k-Connectivity in Secure Wireless Sensor Networks with Physical Link Constraints – The On/Off Channel Model

Jun Zhao, *Student Member, IEEE,* Osman Yağan, *Member, IEEE,* and Virgil Gligor, *Senior Member, IEEE*

***Abstract*—Random key predistribution scheme of Eschenauer and Gligor (EG) is a typical solution for ensuring secure communications in a wireless sensor network (WSN). Connectivity of the WSNs under this scheme has received much interest over the last decade, and most of the existing work is based on the assumption of unconstrained sensor-to-sensor communications. In this paper, we study the k-connectivity of WSNs under the EG scheme with physical link constraints; k-connectivity is defined as the property that the network remains connected despite the failure of any $(k-1)$ sensors. We use a simple communication model, where unreliable wireless links are modeled as independent on/off channels, and derive zero-one laws for the properties that $i)$ the WSN is k-connected, and $ii)$ each sensor is connected to at least k other sensors. These zero-one laws improve the previous results by Rybarczyk on the k-connectivity under a fully connected communication model. Moreover, under the on/off channel model, we provide a stronger form of the zero-one law for the 1-connectivity as compared to that given by Yağan. We also discuss the applicability of our results in a different network application, namely in a large-scale, distributed publish-subscribe service for online social networks.**

***Index Terms*—Wireless sensor networks, key predistribution, random key graphs, k-connectivity, minimum node degree.**

I. Introduction

A. Motivation and Background

Many designs of secure wireless sensor networks (WSNs) (e.g., [2], [7], [10]) rely on a basic key predistribution scheme proposed by Eschenauer and Gligor [13]. That is, for keying a network comprising n sensor nodes[1], this scheme uses an offline *key pool* $\mathcal{P}$ containing P_n keys, where P_n is a function of n. Before deployment, each node is independently equipped with K_n *distinct* keys selected uniformly at random from $\mathcal{P}$; as the notation suggests K_n is also assumed to be a function of n. The K_n keys in each node comprise the node's *key ring*. After deployment, two communicating nodes can establish a *secure link* if they share a key. More specifically, a secure link exists between two nodes only if their key rings have at least one key in common, as message secrecy and authenticity are obtained by using efficient symmetric-key encryption modes [16], [19], [25].

In this paper, we consider the k-connectivity of secure WSNs operating under the key predistribution scheme of Eschenauer-Gligor. A network (or graph) is said to be k-connected if for each pair of nodes there exist at least k mutually disjoint paths connecting them. An equivalent definition of k-connectivity is that a network is k-connected if the network remains connected despite the failure of any $(k-1)$ nodes [24]; a network is said to be simply connected if it is 1-connected.

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 resiliency against network disconnection due to battery depletion, in both normal mode of operation and under battery-depletion attacks [20], [28]. Furthermore, it enables flexible communication-load balancing across multiple paths so that network energy consumption is distributed without penalizing any access path [14]. In addition, k-connectivity is useful in terms of achieving consensus despite adversarial nodes in the network. Specifically, it is known that for a network to achieve consensus in the presence of adversarial nodes, a necessary and sufficient condition is that the number of adversary-controlled nodes be less than half of the network connectivity *and* less than one third of the number of network nodes [9], [33]. In other words, if $k=2f+1$ where f is the number of adversary-controlled nodes, k-connectivity guarantees that consensus can be reached in a network with $n \gg f$ nodes.

With this motivation in mind, our goal is to study the k-connectivity of secure WSNs and we will do so by analyzing the induced *random graph* models. To begin with, the basic key predistribution scheme is often modeled by a *random key graph*, $G(n, K_n, P_n)$, also known as a *uniform random intersection graph*, whose properties have been extensively analyzed [3], [5], [26], [29], [32]. Random key graphs have also recently been used for various applications, e.g., cryptanalysis of hash functions [4], trust networks [17], recommender systems using collaborative filtering [21], and modeling "small world" networks [31]. The zero-one laws for k-connectivity [27] and 1-connectivity [3], [26], [32] of random key graphs have already been established. However, in the context of wireless sensor networks, the application of random key graph requires the assumption of a fully connected communication model; i.e., *any* pair of nodes must have a

The authors are with CyLab, Carnegie Mellon University, Pittsburgh, PA 15213 USA. J. Zhao and V. Gligor are also with the Department of Electrical and Computer Engineering, Carnegie Mellon University. (e-mail: junzhao@cmu.edu, oyagan@andrew.cmu.edu, gligor@cmu.edu).

[1]We consider the terms sensor, node and vertex interchangeable.

direct communication link in between.

B. Contributions

Our main goal is to study the k-connectivity of secure WSNs under *physical link constraints*; i.e., when the assumption of a fully connected communication model is dropped. To this end, we say that a secure link exists between two nodes if and only if their key rings have at least one key in common *and* the physical link constraint between them is satisfied. Specifically, in this paper, we consider a simple communication model that consists of independent channels that are either *on* (with probability p_n) or *off* (with probability $1 - p_n$). Under this on/off channel model, a secure link exists between two sensors as long as their key rings have at least one key in common *and* the channel between them is *on*. We denote the graph representing the underlying network as $\mathbb{G}_{on}$; see Section III for precise definitions of the system model.

We derive zero-one laws in the random graph $\mathbb{G}_{on}$ for k-connectivity and the property that the *minimum node degree* is at least k; see Theorem 1. To the best of our knowledge, these results constitute the first complete analysis of the k-connectivity of WSNs under physical link constraints and may provide useful design guidelines in dimensioning the EG scheme; i.e., in selecting its parameters to ensure the desired k-connectivity property. The main result of the paper also implies a zero-one law for k-connectivity in random key graph $G(n, K_n, P_n)$ (see Corollary 2), and the established result is shown to improve that given previously by Rybarczyk [26]; see Section IV-D for details. Moreover, for the 1-connectivity of $\mathbb{G}_{on}$, we provide a stronger form of the zero-one law as compared to that given by Yağan [30]; see Section IV-D. Finally, we discuss a possible application of our k-connectivity results for $\mathbb{G}_{on}$ in a different network domain, namely in large-scale, distributed publish-subscribe service for online social networks.

C. Organization of the Paper

We organize the rest of the paper as follows: In Section II, we survey the relevant results from the literature, while in Section III we give a detailed description of the system model $\mathbb{G}_{on}$. The main results of the paper, namely the zero-one laws for k-connectivity and minimum node degree in $\mathbb{G}_{on}$, are presented (see Theorem 1) in Section IV. The basic ideas that pave the way in establishing Theorem 1 are given in Section V. Sections VI through VIII are devoted to establishing the zero-law part of Theorem 1, whereas the one-law of Theorem 1 is established in Sections IX through XIII. The applications of our results in other network domains are discussed in Section XIV, and the paper is concluded in Section XV by some remarks and future research directions. Some of the technical details are given in Appendices A-C.

II. Related Work

Early work by Erdős and Rényi [11] and Gilbert [15] introduces the random graph $G(n, p)$, which is defined on n nodes and there exists an edge between any two nodes with probability p *independently* of all other edges. The probability p can also be a function of n, in which case we refer to it as p_n. Throughout the paper, we refer to the random graph $G(n, p_n)$ as an Erdős-Rényi (ER) graph following the convention in the literature.

Erdős and Rényi [11] prove that when p_n is $\frac{\ln n + \alpha_n}{n}$, graph $G(n, p_n)$ is *asymptotically almost surely*[2] (a.a.s.) connected (resp., not connected) if $\lim_{n\to\infty} \alpha_n = +\infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$). In later work [12], they further explore k-connectivity [23] in $G(n, p_n)$ and show that if $p_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, $G(n, p_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty} \alpha_n = +\infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$).

Previous work [3], [26], [32] investigates the zero-one law for connectivity in random key graph $G(n, K_n, P_n)$, where P_n and K_n are the key pool size and the key ring size, respectively. Blackburn and Gerke [3] prove that if $K_n \geq 2$ and $P_n = \lfloor n^{\xi} \rfloor$, where ξ is a positive constant, $G(n, K_n, P_n)$ is a.a.s. connected (resp., not connected) if $\liminf_{n\to+\infty} \frac{K_n^2 n}{P_n \ln n} > 1$ (resp., $\limsup_{n\to+\infty} \frac{K_n^2 n}{P_n \ln n} < 1$). Yağan and Makowski [32] demonstrate that if[3] $K_n \geq 2$, $P_n = \Omega(n)$ and $\frac{K_n^2}{P_n} = \frac{\ln n + \alpha_n}{n}$, then $G(n, K_n, P_n)$ is a.a.s. connected (resp., not connected) if $\lim_{n\to\infty} \alpha_n = +\infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$). Rybarczyk [26] obtains the same result without requiring $P_n = \Omega(n)$. She also establishes [27, Remark 1, p. 5] a zero-one law for k-connectivity in $G(n, K_n, P_n)$ by showing the similarity between $G(n, K_n, P_n)$ and a random intersection graph [5] via a coupling argument. Specifically, she proves that if $P_n = \Theta(n^{\xi})$ for some $\xi > 1$ and $\frac{K_n^2}{P_n} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, then the $G(n, K_n, P_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty} \alpha_n = +\infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$).

Recently Yağan [30] gives a zero-one law for connectivity (i.e., 1-connectivity) in graph $G(n, K_n, P_n) \cap G(n, p_n)$, which is the intersection of random key graph $G(n, K_n, P_n)$ and random graph $G(n, p_n)$, and clearly is equivalent to our key graph $\mathbb{G}_{on}$; see Section III. Specifically, he shows that if $K_n \geq 2$, $P_n = \Omega(n)$ and $p_n \cdot \left[1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}\right] \sim \frac{c \ln n}{n}$ hold, and $\lim_{n\to\infty}(p_n \ln n)$ exists, then graph $G(n, K_n, P_n) \cap G(n, p_n)$ is asymptotically almost surely connected (resp., not connected) if $c > 1$ (resp., $c < 1$).

A comparison of our results with the related work is given in Section IV-D.

[2] We say that an event takes place *asymptotically almost surely* if its probability approaches to 1 as $n \to \infty$. Also, we use "resp." as a shorthand for "respectively".

[3] We use the standard asymptotic notation $o(\cdot), O(\cdot), \Theta(\cdot), \Omega(\cdot), \sim$. That is, given two positive functions $f(n)$ and $g(n)$,

1) $f(n) = o(g(n))$ means $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
2) $f(n) = O(g(n))$ means that there exist positive constants c and N such that $f(n) \leq c g(n)$ for all $n \geq N$.
3) $f(n) = \Omega(g(n))$ means that there exist positive constants c and N such that $f(n) \geq c g(n)$ for all $n \geq N$.
4) $f(n) = \Theta(g(n))$ means that there exist positive constants c_1, c_2 and N such that $c_1 g(n) \leq f(n) \leq c_2 g(n)$ for all $n \geq N$.
5) $f(n) \sim g(n)$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$; i.e., $f(n)$ and $g(n)$ are asymptotically equivalent.

III. System Model

A. The Model $\mathbb{G}_{on}$

Consider a vertex set $\mathcal{V} = \{v_1, v_2, \dots, v_n\}$. For each node $v_i \in \mathcal{V}$, we define S_i as the key ring of node v_i; i.e., the set of K_n distinct keys of node v_i that are selected uniformly at random from a key pool $\mathcal{P}$ of P_n keys. The random key graph, denoted $G(n, K_n, P_n)$ is defined on the vertex set $\mathcal{V}$ such that there exists an edge between two distinct nodes v_i and v_j, denoted K_{ij}, if their key rings have at least one key in common; i.e.,

$$K_{ij} = [S_i \cap S_j \neq \emptyset].$$

For any two distinct nodes v_x and v_y, we let S_{xy} denote the intersection of their key rings S_x and S_y; i.e., $S_{xy} = S_x \cap S_y$.

As mentioned in Section I-B, here we assume a communication model that consists of independent channels that are either *on* (with probability p_n) or *off* (with probability $1-p_n$). For distinct nodes v_i and v_j, let C_{ij} denote the event that the communication channel between them is *on*. The events $\{C_{ij},\ 1 \leq i < j \leq n\}$ are mutually independent such that

$$\mathbb{P}[C_{ij}] = p_n, \quad 1 \leq i < j \leq n. \tag{1}$$

This communication model can be modeled by an Erdős-Rényi graph $G(n, p_n)$ on the vertices $\mathcal{V}$ such that there exists an edge between nodes v_i and v_j if the communication channel between them is on; i.e., if the event C_{ij} takes place.

Finally, the graph $\mathbb{G}_{on}(n, K_n, P_n, p_n)$ is defined on the vertices $\mathcal{V}$ such that two distinct nodes v_i and v_j have an edge in between, denoted E_{ij}, if the events K_{ij} and C_{ij} take place at the same time. In other words, we have

$$E_{ij} = K_{ij} \cap C_{ij}, \quad 1 \leq i < j \leq n \tag{2}$$

so that

$$\mathbb{G}_{on}(n, K_n, P_n, p_n) = G(n, K_n, P_n) \cap G(n, p_n). \tag{3}$$

Throughout, we simplify the notation by writing $\mathbb{G}_{on}$ instead of $\mathbb{G}_{on}(n, K_n, P_n, p_n)$.

Throughout, we let $p_s(K_n, P_n)$ be the probability that the key rings of two distinct nodes share at least one key and let $p_e(K_n, P_n, p_n)$ be the probability that there exists a link between two distinct nodes in $\mathbb{G}_{on}$. For simplicity, we write $p_s(K_n, P_n)$ as p_s and write $p_e(K_n, P_n, p_n)$ as p_e. Then for any two distinct nodes v_i and v_j, we have

$$p_s := \mathbb{P}[K_{ij}]. \tag{4}$$

It is easy to derive p_s in terms of K_n and P_n as shown in previous work [3], [26], [32]. In fact, we have

$$p_s = \mathbb{P}[S_i \cap S_j \neq \emptyset] = \begin{cases} 1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}, & \text{if } P_n \geq 2K_n, \\ 1 & \text{if } P_n < 2K_n. \end{cases} \tag{5}$$

Given (2), the independence of the events C_{ij} and K_{ij} ensures that

$$p_e := \mathbb{P}[E_{ij}] = \mathbb{P}[C_{ij}] \cdot \mathbb{P}[K_{ij}] = p_n \cdot p_s \tag{6}$$

from (1) and (4). Substituting (5) into (6), we obtain

$$p_e = p_n \cdot \left[1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}} \right] \quad \text{if } P_n \geq 2K_n. \tag{7}$$

B. Useful Notation for Graph $\mathbb{G}_{on}$

For any event A, we let $\overline{A}$ be the complement of A. Also, for sets S_a and S_b, the relative complement of S_a in S_b is given by $S_a \setminus S_b$.

In graph $\mathbb{G}_{on}$, for each node $v_i \in \mathcal{V}$, we define N_i as the set of neighbors of node v_i. For any two distinct nodes v_x and v_y, there are $(n-2)$ nodes other than v_x and v_y in graph $\mathbb{G}_{on}$. These $(n-2)$ nodes can be split into the four sets N_{xy}, $N_{x\overline{y}}$, $N_{\overline{x}y}$ and $N_{\overline{x}\,\overline{y}}$ in the following manner. Let N_{xy} be the set of nodes that are neighbors of both v_x and v_y; i.e., $N_{xy} = N_x \cap N_y$. 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, $N_{\overline{x}\,\overline{y}}$ 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 clearly have

$$\begin{aligned} N_{xy} &= N_x \cap N_y, \\ N_{x\overline{y}} &= N_x \setminus (N_y \cup \{v_y\}), \\ N_{\overline{x}y} &= N_y \setminus (N_x \cup \{v_x\}), \\ N_{\overline{x}\,\overline{y}} &= \mathcal{V} \setminus (N_x \cup N_y \cup \{v_x, v_y\}), \end{aligned}$$

and

$$N_{xy} \cap N_{x\overline{y}} \cap N_{\overline{x}y} \cap N_{\overline{x}\,\overline{y}} = \mathcal{V} \setminus (\{v_x, v_y\}).$$

For any three distinct nodes v_x, v_y and v_j, recalling that E_{xj} (resp., E_{yj}) is the event that there exists a link between nodes v_x (resp., v_y) and v_j, we define

$$\begin{aligned} E_{xj \cap yj} &:= E_{xj} \cap E_{yj}, & E_{xj \cap \overline{yj}} &:= E_{xj} \cap \overline{E_{yj}}, \\ E_{\overline{xj} \cap yj} &:= \overline{E_{xj}} \cap E_{yj}, \text{ and } & E_{\overline{xj} \cap \overline{yj}} &:= \overline{E_{xj}} \cap \overline{E_{yj}}. \end{aligned}$$

In graph $\mathbb{G}_{on}$, for any non-negative integer ℓ, let X_ℓ be the number of nodes having degree ℓ; let $D_{x,\ell}$ be the event that node v_x has degree ℓ. We define δ as the minimum node degree of graph $\mathbb{G}_{on}$, and define κ as the connectivity of graph $\mathbb{G}_{on}$. Note that the connectivity of a graph is defined as the minimum number of nodes whose deletion renders the graph disconnected; and thus, a graph is k-connected if and only if its connectivity is at least k. Finally, a graph is said to be simply *connected* if its connectivity is at least 1, i.e., if it is 1-connected.

