Connectivity in random graphs induced by a key predistribution scheme – Small key pools

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— **We consider 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 simple proofs for small key pools.**

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

I. Introduction

Security is expected to be a key challenge for wireless sensor networks (WSNs) deployed in hostile environments. With this in mind Eschenauer and Gligor [5] have recently proposed the following *random* key predistribution scheme: 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. Once deployed, two sensor nodes can then establish a secure link between them if they are within (wireless) transmission range of each other *and* if their key rings share at least one key; see [5] for implementation details.

Under the assumption of *full visibility*, namely that nodes are all within communication range of each other, a secure link can be established between two nodes whenever their key rings have at least one key in common. This notion of adjacency defines 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. For sure, the assumption of full visibility does away with the wireless nature of the communication infrastructure supporting WSNs. In return, this simplification allows one to focus on how randomizing the key selections affects the establishment of a secure network. It is this aspect of the distribution scheme that we study here, as 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 helpful guidelines for dimensioning the scheme of Eschenauer and Gligor.

As explained in [14] there are good reasons to conjecture the following zero-one law for graph connectivity in random key graphs: If 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 $\alpha : \mathbb{N}_0 \to \mathbb{R}$, then

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

This conjecture appeared independently in [1, 10]. The zero-law in (2) automatically holds as a consequence of the identical zero-law for the absence of isolated nodes in random key graphs [1, 10]. Progress has recently been made with respect to the one-law in (2) under additional assumptions relating the size of the key pool to the number of nodes, e.g., see [1, 3, 11, 14]. Rybarczyk [9] has just established the conjecture without such assumptions. See Section III for a brief survey of these contributions.

In the aforementioned papers [1, 3, 9, 11, 14], the proofs are rather long and technically involved. Here instead we discuss a number of situations for which the conjectured one-law can be easily recovered when the key pool P_n is "small" compared to n. The basic idea behind these shorter proofs is the following simple observation: The key graph *is* automatically connected if *all* possible key rings have been distributed to the nodes.

The arguments which we develop on the basis of this fact clearly indicate the interplay that exists in random key graphs between the size of the key pool and the number of nodes; this is reflected in the additional assumptions under which the results were given in the papers [1, 3, 11, 14]. For classical Erdős-Renyi graphs no such interplay exists between the edge assignment probability and the number of nodes [2].

The rest of the paper is organized as follows: In Section II we formally introduce the class of random key graphs. Section III is devoted to a brief review of recent results, and in Section IV we provide a key observation which lead to the main results of the paper. In Section VI we report on the case when K and P are fixed. The case $\limsup_{n\to\infty} P_n < \infty$ is considered in Section VII. We close in Section VIII with a direct proof of the case where $P_n = n^\delta$ for some $0 < \delta < \frac{1}{2}$.

978-1-4244-7417-2/10/$26.00 ©2010 IEEE

This paper was originally accepted for inclusion in the program of the International Conference on Information and Communication Systems (ICICS 2009) to take place in Amman (Jordan) during December 2009 [13]. However, the paper was withdrawn due to the fact that neither author could attend the conference, and therefore will not appear in the published proceedings.[1]

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 $K \leq P$. To lighten the notation we group the integers P and K into the ordered pair $\theta \equiv (K, P)$.

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. This notion of adjacency defines the *random key graph* on the vertex set $\{1, \ldots, n\}$, hereafter denoted by $\mathbb{K}(n; \theta)$.

For distinct $i, j = 1, \ldots, n$, 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

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

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 $\mathcal{K}_n$.

Random key graphs form a subclass in the family of *random intersection* graphs, and are also called *uniform random intersection* graphs by some authors [1, 6, 7, 9]. They have been discussed recently in several application contexts, e.g., security of wireless sensor networks [1, 3], clustering analysis [6, 7], recommender systems using global filtering [8], and small world models [12].

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

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

[1]The program of ICICS 2009 is available online at http://www.icics.info/confprog.php.

III. Recent results

To fix the terminology, any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ is said to define a *scaling* provided the natural conditions

$$K_n \leq P_n, \quad n = 1, 2, \ldots \tag{7}$$

are satisfied. With this scaling we can always associate a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ through the relation

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{8}$$

Just set

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

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 to be *admissible* if

$$2 \leq K_n \tag{9}$$

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

Blackburn and Gerke [1, Thm. 5] recently obtained the following zero-one law which generalizes earlier results of Di Pietro et al. [3, Thm. 4.6].

