Connectivity results for random key graphs

Osman Yağan and Armand M. Makowski
Department of Electrical and Computer Engineering
and the Institute for Systems Research
University of Maryland at College Park
College Park, Maryland 20742
oyagan@umd.edu, armand@isr.umd.edu

Abstract— **The random key graph is the random graph induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. We report on recent results concerning a conjectured zero-one law for graph connectivity, and provide an outline for its proof.**

Keywords: Wireless sensor networks, Key predistribution, Random key graphs, Connectivity, Zero-one laws.

I. Introduction

Eschenauer and Gligor [5] have recently proposed the following random key predistribution scheme for wireless sensor networks: Before network deployment, each sensor is independently assigned K distinct cryptographic keys which are selected at random from a pool of P keys. These K keys constitute the key ring of the node and are inserted into its memory. Two sensor nodes can then establish a secure link between them if they are within transmission range of each other and if their key rings have at least one key in common; see [5] for implementation details.

Under the assumption of *full visibility*, namely that nodes are all within communication range of each other, two nodes can communicate securely if their key rings share at least one key. This notion of adjacency induces the *random key* graph $\mathbb{K}(n;(K,P))$ on the vertex set $\{1,\ldots,n\}$ where n is the number of sensor nodes; see Section II for precise definitions.

We seek conditions on n, K and P under which $\mathbb{K}(n;(K,P))$ is a connected graph with high probability. Such conditions would provide encouraging clues as to the feasibility of this distribution scheme in the context of wireless sensor networks. As explained in [7] this search has lead to the following *conjecture* which appeared independently in [1, 6]: As we scale the parameters K and P with n according to

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{1}$$

for some sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, it is conjectured that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n;(K_n,P_n)) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty. \end{cases} \tag{2}$$

This zero-one law for graph connectivity in $\mathbb{K}(n;(K,P))$ mimics a similar one for Erdős-Renyi graphs [2], and in fact can be motivated from it by matching the link assignment probabilities in these two classes of random graphs.

In this short conference paper we report on recent progress made on the conjectured zero-one law (1)-(2). In Section II we formally introduce the class of random key graphs. Section III is devoted to a brief review of recent results. This is followed in Section IV by a presentation of the main contribution, summarized as Theorem 4.1. Its proof is long and technically involved, and therefore omitted given the page limitations; it can be found in [7]. Instead, most of the discussion is devoted to an *outline* of the arguments: In Section V we give a basic roadmap of the proof and identify a probability term that needs to become vanishingly small as n grows large. Bounding arguments to do so are developed in Section VI, and the final steps of the proof are then outlined in Section VII. In the concluding Section VIII we contrast our approach against that used by other authors [1, 4].

A word on notation: All statements involving limits, including asymptotic equivalences, are understood with n going to infinity. The cardinality of any discrete set S is denoted by $|S|$.

II. Random key graphs

The model is parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring with $K < P$. To lighten the notation we often group the integers P and K into the ordered pair $\theta \equiv (P,K)$.

For each node $i = 1,\ldots,n$, let $K_i(\theta)$ denote the random set of K distinct keys assigned to node i. We can think of $K_i(\theta)$ as an $\mathcal{P}_K$-valued rv where $\mathcal{P}_K$ denotes the collection of all subsets of $\{1,\ldots,P\}$ which contain exactly K elements – Obviously, we have $|\mathcal{P}_K| = \binom{P}{K}$. The rvs $K_1(\theta),\ldots,K_n(\theta)$ are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed over $\mathcal{P}_K$ with

$$\mathbb{P}\left[K_i(\theta) = S\right] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K \tag{3}$$

for all $i = 1,\ldots,n$. This corresponds to selecting keys randomly and *without* replacement from the key pool.

Distinct nodes $i, j = 1,\ldots,n$ are said to be adjacent if they share at least one key in their key rings, namely

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset, \tag{4}$$

in which case an undirected link is assigned between nodes i and j. The resulting random graph defines the *random*

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

key graph on the vertex set $\{1,\dots,n\}$, hereafter denoted by $\mathbb{K}(n;\theta)$. Random key graphs, which form a subclass in the family of *random intersection* graphs, are also called *uniform random intersection* graphs by some authors [1] (and references therein).

