k-connectivity of inhomogeneous random key graphs with unreliable links

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

February 21, 2018

Abstract

We consider secure and reliable connectivity in wireless sensor networks that utilize the heterogeneous random key predistribution scheme. We model the unreliability of wireless links by an on/off channel model that induces an Erdős-Rényi graph, while the heterogeneous scheme induces an inhomogeneous random key graph. The overall network can thus be modeled by the intersection of both graphs. We present conditions (in the form of zero-one laws) on how to scale the parameters of the intersection model so that with high probability i) all of its nodes are connected to at least k other nodes, i.e., the minimum node degree of the graph is no less than k; and ii) the graph is k-connected, i.e., the graph remains connected even if *any* $k-1$ nodes leave the network. These results are shown to complement and generalize several previous work in the literature. We also present numerical results to support our findings in the finite-node regime. Finally, we demonstrate via simulations that our results are also useful when the on/off channel model is replaced with the more realistic *disk communication model*.

Keywords: Wireless Sensor Networks, Security, Heterogeneous Random Key Predistribution Scheme, Disk Model, On/Off Channel Model, Random Graphs.

1 Introduction

1.1 Wireless Sensor Networks and Security

Wireless sensor networks (WSNs) enable a broad range of applications in diverse areas such as military, health, and environmental monitoring, among others [3]. A typical WSN consists of hundreds, thousands, or hundreds of thousands of nodes that are often deployed randomly, perhaps with no knowledge of post-deployment configuration. In many applications, WSNs are envisioned to be deployed in *hostile* environments, where eavesdropping, node capture, and denial-of-service attacks are possible, inducing the need for cryptographic protection. Indeed, securing WSNs is a key challenge given their unique features [4]; e.g., limited computational capabilities, limited

A preliminary version of some of the material was presented at the IEEE International Symposium on Information Theory in 2016 [1] and in 2017 [2]. This work has been supported in part by the National Science Foundation through grant CCF-1617934. R. Eletreby was funded (in part) by the Dowd Fellowship from the College of Engineering at Carnegie Mellon University. The authors would like to thank Philip and Marsha Dowd for their financial support and encouragement.

transmission power, and vulnerability to node capture attacks. In particular, classical *asymmetric* cryptosystems are generally slow and require excessive energy and memory consumption. On the other hand, *symmetric* cryptosystems offer a faster and energy-efficient alternative, making them a feasible choice for securing WSNs [5, 6].

Clearly, symmetric cryptosystems require a mechanism for key-establishment that obeys the aforementioned limitations of WSNs and facilitates the possible change of topology over time. *Key predistribution*, namely, installing cryptographic keys to sensor nodes' memory, was shown to be a practical option for key-establishment in large-scale WSNs [5]. In particular, *random* key predistribution schemes are currently regarded as the most feasible solutions for securing WSNs; e.g., see [7, Chapter 13] and [8], and references therein. Random key predistribution schemes were first introduced in the pioneering work of Eschenauer and Gligor [5]. Their scheme, hereafter referred to as the EG scheme, operates as follows: prior to deployment, each sensor node is assigned a *random* set of K cryptographic keys, selected *uniformly* from a key pool of size P (without replacement). After deployment, two nodes can communicate *securely* over an existing channel *if* they share at least one key. The EG scheme led the way to several other variants, including the q-composite scheme [6], and the random pairwise scheme [6] among others. We remark that random key predistribution schemes do not assume any knowledge of the post-deployment *topology*, which is likely the case for many real-world implementations of WSNs that are deployed randomly.

Recently, a new variation of the EG scheme, referred to as the *heterogeneous* random key predistribution scheme, was introduced in [9]. The heterogeneous scheme considers the case when the network includes sensors with varying levels of resources, features, and security or connectivity requirements (e.g., regular nodes vs. cluster heads); it is in fact envisioned [10] that many WSN applications will be heterogeneous. The scheme is described as follows. Given r classes, each sensor is independently classified as a class-i node with probability $\mu_i > 0$ for each $i = 1, \ldots, r$. Then, sensors in class-i are each assigned K_i keys selected uniformly at random from a key pool of size P. Similar to the EG scheme, nodes that share key(s) can communicate securely over an available channel after the deployment; see Section 2 for details.

1.2 *Reliable* Connectivity under Random Key Predistribution

Given the randomness involved in the heterogeneous scheme, there is a positive probability that a pair of nodes may have *no* common keys and hence can not establish a secure communication link in between. This raises an important question as to *whether and how it would be possible to establish a securely connected* network using the heterogeneous random key predistribution scheme. In many WSN applications, it is desirable that the network is *connected*, meaning that every pair of sensors have a secure communication *path* connecting them, in order to allow the exchange of *control* and *data* messages between participating nodes [11].

In addition to having connectivity, *reliability* against the failure of sensors or links is important in WSN applications where sensors are unattended for long periods of time (e.g., environmental monitoring), or, are prone to node-capture attacks (e.g., battlefield surveillance), or, are used in life-critical applications (e.g., patient monitoring). With this in mind, this paper focuses on the question of how we can design a WSN that is securely k-connected under the heterogeneous scheme. A network is said to be k-connected if its connectivity is preserved despite the failure of any $(k-1)$ nodes or links; a network is simply said to be connected if it is 1-connected. Therefore, k-connectivity provides a guarantee of network reliability against the possible failures of sensors or links due to adversarial attacks, battery depletion, or harsh environmental conditions. Also,

k-connectivity ensures that each pair of nodes in the network are connected by at least k mutually disjoint paths [12].

k-connectivity – a fundamental property of graphs – is particularly important in secure sensor networks where nodes operate *autonomously* and are physically *unprotected*. For instance, k-connectivity provides communication security against an adversary that is able to *compromise* up to $(k-1)$ links by launching a sensor capture attack [6]; i.e., two sensors can communicate securely as long as at least one of the k disjoint paths connecting them consists of links that are not compromised by the adversary. Also, k-connectivity improves robustness against network disconnection due to battery depletion, in both normal mode of operation and under battery-depletion attacks [13, 14]. Furthermore, it enables flexible communication-load balancing across multiple paths so that network energy consumption is distributed without penalizing any access path [15]. In addition, k-connectivity is useful in achieving consensus despite adversarial nodes in the network. Specifically, if $k = 2m + 1$ where m is the number of adversary-controlled nodes, k-connectivity guarantees that consensus can be reached in any network with $n \gg m$ nodes [16, 17]. Finally, k-connectivity has important implications on *mobile* connectivity of WSNs. For instance, if a network is k-connected, then any of its $(k-1)$ nodes can be made *mobile*, and move anywhere in the network freely, while the network remains at least 1-connected all the time. So, in applications where only a small number of sensors need to be mobile, whereas others will be static, k-connectivity will be a crucial property that ensures continuous connectivity of the network.

1.3 From shared-key connectivity to wireless connectivity

With these motivations in mind, we seek to obtain conditions such that a WSN is securely k-connected under the heterogeneous random key predistribution scheme. Our approach is based on modeling the WSN by an appropriate random graph and then establishing scaling conditions on the model parameters such that the resulting network is k-connected with high probability (whp) as the number of nodes n gets large.

With $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$, $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$, and n denoting the network size, let $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ denote the random graph, defined on vertices $\{v_1, \ldots, v_n\}$, where any pair of nodes are *adjacent* as long as they share a key. This graph is referred to as the *inhomogeneous random key graph* [9], and generalizes the well-studied (homogeneous) random key graph model induced under the EG scheme [18, 19]; see Section 2 for precise definitions. The inhomogeneous random key graph models the *shared-key* connectivity of the WSN under the heterogeneous scheme; i.e., its edges represents pairs of sensors that share a key, and hence can securely communicate over an *existing* wireless communication channel.

Next, we need to model the *wireless communication* connectivity of the WSN, say using a (possibly random) graph $\mathbb{I}(n; \cdot)$, whose edges represent pairs of sensors who have a wireless communication channel available in between. The overall model of the WSN will then be an intersection of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and $\mathbb{I}(n; \cdot)$ since a pair of sensors can establish a *secure communication link* if they share a key *and* have a wireless channel available. A good candidate to model the wireless connectivity of a WSN would be the disk model [20]: Assuming that nodes are distributed over a bounded region $\mathcal{D}$ of a euclidean plane, nodes v_i and v_j located at $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, respectively, are able to communicate if $\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho$, where ρ denotes the transmission radius. The case when node locations are independently and uniformly distributed over the region $\mathcal{D}$ induces the random geometric graph [12], hereafter denoted $\mathbb{I}(n; \rho)$.

Now, consider a random graph obtained by intersecting the inhomogeneous random key graph

with the random geometric graph, namely, $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$. Indeed, the resulting random graph represents an accurate model for a WSN secured by the heterogeneous random key predistribution scheme, where two nodes are adjacent only if they share a key *and* are within the transmission radius of each other. Unfortunately, analyzing the k-connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$ [21] is likely to be very challenging. For example, despite many attempts, the Gupta-Kumar conjecture [20] on the 1-connectivity of $\mathbb{G}(n;\alpha)\cap\mathbb{I}(n;\rho)$ where $\mathbb{G}(n;\alpha)$ represents an Erdős-Rényi (ER) graph, has remained unsolved until very recently by Penrose [22]; see [21] for a detailed discussion on the difficulties involved in analyzing *intersection* of different types of graphs. We remark that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ is much more complicated than an ER graph (see [9]), and our goal is to analyze k-connectivity for arbitrary $k=1,2,\ldots$.

The preceding discussion brings about a crucial question, namely, *is there any communication model that provides a good approximation of the classical disk model, but also allows a comprehensive analysis of the resulting WSN?* This question was answered in the affirmative in [21,23], where it was shown that an independent on-off channel model – represented by an ER graph $\mathbb{G}(n;\alpha)$ – provides a good approximation of the disk model in settings similar to considered here. Inspired by the success in these previous approaches, here we also model the wireless communication connectivity of the WSN by an ER graph $\mathbb{G}(n;\alpha)$ and study the k-connectivity properties of the intersection model $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$. As soon will become apparent, this approach will enable us to i) establish rigorous results concerning the secure k-connectivity of a WSN albeit using a simplified wireless communication model; ii) demonstrate via simulations that these results do still apply under the more realistic disk model. In particular, simulation results indicate that k-connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$ behaves very similar to that of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$, when α and ρ are *matched* to lead to the same probability of wireless channel availability; i.e., $\alpha=\pi\rho^2$.

1.4 Contributions

As mentioned above, we study the secure k-connectivity of a WSN that employs the heterogeneous random key predistribution scheme. The wireless communication connectivity is modeled by an *on/off communication model* consisting of independent wireless channels each of which is either on (with probability α), or off (with probability $1-\alpha$); this leads to a standard ER graph [24], denoted by $\mathbb{G}(n,\alpha)$. Hence, the overall random graph modeling the WSN becomes the intersection of an inhomogeneous random key graph with an ER graph, denoted $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$.

We establish two main results for $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$; namely, i) a zero-one law for the minimum node degree of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ to be no less than k for any non-negative integer k and ii) a zero-one law for the k-connectivity property of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ for any non-negative integer k. More precisely, we present conditions on how to scale the parameters of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ so that i) its minimum node degree is no less than k and ii) it is k-connected, both with high probability when the number of nodes n gets large.

Our results are supported by a simulation study (see Section 4) demonstrating that i) despite their asymptotic nature, our results can in fact be useful in designing *finite*-node WSNs so that they achieve secure k-connectivity with high probability; and ii) despite the simplicity of the on-off communication model, the probability of k-connectivity in the resulting WSN approximates very well the case where disk model is used. In addition, our results are shown to complement and generalize several previous work in the literature (see Section 3 for details).

1.5 Notation and Conventions

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 event E, we let $\overline{E}$ denote the complement of E. For any discrete set S, we write $|S|$ for its cardinality. For sets S_a and S_b, the relative compliment of S_a in S_b is given by $S_a \setminus S_b$. 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. Namely, we write $a_n = o(b_n)$ as a shorthand for the relation $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$, whereas $a_n = O(b_n)$ means that there exists $c > 0$ such that $a_n \leq cb_n$ for all n sufficiently large. Also, we have $a_n = \Omega(b_n)$ if $b_n = O(a_n)$, or equivalently, if there exists $c > 0$ such that $a_n \geq cb_n$ for all n sufficiently large. Finally, we write $a_n = \Theta(b_n)$ if we have $a_n = O(b_n)$ and $a_n = \Omega(b_n)$ at the same time. 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 sensor nodes labeled as $v_1, v_2, \ldots, v_n$. Each sensor is assigned to one of the r possible classes (e.g., priority levels) according to a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for each $i = 1, \ldots, r$; clearly it is also needed that $\sum_{i=1}^{r} \mu_i = 1$. Prior to deployment, each class-i node is given K_i cryptographic keys selected uniformly at random from a pool of size P. Hence, the key ring Σ_x of node v_x is a $\mathcal{P}_{K_{t_x}}$-valued random variable (rv) where $\mathcal{P}_A$ denotes the collection of all subsets of $\{1, \ldots, P\}$ with exactly A 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

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

After the deployment, two sensors can communicate securely over an existing communication channel if they have at least one key in common.

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

$$K_{xy} := [\Sigma_x \cap \Sigma_y \neq \emptyset]\,. \tag{1}$$

The adjacency condition (1) characterizes the inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ that has been introduced recently in [9]. This model is also known in the literature as the *general random intersection graph*; e.g., see [25–27].

The inhomogeneous random key graph models the *cryptographic* connectivity of the underlying WSN. In particular, the probability p_{ij} that a class-i node and a class-j have a common key, and thus are adjacent in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$, is given by

$$p_{ij} = \mathbb{P}[K_{xy}] = 1 - \binom{P - K_i}{K_j} \Big/ \binom{P}{K_j} \tag{2}$$

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we clearly have $p_{ij} = 1$. We also find it useful define the *mean* probability λ_i of edge occurrence for a class-i node in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$. With arbitrary nodes v_x and v_y, we have

$$\lambda_i = \mathbb{P}[K_{xy} \mid t_x = i] = \sum_{j=1}^{r} p_{ij}\mu_j, \quad i = 1, \ldots, r, \tag{3}$$

as we condition on the class t_y of node v_y.

In this work, we consider the communication topology of the WSN as consisting of independent channels that are either *on* (with probability α) or *off* (with probability $1 - \alpha$). More precisely, let $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$ denote i.i.d Bernoulli rvs, each with success probability α. The communication channel between two distinct nodes v_x and v_y is on (respectively, off) if $B_{xy}(\alpha) = 1$ (respectively if $B_{xy}(\alpha) = 0$). The on/off channel model induces a standard Erdős-Rényi (ER) graph $\mathbb{G}(n; \alpha)$ [28], defined on the vertices $\mathcal{V} = \{v_1, \ldots, v_n\}$ such that v_x and v_y are adjacent, denoted C_{xy}, if $B_{xy}(\alpha) = 1$[1].

We model the overall topology of a WSN by the intersection of an inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and an ER graph $\mathbb{G}(n; \alpha)$. Namely, nodes v_x and v_y are adjacent in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \alpha)$, denoted E_{xy}, if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{G}$. In other words, the edges in the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \alpha)$ represent pairs of sensors that can securely communicate as they have i) a communication link in between that is *on*, and ii) a shared cryptographic key. Therefore, studying the connectivity properties of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \alpha)$ amounts to studying the secure connectivity of heterogeneous WSNs under the on/off channel model.

Hereafter, we denote the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \alpha)$ by the graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$. To simplify the notation, we let $\boldsymbol{\theta} = (\boldsymbol{K}, P)$, and $\boldsymbol{\Theta} = (\boldsymbol{\theta}, \alpha)$. The probability of edge existence between a class-i node v_x and a class-j node v_y in $\mathbb{H}(n; \boldsymbol{\Theta})$ is given by

$$\mathbb{P}[E_{xy} \mid t_x = i, t_y = j] = \mathbb{P}[K_{xy} \cap C_{xy} \mid t_x = i, t_y = j] = \alpha p_{ij}$$

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

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

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.

We close this section with some additional notation that will be useful in the rest of the paper. For any three distinct nodes v_x , v_y and v_j, we define $E_{xj \cap yj} := E_{xj} \cap E_{yj}$, $E_{xj \cap \overline{yj}} := E_{xj} \cap \overline{E_{yj}}$, $E_{\overline{xj} \cap yj} := \overline{E_{xj}} \cap E_{yj}$, and $E_{\overline{xj} \cap \overline{yj}} := \overline{E_{xj}} \cap \overline{E_{yj}}$.

[1] An interesting direction for future work is to consider a heterogeneous link-failure model, where the link between a type-i and type-j node fails with probability $1 - \alpha_{ij}$, for each $i, j = 1, \ldots, r$. Some preliminary results in that case can be found in [29].

3 Main Results and Discussion

3.1 Results

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) as long as the conditions

$$2 \leq K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{5}$$

are satisfied for all $n = 2, 3, \ldots$. Similarly any mapping $\alpha : \mathbb{N}_0 \to (0, 1)$ defines a scaling for the ER graphs. As a result, a mapping $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)$ defines a scaling for the intersection graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ given that condition (5) holds. We remark that under (5), the edge probabilities p_{ij} will be given by (2).

We first present a zero-one law for the minimum node degree being no less than k in the inhomogeneous random key graph intersecting ER graph.

Theorem 3.1. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through*

$$\Lambda_1(n) = \alpha_n \lambda_1(n) = \frac{\log n + (k-1) \log \log n + \gamma_n}{n}, \tag{6}$$

for each $n = 1, 2, \ldots$.

(a) If $\lambda_1(n) = o(1)$, we have

$$\lim_{n \to \infty} \mathbb{P}\left[\begin{array}{l} \textit{Minimum node degree} \\ \textit{of } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \geq k \end{array} \right] = 0 \quad \textit{if } \lim_{n \to \infty} \gamma_n = -\infty$$

(b) We have

$$\lim_{n \to \infty} \mathbb{P}\left[\begin{array}{l} \textit{Minimum node degree} \\ \textit{of } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \geq k \end{array} \right] = 1 \quad \textit{if } \lim_{n \to \infty} \gamma_n = \infty.$$

Next, we present a zero-one law for the k-connectivity of $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$.

Theorem 3.2. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through (6) for each $n = 1, 2, \ldots$.*

(a) If $\lambda_1(n) = o(1)$, we have

$$\lim_{n \to \infty} \mathbb{P}\left[\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \textit{ is } k\textit{-connected}\right] = 0 \quad \textit{if } \lim_{n \to \infty} \gamma_n = -\infty$$

(b) If

$$P_n = \Omega(n), \tag{7}$$

$$\frac{K_{r,n}}{P_n} = o(1), \tag{8}$$

$$\frac{K_{r,n}}{K_{1,n}} = o(\log n), \tag{9}$$

we have

$$\lim_{n \to \infty} \mathbb{P}\left[\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \textit{ is } k\textit{-connected}\right] = 1 \quad \textit{if } \lim_{n \to \infty} \gamma_n = \infty. \tag{10}$$

In words, Theorem 3.1 (respectively Theorem 3.2) states that the minimum node degree in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ is greater than or equal to k (respectively $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ is k-connected) whp if the mean degree of class-1 nodes, i.e., $n\Lambda_1(n)$, is scaled as $(\log n + (k-1)\log\log n + \gamma_n)$ for some sequence γ_n satisfying $\lim_{n\to\infty}\gamma_n = \infty$. On the other hand, if the sequence γ_n satisfies $\lim_{n\to\infty}\gamma_n = -\infty$, then whp $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ has at least one node with degree strictly less than k, and hence is *not* k-connected. This shows that the critical scaling for the minimum node degree of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ being greater than or equal to k (respectively for $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ to be k-connected) is given by $\Lambda_1(n) = \frac{\log n + (k-1)\log\log n}{n}$, with the sequence $\gamma_n : \mathbb{N}_0 \to \mathbb{R}$ measuring the deviation of $\Lambda_1(n)$ from the critical scaling.