Theorem 3.1: *Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$. Then, we always have*

$$\lim_{n\to\infty} P(n; \theta_n) = 0 \quad \textit{if} \quad \limsup_{n\to\infty} \frac{K_n^2}{P_n}\frac{n}{\log n} < 1. \tag{10}$$

Under the additional assumption

$$n \leq P_n \tag{11}$$

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

$$\lim_{n\to\infty} P(n; \theta_n) = 1 \quad \textit{if} \quad \liminf_{n\to\infty} \frac{K_n^2}{P_n}\frac{n}{\log n} > 1. \tag{12}$$

In the process of establishing this result, they also showed [1, Thm. 3] that the conjectured zero-one law (1)-(2) indeed holds in a special case.

Theorem 3.2: *Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ with*

$$K_n = 2, \quad n = 1, 2, \ldots \tag{13}$$

so that its deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ (determined through (8)) now satisfies

$$\frac{4}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{14}$$

Then, we have

$$\lim_{n\to\infty} P(n; (2, P_n)) = \begin{cases} 0 & \textit{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1 & \textit{if } \lim_{n\to\infty} \alpha_n = \infty. \end{cases} \tag{15}$$

Theorem 3.2 requires no constraints on the size of the key pool. For each $n = 2, 3, \ldots$, a simple coupling argument yields

$$P(n; (2, P)) \leq P(n; (K, P)) \tag{16}$$

whenever $2 \leq K \leq P$. Therefore, Theorem 3.2 implies the conjecture (1)-(2) whenever

$$2 \leq K_n \leq P_n \quad \text{and} \quad P_n = o\left(\frac{n}{\log n}\right). \tag{17}$$

The next result is due to Yağan and Makowski; it generalizes Theorem 3.1, and complements Theorem 3.2. A complete proof can be found in [14] (with an outline of the arguments available in [11]).

Theorem 3.3: *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 (8). We have*

$$\lim_{n\to\infty} P(n;\theta_n) = 0 \quad \textit{if } \lim_{n\to\infty} \alpha_n = -\infty. \tag{18}$$

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

$$\sigma n \leq P_n \tag{19}$$

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

$$\lim_{n\to\infty} P(n;\theta_n) = 1 \quad \textit{if } \lim_{n\to\infty} \alpha_n = \infty. \tag{20}$$

The condition (19) is weaker than the growth condition (11) used by Blackburn and Gerke [1]. It is also easy to check that Theorem 3.3 implies the zero-one law (10)-(12). However, Theorem 3.3 cannot hold if the condition (9) fails. This is a simple consequence of the following fact.

Lemma 3.4: *For any mapping $P : \mathbb{N}_0 \to \mathbb{N}_0$ for which the limit $\lim_{n\to\infty} P_n$ exists, we have*

$$\lim_{n\to\infty} P(n;(1,P_n)) = \begin{cases} 0 & \textit{if } \lim_{n\to\infty} P_n > 1 \\ \\ 1 & \textit{if } \lim_{n\to\infty} P_n = 1. \end{cases} \tag{21}$$

Proof. For $n = 2, 3, \ldots$ and any positive integer P_n, the graph $\mathbb{K}(n;(1,P_n))$ is connected if and only if all nodes choose the *same* key. This event happens with probability $P_n^{-(n-1)}$. The conclusion is now immediate once we observe that the condition $\lim_{n\to\infty} P_n = 1$ (resp. $\lim_{n\to\infty} P_n > 1$) requires $P_n = 1$ (resp. $P_n \geq 2$) for all $n = 1, 2, \ldots$ sufficiently large owing to P_n being integer. ■

IV. A BASIC OBSERVATION

Assume given a pair of positive integers K and P such that $K \leq P$, and pick $n = 2, 3, \ldots$. We define the events

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

and

$$A_n(\theta) := \left[\begin{array}{c} \text{All key rings of size } K \\ \text{have been distributed} \end{array}\right].$$

The event $A_n(\theta)$ is always empty under the condition

$$n < \binom{P}{K}. \tag{22}$$

The next observation provides an easy condition for graph connectivity in random key graphs.

