Asymptotically Exact Probability of k-Connectivity in Random Key Graphs *Intersecting* Erdős-Rényi Graphs

Jun Zhao, Osman Yağan*, and Virgil Gligor

{junzhao,oyagan,gligor}@andrew.cmu.edu

Dept. of ECE and CyLab

Carnegie Mellon University

Random Key Graphs??

$\mathbb{G}(n; K, P)$

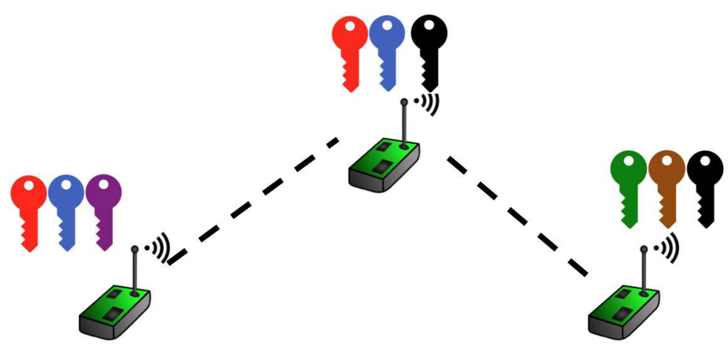
- Vertex set, $\mathcal{V} = \{v_1, \ldots, v_n\}$
- Each vertex v_i is assigned a set S_i of K distinct **objects** selected *uniformly at random* from a pool of size P.
- $S_1, \ldots, S_n$ are iid and uniform in $\{1, \ldots, P\}$ with $|S_i| = K$
- Edge set, $\mathcal{E} = \{v_i \sim v_j : \; S_i \cap S_j \; \neq \; \emptyset\}$

$$\mathbb{P}\left[v_i \sim v_j\right] = 1 - \frac{\binom{P-K}{K}}{\binom{P}{K}}$$

The starting point: Random key predistribution in wireless sensor networks

The Eschenauer-Gligor scheme:

- "Before network deployment, each sensor is **randomly** assigned a set of K **distinct** keys from a (very large) pool of P keys. "
- Pairs of sensors that share a key can communicate **securely**.
- Random key graph models network connectivity when communication constraints are ignored; i.e., under *full visibility*.



Many other application areas

- Common-interest relationship network - Zhao et al., 2013
- Modeling the *small world* effect - Yağan and Makowski 2009
- Recommender systems using collaborative filtering - Marbach 2008
- Clustering and classification analysis - Godehardt & Jaworski '03
- Cryptanalysis of hash functions - Blackburn et al., 2012

A.k.a. **uniform random intersection graphs** in some circles

Progress thus far

Q: Given (n, K, P), compute $\mathbb{P}\left[\mathbb{G}(n; K, P) \text{ has property } \mathcal{A}\right]$

- Zero-one law for absence of isolated nodes – Yağan & Makowski (2008), Blackburn & Gerke (2008)
- Zero-one laws for connectivity – Di Pietro et al (2006, 2008), Yağan & Makowski (2009, 2012), Blackburn & Gerke (2008), Rybarczyk (2009)
- Giant component and diameter – Rybarczyk (2009)
- Triangle containment and clustering properties – Yağan & Makowski (2009,2014)

Main approach: Scale K and P with n, and study

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n; K_n, P_n) \text{ has property } \mathcal{A}\right]$$

Now: Random key graphs with unreliable links

Q: What happens if we **delete** every edge of $\mathbb{G}(n; K, P)$ independently, with a given probability $(1 - p)$?

