2009 First International Conference on Networks & Communications

Random key graphs – Can they be small worlds?

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— **Random key graphs form a class of random graphs naturally associated with the random key predistribution scheme of Eschenauer and Gligor. We compute the clustering coefficients of random key graphs, and then compare them with Erdős-Renyi graphs in the many node regime when the expected average degrees are asymptotically equivalent. On the parameter range of practical relevance in wireless sensor networks, random key graphs are shown to be much more clustered than the corresponding Erdős-Renyi graphs. We also explore the suitability of random key graphs as small worlds in the sense of Watts and Strogatz.**

Keywords: Wireless sensor networks, Security, Key predistribution, Random key graphs, Clustering coefficient, Small world networks.

I. Introduction

Random key graphs have recently been used by Di Pietro et al. [4] to model the random key predistribution scheme of Eschenauer and Gligor [6]. The EG scheme is by now a widely accepted solution for establishing secure connectivity in wireless sensor networks (WSNs) and can be summarized as follows: Before network deployment, each sensor randomly selects K distinct cryptographic keys from a pool of P keys. These K keys form 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 (wireless) transmission range of each other and if their key rings have at least one key in common; see [6] for details.

If we assume that nodes are all within communication range of each other, a situation referred to as *full visibility*, then a secure link can be established between two nodes whenever their key rings have at least one key in common. It is this notion of adjacency which defines the class of *random key* graphs; see Section II for precise definitions.

In determining the feasibility of the EG scheme for WSNs, much effort has been focused on connectivity. In [6] Eschenauer and Gligor analyzed the connectivity of random key graphs by matching them to Erdős-Renyi graphs with identical link probabilities. This approach has served as a point of departure for conjecturing various zero-one laws for connectivity in random key graphs [1], [15]; see the papers [1], [4], [13], [16], [17] for recent developments.

Encouraged by this success, it is natural to wonder whether this "transfer" from Erdős-Renyi graphs to random key graphs applies to other graph properties as well. In the affirmative this would express some form of asymptotic equivalence between random key graphs and Erdős-Renyi graphs, similar to the one obtained for a certain family of random intersection graphs in [7].

We approach this issue by comparing the *clustering coefficients* of the two classes of random graphs. We observe that the clustering coefficient of a random key graph is never smaller than the clustering coefficient of the corresponding Erdős-Renyi graph with *identical* expected average degree. For the parameter range that is practically relevant for large WSNs, we show that random key graphs are *much more clustered* than Erdős-Renyi graphs when expected average degrees are asymptotically equivalent. We also show that the asymptotic equivalence of the two models (in a sense discussed in Section V-A) is possible only when the size of key rings is comparable to the network size, a case not very realistic in WSNs where sensors have limited memory and computational capabilities. This points to the inadequacy of Erdős-Renyi graphs to capture some key properties of the EG scheme in realistic WSN scenarios, and reinforces the call for a direct investigation of random key graphs.

Random key graphs have also appeared in other application areas such as clustering and classification analysis [8], [9], and recommender systems [10], and their study is therefore of interest beyond the context of WSNs. Moreover, building on the observation that random key graphs can display high clustering, we explore whether there are parameter ranges for which the random key graphs exhibit *small world* characteristics in the sense of Watts and Strogatz [14].

The paper is organized as follows: In Section II we formally introduce the class of random key graphs while in Section III, we define ways to match random key graphs to Erdős-Renyi graphs. The main results of the paper, summarized by Theorems 4.1 and 4.3, are presented in Section IV with proofs provided in Section VI and Section VII, respectively. Implications of the results are discussed in Section V.

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 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

978-0-7695-3924-9/09 $26.00 © 2009 IEEE
DOI 10.1109/NetCoM.2009.55

$K_i(\theta)$ 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

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

for all $i = 1,\ldots,n$. This corresponds to selecting keys randomly and *without* replacement. Distinct nodes $i, j = 1,\ldots,n$ are said to be adjacent if they share at least one key in their key rings, namely

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset, \tag{2}$$

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 $\mathbb{K}(n;\theta)$.