Lemma 4.1: *For any given pair $\theta = (K, P)$ with $2 \leq K \leq P$, it is always the case that $\mathbb{K}(n;\theta)$ is connected whenever all the key rings of size K have been distributed, i.e.,*

$$A_n(\theta) \subseteq C_n(\theta). \tag{23}$$

Proof. Fix $2 \leq K \leq P$ and let ω be a sample that belongs to the event $A_n(\theta)$. Pick two distinct nodes, say $i, j = 1, \ldots, n$. We need to show that there is path between them in $\mathbb{K}(n;\theta)(\omega)$. If the key rings $K_i(\theta)(\omega)$ and $K_j(\theta)(\omega)$ have a non-empty intersection, then the two nodes are adjacent and there is a one hop path between them. On the other hand, if these key rings do not intersect, then it is necessarily the case that $2K \leq P$. Under these conditions it is possible to construct an element S of $\mathcal{P}_K$ such that $S \cap K_i(\theta)(\omega) \neq \emptyset$ and $S \cap K_j(\theta)(\omega) \neq \emptyset$. Note that such an argument could not be made for the case $K = 1$. Since all the key rings have been distributed in $\mathbb{K}(n;\theta)(\omega)$ it follows that there exists a node, say ℓ (possibly dependent on ω), distinct from both i and j, such that $K_\ell(\theta)(\omega) = S$. As a result, nodes i and j are connected by a two-hop path passing through ℓ. ■

On $A_n(\theta)$ the random key graph $\mathbb{K}(n;\theta)$ is connected and its *diameter* is therefore well defined. In fact, as should be clear from the proof of Lemma 4.1, on the event $A_n(\theta)$ we have

$$\text{Diam}[\mathbb{K}(n;\theta)] = \begin{cases} 1 & \text{if } P < 2K \\ \\ 2 & \text{if } P \geq 2K. \end{cases} \tag{24}$$

Along these lines, under the condition

$$\frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n}$$

with $c > 0$, Rybarczyk [9] has recently shown that

$$\text{diam}[\mathcal{K}(n;\theta_n)] \sim \frac{\log n}{\log\log n}$$

with high probability where $\mathcal{K}(n;\theta_n)$ is the largest connected component of $\mathbb{K}(n;\theta_n)$.

By virtue of Lemma 4.1, it is now natural to look for conditions under which the event $A_n(\theta)$ occurs with high probability. For this purpose we first consider its complement which corresponds to the event that *some* key ring of size K has *not* been distributed, namely

$$A_n(\theta)^c = \cup_{S\in\mathcal{P}_K} [K_1(\theta) \neq S, \ldots, K_n(\theta) \neq S].$$

By a union bound argument, we get

$$\begin{aligned}\mathbb{P}\left[A_n(\theta)^c\right] &\leq \sum_{S\in\mathcal{P}_K}\mathbb{P}\left[K_1(\theta)\neq S,\ldots,K_n(\theta)\neq S\right]\\ &= \sum_{S\in\mathcal{P}_K}\left(\prod_{i=1}^{n}\mathbb{P}\left[K_i\neq S\right]\right)\\ &= \sum_{S\in\mathcal{P}_K}\mathbb{P}\left[K_1\neq S\right]^n\\ &= \binom{P}{K}\left(1-\frac{1}{\binom{P}{K}}\right)^n \qquad (25)\end{aligned}$$

under the enforced probabilistic assumptions on key ring selection.

V. An easy one-law

Lemma 4.1 and the calculations following it suggest a very simple strategy to obtain versions of the one-law in random key graphs. Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$\binom{P_n}{K_n} \leq n \qquad (26)$$

for all $n = 1, 2, \ldots$ sufficiently large. On that range, it follows from (25) that

$$\begin{aligned}\mathbb{P}\left[A_n(\theta_n)^c\right] &\leq \binom{P_n}{K_n}\left(1-\frac{1}{\binom{P_n}{K_n}}\right)^n\\ &\leq \binom{P_n}{K_n}e^{-\frac{n}{\binom{P_n}{K_n}}} \qquad (27)\end{aligned}$$

by standard bounding arguments. The conclusion

$$\lim_{n\to\infty}\mathbb{P}\left[A_n(\theta_n)^c\right] = 0 \qquad (28)$$

then follows *provided* the condition

$$\lim_{n\to\infty}\binom{P_n}{K_n}e^{-\frac{n}{\binom{P_n}{K_n}}} = 0 \qquad (29)$$

holds under (26). This observation readily leads to the following one-law.

Lemma 5.1: *Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ such that (26) holds for all $n = 1, 2, \ldots$ sufficiently large. We have $\lim_{n\to\infty} P(n;\theta_n) = 1$ provided the condition (29) holds*

In the next three sections we use Lemma 5.1 to derive several one-laws under specific sets of assumptions.

VI. Fixed K and P

The next result has a well-known analog for Erdős-Renyi graphs.