- Let $\mathbb{H}(n; p)$ be an Erdős-Rényi (ER) graph on vertices $\mathcal{V} = \{v_1, \ldots, v_n\}$. I.e., $\mathbb{P}[v_i \sim v_j] = p$ for all $i \neq j$.
- We shall study $\mathbb{G}_{on}(n; K, P, p) = \mathbb{G}(n; K, P) \cap \mathbb{H}(n; p)$
- In $\mathbb{G}_{on}(n; K, P, p)$, $\mathbb{P}[v_i \sim v_j] = p \left[1 - \frac{\binom{P-K}{K}}{\binom{P}{K}}\right]$

With K, P, and p **scaled** with n, what is

$$\lim_{n \to \infty} \mathbb{P}[\mathbb{G}_{on}(n; K_n, P_n, p_n) \text{ has property } \mathcal{A}]?$$

Motivation for $\mathbb{G}_{on}(n; K, P, p)$

- Sensitivity of graph properties in RKG to edge failures.
- In WSNs, link unreliability can be attributed to harsh environmental conditions severely impairing transmissions.
- $\mathbb{H}(n; p)$ representing an **On-Off** communication model, $\mathbb{G}_{on}(n; K, P, p)$ models secure connectivity of a sensor network.
- Distributed publish-subscribe systems: $\mathbb{G}(n; K, P)$ models common-interest relationships, and $\mathbb{H}(n; p)$ may model "friendship" network.
- Many communication problems can be formulated as an **intersection** of multiple random graphs

$\mathbb{G}_{on}(n;K,P,p)$ **vs.** $\mathbb{H}\left(n; p\left[1-\frac{\binom{P-K}{K}}{\binom{P}{K}}\right]\right)$

- Random key graph is not equivalent to an ER graph;

$$\mathbb{G}(n;K,P) \neq_{st} \mathbb{H}(n;p) \quad \text{even with} \quad 1-\frac{\binom{P-K}{K}}{\binom{P}{K}} = p$$

- This is because, edge assignments are **not** independent in $\mathbb{G}(n;K,P)$; they are in fact *positively correlated*
  - ◇ $\mathbb{P}\left[v_i \sim v_j \mid v_i \sim v_k, v_j \sim v_k\right] \neq \mathbb{P}\left[v_i \sim v_j\right]$

$$\mathbb{G}_{on}(n;K,P,p) \neq_{st} \mathbb{H}\left(n; p\left[1-\frac{\binom{P-K}{K}}{\binom{P}{K}}\right]\right)$$

Property of interest: k-connectivity

k-vertex-connected: Network remains connected despite the deletion of any $k-1$ nodes.
k-edge-connected: Defined similarly for the deletion of edges
Min. node degree $\geq k$: All nodes have at least k neighbors

Additional benefits:

- *Efficient Routing.* k-connectivity implies that any two nodes are connected by k mutually independent paths.
- *Achieving consensus.* Let m : # of adversarial nodes. Consensus can be reached if the network is $(2m+1)$-connected
- *Mobile sensor networks.* If k-connected, can assign any $k-1$ sensors as mobile nodes.

MAIN RESULTS

Theorem 1 *Assume that* $P_n = \Omega(n)$, $\frac{K_n}{P_n} = o(1)$, *and define the sequence* α_n *through*

$$p_n \cdot \left[1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}\right] = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{1}$$

If $\lim_{n\to\infty} \alpha_n = \alpha^\star \in (-\infty, +\infty)$, *then*

i) $\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on}(n; K_n, P_n, p_n)\right.$ *has min. vertex degree* $\left.\geq k\right] = e^{-\frac{e^{-\alpha^\star}}{(k-1)!}}$

ii) $\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on}(n; K_n, P_n, p_n)\right.$ *is k-edge-connected*$\left.\right] = e^{-\frac{e^{-\alpha^\star}}{(k-1)!}}$

iii) $\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on}(n; K_n, P_n, p_n)\right.$ *is k-vertex-connected*$\left.\right] = e^{-\frac{e^{-\alpha^\star}}{(k-1)!}}$

Analogous to corresponding results for ER graphs!

