

Connectivity results for random key graphs

Osman Yağan (Advisor: Armand M. Makowski)

Random key graphs ?

- A “new” class of random graphs.
- Related to random intersection graphs.
 - ◊ A.k.a **Uniform** random intersection graphs
- Relevant to a number of applications:
 - ◊ Clustering analysis (Godehardt et al.)
 - ◊ Recommender systems (Marbach 2008)
 - ◊ Random key distribution schemes for wireless sensor networks (Eschenauer and Gligor 2002)

A random key predistribution scheme (Eschenauer and Gligor 2002)

- **Initialization phase:** Each node **randomly** selects a set of K **distinct** keys from a pool of P keys. These K keys form the **key ring** of the node, and are inserted into its memory.
- **Key setup phase:** After discovering their **wireless neighbors**, nodes mutually authenticate the shared keys to verify that the other party owns it. Now, they can communicate securely in one hop.
- **Path-key identification phase:** The key rings being randomly selected, some pairs of wireless neighbors may not share a key. If a path of nodes sharing keys pairwise exists between them, this (secure) path can be used to exchange a **path-key** to establish a direct (and secure) link between them.

Nodes that have a key in common can communicate via a secure link!



Q: Given integers P and K with $K < P$, how do we select the parameters P and K to make the probability of secure connectivity as large as possible?

Random key graph, $\mathbb{K}(n; \theta)$

- n : The number of nodes.
- P : The size of the key pool.
- K : The size of each key ring.
- With $\theta \equiv (P, K)$, let $K_i(\theta)$ denote the **random** set of K **distinct** keys assigned to node i . Assume the random sets $K_1(\theta), \dots, K_n(\theta)$ to be **i.i.d.** with

$$\mathbb{P}[K_i(\theta) = S] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K.$$

- With $\mathbb{P}[K_i(\theta) \cap K_j(\theta) = \emptyset] = \frac{\binom{P-K}{K}}{\binom{P}{K}} = q(\theta)$, we have $1 - q(\theta_n) \sim \frac{K_n^2}{P_n}$.
- Note that the Erdős-Renyi graph $\mathbb{G}(n; p) \neq_{st} \mathbb{K}(n; \theta)$ **even** when the link assignment probabilities are **matched**, i.e., $p = 1 - q(\theta)$.
 - ◊ Edge assignments are **not** independent in $\mathbb{K}(n; \theta)$ while they **are** in $\mathbb{G}(n; p)$!
- We are interested in obtaining zero-one laws for:

$$P^*(n; \theta) := \mathbb{P}[\mathbb{K}(n; \theta) \text{ is connected}]$$

$$P(n; \theta) := \mathbb{P}[\mathbb{K}(n; \theta) \text{ contains no isolated nodes}]$$

Main results

Define the sequence $\alpha : \mathbb{N}_0 \rightarrow \mathbb{R}$ as the *deviation function* associated with the scaling $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ as

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \dots \quad (1)$$

We obtain:

Theorem 1 For any admissible pair $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}$, we have

$$\lim_{n \rightarrow \infty} P(n; \theta_n) = \begin{cases} 0 & \text{if } \lim_{n \rightarrow \infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n \rightarrow \infty} \alpha_n = +\infty \end{cases}$$

Theorem 2 For any admissible pair $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}$, we have

$$\lim_{n \rightarrow \infty} P^*(n; \theta_n) = 0 \quad \text{if } \lim_{n \rightarrow \infty} \alpha_n = -\infty. \quad (2)$$

On the other hand, if there exists some $\sigma > 0$ such that

$$\sigma n \leq P_n \quad (3)$$

for all $n = 1, 2, \dots$ sufficiently large, we have

$$\lim_{n \rightarrow \infty} P^*(n; \theta_n) = 1 \quad \text{if } \lim_{n \rightarrow \infty} \alpha_n = \infty. \quad (4)$$

Rate of convergence?

We expect to establish the validity of the following version of the “double-exponential” result in random key graphs:

Conjecture For any admissible pair $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}$, satisfying (3) we have

$$\lim_{n \rightarrow \infty} P^*(n; \theta_n) = e^{-e^{-c}} \quad \text{if } \lim_{n \rightarrow \infty} \alpha_n = c \quad (1)$$

for some c in \mathbb{R} .

Motivation: Celebrated “double exponential” result for Erdős-Renyi graphs $\mathbb{G}(n; p)$ ($0 < p < 1$): Whenever

$$p_n = \frac{\log n + \gamma}{n} \quad (n \rightarrow \infty)$$

for any $\gamma \in \mathbb{R}$, we have

$$\lim_{n \rightarrow \infty} \mathbb{P}[\mathbb{G}(n; p_n) \text{ is connected}] = e^{-e^{-\gamma}}$$

Theorem 1 and 2 mimic similar ones for Erdős-Renyi graph. Perhaps $\mathbb{K}_n(\theta)$ and $\mathbb{G}(n; p)$ exhibit related asymptotic behavior for graph connectivity!

Graph properties other than connectivity?

- It is natural to wonder whether such a transfer technique from Erdős-Renyi graphs to random key graphs can be applied more generally to other graph properties.
- We consider the small subgraph containment problem in reference [3].
 - ◊ We study the zero-one law for the existence of triangles in random key graphs.
- For the parameter range that is of practical relevance in WSNs, the critical scaling obtained for random key graphs turns out to be *much smaller* than the one for Erdős-Rényi graphs.
- **Conclusion.** The transfer is *not* a valid approach in general, and can be quite misleading in the context of WSNs.

References

- † O. Yağan and A. M. Makowski, “On the random graph induced by a random key predistribution scheme under full visibility,” In Proceedings of the ISIT 2008.
- † O. Yağan and A. M. Makowski, “Connectivity results for random key graphs,” In Proceedings of the ISIT 2009.
- † O. Yağan and A.M. Makowski, “On the existence of triangles in random key graphs,” Available online at <http://www.lib.umd.edu/drum/>, July 2009.

