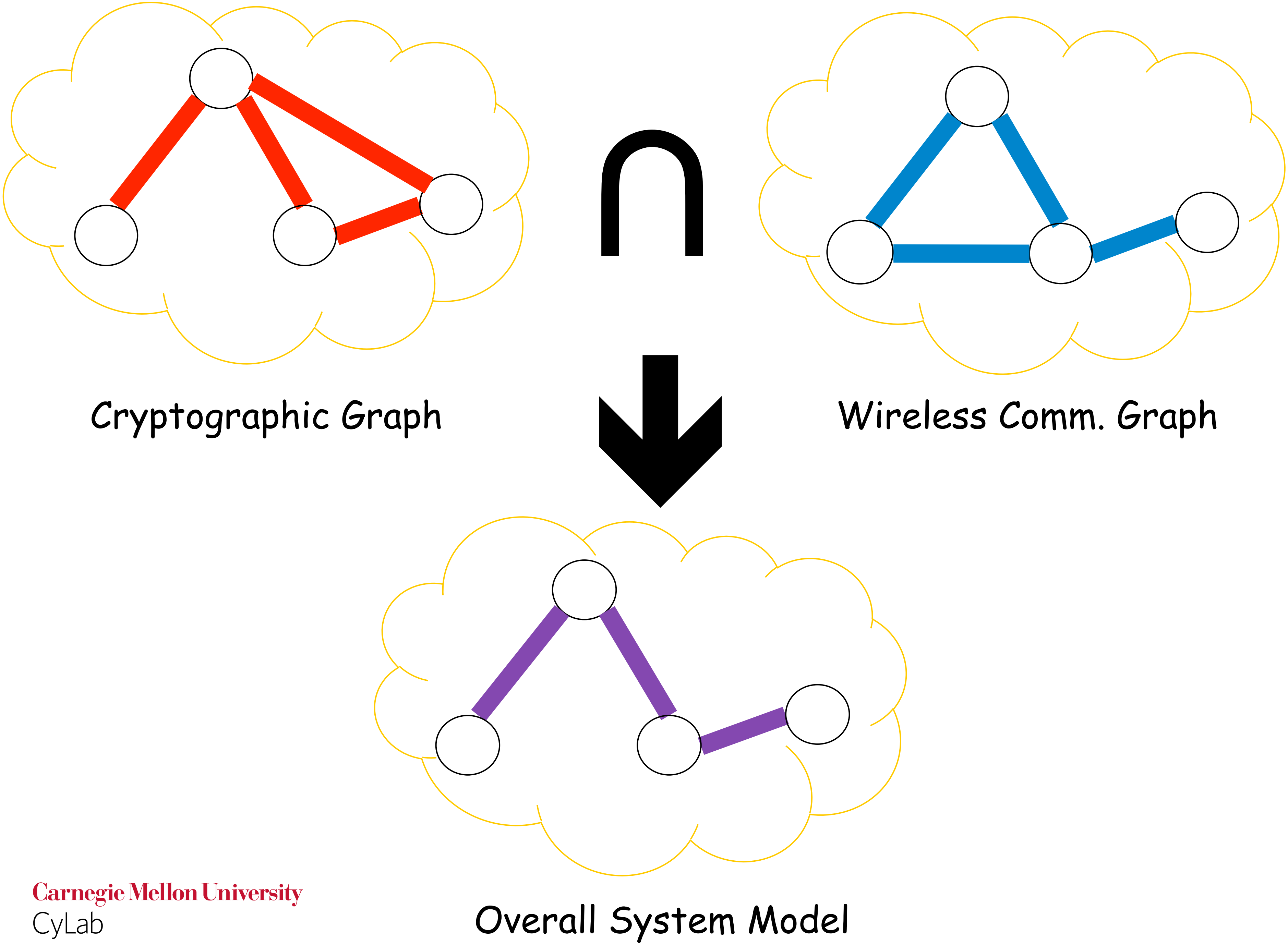
- Determine the probability that the resulting network is *k*-connected as a function of all **network parameters** involved -- This will be done under
  - i) Three key predistribution schemes, and
  - ii) Two wireless communication models