IV. The Zero-One Law of K-Connectivity under an On/Off Channel Model

A. The Main Result

Recall that we denote by $\mathbb{G}_{on}$ the random graph induced by the EG scheme under the on/off channel model. The main result of this paper, given below, establishes zero-one laws for k-connectivity and for the property that the minimum node degree is no less than k in graph $\mathbb{G}_{on}$. Note that throughout this paper, k is a positive integer and does not scale with n. Also, we let $\mathbb{N}$ (resp., $\mathbb{N}_0$) stand for the set of all non-negative (resp., positive) integers.

We refer to any pair of mappings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* as long as it satisfies the natural conditions

$$K_n \leq P_n, \quad n = 1, 2, \dots. \tag{8}$$

Similarly, any mapping $p : \mathbb{N}_0 \to (0,1)$ defines a scaling.

Theorem 1. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$, $p : \mathbb{N}_0 \to (0,1)$ such that $K_n \geq 2$ for all n sufficiently large. We define a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ such that for any $n \in \mathbb{N}_0$, we have*

$$p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}. \quad (9)$$

The properties (a) and (b) below hold.

(a) If $\frac{K_n^2}{P_n} = o(1)$ and either *there exist an $\epsilon > 0$ such that $p_e n > \epsilon$ holds for all n sufficiently large,* or $\lim_{n\to\infty} p_e n = 0$, *then*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \text{ is } k\text{-connected}\right] = 0 \quad \text{if } \lim_{n\to\infty} \alpha_n = -\infty, \quad (10)$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\text{Minimum node degree}\\ \text{of } \mathbb{G}_{on} \text{ is no less than } k\end{array}\right] = 0 \;\; \text{if } \lim_{n\to\infty} \alpha_n = -\infty. \quad (11)$$

(b) If $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$, then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \text{ is } k\text{-connected}\right] = 1 \;\text{ if } \lim_{n\to\infty} \alpha_n = \infty, \quad (12)$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\text{Minimum node degree}\\ \text{of } \mathbb{G}_{on} \text{ is no less than } k\end{array}\right] = 1 \quad \text{if } \lim_{n\to\infty} \alpha_n = \infty. \quad (13)$$

Note that if we combine (10) and (12), we obtain the zero-one law for k-connectivity in $\mathbb{G}_{on}$, whereas combining (11) and (13) leads to the zero-one law for the minimum node degree. Therefore, Theorem 1 presents the zero-one laws of k-connectivity and the minimum node degree in graph $\mathbb{G}_{on}$. We also see from (9) that the critical scaling for both properties is given by $p_e = \frac{\ln n + (k-1)\ln\ln n}{n}$. The sequence $\alpha_n : \mathbb{N}_0 \to \mathbb{R}$ defined through (9) therefore measures by how much the probability p_e deviates from the critical scaling.

In case (b) of Theorem 1, the conditions $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$ indicate that the size of the key pool P_n should grow at least linearly with the number of sensor nodes in the network, and should grow unboundedly with the size of each key ring. These conditions are enforced here merely for technical reasons, but they hold trivially in practical wireless sensor network applications [6], [8], [13]. Again, the condition $\frac{K_n^2}{P_n}$ enforced for the zero-law in Theorem 1 is not a stringent one since the P_n is expected to be several orders of magnitude larger than K_n. Finally, the condition that either $p_e n > \epsilon > 0$ for all n large, or $\lim_{n\to\infty} p_e n = 0$ is made to avoid degenerate situations. In fact, in most cases of interest it holds that $p_e n > \epsilon > 0$ as otherwise the graph $\mathbb{G}_{on}$ becomes *trivially* disconnected. To see this, notice that $p_e n$ a is an upper-bound on the *expected* degree of a node and that the *expected* number of edges in the graph is less than $p_e n^2$; yet, a connected graph on n nodes must have at least $n-1$ edges.

B. Results with an approximation of probability p_s

An analog of Theorem 1 can be given with a simpler form of the scaling than (9); i.e., with p_s replaced by the more easily expressed quantity K_n^2/P_n, and hence with $p_e = p_n K_n^2/P_n$. In fact, in the case of random key graph $G(n, K_n, P_n)$ it is a common practice [3], [26], [32] to replace p_s by $\frac{K_n^2}{P_n}$, owing mostly to the fact that [32]

$$p_s \sim \frac{K_n^2}{P_n} \quad \text{if} \quad \frac{K_n^2}{P_n} = o(1). \quad (14)$$

However, when the random key graph $G(n, K_n, P_n)$ is intersected with a random graph $G(n, p_n)$ (as in the case of $\mathbb{G}_{on}$) the simplification does not occur naturally (even under (14)), and as seen below, simpler forms of the zero-one laws are obtained at the expense of extra conditions enforced on the parameters K_n and P_n.

Corollary 1. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$, $p : \mathbb{N}_0 \to (0,1)$ such that $K_n \geq 2$ for all n sufficiently large. We define a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ such that for any $n \in \mathbb{N}_0$, we have*

$$p_n \cdot \frac{K_n^2}{P_n} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}. \quad (15)$$

The properties (a) and (b) below hold.

(a) If $\frac{K_n^2}{P_n} = O(\frac{1}{\ln n})$ and $\lim_{n\to\infty}(\ln n + (k-1)\ln\ln n + \alpha_n) = \infty$, then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \text{ is } k\text{-connected}\right] = 0 \quad \text{if } \lim_{n\to\infty} \alpha_n = -\infty, \quad (16)$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\text{Minimum node degree}\\ \text{of } \mathbb{G}_{on} \text{ is no less than } k\end{array}\right] = 0 \;\; \text{if } \lim_{n\to\infty} \alpha_n = -\infty. \quad (17)$$

(b) If $P_n = \Omega(n)$ and $\frac{K_n^2}{P_n} = O(\frac{1}{\ln n})$, then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \text{ is } k\text{-connected}\right] = 1 \;\text{ if } \lim_{n\to\infty} \alpha_n = \infty, \quad (18)$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\text{Minimum node degree}\\ \text{of } \mathbb{G}_{on} \text{ is no less than } k\end{array}\right] = 1 \quad \text{if } \lim_{n\to\infty} \alpha_n = \infty. \quad (19)$$

Note that the condition $\frac{K_n^2}{P_n} = O(\frac{1}{\ln n})$ enforced in Corollary 1 implies both $\frac{K_n}{P_n} = o(1)$ and $\frac{K_n^2}{P_n} = o(1)$, and thus it is a stronger condition than those enforced in Theorem 1.

Proof. Consider p_n, K_n and P_n as in the statement of Corollary 1 such that (15) holds. As explained above, conditions $\frac{K_n}{P_n} = o(1)$ and $\frac{K_n^2}{P_n} = o(1)$ both hold. The proof is based on Theorem 1. Namely, we will show that if the sequence $\alpha' : \mathbb{N}_0 \to \mathbb{R}$ is defined such that

$$p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha'_n}{n} \quad (20)$$

for any $n \in \mathbb{N}_0$, then it holds that

$$\alpha'_n = \alpha_n \pm O(1) \quad (21)$$

under the enforced assumptions. In view of $\lim_{n\to\infty}(\ln n + (k-1)\ln\ln n + \alpha_n) = \infty$ and (21), we get $\lim_{n\to\infty} p_e n = \infty$ from (20). Thus, for any $\epsilon > 0$, we have $p_e n > \epsilon$ for all n sufficiently large. Hence, all the conditions enforced by Theorem 1 are met, and under (20) and (21), Corollary 1 follows from Theorem 1 since $\lim_{n\to\infty}\alpha'_n = \pm\infty$ if $\lim_{n\to\infty}\alpha_n = \pm\infty$.

We now establish (21). First, as seen by the analysis given in Section V-B below, we can introduce the extra condition $\alpha_n = o(\ln n)$ in proving part (b) of Corollary 1; i.e., in proving the one-law under the condition $\lim_{n\to\infty}\alpha_n = \infty$. This yields $p_n \frac{K_n^2}{P_n} = O(\frac{\ln n}{n})$ under (15). Also, in the case $\lim_{n\to\infty}\alpha_n = -\infty$, we have $\alpha_n < 0$ for all n sufficiently large so that $p_n \frac{K_n^2}{P_n} = O(\frac{\ln n}{n})$. Now, in order to establish (21), we observe from part (a) of Lemma 8[4] that

$$p_s = \frac{K_n^2}{P_n} \pm O\left(\frac{K_n^4}{P_n^2}\right). \tag{22}$$

Then, from (22) and the fact that $p_e = p_s p_n$, we get

$$p_e = p_n \cdot \frac{K_n^2}{P_n} \pm p_n \cdot \frac{K_n^2}{P_n} \cdot O\left(\frac{K_n^2}{P_n}\right). \tag{23}$$

Substituting (15), $p_n \frac{K_n^2}{P_n} = O(\frac{\ln n}{n})$ and $\frac{K_n^2}{P_n} = O\left(\frac{1}{\ln n}\right)$ into (23), we find

$$p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n \pm O(1)}{n}. \tag{24}$$

Comparing the above relation with (20), the desired conclusion (21) follows. ■

C. A Zero-One Law for k-Connectivity in Random Key Graphs

We now provide a useful corollary of Theorem 1 that gives a zero-one law for k-connectivity in the random key graph $G(n, K_n, P_n)$. As discussed in Section IV-D below, this result improves the one given *implicitly* by Rybarczyk [27].

Corollary 2. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n \geq 2$ for all n sufficiently large. With $\alpha : \mathbb{N}_0 \to \mathbb{R}$ given by*

$$\frac{K_n^2}{P_n} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \quad n = 1, 2, \ldots, \tag{25}$$

the following two properties hold.

(a) If either there exists an $\epsilon > 0$ such that $n\frac{K_n^2}{P_n} > \epsilon$ for all n sufficiently large, or $\lim_{n\to\infty} n\frac{K_n^2}{P_n} = 0$, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[G(n, K_n, P_n) \text{ is } k\text{-connected}\right] = 0 \text{ if } \lim_{n\to\infty}\alpha_n = -\infty.$$

(b) If $P_n = \Omega(n)$, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[G(n, K_n, P_n) \text{ is } k\text{-connected}\right] = 1 \text{ if } \lim_{n\to\infty}\alpha_n = \infty.$$

Proof. We first establish the zero-law. Pick K_n, P_n such that (25) holds with $\lim_{n\to\infty} = -\infty$. It is clear that we have $\alpha_n < 0$ for all n sufficiently large so that $\frac{K_n^2}{P_n} = O(\frac{\ln n}{n}) = o(1)$. In view of (22) we thus get

$$p_s = \frac{\ln n + (k-1)\ln\ln n + \alpha_n \pm o(1)}{n}, \quad n = 1, 2, \ldots$$

Let $p_n = 1$ for all n. In this case, graph $\mathbb{G}_{on}$ becomes equivalent to $G(n, K_n, P_n)$ with

$$p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n \pm o(1)}{n}, \quad n = 1, 2, \ldots \tag{26}$$

From (26) and (25), we have $p_e n = n\frac{K_n^2}{P_n} \pm o(1)$ so that i) if there exists an $\epsilon > 0$ such that $n\frac{K_n^2}{P_n} > \epsilon$, then there exists an $\epsilon' > 0$ such that $p_e n > \epsilon'$ for all n sufficiently large and ii) if $\lim_{n\to\infty} n\frac{K_n^2}{P_n} = 0$, then $\lim_{n\to\infty} p_e n = 0$. Thus, all the conditions enforced by part (a) of Theorem 1 are satisfied for the given K_n, P_n and p_n. Comparing (26) with (9), we get $\lim_{n\to\infty}\alpha_n \pm o(1) = -\infty$ and the zero law $\lim_{n\to\infty}\mathbb{P}\left[G(n, K_n, P_n) \text{ is } k\text{-connected}\right] = 0$ follows from (10) of Theorem 1.

We now establish the one-law. Pick K_n, P_n such that (25) holds with $\lim_{n\to\infty}\alpha_n = +\infty$, $P_n = \Omega(n)$ and $K_n \geq 2$ for all n sufficiently large. In view of [32, Lemma 6.1], there exists $\tilde{K}_n$, $\tilde{P}_n$ such that $\tilde{K}_n \geq 2$ for all n sufficiently large,

$$\tilde{K}_n \leq K_n \quad \text{and} \quad \tilde{P}_n = P_n, \quad n = 1, 2, \ldots,$$

and

$$\frac{\tilde{K}_n^2}{\tilde{P}_n} = \frac{\ln n + (k-1)\ln\ln n + \tilde{\alpha}_n}{n}, \quad n = 1, 2, \ldots, \tag{27}$$

with

$$\tilde{\alpha}_n = O(\ln n) \quad \text{and} \quad \lim_{n\to\infty}\tilde{\alpha}_n = \infty.$$

By an easy coupling argument, it is easy to check that

$$\mathbb{P}\left[G(n, \tilde{K}_n, \tilde{P}_n) \text{ is } k\text{-connected}\right] \leq \mathbb{P}\left[G(n, K_n, P_n) \text{ is } k\text{-connected}\right].$$

Therefore, the one-law proof will be completed upon showing

$$\lim_{n\to\infty}\mathbb{P}\left[G(n, \tilde{K}_n, \tilde{P}_n) \text{ is } k\text{-connected}\right] = 1.$$

Under (27) we have $\frac{\tilde{K}_n^2}{\tilde{P}_n} = O(\frac{\ln n}{n}) = o(1)$ since $\tilde{\alpha}_n = O(\ln n)$. It also follows that $\frac{\tilde{K}_n}{\tilde{P}_n} = o(1)$. In view of (22), we get

$$\tilde{p_s} = \frac{\ln n + (k-1)\ln\ln n + \tilde{\alpha}_n \pm o(1)}{n}, \quad n = 1, 2, \ldots,$$

and with $p_n = 1$ for all n sufficiently large, we obtain

$$\tilde{p_e} = \frac{\ln n + (k-1)\ln\ln n + \tilde{\alpha}_n \pm o(1)}{n}, \quad n = 1, 2, \ldots,$$

It is clear that $\lim_{n\to\infty}\tilde{\alpha}_n \pm o(1) = \infty$. Thus, we get the desired one-law by applying (12) of Theorem 1. ■

[4]Except Fact 1 and Lemmas 1-6, the statements of other facts and lemmas are all given in Appendix A.

D. Discussion and Comparison with Related Results

As already noted in the literature [3], [11], [12], [26], [27], [32], Erdős-Rényi graph $G(n,p_n)$ and random key graph $G(n,K_n,P_n)$ have similar k-connectivity properties when they are *matched* through their link probabilities; i.e. when $p_n = p_s$ with p_s as defined in (5). In particular, Erdős and Rényi [12] showed that if $p_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, then $G(n,p_n)$ is asymptotically almost surely k-connected (resp., not k-connected) if $\lim_{n\to\infty}\alpha_n = +\infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$). Also, Rybarczyk [27] has shown under some extra conditions ($P_n = \Theta(n^\xi)$ with $\xi > 1$) that if $p_s = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, then $G(n,K_n,P_n)$ is almost surely k-connected (resp., not k-connected) if $\lim_{n\to\infty}\alpha_n = +\infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$).

From our system model (viz. (3)), we have that

$$\mathbb{G}_{on} = G(n,K_n,P_n) \cap G(n,p_n). \tag{28}$$

Since $G(n,K_n,P_n)$ and $G(n,p_s)$ have similar k-connectivity results, it would seem intuitive to replace $G(n,K_n,P_n)$ with $G(n,p_s)$ in the above equation (28). Since $G(n,p_s)\cap G(n,p_n) = G(n,p_n p_s) = G(n,p_e)$, this would automatically imply Theorem 1 via the earlier results of Erdős and Rényi [12]. Note that from Erdős and Rényi's work [12], under (9), random graph $G(n,p_e)$ is asymptotically almost surely k-connected (resp., not k-connected) if $\lim_{n\to\infty}\alpha_n = +\infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$). In that regard, Theorem 1 confirms the validity of the above intuition.