For distinct $i, j = 1,\ldots,n$, it is easy to check that

$$\mathbb{P}\left[K_i(\theta) \cap K_j(\theta) = \emptyset\right] = q(\theta) \tag{3}$$

with

$$q(\theta) = \begin{cases} 0 & \text{if } \; P < 2K \\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } \; 2K \leq P, \end{cases} \tag{4}$$

whence the probability of link occurrence between any two nodes is $1 - q(\theta)$. The expression (3)-(4) is a simple consequence of the fact that

$$\mathbb{P}\left[S \cap K_i(\theta) = \emptyset\right] = \frac{\binom{P-|S|}{K}}{\binom{P}{K}}, \quad i = 1,\ldots,n \tag{5}$$

for every subset S of $\{1,\ldots,P\}$ with $|S| \leq P - K$. From (4), it is easy to check that $0 \leq q(\theta) < 1$ with $q(\theta) > 0$ if and only if $2K \leq P$.

For distinct $i, j = 1,\ldots,n$, let $E_{ij}(\theta)$ denote the event where (2) takes place. The degree $D_{n,i}(\theta)$ of node i in $\mathbb{K}(n;\theta)$ is then given by

$$D_{n,i}(\theta) := \sum_{j=1, j\neq i}^{n} \mathbf{1}\left[E_{ij}(\theta)\right], \quad i = 1,\ldots,n \tag{6}$$

while the average degree is defined by

$$\bar{D}_n(\theta) := \frac{1}{n}\sum_{i=1}^{n} D_{n,i}(\theta). \tag{7}$$

III. Matching random key graphs

In what follows we shall compare random key graphs to related Erdős-Renyi graphs [5]. We first introduce some notation: For each p in $[0,1]$ let $\mathbb{G}(n;p)$ denote the Erdős-Renyi graph on the vertex set $\{1,\ldots,n\}$ with link assignment probability p. In analogy with earlier notation let $E_{ij}(p)$ denote the event where there is an (undirected) link assigned between the distinct nodes i and j. Thus, the random graph $\mathbb{G}(n;p)$ is characterized by having the $\frac{n(n-1)}{2}$ (undirected) links between the n nodes be independently assigned with probability p, i.e., the events $\{E_{ij}(p),\ 1 \leq i < j \leq n\}$ are mutually independent events, each of probability p – Of course it is always understood that $E_{ij}(p) = E_{ji}(p)$ for distinct $i, j = 1,\ldots,n$. In analogy with (6) and (7), the degree $D_{n,i}(p)$ of node i in $\mathbb{G}(n;p)$ is now defined as

$$D_{n,i}(p) := \sum_{j=1, j\neq i}^{n} \mathbf{1}\left[E_{ij}(p)\right], \quad i = 1,\ldots,n \tag{8}$$

and the average degree is given by

$$\bar{D}_n(p) := \frac{1}{n}\sum_{i=1}^{n} D_{n,i}(p). \tag{9}$$

We can match random key graphs with Erdős-Renyi graphs in a number of ways. One possibility is to fix the number n of nodes and then equate their expected average degrees.

Definition 3.1: Fix $n = 2, 3, \ldots$. With p in $[0,1]$ and positive integers K and P such that $K \leq P$, we say that $\mathbb{G}(n;p)$ is matched to $\mathbb{K}(n;\theta)$ if $\mathbb{E}\left[\bar{D}_n(p)\right] = \mathbb{E}\left[\bar{D}_n(\theta)\right]$.

For each $n = 2, 3, \ldots$, exchangeability yields

$$\mathbb{E}\left[\bar{D}_n(\theta)\right] = (n-1)(1 - q(\theta)) \tag{10}$$

and

$$\mathbb{E}\left[\bar{D}_n(p)\right] = (n-1)p \tag{11}$$

so that $\mathbb{G}(n;p)$ is matched to $\mathbb{K}(n;\theta)$ if $p = 1 - q(\theta)$.

