Performance of the Heterogeneous Key Predistribution Scheme under a Heterogeneous ON/OFF Channel Model

Rashad Eletreby and Osman Yağan
Department of Electrical and Computer Engineering and CyLab,
Carnegie Mellon University, Pittsburgh, PA, 15213 USA
reletreby@cmu.edu, oyagan@ece.cmu.edu

***Abstract*—We investigate the secure connectivity of wireless sensor networks under a heterogeneous random key predistribution scheme. This scheme has recently been introduced as a generalization of the Eschenauer and Gligor scheme and accounts for the cases when the network comprises sensor nodes with varying level of resources and/or connectivity requirements, e.g., regular nodes vs. cluster heads. Our paper is the first to consider the heterogeneous random key predistribution scheme under a heterogeneous on/off channel model. In particular, we study a random graph formed by the intersection of an inhomogeneous random key graph with an inhomogeneous Erdős-Rényi graph. The former graph is naturally induced by the heterogeneous random key predistribution scheme while the latter constitutes a heterogeneous on/off channel model; wherein, the wireless channel between a class-i node and a class-j node is on with probability α_{ij}. We present conditions (in the form of zero-one laws) on how to scale the parameters of the intersection model so that it has no isolated node with high probability as the number of nodes gets large. We also present numerical results to support these zero-one laws in the finite-node regime.**

***Index Terms*—General Random Intersection Graphs, Wireless Sensor Networks, Security, Inhomogeneous Random Key Graphs, Inhomogeneous ER Graphs, Connectivity, Reliability.**

1. Introduction

Wireless sensor networks (WSNs) consist of low-cost, low-power, small sensor nodes that are typically deployed randomly in large numbers (order of hundreds, thousands, or in some cases millions) [1]. There are numerous applications that utilize WSNs such as military applications, health monitoring, environmental monitoring, etc. Secrecy of WSNs has been thoroughly investigated during the past decade. WSNs are typically deployed in hostile environments (e.g., battlefields), making it crucial to use cryptographic protection to secure sensor communications. In [2, Chapter 13 and references therein] and [3], authors review several key distribution schemes for WSNs and investigate their applicability given the classical constraints of a sensor node, namely: limited computational capabilities, limited transmission power, lack of a priori knowledge of deployment configuration, and vulnerability to node capture attacks. We refer the reader to [4], [5] for a detailed analysis of security challenges in WSNs.

In [6], Yağan introduced a new variation of the Eschenauer and Gligor (EG) key predistribution scheme [7], referred to as the heterogeneous key predistribution scheme. The heterogeneous key predistribution scheme accounts for the cases when the network comprises sensor nodes with varying level of resources and/or connectivity requirements, e.g., regular nodes vs. cluster heads, which is likely to be the case for many WSN applications [8]. According to this scheme, each sensor node belongs to a specific priority class and is given a number of keys corresponding to its class. More specifically, Given r classes, a sensor node is classified as a class-i node with probability μ_i, resulting in a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$, for $i = 1, \ldots, r$ and $\sum_{i=1}^{r} \mu_i = 1$. Sensors belonging to class-i are each given K_i keys selected uniformly at random (without replacement) from a key pool of size P. As with the EG scheme, pairs of sensors that share key(s) can communicate securely over an available channel after deployment.

Let $\mathbb{K}(n, \boldsymbol{\mu}, \boldsymbol{K}, P)$ denote the random graph induced by the heterogeneous key predistribution scheme described above, where $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$ and n denotes the number of nodes. A pair of nodes are adjacent as long as they share a key. This model is referred to as the *inhomogeneous* random key graph in [6]; wherein, zero-one laws for the properties that $\mathbb{K}(n, \boldsymbol{\mu}, \boldsymbol{K}, P)$ i) has no isolated nodes and ii) is connected are established under the assumption of *full visibility*. Namely, it was assumed that all wireless channels are reliable and secure communications among participating nodes require only the existence of a shared key.

Our paper is motivated by the fact that the full visibility assumption is too optimistic and is not likely to hold in most WSN applications; e.g., the wireless medium of communication is often unreliable and sensors typically have limited communication ranges. To that end, we study the secure connectivity of heterogeneous WSNs under a heterogeneous on/off communication model; wherein, the communication channel between two nodes of class-i and class-j is on with probability α_{ij}. The heterogeneous on/off communication model induces the inhomogeneous Erdős-Rényi (ER) graph [9], [10], denoted hereafter by $\mathbb{G}(n, \boldsymbol{\alpha})$. The overall WSN can then be modeled by a random graph model formed by the intersection of an inhomogeneous random key graph and an inhomogeneous ER graph. We denote the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\alpha})$ by $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \boldsymbol{\alpha})$.

Our main contribution is as follows. We present conditions

(in the form of zero-one laws) on how to scale the parameters of the intersection model $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ so that it has no secure node which is isolated with high probability when the number of nodes n gets large. Our result generalizes several results in the literature, including the zero-one laws for absence of isolated nodes in inhomogeneous random key graphs intersecting homogeneous ER graphs [11], and in homogeneous random key graphs intersecting homogeneous ER graphs [12].

We close with a word on notation and conventions in use. All limiting statements, including asymptotic equivalence are considered with the number of sensor nodes n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega,\mathcal{F},\mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. We say that an event holds with high probability (whp) if it holds with probability 1 as $n\to\infty$. For any discrete set S, we write $|S|$ for its cardinality. In comparing the asymptotic behaviors of the sequences $\{a_n\},\{b_n\}$, we use $a_n=o(b_n)$, $a_n=\omega(b_n)$, $a_n=O(b_n)$, $a_n=\Omega(b_n)$, and $a_n=\Theta(b_n)$, with their meaning in the standard Landau notation. We also use $a_n\sim b_n$ to denote the asymptotic equivalence $\lim_{n\to\infty}a_n/b_n=1$.

2. The Model

We consider a network consisting of n sensors labeled as $v_1,v_2,\ldots,v_n$. Each sensor node is classified into one of the r classes, e.g., priority levels, according to a probability distribution $\boldsymbol{\mu}=\{\mu_1,\mu_2,\ldots,\mu_r\}$ with $\mu_i>0$ for $i=1,\ldots,r$ and $\sum_{i=1}^r\mu_i=1$. Then, a class-i node is assigned K_i cryptographic keys selected uniformly at random and *without replacement* from a key pool of size P. It follows that the key ring Σ_x of node x is an $\mathcal{P}_{K_{t_x}}$-valued random variable (rv) where $\mathcal{P}_{K_{t_x}}$ denotes the collection of all subsets of $\{1,\ldots,P\}$ with exactly K_{t_x} elements and t_x denotes the class of node v_x. The rvs $\Sigma_1,\Sigma_2,\ldots,\Sigma_n$ are then i.i.d. with

$$\mathbb{P}[\Sigma_x=S\mid t_x=i]=\binom{P}{K_i}^{-1},\quad S\in\mathcal{P}_{K_i}.$$