The scaling condition (6) can be given a more explicit form under some additional constraints. In particular, it was shown in [9, Lemma 4.2] that if $\lambda_1(n) = o(1)$ then

$$\lambda_1(n) \sim \frac{K_{1,n}K_{\text{avg},n}}{P_n} \tag{11}$$

where $K_{\text{avg},n} = \sum_{j=1}^{r}\mu_j K_{j,n}$ denotes the *mean* key ring size in the network. This shows that the minimum key ring size $K_{1,n}$ is of paramount importance in controlling the connectivity and reliability of the WSN; as explained previously, it then also controls the number of *mobile* sensors that can be accommodated in the network. For example, with the mean number $K_{\text{avg},n}$ of keys per sensor is fixed, we see that reducing $K_{1,n}$ by half means that the smallest α_n (that gives the largest link failure probability $1-\alpha_n$) for which the network remains k-connected whp is increased by two-fold for any given k; e.g., see Figure 3 for a numerical example demonstrating this.

3.2 Comments on the additional technical conditions

We first comment on the additional technical condition $\lambda_1(n) = o(1)$. This is enforced here mainly for technical reasons for the proof of the zero-law of Theorem 3.1 (and thus of Theorem 3.2) to work. A similar condition was also required in [17, Thm 1] for establishing the zero-law for the minimum node degree being no less than k in the *homogeneous* random key graph intersecting ER graph. In view of (11), this condition is equivalent to

$$K_{1,n}K_{\text{avg},n} = o(P_n). \tag{12}$$

In real-world WSN applications the key pool size P_n is envisioned to be orders of magnitude larger than any key ring size in the network [5, 30]. As discussed below in more details, this is needed to ensure the resilience of the network against adversarial attacks. Concluding, (12) (and thus $\lambda_1(n) = o(1)$) is indeed likely to hold in most applications.

Conditions (7) and (8) are also likely to be needed in practical WSN implementations in order to ensure the *resilience* of the network against node capture attacks; e.g., see [5, 30]. To see this, assume that an adversary captures a number of sensors, compromising all the keys that belong to the captured nodes. If $P_n = O(K_{r,n})$ contrary to (8), then it would be possible for the adversary to compromise a positive fraction of the key pool (i.e., $\Omega(P_n)$ keys) by capturing only a constant number of sensors that are of type r. Similarly, if $P_n = o(n)$, contrary to (7), then again it would be possible for the adversary to compromise $\Omega(P_n)$ keys by capturing only $o(n)$ sensors (whose type does not matter in this case). In both cases, the WSN would fail to exhibit the *unassailability* property [31, 32] and would be deemed as vulnerable against adversarial attacks. We remark that both (7) and (8) were required in [9,17] for obtaining the one-law for connectivity and k-connectivity, respectively, in similar settings to ours.

Finally, the condition (9) is enforced mainly for technical reasons and takes away from the flexibility of assigning very small key rings to a certain fraction of sensors when k-connectivity is considered; we remark that (9) is not needed for the minimum node degree result given at Theorem 3.1. An equivalent condition was also needed in [9] for establishing the one-law for connectivity in inhomogeneous random key graphs. We refer the reader to [9, Section 3.2] for an extended discussion on the feasibility of (9) for real-world WSN implementations, as well as possible ways to replace it with milder conditions.

We close by providing a concrete example that demonstrates how all the conditions required by Theorem 3.2 can be met in a real-world implementation. Consider any number r of sensor types, and pick any probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for all $i = 1, \ldots, r$. For any channel probability $\alpha_n = \Omega(\frac{\log n}{n})$, set $P_n = n \log n$ and use

$$K_{1,n} = \frac{(\log n)^{1/2+\varepsilon}}{\sqrt{\alpha_n}} \quad \text{and} \quad K_{r,n} = \frac{(1+\varepsilon)(\log n)^{3/2-\varepsilon}}{\mu_r \sqrt{\alpha_n}}$$

with any $\varepsilon > 0$. Other key ring sizes $K_{1,n} \leq K_{2,n}, \ldots, K_{r-1,n} \leq K_{r,n}$ can be picked arbitrarily. In view of Theorem 3.2 and the fact [9, Lemma 4.2] that $\lambda_1(n) \sim \frac{K_{1,n} K_{\text{avg},n}}{P_n}$, the resulting network will be k-connected whp for any $k = 1, 2, \ldots$. Of course, there are many other parameter scalings that one can choose.

3.3 Comparison with related work

The classical Eschenauer-Gligor scheme induces a class of random graphs denoted by the *homogeneous random key graphs*, $\mathbb{K}(n; K, P)$, where all nodes belong to the same class and receive the same number K of keys. Several properties of the homogeneous random key graph, $\mathbb{K}(n; K, P)$, have been extensively studied in literature. In particular, the 1-connectivity of $\mathbb{K}(n; K, P)$ has been investigated in [19,30,33,34] under *full* visibility, i.e., when all pairs of nodes have a communication channel in between. Therein, authors provided scaling conditions on the key ring size K_n and the key pool size P_n as functions of the network size n such that the resulting network is connected with high probability as the number of nodes gets large. Moreover, the k-connectivity property of $\mathbb{K}(n; K, P)$ was investigated under full visibilty in [35].

Our paper extends these results to the heterogeneous setting, where sensor nodes have different levels of resources and security/connectivity requirements, thus possibly belonging to different classes. Such heterogeneity induces the need for the *inhomogeneous* random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ as an accurate model for the crypto-connectivity of the resulting WSN. Also, unlike the aforementioned results that assume full visibility, our paper considers the wireless connectivity of the network through the on/off channel model.

In [17], Zhao et al. investigated the k-connectivity property of $\mathbb{K}(n; , K, P)$ under an an/off channel model. There, zero-one laws for the property that the minimum node degree is no less than k and the property that the graph is k-connected were established for $\mathbb{H}(n, K, P, \alpha)$, where $\mathbb{H}(n, K, P, \alpha) := \mathbb{K}(n, K, P) \cap \mathbb{G}(n; \alpha)$. Clearly, our paper expands these results to the heterogeneous setting as we consider the intersection of the *inhomogeneous* random key graph with ER graph. In particular, with $r = 1$, i.e., when all nodes belong to the same class and thus receive the same number K of keys, Theorem 3.1 and Theorem 3.2 recover the results of Zhao et al. (See [17, Theorems 1-2]).

In comparison with the existing literature on similar models, our result can be seen to extend the work by Eletreby and Yağan in [36]. Therein, the authors established a zero-one law for the 1-

connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$, i.e., for a WSN under the heterogeneous key predistribution scheme and on-off channel model. Although these results form a crucial starting point towards the analysis of the heterogeneous key predistribution scheme, they do not guarantee that the WSN would remain connected when sensors fail due to battery depletion or get captured by an adversary. Moreover, the results in [36] are not applicable for *mobile* WSNs since the mobility of even a single sensor may render the network disconnected. The results established here fill these gaps by establishing k-connectivity results.

Our paper also generalizes the work by Yağan [9] who considered the inhomogeneous random key graph $\mathbb{K}(n,\boldsymbol{\mu},\boldsymbol{K},P)$ under *full* visibility; i.e., when all pairs of nodes have a communication channel in between. There, Yağan established zero-one laws for the absence of isolated nodes (i.e., absence of nodes with degree zero) and 1-connectivity. Our work generalizes Yağan's results on two fronts. Firstly, we consider more practical WSN scenarios where the unreliability of wireless communication channels are taken into account through the on/off channel model. Secondly, in addition to the properties that the graph has no isolated nodes (i.e., the minimum node degree is no less than 1) and is 1-connected, we consider general minimum node degree and connectivity values, $k = 0, 1, \ldots$.

4 Numerical Results

We now present numerical results to support Theorems 3.1 and 3.2 in the finite node regime. Moreover, we also verify the validity of our claim that the on/off channel model serves as a good approximation of the disk model. In all experiments, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10^4$.

To compare the connectivity behavior of the heterogeneous key predistribution scheme under the disk model with that of the on-off channel model, consider 500 nodes distributed uniformly and independently over a folded unit square $[0,1]^2$ with toroidal (continuous) boundary conditions. Since there are no border effects, we get

$$\mathbb{P}\left[\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho\right] = \pi\rho^2, \qquad i \neq j, \quad i,j = 1,\ldots,n$$

whenever $\rho < 0.5$. Thus, in order to match the two communication models $\mathbb{G}(n,\alpha)$ and $\mathbb{I}(n,\rho)$, we set $\alpha = \pi\rho^2$. Now, recall that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha) = \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$, and let $\widetilde{\mathbb{H}}(n;\boldsymbol{\mu},\boldsymbol{\theta},\rho) = \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{I}(n;\rho)$. In what follows, we present several simulation results comparing the (empirical) probabilities that $\mathbb{H}$ and $\widetilde{\mathbb{H}}$ are k-connected, respectively.

In our first set of experiments, we consider the channel parameters $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$, while varying the parameter K_1, i.e., the smallest key ring size, from 10 to 40. 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 $(\boldsymbol{K},\alpha)$, we generate 1000 independent samples of the graphs $\mathbb{H}$ and $\widetilde{\mathbb{H}}$, and count the number of times (out of a possible 1000) that the obtained graphs i) have minimum node degree no less than 2 and ii) are 2-connected. Dividing the counts by 1000, we obtain the (empirical) probabilities for the events of interest. In all cases considered here, we observe that $\mathbb{H}$ (resp. $\widetilde{\mathbb{H}}$) is 2-connected whenever it has minimum node degree no less than 2 yielding the same empirical probability for both events. This supports the fact that the properties of k-connectivity and minimum node degree being larger than k are asymptotically equivalent in $\mathbb{H}$.

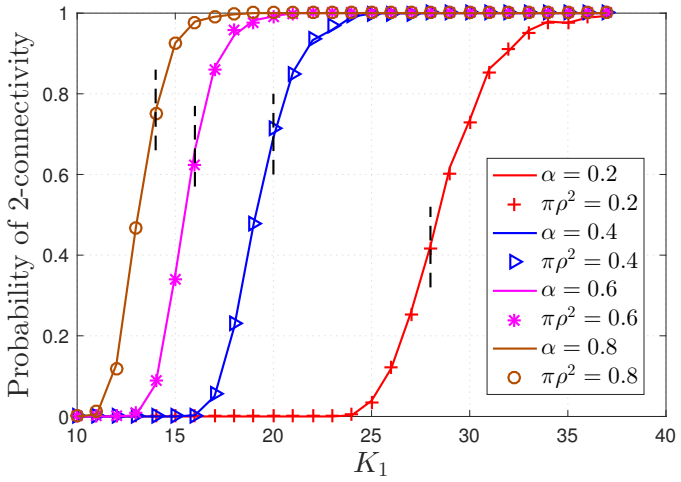

Figure 1: Empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ and $\widetilde{\mathbb{H}}(n;\boldsymbol{\mu},\boldsymbol{\theta},\rho)$ are 2-connected as a function of $\boldsymbol{K}$ for $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$ with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 1000 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.2.

The results obtained for the empirical probabilities of 2-connectivity are depicted in Figure 1, where lines represent the results under the on-off model (i.e., $\mathbb{H}$), while symbols represent the results under the disk model (i.e., $\widetilde{\mathbb{H}}$). In all cases, we see that empirical probabilities are almost identical, supporting the claim that the on/off channel model serves as a good approximation of the disk model (under $\alpha = \pi\rho^2$). More importantly, this shows that our main results are likely to hold also under the disk communication model. For each curve in Figure 1, we also show the critical threshold of connectivity "predicted" by Theorem 3.2 by a vertical dashed line. More specifically, the vertical dashed lines stand for the minimum integer value of K_1 that satisfies

$$\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left(1 - \frac{\binom{P-K_j}{K_1}}{\binom{P}{K_1}} \right) > \frac{1}{\alpha} \frac{\log n + (k-1)\log\log n}{n} \tag{13}$$

with any given k and α. We see from Figure 1 that the probability of k-connectivity transitions from zero to one within relatively small variations in K_1. Moreover, the critical values of K_1 obtained by (13) lie within the transition interval.

In Figure 2, we consider four different values for k, namely we set $k = 4$, $k = 6$, $k = 8$, and $k = 10$ while varying K_1 from 10 to 40 and fixing $\alpha = \pi\rho^2 = 0.4$. 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 $\mathbb{H}$ and $\widetilde{\mathbb{H}}$ are k-connected versus K_1. The critical threshold of connectivity asserted by Theorem 3.2 is again shown by a vertical dashed line. Again, we see that numerical results are in parallel with Theorem 3.2, and that the k-connectivity behaviors of $\mathbb{H}$ and $\widetilde{\mathbb{H}}$ are very close to each other.

Figure 3 is generated in a similar manner with Figure 1, this time with an eye towards understanding the impact of the minimum key ring size K_1 on network connectivity. To that end, we fix the number of classes at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and consider four different key ring sizes $\boldsymbol{K}$ each with

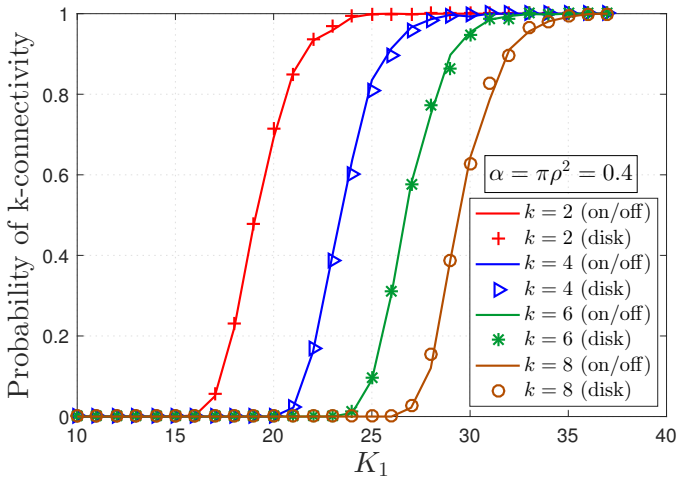

Figure 2: Empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ and $\widetilde{\mathbb{H}}(n;\boldsymbol{\mu},\boldsymbol{\theta},\rho)$ are k-connected as a function of K_1 for $k = 4$, $k = 6$, $k = 8$, and $k = 10$, with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 1000 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.2.

mean 40; we consider $\boldsymbol{K} = \{10, 70\}$, $\boldsymbol{K} = \{20, 60\}$, $\boldsymbol{K} = \{30, 50\}$, and $\boldsymbol{K} = \{40, 40\}$. We compare the probability of 2-connectivity in the resulting networks while varying α (and consequently $\pi\rho^2$) from zero to one. We see that although the average number of keys per sensor is kept constant in all four cases, network connectivity improves dramatically as the minimum key ring size K_1 increases; e.g., with $\alpha = \pi\rho^2 = 0.2$, the probability of connectivity is one when $K_1 = K_2 = 40$ while it drops to zero if we set $K_1 = 10$ while increasing K_2 to 70 so that the mean key ring size is still 40. Once again, we see that the results under the on-off model are very similar to those obtained under the disk model. In fact, Figure 3 suggests that our work can be useful in determining the minimum transmission radius ρ needed to achieve a certain probability of k-connectivity in the network; e.g., to guarantee 2-connectivity almost surely with $K_1 = 20$ and $K_2 = 60$ (with other parameters as in the caption of Figure 3), we need to have at least $\pi\rho^2 = 0.38$.

Finally, we examine the reliability of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ by looking at the probability of 1-connectivity as the number of deleted (i.e., failed) nodes increases. From a mobility perspective, this is equivalent to investigating the probability of a WSN remaining connected as the number of *mobile* sensors leaving the network increases. In Figure 4, we set $n = 500, \boldsymbol{\mu} = \{1/2, 1/2\}, \alpha = 0.4, P = 10^4$, and select K_1 and $K_2 = K_1 + 10$ from (13) for $k = 8$, $k = 10$, $k = 12$, and $k = 14$. With these settings, we would expect (for very large n) the network to remain connected whp after the deletion of up to 7, 9, 11, and 13 nodes, respectively. Using the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ is connected as a function of the number of deleted nodes[2] in each case. We see that even with $n = 500$ nodes, the resulting reliability is close to the levels expected to be attained asymptotically as n goes to infinity. In particular, we see that the

[2]We choose the nodes to be deleted from the *minimum vertex cut* of $\mathbb{H}$, defined as the minimum cardinality set whose removal renders it disconnected. This captures the worst-case nature of the k-connectivity property in a computationally efficient manner (as compared to searching over all k-sized subsets and deleting the one that gives maximum damage).

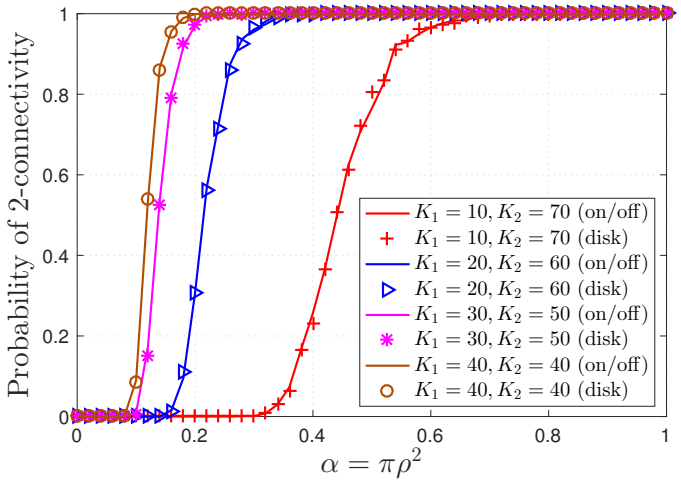

Figure 3: Empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ and $\widetilde{\mathbb{H}}(n;\boldsymbol{\mu},\boldsymbol{\theta},\rho)$ are 2-connected with $n = 500, \boldsymbol{\mu} = (1/2, 1/2)$, and $P = 10^4$; we consider four choices of $\boldsymbol{K} = (K_1, K_2)$ each with the same mean.

probability of remaining connected when $(k-1)$ nodes leave the network is around 0.75 for the first two cases and around 0.90 for the other two cases.

5 Other application areas: A novel model for spreading processes on complex networks

Complex networks denote a class of real-world networks that exhibit non-trivial structural properties that are neither purely regular nor purely random [37]. Examples of complex networks include brain networks [38], the World Wide Web [39], transportation networks [40], and indeed, social networks [41]. Spreading processes, such as information [42, 43] or infectious disease [44, 45] propagation, are fundamental phenomena occurring in complex networks. The study of spreading processes on complex networks is significant to our understanding of how information or diseases propagate on a network, and illustrates the delicate interplay between the structure of the network and the dynamics of propagation.

Over the coarse of the past decade, researchers proposed multiple *generative* models to create networks that resemble the *structure* of real-world complex networks, allowing for large-scale simulations and predictions of how a spreading process would behave in real-life. The inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ (presented herein solely from a security perspective) can also be seen as a useful and natural generative model for real-world *common-interest* social networks. A common interest relationship between two friends manifests from their selection of common interests or hobbies from a large pool [46]. This can be modeled by an inhomogeneous random key graph, where each individual has a set of interests (possibly of different sizes) sampled from a large pool of interests and two individuals are connected if they happen to share an interest. Moreover, this model generates networks that are highly clustered, have small diameter [47] (hence, small-world [48]), and with tunable degree distribution [49], making it a very plausible and intuitive model for real-world social networks. In fact, most real-world social networks were shown to be highly

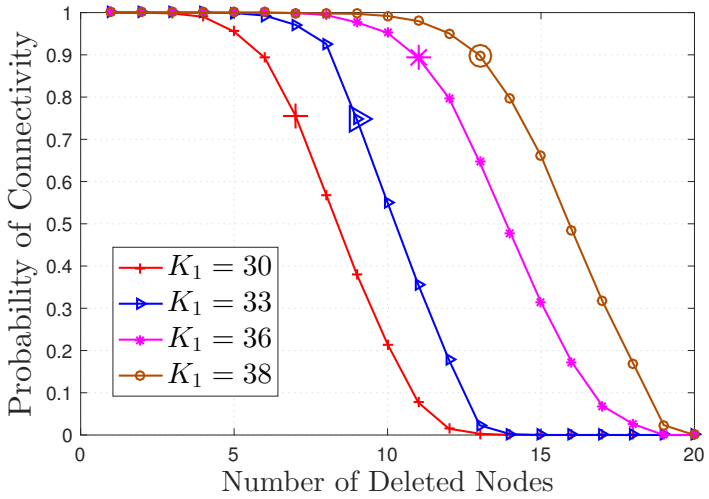

Figure 4: Empirical probability that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\theta},\alpha)$ remains connected after deleting nodes from the *minimum vertex cut* set. We fix $n = 500, \boldsymbol{\mu} = (1/2, 1/2), \alpha = 0.4, P = 10^4$, and choose K_1 and $K_2 = K_1 + 10$ from (13) for each $k = 8$, $k = 10$, $k = 12$, and $k = 14$; i.e., we use $K_1 = 30, 33, 36, 38$, respectively.

clustered and have small diameter [39, 48].