When the parameters K and P vary with the number n of nodes, we modify Definition 3.1 as follows: Let any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying the natural condition

$$K_n \leq P_n \quad n = 1, 2, \ldots$$

define a *scaling* for random key graphs. Similarly, let any mapping $p : \mathbb{N}_0 \to [0,1]$ be a scaling for Erdős-Renyi graphs. The notion of *asymptotic matching* can now be introduced relative to such scalings.

Definition 3.2: The scalings $p : \mathbb{N}_0 \to [0,1]$ and $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ are asymptotically matched if

$$\mathbb{E}\left[\bar{D}_n(p_n)\right] \sim \mathbb{E}\left[\bar{D}_n(\theta_n)\right]. \tag{12}$$

In view of (10) and (11) this condition is equivalent to

$$p_n \sim (1 - q(\theta_n)). \tag{13}$$

A more compact form of (13) is available when the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfies the additional condition $\lim_{n\to\infty} q(\theta_n) = 1$. This is a consequence of the following result already obtained in [17, Lemma 8.3].

Lemma 3.3: For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, we have

$$\lim_{n\to\infty} q(\theta_n) = 1 \quad \textit{if and only if} \quad \lim_{n\to\infty} \frac{K_n^2}{P_n} = 0, \tag{14}$$

and under either condition the asymptotic equivalence

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n} \tag{15}$$

holds.

Under (14) the scaling $p : \mathbb{N}_0 \to [0,1]$ is asymptotically matched to the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ if and only if

$$p_n \sim \frac{{K_n}^2}{P_n}. \tag{16}$$

Since $1 \leq K_n \leq {K_n}^2$ for all $n = 1, 2, \ldots$, the condition (14) also implies

$$\lim_{n\to\infty} \frac{K_n}{P_n} = 0. \tag{17}$$

IV. Main results

A. Computing clustering coefficients

There are several possible definitions for clustering coefficients in graphs [12], and the following definition is a popular one: The clustering coefficient of an undirected graph G with vertex set $\{1, \ldots, n\}$ is often defined as the "fraction of transitive triples" given by

$$C^\star(G) := \frac{3 \times \text{number of triangles in } G}{\frac{1}{2}\sum_{i=1}^n d_i(d_i - 1)} \tag{18}$$

where d_i is the degree of node i in G. Related but simpler definitions are possible when considering random graphs with exchangeable link assignments (as is the case for the random graphs of interest here), e.g., [3]. Here we define the clustering coefficients of the random key graph $\mathbb{K}(n;\theta)$ and of the Erdős-Renyi graph $\mathbb{G}(n;p)$ by

$$C(\theta) = \mathbb{P}\left[E_{12}(\theta) \mid E_{13}(\theta) \cap E_{23}(\theta)\right] \tag{19}$$

and

$$C(p) = \mathbb{P}\left[E_{12}(p) \mid E_{13}(p) \cap E_{23}(p)\right], \tag{20}$$

respectively. These quantities are expected to provide a good approximation for (18) when n is large with

$$\lim_{n\to\infty} C^\star(\mathbb{K}(n;\theta)) = C(\theta) \quad a.s. \tag{21}$$

and

$$\lim_{n\to\infty} C^\star(\mathbb{G}(n;p)) = C(p) \quad a.s. \tag{22}$$

Although the authors are not aware of arguments formally validating (21) and (22), simulation results do support both claims; see Table I in Section IV-B. As a result, throughout we shall use instead the simpler definitions (19)-(20) for reasons of analytical tractability.

B. Fixed parameters θ and p

The case of *fixed* parameters is presented first.

