THE INSTITUTE FOR SYSTEMS RESEARCH

ISR TECHNICAL REPORT 2009-4

Amllcargtgrw gl p_lbmk icw ep_nfq -
Qgknjc npmmdq dmp qncag_j a_qcq

Mqk_l W_e_l _lb ?pk_lb K, K_imuqig

Connectivity in random key graphs – Simple proofs for special cases

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 some special cases.**

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

I. Introduction

It is envisioned that security will be a key issue in wireless sensor networks given that they are usually deployed in hostile environments. Because traditional methods have been found inadequate for such networks, the following random key predistribution scheme proposed by Eschenauer and Gligor [6] has instead received some attention: Before the deployment of network, 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 share at least one key; see [6] for implementation details.

Under the assumption of *full visibility*, namely that nodes are all within communication range of each other, the constraint of being within transmission range is always in effect and a secure link can be established between two nodes whenever their key rings have at least one key in common. 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.

It is natural to seek conditions on n, K and P under which $\mathbb{K}(n;(K,P))$ is a connected graph with high probability – Such conditions might be helpful in dimensioning this distribution scheme in the context of wireless sensor networks. As explained in Section III, this search has lead to *conjecturing* the following zero-one law for graph connectivity in $\mathbb{K}(n;(K.P))$: 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 $\alpha : \mathbb{N}_0 \rightarrow \mathbb{R}$, 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], [11].

Progress has recently been made on this conjecture by the authors [13] and by others [1], [4]. The proof of our main results is rather long and technically involved, and is therefore omitted given the page limitations; it can be found in [13] with an outline available in [12]. Instead, we discuss a number of situations that are not considered in [13] for which the conjectured zero-one law can be easily recovered. In that sense this short paper should be viewed as a complement to the papers [12], [13].

The rest of the paper is organized as follows: In Section II we formally introduce the class of random key graphs. Section IV is devoted to a brief review of recent results followed in Section V by a key observation leading to the main results of the paper. In section VII we report on the results regarding to the conjecture for the case where K and P are fixed. The case where $\limsup_{n\to\infty} P_n < \infty$ is considered in Section VIII and we conclude by the discussion of the case where $K = 2$ and $P_n = n^\delta$ for some $0 < \delta < \frac{1}{2}$ in Section IX.

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 which are *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 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

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

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 completely regular graph $K_{n,n}$.

Random key graphs, which form a subclass in the family of *random intersection* graphs, are also called *uniform intersection* graphs by some authors [1]. They have been discussed recently in several application contexts, e.g., security of wireless sensor networks [1] [4], clustering analysis [7] [8] and recommender systems using global filtering [9].

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

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

III. Origins of the conjecture

As indicated earlier, we wish to select P and K so that $P(n; \theta)$ is as large (i.e., as close to one) as possible. In their original work, Eschenauer and Gligor [6] approached this issue as follows:

(i) Let $\mathbb{G}(n; p)$ denote the Erdős-Renyi graph on n vertices with edge probability p ($0 < p \leq 1$) [2], [5]. Despite strong similarities, random key graphs are *not* statistically equivalent to Erdős-Renyi graphs. This is so because edge assignments are correlated in $\mathbb{K}(n; \theta)$ but independent in $\mathbb{G}(n; p)$. Yet, setting aside this fact, they boldly replaced $\mathbb{K}(n; \theta)$ by a proxy Erdős-Renyi graph $\mathbb{G}(n; p)$ with p and θ are related through

$$p = 1 - q(\theta). \tag{7}$$

This constraint ensures that link assignment probabilities in $\mathbb{K}(n; \theta)$ and $\mathbb{G}(n; p)$ coincide.