For distinct $i,j=1,\dots,n$, it is a simple matter to check that

$$\mathbb{P}\left[K_i(\theta)\cap K_j(\theta)=\emptyset\right]=q(\theta) \tag{5}$$

with

$$q(\theta)=\begin{cases}0 & \text{if } P<2K\\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } 2K\le P.\end{cases} \tag{6}$$

The case $P<2K$ is clearly not interesting: It corresponds to an edge existing between every pair of nodes, so that $\mathbb{K}(n;\theta)$ coincides with the complete graph K_n.

With $n=2,3,\dots$ and positive integers K and P such that $K\le P$, let $P(n;\theta)$ denote the probability that the random key graph $\mathbb{K}(n;\theta)$ is connected, namely

$$P(n;\theta):=\mathbb{P}\left[\mathbb{K}(n;\theta)\text{ is connected}\right],\quad \theta=(K,P).$$

III. Related work

To set the stage we begin by surveying recent results concerning the conjectured zero-one law (1)-(2).

Di Pietro et al. have shown [4, Thm. 4.6] that for large n, the random key graph will be connected with very high probability if P_n and K_n are selected such that

$$K_n\ge 5,\ n\le P_n \quad\text{and}\quad \frac{K_n^2}{P_n}\sim c\,\frac{\log n}{n} \tag{7}$$

for some $c\ge 16$.[1] They also observe that for large n, the random key graph will be disconnected with very high probability if the scaling satisfies

$$\frac{K_n^2}{P_n}=o\left(\frac{\log n}{n}\right).$$

In [1] Blackburn and Gerke recently generalized the results of Di Pietro et al.. Under the conditions

$$K_n\ge 2 \quad\text{and}\quad n\le P_n,\quad n=1,2,\dots \tag{8}$$

they showed [1, Thm. 5] that

$$\lim_{n\to\infty}P(n;\theta_n)=0 \quad\text{if}\quad \limsup_{n\to\infty}\frac{K_n^2}{P_n}\frac{n}{\log n}<1 \tag{9}$$

and

$$\lim_{n\to\infty}P(n;\theta_n)=1 \quad\text{if}\quad \liminf_{n\to\infty}\frac{K_n^2}{P_n}\frac{n}{\log n}>1. \tag{10}$$

In the process of establishing (9)-(10), they also showed [1, Thm. 3] that the conjectured zero-one law (1)-(2) holds when $K_n\equiv 2$ *without* any additional constraint on the size of the key pool. From this last result it then follows that (1)-(2) holds when $P_n=o\left(\frac{n}{\log n}\right)$ with $2\le K_n\le P_n$. To the best of our knowledge, this is the only regime for which the conjecture (1)-(2) has been shown to hold thus far.

[1] In the conference version of this work [3, Thm. 4.6] the result is claimed to hold for $c>8$.

IV. The main result

To fix the terminology, any pair of functions $P,K:\mathbb{N}_0\to\mathbb{N}_0$ is called a *scaling*, and we can always associate with it a sequence $\alpha:\mathbb{N}_0\to\mathbb{R}$ through the relation

$$\frac{K_n^2}{P_n}=\frac{\log n+\alpha_n}{n},\quad n=1,2,\dots \tag{11}$$

We refer to this sequence $\alpha:\mathbb{N}_0\to\mathbb{R}$ as the *deviation function* associated with the scaling $P,K:\mathbb{N}_0\to\mathbb{N}_0$. A scaling $P,K:\mathbb{N}_0\to\mathbb{N}_0$ is said be *admissible* if

$$K_n\le P_n,\quad n=1,2,\dots \tag{12}$$

and

$$2\le K_n \tag{13}$$

for *all* $n=1,2,\dots$ *sufficiently* large.

Our main result is given next.