Theorem 4.1: For positive integers K, P such that $K \leq P$, we have

$$\frac{C(\theta)}{C(p(\theta))} = 1 + \frac{q(\theta)^2 - r(\theta)}{(1 - q(\theta))^3} \cdot q(\theta) \tag{23}$$

with $p(\theta) := 1 - q(\theta)$ and

$$r(\theta) := \begin{cases} 0 & \text{if } P < 3K \\ \frac{\binom{P-2K}{K}}{\binom{P}{K}} & \text{if } 3K \leq P. \end{cases} \tag{24}$$

K	P	$C(\theta)$	$\widehat{C}_n^\star(\theta)$	$C(p)$	$\widehat{C}_n^\star(p)$
4	10^3	0.2590	0.2587	0.0160	0.0159
8	5×10^3	0.1348	0.1349	0.0127	0.0128
16	2×10^4	0.0737	0.0736	0.0127	0.0128
20	4×10^4	0.0590	0.0590	0.0100	0.0100
24	10^5	0.0469	0.0468	0.0057	0.0057
32	10^5	0.0408	0.0408	0.0102	0.0102
40	5×10^5	0.0280	0.0280	0.0032	0.0031
64	10^6	0.0196	0.0196	0.0041	0.0041

TABLE I
CLUSTERING COEFFICIENTS FOR FIXED θ AND $p = 1 - q(\theta)$

The proof of Theorem 4.1 is given in Section VI. Since $r(\theta) \leq q^2(\theta)$ by direct inspection, we conclude from (23) that

$$\frac{C(\theta)}{C(p(\theta))} \geq 1. \tag{25}$$

Thus, the clustering coefficient of a random key graph is at least as large as that of the Erdős-Renyi graph matched to it. In fact, the lower bound in (25) is achieved only when $P < 2K$, i.e., from (4) we get

$$\frac{C(\theta)}{C(p(\theta))} = 1, \quad P < 2K.$$

It is a simple matter to check that for $K = 1$, (23) reads

$$\frac{C(1,P)}{C(p(\theta))} = P, \quad P = 1, 2, \ldots,$$

while for $K = 2$ we have

$$\frac{C(2,P)}{C(p(\theta))} = \frac{P}{2} \cdot \frac{2P^3 - 4P^2 - P + 3}{(2P-3)^3} \geq \frac{P}{8}, \quad P = 2, 3, \ldots.$$

It is also straightforward to show that

$$1 \leq \frac{C(\theta)}{C(p(\theta))} \leq P.$$

In WSNs the size of the key pool P is expected to be in the range $2^{17} - 2^{20}$ [6]. Thus, as P can be made very large, the parameters can be selected so that the corresponding random key graph has a much larger clustering coefficient than the Erdős-Renyi graph matched to it. In Table I we compare the clustering coefficients of random key graphs and Erdős-Renyi graphs for several realistic parameter values. The numerical values of $C(p)$ and $C(\theta)$ are obtained directly from the expressions (33) and (44), respectively. On the other hand, $\widehat{C}_n^\star(\theta)$ and $\widehat{C}_n^\star(p)$ stand for the clustering coefficient of $\mathbb{K}(n;\theta)$ and $\mathbb{G}(n;p)$, respectively, calculated through (18) and averaged over 1000 realizations; the number of nodes is set to $n = 1000$ in all simulations. The data support the claim that the definitions (18) and (19)-(20) capture essentially the same feature, i.e., the results given in Table I can be taken as an indication of the validity of (21)-(22).

C. Zero-one laws for connectivity

Before dealing in Section IV-D with the situation where the parameters vary with n, we summarize the relevant zero-one laws for connectivity in the two classes of random graphs. The

following zero-one law for Erdős-Renyi graphs is well known [5]: For any scaling $p : \mathbb{N}_0 \to [0,1]$ satisfying

$$p_n \sim c \cdot \frac{\log n}{n} \tag{26}$$

for some $c > 0$, it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n; p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c. \end{cases}$$

Analogous results are available for random key graphs; see the recent papers [1], [4], [13], [17].