(ii) In Erdős-Renyi graphs the property of graph connectivity is known to exhibit the following zero-one law [2]: If we scale the edge assignment probability p according to

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

for some sequence $\alpha : \mathbb{N}_0 \rightarrow \mathbb{R}$, then

$$\begin{aligned} &\lim_{n \to \infty} \mathbb{P}\left[\mathbb{G}(n; p_n) \text{ is connected}\right] \\ &= \begin{cases} 0 & \text{if } \ \lim_{n \to \infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \ \lim_{n \to \infty} \alpha_n = +\infty. \end{cases} \end{aligned} \tag{9}$$

(iii) Under the substitution (7), these classical results suggest scaling the parameters K and P with n according to

$$1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{10}$$

for some sequence $\alpha : \mathbb{N}_0 \rightarrow \mathbb{R}$. In view of (9) it is then not too unreasonable to expect that the following zero-one law

$$\lim_{n \to \infty} P(n; \theta_n) = \begin{cases} 0 & \text{if } \ \lim_{n \to \infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \ \lim_{n \to \infty} \alpha_n = +\infty \end{cases} \tag{11}$$

should hold.

Of course, for this approach to be operationally useful, a good approximation to the right handside of (7) is needed. Eschenauer and Gligor provided such an approximation with the help of Stirling's formula. However, as already indicated by DiPietro et al. [3], [4], it is easy to check that

$$1 - \frac{\binom{P-K}{K}}{\binom{P}{K}} \simeq \frac{K^2}{P} \tag{12}$$

under reasonable assumptions. Thus, if instead of scaling the parameters according to (10), we scale them according to (1), it is natural to conjecture that the zero-one law (11) should still hold.

IV. Recent results

We now turn to recently obtained results [1], [13] concerning (1)-(2). To fix the terminology, any pair of functions $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ is said to define a *scaling*, and we can always associate with it a sequence $\alpha : \mathbb{N}_0 \rightarrow \mathbb{R}$ through the relation

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{13}$$

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

$$K_n \leq P_n, \quad n = 1, 2, \ldots \tag{14}$$

and

$$2 \leq K_n \tag{15}$$

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. [4, Thm. 4.6].

Theorem 4.1: Consider an admissible scaling $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$. *Then, we always have*

$$\lim_{n \to \infty} P(n; \theta_n) = 0 \quad \textit{if} \quad \limsup_{n \to \infty} \frac{K_n^2}{P_n} \frac{n}{\log n} < 1. \tag{16}$$

Under the additional assumption

$$n \leq P_n \tag{17}$$

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

$$\lim_{n\to\infty} P(n;\theta_n) = 1 \quad \textit{if} \quad \liminf_{n\to\infty} \frac{K_n^2}{P_n}\frac{n}{\log n} > 1. \tag{18}$$

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 4.2: 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 (13), namely*

$$\frac{4}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{19}$$

If

$$K_n = 2, \quad n = 1, 2, \ldots \tag{20}$$

then we have

$$\lim_{n\to\infty} P(n;(2,P_n)) = \begin{cases} 0 & \textit{if } \lim_{n\to\infty}\alpha_n = -\infty \\ \\ 1 & \textit{if } \lim_{n\to\infty}\alpha_n = \infty. \end{cases} \tag{21}$$

In Theorem 4.2 there are no constraints on the size of the key pool. Equipped with this result, it is now a small step to conclude that (1)-(2) does hold when $2 \leq K_n \leq P_n$ whenever

$$P_n = o\left(\frac{n}{\log n}\right). \tag{22}$$

The next result is due to Yağan and Makowski; it generalizes Theorem 4.1, and complements Theorem 4.2. A complete proof can be found in [13].

Theorem 4.3: 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 (13). We have*

$$\lim_{n\to\infty} P(n;\theta_n) = 0 \quad \textit{if } \lim_{n\to\infty}\alpha_n = -\infty. \tag{23}$$

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

$$\sigma n \leq P_n \tag{24}$$

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

$$\lim_{n\to\infty} P(n;\theta_n) = 1 \quad \textit{if } \lim_{n\to\infty}\alpha_n = \infty. \tag{25}$$

The condition (24) is weaker than the growth condition (17) used by Blackburn and Gerke [1]. It is also easy to check that Theorem 4.3 implies the zero-one law (16)-(18). Note that Theorem 4.3 cannot hold if the condition (15) fails. This is a simple consequence of the following simple observation.