We now compare our results with those of Rybarczyk [27] for the k-connectivity of random key graph $G(n,K_n,P_n)$. As already noted, Rybarczyk [27, Remark 1, p. 5] has established an analog of Corollary 2, but with conditions much *stronger* than ours. In particular, she assumed that $P_n = \Theta(n^\xi)$ with $\xi > 1$. In comparison, Corollary 2 established here enforces only that $P_n \geq \Omega(n)$, which is clearly a weaker condition than $P_n = \Theta(n^\xi)$ with $\xi > 1$. Moreover, our condition $P_n \geq \Omega(n)$ requires (from (25)) only that $K_n = \Omega(\sqrt{\ln n})$ for the one-law to hold. However, the condition $P_n = \Theta(n^\xi)$ with $\xi > 1$ enforced in [27] requires the key ring sizes to satisfy $K_n = \Omega(\sqrt{n^{\xi-1}\ln n})$ with $\xi - 1 > 0$; this is a much stronger requirement as compared to $K_n = \Omega(\sqrt{\ln n})$. This difference between the conditions on K_n is particularly relevant in the context of WSNs since the parameter K_n controls the number of keys kept in each sensor's memory. Since sensor nodes are expected [13] to have very limited memory (and computational capability), it is desirable to have small key ring sizes.

Finally, we compare Theorem 1 with the zero-one law given by Yağan [30] for the 1-connectivity of $\mathbb{G}_{on}$. As mentioned in Section II above, he shows that if

$$p_e \sim c\frac{\ln n}{n} = \frac{\ln n + (c-1)\ln n}{n} \tag{29}$$

then $\mathbb{G}_{on}$ is a.a.s. connected if $c > 1$, and it is a.a.s. not connected if $c < 1$. This was done under the additional conditions that $P_n = \Omega(n)$ (required only for the one-law) and that $\lim_{n\to\infty} p_n \ln n$ exists (required only for the zero-law). On the other hand, Theorem 1 given here establishes (by setting $k = 1$) that, if

$$p_e = \frac{\ln n + \alpha_n}{n} \tag{30}$$

then $\mathbb{G}_{on}$ is a.a.s. connected if $\lim_{n\to\infty}\alpha_n = \infty$, and it is a.a.s. not connected if $\lim_{n\to\infty}\alpha_n = -\infty$. This result relies on the extra conditions $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$ for the one-law and on $\frac{K_n^2}{P_n} = o(1)$ for the zero-law.

In a nutshell, our 1-connectivity result for $\mathbb{G}_{on}$ is somewhat more fine-grained than Yağan's [30] since a deviation of $\alpha_n = \pm\Omega(\ln n)$ is required to get the zero-one law in the form (29), whereas in our formulation (30), it suffices to have an unbounded deviation; e.g., even $\alpha_n = \pm \ln\ln\cdots\ln n$ will do. Put differently, we cover the case of $c = 1$ in (29) (i.e., the case when $p_e \sim \frac{\ln n}{n}$) and show that $\mathbb{G}_{on}$ could be almost surely connected or not connected, depending on the limit of α_n; in fact, if (29) holds with $c > 1$, we see from Theorem 1 that $\mathbb{G}_{on}$ is not only 1-connected but also k-connected for any $k = 1, 2, \ldots$. However, it is worth noting that the additional conditions assumed in [30] are *weaker* than those we enforce in Theorem 1 for $k = 1$.

V. Basic Ideas for Proving Theorem 1

A. The Relationship of k-Connectivity and the Minimum Node Degree

For any graph G, if G is k-connected, then the minimum node degree of G is no less than k [24]. This can be seen by contradiction. Suppose that the graph G is k-connected and there exists a node v with degree $d_v < k$. Then if we remove all of the d_v neighbors of the node v from G, the resulting graph will be disconnected since v will be isolated. However, this contradicts the k-connectivity of the original graph G and the claim follows. Therefore, we have

$$[G \text{ is } k\text{-connected}] \subseteq \begin{bmatrix} \text{Minimum node degree} \\ \text{of } G \text{ is no less than } k \end{bmatrix}$$

and the inequality

$$\mathbb{P}[G \text{ is } k\text{-connected}] \leq \mathbb{P}\begin{bmatrix} \text{Minimum node degree} \\ \text{of } G \text{ is no less than } k \end{bmatrix}$$

follows immediately.

It is now clear that (11) implies (10) and (12) implies (13). Thus, in order to prove Theorem 1, we only need to show (11) under the conditions of case (a), and (12) under the conditions of case (b).

B. Confining α_n

As seen in Section V-A, Theorem 1 will follow if we show (11) and (12) under the appropriate conditions. In this subsection, we show that the extra condition $\alpha_n = o(\ln n)$ can be introduced in the proof of (12). Namely, we will show that

$$\begin{aligned} &\text{part (b) of Theorem 1 under } \alpha_n = o(\ln n) \\ &\Rightarrow \text{part (b) of Theorem 1} \end{aligned} \tag{31}$$

We write $\mathbb{G}_{on}$ as $\mathbb{G}_{on}(n,K_n,P_n,p_n)$ and remember that given K_n, P_n and p_n, one can determine α_n from (9) with the help of (7).

Assume that part (b) of Theorem 1 holds under the extra condition $\alpha_n = o(\ln n)$. The desired result (31) will follow if we establish

$$\lim_{n\to\infty} \mathbb{P}\left[G(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n) \text{ is } k\text{-connected}\right] = 1 \tag{32}$$

for any $\tilde{K}_n$, $\tilde{P}_n$ and $\tilde{p}_n$ such that $\frac{\tilde{K}_n}{\tilde{P}_n} = o(1)$, $\tilde{P}_n = \Omega(n)$, and

$$\tilde{p}_e = \frac{\ln n + (k-1)\ln\ln n + \tilde{\alpha}_n}{n} \tag{33}$$

holds with $\lim_{n\to\infty} \tilde{\alpha}_n = +\infty$. We will prove (32) by a coupling argument. Namely, we will show that there exist scalings $\hat{K}_n$, $\hat{P}_n$ and $\hat{p}_n$ such that

$$\frac{\hat{K}_n}{\hat{P}_n} = o(1) \quad \text{and} \quad \hat{P}_n = \Omega(n) \tag{34}$$

and

$$\hat{p}_e = \frac{\ln n + (k-1)\ln\ln n + \hat{\alpha}_n}{n} \tag{35}$$

with

$$\hat{\alpha}_n = o(\ln n) \quad \text{and} \quad \lim_{n\to\infty} \hat{\alpha}_n = \infty, \tag{36}$$

and that we have

$$\begin{aligned} &\mathbb{P}[\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n) \text{ is } k\text{-connected }] \\ &\geq \mathbb{P}[\mathbb{G}_{on}(n, \hat{K}_n, \hat{P}_n, \hat{p}_n) \text{ is } k\text{-connected }]. \end{aligned} \tag{37}$$

Notice that $\hat{K}_n$, $\hat{P}_n$ and $\hat{p}_n$ satisfy all the conditions enforced by part (b) of Theorem 1 together with the extra condition $\hat{\alpha}_n = o(\ln n)$. Thus, we get

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{G}_{on}(n, \hat{K}_n, \hat{P}_n, \hat{p}_n) \text{ is } k\text{-connected }] = 1 \tag{38}$$

by the initial assumption, and (32) follows immediately from (37) and (38). Therefore, given any $\tilde{K}_n$, $\tilde{P}_n$ and $\tilde{p}_n$ as stated above, if we can show the existence of $\hat{K}_n$, $\hat{P}_n$ and $\hat{p}_n$ that satisfy (34)-(37), then the desired conclusion (31) will follow.

We now establish the existence of $\hat{K}_n$, $\hat{P}_n$ and $\hat{p}_n$ that satisfy (34)-(37). Let $\hat{P}_n = \tilde{P}_n$ and $\hat{K}_n = \tilde{K}_n$ so that (34) is satisfied automatically. Let $\hat{\alpha}_n = \min\{\tilde{\alpha}_n, \ln\ln n\}$. Hence, we have $\hat{\alpha}_n \leq \tilde{\alpha}_n$, $\hat{\alpha}_n = o(\ln n)$ and $\lim_{n\to\infty} \hat{\alpha}_n = +\infty$ so that (36) is also satisfied. The remaining parameter $\hat{p}_n$ will be defined through

$$\hat{p}_n \cdot \left[1 - \frac{\binom{\hat{P}_n - \hat{K}_n}{\hat{K}_n}}{\binom{\hat{P}_n}{\hat{K}_n}}\right] = \frac{\ln n + (k-1)\ln\ln n + \hat{\alpha}_n}{n} \tag{39}$$

so that $\hat{p}_e = \hat{p}_n \cdot \left[1 - \frac{\binom{\hat{P}_n - \hat{K}_n}{\hat{K}_n}}{\binom{\hat{P}_n}{\hat{K}_n}}\right]$ satisfies (35). Thus, it remains to establish (37).

Comparing (39) with (33), it follows that $\hat{p}_n \leq \tilde{p}_n$ since $\hat{K}_n = \tilde{K}_n$, $\hat{P}_n = \tilde{P}_n$ and $\hat{\alpha}_n \leq \tilde{\alpha}_n$. Consider graphs $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n)$, $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n)$ that have the same number of nodes n, the same key ring size $\tilde{K}_n$ and the same key pool size $\tilde{P}_n$, but have different channel probabilities $\tilde{p}_n$ and $\hat{p}_n$. We will show that there exists a coupling such that $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n)$ is a spanning *subgraph* of $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n)$ so that, as shown by Rybarczyk [27, pp. 7], we have

$$\begin{aligned} &\mathbb{P}[\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n) \text{ has property } \mathscr{P}] \\ &\leq \mathbb{P}[\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n) \text{ has property } \mathscr{P}]. \end{aligned} \tag{40}$$

for any monotone increasing[5] graph property $\mathscr{P}$. It is straightforward to see that the property of being k-connected and the property that the minimum node degree is no less than k are both monotone increasing graph properties. Therefore, (37) will follow immediately (with $\hat{K}_n = \tilde{K}_n$ and $\hat{P}_n = \tilde{P}_n$) if (40) holds.

We now give the coupling argument that leads to (40). As seen from (3), $\mathbb{G}_{on}$ is the intersection of a random key graph $G(n, K_n, P_n)$ and an Erdős-Rényi graph $G(n, p_n)$. Using graph coupling, we use the same random key graph $G(n, \tilde{K}_n, \tilde{P}_n)$ to help construct both $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n)$ and $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n)$. Then we have

$$\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n) = G(n, \tilde{K}_n, \tilde{P}_n) \cap G(n, \tilde{p}_n) \tag{41}$$

$$\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n) = G(n, \tilde{K}_n, \tilde{P}_n) \cap G(n, \hat{p}_n). \tag{42}$$

Since $\hat{p}_n \leq \tilde{p}_n$, we couple $G(n, \hat{p}_n)$ and $G(n, \tilde{p}_n)$ in the following manner. Pick independent Erdős-Rényi graphs $G(n, \hat{p}_n/\tilde{p}_n)$ and $G(n, \tilde{p}_n)$ on the same vertex set. It is clear that the intersection $G(n, \hat{p}_n/\tilde{p}_n) \cap G(n, \tilde{p}_n)$ will still be an Erdős-Rényi graph (due to independence) with an edge probability given by $\tilde{p}_n \cdot \frac{\hat{p}_n}{\tilde{p}_n} = \hat{p}_n$. In other words, we have $G(n, \hat{p}_n/\tilde{p}_n) \cap G(n, \tilde{p}_n) = G(n, \hat{p}_n)$. Consequently, under this coupling, $G(n, \hat{p}_n)$ is a spanning subgraph of $G(n, \tilde{p}_n)$. Then from (41) and (42), $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \hat{p}_n)$ is a spanning subgraph of $\mathbb{G}_{on}(n, \tilde{K}_n, \tilde{P}_n, \tilde{p}_n)$ and (40) follows.

C. The Method of First and Second Moments

We present the following fact which uses the method of evaluating the first and second moments to derive the zero-one laws for the minimum node degree of a graph. We use $\mathbb{E}[\cdot]$ to denote the expected value of the random variable in $[\cdot]$.

Fact 1. *For any graph G with n nodes, let X_ℓ be the number of nodes having degree ℓ in G, where $\ell = 0, 1, \ldots, n-1$; and let δ be the minimum node degree of G. Then the following three properties hold for any positive integer k.*

(a) For any non-negative integer ℓ, if $\mathbb{E}[X_\ell] = o(1)$, then

$$\lim_{n\to\infty} \mathbb{P}[\delta = \ell] = 0. \tag{43}$$

(b) If (43) holds for $\ell = 0, 1, \ldots, k-1$, then

$$\lim_{n\to\infty} \mathbb{P}[\delta \geq k] = 1.$$

(c) If $\mathbb{E}\left[\left(X_\ell\right)^2\right] \sim \left\{\mathbb{E}\left[X_\ell\right]\right\}^2$ and $\mathbb{E}\left[X_\ell\right] \to +\infty$ as $n \to \infty$ hold for some $\ell = 0, 1, \ldots, k-1$, then

$$\lim_{n\to\infty} \mathbb{P}[\delta \geq k] = 0.$$

A proof of Fact 1 is given in Appendix B-A.

[5] A graph property is called monotone increasing if it holds under the addition of edges in a graph.

VI. Establishing (11) (The Zero-Law for the Minimum Node Degree in $\mathbb{G}_{on}$)

Our main goal in this section is to establish (11) under the following conditions:

$$(9), K_n \geq 2 \text{ for all } n \text{ sufficiently large }, \frac{K_n^2}{P_n} = o(1) \quad (44)$$

$$\lim_{n\to+\infty} \alpha_n = -\infty \text{ and } p_e n > \epsilon > 0 \text{ or } \lim_{n\to\infty} p_e n = 0. \quad (45)$$

From property (c) of Fact 1, we see that the proof will be completed if we demonstrate the following two results under the conditions (44) and (45):

$$\lim_{n\to\infty} \mathbb{E}\big[X_\ell\big] = +\infty, \quad (46)$$

and

$$\mathbb{E}\left[\left(X_\ell\right)^2\right] \sim \left\{\mathbb{E}\big[X_\ell\big]\right\}^2. \quad (47)$$

for some $\ell = 0, 1, \ldots, k-1$.

The first step in establishing (46) and (47) is to compute the moments $\mathbb{E}\left[X_\ell\right]$ and $\mathbb{E}\left[\left(X_\ell\right)^2\right]$. This step is taken in the next Lemma. Recall that in graph $\mathbb{G}_{on}$, X_ℓ stands for the number of nodes with degree ℓ for each $\ell = 0, 1, \ldots$. Also, $D_{x,\ell}$ is the event that node v_x has degree ℓ for each $x = 1, 2, \ldots, n$.

Lemma 1. *In $\mathbb{G}_{on}$, for any non-negative integer ℓ and any two distinct nodes v_x and v_y, we have*

$$\mathbb{E}\big[X_\ell\big] = n\mathbb{P}\left[D_{x,\ell}\right], \quad (48)$$

$$\mathbb{E}\left[\left(X_\ell\right)^2\right] = n\mathbb{P}\left[D_{x,\ell}\right] + n(n-1)\mathbb{P}\left[D_{x,\ell} \bigcap D_{y,\ell}\right]. \quad (49)$$

A proof of Lemma 1 is given in Appendix C-A.

In view of (48), we will obtain (46) once we show that

$$\lim_{n\to+\infty} \left(n\mathbb{P}\left[D_{x,\ell}\right]\right) = +\infty. \quad (50)$$

under the conditions (44) and (45). Also, from (48) and (49), we get

$$\frac{\mathbb{E}\left[\left(X_\ell\right)^2\right]}{\left\{\mathbb{E}\big[X_\ell\big]\right\}^2} = \frac{1}{n\mathbb{P}\left[D_{x,\ell}\right]} + \frac{n-1}{n} \cdot \frac{\mathbb{P}\left[D_{x,\ell} \bigcap D_{y,\ell}\right]}{\left\{\mathbb{P}\left[D_{x,\ell}\right]\right\}^2}. \quad (51)$$

Thus, (47) will follow upon showing (50) and

$$\mathbb{P}\left[D_{x,\ell} \bigcap D_{y,\ell}\right] \sim \left\{\mathbb{P}\left[D_{x,\ell}\right]\right\}^2 \quad (52)$$

for some $\ell = 0, 1, \ldots, k-1$ under the conditions (44) and (45).