The intersection model $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\alpha)$ considered here can be useful in studying the propagation of epidemics or information on complex networks as well. A simple model for the spread of epidemics (or information) on complex networks is the so called Susceptible-Infected-Recovered (SIR) model. Therein, a disease is transmitted to a susceptible individual upon contact with an infected individual. Later on, infected individuals recover from the disease and gain immunity from it. The outbreak size is precisely the number of recovered individuals at the steady state. This model results in reasonable predictions for the cases where recovery grants lasting resistance. In [45], it was shown that under some conditions, the dynamics of the SIR model on a given network maps to a *bond-percolation* problem with the average *transmissibility* of the disease as the percolation parameter. Namely, with α being the average transmissibility, if we are to occupy each edge in the graph with probability α, the final outbreak size would be the size of the cluster of vertices that can be reached from the initially infected vertex by traversing only the occupied edges [45]. Typically, one is interested in deriving the threshold value of α for which a *giant* connected component emerges, indicating that the disease has reached a positive fraction of the population.

Intersecting the inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ with an ER graph $\mathbb{G}(n;\alpha)$ is essentially equivalent to *occupying* each edge of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ independently with probability α. Hence, the scaling condition for which the one-law of Theorem 3.2 holds gives us a threshold value of α for which the network becomes k-connected, implying that a strain of a disease or a piece of information would infect the entire population i) no matter which individual starts the process, and ii) even if any $k-1$ individuals leave the network (e.g., disease-induced mortality). In particular, let $\hat{\alpha}_n := \left(\log n + (k-1)\log\log n + \gamma_n\right)/(n\lambda_1(n))$ (with $\lim_{n\to\infty}\gamma_n = \infty$ and under the enforced conditions of the one-law of Theorem 3.2). If the average transmissibility of a disease α satisfies $\alpha_n > \hat{\alpha}_n$, a single giant component containing all of the vertices emerge (because in this case

the network is k-connected by virtue of Theorem 3.2), allowing the disease to infect every single vertex. Moreover, the giant component would persist even if any $k-1$ vertices leave the network. Therefore, our results on the k-connectivity of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\alpha)$ provide a threshold on the average transmissibility a disease should have in order to persist in a given population, even when some individuals leave the network, and subsequently cut some of the propagation pathways.

6 Preliminaries

A number of technical results are collected here for easy referencing.

Proposition 6.1 ([9, 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*

$$\lambda_1(n) \leq \lambda_2(n) \leq \ldots \leq \lambda_r(n), \qquad n = 2, 3, \ldots. \tag{14}$$

In view of (4), Proposition 6.1 implies that

$$\Lambda_1(n) \leq \Lambda_2(n) \leq \ldots \leq \Lambda_r(n), \qquad n = 2, 3, \ldots. \tag{15}$$

Proposition 6.2. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through (6) for each $n = 1, 2, \ldots$. Under (7) and (9), we have*

$$K_{1,n} = \omega(1) \tag{16}$$

when $\lim_{n\to\infty} \gamma_n = +\infty$.

Proof. From (6), we clearly have

$$\lambda_1(n) > \frac{\log n}{n\alpha_n} \tag{17}$$

for all n sufficiently large when $\lim_{n\to\infty} \gamma_n = +\infty$. We also know from [19, Lemmas 7.1-7.2] that

$$p_{1j}(n) \leq \frac{K_{1,n}K_{j,n}}{P_n - K_{j,n}} \leq 2\frac{K_{1,n}K_{j,n}}{P_n}, \quad j = 1, \ldots, r$$

where the last bound follows from (5). This leads to

$$\lambda_1(n) = \sum_{j=1}^{r} \mu_j p_{1j} \leq 2\sum_{j=1}^{r} \mu_j \frac{K_{1,n}K_{j,n}}{P_n} \leq 2\frac{K_{1,n}K_{r,n}}{P_n} \tag{18}$$

Combining (17) and (18) we get

$$K_{1,n}^2 \frac{K_{r,n}}{K_{1,n}} > \frac{P_n}{2}\frac{\log n}{n\alpha_n}$$

for all n sufficiently large. Under (7) and (9), this immediately establishes (16) since $\alpha_n \leq 1$. ■

Fact 6.3. *For any positive constants ℓ_1, ℓ_2, the function*

$$f(x) = x^{\ell_1}(1-x)^{n-\ell_2}, \quad x \in (0,1) \tag{19}$$

is monotone decreasing in x for all n sufficiently large.

Proof. Differentiating $f(x)$ with respect to $x \in (0,1)$, we get

$$\begin{aligned}\frac{d}{dx}f(x) &= \ell_1 x^{\ell_1-1}(1-x)^{n-\ell_2} - (n-\ell_2)x^{\ell_1}(1-x)^{n-\ell_2-1} \\ &= x^{\ell_1-1}(1-x)^{n-\ell_2-1}(\ell_1(1-x)-(n-\ell_2)x).\end{aligned}$$

The conclusion follows since $(\ell_1(1-x)-(n-\ell_2)x) < 0$ for all n sufficiently large, for any positive ℓ_1, ℓ_2 and $x \in (0,1)$. ■

Fact 6.4 ([17, Fact 3])**.** *Let x and y be both positive functions of n. If $x = o(1)$, and $x^2 y = o(1)$ hold, then*

$$(1-x)^y \sim e^{-xy}$$

We will use several bounds given below throughout the paper:

$$(1 \pm x) \leq e^{\pm x}, \quad x \in (0,1) \tag{20}$$

$$(x+y)^p \leq 2^{p-1}\left(x^p + y^p\right), \quad x, y \geq 0, \quad p \geq 1 \tag{21}$$

$$\binom{n}{\ell} \leq \left(\frac{en}{\ell}\right)^{\ell}, \quad \ell = 1, \ldots, n, \quad n = 1, 2, \ldots \tag{22}$$

$$\sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \leq 2^n \tag{23}$$

$$\binom{n}{\ell} \leq n^{\ell}, \quad \ell = 1, \ldots, n, \quad n = 1, 2, \ldots \tag{24}$$

7 Proof of Theorem 3.1

7.1 Establishing the one-law

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

$$X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^{n} \mathbf{1}\left[v_i \text{ is of degree } \ell \text{ in } \mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right]$$

The method of first moment [50, Eqn. (3.10), p. 55] gives

$$\mathbb{P}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0\right] \geq 1 - \mathbb{E}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] \tag{25}$$

The one-law states that the minimum node degree in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ is no less than k asymptotically almost surely (a.a.s.); i.e., $\lim_{n\to\infty} \mathbb{P}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0\right] = 1$, for all $\ell = 0, 1, \ldots, k-1$. Thus, the one-law will follow if we show that

$$\lim_{n\to\infty} \mathbb{E}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] = 0, \quad \ell = 0, 1, \ldots, k-1. \tag{26}$$

We let $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the event that node v_i in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ has degree ℓ for each $i = 1,2,\ldots,n$. Throughout, we simplify the notation by writing $D_{i,\ell}$ instead of $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$. By definition, we have $X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^n \mathbf{1}\left[D_{i,\ell}\right]$ and it follows that

$$\mathbb{E}\left[X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] = \sum_{i=1}^{n} \mathbb{P}\left[D_{i,\ell}\right] = n\mathbb{P}\left[D_{x,\ell}\right] \tag{27}$$

by the exchangeability of the indicator rvs $\{\mathbf{1}\left[D_{i,\ell}\right]; i = 1,\ldots,n\}$.

In view of (25) and (27), we see that (26) and hence the one-law would follow upon showing

$$\lim_{n\to\infty} n\mathbb{P}\left[D_{x,\ell}\right] = 0, \quad \ell = 0,1,\ldots,k-1. \tag{28}$$

We start by deriving the probability of $D_{x,\ell}$. For any node v_x, the events

$$E_{1x}, E_{2x}, \ldots, E_{(x-1)x}, E_{(x+1)x}, \ldots, E_{nx}$$

are mutually independent *conditionally* on the type t_x. It follows from (4) that the degree of a node v_x, i.e., D_x, is conditionally binomial leading to

$$D_x =_{st} \mathrm{Bin}(n-1,\Lambda_i), \quad \text{with probability } \mu_i, \quad i = 1,\ldots,r$$

Thus, we get

$$\begin{aligned}
\mathbb{P}\left[D_{x,\ell}\right] &= \sum_{i=1}^{r} \mu_i \mathbb{P}\left[D_{x,\ell} \mid t_x = i\right] \\
&= \sum_{i=1}^{r} \mu_i \binom{n-1}{\ell} \left(\Lambda_i(n)\right)^\ell \left(1-\Lambda_i(n)\right)^{n-\ell-1} \\
&\le \left((\ell!)^{-1} \sum_{i=1}^{r} \mu_i \left(n\Lambda_i(n)\right)^\ell \left(1-\Lambda_i(n)\right)^{n-\ell-1} \right) \\
&\le (\ell!)^{-1} \left(n\Lambda_1(n)\right)^\ell \left(1-\Lambda_1(n)\right)^{n-\ell-1} \\
&\le (\ell!)^{-1} \left(n\Lambda_1(n)\right)^\ell e^{-(n-\ell-1)\Lambda_1(n)}
\end{aligned}$$

for all n sufficiently large, as we invoke Fact 6.3 together with (15), and note that ℓ is a non-negative integer constant. Combining (6) and (21), and using the fact that $\Lambda_1(n) \le 1$, we see that

$$\begin{aligned}
n\mathbb{P}\left[D_{x,\ell}\right] &\le n(\ell!)^{-1} \left(\log n + (k-1)\log\log n + \gamma_n\right)^\ell e^{-\log n - (k-1)\log\log n - \gamma_n} e^{(\ell+1)\Lambda_1(n)} \\
&\le 2^{\ell-1} \left((\log n)^\ell (1+o(1))^\ell + \gamma_n^\ell \right) e^{-(k-1)\log\log n - \gamma_n} e^{O(1)} \\
&= O(1) e^{-(k-1-\ell)\log\log n - \gamma_n} + O(1)\gamma_n^\ell e^{-(k-1)\log\log n - \gamma_n}.
\end{aligned}$$

When $\lim_{n\to\infty} \gamma_n = \infty$, we readily get the desired conclusion (28). This establishes the one-law.

7.2 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 in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ that are *class*-1 and with degree ℓ. Similar to the discussion given before, we let $Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number of nodes that are class-1 and with degree ℓ in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$, namely,

$$Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^{n} \mathbf{1}\left[v_i \text{ is class 1 and has degree } \ell \text{ in } \mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] \tag{29}$$

Clearly, if we can show that whp there exists at least one class-1 node with a degree strictly less than k under the enforced assumptions (with $\lim_{n\to\infty}\gamma_n = -\infty$) then the zero-law immediately follows.

With a slight abuse of notations, we let $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the event that node v_i in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ is class-1 and has degree ℓ for each $i = 1, 2, \ldots, n$. Throughout, we simplify the notation by writing $D_{i,\ell}$ instead of $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$. Thus, we have $Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^{n}\mathbf{1}\left[D_{i,\ell}\right]$. The method of second moments [50, Remark 3.1, p. 55] gives

$$\mathbb{P}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0\right] \leq 1 - \frac{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right]^2}{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right]}. \tag{30}$$

We have $\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] = n\mathbb{P}\left[D_{x,\ell}\right]$ and

$$\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right] = n\mathbb{P}\left[D_{x,\ell}\right] + n(n-1)\mathbb{P}\left[D_{x,\ell}\cap D_{y,\ell}\right],$$

whence

$$\frac{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right]}{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right]^2} = \frac{1}{n\mathbb{P}\left[D_{x,\ell}\right]} + \frac{n-1}{n}\frac{\mathbb{P}\left[D_{x,\ell}\cap D_{y,\ell}\right]}{\left(\mathbb{P}\left[D_{x,\ell}\right]\right)^2}. \tag{31}$$

From (30) and (31), we see that the zero-law will follow if we show that

$$\lim_{n\to\infty} n\mathbb{P}\left[D_{x,\ell}\right] = \infty, \tag{32}$$

and

$$\mathbb{P}\left[D_{x,\ell}\cap D_{y,\ell}\right] \sim \left(\mathbb{P}\left[D_{x,\ell}\right]\right)^2 \tag{33}$$

for some $\ell = 0, 1, \ldots, k-1$ under the enforced assumptions. The next two results will help establish (32) and (33).

Lemma 7.1. *If $\Lambda_1(n) = o\left(\frac{1}{\sqrt{n}}\right)$, then for any non-negative integer constant ℓ and any node v_x, we have*

$$\mathbb{P}\left[D_{x,\ell}\right] \sim \mu_1\left(\ell!\right)^{-1}\left(n\Lambda_1(n)\right)^\ell e^{-n\Lambda_1(n)} \tag{34}$$

Proof. Considering any class-1 node v_i, and recalling (4), we know that the events

$$E_{1i}, E_{2i}, \ldots, E_{(i-1)i}, E_{(i+1)i}, \ldots, E_{ni}$$

are mutually independent. Thus, it follows that the degree of a given node v_i, conditioned on being class-1, follows a Binomial distribution $\text{Bin}(n-1, \Lambda_1(n))$. Thus,

$$\begin{aligned}\mathbb{P}\left[D_{i,\ell}\right] &= \mu_1 \mathbb{P}\left[D_{i,\ell} \mid t_i = 1\right] \\ &= \mu_1 \binom{n-1}{\ell} \Lambda_1(n)^{\ell} \left(1-\Lambda_1(n)\right)^{n-\ell-1}\end{aligned}$$

Next, given that $\Lambda_1(n) = o\left(\frac{1}{\sqrt{n}}\right)$ and ℓ is constant, it follows that $\Lambda_1(n) = o(1)$ and $\Lambda_1(n)^2(n-\ell-1) = o(1)$. Invoking Fact 6.4, and the fact that $\binom{n-1}{\ell} \sim (\ell!)^{-1} n^{\ell}$, the conclusion (34) follows. ■

Lemma 7.2. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. The following two properties hold*

(a) If $n\Lambda_1(n) = \Omega(1)$, then for any non-negative integer constant ℓ and any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] \sim \mu_1^2 (\ell!)^{-2} (n\Lambda_1(n))^{2\ell} e^{-2n\Lambda_1(n)} \tag{35}$$

(b) For any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,0} \cap D_{y,0}\right] \sim \mu_1^2 e^{-2n\Lambda_1(n)} \tag{36}$$

Note that the events $D_{x,\ell}$ and $D_{y,\ell}$ already imply that nodes v_x and v_y are class-1, i.e., $|\Sigma_x| = |\Sigma_y| = K_1$. In this case, one may conjecture that the proof of Lemma 7.2 would precisely follow that of [17, Lemma 3] for the homogeneous case where all nodes receive the same number of keys K_1. Although the proof does follow that of [17, Lemma 3], we remark that even when we explicitly fix the class of the two particular nodes v_x and v_y, their adjacent nodes could still belong to any class. Hence, extra effort has to be made to precisely bound the probability that some vertex, say v_j, is adjacent to both v_x and v_y, as v_j could be class-i with probability μ_i (e.g., see Lemma A.7). Since the proof of Lemma 7.2 closely (although, not entirely as we mentioned above) follows that of [17, Lemma 3], it is skipped here for brevity and given in Appendix B for completeness.

We now show why the zero-law follows from Lemma 7.1 and Lemma 7.2 by means of establishing (32) and (33) for some $\ell = 0, 1, \ldots, k-1$. First, we see from (6) that $\Lambda_1(n) \leq \frac{\log n + (k-1)\log\log n}{n} = o\left(\frac{1}{\sqrt{n}}\right)$ when $\lim_{n\to\infty} \gamma_n = -\infty$. Invoking Lemma 7.1, this gives

$$n\mathbb{P}\left[D_{x,\ell}\right] \sim n\mu_1 (\ell!)^{-1} (n\Lambda_1(n))^{\ell} e^{-n\Lambda_1(n)} \tag{37}$$

for each $\ell = 0, 1, \ldots$. We will obtain (32) and (33) using subsubsequence principle [50, p. 12] and considering the cases where $n\Lambda_1(n) = \Omega(1)$ and $n\Lambda_1(n) = o(1)$ separately.

7.2.1 The case where there exists an $\epsilon > 0$ such that $n\Lambda_1(n) > \epsilon$ for all n sufficiently large

In this case we will establish (32) and (33) for $\ell = k-1$. Setting $\ell = k-1$ and substituting (6) into (37), we get

$$\begin{aligned}n\mathbb{P}\left[D_{x,\ell}\right] &\sim n\mu_1 \left[(k-1)!\right]^{-1} (n\Lambda_1(n))^{k-1} e^{-\log n - (k-1)\log\log n - \gamma_n} \\ &= \mu_1 \left[(k-1)!\right]^{-1} (\log n + (k-1)\log\log n + \gamma_n)^{k-1} e^{-(k-1)\log\log n - \gamma_n}\end{aligned} \tag{38}$$

Let

$$f_n(k;\gamma_n) := (\log n + (k-1)\log\log n + \gamma_n)^{k-1}\, e^{-(k-1)\log\log n - \gamma_n},$$

and note that $(\log n + (k-1)\log\log n + \gamma_n) \geq \epsilon$ for all n sufficiently large by virtue of the fact that $n\Lambda_1(n) > \epsilon$. Fix n sufficiently large, pick $\zeta \in (0,1)$ and consider the cases when $\gamma_n \leq -(1-\zeta)\log n$ and $\gamma_n > -(1-\zeta)\log n$, separately. In the former case, we get

$$f_n(k;\gamma_n) \geq \epsilon e^{-(k-1)\log\log n + (1-\zeta)\log n},$$

and in the latter case, we get

$$f_n(k;\gamma_n) \geq (\zeta \log n)^{k-1}\, e^{-(k-1)\log\log n - \gamma_n} = \zeta^{k-1} e^{-\gamma_n}.$$

Thus, for all n sufficiently large, we have

$$f_n(k;\gamma_n) \geq \min\left\{\epsilon e^{-(k-1)\log\log n + (1-\zeta)\log n}, \zeta^{k-1} e^{-\gamma_n}\right\}.$$

It is now clear that

$$\lim_{n\to\infty} f_n(k;\gamma_n) = \infty, \tag{39}$$

since $\zeta \in (0,1)$ and $\lim_{n\to\infty}\gamma_n = -\infty$. Reporting (39) into (38), we establish (32). Furthermore, from Lemma 7.1 and Lemma 7.2, it is clear that (33) follows for $\ell = k-1$.

7.2.2 The case where $\lim_{n\to\infty} n\Lambda_1(n) = 0$

In this case, we will establish (32) and (33) for $\ell = 0$. Setting $\ell = 0$ in (37), we obtain

$$n\mathbb{P}\left[D_{x,0}\right] \sim n\mu_1 e^{n\Lambda_1(n)} \sim n\mu_1$$

by virtue of the fact that $n\Lambda_1(n) = o(1)$. This readily gives (32). Furthermore, from Lemma 7.1 (with $\ell = 0$) and Lemma 7.2, (33) immediately follows.

The two cases considered cover all the possibilities for the limit of $n\Lambda_1(n)$. By virtue of the subsubsequence principle [50, p. 12], we get (32) and (33) without any condition on the sequence $n\Lambda_1(n)$; i.e., we obtain the zero-law even when the sequence $n\Lambda_1(n)$ does not have a limit!