Theorem 4.1: *Consider an admissible scaling $P,K:\mathbb{N}_0\to\mathbb{N}_0$ with deviation function $\alpha:\mathbb{N}_0\to\mathbb{R}$ determined through (11). We have*

$$\lim_{n\to\infty}P(n;\theta_n)=0 \quad \textit{if } \lim_{n\to\infty}\alpha_n=-\infty. \tag{14}$$

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

$$\sigma n\le P_n \tag{15}$$

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

$$\lim_{n\to\infty}P(n;\theta_n)=1 \quad \textit{if } \lim_{n\to\infty}\alpha_n=\infty. \tag{16}$$

It is easy to check that Theorem 4.1 implies the zero-one law (9)-(10) under (8). The condition (15) is sometimes expressed as $P_n=\Omega(n)$ and is weaker than the growth condition at (8) used by Blackburn and Gerke [1].

The remainder of the paper is devoted to a discussion of the proof of Theorem 4.1; only an outline of the arguments is provided due to space limitations. Also, a careful inspection of the detailed arguments given in [7] points to the validity of the following version of the "double-exponential" result in random key graphs: Under (15) we have

$$\lim_{n\to\infty}P(n;\theta_n)=e^{-e^{-c}} \quad\text{if}\quad \lim_{n\to\infty}\alpha_n=c \tag{17}$$

for some c in $\mathbb{R}$. Work on this issue will be reported elsewhere.

V. A roadmap for the proof of Theorem 4.1

Fix $n=2,3,\dots$, and consider positive integers K and P such that $2\le K\le P$. We define the events

$$C_n(\theta):=\left[\mathbb{K}_n(\theta)\text{ is connected}\right]$$

and

$$I_n(\theta):=\left[\mathbb{K}_n(\theta)\text{ contains no isolated nodes}\right].$$

If the random key graph $\mathbb{K}(n;\theta)$ is connected, then it does not contain isolated nodes, whence $C_n(\theta)$ is a subset of $I_n(\theta)$, and we conclude to

$$\mathbb{P}\left[C_n(\theta)\right]\le\mathbb{P}\left[I_n(\theta)\right] \tag{18}$$

and

$$\mathbb{P}\left[C_n(\theta)^c\right] = \mathbb{P}\left[C_n(\theta)^c \cap I_n(\theta)\right] + \mathbb{P}\left[I_n(\theta)^c\right]. \tag{19}$$

In [6], we established the following zero-one law for the absence of isolated nodes by the method of first and second moments applied to the number of isolated nodes in the random key graph. This result was also obtained independently by Blackburn and Gerke [1].

Theorem 5.1: *For any admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, it holds that*

$$\lim_{n\to\infty} \mathbb{P}\left[I_n(\theta_n)\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{20}$$

where the function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is determined through (11).

Pick an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is determined through (11). If $\lim_{n\to\infty} \alpha_n = -\infty$, then $\lim_{n\to\infty} \mathbb{P}\left[I_n(\theta_n)\right] = 0$ by the zero-law for the absence of isolated nodes, whence $\lim_{n\to\infty} \mathbb{P}\left[C_n(\theta_n)\right] = 0$ with the help of (18). If $\lim_{n\to\infty} \alpha_n = \infty$, then $\lim_{n\to\infty} \mathbb{P}\left[I_n(\theta_n)\right] = 1$ by the one-law for the absence of isolated nodes and the desired conclusion $\lim_{n\to\infty} \mathbb{P}\left[C_n(\theta_n)\right] = 1$ will follow via (19) if we can show that

$$\lim_{n\to\infty} \mathbb{P}\left[C_n(\theta_n)^c \cap I_n(\theta_n)\right] = 0 \tag{21}$$

under appropriate conditions on the scaling.