Theorem 4.2: For any scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying

$$\frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \tag{27}$$

for some $c > 0$, it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \theta_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c. \end{cases}$$

The version given in Theorem 4.2 is not the strongest to be found in the literature – For instance, it has nothing to say when $P_n = O(n^\delta)$ for some $0 < \delta < 1$; see [1] for an alternative formulation covering this situation. However the form of the condition (27) has the advantage of naturally suggesting a formal similarity between the zero-one laws for graph connectivity in random key graphs and in Erdős-Renyi graphs. Indeed one easily passes from one to the other with the help of the following observation: In random key graphs the term $\frac{K_n^2}{P_n}$ can be interpreted as a proxy for the probability of link assignment,[1] and therefore plays a role analogous to that of p_n in Erdős-Renyi graphs.

D. Parameters θ and p varying with n

It is now natural to wonder if the transfer above can also be used in studying other (if not all) graph properties. In the affirmative this would suggest some form of *asymptotic equivalence* between random key graphs and Erdős-Renyi graphs whenever the asymptotic matching condition (13) is satisfied. A similar situation was encountered for the family of random intersection graphs discussed in [7]. However, this possibility is already dispelled here by observations made in [1] and [4] that random key graphs are likely to have many more *triangles* than Erdős-Renyi graphs. The next result formally shows that the clustering coefficients of the two random graphs can indeed be quite different, especially for the parameter range of practical interest in the context of WSNs. A proof is given in Section VII.

Theorem 4.3: Consider a scaling $p : \mathbb{N}_0 \to [0,1]$ that is asymptotically matched to the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. Under condition (14) we have

$$\frac{C(\theta_n)}{C(p_n)} \sim 1 + \frac{P_n}{K_n^3}. \tag{28}$$

[1]This is indeed the case under the conditions of Lemma 3.3.

In particular, under the assumptions of Theorem 4.3, we find

$$\lim_{n\to\infty} \frac{C(\theta_n)}{C(p_n)} = 1 \quad \text{if} \quad \lim_{n\to\infty} \frac{K_n^3}{P_n} = \infty \tag{29}$$

and

$$\lim_{n\to\infty} \frac{C(\theta_n)}{C(p_n)} = \infty \quad \text{if} \quad \lim_{n\to\infty} \frac{K_n^3}{P_n} = 0 \tag{30}$$

Thus, asymptotically matched random key graphs and Erdős-Renyi graphs can have vastly different clustering coefficients.

V. Discussion

A. Behaving like Erdős-Renyi graphs?

As seen at the end of Section VII, the arguments for Theorem 4.3 can easily be modified to yield

$$\lim_{n\to\infty} \frac{\mathbb{P}\left[E_{12}(\theta_n) \mid E_{13}(\theta_n) \cap E_{23}(\theta_n)\right]}{\mathbb{P}\left[E_{12}(\theta_n)\right]} = 1 \tag{31}$$

for any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ which satisfies (14) provided the condition (29) holds. This is equivalent to

$$\mathbb{P}\left[E_{12}(\theta_n) \mid E_{13}(\theta_n) \cap E_{23}(\theta_n)\right] \sim \mathbb{P}\left[E_{12}(\theta_n)\right].$$

Thus, in the parameter range characterized by (29), the two events $E_{12}(\theta_n)$ and $E_{13}(\theta_n) \cap E_{23}(\theta_n)$ are nearly independent. Given that the events $E_{13}(\theta_n)$ and $E_{23}(\theta_n)$ are always independent by virtue of (5), the three events $E_{12}(\theta_n)$, $E_{13}(\theta_n)$ and $E_{23}(\theta_n)$ are now nearly mutually independent. This situation is reminiscent of what happens in Erdős-Renyi graphs where the corresponding events *are* always mutually independent. This suggests that any parameter range where random key graphs behave asymptotically like Erdős-Renyi graphs should satisfy (29).

The tradeoff between connectivity and security in WSNs [4] makes it desirable to keep $\frac{K_n^2}{P_n}$ as close as possible to the critical connectivity threshold $\frac{\log n}{n}$ given in Theorem 4.2. Thus, under (27) with $c > 1$ (but close to one), condition (29) requires

$$K_n \gg \frac{n}{\log n}. \tag{32}$$

Given the limited memory and computational power of the sensor nodes, such key ring sizes are impractical. They would also lead to *high* node degrees, which in turn would decrease the *resiliency* of the network against node capture attacks. As (32) is not likely to hold in a WSN, Erdős-Renyi graphs may not adequately capture some of the properties of the EG scheme in realistic settings, and random key graphs need to be employed in order to get a fuller picture!