8 Proof of Theorem 3.2

8.1 Establishing the zero-law

Let κ denote the the vertex connectivity of $\mathbb{H}(n,\boldsymbol{\mu},\boldsymbol{\Theta}_n)$, i.e., the minimum number of nodes to be deleted to make the graph disconnected. Also, let δ denote the minimum node degree in $\mathbb{H}(n,\boldsymbol{\mu},\boldsymbol{\Theta}_n)$. It is clear that if a random graph is k-connected, meaning that $\kappa \geq k$, then it does not have any node with degree less than k. Thus $[\kappa \geq k] \subseteq [\delta \geq k]$ and the conclusion

$$\mathbb{P}[\kappa \geq k] \leq \mathbb{P}[\delta \geq k] \tag{40}$$

immediately follows. In view of (40), we obtain the zero-law for k-connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) \text{ is } k\text{-connected}] = 0,$$

when $\lim_{n\to\infty}\gamma_n = -\infty$ from the zero-law part of Theorem 3.1. Put differently, the conditions that lead to the zero-law part of Theorem 3.1, i.e., $\lambda_1(n) = o(1)$ and $\lim_{n\to\infty}\gamma_n = -\infty$, automatically lead to the zero-law part of Theorem 3.2.

8.2 Establishing the one-law

Before we proceed with the proof of the one-law of Theorem 3.2, we take a moment to explain why the probabilistic bounds that we derive next look substantially different than those given in [17] for the homogeneous case. In establishing the zero-law of Theorem 3.1, it was sufficient to show that there exists at least one node of class-1 with degree less than k to prove that the minimum node degree is less than k with high probability. As we fixed the key ring size of the node(s) under consideration, the heterogeneity *partially* vanished, rendering our probabilistic bounds closely related to the ones given in [17], except for some cases, as discussed in Section 7.2. However, as we establish the one-law of Theorem 3.2, the heterogeneity of the key ring sizes comes into play, leading to considerably more difficult expressions and substantially different bounds than the ones given in [17] for the homogeneous case. This will become apparent in Sections 9 and 10, where we prove a key result that establishes the one-law for k-connectivity.

An important step towards establishing the one-law of Theorem 3.2 is presented in Appendix C. There, we show that it suffices to establish the one law in Theorem 3.2 under the additional condition that $\gamma_n = o(\log n)$, which leads to a number of useful consequences. Let a sequence $\beta_{\ell,n} : \mathbb{N} \times \mathbb{N}_0 \to \mathbb{R}$ be defined through the relation

$$\Lambda_1(n) = \frac{\log n + \ell \log\log n + \beta_{\ell,n}}{n} \tag{41}$$

for each $n \in \mathbb{N}_0$ and $\ell \in \mathbb{N}$. Put differently, we have

$$\beta_{\ell,n} := n\Lambda_1(n) - \log n - \ell \log\log n, \qquad \begin{matrix} n = 1, 2, \dots \\ \ell = 0, 1, \dots, \end{matrix}$$

where as in (4), $\Lambda_1(n)$ is given by

$$\Lambda_1(n) = \sum_{j=1}^{r} \mu_j \alpha_n p_{1j} = \sum_{j=1}^{r} \mu_j \alpha_n \left(1 - \frac{\binom{P_n - K_{i,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \right).$$

In view of the arguments in Appendix C, the one-law (10) follows from the next result.

Theorem 8.1. *Let ℓ be a non-negative constant integer. Under (7), (8), (9), and (41) with $\beta_{\ell,n} = o(\log n)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, we have*

$$\lim_{n\to\infty} \mathbb{P}[\kappa = \ell] = 0.$$

Before we give a formal proof, we first explain why the one-law (10) follows from Theorem 8.1. Comparing (41) with (6) and noting that $\gamma_n = o(\log n)$, we get

$$\beta_{\ell,n} = (k - 1 - \ell) \log\log n + \gamma_n = o(\log n) \tag{42}$$

Moreover, for $\ell = 0, 1, \dots, k-1$, we have

$$\lim_{n\to\infty} \beta_{\ell,n} = +\infty \tag{43}$$

by recalling the fact that $\lim_{n\to\infty}\gamma_n = +\infty$. Recalling (42) and (43), we notice that the conditions needed for Theorem 8.1 are met when $\ell = 0, 1, \ldots, k-1$; thus, we have $\mathbb{P}[\kappa = \ell] = o(1)$ for $\ell = 0, 1, \ldots, k-1$, which in turn implies that $\lim_{n\to\infty}\mathbb{P}[\kappa \geq k] = 1$, i.e., the one-law.

We now give a road map to the proof of Theorem 8.1. By a simple union bound, we get

$$\mathbb{P}[\kappa = \ell] \leq \mathbb{P}[\delta \leq \ell] + \mathbb{P}[(\kappa = \ell) \cap (\delta > \ell)].$$

It is now immediate that Theorem 8.1 is established once we show that

$$\lim_{n\to\infty}\mathbb{P}[\delta \leq \ell] = 0 \tag{44}$$

and

$$\lim_{n\to\infty}\mathbb{P}[(\kappa = \ell) \cap (\delta > \ell)] = 0 \tag{45}$$

under the enforced assumptions of Theorem 8.1. We start by establishing (44). Following the analysis of Section 7.1, it is easy to see that

$$\begin{aligned} n\mathbb{P}[D_{x,\ell}] &\leq 2^{\ell-1}\left((\log n)^{\ell}(1+o(1))^{\ell} + \beta_{\ell,n}^{\ell}\right)e^{-\ell\log\log n - \beta_{\ell,n}}e^{O(1)} \\ &= O(1)e^{-\beta_{\ell,n}} + O(1)\beta_{\ell,n}^{\ell}e^{-\ell\log\log n - \beta_{\ell,n}}, \end{aligned}$$

and it follows that $\lim_{n\to\infty} n\mathbb{P}[D_{x,\ell}] = 0$ as long as $\lim_{n\to\infty}\beta_{\ell,n} = +\infty$. From (25) and (27), this yields

$$\lim_{n\to\infty}\mathbb{P}[\delta = \ell] = 0 \quad \text{when } \lim_{n\to\infty}\beta_{\ell,n} = +\infty \tag{46}$$

However, from (41) it is easy to see that $\beta_{\ell,n}$ is monotonically decreasing in ℓ. Thus, the fact that $\lim_{n\to\infty}\beta_{\ell,n} = +\infty$ for some ℓ implies

$$\lim_{n\to\infty}\beta_{\hat{\ell},n} = +\infty, \quad \hat{\ell} = 0, 1, \ldots, \ell$$

From (46) this in turn implies that $\mathbb{P}[\delta = \hat{\ell}] = o(1)$ for $\hat{\ell} = 0, 1, \ldots, \ell$, or equivalently (44).

We now focus on establishing (45) under the enforced assumptions of Theorem 8.1. The proof is based on finding a tight upper bound on the probability $\mathbb{P}[(\kappa = \ell) \cap \delta > \ell]$ and showing that this bound goes to zero as n goes to infinity. Let $\mathcal{N}$ denote the collection of all non-empty subsets of $\{v_1, v_2, \ldots, v_n\}$. Define $\mathcal{N}_* = \{T : T \in \mathcal{N},\ |T| \geq 2\}$ and

$$\mathcal{E}(\boldsymbol{J}) = \cup_{T\in\mathcal{N}_*}\left[|\cup_{v_i\in T}\Sigma_i| \leq J_{|T|}\right]$$

where $\boldsymbol{J} = [J_2, J_3, \ldots, J_n]$ is an $(n-1)$-dimensional integer-valued array. $\mathcal{E}(\boldsymbol{J})$ encodes the event that for at least one $|T| = 2, \ldots, n$, the total number of distinct keys held by at least one set of $|T|$ sensors is less than or equal to $J_{|T|}$. Now, define

$$m_n := \min\left(\left\lfloor\frac{P_n}{K_{1,n}}\right\rfloor, \left\lfloor\frac{n}{2}\right\rfloor\right) \tag{47}$$

and let

$$J_i = \begin{cases} \max\left(\lfloor(1+\epsilon)K_{1,n}\rfloor, \lfloor i\zeta K_{1,n}\rfloor\right) & i = 2, \ldots, m_n \\ \lfloor\psi P_n\rfloor & i = m_n+1, \ldots, n \end{cases} \tag{48}$$

for some ζ, ψ in $(0,1)$ to be specified later at (49) and (50), respectively. A crude bounding argument gives

$$\mathbb{P}\left[(\kappa = \ell) \cap \delta > \ell\right] \leq \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] + \mathbb{P}\left[(\kappa = \ell) \cap \delta > \ell \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]$$

Hence, establishing (45) consists of establishing the following two results.

Proposition 8.2. *Let ℓ be a non-negative constant integer. Assume that (41) holds with $\beta_{\ell,n} > 0$, and that we have (8) and (9). Also, assume that (7) holds such that*

$$P_n \geq \sigma n$$

for some $\sigma > 0$ for all n sufficiently large. Then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] = 0,$$

where $\boldsymbol{J}$ is as defined in (48) with arbitrary $\epsilon \in (0,1)$, constant $\zeta \in (0, \frac{1}{2})$ selected small enough such that

$$\max\left(2\zeta\sigma, \zeta\left(\frac{e^2}{\sigma}\right)^{\frac{\zeta}{1-2\zeta}}\right) < 1 \tag{49}$$

and $\psi \in (0, \frac{1}{2})$ selected small enough such that

$$\max\left(2\left(\sqrt{\psi}\left(\frac{e}{\psi}\right)^{\psi}\right)^{\sigma}, \sqrt{\psi}\left(\frac{e}{\psi}\right)^{\psi}\right) < 1 \tag{50}$$

Proof. The proof follows the same steps with [9, Proposition 7.2] to show that it suffices to establish Proposition 8.2 for the homogenous case where all key rings are of the same size $K_{1,n}$. This is evident upon realizing that with $U_\ell(\boldsymbol{\mu}, \boldsymbol{\theta}) = |\cup_{i=1}^{\ell} \Sigma_i|$ and $U_\ell(K_{1,n}, P_n) =_{st} U_\ell(\boldsymbol{\mu} = \{1, 0, \ldots, 0\}, \boldsymbol{\theta})$, we have

$$U_\ell(K_{1,n}, P_n) \preceq U_\ell(\boldsymbol{\mu}, \boldsymbol{\theta}),$$

where $\preceq$ denotes the usual stochastic ordering. After this reduction, the proof reduces to [17, Proposition 3]. Results only require conditions (7), (16), and $K_{1,n} = o(P_n)$ to hold. We note that $K_{1,n} = o(P_n)$ follows from (8) and the fact that $K_{1,n} \leq K_{r,n}$. Also, (16) follows under the enforced assumptions as shown in Proposition 6.2. ■

Proposition 8.3. *Let ℓ be a non-negative constant integer. Under (7), (8), (9), and (41) with $\beta_{\ell,n} = o(\log n)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[(\kappa = \ell) \cap (\delta > \ell) \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] = 0$$

The proof of Proposition 8.3 is given in Section 9. Proposition 8.2 and Proposition 8.3 establish (45) which, combined with (44), establish Theorem 8.1. We remark that Theorem 8.1 establishes the one-law.

9 Proof of Proposition 8.3

For notation simplicity, we denote $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\alpha)$ by $\mathbb{H}$. Let $\mathbb{H}(U)$ be a subgraph of $\mathbb{H}$ restricted to the vertex set U. For any subset of nodes U, define $U^c := \{v_1,\ldots,v_n\}\setminus U$. We also let $\mathcal{N}_{U^c}$ denote the collection of all non-empty subsets of $\{v_1,v_2,\ldots,v_n\}\setminus U$. We note that a subset T of $\mathcal{N}_{U^c}$ is isolated in $\mathbb{H}(U^c)$ if there are no edges in $\mathbb{H}$ between nodes in T and nodes in $U^c\setminus T$, i.e.,

$$\overline{E_{ij}}, \quad v_i\in T, \quad v_j\in U^c\setminus T.$$

Next, we present key observations that pave the way to establishing Proposition 8.3. If $\kappa=\ell$ but $\delta>\ell$, then there exists subsets U and T of nodes with $U\in\mathcal{N}$, $|U|=\ell$, $T\in\mathcal{N}_{U^c}$, $|T|\geq 2$ such that $\mathbb{H}(T)$ is connected while T is isolated in $\mathbb{H}(U^c)$. This ensures that $\mathbb{H}$ can be disconnected by deleting a properly selected set of ℓ nodes, i.e., the set U. This would not be possible for sets $T\in\mathcal{N}_{U^c}$ with $|T|=1$ since we have $\delta\geq\ell+1$ which implies that the single node in T is connected to at least one node in $U^c\setminus T$. Finally, having $\kappa=\ell$ ensures that $\mathbb{H}$ remains connected after removing $(\ell-1)$ nodes. Then, if there exists a subset U with $|U|=\ell$ such that some $T\in\mathcal{N}_{U^c}$ is isolated in $\mathbb{H}(U^c)$, each node in U must be connected to at least one node in T and at least one node in $U^c\setminus T$. This can be proved by contradiction. Consider subsets $U\in\mathcal{N}$ with $|U|=\ell$, and $T\in\mathcal{N}_{U^c}$ with $|T|\geq 2$, such that T is isolated from $U^c\setminus T$. Suppose there exists a node $v_i\in U$ such that v_i is connected to at least one node in T but not connected to any node in $U^c\setminus T$. In this case, it is easy to see that there are no edges between nodes in $U^c\setminus T$ and nodes in $\{v_i\}\cup T$. Thus, the graph could have been made disconnected by removing nodes in $U\setminus\{v_i\}$. But $|U\setminus\{v_i\}|=\ell-1$, and this contradicts the fact that $\kappa=\ell$.

We now present several events that characterize the aforementioned observations. For each non-empty subset $T\subseteq U^c$, we define $\mathcal{C}_T$ as the event that $\mathbb{H}(T)$ is itself connected, and $\mathcal{D}_{U,T}$ as the event that T is isolated in $\mathbb{H}(U^c)$, i.e.,

$$\mathcal{D}_{U,T} := \bigcap_{\substack{v_i\in T\\ v_j\in U^c\setminus T}} \overline{E_{ij}},$$

Moreover, we define $\mathcal{B}_{U,T}$ as the event that each node in U has an edge with at least one node in T, i.e.,

$$\mathcal{B}_{U,T} := \bigcap_{v_i\in U}\bigcup_{v_j\in T} E_{ij},$$

and finally, we let $\mathcal{A}_{U,T} := \mathcal{B}_{U,T}\cap\mathcal{D}_{U,T}\cap\mathcal{C}_T$. It is clear that $\mathcal{A}_{U,T}$ encodes the event that $\mathbb{H}(T)$ is itself connected, each node in U has an edge with at least one node in T, but T is isolated in $\mathbb{H}(U^c)$. The aforementioned observations enable us to express the event $[(\kappa=\ell)\cap(\delta>\ell)]$ in terms of the event sequence $\mathcal{A}_{U,T}$. In particular, we have

$$[(\kappa=\ell)\cap(\delta>\ell)]\subseteq \bigcup_{U\in\mathcal{N}_{n,\ell},T\in\mathcal{N}_{U^c},|T|\geq 2} \mathcal{A}_{U,T}$$

with $\mathcal{N}_{n,\ell}$ denoting the collection of all subsets of $\{v_1,\ldots,v_n\}$ with exactly ℓ elements. We also note that the union need only to be taken over all subsets T with $2\leq|T|\leq\left\lfloor\frac{n-\ell}{2}\right\rfloor$. This is because if the vertices in T form a component then so do the vertices in $\mathcal{N}_{U^c}\setminus T$. Now, using a standard

union bound, we obtain

$$\mathbb{P}\left[(\kappa=\ell)\cap(\delta>\ell)\cap\overline{\mathcal{E}(\boldsymbol{J})}\right] \leq \sum_{U\in\mathcal{N}_{n,\ell},T\in\mathcal{N}_{U^c},2\leq|T|\leq\left\lfloor\frac{n-\ell}{2}\right\rfloor} \mathbb{P}\left[\mathcal{A}_{U,T}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]$$
$$= \sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor} \sum_{U\in\mathcal{N}_{n,\ell},T\in\mathcal{N}_{U^c,m}} \mathbb{P}\left[\mathcal{A}_{U,T}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]$$

where $\mathcal{N}_{U^c,m}$ denotes the collection of all subsets of U^c with exactly m elements. Now, for each $m=1,\ldots,n-\ell-1$, we simplify the notation by writing $\mathcal{A}_{\ell,m} := \mathcal{A}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, $\mathcal{D}_{\ell,m} := \mathcal{D}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, $\mathcal{B}_{\ell,m} := \mathcal{B}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, and $\mathcal{C}_m := \mathcal{C}_{\{v_{\ell+1},\ldots,v_{\ell+m}\}}$. From exchangeability, we get

$$\mathbb{P}\left[\mathcal{A}_{U,T}\right] = \mathbb{P}\left[\mathcal{A}_{\ell,m}\right], \quad U\in\mathcal{N}_{n,\ell}, \quad T\in\mathcal{N}_{U^c,m}$$

and the key bound

$$\mathbb{P}\left[(\kappa=\ell)\cap(\delta>\ell)\cap\overline{\mathcal{E}(\boldsymbol{J})}\right] \leq \sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor}\binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right] \tag{51}$$

is readily obtained upon noting that $|\mathcal{N}_{n,\ell}| = \binom{n}{\ell}$ and $|\mathcal{N}_{U^c,m}| = \binom{n-\ell}{m}$. Thus, Proposition 8.3 will be established if we show that

$$\lim_{n\to\infty}\sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor}\binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right] = 0. \tag{52}$$

We now derive bounds for the probabilities $\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]$. First, for $m=2,\ldots,n-\ell-1$, we have

$$\mathcal{D}_{\ell,m} := \bigcap_{j=m+\ell+1}^{n}\left[\left(\cup_{i\in\nu_{m,j}}\Sigma_i\right)\cap\Sigma_j=\emptyset\right] \tag{53}$$

where $\nu_{m,j}$ is defined as

$$\nu_{m,j} := \{i=\ell+1,\ldots,\ell+m : C_{ij}\}$$

for each $j=1,\ldots,\ell$ and $j=m+\ell+1,\ldots,n$. Put differently, $\nu_{m,j}$ is the set of indices in $i=\ell+1,\ldots,\ell+m$ for which nodes v_j and v_i are adjacent in the ER graph $\mathbb{G}(n;\alpha_n)$. Then, (53) follows from the fact that for v_j to be isolated from $\{v_{\ell+1},\ldots,v_{\ell+m}\}$ in $\mathbb{H}$, Σ_j needs to be disjoint from each of the key rings $\{\Sigma_i : i\in\nu_{m,j}\}$.

Now, using the law of iterated expectation, we get

$$\mathbb{P}\left[\mathcal{D}_{\ell,m}\,\middle|\,\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] = \mathbb{E}\left[\mathbf{1}\left[\mathcal{D}_{\ell,m}\right]\,\middle|\,\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]$$
$$= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{D}_{\ell,m}\right]\,\middle|\,\substack{\Sigma_{\ell+1},\ldots,\Sigma_n\\ C_{ij},i=\ell+1,\ldots,\ell+m\\ j=\ell+m+1,\ldots,n}\right]\,\middle|\,\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]$$
$$= \mathbb{E}\left[\prod_{j=\ell+m+1}^{n}\left(\frac{\binom{P-|\cup_{i\in\nu_{m,j}}\Sigma_i|}{|\Sigma_j|}}{\binom{P}{|\Sigma_j|}}\right)\,\middle|\,\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]$$

$$= \mathbb{E}\left[\frac{\binom{P-|\cup_{i\in\nu_m}\Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]^{n-\ell-m} \tag{54}$$

by independence of the random variables $\nu_{m,j}$ and $|\Sigma_j|$ for $j = \ell+m+1,\ldots,n$. Here we define ν_m and $|\Sigma|$ as generic random variables following the same distribution with any of $\{\nu_{m,j}, j = \ell+m+1,\ldots,n\}$ and $\{|\Sigma_j|, j = \ell+m+1,\ldots,n\}$, respectively. Put differently, ν_m is a Binomial rv with parameters m and α, while $|\Sigma|$ is a rv that takes the value K_j with probability μ_j.