As we embark on establishing (21), we find it convenient to refer to an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as being *strongly admissible* if its deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies the additional growth condition

$$\alpha_n = o(n). \tag{22}$$

Strong admissibility has implications which turn out to be technically helpful in some of the proofs: Under (22) it is always the case from (11) that

$$\lim_{n\to\infty} \frac{K_n^2}{P_n} = 0. \tag{23}$$

Since $1 \le K_n \le K_n^2$ for all $n = 1, 2, \ldots$, this last convergence implies

$$\lim_{n\to\infty} \frac{K_n}{P_n} = 0 \quad \text{and} \quad \lim_{n\to\infty} P_n = \infty. \tag{24}$$

As a result,

$$\lim_{n\to\infty} \frac{P_n}{K_n} = \infty \tag{25}$$

so that $2K_n \le P_n$ for all $n = 1, 2, \ldots$ sufficiently large. In other words, the random key graph does not degenerate into a complete graph under strongly admissible scalings. Finally, it is easy to check [7] that (23) implies

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n}. \tag{26}$$

The relevance of strong admissibility flows from the following facts.

Lemma 5.2: *Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Assume that (15) holds for all $n = 1, 2, \ldots$ sufficiently large. Then, there always exists a strongly admissible scaling $\tilde{K}, \tilde{P} : \mathbb{N}_0 \to \mathbb{N}_0$ with*

$$\tilde{K}_n \le K_n \quad \text{and} \quad \tilde{P}_n = P_n, \quad n = 1, 2, \ldots \tag{27}$$

whose deviation function $\tilde{\alpha} : \mathbb{N}_0 \to \mathbb{R}$ satisfies both conditions $\lim_{n\to\infty} \tilde{\alpha}_n = \infty$ and $\tilde{\alpha}_n = o(n)$.

An easy coupling argument based on (27) implies

$$P(n; \tilde{\theta}_n) \le P(n; \theta_n), \quad n = 2, 3, \ldots$$

Thus, we need only show (16) under (15) for strongly admissible scalings, and this leads to taking the following useful reduction step.

Proposition 5.3: *Consider any strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Under the condition (15), we have (21).*

VI. Bounding arguments (Outline)

We shall establish Proposition 5.3 by finding a sufficiently tight upper bound on the probability appearing in (21), and then showing that it goes to zero as well. The additional condition (15) and strong admissibility of the scaling will play a crucial role in carrying out this argument. We outline the approach with *most* of the lengthy technical details available in [7].

Throughout the discussion, let K and P denote given positive integers such that $2 \le K \le P$, and fix $n = 2, 3, \ldots$. For any non-empty subset S of nodes, i.e., $S \subseteq \{1, \ldots, n\}$, consider the graph $\mathbb{K}(n; \theta)(S)$ (with vertex set S) defined as the subgraph of $\mathbb{K}(n; \theta)$ restricted to the nodes in S. The set S is said to be *isolated* in $\mathbb{K}(n; \theta)$ if there there are no edges (in $\mathbb{K}(n; \theta)$) between the nodes in S and the nodes in the complement $S^c = \{1, \ldots, n\} - S$. Let $C_n(\theta; S)$ denote the event that the subgraph $\mathbb{K}(n; \theta)(S)$ is itself connected. We also introduce the event $B_n(\theta; S)$ that S is isolated in $\mathbb{K}(n; \theta)$, i.e.,

$$B_n(\theta; S) := \left[K_i(\theta) \cap K_j(\theta) = \emptyset, \ i \in S, \ j \in S^c\right].$$

Finally, we set

$$A_n(\theta; S) := C_n(\theta; S) \cap B_n(\theta; S).$$

The following basic observation has been used in the context of Erdős-Renyi graphs [2], and underpins the arguments in both [1] and [3]: If $\mathbb{K}(n; \theta)$ is *not* connected and yet contains *no* isolated nodes, then there must exist a non-empty subset S of nodes with $2 \le |S| \le \lfloor \frac{n}{2} \rfloor$ such that $\mathbb{K}(n; \theta)(S)$ is connected while S is isolated in $\mathbb{K}(n; \theta)$. Thus, we have

$$C_n(\theta)^c \cap I_n(\theta) \subseteq \cup_{S \in \mathcal{N}: 2 \le |S| \le \lfloor \frac{n}{2} \rfloor} A_n(\theta; S) \tag{28}$$

with $\mathcal{N}$ denoting the collection of all subsets of $\{1, \ldots, n\}$. A standard union bound argument then gives

$$\mathbb{P}\left[C_n(\theta)^c \cap I_n(\theta)\right] \le \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{S \in \mathcal{N}_r} \mathbb{P}\left[A_n(\theta; S)\right] \right)$$

where for each $r = 1, \ldots, n$, we use $\mathcal{N}_r$ to denote the collection of all subsets of $\{1, \ldots, n\}$ with exactly r elements.