B. Small worlds

Since random key graphs can be highly clustered, a natural question arises as to their suitability to model the *small world effect*. This notion is linked to a well-known series of experiments conducted by Milgram [11] in the late sixties. The results, commonly known as six degrees of separation, suggest that the social network of people in the United States is *small* in the sense that the path lengths between pairs of individuals are short. As a way to capture Milgram's experiments, Watts

and Strogatz [14] defined *small worlds* as network models that are highly clustered and yet have a small average path length. More precisely, a random graph is considered to be a small world if its average path length is of the same order as that of an Erdős-Renyi graph with the same expected average degree, but with a much larger clustering coefficient.

The results of this paper already show that random key graphs can satisfy the high clustering coefficient requirement of a small world. Recently Rybarczyk [13] has shown under (27) 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 $\mathbb{K}(n;\theta_n)$. This suggests that the diameter, hence the average path length, in random key graphs is *small* as was the case with Erdős-Renyi graphs [2]. We also note [18, Corollary 5.2] that random key graphs have *very small* (≤ 2) diameter under certain parameter ranges. Therefore, random key graphs may indeed be considered as good candidate models for small worlds!

VI. A proof of Theorem 4.1

Recall the definitions (19) and (20). Obviously, by independence we have

$$C(p) = p, \quad p \in [0,1] \tag{33}$$

while exchangeability gives

$$C(\theta) = \frac{\mathbb{P}\left[E_{12}(\theta) \cap E_{13}(\theta) \cap E_{23}(\theta)\right]}{\mathbb{P}\left[E_{13}(\theta) \cap E_{23}(\theta)\right]}. \tag{34}$$

The events $E_{12}(\theta)$, $E_{13}(\theta)$ and $E_{23}(\theta)$ are not mutually independent, and calculating the probability terms in (34) will require some care. For this purpose we define the events

$$A(\theta) := E_{13}(\theta) \cap E_{23}(\theta) \tag{35}$$

and

$$B(\theta) := E_{12}(\theta) \cap E_{13}(\theta) \cap E_{23}(\theta). \tag{36}$$

In the forthcoming computations we omit the explicit dependence on θ when no confusion arises from doing so.

Lemma 6.1: The probability of the event $A(\theta)$ is given by

$$\mathbb{P}\left[A(\theta)\right] = (1-q(\theta))^2. \tag{37}$$

Proof. Under the enforced independence assumptions we find

$$\begin{aligned}
&\mathbb{P}\left[A(\theta)\right] \\
&= \sum_{|S|=K} \mathbb{P}\left[K_3 = S, S \cap K_1 \neq \emptyset, S \cap K_2 \neq \emptyset\right] \\
&= \sum_{|S|=K} \mathbb{P}\left[K_3 = S\right] \mathbb{P}\left[S \cap K_1 \neq \emptyset\right] \mathbb{P}\left[S \cap K_2 \neq \emptyset\right] \\
&= \left(1-q(\theta)\right)^2
\end{aligned} \tag{38}$$

as we make use of (5) with $\sum_{|S|=K} \mathbb{P}\left[K_3 = S\right] = 1$. ∎

In what follows we make repeated use of the elementary fact that for any pair of events, say E and F, we have

$$\mathbb{P}\left[E \cap F\right] = \mathbb{P}\left[E\right] - \mathbb{P}\left[E \cap F^c\right]. \tag{39}$$

In particular, we conclude from Lemma 6.1 that

$$\begin{aligned}
&\mathbb{P}\left[K_1(\theta) \cap K_3(\theta) = \emptyset,\ K_2(\theta) \cap K_3(\theta) \neq \emptyset\right] \\
&= \mathbb{P}\left[K_1(\theta) \cap K_3(\theta) \neq \emptyset,\ K_2(\theta) \cap K_3(\theta) = \emptyset\right] \\
&= q(\theta)(1-q(\theta))
\end{aligned} \tag{40}$$

and

$$\mathbb{P}\left[K_1(\theta) \cap K_3(\theta) = \emptyset,\ K_2(\theta) \cap K_3(\theta) = \emptyset\right] = q(\theta)^2. \tag{41}$$

These facts are now used in computing the probability of $B(\theta)$.