Next, we bound the probabilities $\mathbb{P}[\mathcal{B}_{\ell,m}]$. We know that

$$\mathcal{B}_{\ell,m} := \cap_{i=1}^{\ell} \cup_{j=\ell+1}^{m} E_{ij}.$$

Thus,

$$\begin{aligned}
\mathbb{P}\left[\mathcal{B}_{\ell,m} \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] &= \mathbb{E}\left[\mathbf{1}\left[\mathcal{B}_{\ell,m}\right] \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{B}_{\ell,m}\right] \;\middle|\; \substack{\Sigma_1,\ldots,\Sigma_{\ell+m} \\ C_{ij}, i=\ell+1,\ldots,\ell+m \\ j=1,\ldots,\ell}\right] \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[\prod_{j=1}^{\ell}\left(1 - \frac{\binom{P-|\cup_{i\in\nu_{m,j}}\Sigma_i|}{|\Sigma_j|}}{\binom{P}{|\Sigma_j|}}\right) \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[1 - \frac{\binom{P-|\cup_{i\in\nu_m}\Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]^{\ell}
\end{aligned} \tag{55}$$

by independence of the random variables $\nu_{m,j}$ and $|\Sigma_j|$ for $j = 1,\ldots,\ell$.

We note that, on the event $\overline{\mathcal{E}(\boldsymbol{J})}$, we have

$$|\cup_{i\in\nu_m}\Sigma_i| \geq \left(J_{|\nu_m|}+1\right)1\left[|\nu_m|>1\right]$$

and it is always the case that $|\cup_{i\in\nu_m}\Sigma_i| \geq K_1 1\left[|\nu_m|>0\right]$ and

$$|\cup_{i\in\nu_m}\Sigma_i| \leq |\nu_m| K_r. \tag{56}$$

Next, we define

$$L(\nu_m) = \max\left(K_1 1\left[|\nu_m|>0\right], \left(J_{|\nu_m|}+1\right)1\left[|\nu_m|>1\right]\right)$$

so that on $\overline{\mathcal{E}(\boldsymbol{J})}$, we have

$$|\cup_{i\in\nu_m}\Sigma_i| \geq L(\nu_m). \tag{57}$$

Using (57) in (54) and (56) in (55), we get

$$\begin{aligned}
\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] &= \mathbb{E}\left[\mathbf{1}\left[\mathcal{C}_m\right]\mathbf{1}\left[\mathcal{B}_{\ell,m}\right]\mathbf{1}\left[\mathcal{D}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{C}_m\right]\mathbf{1}\left[\mathcal{B}_{\ell,m}\right]\mathbf{1}[\mathcal{D}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}] \;\middle|\; \substack{\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m} \\ C_{ij}, i,j=\ell+1,\ldots,\ell+m}\right]\right] \\
&\leq \mathbb{P}\left[\mathcal{C}_m\right]\mathbb{E}\left[1 - \frac{\binom{P-|\nu_m|K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]^{\ell} \mathbb{E}\left[\frac{\binom{P-L(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]^{n-\ell-m}
\end{aligned} \tag{58}$$

since $\mathcal{C}_m$ is fully determined by the rvs $\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}$ and $\{C_{ij}, i,j=\ell+1,\ldots,\ell+m\}$ while $\mathcal{B}_{\ell,m}$, $\mathcal{D}_{\ell,m}$, and $\mathcal{E}(\boldsymbol{J})$ are independent from $\{C_{ij}, i,j=\ell+1,\ldots,\ell+m\}$. Here, we also used the fact that given $\{\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\}$, $\mathcal{D}_{\ell,m}$ is independent from $\mathcal{B}_{\ell,m}$.

The following lemma provides upper bounds for (58).

Lemma 9.1. *Let $\boldsymbol{J}$ be defined as in (48) for some $\epsilon \in (0,1)$, $\zeta \in \left(0,\frac{1}{2}\right)$ such that (49) holds, $\psi \in \left(0,\frac{1}{2}\right)$ such that (50) holds. Assume that $\Lambda_1(n) = o(1)$ and (7), (8), and (9) hold. Then for all n sufficiently large, and for each $m = 2,3,\ldots,n$, we have*

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] \\
&\leq \min\left\{1, m^{m-2}\left(\alpha_n p_{rr}(n)\right)^{m-1}\right\}\left(\mathbf{1}\left[m > \left\lfloor \frac{P_n - K_{r,n}}{2K_{r,n}}\right\rfloor\right] + \mathbf{1}\left[m \leq \left\lfloor \frac{P_n - K_{r,n}}{2K_{r,n}}\right\rfloor\right]\left(1 - e^{-3m\alpha_n p_{rr}(n)}\right)^{\ell}\right)\cdot \\
&\cdot\left(\min\left\{1-\Lambda_1(n), e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}, e^{-\psi K_{1,n}}\mathbf{1}\left[m > m_n\right] + \min\left\{1-\mu_r+\mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right\}\right\}\right)^{n-m-\ell}
\end{aligned} \tag{59}$$

The proof of Lemma 9.1 is given in Appendix D. Now, the proof of Proposition 8.3 will be completed upon establishing (52) by means of Lemma 9.1. We devote Section 10 to establishing (52).

10 Establishing (52)

In this section, we make several use of the following lemma.

Lemma 10.1. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$ such that (41) holds with $\beta_{\ell,n} = o(\log n)$. We have*

$$\frac{1}{2}\frac{\log n}{n} \leq \alpha_n p_{1r}(n) \leq \frac{2}{\mu_r}\frac{\log n}{n}, \tag{60}$$

for all n sufficiently large, i.e., $\alpha_n p_{1r}(n) = \Theta\left(\frac{\log n}{n}\right)$. If in addition (9) holds, we have

$$\alpha_n p_{rr}(n) = o\left(\log n\right)\alpha_n p_{1r}(n) = o\left(\frac{(\log n)^2}{n}\right) \tag{61}$$

and

$$\alpha_n p_{1r}(n) = o\left(\log n\right)\alpha_n p_{11}(n) \tag{62}$$

The proof of Lemma 10.1 is given in Appendix E.

We now proceed with establishing (52). We start by defining $f_{n,\ell,m}$ as

$$f_{n,\ell,m} = \binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]$$

Thus, establishing (52) becomes equivalent to showing

$$\lim_{n\to\infty}\sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor} f_{n,\ell,m} = 0. \tag{63}$$

We will establish (63) in several steps with each step focusing on a specific range of the summation over m. Throughout, we consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$ such that (41) holds with $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$ and $\beta_{\ell,n} = o(\log n)$, and (7), (8), (9) hold. We will make repeated use of the bounds (22), (23), (24), and (61).

10.0.1 The case where $2 \le m \le M$

This range considers fixed values of m. Pick an integer M to be specified later at (70). We note that on this range we have $m \le \lfloor \frac{P_n - K_{r,n}}{2K_{r,n}} \rfloor$ for all n sufficiently large by virtue of (8). On the same range we also have

$$1 - e^{-3m\alpha_n p_{rr}(n)} \le 3m\alpha_n p_{rr}(n) \tag{64}$$

by virtue of (61), (20), and the fact that m is bounded.

Using (24), (59), (61), and (64), and noting that $\Lambda_1(n) = o(1)$ under (41) with $\beta_{\ell,n} = o(\log n)$, we get

$$\begin{aligned}
f_{n,\ell,m} &\le n^\ell n^m m^{m-2} \left(\alpha_n p_{rr}(n)\right)^{m-1} (3m)^\ell \left(\alpha_n p_{rr}(n)\right)^\ell e^{-\left(1+\frac{\epsilon}{2}\right)(n-m-\ell)\Lambda_1(n)} \\
&= O(1) n^{\ell+m} \left(\alpha_n p_{rr}(n)\right)^{\ell+m-1} e^{-\left(1+\frac{\epsilon}{2}\right)(n-m-\ell)\Lambda_1(n)} \\
&= o(1) n^{\ell+m} \left(\frac{(\log n)^2}{n}\right)^{\ell+m-1} e^{-\left(1+\frac{\epsilon}{2}\right)\left(\log n + \ell \log\log n + \beta_{\ell,n}\right)} \\
&= o(1) n^{-\frac{\epsilon}{2}} (\log n)^{\ell\left(1-\frac{\epsilon}{2}\right)+2(m-1)} e^{-\left(1+\frac{\epsilon}{2}\right)\beta_{\ell,n}} \\
&= o(1)
\end{aligned}$$

since ℓ is non-negative integer constant, m is bounded, and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$. This establishes

$$\lim_{n\to\infty} \sum_{m=2}^{M} f_{n,\ell,m} = 0.$$

10.0.2 The case where $M+1 \le m \le \min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}$

Our goal in this and the next subsubsection is to cover the range $M+1 \le m \le \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor$. Since the bound given at (59) takes a different form when $m > m_n$ (with m_n defined at (47)), we first consider the range $M+1 \le m \le \min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}$; we note from (8) and (5) that $\lim_{n\to\infty} m_n = \infty$.

On the range considered here, we have from (22), (24), and (59) that

$$\sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} \le \sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} n^\ell \left(\frac{en}{m}\right)^m m^{m-2} \left(\alpha_n p_{rr}(n)\right)^{m-1} \left(1 - \mu_r \left(1 - e^{-\alpha_n p_{1r}(n)\zeta m}\right)\right)^{n-m-\ell} \tag{65}$$

From the upper bound in (60) and the fact that $m \le \frac{\mu_r n}{2\zeta \log n}$ for all n sufficiently large, we have

$$\alpha_n p_{1r}(n) \zeta m \le \frac{2\log n}{\mu_r n} \zeta \frac{\mu_r n}{2\zeta \log n} = 1.$$

Using the fact that $1-e^{-x} \geq \frac{x}{2}$ for all $0 \leq x \leq 1$, we get

$$1-\mu_r\left(1-e^{-\alpha_n p_{1r}(n)\zeta m}\right) \leq 1-\frac{\mu_r \alpha_n p_{1r}(n)\zeta m}{2} \leq e^{-\zeta m \mu_r \frac{\log n}{4n}} \tag{66}$$

as we invoke the lower bound in (60). Reporting this last bound and (61) into (65), and noting that

$$n-m-\ell \geq \frac{n-\ell}{2} \geq \frac{n}{3}, \qquad m=2,3,\ldots,\left\lfloor \frac{n-\ell}{2} \right\rfloor, \tag{67}$$

we get

$$\begin{aligned}\sum_{m=M+1}^{\min\{m_n,\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor\}} f_{n,\ell,m} &\leq \sum_{m=M+1}^{\min\{m_n,\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor\}} n^{\ell+m} e^m \left(\frac{(\log n)^2}{n}\right)^{m-1} e^{-\zeta m \mu_r \log n \frac{n-m-\ell}{4n}} \\ &\leq n^{\ell+1} \sum_{m=M+1}^{\infty} \left(e\,(\log n)^2\, e^{-\zeta \frac{\mu_r}{12}\log n}\right)^m \end{aligned} \tag{68}$$

for all n sufficiently large. Given that $\zeta, \mu_r > 0$ we have

$$e\,(\log n)^2\, e^{-\zeta \frac{\mu_r}{12}\log n} = o(1). \tag{69}$$

Thus, the geometric series in (68) is summable, and we have

$$\sum_{m=M+1}^{\min\{m_n,\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor\}} f_{n,\ell,m} \leq O(1) n^{\ell+1-(M+1)\zeta\frac{\mu_r}{12}} \left(e \log n\right)^{2(M+1)}$$

and it follows that

$$\lim_{n\to\infty} \sum_{m=M+1}^{\min\{m_n,\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor\}} f_{n,\ell,m} = 0$$

for any positive integer M with

$$M > \frac{12(\ell+1)}{\zeta \mu_r}. \tag{70}$$

This choice is permissible given that $\zeta, \mu_r > 0$.

10.0.3 The case where $\min\{\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor, m_n\} < m \leq \lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor$

Clearly, this range becomes obsolete if $m_n \geq \lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor$. Thus, it suffices to consider the subsequences for which the range $m_n+1 \leq m \leq \lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor$ is non-empty. On this range, following the same arguments that lead to (65) and (68) gives

$$\sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor} f_{\ell,n,m} \leq \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n}\rfloor} n^{\ell+1} \left(e(\log n)^2\right)^m \left(1-\mu_r\left(1-e^{-\zeta m \alpha_n p_{1r}(n)}\right)+e^{-\psi K_{1,n}}\right)^{\frac{n}{3}}$$

$$\leq n^{\ell+1} \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} \left(e \left(\log n \right)^2 \right)^m \left(e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}} \right)^{\frac{n}{3}} \tag{71}$$

where in the last step we used (66) in view of $m \leq \frac{\mu_r n}{2\zeta \log n}$. Next, we write

$$\begin{aligned} e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}} &= e^{-\zeta m \mu_r \frac{\log n}{4n}} \left(1 + e^{-\psi K_{1,n} + \zeta m \mu_r \frac{\log n}{4n}} \right) \\ &\leq \exp \left\{ -\zeta m \mu_r \frac{\log n}{4n} + e^{-\psi K_{1,n} + \zeta m \mu_r \frac{\log n}{4n}} \right\} \\ &\leq \exp \left\{ -\zeta m \mu_r \frac{\log n}{4n} \left(1 - \frac{e^{-\psi K_{1,n} + \frac{\mu_r^2}{8}}}{\zeta m \mu_r \frac{\log n}{4n}} \right) \right\} \end{aligned} \tag{72}$$

where the last inequality is obtained from $m \leq \frac{\mu_r n}{2\zeta \log n}$. Using the fact that $m > m_n = \min\{\lfloor \frac{P_n}{K_{1,n}} \rfloor, \lfloor \frac{n}{2} \rfloor\}$ and that $P_n \geq \sigma n$ for some $\sigma > 0$ under (7), we have

$$\begin{aligned} \frac{e^{-\psi K_{1,n} + \frac{\mu_r^2}{8}}}{\zeta m \mu_r \frac{\log n}{4n}} &\leq \max \left\{ \frac{K_{1,n}}{P_n}, \frac{2}{n} \right\} 4n \frac{e^{-\psi K_{1,n}}}{\zeta \mu_r \log n} \cdot e^{\frac{\mu_r^2}{8}} \\ &\leq \max \left\{ \frac{4K_{1,n} e^{-\psi K_{1,n}}}{\zeta \mu_r \sigma \log n}, \frac{8 e^{-\psi K_{1,n}}}{\zeta \mu_r \log n} \right\} \cdot e^{\frac{\mu_r^2}{8}} \\ &= o(1) \end{aligned}$$

by virtue of (16) and the facts that $\zeta, \mu_r, \sigma > 0$. Reporting this into (72), we see that for for any $\varepsilon > 0$, there exists a finite integer $n^*(\varepsilon)$ such that

$$\left(e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}} \right) \leq e^{-\zeta m \mu_r \frac{\log n}{4n} (1-\varepsilon)} \tag{73}$$

for all $n \geq n^*(\varepsilon)$. Using (73) in (71), we get

$$\begin{aligned} \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{\ell,n,m} &\leq n^{\ell+1} \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} \left(e \left(\log n \right)^2 \right)^m \left(e^{-\zeta m \mu_r \frac{\log n}{4n} (1-\varepsilon)} \right)^{\frac{n}{3}} \\ &\leq n^{\ell+1} \sum_{m=m_n+1}^{\infty} \left(e \left(\log n \right)^2 e^{-\zeta \mu_r \frac{\log n}{12} (1-\varepsilon)} \right)^m \end{aligned} \tag{74}$$

Similar to (69), we have $e \left(\log n \right)^2 e^{-\zeta \mu_r \frac{\log n}{12} (1-\varepsilon)} = o(1)$ so that the sum in (74) converges. Following a similar approach to that in Section 10.0.2, we then see that

$$\sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{n,\ell,m} = O(1) n^{\ell+1-m_n \frac{\zeta \mu_r (1-\varepsilon)}{12}} (e \log n)^{2(m_n+1)} = o(1)$$

since $\lim_{n \to \infty} m_n = \infty$ under the enforced assumptions.

10.0.4 The case where $\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1 \le m \le \lfloor \nu n \rfloor$

We consider $\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1 \le m \le \lfloor \nu n \rfloor$ for some $\nu \in (0, \frac{1}{2})$ to be specified later at (76). Recalling (22), (24), (59), (60), and (67), and noting that $\binom{n}{m}$ is monotone increasing in m when $0 \le m \le \lfloor \frac{n}{2} \rfloor$, we get

$$\begin{aligned}
\sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} f_{n,\ell,m} &\le \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} n^{\ell} \binom{n}{\lfloor \nu n \rfloor} \left(1 - \mu_r + \mu_r e^{-\zeta m \alpha_n p_{1r}(n)} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&\le n^{\ell} \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\zeta \frac{\mu_r n}{2\zeta \log n} \frac{\log n}{2n}} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&\le n^{\ell} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&= n^{\ell} \left(\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right)\right)^{\frac{n}{3}} \qquad (75)
\end{aligned}$$

for all n sufficiently large.

We have $1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} < 1$ from $\mu_r > 0$ and $e^{-\psi K_{1,n}} = o(1)$ from (16). Also, it holds that $\lim_{\nu \to 0} \left(\frac{e}{\nu}\right)^{3\nu} = 1$. Thus, if we pick ν small enough to ensure that

$$\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}}\right) < 1, \qquad (76)$$

then for any $0 < \varepsilon < 1 - (e/\nu)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}}\right)$ there exists a finite integer $n^{\star}(\varepsilon)$ such that

$$\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right) \le 1 - \varepsilon, \quad \forall n \ge n^{\star}(\varepsilon).$$

Reporting this into (75), we get

$$\lim_{n \to \infty} \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} f_{n,\ell,m} = 0$$

since $\lim_{n \to \infty} n^{\ell} (1 - \varepsilon)^{n/2} = 0$ for any positive integer ℓ.

10.0.5 The case where $\lfloor \nu n \rfloor + 1 \le m \le \lfloor \frac{n-\ell}{2} \rfloor$

In this range, we use (23), (24), (59), and (67) to get

$$\begin{aligned}
\sum_{m=\lfloor \nu n \rfloor + 1}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,m} &\le n^{\ell} \sum_{m=\lfloor \nu n \rfloor + 1}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{m} \left(e^{-\zeta m \alpha_n p_{11}(n)} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&\le n^{\ell} \left(\sum_{m=\lfloor \nu n \rfloor + 1}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{m}\right) \left(e^{-\zeta \nu n \alpha_n p_{11}(n)} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}}
\end{aligned}$$

$$\leq n^{\ell}\left(8e^{-\zeta\nu n\alpha_n p_{11}(n)}+8e^{-\psi K_{1,n}}\right)^{\frac{n}{3}}$$

Noting that $\zeta,\nu,\psi>0$ and recalling (62) and the lower bound of (60), we get

$$e^{-\zeta\nu n\alpha_n p_{11}(n)}=e^{-\zeta\nu n\frac{w_n}{\log n}\alpha_n p_{1r}(n)}\leq e^{-\frac{\zeta\nu w_n}{2}}$$

for some sequence w_n satisfying $\lim_{n\to\infty}w_n=+\infty$. It is now obvious that $e^{-\zeta\nu n\alpha_n p_{11}(n)}=o(1)$. Moreover, we have $e^{-\psi K_{1,n}}=o(1)$ from (16). The conclusion

$$\lim_{n\to\infty}\sum_{m=\lfloor\nu n\rfloor+1}^{\lfloor\frac{n-\ell}{2}\rfloor}f_{n,\ell,m}=0$$

immediately follows and the proof of one-law is completed.

References

[1] R. Eletreby and O. Yağan, "Minimum node degree in inhomogeneous random key graphs with unreliable links," in *Information Theory (ISIT), 2016 IEEE International Symposium on.* IEEE, 2016, pp. 2464–2468.

[2] ——, "Secure and reliable connectivity in heterogeneous wireless sensor networks," in *Information Theory (ISIT), 2017 IEEE International Symposium on.* IEEE, 2017, pp. 2880–2884.