Poisson Convergence

$\phi_h(n; K_n, P_n, p_n)$: number of nodes in $\mathbb{G}_{on}$ with degree $h = 0, 1, \ldots$

Theorem 2 *Assume that* $P_n = \Omega(n)$, $\frac{K_n}{P_n} = o(1)$, *and let* α_n *be defined through (1). If* $\lim_{n\to\infty} \alpha_n = \alpha^\star \in (-\infty, +\infty)$, *then*

$$\lim_{n\to\infty} \mathbb{P}[\phi_{k-1}(n; K_n, P_n, p_n) = \ell] = \frac{e^{-\lambda}\lambda^\ell}{\ell!}, \quad \ell = 0, 1, 2, \ldots,$$

where

$$\lambda = e^{-\alpha^\star}/(k-1)!$$

In other words, $\phi_{k-1}(n; K_n, P_n, p_n)$ *tends to a Poisson distribution with parameter* λ.

Previous state-of-the-art for $\mathbb{G}_{on}$

- Zero-one law for 1-connectivity: Yağan, IT 2012
- Zero-one law for k-connectivity: Zhao et al., IT 2015

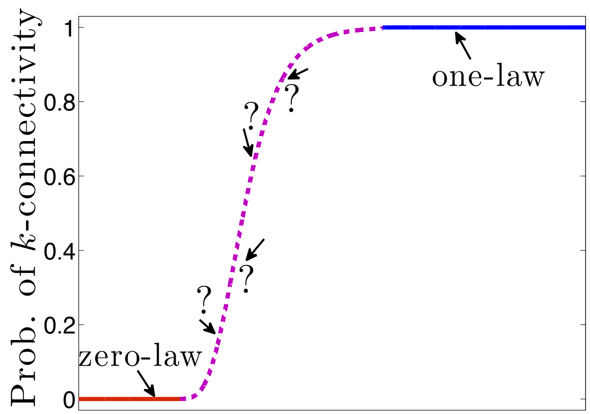
Theorem 3 (Zhao,Yağan, Gligor 2015) *Assume that* $P_n = \Omega(n)$, *and define the sequence* α_n *through (1). We have*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on}(n; K_n, P_n, p_n) \text{ is } k\text{-connected}\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty. \end{cases}$$

Theorem 3 holds for k-edge-connectivity, k-vertex-connectivity, and min. node degree $\geq k$

Zero-one laws vs. Exact Probability?

- The story is not complete with zero-one laws.
  - ◇ What if $\lim_{n\to\infty} \alpha_n = \alpha^\star \in (-\infty, \infty)$?



- May be you want to be 10-connected for sure, but are also interested in the odds of surviving a 15-node failure.
- Given the trade-offs involved, it is desirable to obtain the probability of k-connectivity for any $\alpha^\star$ value.

Corollaries of Theorem 1

- With $p_n = 1$, $n = 2, 3, \ldots$, $\mathbb{G}_{on}(n; K_n, P_n, p_n) =_{st} \mathbb{G}(n; K_n, P_n)$
  - ◇ Theorem 1 gives asymptotically exact probability of k-connectivity in random key graph.
- With $k = 1$,
  - ◇ Theorem 1 gives asymptotically exact probability of 1-connectivity in $\mathbb{G}_{on}$