Lemma 4.4: For any mapping $P : \mathbb{N}_0 \to \mathbb{N}_0$ *for which the limit* $\lim_{n\to\infty} P_n$ *exists, we have*

$$\lim_{n\to\infty} P(n;(1,P_n)) = \begin{cases} 0 & \textit{if } \lim_{n\to\infty} P_n > 1 \\ \\ 1 & \textit{if } \lim_{n\to\infty} P_n = 1. \end{cases} \tag{26}$$

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. ■

V. A BASIC OBSERVATION

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

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

and

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

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

$$n < \binom{P}{K}. \tag{27}$$

The next observation provides an easy condition for graph connectivity in the random key graph $\mathbb{K}(n;\theta)$.

Lemma 5.1: It is always the case that $\mathbb{K}(n;\theta)$ *is connected whenever all the key rings have been assigned, i.e.,*

$$A_n(\theta) \subseteq C_n(\theta). \tag{28}$$

Proof. 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 must necessarily be the case that $2K \leq P$. Under these conditions it is possible to construct an element S of $\mathcal{P}_K$ with the property that $S \cap K_i(\theta)(\omega) \neq \emptyset$ and $S \cap K_j(\theta)(\omega) \neq \emptyset$. 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. ■

Corollary 5.2: On $A_n(\theta)$ the random key graph $\mathbb{K}(n;\theta)$ has *diameter* either 1 or 2. Indeed, as should be clear from the proof of Lemma 5.1, we have

$$\text{Diam}[\mathbb{K}(n;\theta)] = \begin{cases} 1 & \text{if } P < 2K \\ \\ 2 & \text{if } P \geq 2K. \end{cases} \tag{29}$$

By virtue of Lemma 5.1, it is now natural to look for the conditions for which the event $A_n(\theta)$ occurs with high probability. For this purpose we first consider the complement of $A_n(\theta)$ which corresponds to the event where *some* key ring has *not* been distributed, namely

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

As a result, by a union bound argument, we get

$$\begin{aligned} \mathbb{P}\left[A_n(\theta)^c\right] &\leq \sum_{S \in \mathcal{P}_K} \mathbb{P}\left[K_1(\theta) \neq S, \ldots, K_n(\theta) \neq S\right] \\ &= \sum_{S \in \mathcal{P}_K} \left(\prod_{i=1}^{n} \mathbb{P}\left[K_i \neq S\right] \right) \\ &= \sum_{S \in \mathcal{P}_K} \mathbb{P}\left[K_1 \neq S\right]^n \\ &= \binom{P}{K} \left(1 - \frac{1}{\binom{P}{K}}\right)^n \qquad (30) \end{aligned}$$

under the enforced assumptions on key ring selection.

VI. An easy one-law

Lemma 5.1 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 $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ such that

$$\binom{P_n}{K_n} \leq n \qquad (31)$$

for all $n = 1, 2, \ldots$ sufficiently large. On that range, from (30) we get

$$\begin{aligned} \mathbb{P}\left[A_n(\theta_n)^c\right] &\leq \binom{P_n}{K_n} \left(1 - \frac{1}{\binom{P_n}{K_n}}\right)^n \\ &\leq \binom{P_n}{K_n} e^{-\frac{n}{\binom{P_n}{K_n}}} \qquad (32) \end{aligned}$$

by standard bounding arguments. The conclusion

$$\lim_{n \rightarrow \infty} \mathbb{P}\left[A_n(\theta_n)^c\right] = 0 \qquad (33)$$

follows *provided*

$$\lim_{n \rightarrow \infty} \binom{P_n}{K_n} e^{-\frac{n}{\binom{P_n}{K_n}}} = 0 \qquad (34)$$

under (31). This discussion readily leads to the following one law.

Lemma 6.1: Consider an admissible scaling $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ such that (31) holds for all $n = 1, 2, \ldots$ sufficiently large. We have

$$\lim_{n \rightarrow \infty} P(n; \theta_n) = 1 \qquad (35)$$

provided the condition (34) holds

In the next three sections we use Lemma 6.1 to derive several zero-one laws under specific sets of assumptions.

VII. Fixed K and P

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

Lemma 7.1: For any given pair $\theta = (K, P)$ with $2 \leq K \leq P$, we have $\lim_{n \rightarrow \infty} P(n; \theta) = 1$.