[3] 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.

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 8, no. 2, pp. 2–23, Second 2006.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of ACM CCS 2002*, pp. 41–47.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of IEEE S&P 2003.*

[7] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds., *Wireless Sensor Networks.* Kluwer Academic Publishers, 2004.

[8] 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.

[9] O. Yağan, "Zero-one laws for connectivity in inhomogeneous random key graphs," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4559–4574, Aug 2016.

[10] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proc. of IEEE INFOCOM 2005.*

[11] R. J. La and E. Seo, "Network connectivity with a family of group mobility models," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 504–517, March 2012.

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

[13] X. Li, P. Wan, Y. Wang, and C. Yi, "Fault tolerant deployment and topology control in wireless networks," in *Proc. of ACM MobiHoc*, 2003.

[14] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc. of the 7th International Workshop on Security Protocols*, 2000, pp. 172–194.

[15] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, pp. 11–25, October 2001.

[16] D. Dolev, "The byzantine generals strike again," 1981.

[17] J. Zhao, O. Yağan, and V. Gligor, "k-connectivity in random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3810–3836, July 2015.

[18] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009, pp. 2403–2407.

[19] ——, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2983–2999, 2012.

[20] 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.

[21] 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.

[22] M. D. Penrose *et al.*, "Connectivity of soft random geometric graphs," *The Annals of Applied Probability*, vol. 26, no. 2, pp. 986–1028, 2016.

[23] O. Yağan and A. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *Information Theory, IEEE Transactions on*, vol. 59, no. 3, pp. 1740–1760, March 2013.

[24] P. Erdős and A. Rényi, "On random graphs, I," *Publicationes Mathematicae (Debrecen)*, vol. 6, pp. 290–297, 1959.

[25] J. Zhao, O. Yağan, and V. Gligor, "On the strengths of connectivity and robustness in general random intersection graphs," in *Proc. of IEEE CDC 2014*, pp. 3661–3668.

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

[27] 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.

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

[29] R. Eletreby and O. Yağan, "Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs," in *Proc. of IEEE ISIT 2017*, June.

[30] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 3, Mar 2008.

[31] A. Mei, A. Panconesi, and J. Radhakrishnan, "Unassailable sensor networks," in *Proc. of the 4th International Conference on Security and Privacy in Communication Netowrks*, ser. SecureComm '08. New York, NY, USA: ACM, 2008.

[32] O. Yağan and A. M. Makowski, "Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?" *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, pp. 1–14, 2016.

[33] S. R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics*, vol. 309, no. 16, pp. 5130–5140, 2009.

[34] K. Rybarczyk, "Diameter, connectivity, and phase transition of the uniform random intersection graph," *Discrete Mathematics*, vol. 311, no. 17, pp. 1998–2019, 2011.

[35] ——, "Sharp threshold functions for random intersection graphs via a coupling method," *the electronic journal of combinatorics*, vol. 18, no. 1, p. P36, 2011.

[36] R. Eletreby and O. Yağan, "Connectivity of wireless sensor networks secured by heterogeneous key predistribution under an on/off channel model," *IEEE Transactions on Control of Network Systems*, 2018.

[37] A.-L. Barabási, *Network science*. Cambridge university press, 2016.

[38] E. Bullmore and O. Sporns, "Complex brain networks: graph theoretical analysis of structural and functional systems," *Nature Reviews Neuroscience*, vol. 10, no. 3, p. 186, 2009.

[39] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[40] V. Colizza, A. Barrat, M. Barthélemy, and A. Vespignani, "The role of the airline transportation network in the prediction and predictability of global epidemics," *Proceedings of the National Academy of Sciences*, vol. 103, no. 7, pp. 2015–2020, 2006.

[41] F. Vega-Redondo, *Complex social networks*. Cambridge University Press, 2007, no. 44.

[42] O. Yağan, D. Qian, J. Zhang, and D. Cochran, "Conjoining speeds up information diffusion in overlaying social-physical networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1038–1048, June 2013.

[43] E. Bakshy, I. Rosenn, C. Marlow, and L. Adamic, "The role of social networks in information diffusion," in *Proc. of WWW 2012*. New York, NY, USA: ACM, pp. 519–528.

[44] S. Eubank, H. Guclu, V. Anil Kumar, M. V. Marathe, and e. al, "Modeling disease outbreaks in realistic urban social networks," *Nature*, vol. 429, no. 6988, pp. 180–4, May 13 2004.

[45] M. E. J. Newman, "Spread of epidemic disease on networks," *Phys. Rev. E*, vol. 66, p. 016128, Jul 2002.

[46] J. Zhao, O. Yağan, and V. Gligor, "On connectivity and robustness in random intersection graphs," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2121–2136, May 2017.

[47] O. Yağan and A. M. Makowski, "Counting triangles, tunable clustering and the small-world property in random key graphs (Extended version)," *ArXiv e-prints*, Jan. 2017.

[48] D. J. Watts and S. H. Strogatz, "Collective dynamics of'small-world'networks," *nature*, vol. 393, no. 6684, p. 440, 1998.

[49] M. Deijfen and W. Kets, "Random intersection graphs with tunable degree distribution and clustering," *Probability in the Engineering and Informational Sciences*, vol. 23, no. 4, p. 661674, 2009.

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

[51] 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.

Appendices

A Additional Preliminaries

Proposition A.1 ([9, Proposition 4.4])**.** *For any set of positive integers $K_1, \ldots, K_r, P$ and any scalar $a \geq 1$, we have*

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

Proposition A.2. *Consider a random variable Z defined as*

$$Z = 1 - p_{1i} = \frac{\binom{P-K_1}{K_i}}{\binom{P}{K_i}}, \quad \text{with probability } \mu_i, \quad i = 1, \ldots, r.$$

We have $var[Z] \leq \frac{1}{4} (p_{1r})^2$.

Proof. Recalling (14), we see that p_{ij} increases with both i and j, and it follows that

$$1 - p_{1r} \leq Z \leq 1 - p_{11},$$

From Popoviciu's inequality [51, pp. 9], we see that

$$\text{var}[Z] \leq \frac{1}{4} (Z_{\max} - Z_{\min})^2 = \frac{1}{4} (p_{1r} - p_{11})^2 \leq \frac{1}{4} (p_{1r})^2$$

since $p_{1r} \geq p_{11} \geq 0$. ■

Fact A.3. *If $\lambda_1(n) = o(1)$, then*

$$p_{1i}(n) = o(1), \quad i = 1, \ldots, r$$

Proof. Recalling (3), we obtain

$$p_{1i}(n) \leq \left(\frac{1}{\mu_i} \right) \lambda_1(n) = O(\lambda_1(n)) = o(1)$$

under the given assumption that $\lambda_1(n) = o(1)$. ■

Fact A.4. *For $0 \leq x \leq 1$, the following properties hold.*
(a) [17, Fact 2] If $0 < y < 1$, then $(1-x)^y \leq 1 - xy$.
(b) Let $a > 1$. Then, $1 - x^a \leq a(1-x)$.

Proof. By a crude bounding, we have

$$1 - x^a = \int_x^1 a t^{a-1} \, dt \leq \int_x^1 a \, dt = a(1-x).$$

■

Fact A.5 ([17, Fact 5])**.** *Let a, x, and y be positive integers satisfying $y \geq (2a+1)x$. Then,*

$$\frac{\binom{y-ax}{x}}{\binom{y}{x}} \geq \left[\frac{\binom{y-x}{x}}{\binom{y}{x}}\right]^{2a}$$

Fact A.6. *Let $x \in (0,1)$ and $a > 1$. Then,*

$$1 - x^a \leq a(1-x)$$

Lemma A.7. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (5) holds, a scaling $\alpha : \mathbb{N}_0 \to (0,1)$, and $\Lambda_1(n) = \frac{\log n + (k-1)\log\log n + \gamma_n}{n}$. The following properties hold for any three distinct nodes v_x, v_y, and v_j.*

(a) We have

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}, t_x = 1, t_y = 1\right] \leq \left(1 + \frac{1}{4\mu_r^2}\right)\lambda_1(n)^2 \tag{A.2}$$

(b) If $\lambda_1(n) = o(1)$, then for any $u = 0, 1, \ldots, K_{1,n}$, we have

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u), t_x = 1, t_y = 1\right] = \frac{u}{K_{1,n}}\lambda_1(n) \pm O\left((\lambda_1(n))^2\right),$$

and

$$\mathbb{P}\left[E_{xj \cup yj} \mid (|S_{xy}| = u), t_x = 1, t_y = 1\right] = 2\Lambda_1(n) - \frac{\alpha_n u}{K_{1,n}}\Lambda_1(n) \pm O\left((\Lambda_1(n))^2\right) \tag{A.3}$$

Proof. We know that

$$\begin{aligned}
&\mathbb{P}\left[(K_{xj} \cap K_{yj}) \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] \\
&= 1 - \mathbb{P}\left[\left(\overline{K_{xj}} \cup \overline{K_{yj}}\right) \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] \\
&= 1 - \mathbb{P}\left[\overline{K_{xj}} \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] - \mathbb{P}\left[\overline{K_{yj}} \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] + \\
&\quad \mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right]
\end{aligned} \tag{A.4}$$

It is easy to see that

$$\begin{aligned}
\mathbb{P}\left[\overline{K_{xj}} \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] &= \mathbb{P}\left[\overline{K_{xj}} \;\middle|\; t_x = 1\right] \\
&= \sum_{i=1}^{r} \mu_i \left(1 - p_{1i}(n)\right)
\end{aligned}$$

$$= 1 - \lambda_1(n) \tag{A.5}$$

Similarly, it is easy to see that

$$\mathbb{P}\left[\overline{K_{yj}} \;\middle|\; (|S_{xy}| = u), t_x = 1, t_y = 1\right] = 1 - \lambda_1(n) \tag{A.6}$$

Next, by recalling (A.1), we observe that

$$\begin{aligned}
\mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \;\middle|\; \overline{K_{xy}}, t_x = 1, t_y = 1\right] &= \mathbb{P}\left[\Sigma_j \in \mathcal{P} \setminus \{\Sigma_x \cup \Sigma_y\} \;\middle|\; t_x = 1, t_y = 1\right] \\
&= \sum_{i=1}^{r} \mu_i \frac{\binom{P_n - 2K_{1,n}}{K_{i,n}}}{\binom{P_n}{K_{i,n}}} \\
&\leq \sum_{i=1}^{r} \mu_i \left(\frac{\binom{P_n - K_{1,n}}{K_{i,n}}}{\binom{P_n}{K_{i,n}}}\right)^2 \\
&= \mathbb{E}\left[Z_n\left(\boldsymbol{\mu}, \boldsymbol{\theta}_n\right)^2\right] \\
&= \left(\mathbb{E}\left[Z_n\left(\boldsymbol{\mu}, \boldsymbol{\theta}_n\right)\right]\right)^2 + \operatorname{var}\left[Z_n\left(\boldsymbol{\mu}, \boldsymbol{\theta}_n\right)\right]
\end{aligned} \tag{A.7}$$

where $Z_n\left(\boldsymbol{\mu}, \boldsymbol{\theta}_n\right)$ is a rv that takes the value $1 - p_{1i}(n)$ with probability μ_i for $i = 1, \ldots, r$. Note that

$$\mathbb{E}\left[Z_n\left(\boldsymbol{\mu}, \boldsymbol{\theta}_n\right)\right] = \sum_{i=1}^{r} \mu_i \left(1 - p_{1i}\right) = 1 - \lambda_1(n), \tag{A.8}$$

and

$$\lambda_1(n) = \sum_{i=1}^{r} \mu_i p_{1i}(n) \geq \mu_r p_{1r} \tag{A.9}$$

for positive $\boldsymbol{\mu}$. Recalling Proposition A.2, and using (A.8) and (A.9) in (A.7), we get

$$\begin{aligned}
\mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \;\middle|\; \overline{K_{xy}}, t_x = 1, t_y = 1\right] &\leq \left(1 - \lambda_1(n)\right)^2 + \frac{1}{4}\frac{\lambda_1(n)^2}{\mu_r^2} \\
&= 1 - 2\lambda_1(n) + \lambda_1(n)^2\left(1 + \frac{1}{4\mu_r^2}\right)
\end{aligned} \tag{A.10}$$

The desired conclusion (A.2) follows from (A.4) in view of (A.5), (A.6), and (A.10). ■

Proof of part (b) of the lemma is very similar to that of [17, Lemma 9], and therefore is skipped here for brevity.

Lemma A.8. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (5) holds, a scaling $\alpha : \mathbb{N}_0 \to (0, 1)$, $\Lambda_1(n) = \frac{\log n + (k-1)\log\log n + \gamma_n}{n}$, with $\lim_{n\to\infty} \gamma_n = -\infty$. Let m_1, m_2, and m_3 be non-negative integer constants. We define event $\mathcal{F}$ as follows.*

$$\mathcal{F} := \left[|N_{xy}| = m_1\right] \cap \left[|N_{x\overline{y}}| = m_2\right] \cap \left[|N_{\overline{x}y}| = m_3\right]. \tag{A.11}$$

Then, given u in $\{0,1,\ldots,K_{1,n}\}$ and $\Lambda_1(n)=o(\frac{1}{\sqrt{n}})$ under $\lim_{n\to\infty}\gamma_n=-\infty$, we have

$$\begin{aligned}\mathbb{P}\left[\mathcal{F}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\sim{}&\frac{n^{m_1+m_2+m_3}}{m_1!\,m_2!\,m_3!}e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)}\cdot\\&\cdot\left(\mathbb{P}\left[E_{xj\cap yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^{m_1}\\&\cdot\left(\mathbb{P}\left[E_{xj\cap\overline{yj}}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^{m_2}\\&\cdot\left(\mathbb{P}\left[E_{\overline{xj}\cap yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^{m_3}\end{aligned}$$

with j distinct from x and y.

Proof. The proof of Lemma A.8 is very similar with [17, Lemma 4]; in fact, it would follow directly from [17, Eq. (212)-(213)] if we show that

$$\left(\mathbb{P}\left[E_{\overline{xj}\cap\overline{yj}}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^{n-m_1-m_2-m_3-2}\sim e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)}.\tag{A.12}$$

Recalling Lemma A.7 and the fact that $\Lambda_1(n)\le\frac{\log n+(k-1)\log\log n}{n}$ for all n sufficiently large under $\lim_{n\to\infty}\gamma_n=-\infty$, we get

$$\begin{aligned}&\mathbb{P}\left[E_{\overline{xj}\cap\overline{yj}}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\\&=1-\mathbb{P}\Big[E_{xj\cup yj}\;\Big|\;(|S_{xy}|=u),t_x=1,t_y=1\Big]&\text{(A.13)}\\&=1-\left(2\Lambda_1(n)-\frac{\alpha_n u}{K_{1,n}}\Lambda_1(n)\pm O\left((\Lambda_1(n))^2\right)\right)\\&=1-O\left(\frac{\log n}{n}\right)=1-o(1).&\text{(A.14)}\end{aligned}$$

Also,

$$\begin{aligned}&(n-m_1-m_2-m_3-2)\left(\mathbb{P}\left[E_{xj\cup yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^2\\&\quad=(n-m_1-m_2-m_3-2)\left[O\left(\frac{\log n}{n}\right)\right]^2=o(1)&\text{(A.15)}\end{aligned}$$

Invoking Fact 6.4 for (A.13), and using (A.14) and (A.15), we get

$$\begin{aligned}\left(\mathbb{P}\left[E_{\overline{xj}\cap\overline{yj}}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right)^{n-m_1-m_2-m_3-2}&\sim e^{(n-m_1-m_2-m_3)\mathbb{P}\left[E_{xj\cup yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]}\\&\sim e^{-n\left[2\Lambda_1(n)-\frac{\alpha_n u}{K_{1,n}}\Lambda_1(n)\pm o\left(\frac{1}{n}\right)\right]}e^{(m_1+m_2+m_3+2)o(1)}\\&\sim e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)}.&\text{(A.16)}\end{aligned}$$

This gives (A.12) and Lemma A.8 is established in view of [17, Lemma 4]. ∎

Lemma A.9 ([17, Lemma 10])**.** *If $P_n \geq 2K_{1,n}$, we have*

$$\mathbb{P}\left[|S_{xy}|= u \,\middle|\, t_x = 1, t_y = 1\right] \leq \frac{1}{u!}\left(\frac{K_{1,n}^2}{P_n - K_{1,n}}\right)^u$$

Lemma A.10. *With $m \geq 2$ and $\Lambda_1(n) = o(1)$, we have*

$$\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)},$$

for all n sufficiently large and any $\epsilon \in (0,1)$, where we define

$$Q(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m|= 1\right] + \left(\lfloor(1+\epsilon)\,K_{1,n}\rfloor + 1\right)\mathbf{1}\left[|\nu_m|> 1\right].$$

Proof. Consider fixed $\boldsymbol{K}, P$. We have

$$Q(\nu_m) \geq K_1\left(\mathbf{1}\left[|\nu_m|= 1\right] + (1+\epsilon)\mathbf{1}\left[|\nu_m|> 1\right]\right)$$

Thus, by recalling (A.1), we get

$$\begin{aligned}\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \mathbb{E}\left[\frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}^{\mathbf{1}[|\nu_m|=1]+(1+\epsilon)\mathbf{1}[|\nu_m|>1]}\right] \\ &= \mathbb{E}\left[Z^{\mathbf{1}[|\nu_m|=1]+(1+\epsilon)\mathbf{1}[|\nu_m|>1]}\right]\end{aligned}$$

where $Z = \frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}$. Taking the expectation over $|\nu_m|$, we get

$$\begin{aligned}\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \mathbb{E}\Big[(1-\alpha)^m + m\alpha\,(1-\alpha)^{m-1}\,Z + \Big(1-(1-\alpha)^m - m\alpha\,(1-\alpha)^{m-1}\Big)\,Z^{1+\epsilon}\Big] \\ &\leq \mathbb{E}\Big[(1-\alpha)^2 + 2\alpha\,(1-\alpha)\,Z + \Big(1-(1-\alpha)^2 - 2\alpha\,(1-\alpha)\Big)\,Z^{1+\epsilon}\Big] \\ &= (1-\alpha)^2 + 2\alpha\,(1-\alpha)\,\mathbb{E}[Z] + \alpha^2\mathbb{E}\left[Z^{1+\epsilon}\right]\end{aligned}$$

by virtue of the fact that

$$(1-\alpha)^m + m\alpha\,(1-\alpha)^{m-1}\,T + \Big(1-(1-\alpha)^m - m\alpha\,(1-\alpha)^{m-1}\Big)\,T^{1+\epsilon}$$

is monotonically decreasing in m (see [17, Lemma 12]).

Next, we have

$$\mathbb{E}\left[Z\right] = \sum_{j=1}^{r}\mu_j\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} = 1-\lambda_1$$

Also by recalling Fact A.4, we get

$$\begin{aligned}
\mathbb{E}\left[Z^{1+\epsilon}\right] &= \mathbb{E}\left[\left(\frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right)^{1+\epsilon}\right] \\
&= \sum_{j=1}^{r} \mu_j \left(\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}}\right)^{1+\epsilon} \\
&= \sum_{j=1}^{r} \mu_j (1-p_{1j})(1-p_{1j})^{\epsilon} \\
&\leq \sum_{j=1}^{r} \mu_j (1-p_{1j})(1-\epsilon p_{1j}) \\
&= 1-\lambda_1(1+\epsilon)+\epsilon\sum_{j=1}^{r}\mu_j p_{1j}^2.
\end{aligned}$$

Note that

$$\sum_{j=1}^{r} \mu_j \left(1-p_{1j}\right)^2 = 1-2\lambda_1+\sum_{j=1}^{r}\mu_j p_{1j}^2$$

and we have from (A.7) and (A.10) that

$$\sum_{j=1}^{r} \mu_j \left(1-p_{1j}\right)^2 \leq 1-2\lambda_1+\lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)$$

This gives

$$\sum_{j=1}^{r}\mu_j p_{1j}^2 \leq \lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)$$

and we get

$$\begin{aligned}
\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq (1-\alpha)^2+2\alpha(1-\alpha)(1-\lambda_1)+\alpha^2\left(1-\lambda_1(1+\epsilon)+\epsilon\lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)\right) \\
&= 1-\Lambda_1\left(2-(1-\epsilon)\alpha-\epsilon\left(1+\frac{1}{4\mu_r^2}\right)\Lambda_1\right)
\end{aligned}$$

Now, consider a scaling such that $\Lambda_1(n)=o(1)$. We have $\Lambda_1(n)\leq\frac{4\mu_r^2}{2(4\mu_r^2+1)}$ for all n sufficiently large. Given also that $\alpha_n\leq 1$, we get

$$\mathbb{E}\left[\frac{\binom{P_n-Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq 1-\Lambda_1\left(2-(1-\epsilon)-\frac{\epsilon}{2}\right) \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}$$

for all n sufficiently large. This completes the proof. ■

B Proof of Lemma 7.2

The law of total probability gives

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] = \mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] + \mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}\right]. \tag{B.1}$$

Thus, Lemma 7.2 will be established upon showing the next two results.