Lemma 6.1: *For any given pair $\theta = (K, P)$ with $2 \leq K \leq P$, we have $\lim_{n\to\infty} P(n;\theta) = 1$.*

The pair $\theta = (K, P)$ with $2 \leq K \leq P$ corresponds to a scaling whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is given by

$$\alpha_n := n\frac{K^2}{P} - \log n, \quad n = 1, 2, \ldots$$

so that $\lim_{n\to\infty}\alpha_n = \infty$. The conclusion of Lemma 6.1 does not follow from either Theorem 3.1 or Theorem 3.3 since conditions (11) and (19) are not satisfied with $P_n \equiv P$. The result is nevertheless a consequence of Theorem 3.2; see comments following it as we note that condition (17) holds.

We give two proofs of Lemma 6.1, both based on the observation captured by Lemma 4.1.

Proof 1 – There is no loss of generality in assuming that the rvs $\{K_i(\theta),\ i = 1, 2, \ldots\}$ are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. The definition

$$\nu := \inf\left(n = 1, 2, \ldots :\ \{K_1(\theta), \ldots, K_n(\theta)\} = \mathcal{P}_K\right)$$

is then well posed (with the usual convention that $\nu = \infty$ if the defining set is empty). The $\mathbb{N}\cup\{\infty\}$-valued rv ν gives the smallest value of n for which all $\binom{P}{K}$ possible key rings are distributed in $\mathbb{K}(n;\theta)$. It is easy to see that $\nu < \infty$ a.s. so that

$$\lim_{n\to\infty}\mathbb{P}\left[n < \nu\right] = 0. \qquad (30)$$

This is a consequence of the fact that *simultaneously* we have

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left[K_i(\theta) = S\right] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K \quad a.s.$$

This is a consequence of the Strong Law of Large Numbers and of the fact that the set $\mathcal{P}_K$ is finite.

Now, for each $n = 2, 3, \ldots$, because $K \geq 2$, it follows from Lemma 4.1 that the graph $\mathbb{K}(n;\theta)$ is connected whenever $\nu \leq n$, whence

$$\begin{aligned}P(n;\theta) &= \mathbb{P}\left[C_n(\theta)\cap[\nu\leq n]\right] + \mathbb{P}\left[C_n(\theta)\cap[n<\nu]\right]\\ &= \mathbb{P}\left[\nu\leq n\right] + \mathbb{P}\left[C_n(\theta)\cap[n<\nu]\right].\end{aligned}$$

The desired conclusion is obtained upon letting n go to infinity in this last relation and making use of (30). ■

Proof 2 – It follows from (25) that

$$\mathbb{P}\left[A_n(\theta)\right] \geq 1 - \binom{P}{K}\left(1-\frac{1}{\binom{P}{K}}\right)^n$$

for all $n = 1, 2, \ldots$ sufficiently large to ensure $\binom{P}{K} \leq n$. The conclusion $\lim_{n\to\infty}\mathbb{P}\left[A_n(\theta)\right] = 1$ is now immediate and we get the result by making use of the inclusion (23). ■

VII. The case $\limsup_{n\to\infty} P_n < \infty$

Lemma 6.1 leads to a proof of the conjectured one-law for scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying the property

$$\bar{P} := \limsup_{n\to\infty} P_n = \inf_{n\geq 1}\left(\sup_{m\geq n} P_m\right) < \infty. \qquad (31)$$

Lemma 7.1: *For any admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (31). we have $\lim_{n\to\infty} P(n, \theta_n) = 1$.*

Here as well we give two different proofs.

Proof 1 – Given the integer-valued nature of the sequence $\{P_n,\ n = 1, 2, \ldots\}$ the finiteness assumption on $\bar{P}$ implies

that $\bar{P}$ is itself a finite integer. As a result, there exists a finite integer $n^\star$ such that $P_n \leq \bar{P}+1$ for all $n \geq n^\star$.

Under the admissibility constraint (9), there exists a finite number, say L, of distinct pairs $(K_1^\star, P_1^\star), \ldots, (K_L^\star, P_L^\star)$ such that for each $\ell = 1, \ldots, L$, it holds

$$2 \leq K_\ell^\star \leq P_\ell^\star \leq \bar{P}+1$$

and

$$(K_n, P_n) = (K_\ell^\star, P_\ell^\star), \quad n \in N_\ell$$

where $N_1, \ldots, N_L$ are disjoint and countably infinite subsets of $\mathbb{N}_0$ with

$$\cup_{\ell=1}^{L} N_\ell = \{n^{\star\star}, n^{\star\star}+1, \ldots\}$$

for some $n^{\star\star} \geq n^\star$ (so as to ensure set equality). Applying Lemma 6.1 we obtain

$$\lim_{n \in N_\ell} P(n; \theta_n) = 1, \quad \ell = 1, \ldots, L$$

where $\lim_{n \in N_\ell}$ indicates that the limit is taken with n going to infinity along the subsequence defined by N_ℓ. The conclusion $\lim_{n\to\infty} P(n, \theta_n) = 1$ easily follows from the fact that the sets $N_1, \ldots, N_L$ are disjoint, and that the limit points of these L subsequences coincide. ■