Now, for each $r = 1, \ldots, n-1$, we simplify the notation by writing $A_{n,r}(\theta) := A_n(\theta; \{1, \ldots, r\})$, $B_{n,r}(\theta) := B_n(\theta; \{1, \ldots, r\})$ and $C_r(\theta) := C_n(\theta; \{1, \ldots, r\})$. This notation is consistent with $C_n(\theta)$ as defined earlier in Section V. Under the enforced assumptions, it is a simple matter to check that

$$\mathbb{P}[A_n(\theta; S)] = \mathbb{P}[A_{n,r}(\theta)], \quad S \in \mathcal{N}_r$$

and the bound

$$\mathbb{P}[C_n(\theta)^c \cap I_n(\theta)] \leq \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}[A_{n,r}(\theta)] \tag{29}$$

follows upon noting that $|\mathcal{N}_r| = \binom{n}{r}$.

For each $r = 2, \ldots, n-1$, define the event

$$C_r^\star(\theta) := C_r(\theta) \cap [U_r(\theta) \leq P - K]$$

where

$$U_r(\theta) := |\cup_{i=1}^r K_i(\theta)|. \tag{30}$$

The rv $U_r(\theta)$ counts the number of *distinct* keys assigned to the nodes $\{1, \ldots, r\}$.

The event $C_r(\theta)$ is determined by the r rvs $K_1(\theta), \ldots, K_r(\theta)$, and conditioning upon them, we get

$$\begin{aligned} \mathbb{P}[A_{n,r}(\theta)] &= \mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta)] \\ &= \mathbb{E}\left[\mathbf{1}[C_r^\star(\theta)] \cdot \left(\frac{\binom{P-U_r(\theta)}{K}}{\binom{P}{K}}\right)^{n-r}\right] \\ &\leq \mathbb{E}\left[\mathbf{1}[C_r^\star(\theta)] \cdot e^{-(n-r)\frac{K}{P} \cdot U_r(\theta)}\right]. \end{aligned} \tag{31}$$

In this last step we made use of the easy bound

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} \leq e^{-\frac{K}{P}L}$$

where K, L and P are positive integers such that $K + L \leq P$; see [7] for details.

Next, for each positive integer x, define the event $E_r(\theta; x)$ by

$$E_r(\theta; x) := [U_r(\theta) \leq x].$$

We always have $U_r(\theta) \geq K$ while on the event $C_r^\star(\theta) \cap E_r(\theta; x)^c$ the inequality $U_r(\theta) \geq x + 1$ holds. Reporting these facts into (31) we get the following bound.

Lemma 6.1: *For $r = 1, \ldots, n$, we have*

$$\begin{aligned} & \mathbb{P}[A_{n,r}(\theta)] \\ \leq\ & \mathbb{P}[E_r(\theta; x)]\, e^{-(n-r)\frac{K^2}{P}} + \mathbb{P}[C_r^\star(\theta)]\, e^{-(n-r)\frac{K}{P}(x+1)} \\ \leq\ & \mathbb{P}[E_r(\theta; x)]\, e^{-(n-r)\frac{K^2}{P}} + \mathbb{P}[C_r(\theta)]\, e^{-(n-r)\frac{K}{P}(x+1)} \end{aligned} \tag{32}$$

for each positive integer x.