Proposition B.1. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. The following hold*

(a) If $n\Lambda_1(n) = \Omega(1)$, then for any non-negative integer constant ℓ and any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] \sim \mu_1^2 \left(\ell!\right)^{-2} \left(n\Lambda_1(n)\right)^{2\ell} e^{-2n\Lambda_1(n)} \tag{B.2}$$

(b) For any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,0} \cap D_{y,0} \cap \overline{E_{xy}}\right] \sim \mu_1^2 e^{-2n\Lambda_1(n)} \tag{B.3}$$

Proposition B.2. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. If $n\Lambda_1(n) = \Omega(1)$, then for any non-negative integer ℓ and any distinct nodes v_x and v_y, we have*

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}\right] = o\left(\mathbb{P}\left[D_{x,\ell} \cap \mathcal{D}_{y,\ell} \cap \overline{E_{xy}}\right]\right) \tag{B.4}$$

We establish Propositions B.1 and B.2 in the following two subsections respectively. Next, we show why Lemma 7.2 follows from Propositions B.1 and B.2. If $n\Lambda_1(n) = \Omega(1)$, then for any non-negative integer constant ℓ, we observe that (35) follows from (B.2) and (B.4) in view of (B.1). Now, considering the case when $\ell = 0$, we see that (B.3) directly implies (36) by virtue of (B.1) and the fact that $\mathbb{P}\left[D_{x,0} \cap D_{y,0} \cap E_{xy}\right] = 0$ since it is impossible for nodes v_x and v_y to be adjacent to each other (i.e., under E_{xy}) when both nodes have zero degree.

B.1 Proof of Proposition B.1

Consider the vertex set $\mathcal{V} = \{v_1, \ldots, v_n\}$. For each node $v_i \in \mathcal{V}$, we define N_i as the set of neighbors of node v_i. Also, for any pair of vertices v_x, v_y, we let N_{xy} be the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are neighbors of both v_x and v_y; i.e., $N_{xy} = N_x \cap N_y$. We also let $N_{x\overline{y}}$ denote the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are neighbors of v_x, but are not neighbors of v_y. Similarly, $N_{\overline{x}y}$ is defined as the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are not neighbors of v_x, but are neighbors of v_y. Finally, $N_{\overline{xy}}$ is the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are not connected to either v_x or v_y. We also define $S_{xy} = \Sigma_x \cap \Sigma_y$.

We start by defining the series of events A_h as follows

$$A_h := \left[|N_{xy}| = h\right] \cap \left[|N_{x\overline{y}}| = \ell - h\right] \cap \left[|N_{\overline{x}y}| = \ell - h\right].$$

It is simple to see that

$$D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}} = \bigcup_{h=0}^{\ell} \left(A_h \cap \overline{E_{xy}} \cap [t_x = 1] \cap [t_y = 1]\right),$$

whence we get

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] = \sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{E_{xy}} \cap [t_x = 1] \cap [t_y = 1]\right] \tag{B.5}$$

since the events $\{A_h, h = 0, \ldots, \ell\}$ are mutually exclusive.

Furthermore, since $\overline{E_{xy}} = \overline{K_{xy}} \cup \overline{C_{xy}} = \overline{K_{xy}} \cup \left(K_{xy} \cap \overline{C_{xy}}\right)$ and

$$K_{xy} \cap [t_x = 1] \cap [t_y = 1] = \cup_{u=1}^{K_{1,n}} (|S_{xy}| = u)$$

we have under $t_x = t_y = 1$ that

$$\begin{aligned} \overline{E_{xy}} &= \overline{K_{xy}} \cup \left\{ \left[\bigcup_{u=1}^{K_{1,n}} (|S_{xy}| = u) \right] \cap \overline{C_{xy}} \right\} \\ &= \overline{K_{xy}} \cup \left(\bigcup_{u=1}^{K_{1,n}} \mathcal{X}_u \right) \end{aligned} \tag{B.6}$$

where we define the event $\mathcal{X}_u$ as

$$\mathcal{X}_u = (|S_{xy}| = u) \cap \overline{C_{xy}}, \quad u = 1, \ldots, K_{1,n} \tag{B.7}$$

Now, we get

$$\mathbb{P}\left[A_h \cap \overline{E_{xy}} \cap [t_x = 1] \cap [t_y = 1]\right] = \mathbb{P}\left[A_h \cap \overline{K_{xy}} \cap [t_x = 1] \cap [t_y = 1]\right] + \sum_{u=1}^{K_{1,n}} \mathbb{P}\left[A_h \cap \mathcal{X}_u \cap [t_x = 1] \cap [t_y = 1]\right], \tag{B.8}$$

by virtue of (B.6) and the fact that the events $\overline{K_{xy}}, \mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_{K_{1,n}}$ are mutually disjoint. Combining (B.5) and (B.8) we obtain

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] = \mu_1^2 \sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right] + \mu_1^2 \sum_{h=0}^{\ell} \sum_{u=1}^{K_{1,n}} \mathbb{P}\left[A_h \cap \mathcal{X}_u \,\middle|\, t_x = 1, t_y = 1\right]. \tag{B.9}$$

Proposition B.1 is established by virtue of (B.9) and the following two results.

Proposition B.3. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. Then for any non-negative integer ℓ, we have*

$$\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \mid t_x = t_y = 1\right] \sim (\ell!)^{-2} (n\Lambda_1(n))^{2\ell} e^{-2n\Lambda_1(n)} \tag{B.10}$$

Proposition B.4. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. If $n\Lambda_1(n) = \Omega(1)$, then*

$$\sum_{h=0}^{\ell} \sum_{u=1}^{K_{1,n}} \mathbb{P}\left[A_h \cap \mathcal{X}_u \,\middle|\, t_x = 1, t_y = 1\right] = o\left(\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right] \right) \tag{B.11}$$

for any $\ell = 0, 1, \ldots$. Furthermore, we have (B.11) for $\ell = 0$ without requiring the condition $n\Lambda_1(n) = \Omega(1)$.

Before we prove Propositions B.3 and B.4, we explain why Proposition B.1 follows from these two results. Combining (B.10) and (B.11) we establish (B.2) in view of (B.9). Furthermore, by using (B.10) and (B.11) with $\ell = 0$, we readily obtain (B.3) in view of (B.9). This establishes Proposition B.1.

B.1.1 Proof for Proposition B.3

We write

$$\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right] = \sum_{h=0}^{\ell} \mathbb{P}\left[A_h \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \mathbb{P}\left[\overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right],$$

where

$$\mathbb{P}\left[\overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right] = 1 - p_{11}(n) \sim 1 \tag{B.12}$$

under the assumption $\lambda_1(n) = o(1)$ and Fact A.3. Also, using Lemma A.8 with $u = 0$, $m_1 = h$, and $m_2 = m_3 = \ell - h$, we see that

$$\begin{aligned}
\mathbb{P}\left[A_h \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \sim{}& \frac{n^{2\ell-h}}{h!\left((\ell-h)!\right)^2} e^{-2n\Lambda_1(n)} \cdot \\
& \cdot \left(\mathbb{P}\left[E_{xj\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]\right)^h \\
& \cdot \left(\mathbb{P}\left[E_{xj\cap\overline{yj}} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]\right)^{\ell-h} \\
& \cdot \left(\mathbb{P}\left[E_{\overline{xj}\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]\right)^{\ell-h}.
\end{aligned} \tag{B.13}$$

Next, we evaluate the three probability terms appearing in (B.13). We know that

$$\begin{aligned}
\mathbb{P}\left[E_{xj\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] &= \mathbb{P}\left[C_{xj} \cap C_{yj}\right] \cdot \mathbb{P}\left[K_{xj} \cap K_{yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \\
&= \alpha_n^2 \mathbb{P}\left[K_{xj} \cap K_{yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \\
&\leq \left(1 + \frac{1}{4\mu_r^2}\right) \Lambda_1(n)^2
\end{aligned} \tag{B.14}$$

by virtue of Lemma A.7. We also see that

$$\begin{aligned}
\mathbb{P}\left[E_{xj\cap\overline{yj}} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] &= \mathbb{P}\left[E_{xj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] - \mathbb{P}\left[E_{xj\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \\
&= \mathbb{P}\left[E_{xj} \,\middle|\, t_x = 1\right] - \mathbb{P}\left[E_{xj\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \\
&= \Lambda_1(n) - O\left(\Lambda_1(n)^2\right) \\
&\sim \Lambda_1(n)
\end{aligned} \tag{B.15}$$

as we invoke (B.14) and use the fact that $\Lambda_1(n) = o(1)$ under $\lim_{n\to\infty} \gamma_n = -\infty$. It is also easy to see that

$$\mathbb{P}\left[E_{\overline{xj}\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \sim \Lambda_1(n) \tag{B.16}$$

via similar arguments.

For $h = 1, 2, \ldots, \ell$, we observe from (B.13), (B.14), (B.15), and (B.16) that

$$\begin{aligned}
\frac{\mathbb{P}\left[A_h \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]}{\mathbb{P}\left[A_0 \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]} &\sim \frac{n^{-h}\,(\ell!\,)^2}{h!\,((\ell-h)!\,)^2}\left(\frac{\mathbb{P}\left[E_{xj\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]}{\mathbb{P}\left[E_{xj\cap \overline{yj}} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]}\cdot\right. \\
&\left.\cdot\,\frac{1}{\mathbb{P}\left[E_{\overline{xj}\cap yj} \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right]}\right)^h \\
&\leq \frac{n^{-h}\,(\ell!\,)^2}{h!\,((\ell-h)!\,)^2}\left(\frac{\left(1+\frac{1}{4\mu_r^2}\right)\Lambda_1(n)^2}{\Lambda_1(n)^2(1-o(1))}\right)^h \\
&= o(1) \qquad \text{(B.17)}
\end{aligned}$$

Similarly, setting $h = 0$, we obtain

$$\mathbb{P}\left[A_0 \,\middle|\, \overline{K_{xy}}, t_x = 1, t_y = 1\right] \sim (\ell!\,)^{-2}\,(n\Lambda_1(n))^{2\ell}\,e^{-2n\Lambda_1(n)} \qquad \text{(B.18)}$$

The conclusion (B.10) follows by combining (B.12), (B.17), (B.18), and noting that ℓ is constant.

B.1.2 Proof of Proposition B.4

Our approach is to find an upper bound to the left hand side of (B.11) and show that this upper bound is $o\left(\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \cap \overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right]\right)$. It will be clear that the condition $n\Lambda_1(n) = \Omega(1)$ needed to establish (B.11) is not needed for the case when $\ell = 0$.

We know that

$$\begin{aligned}
\mathbb{P}\left[A_h \cap \mathcal{X}_u \,\middle|\, t_x = 1, t_y = 1\right] &= \mathbb{P}\left[A_h \cap |S_{xy}| = u \cap \overline{C_{xy}} \,\middle|\, t_x = 1, t_y = 1\right] \\
&\leq \mathbb{P}\left[A_h \cap |S_{xy}| = u \,\middle|\, t_x = 1, t_y = 1\right]
\end{aligned}$$

Thus,

$$\begin{aligned}
\sum_{h=0}^{\ell}\sum_{u=1}^{K_{1,n}}\mathbb{P}\left[A_h \cap \mathcal{X}_u \,\middle|\, t_x = 1, t_y = 1\right] &\leq \sum_{h=0}^{\ell}\sum_{u=1}^{K_{1,n}}\mathbb{P}\left[A_h \cap |S_{xy}| = u \,\middle|\, t_x = 1, t_y = 1\right] \\
&= \sum_{u=1}^{K_{1,n}}\mathbb{P}\left[|S_{xy}| = u \,\middle|\, t_x = 1, t_y = 1\right]\cdot \\
&\quad\cdot\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \,\middle|\, (|S_{xy}| = u), t_x = 1, t_y = 1\right]
\end{aligned}$$

Now, since $E_{xj} = C_{xj} \cap K_{xj}$ and $E_{yj} = C_{yj} \cap K_{yj}$, it is clear that E_{xj} and E_{yj} are each independent of the event $|S_{xy}| = u$. It follows that

$$\mathbb{P}\left[E_{xj\cap yj} \,\middle|\, (|S_{xy}| = u), t_x = 1, t_y = 1\right] \leq \mathbb{P}\left[E_{xj} \,\middle|\, (|S_{xy}| = u), t_x = 1, t_y = 1\right]$$

$$= \Lambda_1(n). \tag{B.19}$$

Similarly, we have

$$\mathbb{P}\left[E_{xj\cap\overline{yj}} \;\middle|\; (|S_{xy}|= u), t_x = 1, t_y = 1\right] \leq \Lambda_1(n) \tag{B.20}$$

and

$$\mathbb{P}\left[E_{\overline{xj}\cap yj} \;\middle|\; (|S_{xy}|= u), t_x = 1, t_y = 1\right] \leq \Lambda_1(n) \tag{B.21}$$

Now, using Lemma A.8 with $m_1 = h$, and $m_2 = m_3 = \ell - h$, (B.19), (B.20), and (B.21), it follows that

$$\mathbb{P}\left[A_h \;\middle|\; (|S_{xy}|= u), t_x = 1, t_y = 1\right] \leq 2n^{2\ell-h} e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)} (\Lambda_1(n))^{2\ell-h}$$

for all n sufficiently large. Thus, we get

$$\sum_{h=0}^{\ell}\sum_{u=1}^{K_{1,n}} \mathbb{P}\left[A_h \cap \mathcal{X}_u \;\middle|\; t_x = 1, t_y = 1\right] \leq \sum_{u=1}^{K_{1,n}} \left(\mathbb{P}\left[|S_{xy}|= u \;\middle|\; t_x = 1, t_y = 1\right] 2e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)} \cdot \cdot \sum_{h=0}^{\ell} (n\Lambda_1(n))^{2\ell-h} \right) \tag{B.22}$$

Now, if $n\Lambda_1(n) = \Omega(1)$ it follows that

$$\sum_{h=0}^{\ell} (n\Lambda_1(n))^{2\ell-h} = O\left((n\Lambda_1(n))^{2\ell}\right). \tag{B.23}$$

Note that (B.23) follows trivially for $\ell = 0$ with no condition on $n\Lambda_1(n)$. Combining (B.22), (B.23) and Lemma A.9, we get

$$\sum_{h=0}^{\ell}\sum_{u=1}^{K_{1,n}} \mathbb{P}\left[A_h \cap \mathcal{X}_u \;\middle|\; t_x = 1, t_y = 1\right] \leq O\left((n\Lambda_1(n))^{2\ell} e^{-2n\Lambda_1(n)}\right) \sum_{u=1}^{K_{1,n}} \left(\frac{K_{1,n}^2}{P_n - K_{1,n}} e^{\frac{\alpha_n}{K_{1,n}}n\Lambda_1(n)}\right)^u \tag{B.24}$$

In view of Proposition B.3 (and the fact that ℓ is constant), we will immediately establish the desired result (B.11) from (B.24) if we show that

$$\frac{K_{1,n}^2}{P_n - K_{1,n}} e^{\frac{\alpha_n}{K_{1,n}}n\Lambda_1(n)} = o(1). \tag{B.25}$$

Next, we establish (B.25). From (5), we get for all n sufficiently large that

$$\frac{K_{1,n}^2}{P_n - K_{1,n}} \leq 2\frac{K_{1,n}^2}{P_n} \leq 4p_{11}(n)$$

where the last bound used the fact that $\frac{K_{1,n}^2}{P_n} \sim p_{11}(n)$ when $p_{11}(n) = o(1)$ (e.g., see [9, Lemma 4.2]); this in turn follows from the assumption that $\lambda_1(n) = o(1)$ in view of Fact A.3. It is also clear from the definition $\lambda_1(n) = \sum_{i=1}^r \mu_i p_{1i}(n)$ that $p_{11}(n) \leq \frac{1}{\mu_1}\lambda_1(n)$. Thus, for all n large, we get

$$\frac{K_{1,n}^2}{P_n - K_{1,n}} \leq \frac{4}{\mu_1}\lambda_1(n). \tag{B.26}$$

Now, with $\Lambda_1(n) \leq \frac{\log n + (k-1)\log\log n}{n}$ for all n sufficiently large under $\lim_{n\to\infty}\gamma_n = -\infty$, we see that

$$n\Lambda_1(n) = n\alpha_n\lambda_1(n) \leq \frac{3}{2}\log n \tag{B.27}$$

for all n sufficiently large. Combining (B.26) and (B.27) and the fact that $K_{1,n} \geq 2$, we obtain

$$\frac{K_{1,n}^2}{P_n - K_{1,n}} e^{\frac{\alpha_n}{K_{1,n}} n\Lambda_1(n)} = O(1)\lambda_1(n)e^{\frac{3}{4}\alpha_n \log n}. \tag{B.28}$$

Next, we define $F(n) = \lambda_1(n)e^{\frac{3}{4}\alpha_n \log n}$. Fix n sufficiently large such that (B.26) and (B.27). We consider the cases when $\alpha_n \leq \frac{1}{\log n}$ and $\alpha_n > \frac{1}{\log n}$. In the former case, $F(n) \leq \lambda_1(n)e^{3/4}$ follows directly. In the latter case we use (B.27) to get

$$F(n) \leq \frac{3}{2}\frac{\log n}{n\alpha_n} e^{\frac{3}{4}\alpha_n \log n} \leq \frac{3}{2}\frac{(\log n)^2}{n} n^{\frac{3}{4}}$$

by virtue of the fact that $\alpha_n \log n \leq \log n$. Combining the two bounds, we have

$$F(n) \leq \max\left\{\lambda_1(n)e^{0.75}, 1.5n^{-0.25}(\log n)^2\right\}$$

for all n sufficiently large. In view of $\lambda_1(n) = o(1)$ this immediately gives $\lim_{n\to\infty} F(n) = 0$, and the conclusion (B.25) follows in view of (B.28). The desired result (B.11) is now established from (B.24) and (B.25) for constant ℓ. Note that for $\ell = 0$, we have (B.11) without requiring $n\Lambda_1(n) = \Omega(1)$, since that extra condition is used only once in obtaining (B.23) which holds trivially for $\ell = 0$. This establishes Proposition B.4.