We establish (50) and (52) with the help of the following Lemmas 2 and 3.

Lemma 2. *If $p_e = o\left(\frac{1}{\sqrt{n}}\right)$, then for any non-negative integer constant ℓ and any node v_x,*

$$\mathbb{P}\left[D_{x,\ell}\right] \sim (\ell!)^{-1} \left(p_e n\right)^\ell e^{-p_e n}. \quad (53)$$

A proof of Lemma 2 is given in Appendix C-B.

Lemma 3. *Let $p_s = o(1)$, $K_n \geq 2$ for all n sufficiently large, $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = -\infty$. Then, properties (a) and (b) below hold.*

(a) If there exist an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, then for any non-negative integer constant ℓ and any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] \sim (\ell!)^{-2} \left(p_e n\right)^{2\ell} e^{-2p_e n}. \quad (54)$$

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

$$\mathbb{P}\left[D_{x,0} \cap D_{y,0}\right] \sim e^{-2p_e n}. \quad (55)$$

Proof. Recall that E_{xy} is the event that there exists a link between nodes v_x and v_y. Then

$$\begin{aligned}&\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] \\ &= \mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}] + \mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}]. \end{aligned} \quad (56)$$

Thus, Lemma 3 will follow after we prove the following two propositions.

Proposition 1. *Let $p_s = o(1)$, $K_n \geq 2$ for all n sufficiently large and $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = -\infty$. Then, the following two properties hold.*

(a) If there exist an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, then for any non-negative integer constant ℓ, we have

$$\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}] \sim (\ell!)^{-2} \left(p_e n\right)^{2\ell} e^{-2p_e n}. \quad (57)$$

(b) We have

$$\mathbb{P}[D_{x,0} \cap D_{y,0} \cap \overline{E_{xy}}] \sim e^{-2p_e n}. \quad (58)$$

Proposition 2. *Let $p_s = o(1)$, $K_n \geq 2$ for all n sufficiently large and $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = -\infty$. If there exists an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, then for any positive integer constant ℓ, we have*

$$\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}] = o\left(\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}]\right). \quad (59)$$

Propositions 1 and 2 are established in Section VII and Section VIII, respectively. Now, we complete the proof of Lemma 3 . It is clear that under the condition $p_e n > \epsilon > 0$, (54) follows from (57) and (59) in view of (56). For the case $\ell = 0$, we obtain (55) by using (58) in (56) and noting that $\mathbb{P}[D_{x,0} \cap D_{y,0} \cap E_{xy}] = 0$ always holds; it is not possible for nodes v_x and v_y to have degree zero and yet to have an edge in between. ■

We now complete the proof of (50) and (52) under (44) and (45). First, in view of (9) and the condition $\lim_{n\to\infty} \alpha_n = -\infty$, we obtain $p_e \leq \frac{\ln n + (k-1)\ln\ln n}{n}$ for all n sufficiently large. Thus, $p_e = o\left(\frac{1}{\sqrt{n}}\right)$, and we use Lemma 2 to get

$$n\mathbb{P}\left[D_{x,\ell}\right] \sim n \cdot (\ell!)^{-1} \left(p_e n\right)^\ell e^{-p_e n} \quad (60)$$

for each $\ell = 0, 1, \ldots$. The proof will be given in two steps. First, in the case where there exists an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, we will establish (50) and (52) for $\ell = k-1$. Next, for the case where $\lim_{n\to\infty} p_e n = 0$, we will show that (50) and (52) hold for $\ell = 0$.

Assume now that $p_e n > \epsilon > 0$ for all n sufficiently large. Substituting (9) into (60) with $\ell = k-1$, we get

$$\begin{aligned} &n\mathbb{P}\left[D_{x,k-1}\right] \qquad (61)\\ &\sim n \cdot \left[(k-1)!\right]^{-1} \left(p_e n\right)^{k-1} e^{-\ln n - (k-1)\ln\ln n - \alpha_n} \\ &= \left[(k-1)!\right]^{-1} \\ &\quad \times \left(\ln n + (k-1)\ln\ln n + \alpha_n\right)^{k-1} e^{-(k-1)\ln\ln n - \alpha_n}. \end{aligned}$$

Let

$$\begin{aligned} &f_n(k;\alpha_n) \\ &\quad := \left(\ln n + (k-1)\ln\ln n + \alpha_n\right)^{k-1} e^{-(k-1)\ln\ln n - \alpha_n}, \end{aligned}$$

and observe that we have $\ln n + (k-1)\ln\ln n + \alpha_n \geq \epsilon$ for all n sufficiently large since $p_e n > \epsilon$. On that range, fix n, pick $0 < \gamma < 1$ and consider the cases $\alpha_n \leq -(1-\gamma)\ln n$ and $\alpha_n > -(1-\gamma)\ln n$. In the former case, we have

$$f_n(k;\alpha_n) \geq \epsilon \cdot e^{-(k-1)\ln\ln n + (1-\gamma)\ln n},$$

whereas in the latter we obtain

$$f_n(k;\alpha_n) \geq \left(\gamma \ln n\right)^{k-1} e^{-(k-1)\ln\ln n - \alpha_n} = \gamma^{k-1} e^{-\alpha_n}.$$

Thus, for all n sufficiently large, we have

$$f_n(k;\alpha_n) \geq \min\left\{\epsilon \cdot e^{-(k-1)\ln\ln n + (1-\gamma)\ln n}, \gamma^{k-1} e^{-\alpha_n}\right\}.$$

It is now easy to see that $\lim_{n\to\infty} f_n(k;\alpha_n) = \infty$ since $0 < \gamma < 1$ and $\lim_{n\to\infty} \alpha_n = -\infty$. Substituting this into (61), we obtain (50) with $\ell = k-1$. In addition, from (53) of Lemma 2, and (54) of Lemma 3, it is clear that (52) follows with $\ell = k-1$. As mentioned already, (50) and (52) imply (46) and (47) in view of Lemma 1, and the zero-law (11) is now established for the case when $p_e n > \epsilon > 0$.

We now turn to the case where $\lim_{n\to\infty} p_e n = p_e^\star = 0$. This time, we let $\ell = 0$ in (60) and obtain

$$n\mathbb{P}\left[D_{x,0}\right] \sim n e^{-2p_e n} \sim n.$$

We clearly have (50) for $\ell = 0$. Also, from (53) of Lemma 2 with $\ell = 0$, and (55) of Lemma 3, we obtain (52) for $\ell = 0$. Having obtained (50) and (52) for $\ell = 0$, we get (46) and (47) and the zero-law (11) is now established by virtue of Fact 1 (c). ■

VII. A Proof of Proposition 1

We start by noting that $D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}$ stands for the event that nodes v_x and v_y both have ℓ neighbors but are not neighbors with each other. To compute its probability, we specify all the possible cardinalities of sets N_{xy}, $N_{x\overline{y}}$ and $N_{\overline{x}y}$, defined in Section III-B. In other words, we specify the number of nodes that are neighbors of both v_x and v_y, the number of nodes that are neighbors of v_x but not neighbors of v_y, and the number of nodes that are neighbors of v_y but not neighbors of v_x. To this end, we define the series of events A_h in the following manner

$$A_h = \left[|N_{xy}| = h\right] \bigcap \left[|N_{x\overline{y}}| = \ell - h\right] \bigcap \left[|N_{\overline{x}y}| = \ell - h\right] \quad (62)$$

for each $h = 0, 1, \ldots, \ell$; here, $|S|$ denotes the cardinality of the discrete set S.

It is now a simple matter to check that

$$D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}} = \bigcup_{h=0}^{\ell} \left(A_h \cap \overline{E_{xy}}\right). \qquad (63)$$

for each $\ell = 0, 1, \ldots$. Using (63) and the fact that the events A_h ($h = 0, 1, \ldots, \ell$) are mutually exclusive, we obtain

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] = \sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{E_{xy}}\right]. \qquad (64)$$

We begin computing the right hand side (R.H.S.) of (64) by evaluating $\overline{E_{xy}}$, i.e., the event that there is no link between nodes v_x and v_y. From our system model (viz. (2)) we have $E_{xy} = K_{xy} \cap C_{xy}$. Hence

$$\overline{E_{xy}} = \overline{K_{xy}} \cup \overline{C_{xy}} = \overline{K_{xy}} \cup (K_{xy} \cap \overline{C_{xy}}). \qquad (65)$$

Note that, by definition, events K_{xy} and $|S_{xy}| \geq 1$ are equivalent. Also, we always have $|S_{xy}| \leq |S_x| = K_n$. Hence, we get

$$K_{xy} = \bigcup_{u=1}^{K_n} (|S_{xy}| = u). \qquad (66)$$

For each $u = 1, 2, \ldots, K_n$, we define event $\mathcal{X}_u$ as follows:

$$\mathcal{X}_u = (|S_{xy}| = u) \cap \overline{C_{xy}} \qquad (67)$$

Applying (66) to (65) and using (67), we obtain

$$\begin{aligned} \overline{E_{xy}} &= \overline{K_{xy}} \cup \left\{\left[\bigcup_{u=1}^{K_n} (|S_{xy}| = u)\right] \cap \overline{C_{xy}}\right\} \\ &= \overline{K_{xy}} \cup \left(\bigcup_{u=1}^{K_n} \mathcal{X}_u\right). \qquad (68) \end{aligned}$$

From (68) and the fact that the events $\overline{K_{xy}}, \mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_{K_n}$ are mutually disjoint, we obtain

$$\mathbb{P}\left[A_h \cap \overline{E_{xy}}\right] = \mathbb{P}\left[A_h \cap \overline{K_{xy}}\right] + \sum_{u=1}^{K_n} \mathbb{P}\left[A_h \cap \mathcal{X}_u\right]. \qquad (69)$$

Substituting (69) into (64), we get

$$\begin{aligned} &\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell} \cap \overline{E_{xy}}\right] \\ &= \sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}}\right] + \sum_{h=0}^{\ell} \sum_{u=1}^{K_n} \mathbb{P}\left[A_h \cap \mathcal{X}_u\right]. \qquad (70) \end{aligned}$$

Proposition 1 will follow once we establish the next two results.

Proposition 1.1. *Let ℓ be a non-negative integer constant. If $p_s = o(1)$, $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = -\infty$, then*

$$\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}}\right] \sim (\ell!)^{-2} \left(p_e n\right)^{2\ell} e^{-2p_e n}. \qquad (71)$$

Proposition 1.2. *Let ℓ be a non-negative integer constant. Consider $p_s = o(1)$, $K_n \geq 2$ for all n sufficiently large and $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = -\infty$. Then, the following two properties hold.*

(a) If there exists an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, then we have

$$\sum_{h=0}^{\ell}\sum_{u=1}^{K_n}\mathbb{P}\left[A_h \cap \mathcal{X}_u\right] = o\left(\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \cap \overline{K_{xy}}\right]\right). \tag{72}$$

(b) We have

$$\sum_{u=1}^{K_n}\mathbb{P}\left[A_0 \cap \mathcal{X}_u\right] = o\left(\mathbb{P}\left[A_0 \cap \overline{K_{xy}}\right]\right). \tag{73}$$

In order to see why Proposition 1 is established by Propositions 1.1 and 1.2, consider p_s and p_e as stated in Proposition 1. Then from Propositions 1.1 and 1.2, (71) and (72) hold. Substituting (71) and (72) into (70), we get (57). Also, using (71) with $\ell = 0$ we get $\mathbb{P}\left[A_0 \cap \overline{K_{xy}}\right] \sim e^{-2p_e n}$. Using this and (73) in (70) with $\ell = 0$, we obtain (58) and Proposition 1 is then established. ■

The rest of this section is devoted to establishing Propositions 1.1 and 1.2. We will establish Proposition 2 in the next Section VIII, and this will complete the proof of Lemma 3 and thus the zero-law (11).

A. A Proof of Proposition 1.1

Given $\mathbb{P}[\overline{K_{xy}}] = 1 - p_s \to 1$ as $n \to \infty$, it is clear that

$$\begin{aligned}\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \cap \overline{K_{xy}}\right] &= \mathbb{P}[\overline{K_{xy}}]\cdot\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right] \\ &\sim \sum_{h=0}^{\ell}\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right]\end{aligned} \tag{74}$$

We now present the following Lemma 4, which evaluates a generalization of $\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right]$. In addition to the proof of Proposition 1.1 here, the proofs of Propositions 1.2 and 2.1 also use Lemma 4.

Lemma 4. *Let m_1, m_2 and m_3 be non-negative integer constants. We define event $\mathcal{F}$ as follows.*

$$\mathcal{F} := [|N_{xy}| = m_1]\bigcap[|N_{x\overline{y}}| = m_2]\bigcap[|N_{\overline{x}y}| = m_3]. \tag{75}$$

Then given u in $\{0, 1, \ldots, K_n\}$ and $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty}\alpha_n = -\infty$, we have

$$\begin{aligned}\mathbb{P}\left[\mathcal{F} \mid (|S_{xy}| = u)\right] \sim\ & \frac{n^{m_1+m_2+m_3}}{m_1!m_2!m_3!}\cdot e^{-2p_e n + \frac{p_e p_n u}{K_n}n} \\ &\times\{\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)]\}^{m_1} \\ &\times\{\mathbb{P}[E_{xj\cap\overline{yj}} \mid (|S_{xy}| = u)]\}^{m_2} \\ &\times\{\mathbb{P}[E_{\overline{xj}\cap yj} \mid (|S_{xy}| = u)]\}^{m_3}\end{aligned} \tag{76}$$

with j distinct from x and y.

A proof of Lemma 4 is given in Appendix C-C.

Given the definition of A_h in (62) and $\overline{K_{xy}} \Leftrightarrow (|S_{xy}| = 0)$, we let $m_1 = h, m_2 = m_3 = \ell - h$ and $u = 0$ in Lemma 4 in order to compute $\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right]$. We get

$$\begin{aligned}&\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right] \\ &\sim \frac{n^{2\ell-h}}{h![(\ell-h)!]^2}\cdot e^{-2p_e n}\cdot\left\{\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}]\right\}^h \\ &\quad\times\{\mathbb{P}[E_{\overline{xj}\cap yj} \mid \overline{K_{xy}}]\}^{\ell-h}\{\mathbb{P}[E_{xj\cap\overline{yj}} \mid \overline{K_{xy}}]\}^{\ell-h}.\end{aligned} \tag{77}$$

In order to compute the R.H.S. of (77), we evaluate the following three terms in turn:

$$\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}], \mathbb{P}[E_{xj\cap\overline{yj}} \mid \overline{K_{xy}}], \text{ and } \mathbb{P}[E_{\overline{xj}\cap yj} \mid \overline{K_{xy}}].$$

For the first term $\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}]$, we use $E_{xj} = K_{xj} \cap C_{xj}$ and $E_{yj} = K_{yj} \cap C_{yj}$ to obtain

$$\begin{aligned}&\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}] \\ &= \mathbb{P}[(C_{xj} \cap C_{yj}) \cap (K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}].\end{aligned} \tag{78}$$

Since $C_{xj} \cap C_{yj}$ is independent of both $K_{xj} \cap K_{yj}$ and $\overline{K_{xy}}$, and C_{xj} and C_{yj} are independent, we obtain from (78) that

$$\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}] = {p_n}^2\cdot\mathbb{P}[K_{xj} \cap K_{yj} \mid \overline{K_{xy}}] \tag{79}$$

as we recall that $\mathbb{P}[C_{xj}] = \mathbb{P}[C_{yj}] = p_n$ from our system model (viz. (1)). From Lemma 9 (Appendix A-B), we have $\mathbb{P}[(K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}] \leq p_s^2$. Substituting this into (79) and using the definition $p_e = p_n p_s$, we get

$$\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}] \leq {p_e}^2. \tag{80}$$

We now evaluate the second term $\mathbb{P}[E_{xj\cap\overline{yj}} \mid \overline{K_{xy}}]$ by first computing $\mathbb{P}[E_{xj} \mid \overline{K_{xy}}]$. It is clear that E_{xj} is independent of $\overline{K_{xy}}$. Hence,

$$\mathbb{P}[E_{xj} \mid \overline{K_{xy}}] = p_e. \tag{81}$$

Since $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty}\alpha_n = -\infty$, we have $p_e = o\left(\frac{1}{\sqrt{n}}\right)$. From (80), (81) and $p_e = o\left(\frac{1}{\sqrt{n}}\right)$, we now get

$$\begin{aligned}\mathbb{P}[E_{xj\cap\overline{yj}} \mid \overline{K_{xy}}] &= \mathbb{P}[E_{xj} \mid \overline{K_{xy}}] - \mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}] \\ &= p_e - O\left({p_e}^2\right) \sim p_e.\end{aligned} \tag{82}$$

Proceeding similarly, for the third term $\mathbb{P}[E_{\overline{xj}\cap yj} \mid \overline{K_{xy}}]$, we have

$$\mathbb{P}[E_{\overline{xj}\cap yj} \mid \overline{K_{xy}}] \sim p_e. \tag{83}$$

Now we compute the R.H.S. of (77). Substituting (82) and (83) into R.H.S. of (77), given constant ℓ, we obtain

$$\begin{aligned}&\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right] \\ &\sim \frac{n^{2\ell-h}}{h![(\ell-h)!]^2}\cdot e^{-2p_e n}\cdot\left\{\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}]\right\}^h\cdot p_e^{2(\ell-h)}.\end{aligned} \tag{84}$$

for each $h = 0, 1, \ldots, \ell$. Thus, for $h = 0$, we have

$$\mathbb{P}\left[A_0 \mid \overline{K_{xy}}\right] \sim (\ell!)^{-2}(p_e n)^{2\ell}e^{-2p_e n}. \tag{85}$$

For $h = 1, 2, \ldots, \ell$, we use (80) and (84) to get

$$\begin{aligned}\frac{\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right]}{\mathbb{P}\left[A_0 \mid \overline{K_{xy}}\right]} &\sim \frac{n^{-h}(\ell!)^2}{h![(\ell-h)!]^2}\left\{\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}]\right\}^h p_e^{-2h} \\ &\leq \frac{n^{-h}(\ell!)^2}{h![(\ell-h)!]^2} = o(1).\end{aligned}$$

Thus, we have

$$\mathbb{P}\left[A_h \mid \overline{K_{xy}}\right] = o\left(\mathbb{P}\left[A_0 \mid \overline{K_{xy}}\right]\right), \quad h = 1, 2, \ldots, \ell. \quad (86)$$

Applying (85) and (86) to (74), we obtain the desired conclusion (71) (for Propostion 1.1) by virtue of the fact that ℓ is constant. ■

B. A Proof of Proposition 1.2

Notice that (73) can be obtained from (72) by setting $\ell = 0$. Thus, in the discussion given below, we will establish (72) for each $\ell = 0, 1, \ldots$ under the condition that there exist an $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, and show that this extra condition is *not* needed if $\ell = 0$.