The constraints $K \leq U_r(\theta) \leq \min(rK, P)$ automatically imply $U_r(\theta) \leq P - K$ whenever $rK \leq P - K$, i..e., $(r+1)K \leq P$. Thus, $C_r^\star(\theta) = C_r(\theta)$ for all $r = 1, \ldots, r_n(\theta)$ where we have set

$$r_n(\theta) := \min\left(r(\theta), \left\lfloor \frac{n}{2} \right\rfloor\right) \quad \text{with } r(\theta) := \left\lfloor \frac{P}{K} \right\rfloor - 1.$$

The next two results provide clues as to how we could bound the terms in (32). The first result shows that the probability of $C_r(\theta)$ can indeed be bounded in terms of known quantities.

Lemma 6.2: *For each $r = 2, \ldots, n$, we have*

$$\mathbb{P}[C_r(\theta)] \leq r^{r-2}(1 - q(\theta))^{r-1}. \tag{33}$$

The basic idea behind this bound was already used in the context of Erdős-Renyi graphs [2] where the analog of (33) holds with $1 - q(\theta)$ playing the role of probability of link assignment.

Proof. If $\mathbb{K}(n; \theta)(S)$ (with $S = \{1, \ldots, r\}$) is a connected graph, then it must contain a spanning tree. As a result, with $\mathcal{T}_r$ denoting the collection of all trees with vertices $1, \ldots, r$, a union bound argument gives

$$\mathbb{P}[C_r(\theta)] \leq \sum_{T \in \mathcal{T}_r} \mathbb{P}[T \subset \mathbb{K}(n; \theta)(S)] \tag{34}$$

where the notation $T \subset \mathbb{K}(n; \theta)(S)$ indicates that the tree T is a subgraph of $\mathbb{K}(n; \theta)(S)$.

Each tree T in $\mathcal{T}_r$ is uniquely determined by $r - 1$ edges and contains no loops. Moreover, for every $i = 1, \ldots, r$, we note that

$$\mathbb{P}[K_i(\theta) \cap K_j(\theta) \neq \emptyset,\ j \in J] = \prod_{j \in J} \mathbb{P}[K_i(\theta) \cap K_j(\theta) \neq \emptyset]$$

with J any subset of $\{1, \ldots, r\}$ not containing i. Exploiting these facts we readily show by induction (on r) that

$$\mathbb{P}[T \subset \mathbb{K}(n; \theta)(S)] = (1 - q(\theta))^{r-1}, \quad T \in \mathcal{T}_r; \tag{35}$$

see [7] for details. By Cayley's formula there are r^{r-2} trees on r vertices, i.e., $|\mathcal{T}_r| = r^{r-2}$, and (33) follows from (34) via (35). ∎

The following rough estimates for the distribution of the rv $U_r(\theta)$ will be adequate to handle the first term in the bound (32).

Lemma 6.3: *For all $r = 1, 2, \ldots$, we have the bound*

$$\mathbb{P}[U_r(\theta) \leq x] \leq \binom{P}{x} \left(\frac{x}{P}\right)^{rK}$$

whenever $x = 1, \ldots, \min(rK, P)$.

VII. Completing the proof of Proposition 5.3 (Outline)

Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as in the statement of Proposition 5.3. In view of the discussion leading to (29) we need to show

$$\lim_{n \to \infty} \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}[A_{n,r}(\theta_n)] = 0. \tag{36}$$

Under (22) we necessarily have $\lim_{n\to\infty} r_n(\theta_n) = \infty$ (via (25)), and for any given integer $R \geq 2$ (to be specified shortly) it is the case that

$$R < r_n(\theta_n), \quad n \geq n^\star(R) \tag{37}$$

for some finite integer $n^\star(R)$. On that range we introduce the decomposition

$$\begin{aligned}\sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] &= \sum_{r=2}^{R} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] \\ &+ \sum_{r=R+1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] \\ &+ \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right].\end{aligned} \tag{38}$$

Let n go to infinity in (38): The desired convergence (36) will be established if we show

$$\lim_{n\to\infty} \sum_{r=2}^{R} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0, \tag{39}$$

$$\lim_{n\to\infty} \sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0 \tag{40}$$

and

$$\lim_{n\to\infty} \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0. \tag{41}$$