Lemma 6.2: We have

$$\mathbb{P}[B(\theta)] = (1-q(\theta))^3 + q(\theta)^3 - q(\theta)r(\theta). \tag{42}$$

Proof. We find

$$\begin{aligned}
&\mathbb{P}\left[B(\theta)\right] \\
&= \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset,\ K_1 \cap K_3 \neq \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&= \mathbb{P}\left[K_1 \cap K_3 \neq \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&\quad - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 \neq \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&= \mathbb{P}\left[A(\theta)\right] - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&\quad + \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&= \mathbb{P}\left[A(\theta)\right] - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_2 \cap K_3 \neq \emptyset\right] \\
&\quad + \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset\right] \\
&\quad - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\
&= (1-q(\theta))^2 - q(\theta)(1-q(\theta)) + q(\theta)^2 \\
&\quad - q(\theta)\mathbb{P}\left[K_1 \cap (K_2 \cup K_3) = \emptyset \mid K_2 \cap K_3 = \emptyset\right] \\
&= (1-q(\theta))^2 - q(\theta)(1-q(\theta)) + q(\theta)^2 - q(\theta)r(\theta) \\
&= (1-q(\theta))^3 + q(\theta)^3 - q(\theta)r(\theta)
\end{aligned} \tag{43}$$

upon using (37), (40) and (41) in (43). ∎

Substituting (37) and (42) into (34), we now obtain

$$C(\theta) = \frac{\mathbb{P}\left[B(\theta)\right]}{\mathbb{P}\left[A(\theta)\right]} = 1 - q(\theta) + \frac{q(\theta)^2 - r(\theta)}{(1-q(\theta))^2} \cdot q(\theta) \tag{44}$$

and (23) follows directly from (33) and (44). ∎

VII. A proof of Theorem 4.3

Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ which satisfies (14) and replace θ by θ_n in (44) according to this scaling. We find

$$C(\theta_n) = 1 - q(\theta_n) + \left(1 - \frac{r(\theta_n)}{q(\theta_n)^2}\right) \cdot \frac{q(\theta_n)^3}{(1-q(\theta_n))^2} \tag{45}$$

for all $n = 2, 3, \ldots$.

Lemma 7.1: For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ that satisfies (14), we have

$$1 - \frac{r(\theta_n)}{q(\theta_n)^2} \sim \frac{{K_n}^3}{{P_n}^2}. \tag{46}$$

Proof. With positive integers K, P such that $3K \leq P$, we can write

$$\frac{r(\theta)}{q(\theta)^2} = \prod_{\ell=0}^{K-1} \left(1 - \left(\frac{K}{P-K-\ell}\right)^2\right)$$

and an elementary bounding argument yields

$$\left(1 - \left(\frac{K}{P-2K}\right)^2\right)^K \leq \frac{r(\theta)}{q(\theta)^2} \leq \left(1 - \left(\frac{K}{P-K}\right)^2\right)^K.$$

Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (14) and note from (17) that $3K_n \leq P_n$ for all $n = 1, 2, \ldots$ sufficiently large. On that range, use this scaling to replace θ by θ_n in the inequalities above. This yields

$$1 - \left(1 - \left(\frac{K_n}{P_n - K_n}\right)^2\right)^{K_n} \leq 1 - \frac{r(\theta_n)}{q(\theta_n)^2} \qquad (47)$$

and

$$1 - \frac{r(\theta_n)}{q(\theta_n)^2} \leq 1 - \left(1 - \left(\frac{K_n}{P_n - 2K_n}\right)^2\right)^{K_n}. \qquad (48)$$