Let $\boldsymbol{K}=\{K_1,K_2,\ldots,K_r\}$ and assume without loss of generality that $K_1\le K_2\le\ldots\le K_r$. Consider a random graph $\mathbb{K}$ induced on the vertex set $\mathcal{V}=\{v_1,\ldots,v_n\}$ such that a pair of distinct nodes v_x and v_y are adjacent in $\mathbb{K}$, denoted by $v_x\sim_K v_y$, if they have at least one cryptographic key in common, i.e.,

$$v_x\sim_K v_y\quad\text{if}\quad\Sigma_x\cap\Sigma_y\neq\emptyset. \tag{1}$$

The adjacency condition (1) defines the inhomogeneous random key graph denoted by $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ [6]. This model is also known in the literature as the *general random intersection graph*; e.g., see [13]–[15]. The probability p_{ij} that a class-i node and a class-j node are adjacent is given by

$$p_{ij}=1-\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} \tag{2}$$

as long as $K_i+K_j\le P$; otherwise if $K_i+K_j>P$, we have $p_{ij}=1$. Let λ_i denote the *mean* probability that a class-i node is connected to another node in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$. We have

$$\lambda_i=\mathbb{P}[v_x\sim_K v_y\mid t_x=i]=\sum_{j=1}^r p_{ij}\mu_j. \tag{3}$$

We aim to investigate the performance of the heterogeneous key predistribution scheme without the *full visibility* assumption [6]. More precisely, to account for the possibility that communication channels between two nodes may not be available, e.g., due to deep fading, interference, etc., we assume a heterogeneous on/off channel model; wherein, the communication channel between two nodes of type-i and type-j is on with probability α_{ij}. Consider a random graph $\mathbb{G}$ induced on the vertex set $\mathcal{V}=\{v_1,\ldots,v_n\}$ such that a distinct class-i node v_x and a distinct class-j node v_y are adjacent in $\mathbb{G}$, denoted by $v_x\sim_G v_y$, if $B_{xy}(\alpha_{ij})=1$ where $B_{xy}(\alpha_{ij})$ denotes a Bernoulli rv with success probability α_{ij}. This adjacency conditions induces the inhomogeneous ER graph $\mathbb{G}(n;\boldsymbol{\alpha})$ on the vertex set $\mathcal{V}$, which has received some interest recently [9], [10], and would account for the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. Although the on/off channel model may be considered too simple, it allows a comprehensive analysis of the properties of interest and is often a good approximation of more realistic channel models, e.g., the disk model [16]. In fact, the simulations results in [12] suggest that the connectivity behavior of the EG scheme under the on/off channel model is asymptotically equivalent to that under the disk model.

Our system model is obtained by the intersection of the inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ with the inhomogeneous ER graph $\mathbb{G}(n;\boldsymbol{\alpha})$. We denote the intersection graph by $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$, i.e., $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha}):=\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\alpha})$. A distinct class-$i$ node v_x is adjacent to a distinct class-j node v_y in $\mathbb{H}$ if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{G}$. In words, the edges in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ represent pairs of sensors that share cryptographic key(s) *and* have a communication channel in between that is on, and hence can communicate securely. Therefore, studying the connectivity properties of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ amounts to studying the secure connectivity of heterogeneous WSNs under the heterogeneous on/off channel model.

To simplify the notation, we let $\boldsymbol{\theta}=(\boldsymbol{K},P)$, and $\boldsymbol{\Theta}=(\boldsymbol{\theta},\boldsymbol{\alpha})$. By independence, we see that the probability of edge assignment between a class-i node v_x and a class-j node v_y in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ is given by

$$\mathbb{P}[v_x\sim v_y\mid t_x=i,t_y=j]=\alpha_{ij}p_{ij}$$

Similar to (3), we denote the mean edge probability for a class-i node in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ as Λ_i. It is clear that

$$\Lambda_i=\sum_{j=1}^r\mu_j\alpha_{ij}p_{ij},\quad i=1,\ldots,r. \tag{4}$$

We denote the minimum mean edge probability in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ as Λ_m, i.e.,

$$m := \arg\min_i \Lambda_i.$$

We also let

$$d := \arg\max_j \alpha_{mj}, \tag{5}$$

$$s := \arg\max_j \alpha_{mj} p_{mj}. \tag{6}$$

Throughout, we assume that the number of classes r is fixed and does not scale with n, and so are the probabilities $\mu_1, \ldots, \mu_r$. All of the remaining parameters are assumed to be scaled with n.

3. Main Results and Discussion

We refer to a mapping $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ as a *scaling* (for the inhomogeneous random key graph) if

$$1 \leq K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{7}$$

hold for all $n = 2, 3, \ldots$. Similarly any mapping $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ defines a scaling for the inhomogeneous ER graphs. A mapping $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)^{r\times r}$ defines a scaling for the intersection graph $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ given that condition (7) holds. We remark that under (7), the edge probabilities p_{ij} will be given by (2).

A. Results

We present a zero-one law for the absence of isolated nodes in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$.

Theorem 3.1. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ such that*

$$\Lambda_m(n) \sim c\frac{\log n}{n} \tag{8}$$

holds for some $c > 0$.

i) If

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = 0,$$

or

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = \alpha^* \in (0,\infty],$$
$$\lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^{**} \in (0,\infty].$$

Then, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) \text{ } has\\ no \text{ } isolated \text{ } nodes\end{array}\right] = 0 \quad if\ c < 1$$

ii) We have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) \text{ } has\\ no \text{ } isolated \text{ } nodes\end{array}\right] = 1 \quad if\ c > 1$$

The scaling condition (8) will often be used in the form

$$\Lambda_m(n) = c_n\frac{\log n}{n},\ n = 2, 3, \ldots \tag{9}$$

with $\lim_{n\to\infty} c_n = c > 0$.

Theorem 3.1 states that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ has no isolated node whp if the minimum mean degree, i.e., $n\Lambda_m$, is scaled as $(1+\epsilon)\log n$ for some $\epsilon > 0$. On the other hand, if this minimum mean degree scales as $(1-\epsilon)\log n$ for some $\epsilon > 0$, then whp $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ has a class-m node that is isolated, and hence not connected. We remark that $\alpha^{**} \leq \alpha^*$ since $\alpha_{mm}(n) \leq \alpha_{md}(n)$ for $n = 1, 2, \ldots$.

The zero-one law established here for the absence of isolated nodes in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ shall be regarded as a crucial first step towards establishing the connectivity result. In fact, Theorem 3.1 already implies the zero-law for connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\\ \text{is connected}\end{array}\right] = 0 \quad \text{if } c < 1.$$

This is because a graph can not be connected if it contains an isolated node. Also, for several classes of random graphs it is known that the conditions that ensure connectivity coincide with those ensuring absence of isolated nodes; e.g., random key graphs [17], (homogeneous) ER graphs [18], and random geometric key graphs [19]. This prompts us to introduce the following conjecture.