Proof 2 – Under the finiteness condition (31) we have

$$\limsup_{n\to\infty} \binom{P_n}{K_n} < \infty.$$

Hence, both conditions (26) and (29) hold, and the result follows from Lemma 5.1. ■

VIII. Small key pools with $K_n = 2$

With $K_n = 2$, we note that

$$\binom{P_n}{2} = \frac{P_n(P_n-1)}{2} \leq P_n^2, \quad n = 1, 2, \ldots.$$

Therefore, the condition (26) holds whenever

$$P_n^2 \leq n \tag{32}$$

for all $n = 1, 2, \ldots$ sufficiently large. Since the mapping $t \to te^{-\frac{n}{t}}$ is increasing on $(0, \infty)$, the convergence condition (29) is implied whenever

$$\lim_{n\to\infty} P_n^2 e^{-\frac{n}{P_n^2}} = 0. \tag{33}$$

This observation leads to the following one-law.

Lemma 8.1: *Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (13) such that*

$$P_n = O(n^\delta) \tag{34}$$

for some δ in $(0, \frac{1}{2})$. Then we have

$$\lim_{n\to\infty} P(n; (2, P_n)) = 1.$$

This is of course a weaker version of Theorem 3.2 but as the discussion below shows, its proof is much simpler and comes with the additional benefit of pointing out the underlying reason for connectivity when P_n is *much smaller* than n – In that case it is very likely that all the possible key rings are eventually assigned!

Proof. Condition (34) implies the existence of a constant $C > 0$ such that

$$P_n \leq Cn^\delta, \quad n \geq n^\star$$

for some finite integer $n^\star$. Therefore, (32) is automatically satisfied for δ in the prescribed range and condition (26) holds.

Next, by the aforementioned monotonicity, we also get

$$P_n^2 e^{-\frac{n}{P_n^2}} \leq C^2 n^{2\delta} e^{-C^{-2} n^{1-2\delta}}, \quad n \geq n^\star$$

and the convergence (33) follows since we have $2\delta < 1$ here. The desired conclusion is now immediate by Lemma 5.1. ■

As was the case with Theorem 3.2, it follows from (16) and Lemma 8.1 that $\lim_{n\to\infty} P(n; \theta_n) = 1$ whenever

$$2 \leq K_n \leq P_n$$

for all $n = 1, 2, \ldots$ sufficiently large under the condition (34) with δ in $(0, \frac{1}{2})$.

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," *Discrete Mathematics* **309** (2009), pp. 5130-5140.

[2] B. Bollobás, *Random Graphs*, Second Edition, 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, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[4] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.* **5** (1960), pp. 17-61.

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

[6] E. Godehardt and J. Jaworski "Two models of random intersection graphs for classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **22**, Eds. O. Optiz and M. Schwaiger, Springer, Berlin (2003), pp. 67-82.

[7] E. Godehardt, J. Jaworski and K. Rybarczyk, "Random intersection graphs and classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **33**, Eds. H.J. Lens and R,. Decker, Eds., Springer, Berlin (2007), pp. 67-74.

[8] P. Marbach, "A lower-bound on the number of rankings required in recommender systems using collaborative filtering," Proceedings of the 42nd Annual Conference on Information Sciences and Systems (CISS 2008), Princeton University, Princeton (NJ), March 2008.

[9] K. Rybarczyk "Diameter, connectivity and phase transition of the uniform random intersection graph," Submitted to *Discrete Mathematics*, July 2009.

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

[11] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," Proceedings of the IEEE International Symposium on Information Theory (ISIT 2009), Seoul (Korea), June 2009.

[12] O. Yağan and A. M. Makowski, "Random key graphs – Can they be small worlds?," Proceedings of the First Workshop on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks, Chennai (India), December 2009.

[13] O. Yağan and A. M. Makowski, "Connectivity in random graphs induced by a key predistribution scheme – Small key pools," Accepted for inclusion in the program of the International Conference on Information and Communication Systems (ICICS 2009), Amman (Jordan), December 2009. Withdrawn.

[14] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Submitted to *IEEE Transactions on Information Theory*, January 2010. Available online at arXiv:0908.3644v1 [math.CO]. Earlier draft available online at http://hdl.handle.net/1903/8716, January 2009.