We start by finding an upper bound on the left hand side (L.H.S.) of (72). Given the definition of $\mathcal{X}_u$ in (67), we obtain

$$\mathbb{P}\left[A_h \cap \mathcal{X}_u\right] \leq \mathbb{P}\left[A_h \cap (|S_{xy}| = u)\right].$$

Then, we have

$$\begin{aligned}
&\sum_{h=0}^{\ell}\sum_{u=1}^{K_n}\mathbb{P}\left[A_h \cap \mathcal{X}_u\right] \\
&\leq \sum_{h=0}^{\ell}\sum_{u=1}^{K_n}\mathbb{P}\left[A_h \cap (|S_{xy}| = u)\right] \\
&= \sum_{u=1}^{K_n}\left\{\mathbb{P}[|S_{xy}| = u]\cdot\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \mid (|S_{xy}| = u)\right]\right\}. \quad (87)
\end{aligned}$$

We now compute the R.H.S. of (87). First, from Lemma 10, we note that

$$\mathbb{P}[|S_{xy}| = u] \leq \frac{1}{u!}\left(\frac{K_n^2}{P_n - K_n}\right)^u. \quad (88)$$

Next, we compute $\mathbb{P}\left[A_h \mid (|S_{xy}| = u)\right]$. Given the definition of A_h in (62), we let $m_1 = h$ and $m_2 = m_3 = \ell - h$ in Lemma 4 and obtain

$$\begin{aligned}
\mathbb{P}\left[A_h \mid (|S_{xy}| = u)\right] \sim\ & \frac{n^{2\ell-h}}{h![(\ell-h)!]^2}\cdot e^{-2p_e n + \frac{p_e p_n u}{K_n}n} \\
&\times\left\{\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)]\right\}^h \\
&\times\left\{\mathbb{P}[E_{\overline{xj}\cap yj} \mid (|S_{xy}| = u)]\right\}^{\ell-h} \\
&\times\left\{\mathbb{P}[E_{xj\cap\overline{yj}} \mid (|S_{xy}| = u)]\right\}^{\ell-h}. \quad (89)
\end{aligned}$$

We evaluate the following three terms in turn:

$$\mathbb{P}[E_{xj\cap yj} \mid \overline{K_{xy}}], \mathbb{P}[E_{xj\cap\overline{yj}} \mid \overline{K_{xy}}], \text{ and } \mathbb{P}[E_{\overline{xj}\cap yj} \mid \overline{K_{xy}}].$$

From $E_{xj} = C_{xj} \cap K_{xj}$ and $E_{yj} = C_{yj} \cap K_{yj}$, it is clear that E_{xj} and E_{yj} are both independent of $(|S_{xy}| = u)$.Then using crude bounding arguments, we obtain

$$\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)] \leq \mathbb{P}[E_{xj} \mid (|S_{xy}| = u)] = p_e \quad (90)$$

$$\mathbb{P}[E_{xj\cap\overline{yj}} \mid (|S_{xy}| = u)] \leq \mathbb{P}[E_{xj} \mid (|S_{xy}| = u)] = p_e \quad (91)$$

$$\mathbb{P}[E_{\overline{xj}\cap yj} \mid (|S_{xy}| = u)] \leq \mathbb{P}[E_{yj} \mid (|S_{xy}| = u)] = p_e. \quad (92)$$

Applying (90), (91) and (92) to (89), we obtain

$$\begin{aligned}
\mathbb{P}\left[A_h \mid (|S_{xy}| = u)\right] &\leq 2n^{2\ell-h}\cdot e^{-2p_e n + \frac{p_e p_n n u}{K_n}}\cdot(p_e)^{2\ell-h} \\
&= 2e^{-2p_e n + \frac{p_e p_n n u}{K_n}}\left(p_e n\right)^{2\ell-h} \quad (93)
\end{aligned}$$

for all n sufficiently large.

Returning to the evaluation of R.H.S. of (87), we apply (93) to (87) and obtain

$$\begin{aligned}
&\sum_{h=0}^{\ell}\sum_{u=1}^{K_n}\mathbb{P}\left[A_h \cap \mathcal{X}_u\right] \\
&\leq \sum_{u=1}^{K_n}\left\{\mathbb{P}[|S_{xy}| = u]\cdot 2e^{-2p_e n + \frac{p_n u}{K_n}\cdot p_e n}\cdot\sum_{h=0}^{\ell}\left(p_e n\right)^{2\ell-h}\right\} \\
&\hfill (94)
\end{aligned}$$

for all n sufficiently large. Given (94), it is clear that (72) follows once we prove

$$\text{R.H.S. of (94)} = o\left(\sum_{h=0}^{\ell}\mathbb{P}\left[A_h \cap \overline{K_{xy}}\right]\right). \quad (95)$$

Using the condition that $p_e n > \epsilon > 0$ for all n sufficiently large, it follows that

$$\sum_{h=0}^{\ell}\left(p_e n\right)^{2\ell-h} = O\left(p_e n\right)^{2\ell}. \quad (96)$$

Notice that (96) follows trivially for $\ell = 0$ without relying on the condition $p_e n > \epsilon > 0$. Applying (88) and (96) to R.H.S. of (94), we get

$$\begin{aligned}
&\text{R.H.S. of (94)} \\
&= O(1)\cdot\left(p_e n\right)^{2\ell}e^{-2p_e n}\cdot\sum_{u=1}^{K_n}\left(\frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n}{K_n}\cdot p_e n}\right)^u. \\
&\hfill (97)
\end{aligned}$$

From (71) and (97), we have

$$\begin{aligned}
&\text{R.H.S. of (94)} \\
&= \sum_{h=0}^{\ell}\mathbb{P}\left[A_h \cap \overline{K_{xy}}\right]\cdot O((\ell!)^2)\cdot\sum_{u=1}^{K_n}\left(\frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n p_e n}{K_n}}\right)^u. \\
&\hfill (98)
\end{aligned}$$

If we show that

$$\frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n}{K_n}\cdot p_e n} = o(1), \quad (99)$$

then we obtain

$$\sum_{u=1}^{K_n}\left(\frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n p_e n}{K_n}}\right)^u \leq \frac{\frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n}{K_n}\cdot p_e n}}{1 - \frac{K_n^2}{P_n - K_n}\cdot e^{\frac{p_n}{K_n}\cdot p_e n}} = o(1), \quad (100)$$

leading to (72) given (98) and the fact that ℓ is constant. Now we prove (99). Given $p_e = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty}\alpha_n = -\infty$ we have $p_e \leq \frac{3}{2}\cdot\frac{\ln n}{n}$ for all sufficiently large n. Recalling also that $K_n \geq 2$, we get

$$e^{\frac{p_n p_e n}{K_n}} \leq e^{\frac{3}{4}p_n \ln n}. \quad (101)$$

on the same range. From Lemma 8, property (c) (Appendix A-B), it holds under $p_s = o(1)$ that $p_s \sim \frac{K_n^2}{P_n}$ so that $\frac{K_n^2}{P_n} = o(1)$ and $\frac{K_n}{P_n} = o(1)$. We now obtain

$$\frac{K_n^2}{P_n - K_n} \sim \frac{K_n^2}{P_n} \sim p_s.$$

Then $\frac{K_n^2}{P_n - K_n} \leq 2p_s$ follows for all n sufficiently large. In view of this inequality and (101), we find

$$\frac{K_n^2}{P_n - K_n} \cdot e^{\frac{p_n}{K_n} \cdot p_e n} \leq 2p_s \cdot e^{\frac{3}{4} p_n \ln n} \tag{102}$$

for all n sufficiently large.

In order to evaluate the R.H.S. of (102), we define

$$F(n) = 2p_s \cdot e^{\frac{3}{4} p_n \ln n}. \tag{103}$$

With $p_n p_s = p_e \leq \frac{3}{2} \cdot \frac{\ln n}{n}$ for all n sufficiently large, we note that

$$p_s \leq \frac{3}{2} \frac{\ln n}{n p_n}. \tag{104}$$

Now, fix n large enough such that (102) and (104) hold. We consider the cases $p_n \leq \frac{1}{\ln n}$ and $p_n > \frac{1}{\ln n}$, separately. In the former case, we have $F(n) \leq 2p_s e^{3/4}$ immediately from (103). In the latter case we use the bound (104) to get

$$F(n) \leq 3 \frac{\ln n}{n p_n} e^{\frac{3}{4} p_n \ln n} < 3 \frac{(\ln n)^2}{n} \cdot n^{3/4}$$

upon noting also that $p_n \leq 1$. Combining the two bounds, we have that

$$F(n) \leq \max \left\{ 2p_s e^{3/4} \,,\, 3n^{-1/4} (\ln n)^2 \right\} \tag{105}$$

for all n sufficiently large. Letting n go to infinity and recalling that $p_s = o(1)$ we obtain $\lim_{n \to \infty} F(n) = 0$. This establishes (99) in view of (102), and (95) follows from (98) and (100) for constant ℓ. From (94) and (95), we finally establish the desired conclusion (72). Note that (73) also follows since the extra condition $p_e n > \epsilon > 0$ is used only once in obtaining (96) which holds trivially for $\ell = 0$. The proof of Proposition 1.2 is thus completed. ■

VIII. A Proof of Proposition 2

Given (70) and Proposition 1.2 (property (a)), it is clear that Proposition 2 will follow once we show that

$$\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}] = o\left(\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \right] \right) \tag{106}$$

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

In order to establish (106), we evaluate $\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}]$ proceeding similarly as in the proof of Proposition 1. This time, we first find an event equivalent to $D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}$, namely to the event that nodes v_x and v_y both have ℓ neighbors and are also neighbors with each other. The intuition is also to consider all the possibilities for the number of nodes that are neighbors of both v_x and v_y, the number of nodes that are neighbors of v_x but not neighbors of v_y, and the number of nodes that are neighbors of v_y but not neighbors of v_x. To this end, we define the series of events B_h in the following manner

$$\begin{aligned} B_h = (|N_{xy}| = h) \bigcap (|N_{x\overline{y}}| = \ell - h - 1) \\ \bigcap (|N_{\overline{x}y}| = \ell - h - 1) \,. \end{aligned} \tag{107}$$

for each $h = 0, 1, \ldots, \ell - 1$. An analog of (63) follows immediately for any positive integer ℓ.

$$D_{x,\ell} \cap D_{y,\ell} \cap E_{xy} = \bigcup_{h=0}^{\ell-1} (B_h \cap E_{xy}) \,. \tag{108}$$

The minus one term on ℓ is due to the fact that x and y are neighbors to each other in event E_{xy}, and thus in event $D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}$ there can be at most $\ell - 1$ nodes that are neighbors of both x and y.

Given (108) and mutually exclusive events B_h ($h = 0, 1, \ldots, \ell - 1$), we obtain

$$\mathbb{P}[D_{x,\ell} \cap D_{y,\ell} \cap E_{xy}] = \sum_{h=0}^{\ell-1} \mathbb{P}\left[B_h \cap E_{xy} \right]. \tag{109}$$

We will establish Proposition 2 by obtaining the following result which evaluates the R.H.S. of (109).

Proposition 2.1. *Let ℓ be a positive integer constant. If $p_s = o(1)$, $p_e = \frac{\ln n + \ln \ln n + \alpha_n}{n}$ with $\lim_{n \to \infty} \alpha_n = -\infty$ and there exists $\epsilon > 0$ such that $p_e n > \epsilon$ for all n sufficiently large, then*

$$\sum_{h=0}^{\ell-1} \mathbb{P}\left[B_h \cap E_{xy} \right] = o\left(\sum_{h=0}^{\ell} \mathbb{P}\left[A_h \cap \overline{K_{xy}} \right] \right). \tag{110}$$

In order to see why Proposition 2 follows from Proposition 2.1, observe that (110) establishes (106) with the help of (109). As noted at the beginning of this section, this establishes Proposition 2.

Proof. As given in (66), $K_{xy} = \bigcup_{u=1}^{K_n} [|S_{xy}| = u]$. Using this and the fact that $E_{xy} = K_{xy} \cap C_{xy}$, we get

$$E_{xy} = \bigcup_{u=1}^{K_n} \left[(|S_{xy}| = u) \bigcap C_{xy} \right].$$

We use $\mathcal{Y}_u$ to denote the event $(|S_{xy}| = u) \cap C_{xy}$, where $u = 1, 2, \ldots, K_n$. Thus, we obtain $E_{xy} = \bigcup_{u=1}^{K_n} \mathcal{Y}_u$. Then considering the disjointness of the events $Y_1, Y_2, \ldots, Y_{K_n}$, we get

$$\mathbb{P}\left[B_h \cap E_{xy} \right] = \mathbb{P}\left[B_h \cap \left(\bigcup_{u=1}^{K_n} \mathcal{Y}_u \right) \right] = \sum_{u=1}^{K_n} \mathbb{P}\left[B_h \cap \mathcal{Y}_u \right]. \tag{111}$$

Given $\mathcal{Y}_u = [(|S_{xy}| = u) \cap C_{xy}]$, we obtain

$$\mathbb{P}\left[B_h \cap \mathcal{Y}_u \right] \leq \mathbb{P}\left[B_h \cap (|S_{xy}| = u) \right]. \tag{112}$$

Applying (112) to (111), it follows that

$$\begin{aligned} &\sum_{h=0}^{\ell-1} \mathbb{P}\left[B_h \cap E_{xy} \right] \\ &\leq \sum_{h=0}^{\ell-1} \sum_{u=1}^{K_n} \mathbb{P}\left[B_h \cap (|S_{xy}| = u) \right] \\ &= \sum_{u=1}^{K_n} \left\{ \mathbb{P}[|S_{xy}| = u] \cdot \sum_{h=0}^{\ell-1} \mathbb{P}\left[B_h \mid (|S_{xy}| = u) \right] \right\}. \end{aligned} \tag{113}$$

Note that R.H.S. of (113) is similar to the R.H.S. of (87). Thus, the manners to evaluate them are also similar. We first calculate $\mathbb{P}[B_h \mid (|S_{xy}| = u)]$. Given the definition of B_h in (107), we let $m_1 = h$ and $m_2 = m_3 = \ell - h - 1$ in Lemma 4 in order to obtain

$$\begin{aligned}\mathbb{P}[B_h \mid (|S_{xy}| = u)] \sim \frac{n^{2\ell-h-2}}{h![(\ell-h-1)!]^2} \cdot e^{-2p_e n + \frac{p_e p_n u}{K_n} n} \\ \times \{\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)]\}^h \\ \times \{\mathbb{P}[E_{\overline{xj}\cap yj} \mid (|S_{xy}| = u)]\}^{\ell-h-1} \\ \times \{\mathbb{P}[E_{xj\cap \overline{yj}} \mid (|S_{xy}| = u)]\}^{\ell-h-1}.\end{aligned} \tag{114}$$

Substituting (90), (91) and (92) into (114), we obtain

$$\mathbb{P}[B_h \mid (|S_{xy}| = u)] \leq 2e^{-2p_e n + \frac{p_e p_n n u}{K_n}} (p_e n)^{2\ell-h-2}. \tag{115}$$

for all n sufficiently large.