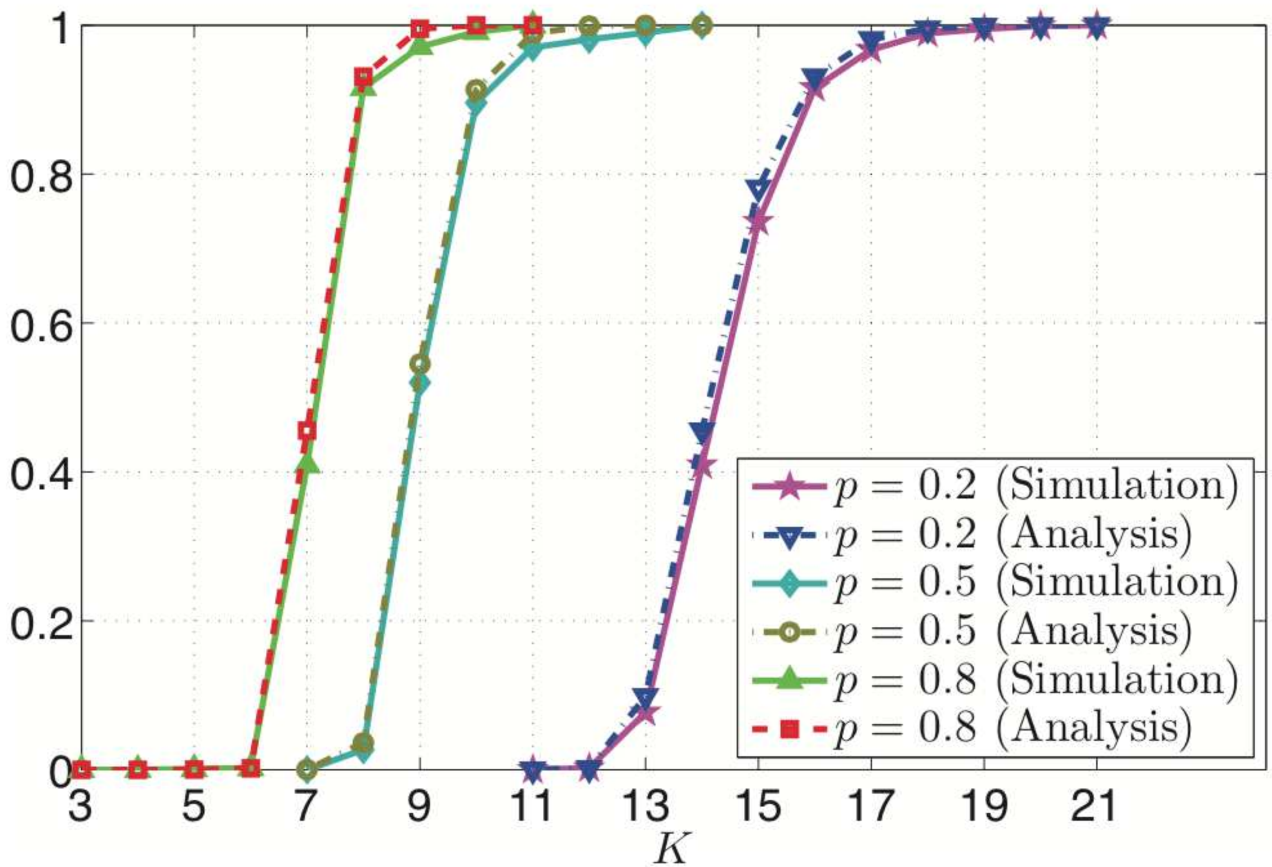
Graph	Property	Results	Work
$\mathbb{G}_{on}(n; K_n, P_n, p_n)$	k-connectivity & Min. node degree $\geq k$	exact probability	**this paper**
		zero–one law	Zhao et al. 2013
	1-connectivity & Absence of isolated vertices	exact probability	**this paper**
		zero–one law	Yağan 2012
$\mathbb{G}(n; K_n, P_n)$	k-connectivity & Min. node degree $\geq k$	exact probability	**this paper**
		zero–one law	Rybarczyk 2011
	1-connectivity & Absence of isolated vertices	exact probability	Rybarczyk 2011
		zero–one law	Di Pietro, Y&M

Connections to the Network Reliability Problem

- Start with a fixed, deterministic graph $\mathcal{H}$.
- Obtain $\mathbb{G}(\mathcal{H}; p)$ by deleting each edge of $\mathcal{H}$ independently with probability $1 - p$.
- **Network reliability problem:** Find the probability that $\mathbb{G}(\mathcal{H}; p)$ is **connected** as a function of p.
- For arbitrary graphs $\mathcal{H}$ the problem is $\#P$-complete
  - ◇ No polynomial algorithm exists, unless $P = NP$.

With $k = 1$, our results constitute an **asymptotic solution** of the network reliability problem for random key graphs.

What about finite n?



$\mathbb{P}\left[\mathbb{G}_{on}(n; K, P, p)\right.$ *is* 1-*vertex-connected*$\left.\right]$ *versus* K, *with* $n = 2,000$, $P = 10,000$ *and* $p = 0.2, 0.5, 0.8$

Thanks!

Visit `www.ece.cmu.edu/~oyagan` **for references..**