Conjecture 3.2. *Consider a probability distribution $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_r)$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\boldsymbol{\alpha} = (\alpha_{ij}) : \mathbb{N}_0 \to (0,1)^{r\times r}$ such that (8) holds. With either*

i)

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = 0,$$

or

ii)

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = \alpha^* \in (0,\infty],$$
$$\lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^{**} \in (0,\infty],$$

and possibly under some additional conditions, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\\ \textit{is connected}\end{array}\right] = \left\{\begin{array}{ll} 0 & \textit{if } c < 1\\ 1 & \textit{if } c > 1\end{array}\right.$$

B. Comparison with related work

Our main result extends the results established by Eletreby and Yağan in [11] for the inhomogeneous random key graph intersecting the (homogeneous) ER graph. There, zero-one laws for the property that the graph has no isolated nodes and the property that the graph is connected were established. It is clear that our work generalizes the model given in [11] by considering the *inhomogeneous* ER graph, enabling the analysis of networks with heterogeneous radio capabilities. Indeed, when $\alpha_{ij}(n) = \alpha(n)$ for $i, j = 1, \ldots, r$ and each $n = 1, 2, \ldots$, our result recovers the absence of isolated nodes result given in [11].

In [6], zero-one laws for the property that the graph has no isolated nodes and the property that the graph is connected were established for the inhomogeneous random key graph $\mathbb{K}(n,\boldsymbol{\mu},\boldsymbol{K},P)$ under the full visibility assumption. It is clear

that, although a crucial first step in the study of heterogeneous key predistribution schemes, the full visibility assumption is not likely to hold in most practical settings. In fact, by setting $\alpha_{ij}(n) = 1$ for $i, j = 1, \ldots, r$ and each $n = 1, 2, \ldots$ (i.e., by assuming that all wireless channels are *on*), our absence of isolated nodes result reduces to that given in [6].

Finally, Yağan in [12] considered the homogeneous random key graph (where all nodes receive K_n keys), intersecting the homogeneous ER graph [20]. Our work generalizes [12] by considering the intersection of the *inhomogeneous* ER graph with a more general random graph model that accounts for the cases where nodes can be assigned different number of keys; i.e., with the *inhomogeneous* random key graph. In fact, with $r = 1$, i.e., when α is a scalar and all nodes belong to the same class and thus receive the same number of keys, our absence of isolated node result recovers the result given in [12].

C. Significance of the results

1) Network Reliability Problem: The problem studied in this paper is closely connected to the popular *network reliability problem* [18, Section 7.5], described as follows: Starting with a fixed, deterministic graph $\mathcal{H}$, obtain $\mathbb{I}(\mathcal{H}; p)$ by deleting each edge of $\mathcal{H}$ independently with probability $1-p$. Network reliability problem is often translated to finding the probability that $\mathbb{I}(\mathcal{H}; p)$ is connected as a function of p. For arbitrary graphs, $\mathcal{H}$, this problem is shown [21], [22] to be $\#P$-complete, meaning that no polynomial algorithm exists for its solution, unless $P = NP$. Our result given above constitutes a crucial first step towards the asymptotic solution of the network reliability problem for inhomogeneous random key graphs when edges are deleted with *different* probabilities. Put differently, we consider a generic network reliability problem; wherein, different links fail with different probabilities. In fact, this generic failure model paves the way for many interesting problems. Although asymptotic in nature, our result can still provide useful insights about the reliability properties of random key graphs with number of vertices n being on the order of thousands.

2) Common-Interest Friendship Networks: We demonstrate an application of our result in the context of a common-interest friendship network, denoted by G_c. A common interest relationship between two friends manifests from their selection of common objects from a pool of available objects. Clearly, this is modeled by the inhomogeneous random key graph; the inhomogeneity enables capturing the different number of interests that people might have. The friendship network is modeled by an inhomogeneous ER graph, meaning that any two individuals are connected with a probability that is based on their corresponding *classes* independently from other individuals. The class of an individual could represent her job title, current city, academic degree, etc. As a result, G_c becomes the intersection of the inhomogeneous random key graph with the inhomogeneous ER graph. Our results on its absence of isolated nodes constitutes the first step in revealing the conditions under which global information diffusion can take place in the common-interest network. In particular, when G_c is connected, global information diffusion is possible.

4. Numerical Results

We now present numerical results and simulations to check the validity of Theorem 3.1 in the finite node regime. In all experiments, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10^4$. For better visualization, we use the curve fitting tool of MATLAB.

In Figure 1, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} 0.3 & \alpha_{12} \\ \alpha_{12} & 0.3 \end{bmatrix}$$

and consider the channel parameters $\alpha_{12} = 0.2$, $\alpha_{12} = 0.4$, and $\alpha_{12} = 0.6$, while varying the parameter K_1 (i.e., the smallest key ring size) from 10 to 35. The number of classes is fixed to 2, with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For each value of K_1, we set $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \boldsymbol{\alpha})$, we generate 400 independent samples of the graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ and count the number of times (out of a possible 400) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 400, we obtain the (empirical) probabilities for the events of interest. In all cases considered here, we observe that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected whenever it has no isolated nodes yielding the same empirical probability for both events. This confirms the asymptotic equivalence of the connectivity and absence of isolated nodes properties in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ as we give by Conjecture 3.2.

For each value of α_{12}, we show the critical threshold of connectivity "predicted" by Conjecture 3.2 by a vertical dashed line. More specifically, the vertical dashed lines stand for the minimum integer value of K_1 that satisfies

$$\Lambda_m(n) = \sum_{j=1}^{2} \mu_j \alpha_{mj} \left(1 - \frac{\binom{P-K_j}{K_m}}{\binom{P}{K_m}} \right) > \frac{\log n}{n}. \qquad (10)$$

We see from Figure 1 that the probability of connectivity transitions from zero to one within relatively small variations of K_1. Moreover, the critical values of K_1 obtained by (10) lie within this transition interval. We finally note that for each parameter pair $(\boldsymbol{K}, \boldsymbol{\alpha})$ in Fig 1, we have $\Lambda_m = \Lambda_1$.

Next, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{11} & 0.2 \\ 0.2 & 0.2 \end{bmatrix}$$

in Figure 2, and consider the channel parameters $\alpha_{11} = 0.2$, $\alpha_{11} = 0.4$, and $\alpha_{11} = 0.6$, while varying the parameter K_1 (i.e., the smallest key ring size) from 10 to 35. The number of classes is fixed to 2, with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For each value of K_1, we set $K_2 = K_1 + 5$. Using the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected versus K_1. As before, the critical threshold of connectivity asserted by Conjecture 3.2 is shown by a vertical dashed line in each curve. One interesting observation of Figure 2 is how the behavior of the probability of connectivity changes with α_{11}. In fact, when $\alpha_{11} = 0.2$, we have $\Lambda_m = \Lambda_1$, while for $\alpha_{11} \geq 0.4$, we have $\Lambda_m = \Lambda_2$. Consequently, the

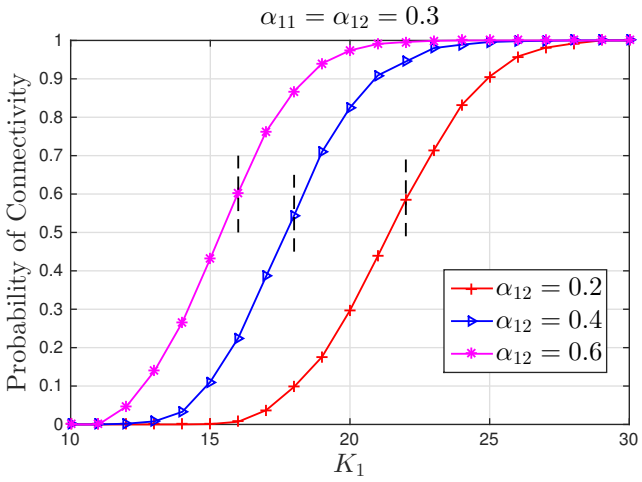

Fig. 1. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected as a function of $\boldsymbol{K}$ for $\alpha_{12} = 0.2$, $\alpha_{12} = 0.4$, and $\alpha_{12} = 0.6$ with $n = 500$ and $P = 10^4$; in each case, $\alpha_{11} = \alpha_{22} = 0.3$. The empirical probability value is obtained by averaging over 400 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Conjecture 3.2.