Returning to the evaluation of the R.H.S. of (113), we apply (115) to (113) and obtain for all n sufficiently large,

$$\begin{aligned}&\sum_{h=0}^{\ell-1} \mathbb{P}[B_h \cap E_{xy}] \\ &\leq \sum_{u=1}^{K_n} \left\{ \mathbb{P}[|S_{xy}| = u] \cdot 2e^{-2p_e n + \frac{p_n u}{K_n} \cdot p_e n} \cdot \sum_{h=0}^{\ell} (p_e n)^{2\ell-h-2} \right\} \\ &= (p_e n)^{-2} \times \text{R.H.S. of (94)}.\end{aligned} \tag{116}$$

From the fact that $p_e n > \epsilon > 0$ for all n sufficiently large, it follows that

$$\sum_{h=0}^{\ell-1} \mathbb{P}[B_h \cap E_{xy}] = O\left(\text{R.H.S. of (94)}\right). \tag{117}$$

Given (95) and (117), we obtain (110) and this completes the proof of Proposition 2. ■

Having established Propositions 1 and 2, we complete the proof of Lemma 3, and the zero-law (11) follows as explained in Section VI.

IX. Establishing (12) (The One-Law for k-Connectivity in $\mathbb{G}_{on}$)

As shown in Section V-B, we can enforce the extra condition $\alpha_n = o(\ln n)$ in establishing (12) (i.e., the one-law for k-connectivity in $\mathbb{G}_{on}$). Therefore, we will establish (12) under the following conditions:

$$(9), K_n \geq 2 \text{ for all } n \text{ sufficiently large }, P_n = \Omega(n), \tag{118}$$

$$\frac{K_n}{P_n} = o(1), \lim_{n\to\infty} \alpha_n = +\infty \text{ and } \alpha_n = o(\ln n). \tag{119}$$

In graph $\mathbb{G}_{on}$, consider scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ as in Theorem 1. We find it useful to define a sequence $\beta_{\ell,n} : \mathbb{N} \times \mathbb{N}_0 \to \mathbb{R}$ through the relation

$$p_e = \frac{\ln n + \ell \ln\ln n + \beta_{\ell,n}}{n} \tag{120}$$

for each $n \in \mathbb{N}_0$ and each $\ell \in \mathbb{N}$. (120) follows by just setting

$$\beta_{\ell,n} := np_e - \ln n - \ell \ln\ln n. \tag{121}$$

The one-law (12) will follow from the next key result. Recall that, as defined in Section III-B, κ is the connectivity of the graph $\mathbb{G}_{on}$, namely the minimum number nodes whose deletion makes it disconnected.

Lemma 5. *Let ℓ be a non-negative constant integer. If $K_n \geq 2$ for any sufficiently large n, $P_n = \Omega(n)$, $\frac{K_n}{P_n} = o(1)$, and (120) holds with $\beta_{\ell,n} = o(\ln n)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, then*

$$\lim_{n\to\infty} \mathbb{P}[\kappa = \ell] = 0. \tag{122}$$

We now explain why the one-law (12) follows from Lemma 5. Consider p_n, K_n and P_n such that (118) and (119) hold. Comparing (9) and (120), we get

$$\beta_{\ell,n} = (k - 1 - \ell)\ln\ln n + \alpha_n. \tag{123}$$

Since $\alpha_n = o(\ln n)$ and $\lim_{n\to\infty} \alpha_n = +\infty$, we have for each $\ell = 0, 1, \ldots, k-1$ that

$$\lim_{n\to\infty} \beta_{\ell,n} = +\infty \quad \text{and} \quad \beta_{\ell,n} = o(\ln n). \tag{124}$$

Given (124), we use Lemma 5 and obtain

$$\lim_{n\to\infty} \mathbb{P}[\kappa = \ell] = 0, \quad \ell = 0, 1, \ldots, k-1.$$

For any constant k, this implies $\lim_{n\to\infty} \mathbb{P}[\kappa \geq k] = 1$, or equivalently

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{G}_{on} \text{ is } k\text{-connected}] = 1.$$

This completes the proof of the one-law (12). ■

The remaining part of this section is devoted to the proof of Lemma 5.

Proof. We present the steps of proving Lemma 5 below. First, by a crude bounding argument, we get

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

where δ is the minimum node degree of graph $\mathbb{G}_{on}$, as defined in Section III-B. We will prove Lemma 5 by establishing the following two results under the enforced assumptions:

$$\lim_{n\to\infty} \mathbb{P}[\delta \leq \ell] = 0 \quad \text{if} \ \lim_{n\to\infty} \beta_{\ell,n} = +\infty, \tag{125}$$

and

$$\lim_{n\to\infty} \mathbb{P}[\kappa = \ell \ \cap \ \delta > \ell] = 0 \quad \text{if} \ \lim_{n\to\infty} \beta_{\ell,n} = +\infty. \tag{126}$$

We first establish (125). First, from $\ell \ln\ln n = o(\ln n)$, $\beta_{\ell,n} = o(\ln n)$ and $p_e = \frac{\ln n + \ell \ln\ln n + \beta_{\ell,n}}{n}$, it is clear that $p_e \sim \frac{\ln n}{n}$. Then $p_e = o\big(\frac{1}{\sqrt{n}}\big)$. Thus, from Lemmas 1 and 2, we get

$$\mathbb{E}\big[X_\ell\big] = n\mathbb{P}[D_{x,\ell}] \sim n \cdot (\ell!)^{-1} (p_e n)^\ell e^{-p_e n}. \tag{127}$$

Substituting $p_e \sim \frac{\ln n}{n}$ and (120) into (127), we get

$$\mathbb{E}\big[X_\ell\big] \sim n\, (\ell!)^{-1} (\ln n)^\ell e^{-\ln n - \ell \ln\ln n - \beta_{\ell,n}} = (\ell!)^{-1} e^{-\beta_{\ell,n}}.$$

In view of the fact that $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, we thus obtain $\mathbb{E}\big[X_\ell\big] = o(1)$. Then from property (a) of Fact 1 (Section V-C), we get

$$\lim_{n\to\infty} \mathbb{P}[\delta = \ell] = 0. \tag{128}$$

As seen from (121), $\beta_{\ell,n}$ is decreasing in ℓ. Thus, we have $\lim_{n\to\infty} \beta_{\ell^\star,n} = +\infty$ for each $\ell^\star = 0, 1, \ldots, \ell$. It is also immediate from (121) that $\beta_{\ell^\star,n} = o(\ln n)$ since $\beta_{\ell,n} = o(\ln n)$.

Therefore, using the same arguments that lead to (128), we obtain

$$\lim_{n\to\infty} \mathbb{P}[\delta = \ell^\star] = 0, \quad \ell^\star = 0, 1, \ldots, \ell,$$

and (125) follows immediately.

As (125) is established, it remains to prove (126) in order to complete the proof of Lemma 5. The basic idea in establishing (126) is to find a sufficiently tight upper bound on the probability $\mathbb{P}\left[\kappa = \ell \ \cap \ \delta > \ell\right]$ and then to show that this bound tends to zero as n goes to $+\infty$. This approach is similar to the one used for proving the one-law for k-connectivity in Erdős-Rényi graphs [12], as well as to the approach used by Yağan [30] to establish the one-law for connectivity in the graph $\mathbb{G}_{on}$.

We start by obtaining the needed upper bound. Let $\mathcal{N}$ denote the collection of all non-empty subsets of $\{v_1, \ldots, v_n\}$. We define $\mathcal{N}_* = \{T \mid T \in \mathcal{N}, |T| \geq 2\}$ and $\mathcal{K}_T = \cup_{v_i \in T} S_i$. For the reasons that will later become apparent we find it useful to introduce the event $\mathcal{E}(\boldsymbol{J})$ in the following manner:

$$\mathcal{E}(\boldsymbol{J}) = \bigcup_{T \in \mathcal{N}^*} \left[|\mathcal{K}_T| \ \leq \ J_{|T|}\right], \tag{129}$$

where $\boldsymbol{J} = [J_2, J_3, \ldots, J_n]$ is an $(n-1)$-dimensional integer valued array. Let

$$r_n := \min\left(\left\lfloor \frac{P_n}{K_n} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor\right). \tag{130}$$

We define J_i as follows:

$$J_i = \begin{cases} \max\{\lfloor (1+\varepsilon)K_n \rfloor, \lfloor \lambda K_n i \rfloor\} & i = 2, \ldots, r_n, \\ \lfloor \mu P_n \rfloor & i = r_n + 1, \ldots, n. \end{cases} \tag{131}$$

for some arbitrary constant $0 < \varepsilon < 1$ and constants λ, μ in $(0, \frac{1}{2})$ that will be specified later; see (134)-(135) below.

By a crude bounding argument we now get

$$\begin{aligned} &\mathbb{P}\left[(\kappa = \ell) \ \cap \ (\delta > \ell)\right] \\ &\leq \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] + \mathbb{P}\left[(\kappa = \ell) \ \cap \ (\delta > \ell) \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right]. \end{aligned} \tag{132}$$

Hence, a proof of (126) consists of establishing the following two propositions.

Proposition 3. *Let ℓ be a non-negative constant integer. If (120) holds with $\beta_{\ell,n} > 0$, $K_n \geq 2$ and $P_n \geq \sigma n$ for some $\sigma > 0$ for all n sufficiently large and $\frac{K_n}{P_n} = o(1)$, then*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] = 0, \tag{133}$$

where $\boldsymbol{J} = [J_2, J_3, \ldots, J_n]$ is as specified in (131) with arbitrary ε in $(0,1)$, constant λ in $(0, \frac{1}{2})$ is selected small enough to ensure

$$\max\left(2\lambda\sigma, \lambda\left(\frac{e^2}{\sigma}\right)^{\frac{\lambda}{1-2\lambda}}\right) < 1, \tag{134}$$

and constant μ in $(0, \frac{1}{2})$ is selected so that

$$\max\left(2\left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}, \sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right) < 1. \tag{135}$$

A proof of Proposition 3 is given in Section X below. Note that for any $\sigma > 0$, $\lim_{\lambda \downarrow 0} \lambda \left(\frac{e^2}{\sigma}\right)^{\frac{\lambda}{1-2\lambda}} = 0$ so that the condition (134) can always be met by suitably selecting constant $\lambda > 0$ small enough. Also, we have $\lim_{\mu \downarrow 0} \left(\frac{e}{\mu}\right)^{\mu} = 1$, whence $\lim_{\mu \downarrow 0} \sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu} = 0$, and (135) can be made to hold for any constant $\sigma > 0$ by taking $\mu > 0$ sufficiently small. Finally, we remark that the condition $P_n \geq \sigma n$ for some $\sigma > 0$ is equivalent to having $P_n = \Omega(n)$.

Proposition 4. *Let ℓ be a non-negative constant integer. If $K_n \geq 2$ and $P_n \geq \sigma n$ for some $\sigma > 0$ for all n sufficiently large, $\frac{K_n}{P_n} = o(1)$, and (120) holds with $\beta_{\ell,n} = o(\ln n)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, then*

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

where $\boldsymbol{J} = [J_2, J_3, \ldots, J_n]$ is as specified in (131) with arbitrary ε in $(0,1)$, constant μ in $(0, \frac{1}{2})$ selected small enough to ensure (135) and constant $\lambda \in (0, \frac{1}{2})$ selected such that it satisfies (134).

A proof of Proposition 4 is given in Section XI below.

Using Proposition 3 and Proposition 4 (with the same constants ε, λ, μ) in (132), we obtain the desired conclusion (126). The proof of Lemma 5 is now completed. ■

X. A Proof of Proposition 3

We begin by finding an upper bound on the probability $\mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right]$. To this end, we define

$$Y_i = \begin{cases} \lfloor \lambda K_n i \rfloor & i = 2, \ldots, r_n, \\ \lfloor \mu P_n \rfloor & i = r_n + 1, \ldots, n. \end{cases} \tag{136}$$

From (131) and (136), we get

$$J_i = \begin{cases} \max\{\lfloor (1+\varepsilon)K_n \rfloor, Y_i\} & i = 2, \ldots, r_n, \\ Y_i & i = r_n + 1, \ldots, n. \end{cases} \tag{137}$$

We also define

$$\mathcal{N}_- := \{T \mid T \in \mathcal{N}, 2 \leq |T| \leq r_n\},$$

and

$$\mathcal{N}_+ := \{T \mid T \in \mathcal{N}, |T| > r_n\}.$$

Using the definition (129) and the fact that $J_i = Y_i$ for $i = r_n + 1, r_n + 2, \ldots, n$, we get

$$\mathcal{E}(\boldsymbol{J}) = \left(\bigcup_{T \in \mathcal{N}_-} \left[|\mathcal{K}_T| \leq J_{|T|}\right]\right) \cup \left(\bigcup_{T \in \mathcal{N}_+} \left[|\mathcal{K}_T| \leq Y_{|T|}\right]\right). \tag{138}$$

Given $J_i = \max\{\lfloor (1+\varepsilon)K_n \rfloor, Y_i\}$ for $i = 2, 3, \ldots, r_n$, we have

$$\begin{aligned} &\left(\bigcup_{T \in \mathcal{N}_-} \left[|\mathcal{K}_T| \leq J_{|T|}\right]\right) \\ &= \left(\bigcup_{T \in \mathcal{N}_-} \left[|\mathcal{K}_T| \leq (1+\varepsilon)K_n\right]\right) \cup \left(\bigcup_{T \in \mathcal{N}_-} \left[|\mathcal{K}_T| \leq Y_{|T|}\right]\right). \end{aligned} \tag{139}$$

From (138), (139) and the fact that $\mathcal{N}^* = \mathcal{N}_- \cup \mathcal{N}_+$, we obtain

$$\mathcal{E}(\boldsymbol{J}) = \left(\bigcup_{T \in \mathcal{N}_-} [|\mathcal{K}_T| \leq (1+\varepsilon)K_n] \right) \cup \left(\bigcup_{T \in \mathcal{N}^*} [|\mathcal{K}_T| \leq Y_{|T|}] \right). \tag{140}$$

It is easy to check by direct inspection that

$$\bigcup_{T \in \mathcal{N}_-} [|\mathcal{K}_T| \leq (1+\varepsilon)K_n] = \bigcup_{T \in \mathcal{N}_{n,2}} [|\mathcal{K}_T| \leq (1+\varepsilon)K_n] \tag{141}$$

where $\mathcal{N}_{n,2}$ denotes the collection of all subsets of $\{v_1, \ldots, v_n\}$ with exactly two elements. With $\boldsymbol{Y} = [Y_2, Y_3, \ldots, Y_n]$ and

$$\mathcal{E}(\boldsymbol{Y}) = \bigcup_{T \in \mathcal{N}^*} [|\mathcal{K}_T| \leq Y_{|T|}] \tag{142}$$

it is also easy to see that

$$\mathcal{E}(\boldsymbol{J}) = \left(\bigcup_{T \in \mathcal{N}_{n,2}} [|\mathcal{K}_T| \leq (1+\varepsilon)K_n] \right) \cup \mathcal{E}(\boldsymbol{Y}).$$

upon using (141) and (142) in (140).

Using a standard union bound, we now get

$$\mathbb{P}[\mathcal{E}(\boldsymbol{J})] \leq \mathbb{P}[\mathcal{E}(\boldsymbol{Y})] + \sum_{T \in \mathcal{N}_{n,2}} \mathbb{P}[|\mathcal{K}_T| \leq (1+\varepsilon)K_n].$$

It was shown in [30, Proposition 7.2] that given $P_n = \Omega(n)$ and $\lim_{n\to\infty} K_n = \infty$, we have

$$\mathbb{P}[\mathcal{E}(\boldsymbol{Y})] = o(1). \tag{143}$$

Noting that $\lim_{n\to\infty} K_n = \infty$ holds in view of Lemma 7 and $P_n = \Omega(n)$ by assumption, we conclude that (143) holds under the assumptions enforced in Proposition 3.