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

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

so that $\lim_{n \rightarrow \infty} \alpha_n = \infty$. The conclusion of Lemma 7.1 does not follow from either Theorem 4.1 or Theorem 4.3 since conditions (17) and (24) are not satisfied with $P_n = P$ for all $n = 1, 2, \ldots$. The result is nevertheless a consequence of Theorem 4.2; see comments following it as we note that condition (22) holds.

We give two proofs of Lemma 7.1, both based on the observation captured by Lemma 5.1.

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 $\mathbb{N}^\star$-valued rv so defined 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. This is a consequence of the fact that for every S in $\mathcal{P}_K$ we have

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

by the Strong Law of Large Numbers.

Now, for each $n = 2, 3, \ldots$, because $K \geq 2$, the graph $\mathbb{K}(n; \theta)$ is connected whenever $\nu \leq n$, by Lemma 5.1, 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. ■

Proof 2 – It follows from (30) 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 that $\binom{P}{K} \leq n$. The conclusion $\lim_{n \rightarrow \infty} \mathbb{P}\left[A_n(\theta)\right] = 1$ is now immediate and we get the result by making use of the inclusion (28). ■

VIII. The case $\lim_{n\to\infty} P_n < \infty$

Lemma 7.1 leads to a proof of the conjectured one law for scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ with the property

$$\bar{P} := \limsup_{n\to\infty} P_n = \inf_{n\geq 1}\left(\sup_{m\geq n} P_m\right) < \infty. \tag{36}$$

Lemma 8.1: For any admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ *satisfying (36). 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 constraints (14) and (15), 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 $2 \leq K_\ell^\star$ and $2K_\ell^\star \leq P_\ell^\star$ for each $\ell = 1, \ldots, L$ with the property that

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

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 7.1 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 (36) we have

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

by admissibility of the scaling. Hence, both conditions (31) and (34) hold, and the result follows from Lemma 6.1. ■

IX. Small key pools with $K_n = 2$

With $K_n = 2$, the condition (31) reads

$$\frac{P_n(P_n - 1)}{2} \leq n \tag{37}$$

for all $n = 1, 2, \ldots$ sufficiently large. Since the mapping $t \to te^{-\frac{2n}{t}}$ is increasing on $(0, \infty)$, the convergence condition (34) is implied by

$$\lim_{n\to\infty} P_n^2 e^{-\frac{2n}{P_n^2}} = 0. \tag{38}$$

This leads to the following one-law.

Lemma 9.1: Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ *satisfying (20) such that*

$$P_n = O(n^\delta) \tag{39}$$

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 4.2 but as the discussion below shows, its proof is much simpler and comes with the additional benefit of getting the underlying reason of having connectivity when P_n is *much smaller* than n–In that case it is very likely that all of the possible key rings are assigned!

As was the case with Theorem 4.2, Lemma 9.1 implies $\lim_{n\to\infty} P(n; \theta_n) = 1$ whenever

$$2 \leq K_n \leq P_n$$

for all $n = 1, 2, \ldots$ sufficiently large under the condition (39) for some δ in $(0, \frac{1}{2})$.

Proof. The condition (31) is automatically satisfied under (39). Also there exist a constant $C > 0$ and a finite integer $n^\star$ such that

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

On that range, we get

$$P_n^2 e^{-\frac{2n}{P_n^2}} \leq C^2 n^{2\delta} e^{-2Cn^{1-2\delta}}$$

and the desired conclusion is now immediate as we appeal to Lemma 6.1. ■

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," in *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

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

[6] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the CCS 2002, Washington (DC), November 2002, pp. 41-47.

[7] 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.

[8] 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.

[9] P. Marbach, "A lower-bound on the number of rankings required in recommender systems using collaborativ filtering," CISS 2008, Princeton University, Princeton (NJ), March 2008.

[10] K.B. Singer, *Random Intersection Graphs*, Ph.D. Thesis, The Johns Hopkins University, Baltimore (MD), 1995.

[11] 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, Toronto (ON, Canada), June 2008.

[12] O. Yağan and A.M. Makowski, "Connectivity results for random key graphs," submitted to the program of the ISIT 2009, Seoul (S. Korea).

[13] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Available online at http://www.lib.umd.edu/drum/, January 2009.