We prove the validity of (39), (40) and (41) by repeated applications of Lemma 6.1. We address these three cases by making use of the bounds there with

$$x = \lfloor (1+\varepsilon) K_n \rfloor, \quad \varepsilon \in (0, \frac{1}{2})$$

$$x = \lfloor \lambda r K_n \rfloor, \quad \lambda \in (0,1)$$

and

$$x = \lfloor \mu P_n \rfloor, \quad \mu \in (0,1),$$

respectively. The parameters $\lambda > 0$ and $\mu > 0$ are taken sufficiently small to ensure that certain quantities are below various thresholds. Once $\lambda > 0$ has been specified, the integer R appearing at (37) needs to be selected so that $2 < \lambda(R+1)$. The arguments leading to (39), (40) and (41) are carried out with the help of the bounds in Lemma 6.2 and Lemma 6.3. The details are quite involved and can be found in [7].

VIII. Concluding remarks

We close by highlighting key differences between our approach and the one in [1, 3]. The observation yielding (29), which forms the basis of our discussion, is also used in some form as the starting point in both these references. However, these authors do not take advantage of the fact that the event $C_r(\theta)$ has a probability for which a sufficiently tight bound is available, namely (34) – This is a consequence of the *exact* expression (35). Through this bound, we leverage strong admissibility (via (26)) to get

$$(1 - q(\theta_n)) \leq (1+\delta) \cdot \frac{K_n^2}{P_n}$$

for n sufficiently large with any $0 < \delta < 1$, in which case

$$\mathbb{P}\left[C_r(\theta_n)\right] \leq r^{r-2} \left((1+\delta) \cdot \frac{K_n^2}{P_n} \right)^{r-1}$$

for each $r = 2, 3, \ldots$. The form (1) of the scaling can now be brought to bear – Such an argument cannot necessarily be made if the scaling is merely admissible.

From (31) we could have also obtained the bounds

$$\mathbb{P}\left[A_{n,r}(\theta)\right] \leq \mathbb{P}\left[C_r(\theta)\right] e^{-(n-r)\frac{K_n^2}{P_n}}, \quad r = 1, 2, \ldots, n \tag{42}$$

Unfortunately, these bounds are too loose to be useful, and it was this state of affairs that provided the impetus to develop the bounds in Lemma 6.1.

The decomposition (38) is necessary for efficiently bounding the rv $U_r(\theta_n)$. Indeed, if it were the case that $U_r(\theta_n) = rK_n$ for each $r = 1, \ldots, n$, then the conjecture (1)-(2) would readily follow as in Erdős-Renyi graphs [2] without recourse to the decomposition (38). However, the constraint $U_r(\theta_n) \leq \min(rK_n, P_n)$ already suggests that we consider separately the cases $rK_n \leq P_n$ and $P_n < rK_n$. In the range $r = 1, \ldots, \lfloor \frac{P_n}{K_n} \rfloor$, it is tempting to use Lemma 6.1 with $x = \lfloor \lambda r K_n \rfloor$ and sufficiently small λ in $(0,1)$ – This was the approach taken in the references [1] and [3]. Unfortunately the resulting bounds will not suffice for the following reason: For small values of r the obvious bound $U_r(\theta_n) \geq K_n$ might be tighter than $U_r(\theta_n) \geq \lfloor \lambda r K_n \rfloor$, and a further decomposition is then needed to obtain the desired results.

Acknowledgment

This work was supported by NSF Grant CCF-07290.

References

[1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," May 2008. arXiv:0805.2814v2 [math.CO]

[2] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[3] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Sensor networks that are provably secure," in Proceedings of SecureComm 2006, Baltimore (MD), August 2006.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[5] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington (DC), November 2002, pp. 41-47.

[6] O. Yağan and A. M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," in Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), Toronto (ON, Canada), June 2008.

[7] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Available online at http://hdl.handle.net/1903/8716, January 2009.