For each $c = 1, 2$, we obtain

$$\left(\frac{K_n}{P_n - cK_n}\right)^2 = \frac{K_n^2}{P_n^2}\left(1 - c\frac{K_n}{P_n}\right)^{-2},$$

whence

$$\lim_{n\to\infty} K_n \left(\frac{K_n}{P_n - cK_n}\right)^2 = 0$$

by virtue of (14) and (17). Finally, let n go to infinity in (47) and (48), and use the elementary convergence relation

$$(1-a)^b \sim 1 - ab \qquad \text{if } ab \to 0$$

with

$$a = \left(\frac{K_n}{P_n - cK_n}\right)^2, \quad \text{and} \quad b = K_n.$$

Noting that

$$K_n \left(\frac{K_n}{P_n - cK_n}\right)^2 \sim \frac{K_n^3}{P_n^2},$$

we immediately obtain (46) by a sandwich argument. ∎

Using (14), (15) and (46) in (45), we find

$$C(\theta_n) \sim \frac{{K_n}^2}{P_n} + \frac{1}{K_n}. \qquad (49)$$

Pick a scaling $p : \mathbb{N}_0 \to [0, 1]$ that is asymptotically matched to the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. From (16) and (33) we conclude

$$C(p_n) = p_n \sim \frac{{K_n}^2}{P_n}, \qquad (50)$$

and (28) follows directly from (49) and (50). This completes the proof of Theorem 4.3. ∎

With the help of (19) we conclude that (45) also implies

$$\frac{\mathbb{P}\left[E_{12}(\theta_n) \mid E_{13}(\theta_n) \cap E_{23}(\theta_n)\right]}{\mathbb{P}\left[E_{12}(\theta_n)\right]} = 1 + \left(1 - \frac{r(\theta_n)}{q(\theta_n)^2}\right) \cdot \frac{q(\theta_n)^3}{(1 - q(\theta_n))^3} \qquad (51)$$

for all $n = 2, 3, \ldots$. Let n go to infinity in this last expression: Using (14) and (15) we readily get (31) under the condition (29).

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] F. Chung and L. Lu, "The diameter of sparse random graphs," *Advances in Applied Mathematics* **26** (2001), pp. 257-279.

[3] M. Deijfen and W. Kets, "Random intersection graphs with tunable degree distribution and clustering," *Probability in the Engineering and Informational Sciences* **23** (2009), pp. 661-674.

[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] 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," Proceedings of the ACM Conference on Computer and Communications Security (2002), Washington (DC), November 2002.

[7] J. Fill, E.R. Scheinerman and K.B. Cohen-Singer, "Random intersection graphs when $m = \omega(n)$: An equivalence theorem relating the evolution of the $G(n, m, p)$ and $G(n, p)$ models," *Random Structures and Algorithms* **16** (2000), pp. 249-258.

[8] 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.

[9] 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.

[10] 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.

[11] S. Milgram, "The small world problem," *Psychology Today* **2**(1967), pp. 60-67.

[12] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review* **45** (2003), pp. 167-256.

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

[14] D. Watts and S. Strogatz, "Collective dynamics of "small-world" networks," *Nature* **393** (1998), pp. 440-442.

[15] 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.

[16] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," Proceedings of the ISIT 2009, Seoul (Korea), June 2009.

[17] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Submitted to *Random Structures and Algorithms*, August 2009. Available online at arXiv:0908.3644v1 [math.CO]. Earlier draft available online at http://hdl.handle.net/1903/8716, January 2009.

[18] O. Yağan and A. M. Makowski, "Connectivity in random graphs induced by a key predistribution scheme – Small key pools," Proceedings of the International Conference on Information and Communication Systems (ICICS 2009), Amman (Jordan), December 2009. Also available online at http://hdl.handle.net/1903/9055, January 2009.