B.2 Proof of Proposition B.2

Recalling Proposition B.4 and (B.9), Proposition B.2 will follow if we show that

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}\right] = o\left(\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \,\middle|\, t_x = 1, t_y = 1\right]\right), \tag{B.29}$$

for each $\ell = 1, \ldots$. To establish (B.29), we define the series of events B_h as follows

$$B_h := [|N_{xy}| = h] \cap [|N_{x\bar{y}}| = \ell - h - 1] \cap [|N_{\bar{x}y}| = \ell - h - 1],$$

for each $h = 0, 1, \ldots, \ell - 1$. Now, it is easy to see that

$$D_{x,\ell} \cap D_{y,\ell} \cap E_{xy} = \bigcup_{h=0}^{\ell-1} (B_h \cap E_{xy} \cap [t_x = 1] \cap [t_y = 1]). \tag{B.30}$$

Note that h varies from 0 to $\ell-1$ in (B.30) because given the event E_{xy}, nodes x and y are adjacent; thus, they could have at most $\ell-1$ nodes in common when their degrees are ℓ. Since the events B_h are mutually exclusive for $h=0,\ldots,\ell-1$, we get

$$\mathbb{P}\left[D_{x,\ell}\cap D_{y,\ell}\cap E_{xy}\right]=\sum_{h=0}^{\ell-1}\mathbb{P}\left[B_h\cap E_{xy}\cap[t_x=1]\cap[t_y=1]\right]$$

Thus, the proof of Proposition B.2 will be completed upon showing

$$\sum_{h=0}^{\ell-1}\mathbb{P}\left[B_h\cap E_{xy}\cap[t_x=1]\cap[t_y=1]\right]=o\left(\sum_{h=0}^{\ell}\mathbb{P}\left[A_h\cap\overline{K_{xy}}\;\middle|\;t_x=1,t_y=1\right]\right)\tag{B.31}$$

under the enforced assumptions of Proposition B.2, namely, with $\lim_{n\to\infty}\gamma_n=-\infty$, and $n\Lambda_1(n)=\Omega(1)$. Proceeding as before, and noting that $\mathbb{P}[E_{xy}]=\alpha\mathbb{P}[K_{xy}]$ we write

$$\begin{aligned}\sum_{h=0}^{\ell-1}\mathbb{P}\left[B_h\cap E_{xy}\cap[t_x=1]\cap[t_y=1]\right]&=\mu_1^2\alpha\sum_{h=0}^{\ell-1}\sum_{u=1}^{K_{1,n}}\mathbb{P}\left[B_h\cap(|S_{xy}|=u)\;\middle|\;t_x=1,t_y=1\right]\\&\le\mu_1^2\sum_{u=1}^{K_{1,n}}\mathbb{P}\left[(|S_{xy}|=u)\right]\sum_{h=0}^{\ell-1}\mathbb{P}\left[B_h\;\middle|\;|S_{xy}|=u,t_x=t_y=1\right]\end{aligned}\tag{B.32}$$

Next, by recalling Lemma A.8 with $m_1=h$, $m_2=m_3=\ell-h-1$, we get

$$\begin{aligned}\mathbb{P}\left[B_h\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]&\sim\frac{n^{2\ell-h-2}}{h!\left((\ell-h-1)!\right)^2}e^{-2n\Lambda_1(n)+\frac{u\alpha_n\Lambda_1(n)}{K_{1,n}}n}\\&\times\left\{\mathbb{P}\left[E_{xj\cap yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right\}^h\\&\times\left\{\mathbb{P}\left[E_{xj\cap\overline{yj}}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right\}^{\ell-h-1}\\&\times\left\{\mathbb{P}\left[E_{\overline{xj}\cap yj}\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\right\}^{\ell-h-1}.\end{aligned}$$

Recalling (B.19), (B.20), and (B.21), we get

$$\mathbb{P}\left[B_h\;\middle|\;(|S_{xy}|=u),t_x=1,t_y=1\right]\le2e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)}\left(n\Lambda_1(n)\right)^{2\ell-h-2}\tag{B.33}$$

for all n sufficiently large. Using (B.33) in (B.32), we get for all n sufficiently large that

$$\begin{aligned}\sum_{h=0}^{\ell-1}\mathbb{P}\left[B_h\cap E_{xy}\cap[t_x=1]\cap[t_y=1]\right]&\le\mu_1^2\sum_{u=1}^{K_{1,n}}\left(\mathbb{P}\left[|S_{xy}|=u\;\middle|\;t_x=1,t_y=1\right]2e^{-2n\Lambda_1(n)+\frac{u\alpha_n}{K_{1,n}}n\Lambda_1(n)}\cdot\right.\\&\qquad\left.\cdot\sum_{h=0}^{\ell}\left(n\Lambda_1(n)\right)^{2\ell-h-2}\right)\\&=\mu_1^2\left(n\Lambda_1(n)\right)^{-2}\times\text{ right hand side of }(B.22)\\&=O\left(\text{ right hand side of }(B.22)\right)\end{aligned}\tag{B.34}$$

since $n\Lambda_1(n) = \Omega(1)$. We have shown in the proof of Proposition B.4 that

$$\text{right hand side of } (B.22) = o\left(\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \mid t_x = t_y = 1\right]\right)$$

Together with (B.34) this establishes (B.31) and the proof of Proposition B.2 is complete.

C Confining γ_n

In this section, we show that establishing the one-law of Theorem 3.2 under the additional constraint

$$\gamma_n = o(\log n) \tag{C.1}$$

establishes the one-law for the case when that additional constraint is not present. Namely, we will show that for any scaling that satisfies conditions (7), (8), (9), and (6) with $\lim_{n\to\infty} \gamma_n = +\infty$, there exists a scaling that satisfies the same conditions with $\lim_{n\to\infty} \gamma_n = +\infty$ *and* $\gamma_n = o(\log n)$, such that the probability of k-connectivity under the latter scaling (with $\gamma_n = o(\log n)$) is less than or equal to that under the former scaling.

Firstly, consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1^*, K_2^*, \ldots, K_r^*, P^* : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\alpha^* : \mathbb{N}_0 \to (0, 1)$ such that

$$\Lambda_1^*(n) = \alpha_n^* \lambda_1^*(n) = \frac{\log n + (k-1)\log\log n + \gamma_n^*}{n}, \tag{C.2}$$

for each $n = 1, 2, \ldots$. Assume that

$$P_n^* = \Omega(n), \quad \frac{K_{r,n}^*}{P_n^*} = o(1), \quad \text{and} \quad \frac{K_{r,n}^*}{K_{1,n}^*} = o(\log n) \tag{C.3}$$

and that we have $\lim_{n\to\infty} \gamma_n^* = +\infty$; i.e., the *-scaling satisfies all conditions enforced by part (b) of Theorem 3.2.

Now, with the same distribution $\boldsymbol{\mu}$, consider a scaling $\hat{K}_1, \hat{K}_2, \ldots, \hat{K}_r, \hat{P} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\hat{\alpha} : \mathbb{N}_0 \to (0, 1)$ such that $\hat{P}_n = P_n^*$ and $\hat{\boldsymbol{K}}_n = \boldsymbol{K}_n^*$. Obviously, we have $\hat{\lambda}_1(n) = \lambda_1^*(n)$ by recalling (2) and (3) and also that

$$\hat{P}_n = \Omega(n), \quad \frac{\hat{K}_{r,n}}{\hat{P}_n} = o(1), \quad \text{and} \quad \frac{\hat{K}_{r,n}}{\hat{K}_{1,n}} = o(\log n).$$

Next, let $\hat{\gamma}_n := \min(\gamma_n^*, \log\log n)$ and define $\hat{\alpha}_n$ through

$$\hat{\alpha}_n \hat{\lambda}_1(n) = \frac{\log n + (k-1)\log\log n + \hat{\gamma}_n}{n}. \tag{C.4}$$

Clearly, we have $\hat{\gamma}_n = o(\log n)$ and $\lim_{n\to\infty} \hat{\gamma}_n = +\infty$. This establishes that for any scaling satisfying the conditions of part (b) of of Theorem 3.2, there exists another scaling (with the same $\boldsymbol{\mu}, \boldsymbol{K}_n$, and P_n) that satisfies all of the same conditions *and* (C.1). In addition, this latter scaling has a smaller probability of a channel being *on* than the original scaling; i.e., we have

$$\hat{\alpha}_n \le \alpha_n^*, \qquad n = 2, 3, \ldots \tag{C.5}$$

by virtue of the fact that $\hat{\gamma}_n \leq \gamma_n^*$ for all n.

In view of the above, we will establish that part (b) of Theorem 3.2 under $\gamma_n = o(\log n)$ implies Theorem 3.2 if we show that

$$\mathbb{P}\left[\begin{matrix}\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n^*,P_n^*,\alpha_n^*)\\ \text{is } k-\text{connected}\end{matrix}\right] \geq \mathbb{P}\left[\begin{matrix}\mathbb{H}(n;\boldsymbol{\mu},\hat{\boldsymbol{K}}_n,\hat{P}_n,\hat{\alpha}_n)\\ \text{is } k-\text{connected}\end{matrix}\right] \tag{C.6}$$

This is clear since (C.6) would ensure that if $\mathbb{H}(n;\boldsymbol{\mu},\hat{\boldsymbol{K}}_n,\hat{P}_n,\hat{\alpha}_n)$ is k-connected asymptotically almost surely (as would be deduced from Theorem 3.2 under $\gamma_n = o(\log n)$), then so would $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n^*,P_n^*,\alpha_n^*)$.

In view of (C.5), we get (C.6) by means of an easy coupling argument showing that $\mathbb{H}(n;\boldsymbol{\mu},\hat{\boldsymbol{K}}_n,\hat{P}_n,\hat{\alpha}_n)$ is a spanning subgraph of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n^*,P_n^*,\alpha_n)$. This follows from the fact that under (C.5) the corresponding ER graphs satisfy

$$\mathbb{G}(n;\hat{\alpha}_n) \subseteq \mathbb{G}(n;\alpha_n^*)$$

meaning that for any monotone increasing graph property $\mathcal{P}$ (e.g., k-connectivity), the probability of that $\mathbb{G}(n;\alpha_n^*)$ has $\mathcal{P}$ is larger than that of $\mathbb{G}(n;\hat{\alpha}_n)$; see [17, Section V.B] for details.

D Proof of Lemma 9.1

Lemma 9.1 will be established by bounding each term in (58). First, we note from [9, Proposition 9.1] that

$$\mathbb{P}\left[\mathcal{C}_m\right] \leq m^{m-2}\left(\alpha_n p_{rr}(n)\right)^{m-1}$$

Next, we derive upper bounds on the terms $\mathbb{E}\left[1-\frac{\binom{P-|\nu_m|K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$ and $\mathbb{E}\left[\frac{\binom{P-L(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$, respectively. It is clear that Lemma 9.1 will follow if we show that

$$\mathbb{E}\left[1-\frac{\binom{P_n-|\nu_m|K_{r,n}}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq 1-e^{-3\alpha_n p_{rr}(n)m} \tag{D.1}$$

for all $m \leq \lfloor\frac{P-K_{r,n}}{2K_{r,n}}\rfloor$ and that

$$\mathbb{E}\left[\frac{\binom{P_n-L(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq \min\Bigg(1-\Lambda_1(n), e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}, \min\left(1-\mu_r+\mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right)+ e^{-\psi K_{1,n}}\mathbf{1}\left[m>m_n\right]\Bigg). \tag{D.2}$$

We establish (D.1) and (D.2) in turn in the next two sections.

D.1 Establishing (D.1)

First, with $m \leq \frac{P-K_r}{2K_r}$, we have $|\nu_m| \leq m \leq \frac{P-K_r}{2K_r}$ and using Fact A.5 we get

$$\mathbb{E}\left[1-\frac{\binom{P-|\nu_m|K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \mathbb{E}\left[1-\left(\frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right)^{2|\nu_m|}\right] = 1-\mathbb{E}\left[W^{2|\nu_m|}\right] \tag{D.3}$$

where we set $W = \frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}$. We also have

$$\begin{aligned}\mathbb{E}\left[W^{2|\nu_m|}\right] &= \mathbb{E}\left[\sum_{j=0}^{m}\binom{m}{j}\alpha^j(1-\alpha)^{m-j}W^{2j}\right] \\ &= \mathbb{E}\left[\left(1-\alpha\left(1-W^2\right)\right)^m\right] \\ &\geq \mathbb{E}\left[(1-2\alpha(1-W))^m\right] \end{aligned} \tag{D.4}$$

using Fact A.4 in the last step. We also know that

$$W = \frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}} \geq \frac{\binom{P-K_r}{K_r}}{\binom{P}{K_r}} = 1 - p_{rr} \tag{D.5}$$

Thus,

$$\alpha_n(1-W_n) \leq \alpha_n p_{rr}(n) \leq \frac{1}{4}$$

for all n sufficiently large by virtue of (61) and that $\beta_{\ell,n} = o(\log n)$. Using the fact that $1-2x \geq e^{-3x}$ for all $0 \leq x \leq \frac{1}{4}$, we then get from (D.4) and (D.5) that

$$\mathbb{E}\left[W_n^{2|\nu_m|}\right] \geq \mathbb{E}\left[e^{-3\alpha_n(1-W_n)m}\right] \geq e^{-3\alpha_n p_{rr}(n)m}$$

for all n sufficiently large. The desired conclusion (D.1) now follows immediately by means of (D.3).

D.2 Establishing (D.2)

Let $\boldsymbol{Y}$ be defined as follows

$$Y_i = \begin{cases} \lfloor i\zeta K_{1,n} \rfloor & i = 2, \ldots, m_n \\ \lfloor \psi P_n \rfloor & i = m_n+1, \ldots, n \end{cases}$$

where $\zeta \in (0, \frac{1}{2})$ selected small enough such that (49) holds, and $\psi \in (0, \frac{1}{2})$ selected small enough such that (50) holds. Recalling (48), we see that

$$J_i = \begin{cases} \max\left(\lfloor (1+\epsilon)K_{1,n} \rfloor, Y_i\right) & i = 2, \ldots, m_n \\ Y_i & i = m_n+1, \ldots, n \end{cases}$$

Next, we let

$$M(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m| = 1\right] + \max\left(K_{1,n}, Y_{|\nu_m|}+1\right)\mathbf{1}\left[|\nu_m| > 1\right],$$

and

$$Q(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m| = 1\right] + \left(\lfloor (1+\epsilon)K_{1,n} \rfloor + 1\right)\mathbf{1}\left[|\nu_m| > 1\right].$$

We also recall that

$$L(\nu_m) = \max\left(K_{1,n}\mathbf{1}\left[|\nu_m| > 0\right], \left(J_{|\nu_m|}+1\right)\mathbf{1}\left[|\nu_m| > 1\right]\right)$$

Let's consider the following three cases

1. $|\nu_m|= 0$: In this case we have $L(\nu_m) = M(\nu_m) = Q(\nu_m) = 0$.
2. $|\nu_m|= 1$: In this case we have $L(\nu_m) = M(\nu_m) = Q(\nu_m) = K_{1,n}$.
3. $|\nu_m|\geq 2$: In this case we have
   - $L(\nu_m) = \max\left(K_{1,n}, J_{|\nu_m|}+1\right)$.
   - $M(\nu_m) = \max\left(K_{1,n}, Y_{|\nu_m|}+1\right)$.
   - $Q(\nu_m) = \lfloor (1+\epsilon)\, K_{1,n} \rfloor + 1$.

More specifically, considering the case when $|\nu_m|= 2, 3, \ldots, m_n$, we have

$$J_{|\nu_m|} = \max\left((1+\epsilon)K_{1,n}, Y_{|\nu_m|}\right)$$

and it follows that

$$\begin{aligned} L(\nu_m) &= \max\left(K_{1,n}, \lfloor (1+\epsilon)K_{1,n} \rfloor + 1, Y_{|\nu_m|}+1\right) \\ &= \max\left(\lfloor (1+\epsilon)K_{1,n} \rfloor + 1, M(\nu_m)\right) \\ &= \max\left(Q(\nu_m), M(\nu_m)\right) \end{aligned}$$

Also, when $|\nu_m|= m_n+1, \ldots, n$, we clearly have $J_{|\nu_m|} = Y_{|\nu_m|}$, and thus

$$L(\nu_m) = M(\nu_m) = \max\left(K_{1,n}, \lfloor \psi P_n \rfloor + 1\right).$$

Since $K_{1,n} \leq K_{r,n} = o(P_n)$ in view of (8), we have

$$\lfloor \psi P_n \rfloor \geq \lfloor (1+\epsilon)\, K_{1,n} \rfloor$$

for all n sufficiently large. Thus, we can rewrite $L(\nu_m)$ as

$$\begin{aligned} L(\nu_m) &= \max\left(K_{1,n}, \lfloor \psi P_n \rfloor + 1, \lfloor (1+\epsilon)\, K_{1,n} \rfloor + 1\right) \\ &= \max\left(Q(\nu_m), M(\nu_m)\right). \end{aligned}$$

Combining, we conclude that it always holds that $L(\nu_m) = \max\left(Q(\nu_m), M(\nu_m)\right)$, whence

$$\mathbb{E}\left[\frac{\binom{P-L(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \min\left(\mathbb{E}\left[\frac{\binom{P-M(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right], \mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]\right) \tag{D.6}$$

Note that it was shown in [36, Lemma 7.2] that

$$\mathbb{E}\left[\frac{\binom{P-M(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \min\left(1-\Lambda_1(n), \min\left(1-\mu_r+\mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right) + e^{-\psi K_{1,n}} 1\left[m > m_n\right]\right)$$

for all n sufficiently large. On the same range, we also get from Lemma A.10 that

$$\mathbb{E}\left[\frac{\binom{P_n-Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}$$

upon noting that $\Lambda_1(n) = o(1)$ under (41) with $\beta_{\ell,n} = o(\log n)$. Reporting the last two bounds into (D.6), we establish (D.2).

E Proof of Lemma 10.1

From (41) and the fact that $\beta_{\ell,n} = o(\log n)$, we clearly have

$$\frac{1}{2}\frac{\log n}{n} \leq \Lambda_1(n) \leq 2\frac{\log n}{n} \tag{E.1}$$

for all n sufficiently large. We also have

$$\Lambda_1(n) = \alpha_n \sum_{j=1}^{r} \mu_j p_{1j} \geq \mu_r \alpha_n p_{1r}(n)$$

Now, since p_{1j} is monotone increasing in $j = 1, \ldots, r$ by virtue of (14), we also see that

$$\Lambda_1(n) = \alpha_n \sum_{j=1}^{r} \mu_j p_{1j}(n) \leq \alpha_n p_{1r}(n) \sum_{j=1}^{r} \mu_j = \alpha_n p_{1r}(n)$$

Thus, we obtain that

$$\Lambda_1 \leq \alpha_n p_{1r}(n) \leq \frac{1}{\mu_r}\Lambda_1$$

and the conclusion (60) immediately follows by virtue of (E.1) for all n sufficiently large.

Next, we establish (61). Here this will be established by showing that

$$p_{rr}(n) \leq \max\left(2, 4\frac{\log n}{w_n}\right) p_{1r}(n), \quad n = 2, 3, \ldots \tag{E.2}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Fix $n = 2, 3, \ldots$. We have either $p_{1r}(n) > \frac{1}{2}$, or $p_{1r}(n) \leq \frac{1}{2}$. In the former case, it automatically holds that

$$p_{rr}(n) \leq 2p_{1r}(n) \tag{E.3}$$

by virtue of the fact that $p_{rr}(n) \leq 1$.

Assume now that $p_{1r}(n) \leq \frac{1}{2}$. We know from [19, Lemmas 7.1-7.2] that

$$1 - e^{-\frac{K_{j,n}K_{r,n}}{P_n}} \leq p_{jr}(n) \leq \frac{K_{j,n}K_{r,n}}{P_n - K_{j,n}}, \quad j = 1, \ldots, r \tag{E.4}$$

and it follows that

$$\frac{K_{1,n}K_{r,n}}{P_n} \leq \log\left(\frac{1}{1 - p_{1r}(n)}\right) \leq \log 2 < 1. \tag{E.5}$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ with x in $(0, 1)$, we then get

$$p_{1r}(n) \geq \frac{K_{1,n}K_{r,n}}{2P_n}. \tag{E.6}$$

In addition, using the upper bound in (E.4) with $j = r$ gives

$$p_{rr}(n) \leq \frac{K_{r,n}^2}{P_n - K_{r,n}} \leq 2\frac{K_{r,n}^2}{P_n}$$

as we invoke (5). Combining the last two bounds we obtain

$$\frac{p_{rr}(n)}{p_{1r}(n)} \leq 4\frac{K_{r,n}}{K_{1,n}} \tag{E.7}$$

Next, combining (9) and (E.7), we get

$$p_{rr}(n) \leq 4\frac{\log n}{w_n} p_{1r}(n) \tag{E.8}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Combining (E.3) and (E.8), we readily obtain (E.2).

It is easy to see that (62) can be established using the same steps with the proof of (E.2).