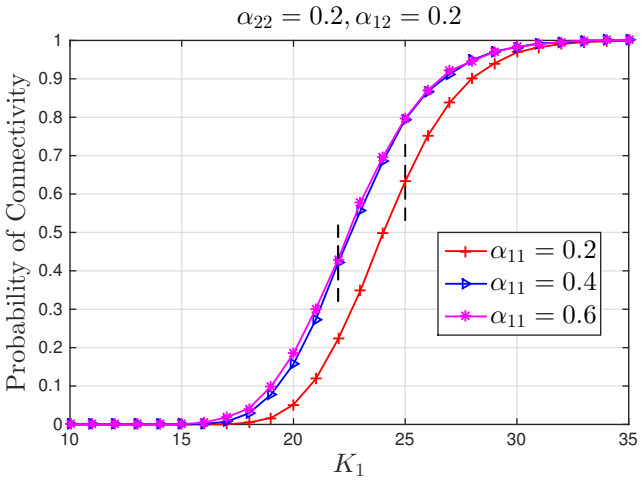

Fig. 2. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected as a function of $\boldsymbol{K}$ for $\alpha_{11} = 0.2$, $\alpha_{11} = 0.4$, and $\alpha_{11} = 0.6$ with $n = 500$ and $P = 10^4$; in each case, $\alpha_{12} = \alpha_{22} = 0.2$. The empirical probability value is obtained by averaging over 400 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Conjecture 3.2.

value of α_{11} (which only appears in the calculations of Λ_1) becomes irrelevant to the scaling condition given by (10). We notice from Fig 2, that for $\alpha_{11} \geq 0.4$, fixed α_{12}, and fixed α_{22}, we have the same critical value of K_1 and quite similar behavior of the probability of connectivity.

Finally, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha & 0.2 \\ 0.2 & \alpha \end{bmatrix}$$

and consider four different minimum key ring sizes, $K_1 = 20$, $K_1 = 25$, $K_1 = 30$, and $K_1 = 50$ while varying the parameter α from 0 to 1. The number of classes is fixed to 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and we set $K_2 = K_1 + 5$ for each value of K_1. Using the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected versus α. As before, the critical threshold of connectivity asserted by Conjecture 3.2 is shown by a vertical dashed line in each curve. One interesting observation from Figure 3 is that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ could possibly be connected with $\alpha_{12} > 0$ even when $\alpha = 0$. In fact, what we have in this case is a *bipartite* graph; namely, class-1 nodes are adjacent only to class-2 nodes and class-2 nodes are adjacent only to class-1 nodes. Such a behavior confirms the importance of α_{12} over α_{11} and α_{22}. This is also captured in Figure 4; wherein, the probability of connectivity is indeed 0 when $\alpha_{12} = 0$.

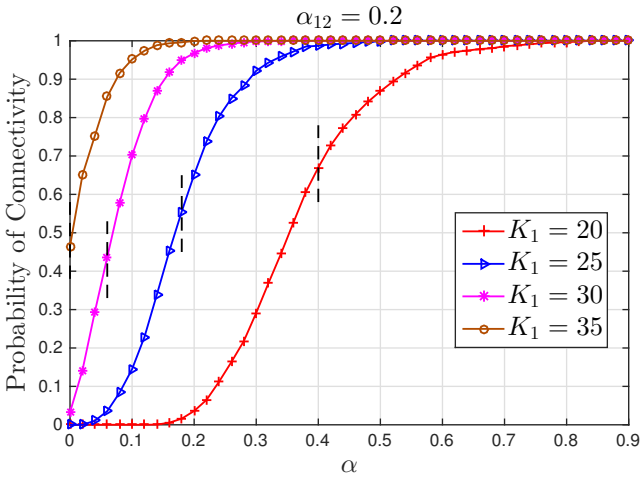

Fig. 3. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected as a function of α for $K_1 = 20$, $K_1 = 25$, $K_1 = 30$, and $K_1 = 35$, with $n = 500$ and $P = 10^4$; in each case, $\alpha_{12} = 0.2$. The empirical probability value is obtained by averaging over 400 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Conjecture 3.2.

5. Preliminaries

Several technical results are collected here for convenience. The first result follows easily from the scaling condition (7).

Proposition 5.1 ([6, Proposition 4.1]). *For any scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, we have*

$$\lambda_1(n) \leq \lambda_2(n) \leq \ldots \leq \lambda_r(n) \tag{11}$$

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

Proposition 5.2 ([6, Proposition 4.4]). *For any set of positive integers $K_1, \ldots, K_r, P$ and any scalar $a \geq 1$, we have*

$$\frac{\binom{P-\lceil aK_i \rceil}{K_j}}{\binom{P}{K_j}} \leq \left(\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} \right)^a, \quad i, j = 1, \ldots, r \tag{12}$$

Lemma 5.3. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r \times r}$ such that (8) holds. We have*

$$c_n \frac{\log n}{n} \leq \alpha_{ms}(n) p_{ms}(n) \leq \frac{c_n}{\mu_s} \frac{\log n}{n} \tag{13}$$

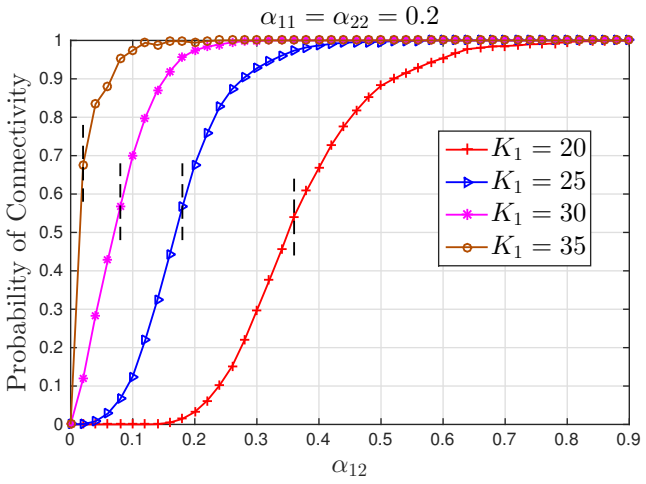

Fig. 4. Empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ is connected as a function of α_{12} for $K_1 = 20$, $K_1 = 25$, $K_1 = 30$, and $K_1 = 35$, with $n = 500$ and $P = 10^4$; in each case, $\alpha_{11} = \alpha_{22} = 0.2$. The empirical probability value is obtained by averaging over 400 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Conjecture 3.2.