Approach: Random Graph Modeling & Analysis

Random Graph Modeling

Random Graphs = Graphs generated by a random process

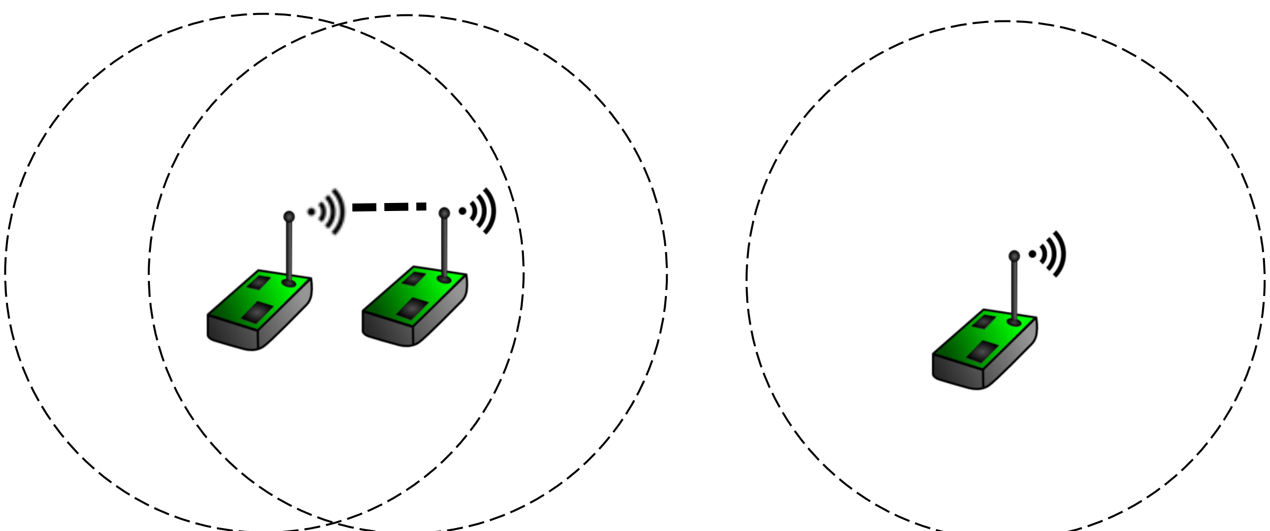
- **Communication Graph:** E.g., the disk model
  - An edge $i \sim j$ exists if $\|x_i - x_j\| \le r$ → transmission range
- **Cryptographic Graph:** Induced by the key predistribution sch.
  - An edge $i \sim j$ exists if sensors i and j have **q** keys in common. (For EG and Pairwise *q=1*)
- **System Model: Communication Graph ∩ Cryptographic Graph**
  - $i \sim j$ if $\|x_i - x_j\| \le r$ ∧ have **q** keys in common.
  - Links represent sensors that can securely communicate



Carnegie Mellon University
CyLab

Preliminary Wireless Comm. Models

- On/Off channel model
  - Each channel either on with prob. p_n or off with prob. (1–p_n)
  - Unreliable links due to barriers / environments / wireless nature
- Disk model
  - Only two sensors within some distance r_n can communicate
  - Transmission range r_n is directly related to sensor transmit power



System Models to be Considered

Scheme/Comm. Model	Graph
EG scheme	Random key graph
q-composite scheme	q-composite key graph
Pairwise scheme	Random K-out graph
on/off channel model	Erdős-Rényi graph
disk model	Random geometric graph

Cryptographic Graphs

Communication Graphs

WSN	Graph
$\mathrm{WSN}^{\mathrm{EG}}_{\mathrm{on/off}}$	random key graph ∩ Erdős-Rényi graph
$\mathrm{WSN}^{\mathrm{EG}}_{\mathrm{disk}}$	random key graph ∩ random geometric graph
$\mathrm{WSN}^{q\text{-composite}}_{\mathrm{on/off}}$	q-composite random key graph ∩ Erdős-Rényi graph
$\mathrm{WSN}^{q\text{-composite}}_{\mathrm{disk}}$	q-composite random key graph ∩ random geometric graph
$\mathrm{WSN}^{\mathrm{pairwise}}_{\mathrm{on/off}}$	random K-out graph ∩ Erdős-Rényi graph
$\mathrm{WSN}^{\mathrm{pairwise}}_{\mathrm{disk}}$	random K-out graph ∩ random geometric graph

A Representative Result

- EG scheme : Random Key Graph
  - n sensors, each equipped with K_n keys selected uniformly at random from a pool of P_n keys.
  - An edge between two nodes (sensors) if and only if they share at least 1 key
  - Notation: $G_{\text{RKG}}(n, K_n, P_n)$
- On-off channel model : Erdős–Rényi graph
  - n nodes
  - An edge between two nodes appear independently with prob. p_n
  - Notation: $G_{\text{ER}}(n, p_n)$
- System Model:

$$\text{WSN}_{\text{on/off}}^{\text{EG}} = G_{\text{RKG}}(n, K_n, P_n) \bigcap G_{\text{ER}}(n, p_n)$$

Zhao, Yagan, Gligor: IT 2014

Theorem 1. For $\text{WSN}^{\text{EG}}_{\text{on/off}}$ modeled by $G_{\text{RKG}}(n, K_n, P_n) \cap G_{\text{ER}}(n, p_n)$ with $P_n \geq 3K_n$ for all n sufficiently large, let sequence α_n for all n be defined through

$$\alpha_n = n\, p_n \frac{K_n^2}{P_n} - \ln n - (k-1)\ln\ln n,$$

If $P_n = \Omega(n)$, then as $n \to \infty$,

$$P\left[\text{WSN}^{\text{EG}}_{\text{on/off}} \text{ is } k\text{-connected}\right] \to \begin{cases} \boxed{e^{-\frac{e^{-\alpha}}{(k-1)!}}, \text{ if } \lim_{n\to\infty} \alpha_n = \alpha \in (-\infty, \infty),} \\ \boxed{0, \quad \text{if } \lim_{n\to\infty} \alpha_n = -\infty,} \\ \boxed{1, \quad \text{if } \lim_{n\to\infty} \alpha_n = +\infty.} \end{cases}$$