In order to compute $\sum_{T \in \mathcal{N}_{n,2}} [|\mathcal{K}_T| \leq (1+\varepsilon)K_n]$, we use exchangeability and the fact that $|\mathcal{N}_{n,2}| = \binom{n}{2}$. With $\mathcal{K}_{1,2} = S_1 \cup S_2$, we find

$$\mathbb{P}[\mathcal{E}(\boldsymbol{J})] \leq o(1) + \binom{n}{2} \mathbb{P}[\mathcal{K}_{1,2} \leq \lfloor (1+\varepsilon)K_n \rfloor]. \tag{144}$$

Then, from (144), the desired conclusion (133) (for Proposition 3) will follow if we show that

$$n^2 \mathbb{P}[\mathcal{K}_{1,2} \leq \lfloor (1+\varepsilon)K_n \rfloor] = o(1). \tag{145}$$

This will also be established by means of the bounds given in [29]. To this end, it was shown [29, Proposition 7.4.11, pp. 137–139] under the condition $\frac{K_n}{P_n} = o(1)$ that

$$\mathbb{P}[\mathcal{K}_{1,2} \leq \lfloor (1+\varepsilon)K_n \rfloor] \leq \left(\Gamma(\varepsilon) \frac{K_n}{P_n} \right)^{K_n(1-\varepsilon)},$$

with $\Gamma(\varepsilon) := (1+\varepsilon)e^{\frac{1+\varepsilon}{1-\varepsilon}}$. Using this bound, we now obtain

$$n^2 \mathbb{P}[\mathcal{K}_{1,2} \leq \lfloor (1+\varepsilon)K_n \rfloor] \leq \left(\Gamma(\varepsilon) n^{\frac{2}{(1-\varepsilon)K_n}} \frac{K_n}{P_n} \right)^{K_n(1-\varepsilon)}. \tag{146}$$

Given $P_n \geq \sigma n$ and $\frac{K_n}{P_n} = o(1)$, there exist a sequence w_n satisfying $\lim_{n\to+\infty} w_n = \infty$ such that for all n sufficiently large, we have

$$P_n \geq \max\{\sigma n, K_n w_n\}.$$

As noted before, it also holds that $\lim_{n\to\infty} K_n = \infty$ in view of Lemma 7. It is now easy to see that

$$n^{\frac{2}{K_n(1-\varepsilon)}} \frac{K_n}{P_n} \leq \min\left\{ n^{-1+\frac{2}{K_n(1-\varepsilon)}} \frac{K_n}{\sigma}, \frac{e^{\frac{2\ln n}{K_n(1-\varepsilon)}}}{w_n} \right\} \leq \max\left\{ \frac{n^{-\frac{1}{2}} \ln n}{\sigma}, \frac{e^{\frac{2}{(1-\varepsilon)}}}{w_n} \right\}$$

for all n sufficiently large to ensure that $K_n \geq 4/(1-\varepsilon)$. The last inequality follows by considering the cases $K_n \geq \ln n$ and $K_n < \ln n$ separately for each n on the given range. It follows that

$$\lim_{n\to\infty} \Gamma(\varepsilon) n^{\frac{2}{K_n(1-\varepsilon)}} \frac{K_n}{P_n} = 0,$$

and the desired conclusion (145) follows from (146). Proposition 3 is now established. ■

XI. A Proof of Proposition 4

We start by introducing some notation. For any non-empty subset U of nodes, i.e., $U \subseteq \{v_1, \ldots, v_n\}$, we define the graph $\mathbb{G}_{on}(U)$ (with vertex set U) as the subgraph of $\mathbb{G}_{on}$ restricted to the nodes in U. If all nodes in U are deleted from $\mathbb{G}_{on}$, the remaining graph is given by $\mathbb{G}_{on}(U^c)$ on the vertices $U^c = \{v_1, \ldots, v_n\} \setminus U$. Let $\mathcal{N}_{U^c}$ denote the collection of all non-empty subsets of $\{v_1, \ldots, v_n\} \setminus U$. We say that a subset T in $\mathcal{N}_{U^c}$ is *isolated* in $\mathbb{G}_{on}(U^c)$ if there are no edges (in $\mathbb{G}_{on}$) between the nodes in T and the nodes in $U^c \setminus T$. This is characterized by

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

With each non-empty subset $T \subseteq U^c$ of nodes, we associate several events of interest: Let $\mathcal{C}_T$ denote the event that the subgraph $\mathbb{G}_{on}(T)$ is itself connected. The event $\mathcal{C}_T$ is completely determined by the random variables (rvs) $\{S_i, \ v_i \in T\}$ and $\{C_{ij}, \ v_i, v_j \in T\}$. We also introduce the event $\mathcal{D}_{U,T}$ to capture the fact that T is isolated in $\mathbb{G}_{on}(U^c)$, i.e.,

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

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

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

We also set

$$\mathcal{A}_{U,T} := \mathcal{B}_{U,T} \cap \mathcal{C}_T \cap \mathcal{D}_{U,T}.$$

The proof starts with the following observations: In graph $\mathbb{G}_{on}$, if the connectivity is ℓ (i.e., $\kappa = \ell$) and yet each node has degree at least $\ell + 1$ (i.e., $\delta > \ell$), then there must exist subsets U, T of nodes with $U \in \mathcal{N}$, $|U| = \ell$ and $T \in \mathcal{N}_{U^c}$,

$|T| \geq 2$, such that $\mathbb{G}_{on}(T)$ is connected while T is isolated in $\mathbb{G}_{on}(U^c)$. This ensures that $\mathbb{G}_{on}$ can be disconnected by deleting an appropriately selected ℓ nodes. Notice that, this would not be possible for sets T in $\mathcal{N}_{U^c}$ with $|T| = 1$, since the degree of the node in T would be at least $\ell+1$ by virtue of the event $\delta > \ell$; this would ensure that the single node in T is connected to at least one node in $U^c \setminus T$. Moreover, the event $\kappa = \ell$ also enforces $\mathbb{G}_{on}$ to remain connected after the deletion of any $\ell - 1$ nodes. Therefore, if there exists a subset U (with $|U| = \ell$) such that some T in $\mathcal{N}_{U^c}$ is isolated in $\mathbb{G}_{on}(U^c)$, then each of the ℓ nodes in U should be connected to at least one node in T *and* to at least one node in $U^c \setminus T$. This can easily be seen by contradiction: Consider subsets $U \in \mathcal{N}$ with $|U| = \ell$, and $T \in \mathcal{N}_{U^c}$ with $|T| \geq 2$, such that there exists no edge between the nodes in T and the nodes in $U^c \setminus T$. Suppose there exists a node v_i in U such that v_i is connected to at least one node in $U^c \setminus T$ but is not connected to any node in T. Then, $\mathbb{G}_{on}$ can be disconnected by deleting the nodes in $U \setminus \{v_i\}$ since there will be no edge between the nodes in T and the nodes in $\{v_i\} \cup U^c \setminus T$. But, $|U \setminus \{v_i\}| = \ell - 1$, and this contradicts the fact that $\kappa = \ell$.

The inclusion

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

is now immediate with $\mathcal{N}_{n,r}$ denoting the collection of all subsets of $\{v_1, \ldots, v_n\}$ with exactly r elements. It is also easy to check that this union need only be taken over all subsets T of $\{v_1, \ldots, v_n\}$ with $2 \leq |T| \leq \lfloor \frac{n-\ell}{2} \rfloor$.

We now use a standard union bound argument to obtain

$$\begin{aligned} &\mathbb{P}\left[(\kappa = \ell) \ \cap \ (\delta > \ell) \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \\ &\leq \sum_{U \in \mathcal{N}_{n,\ell}, T \in \mathcal{N}_{U^c}:\ 2 \leq |T| \leq \lfloor \frac{n-\ell}{2} \rfloor} \mathbb{P}\left[\mathcal{A}_{U,T} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \\ &= \sum_{r=2}^{\lfloor \frac{n-\ell}{2} \rfloor} \sum_{U \in \mathcal{N}_{n,\ell}, T \in \mathcal{N}_{U^c,r}} \mathbb{P}\left[\mathcal{A}_{U,T} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \end{aligned} \tag{147}$$

with $\mathcal{N}_{U^c,r}$ denoting the collection of all subsets of U^c with exactly r elements.

For each $r = 1, \ldots, n - \ell - 1$, we simplify the notation by writing $\mathcal{A}_{\ell,r} := \mathcal{A}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+r}\}}$, $\mathcal{D}_{\ell,r} := \mathcal{D}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+r}\}}$, $\mathcal{B}_{\ell,r} := \mathcal{B}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+r}\}}$ and $\mathcal{C}_r := \mathcal{C}_{\{v_{\ell+1},\ldots,v_{\ell+r}\}}$. Under the enforced assumptions on the system model (viz. Section III), exchangeability yields

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

and the expression

$$\begin{aligned} &\sum_{U \in \mathcal{N}_{n,\ell}, T \in \mathcal{N}_{U^c,r}} \mathbb{P}\left[\mathcal{A}_{U,T} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \\ &= \binom{n}{\ell}\binom{n-\ell}{r} \mathbb{P}\left[\mathcal{A}_{\ell,r} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \end{aligned}$$

follows since $|\mathcal{N}_{n,\ell}| = \binom{n}{\ell}$ and $|\mathcal{N}_{U^c,r}| = \binom{n-\ell}{r}$. Substituting into (147) we obtain the key bound

$$\begin{aligned} &\mathbb{P}\left[(\kappa = \ell) \ \cap \ (\delta > \ell) \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] \\ &\leq \sum_{r=2}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{\ell}\binom{n-\ell}{r} \mathbb{P}\left[\mathcal{A}_{\ell,r} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right]. \end{aligned} \tag{148}$$

The proof of Proposition 4 will be completed once we show

$$\lim_{n\to\infty} \sum_{r=2}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{\ell}\binom{n-\ell}{r} \mathbb{P}\left[\mathcal{A}_{\ell,r} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right] = 0. \tag{149}$$

The means to do so are provided in the next section.

XII. Bounding Probabilities $\mathbb{P}\left[\mathcal{A}_{\ell,r} \ \cap \ \overline{\mathcal{E}(\boldsymbol{J})}\right]$

First, for $r = 2, 3, \ldots, n - \ell - 1$, observe the equivalence

$$\mathcal{D}_{\ell,r} = \bigcap_{j=r+\ell+1}^{n} \left[\left(\cup_{i\in\nu_{r,j}} S_i\right) \cap S_j = \emptyset\right] \tag{150}$$

where $\nu_{r,j}$ is defined via

$$\nu_{r,j} := \{i = \ell+1, \ell+2, \ldots, \ell+r : C_{ij}\} \tag{151}$$

for each $j = 1, 2, \ldots, \ell$ and $j = r+\ell+1, r+\ell+2, \ldots, n$. In words, $\nu_{r,j}$ is the set of indices in $i = \ell+1, \ell+2, \ldots, \ell+r$ for which v_i is connected to the node v_j in the communication graph $G(n; p_n)$. Thus, the event $\left[\left(\cup_{i\in\nu_{r,j}} S_i\right) \cap S_j = \emptyset\right]$ ensures that node v_j is not connected (in $\mathbb{G}_{on}$) to any of the nodes $\{v_{\ell+1}, \ldots, v_{\ell+r}\}$. Under the enforced assumptions on the rvs $S_1, S_2, \ldots, S_n$, we readily obtain the expression

$$\begin{aligned} &\mathbb{P}\left[\mathcal{D}_{\ell,r} \ \middle| \ \begin{array}{r} S_i, \ i = \ell+1, \ldots, \ell+r \\ C_{ij}, \ i = \ell+1, \ldots, \ell+r, \\ j = \ell+r+1, \ldots, n \end{array}\right] \\ &= \prod_{j=r+\ell+1}^{n} \left(\frac{\binom{P_n - |\cup_{i\in\nu_{r,j}} S_i|}{K_n}}{\binom{P_n}{K_n}}\right). \end{aligned}$$

In a similar manner, we find

$$\begin{aligned} &\mathbb{P}\left[\mathcal{B}_{\ell,r} \ \middle| \ \begin{array}{r} S_i, \ i = \ell+1, \ldots, \ell+r \\ C_{ij}, \ i = 1, \ldots, \ell, \\ j = \ell+1, \ldots, \ell+r \end{array}\right] \\ &= \prod_{j=1}^{\ell} \left(1 - \frac{\binom{P_n - |\cup_{i\in\nu_{r,j}} S_i|}{K_n}}{\binom{P_n}{K_n}}\right). \end{aligned}$$

It is clear that the distributional properties of the term $|\cup_{i\in\nu_{r,j}} S_i|$ will play an important role in efficiently bounding $\mathbb{P}\left[\mathcal{D}_{\ell,r}\right]$ and $\mathbb{P}\left[\mathcal{B}_{\ell,r}\right]$. Note that it is always the case that

$$| \cup_{i\in\nu_{r,j}} S_i| \geq K_n \mathbf{1}\left[|\nu_{r,j}| > 0\right]. \tag{152}$$

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

$$| \cup_{i\in\nu_{r,j}} S_i| \geq \left(J_{|\nu_{r,j}|} + 1\right) \cdot \mathbf{1}\left[|\nu_{r,j}| > 1\right] \tag{153}$$

for each $j = r+\ell+1, \ldots, n$. Finally, we note the crude bound

$$| \cup_{i\in\nu_{r,j}} S_i| \leq |\nu_{r,j}| K_n \tag{154}$$

for each $j = 1, \ldots, \ell$.

Conditioning on the rvs $S_{\ell+1},\ldots,S_{r+\ell}$ and $\{C_{ij},\ i,j=\ell+1,\ldots,\ell+r\}$ (which determine the event $\mathcal{C}_r$), we conclude via (152)-(154) that

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,r}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\\
&= \mathbb{P}\left[\mathcal{C}_r\cap\mathcal{B}_{\ell,r}\cap\mathcal{D}_{\ell,r}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\\
&\leq \mathbb{E}\left[\begin{array}{l}\mathbf{1}\left[\mathcal{C}_r\right]\times\prod_{j=1}^{\ell}\left(1-\frac{\binom{P_n-K_n|\nu_{r,j}|}{K_n}}{\binom{P_n}{K_n}}\right)\times\\ \times\prod_{j=r+\ell+1}^{n}\frac{\binom{P_n-L(\nu_{r,j})}{K_n}}{\binom{P_n}{K_n}}\end{array}\right],
\end{aligned}$$

where for notational convenience we have set

$$\begin{aligned}
L(\nu_{r,j}) &= \max\{K_n\cdot\mathbf{1}\left[|\nu_{r,j}|>0\right],\\
&\quad (J_{|\nu_{r,j}|}+1)\cdot\mathbf{1}\left[|\nu_{r,j}|>1\right]\}.
\end{aligned}\tag{155}$$

It is immediate that the rvs $\{|\nu_{r,j}|\}_{j=r+1+\ell}^{n}$ (as well as $\{|\nu_{r,j}|\}_{j=1}^{\ell}$) are independent and identically distributed. Let ν_r denote a generic random variable identically distributed with $\nu_{r,j},\ j=1,\ldots,\ell,r+\ell+1,\ldots,n$. Then, we have

$$|\nu_r| =_{\text{st}} \text{Bin}(r,p_n).\tag{156}$$

where we use the notation $=_{st}$ to indicate distributional equality. Then, we define $L(|\nu_r|)$ as follows:

$$L(\nu_r)=\max\left\{K_n\cdot\mathbf{1}\left[|\nu_r|>0\right],(J_{|\nu_r|}+1)\cdot\mathbf{1}\left[|\nu_r|>1\right]\right\}.\tag{157}$$

Observe that the event $\mathcal{C}_r$ is independent from the set-valued random variables $\nu_{r,j}$ for each $j=1,\ldots,\ell$ and for each $j=r+\ell+1,\ldots,n$. Also, as noted before $\{|\nu_{r,j}|\}_{j=r+1+\ell}^{n}$ (as well as $\{|\nu_{r,j}|\}_{j=1}^{\ell}$) are independent and identically distributed. Using these we obtain

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,r}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\\
&\leq \mathbb{P}\left[\mathcal{C}_r\right]\times\mathbb{E}\left[1-\frac{\binom{P_n-K_n|\nu_r|}{K_n}}{\binom{P_n}{K_n}}\right]^{\ell}\times\mathbb{E}\left[\frac{\binom{P_n-L(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right]^{n-r-\ell}.
\end{aligned}\tag{158}$$

We will give sufficiently tight bounds for each term appearing in the R.H.S. of (158). First, note from Lemma 11 (Appendix A-B) that

$$\mathbb{P}\left[\mathcal{C}_r\right]\leq r^{r-2}p_e^{r-1},\qquad r=2,3,\ldots,n.\tag{159}$$

Next, we give an easy bound on the second term appearing in the R.H.S. of (158). With

$$r\leq\frac{P_n-K_n}{2K_n}\tag{160}$$

it follows that $|\nu_r|\leq r\leq\frac{P_n-K_n}{2K_n}$. Then we use Fact 5 and Fact 2 successively to obtain

$$1-\frac{\binom{P_n-K_n|\nu_r|}{K_n}}{\binom{P_n}{K_n}}\leq 1-(1-p_s)^{2|\nu_r|}\leq 2|\nu_r|p_s.$$

Taking the expectation in the above relation and noting that $\mathbb{E}\left[|\nu_r|\right]=rp_n$ via (156), we get

$$\mathbb{E}\left[1-\frac{\binom{P_n-K_n|\nu_r|}{K_n}}{\binom{P_n}{K_n}}\right]\leq 2rp_sp_n=2rp_e\tag{161}$$

under the condition (160). Finally, for the last term in the R.H.S. of (158), we establish in Lemma 12 (Appendix A-B) that if $\frac{K_n}{P_n}=o(1)$ and $p_e=o(1)$, then

$$\begin{aligned}
&\mathbb{E}\left[\frac{\binom{P_n-L(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right]\\
&\leq\min\left\{e^{-p_e(1+\varepsilon/2)},e^{-p_e\lambda r}+e^{-K_n\mu}\mathbf{1}\left[r>r_n\right]\right\}
\end{aligned}\tag{162}$$

for all n sufficiently large and for each $r=2,3,\ldots,n$.