Proof. We know from (9) that

$$\Lambda_m(n) = \sum_{j=1}^{r} \mu_j \alpha_{mj}(n) p_{mj}(n) = c_n \frac{\log n}{n}.$$

and it is easy to see that

$$\alpha_{ms}(n) p_{ms}(n) \leq \frac{c_n}{\mu_s} \frac{\log n}{n}. \tag{14}$$

Next, from (6), we have

$$\Lambda_m = \sum_{j=1}^{r} \mu_j \alpha_{mj}(n) p_{mj}(n) \leq \alpha_{ms}(n) p_{ms}(n)$$

Thus, we readily obtain the bound

$$\alpha_{ms}(n) p_{ms}(n) \geq c_n \frac{\log n}{n}.$$

■

Other useful bound that will be used throughout is

$$(1 \pm x) \leq e^{\pm x}, \quad x \in (0,1) \tag{15}$$

Finally, we find it useful to write

$$\log(1-x) = -x - \Psi(x) \tag{16}$$

where $\Psi(x) = \int_0^x \frac{t}{1-t}\, \mathrm{dt}$. From L'Hôpital's Rule, we have

$$\lim_{x \to 0} \frac{\Psi(x)}{x^2} = \frac{-x - \log(1-x)}{x^2} = \frac{1}{2}. \tag{17}$$

6. Proof of Theorem 3.1

The proof of Theorem 3.1 relies on the method of first and second moments applied to the number of isolated nodes in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$. Let $I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number of isolated nodes in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$, namely,

$$I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{\ell=1}^{n} \mathbf{1}[v_\ell \text{ is isolated in } \mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \tag{18}$$

The method of first moment [23, Eqn. (3.10), p. 55] gives

$$1 - \mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0]$$

A. Establishing the one-law

It is clear that in order to establish the one-law, namely that $\lim_{n\to\infty} \mathbb{P}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta_n}) = 0\right] = 1$, we need to show that

$$\lim_{n\to\infty} \mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0.$$

Recalling (18), we have

$$\begin{aligned}
&\mathbb{E}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] \\
&= n \sum_{i=1}^{r} \mu_i \mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) \mid t_1 = i\right] \\
&= n \sum_{i=1}^{r} \mu_i \mathbb{P}\left[\cap_{j=2}^{n} [v_j \nsim v_1] \mid v_1 \text{ is class i}\right] \\
&= n \sum_{i=1}^{r} \mu_i \left(\mathbb{P}\left[v_2 \nsim v_1 \mid v_1 \text{ is class i}\right]\right)^{n-1} \qquad (19)
\end{aligned}$$

where (19) follows by the independence of the rvs $\{v_j \nsim v_1\}_{j=1}^{n}$ given Σ_1. By conditioning on the class of v_2, we find

$$\begin{aligned}
\mathbb{P}[v_2 \nsim v_1 \mid t_1 = i] &= \sum_{j=1}^{r} \mu_j \mathbb{P}[v_2 \nsim v_1 \mid t_1 = i, t_2 = j] \\
&= \sum_{j=1}^{r} \mu_j (1 - \alpha_{ij} p_{ij}) = 1 - \Lambda_i(n). \qquad (20)
\end{aligned}$$

Using (20) in (19), and recalling (2), (15) we obtain

$$\begin{aligned}
\mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] &= n \sum_{i=1}^{r} \mu_i \left(1 - \Lambda_i(n)\right)^{n-1} \\
&\leq n \left(1 - \Lambda_m(n)\right)^{n-1} \\
&= n \left(1 - c_n \frac{\log n}{n}\right)^{n-1} \\
&\leq e^{\log n \left(1 - c_n \frac{n-1}{n}\right)}
\end{aligned}$$

Taking the limit as n goes to infinity, we immediately get

$$\lim_{n\to\infty} \mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0.$$

since $\lim_{n\to\infty}(1 - c_n \frac{n-1}{n}) = 1 - c < 0$ under the enforced assumptions (with $c > 1$) and the one-law is established.

B. Establishing the zero-law

Our approach in establishing the zero-law relies on the method of second moment applied to a variable that counts the number of nodes that are class-m and isolated. Clearly if we can show that whp there exists at least one class-m node that is isolated under the enforced assumptions (with $c < 1$) then the zero-law would immediately follow.

Let $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the number of nodes that are class-m and isolated in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, and let

$$x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \mathbf{1}[t_i = m \cap v_i \text{ is isolated in } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)],$$

then we have $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^n x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. By applying the method of second moments [23, Remark 3.1, p. 55] on $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, we get

$$\mathbb{P}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0] \leq 1 - \frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]} \tag{21}$$

where

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{22}$$

and

$$\begin{aligned}\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2] =& n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \\ &+ n(n-1)\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]\end{aligned} \tag{23}$$

by exchangeability and the binary nature of the rvs $\{x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\}_{i=1}^n$. Using (22) and (23), we get

$$\begin{aligned}\frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} =& \frac{1}{n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]} \\ &+ \frac{n-1}{n} \frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}\end{aligned}$$

In order to establish the zero-law, we need to show that

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty,$$

and

$$\limsup_{n\to\infty} \left(\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} \right) \leq 1. \tag{24}$$

Proposition 6.1. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} := \mathbb{N}_0 \to (0,1)^{r\times r}$ such that (8) holds with $\lim_{n\to\infty} c_n = c > 0$. Then, we have*

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty, \quad \textit{if } c < 1$$

Proof. We have

$$\begin{aligned}&n\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] \\ &= n\mathbb{E}\left[\mathbf{1}[t_1 = m \cap v_1 \text{ is isolated in } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)]\right] \\ &= n\mu_m \mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \mid t_1 = m\right] \\ &= n\mu_m \mathbb{P}\left[\cap_{j=2}^n [v_j \nsim v_1] \mid t_1 = m\right] \\ &= n\mu_m \mathbb{P}\left[v_2 \nsim v_1 \mid t_1 = m\right]^{n-1} \\ &= n\mu_m \left(\sum_{j=1}^r \mu_j \mathbb{P}\left[v_2 \nsim v_1 \mid t_1 = m, t_2 = j\right] \right)^{n-1} \\ &= n\mu_m \left(\sum_{j=1}^r \mu_j (1 - \alpha_{mj} p_{mj}) \right)^{n-1} \qquad (25) \\ &= n\mu_m \left(1 - \Lambda_m(n)\right)^{n-1} = \mu_m e^{\beta_n} \qquad (26)\end{aligned}$$

where

$$\beta_n = \log n + (n-1)\log(1 - \Lambda_m(n)).$$

Recalling (16), we get

$$\begin{aligned}\beta_n &= \log n - (n-1)\left(\Lambda_m(n) + \Psi(\Lambda_m(n))\right) \\ &= \log n - (n-1)\left(c_n \frac{\log n}{n} + \Psi\left(c_n \frac{\log n}{n} \right) \right) \\ &= \log n \left(1 - c_n \frac{n-1}{n} \right) \\ &\quad - (n-1)\left(c_n \frac{\log n}{n} \right)^2 \frac{\Psi\left(c_n \frac{\log n}{n} \right)}{\left(c_n \frac{\log n}{n} \right)^2} \qquad (27)\end{aligned}$$