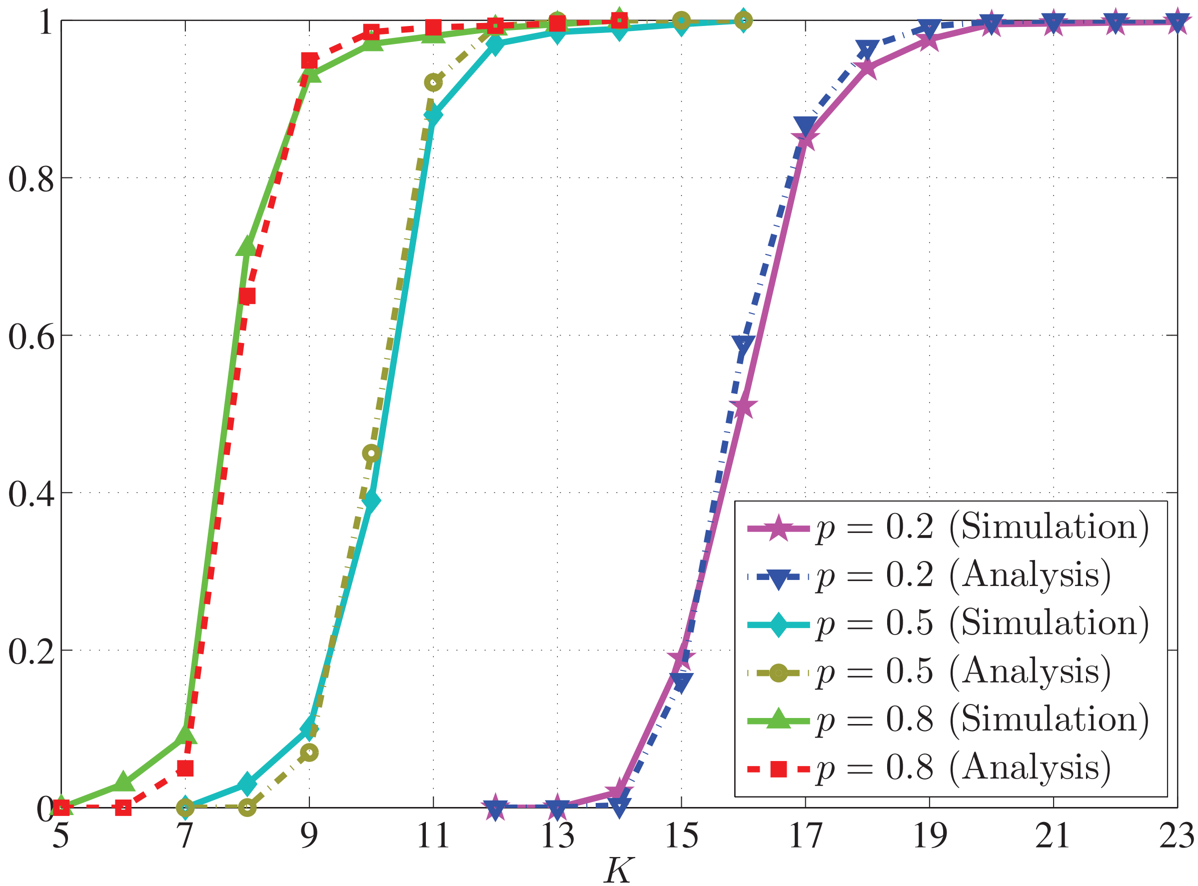
Exact prob.

A zero–law

A one–law

➢ **A precise characterization of *k*-connectivity in wireless sensor networks under the EG scheme**

Simulations with finite number of sensors



Probability that WSN is 2-connected with *n = 2,000*, *P = 10,000*

Contributions thus far

Model	**Results for *k*-connectivity**
EG scheme ∩ on/off channels	Zero-one law + Asymp. probability (ISIT 2013, IT, others in submission)
q-composite scheme ∩ on/off channels	Zero-one law + Asymp. probability (ISIT 2014 – best paper award finalist)
Pairwise scheme ∩ on/off channels	Zero-One law (ISIT 2014, IT, ICC 2015)
EG scheme ∩ disk model	Zero-One law (Allerton 2014)
q-composite scheme ∩ disk model disk model	Zero-One law (In submission)

Applications beyond wireless sensor networks

- Random key graphs ∩ random geometric graphs and Random K-out graphs ∩ random geometric graphs
  - Frequency hopping in wireless networks (keys can be used as an input to pseudo-random number generators, whose output give frequency-hopping sequence)

- Random key graphs
  - Trust networks
  - Cryptanalysis of hash functions
  - Recommender systems using collaborative filtering

- Random key graphs ∩ Erdős-Rényi graphs
  - Common–interest relations in online social networks

Thanks…
Questions??

For references: www.ece.cmu.edu/~oyagan