Recalling (17), we have

$$\lim_{n\to\infty} \frac{\Psi\left(c_n \frac{\log n}{n} \right)}{\left(c_n \frac{\log n}{n} \right)^2} = \frac{1}{2} \tag{28}$$

since $c_n \frac{\log n}{n} = o(1)$. Thus, $\beta_n = \log n \left(1 - c_n \frac{n-1}{n}\right) - o(1)$. Using (26), (27), (28), and letting n go to infinity, we get

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty$$

whenever $\lim_{n\to\infty} c_n = c < 1$. ∎

Proposition 6.2. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} := \mathbb{N}_0 \to (0,1)^{r\times r}$ such that (8) holds with $\lim_{n\to\infty} c_n = c > 0$. Then, we have (24) if $c < 1$.*

Proof. Consider fixed $\boldsymbol{\Theta}$.

$$\begin{aligned}&\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}) x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})\right] \\ &= \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated} \cap t_1 = m, t_2 = m]\right] \\ &= \mu_m^2 \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated}] \,\middle|\, t_1 = m, t_2 = m \right] \\ &= \mu_m^2 \mathbb{E}\left[\mathbf{1}[v_1 \nsim v_2] \prod_{k=3}^n \mathbf{1}[v_k \nsim v_1, v_k \nsim v_2] \,\middle|\, t_1 = t_2 = m \right]\end{aligned}$$

Now we condition on Σ_1 and Σ_2 and note that i) Σ_1 and Σ_2 determine t_1 and t_2; and ii) the events $[v_1 \nsim v_2], \{[v_k \nsim v_1 \cap v_k \nsim v_2]\}_{k=3}^n$ are mutually independent given Σ_1 and Σ_2. Thus, we have

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}) x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})] \\ &= \mu_m^2 \mathbb{E}\Bigg[\mathbb{P}\left[v_1 \nsim v_2 \,\middle|\, \Sigma_1, \Sigma_2 \right] \times \\ &\quad \prod_{k=3}^n \mathbb{P}\left[v_k \nsim v_1 \cap v_k \nsim v_2 \,\middle|\, \Sigma_1, \Sigma_2 \right] \,\Bigg|\, t_1 = t_2 = m \Bigg]\end{aligned} \tag{29}$$

Define the $\{0,1\}$-valued rv $u(\boldsymbol{\theta})$ by

$$u(\boldsymbol{\theta}) := \mathbf{1}[\Sigma_1 \cap \Sigma_2 \neq \emptyset]. \tag{30}$$

Next, with $\ell = 1, 2, \ldots, n-1$, define $\nu_{\ell,j}(\boldsymbol{\alpha})$ by

$$\nu_{\ell,j}(\boldsymbol{\alpha}) := \{i = 1, 2, \ldots, \ell : B_{ij}(\boldsymbol{\alpha}) = 1\} \tag{31}$$

for each $j = \ell+1, \ldots, n$. Namely, $\nu_{\ell,j}(\boldsymbol{\alpha})$ is the set of nodes in $\{1, \ldots, \ell\}$ that are adjacent to node j in $\mathbb{H}(n; \boldsymbol{\alpha})$.

With these definitions in mind, (29) gives

$$\begin{aligned}
&\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}) x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})] \\
&= \mu_m^2 \mathbb{E}\left[(1-\alpha_{mm})^{u(\boldsymbol{\theta})} \prod_{k=3}^{n} \frac{\binom{P-\left|\cup_{i\in\nu_{2,k}(\boldsymbol{\alpha})}\Sigma_i\right|}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}} \right. \\
&\qquad \left. \Bigg| \; t_1 = t_2 = m \right]
\end{aligned}$$

Conditioned on $u(\boldsymbol{\theta}) = 0$ and v_1, v_2 being class-m, we have

$$\left|\cup_{i\in\nu_{2,m}(\boldsymbol{\alpha})}\Sigma_i\right| = |\nu_{2,k}(\boldsymbol{\alpha})|\, K_m.$$

Also, we have

$$\mathbb{P}[u(\boldsymbol{\theta_n}) = 0 \mid t_1 = t_2 = m] = 1 - p_{mm}.$$

Thus, we get

$$\begin{aligned}
&\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}) x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})\; \mathbf{1}[u(\boldsymbol{\theta}) = 0]\right] \\
&= \mu_m^2 (1-p_{mm}) \mathbb{E}\left[\prod_{k=3}^{n} \frac{\binom{P-|\nu_{2,k}(\boldsymbol{\alpha})K_m|}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}} \;\middle|\; t_1 = t_2 = m \right] \\
&= \mu_m^2 (1-p_{mm}) \mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\boldsymbol{\alpha})|K_m}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}} \;\middle|\; t_1 = t_2 = m \right]^{n-2} \\
&= \mu_m^2 (1-p_{mm}) \left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\boldsymbol{\alpha})|K_m}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}} \right.\right. \\
&\qquad \left.\left. \Bigg| \; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \right] \right)^{n-2} \\
&\leq \mu_m^2 (1-p_{mm}) \left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\left(\frac{\binom{P-K_m}{K_j}}{\binom{P}{K_j}} \right)^{|\nu_{2,3}(\boldsymbol{\alpha})|} \right.\right. \\
&\qquad \left.\left. \Bigg| \; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \right] \right)^{n-2}
\end{aligned} \tag{32}$$

where we use (12) in the last step. Now, let

$$Z_j = \frac{\binom{P-K_m}{K_j}}{\binom{P}{K_j}} = 1 - p_{mj}, \quad j = 1, \ldots, r. \tag{33}$$

Then,

$$\begin{aligned}
&\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}) x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}) \mathbf{1}\left[u(\boldsymbol{\theta}) = 0\right]] \\
&\leq \mu_m^2 (1-p_{mm}) \left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|} \;\middle|\; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \right] \right)^{n-2}
\end{aligned} \tag{34}$$

It is clear that $|\nu_{2,3}(\boldsymbol{\alpha})|$ is the distribution of the sum of two independent Bernoulli rvs with success probabilities that are not necessarily *equal*. Put differently, given t_1, t_2, and t_3, the Bernoulli rv $\mathbf{1}\left[v_1 \sim_G v_3\right]$ has a success probability $\alpha_{t_1 t_3}$ while the Bernoulli rv $\mathbf{1}\left[v_2 \sim_G v_3\right]$ has a success probability $\alpha_{t_2 t_3}$. Since $|\nu_{2,3}(\boldsymbol{\alpha})| =_{st} \mathbf{1}\left[v_1 \sim_G v_3\right] + \mathbf{1}\left[v_2 \sim_G v_3\right]$, it follows that $|\nu_{2,3}(\boldsymbol{\alpha})|$ is a Poisson-Binomial rv. It is now immediate that

$$|\nu_{2,3}(\boldsymbol{\alpha})| \;\middle|\; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \sim \text{Binomial}(2, \alpha_{mj})$$

Hence,

$$\begin{aligned}
&\mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|} \;\middle|\; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \right] \\
&= \sum_{i=0}^{2} \binom{2}{i} \alpha_{mj}^i (1-\alpha_{mj})^{2-i} Z_j^i \\
&= \sum_{i=0}^{2} \binom{2}{i} \alpha_{mj}^i (1-\alpha_{mj})^{2-i} (1-p_{mj})^i \\
&= 1 - 2\alpha_{mj} p_{mj} + (\alpha_{mj} p_{mj})^2
\end{aligned} \tag{35}$$

upon recalling (33). Next, let W be a rv that takes the value $\alpha_{mj} p_{mj}$ with probability μ_j. It follows that

$$\begin{aligned}
&\sum_{j=1}^{r} \mu_j \mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|} \;\middle|\; \begin{matrix} t_1 = t_2 = m \\ t_3 = j \end{matrix} \right] \\
&= 1 - 2\Lambda_m + \sum_{j=1}^{r} \mu_j \left(\alpha_{mj} p_{mj}\right)^2 \\
&= 1 - 2\Lambda_m + \mathbb{E}\left[W^2\right]
\end{aligned}$$

Next, we recall (6) and let

$$k := \arg\min_j \alpha_{mj} p_{mj}$$

Now, in view of Popoviciu's inequality [24, pp. 9], we see that

$$\begin{aligned}
var[W] &\leq \frac{1}{4} \left(W_{\max} - W_{\min}\right)^2 \\
&= \frac{1}{4} \left(\alpha_{ms} p_{ms} - \alpha_{mk} p_{mk}\right)^2 \\
&\leq \frac{1}{4} \left(\alpha_{ms} p_{ms}\right)^2
\end{aligned} \tag{36}$$

We also know from (4) that

$$\alpha_{ms} p_{ms} \leq \frac{1}{\mu_s} \Lambda_m \tag{37}$$

From (36) and (37), we get

$$var[W] \leq \frac{1}{4\mu_s^2} \Lambda_m^2 \tag{38}$$

It is now immediate that

$$\mathbb{E}\left[W^2\right] = \left(\mathbb{E}\left[W\right]\right)^2 + var\left[W\right] \leq \left(1 + \frac{1}{4\mu_s^2}\right) \Lambda_m^2 \tag{39}$$

by virtue of the fact that $\mathbb{E}[W] = \Lambda_m$. Using (39) into (34), we readily obtain

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta})=0\right]]\\&\leq \mu_m^2(1-p_{mm})\left(1-2\Lambda_m+\left(1+\frac{1}{4\mu_s^2}\right)\Lambda_m^2\right)^{n-2}\end{aligned} \tag{40}$$

Next, conditioning on $u(\boldsymbol{\theta})=1$ and $t_1=t_2=m$, we have

$$|\cup_{i\in\nu_{2,k}(\boldsymbol{\alpha})}\Sigma_i| = \begin{cases}0 & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})|=0\\ K_m & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})|=1\\ 2K_m-|\Sigma_1\cap\Sigma_2| & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})|=2\end{cases}$$

and by a crude bounding argument, we have

$$|\cup_{i\in\nu_{2,k}(\boldsymbol{\alpha})}\Sigma_i|\geq K_m\mathbf{1}[|\nu_{2,k}(\boldsymbol{\alpha})|>0] \tag{41}$$

Using (41) and recalling the analysis for $\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta})=0]]$, we obtain

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta})=1]]\\&\leq \mu_m^2(1-\alpha_{mm})p_{mm}\left(\sum_{j=1}^r\mu_j\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]}\right.\right.\\&\qquad\left.\left.\begin{array}{c|c}&t_1=t_2=m\\&t_3=j\end{array}\right]\right)^{n-2}\end{aligned} \tag{42}$$

where

$$\begin{aligned}&\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]}\left|\begin{array}{c}t_1=t_2=m\\t_3=j\end{array}\right.\right]\\&=(1-\alpha_{mj})^2+\left(1-(1-\alpha_{mj})^2\right)Z_j\\&=1-2\alpha_{mj}p_{mj}+\alpha_{mj}^2p_{mj}\end{aligned}$$

and it follows that

$$\begin{aligned}&\sum_{j=1}^r\mu_j\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]}\left|\begin{array}{c}t_1=t_2=m\\t_3=j\end{array}\right.\right]\\&=1-2\Lambda_m+\sum_{j=1}^r\mu_j\alpha_{mj}^2p_{mj}\\&\leq 1-2\Lambda_m+\alpha_{md}\sum_{j=1}^r\mu_j\alpha_{mj}p_{mj}\\&=1-(2-\alpha_{md})\Lambda_m\end{aligned} \tag{43}$$

upon recalling (5). From (42) and (43), we readily obtain

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta})=1\right]]\\&\leq\mu_m^2(1-\alpha_{mm})p_{mm}\left(1-(2-\alpha_{md})\Lambda_m\right)^{n-2}\end{aligned} \tag{44}$$

Combining (40) and (44), we get

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]\\&=\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\left(\mathbf{1}[u(\boldsymbol{\theta})=0]+\mathbf{1}[u(\boldsymbol{\theta})=1]\right)]\\&\leq\mu_m^2(1-p_{mm})\left(1-2\Lambda_m+\left(1+\frac{1}{4\mu_s^2}\right)\Lambda_m^2\right)^{n-2}\\&\quad+\mu_m^2(1-\alpha_{mm})p_{mm}\left(1-(2-\alpha_{md})\Lambda_m\right)^{n-2}\end{aligned} \tag{45}$$

It is also clear that

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})]=\mu_m\left(1-\Lambda_m\right)^{n-1} \tag{46}$$

Combining (45) and (46), we get

$$\begin{aligned}&\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]}{\mathbb{E}[x_{n,1}(\boldsymbol{\theta})]^2}\\&\leq(1-p_{mm})\frac{\left(1-2\Lambda_m+\left(1+\frac{1}{4\mu_s^2}\right)\Lambda_m^2\right)^{n-2}}{\left(1-\Lambda_m\right)^{2(n-1)}}\\&\quad+p_{mm}\frac{\left(1-2\Lambda_m+\alpha_{md}\Lambda_m\right)^{n-2}}{\left(1-\Lambda_m\right)^{2(n-1)}}\\&:=A+B\end{aligned} \tag{47}$$

where we use the fact that $1-\alpha_{mm}\leq 1$.

We now consider a scaling $\boldsymbol{\Theta}:\mathbb{N}_0\to\mathbb{N}_0^{r+1}\times(0,1)^{r\times r}$ as stated in Proposition 6.2 and bound the terms A and B in turn. Our goal is to show that

$$\limsup_{n\to\infty}(A+B)\leq 1. \tag{48}$$

We have

$$\begin{aligned}A&=\frac{1-p_{mm}}{\left(1-\Lambda_m\right)^2}\left(1+\frac{1}{4\mu_s^2}\left(\frac{\Lambda_m}{1-\Lambda_m}\right)^2\right)^{n-2}\\&\leq\frac{1-p_{mm}}{\left(1-\Lambda_m\right)^2}e^{\rho_n}\end{aligned}$$

where

$$\rho_n\leq\left(\frac{c_n}{2\mu_s}\right)^2 n\left(\frac{\log n}{n-c_n\log n}\right)^2=o(1)$$

and

$$\left(1-\Lambda_m(n)\right)^2=1-o(1) \tag{49}$$

since $\Lambda_m(n)=c_n\log n/n$. Thus, we have

$$A\leq(1-p_{mm})\left((1+o(1))\,e^{o(1)}\right) \tag{50}$$

We now consider the second term in (47). Recall (49), we have

$$\begin{aligned}B&=\frac{p_{mm}}{\left(1-\Lambda_m\right)^2}\left(1+\frac{\Lambda_m\left(\alpha_{md}-\Lambda_m\right)}{\left(1-\Lambda_m\right)^2}\right)^{n-2}\\&\leq\frac{p_{mm}}{\left(1-\Lambda_m\right)^2}e^{\psi_n}\end{aligned}$$

Now, recalling (9), we get

$$\begin{aligned}\psi_n&\leq n\frac{\Lambda_m\left(\alpha_{md}-\Lambda_m\right)}{\left(1-\Lambda_m\right)^2}\\&=\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}-\frac{c_n^2\frac{(\log n)^2}{n}}{\left(1-c_n\frac{\log n}{n}\right)^2}\\&=\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}-o(1)\end{aligned}$$

Thus, we have

$$B \leq p_{mm}.\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right).\left((1+o(1))\,e^{o(1)}\right) \tag{51}$$

,

We will now establish the desired result (48) by using (50) and (51). Our approach is to consider the cases i) $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$ and ii) $\lim_{n\to\infty}\alpha_{md}(n)\log n \in (0,\infty]$, $\lim_{n\to\infty}\alpha_{ma}(n)\log n \in (0,\infty]$ separately.

a) Assume that $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$*:* From (51) we get $B \leq (1+o(1))p_{mm}$ and upon using (50) we see that $A+B \leq (1+o(1))$ establishing (48) along subsequences with $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$.

b) Assume that $\lim_{n\to\infty}\alpha_{md}(n)\log n \in (0,\infty]$ *and* $\lim_{n\to\infty}\alpha_{ma}(n)\log n \in (0,\infty]$ *:* From (4), we have

$$\Lambda_m = \sum_{j=1}^{r}\mu_j\alpha_{mj}p_{mj} \geq \mu_m\alpha_{mm}p_{mm}$$

Thus,

$$\begin{aligned}
B &\leq \frac{1}{\mu_m}\frac{\Lambda_m}{\alpha_{mm}}.\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right)\\
&= \frac{1}{\mu_m}\Lambda_m\log n.\frac{\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right)}{\alpha_{mm}\log n}\\
&\leq \frac{1}{\mu_m}c_n\left(\log n\right)^2\frac{n^{-1+\frac{c_n}{\left(1-c_n\frac{\log n}{n}\right)^2}}}{\alpha_{ma}\log n}
\end{aligned}$$

since $\alpha_{md} \leq 1$. We note that

$$\lim_{n\to\infty} -1+\frac{c_n}{\left(1-c_n\frac{\log n}{n}\right)^2} = -1+c < 0$$

for $c < 1$. Thus, it follows that $B = o(1)$ upon noting that $\lim_{n\to\infty}\alpha_{mm}\log n = \alpha_{**} \in (0,\infty]$. From (50) and the fact that $p_{mm} \leq 1$, we have $A \leq 1+o(1)$, and (48) follows. ■

ACKNOWLEDGMENT

This work has been supported in part by National Science Foundation through grant CCF-1617934 and in part by the start-up funds from the Department of Electrical and Computer Engineering at Carnegie Mellon University (CMU). O. Yağan also acknowledges a Berkman Faculty Development Grant from CMU. R. Eletreby also acknowledges William J. Happel fellowship.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[2] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds., *Wireless Sensor Networks*. Norwell, MA, USA: Kluwer Academic Publishers, 2004.

[3] S. A. Çamtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, pp. 05–07, 2005.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004. [Online]. Available: http://doi.acm.org/10.1145/990680.990707

[5] X. Du and H.-H. Chen, "Security in wireless sensor networks," *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60–66, Aug 2008.

[6] O. Yağan, "Zero-one laws for connectivity in inhomogeneous random key graphs," *ArXiv e-prints*, Aug 2015, available online at http://arxiv.org/abs/1508.02407.

[7] 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*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47. [Online]. Available: http://doi.acm.org/10.1145/586110.586117

[8] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2005*, vol. 2, March 2005, pp. 878–890 vol. 2.

[9] L. Devroye and N. Fraiman, "Connectivity of inhomogeneous random graphs," *Random Structures & Algorithms*, vol. 45, no. 3, pp. 408–420, 2014.

[10] B. Bollobás, S. Janson, and O. Riordan, "The phase transition in inhomogeneous random graphs," *Random Structures and Algorithms*, vol. 33, no. 1, pp. 3–122, 2007.

[11] R. Eletreby and O. Yağan, "Reliability of wireless sensor networks under a heterogeneous key predistribution scheme," April 2016, available online at https://arxiv.org/abs/1604.00460.

[12] O. Yağan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3821–3835, June 2012.

[13] J. Zhao, O. Yağan, and V. Gligor, "On the strengths of connectivity and robustness in general random intersection graphs," in *IEEE 53rd Annual Conference on Decision and Control (CDC), 2014*. IEEE, 2014, pp. 3661–3668.

[14] M. Bloznelis, J. Jaworski, and K. Rybarczyk, "Component evolution in a secure wireless sensor network," *Netw.*, vol. 53, pp. 19–26, January 2009.

[15] E. Godehardt and J. Jaworski, "Two models of random intersection graphs for classification," in *Exploratory data analysis in empirical research*. Springer, 2003, pp. 67–81.

[16] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic analysis, control, optimization and applications*. Springer, 1999, pp. 547–566.

[17] O. Yağan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2983–2999, 2012.

[18] B. Bollobás, *Random graphs*. Cambridge university press, 2001, vol. 73.

[19] M. D. Penrose, *Random Geometric Graphs*. Oxford University Press, Jul. 2003.

[20] B. Bollobás, *Random Graphs*, 2nd ed. Cambridge University Press, 2001, cambridge Books Online. [Online]. Available: http://dx.doi.org/10.1017/CBO9780511814068

[21] L. Valiant, "The complexity of enumeration and reliability problems," *SIAM Journal on Computing*, vol. 8, no. 3, pp. 410–421, 1979. [Online]. Available: http://dx.doi.org/10.1137/0208032

[22] J. Provan and M. Ball, "The complexity of counting cuts and of computing the probability that a graph is connected," *SIAM Journal on Computing*, vol. 12, no. 4, pp. 777–788, 1983. [Online]. Available: http://dx.doi.org/10.1137/0212053

[23] S. Janson, T. Łuczak, and A. Ruciński, *Random Graphs. 2000*. Wiley–Intersci. Ser. Discrete Math. Optim, 2000.

[24] S. T. Jensen, "The laguerre-samuelson inequality with extensions and applications in statistics and matrix theory," Ph.D. dissertation, Department of Mathematics and Statistics, McGill University, 1999.