Substituting the bounds (159), (161) and (162) into (158), and noting that each of the terms in the RHS of (158) are trivially upper bounded by 1, we obtain the key bounds on the probabilities $\mathbb{P}\left[\mathcal{A}_{\ell,r}\ \cap\ \overline{\mathcal{E}(\boldsymbol{J})}\right]$ that are summarized in the following Lemma.

Lemma 6. *With $\boldsymbol{J}$ defined in (131) for some ε, λ and μ in $(0,\frac{1}{2})$, if $\frac{K_n}{P_n}=o(1)$ and $p_e=o(1)$, then the following two properties hold.*

(a) For all n sufficiently large and for each $r=2,3,\ldots,\left\lfloor\frac{P_n-K_n}{2K_n}\right\rfloor$, we have

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,r}\ \cap\ \overline{\mathcal{E}(\boldsymbol{J})}\right]\\
&\leq r^{r-2}\left(p_e\right)^{r-1}\cdot\left(2rp_e\right)^{\ell}\\
&\times\left[\min\left\{e^{-p_e(1+\varepsilon/2)},e^{-p_e\lambda r}+e^{-K_n\mu}\mathbf{1}\left[r>r_n\right]\right\}\right]^{n-r-\ell}.
\end{aligned}$$

(b) For all n sufficiently large and for each $r=2,3,\ldots,n$, we have

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,r}\ \cap\ \overline{\mathcal{E}(\boldsymbol{J})}\right]\\
&\leq\min\left\{r^{r-2}\left(p_e\right)^{r-1},1\right\}\\
&\times\left[\min\left\{e^{-p_e(1+\varepsilon/2)},e^{-p_e\lambda r}+e^{-K_n\mu}\mathbf{1}\left[r>r_n\right]\right\}\right]^{n-r-\ell}.
\end{aligned}$$

XIII. Establishing (149)

We now proceed as follows: Given $\frac{K_n}{P_n}=o(1)$ and the definition of r_n in (130), we necessarily have $\lim_{n\to\infty}r_n=+\infty$, and for an given integer $R\geq 2$, we have

$$r_n>R\text{ for any }n\geq n^\star(R)\tag{163}$$

for some finite integer $n^\star(R)$. We define $f_{n,\ell,r}$ as follows.

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

Then, we have

$$\text{L.H.S. of (149)}=\sum_{r=2}^{\lfloor\frac{n-\ell}{2}\rfloor}f_{n,\ell,r}.\tag{164}$$

For the time being, pick an *arbitrarily large* integer $R\geq 2$ (to be specified in Section XIII-B), and on the range $n\geq n^\star(R)$ consider the decomposition

$$\sum_{r=2}^{\lfloor\frac{n-\ell}{2}\rfloor}f_{n,\ell,r}=\sum_{r=2}^{R}f_{n,\ell,r}+\sum_{r=R+1}^{r_n}f_{n,\ell,r}+\sum_{r=r_n+1}^{\lfloor\frac{n-\ell}{2}\rfloor}f_{n,\ell,r}.$$

Let n go to infinity: The desired convergence (149) (for Proposition 4) will be established if we show

$$\sum_{r=2}^{R} f_{n,\ell,r} = o(1), \tag{165}$$

$$\sum_{r=R+1}^{r_n} f_{n,\ell,r} = o(1), \tag{166}$$

and

$$\sum_{r=r_n+1}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,r} = o(1). \tag{167}$$

The next subsections are devoted to proving the validity of (165), (166) and (167) by repeated applications of Lemma 6. Throughout, we also make repeated use of the standard bounds

$$\binom{n}{r} \leq \left(\frac{en}{r}\right)^r \tag{168}$$

valid for all $r, n = 1, 2, \ldots$ with $r \leq n$.

A. Establishing (165)

Positive scalar ε in $(0, 1)$ is picked arbitrarily as stated in Proposition 4. Consider K_n, P_n and p_e as in the statement of Proposition 4. For any arbitrary integer $R \geq 2$, it is clear that (165) will follow upon showing

$$\lim_{n\to\infty} f_{n,\ell,r} = 0 \quad \text{ if } \quad \lim_{n\to\infty} \beta_{\ell,n} = +\infty \tag{169}$$

for each $r = 2, 3, \ldots, R$. On that range, property (a) of Lemma 6 is valid since $r \leq \lfloor \frac{P_n - K_n}{2K_n} \rfloor$ for all n sufficiently large by virtue of the fact that $\frac{K_n}{P_n} = o(1)$.

From the easily obtained bounds $\binom{n}{\ell} \leq n^\ell$ and $\binom{n-\ell}{r} \leq n^r$, we now get

$$\begin{aligned} & f_{n,\ell,r} \\ & \leq n^\ell \cdot n^r \cdot r^{r-2} p_e^{r-1} (2rp_e)^\ell \cdot e^{-p_e(1+\varepsilon/2)(n-r-\ell)} \\ & = (2r)^\ell r^{r-2} \cdot n^{\ell+r} p_e^{\ell+r-1} \cdot e^{-p_e n(1+\varepsilon/2)} \cdot e^{p_e(1+\varepsilon/2)(r+\ell)}. \end{aligned} \tag{170}$$

for each $r = 2, 3, \ldots, R$. Given $p_e = \frac{\ln n + \ell \ln\ln n + \beta_{\ell,n}}{n} \sim \frac{\ln n}{n} = o(1)$ (since $\beta_{\ell,n} = o(\ln n)$), we find

$$\begin{aligned} & \frac{\text{R. H. S. of (170)}}{(2r)^\ell r^{r-2}} \\ & = n^{\ell+r} p_e^{\ell+r-1} \cdot e^{-p_e n(1+\varepsilon/2)} \cdot e^{p_e(1+\varepsilon/2)(r+\ell)} \\ & \sim n^{\ell+r} \left(\frac{\ln n}{n}\right)^{\ell+r-1} \cdot e^{-(\ln n + \ell \ln\ln n + \beta_{\ell,n})(1+\varepsilon/2)} \cdot e^{o(1)} \\ & = n \cdot (\ln n)^{\ell+r-1} \cdot \left[n^{-1} (\ln n)^{-\ell} e^{-\beta_{\ell,n}}\right]^{1+\varepsilon/2} \\ & = n^{-\varepsilon/2} (\ln n)^{r-\ell\varepsilon/2-1} e^{-\beta_{\ell,n}(1+\varepsilon/2)} \\ & = o(1) \end{aligned}$$

by virtue of the facts that r is bounded and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$. We get (169) and the desired result (165) is now established. ■

B. Establishing (166)

Positive scalars λ, μ are given in the statement of Proposition 4. Note that R can be taken to be arbitrarily large by virtue of the previous section. From $\binom{n}{\ell} \leq n^\ell$, $\binom{n-\ell}{r} \leq \left(\frac{e(n-\ell)}{r}\right)^r$ and property (b) of Lemma 6, for $n \geq n^\star(R)$ (with $n^\star(R)$ as specified in (163)) and for each $r = R+1, \ldots, r_n$, we obtain

$$\begin{aligned} f_{n,\ell,r} & \leq n^\ell \cdot \left(\frac{e(n-\ell)}{r}\right)^r \cdot r^{r-2} (p_e)^{r-1} e^{-p_e r\lambda(n-r-\ell)} \\ & \leq n^{\ell+r} e^r (p_e)^{r-1} e^{-p_e r\lambda(n-r-\ell)}. \end{aligned} \tag{171}$$

Now, observe that on the range $r = R+1, R+2, \ldots, \lfloor \frac{n-\ell}{2} \rfloor$, from $r \leq \frac{n-\ell}{2}$, we have for all n sufficiently large, $n - r - \ell \geq \frac{1}{2}(n-\ell) \geq \frac{n}{3}$. This yields

$$e^{-p_e r\lambda(n-r-\ell)} \leq e^{-p_e r\lambda n/3}. \tag{172}$$

Substituting $p_e = \frac{\ln n + \ell \ln\ln n + \beta_{\ell,n}}{n}$ into (172), we also get

$$\begin{aligned} e^{-p_e r\lambda n/3} & = e^{-r\lambda(\ln n + \ell \ln\ln n + \beta_{\ell,n})/3} \\ & = n^{-r\lambda/3} (\ln n)^{-r\lambda\ell/3} e^{-r\lambda\beta_{\ell,n}/3}. \end{aligned} \tag{173}$$

Applying (172), (173) and $p_e \leq \frac{2\ln n}{n}$ to (171), we get

$$\begin{aligned} & f_{n,\ell,r} \\ & \leq n^{\ell+r} e^r \cdot \left(\frac{2\ln n}{n}\right)^{r-1} \cdot n^{-r\lambda/3} (\ln n)^{-r\lambda\ell/3} e^{-r\lambda\beta_{\ell,n}/3} \\ & \leq n^{\ell+1-r\lambda/3} \cdot (2e\ln n)^r \\ & = n^{\ell+1} \cdot (2en^{-\lambda/3} \ln n)^r. \end{aligned} \tag{174}$$

Given $2en^{-\lambda/3} \ln n = o(1)$ and (174), we obtain

$$\begin{aligned} \sum_{r=R+1}^{r_n} f_{n,\ell,r} & \leq \sum_{r=R+1}^{+\infty} n^{\ell+1} \cdot (2en^{-\lambda/3} \ln n)^r \\ & = n^{\ell+1} \cdot \frac{(2en^{-\lambda/3} \ln n)^{R+1}}{1 - 2en^{-\lambda/3} \ln n} \\ & \sim n^{\ell+1-\lambda(R+1)/3} (2e \ln n)^{R+1}. \end{aligned} \tag{175}$$

We pick $R \geq \frac{3(\ell+1)}{\lambda}$ so that $\ell + 1 - \lambda(R+1)/3 \leq -\frac{\lambda}{3}$. As a result, we obtain

$$\text{R.H.S. of (175)} = o(1)$$

and thus

$$\sum_{r=R+1}^{r_n} f_{n,\ell,r} = o(1).$$

(166) is now established. ■

C. Establishing (167)

Positive scalars λ, μ are given in the statement of Proposition 4. We need consider only the case where $r_n \leq \lfloor \frac{n-\ell}{2} \rfloor$ for *infinitely many* n, as otherwise (167) would hold trivially. From $\binom{n}{\ell} \leq n^\ell$, $\binom{n-\ell}{r} \leq \binom{n}{r}$ and property (b) of Lemma 6, we get for $r = r_n + 1, \ldots, \lfloor \frac{n-\ell}{2} \rfloor$,

$$f_{n,\ell,r} \leq n^\ell \binom{n}{r} \left(e^{-p_e r\lambda} + e^{-K_n \mu}\right)^{\frac{n-\ell}{2}}.$$

We will establish (167) in two steps. First set

$$\hat{r}_n = \left\lceil \frac{3}{\lambda p_e} \right\rceil.$$

Obviously, the range $r = r_n+1, \dots, \lfloor \frac{n-\ell}{2} \rfloor$ is intersecting the range $r = \hat{r}_n, \dots, \lfloor \frac{n-\ell}{2} \rfloor$. We first consider the latter range below. For $r = \hat{r}_n, \dots, \lfloor \frac{n-\ell}{2} \rfloor$, it follows that $e^{-p_e r \lambda} \le e^{-3}$. From Lemma 7 (Appendix A-B), $K_n = \Omega\left(\sqrt{\ln n}\right)$ holds. Then $e^{-K_n \mu} = o(1) < \frac{1}{9} - e^{-3}$. Therefore,

$$\left(e^{-p_e r\lambda} + e^{-K_n \mu}\right)^{\frac{n-\ell}{2}} \le \left(\frac{1}{9}\right)^{\frac{n-\ell}{2}} = 3^{\ell - n}.$$

Then

$$\sum_{r=\hat{r}_n}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,r} \le 3^{\ell-n} n^{\ell} \sum_{r=\hat{r}_n}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{r}.$$

Using the binomial formula

$$\sum_{r=\hat{r}_n}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{r} \le \sum_{r=0}^{n} \binom{n}{r} = 2^n,$$

this yields

$$\sum_{r=\hat{r}_n}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,r} \le 3^{\ell} n^{\ell} \left(\frac{2}{3}\right)^n = o(1). \tag{176}$$

If $\hat{r}_n \le r_n + 1$ for all n sufficiently large, then the desired condition (167) is automatically satisfied via (176). On the other hand, if $r_n + 1 < \hat{r}_n$, we should still consider the range $r = r_n + 1, \dots, \hat{r}_n - 1$. On that range, we use arguments similar to those leading to (171) and obtain

$$f_{n,\ell,r} \le n^{\ell+r} e^r \left(p_e\right)^{r-1} \left(e^{-p_e r\lambda} + e^{-K_n \mu}\right)^{n-r-\ell} \tag{177}$$

upon using also property (b) of Lemma 6.

On the range $r = r_n + 1, \dots, \hat{r}_n - 1$, we have

$$r \ge r_n + 1 = \min\left(\left\lfloor \frac{P_n}{K_n} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor\right) + 1 \ge \min\left\{\frac{P_n}{K_n}, \frac{n}{2}\right\},$$

and thus

$$\begin{aligned} \frac{e^{-\mu K_n}}{p_e r\lambda} &\le \frac{e^{-\mu K_n}}{p_e \lambda \cdot \min\{\frac{P_n}{K_n}, \frac{n}{2}\}} \\ &\le \max\left\{\frac{K_n e^{-\mu K_n}}{\sigma\lambda}, \frac{2e^{-\mu K_n}}{\lambda}\right\}. \end{aligned}$$

as we note that $P_n \ge \sigma n$ and $p_e n \ge 1$ for all n sufficiently large.

Given $K_n = \Omega\left(\sqrt{\ln n}\right)$, it follows that

$$\lim_{n\to\infty} K_n e^{-\mu K_n} = 0 \quad \text{and} \quad \lim_{n\to\infty} e^{-\mu K_n} = 0,$$

whence we get

$$\lim_{n\to\infty} \frac{e^{-\mu K_n}}{p_e r\lambda} = 0.$$

Then for any given $0 < \eta < 1$, there exists a finite integer $n^\star(\eta)$ such that for all $n \ge n^\star(\eta)$, we have

$$e^{-\mu K_n} \le e^{-3}\eta \cdot p_e r\lambda \le e^{-3} \cdot (e^{\eta p_e r\lambda} - 1). \tag{178}$$

From $r \le \hat{r}_n - 1 \le \frac{3}{\lambda p_e}$, it follows that $p_e r\lambda \le 3$ and

$$e^{-p_e r\lambda} \ge e^{-3}. \tag{179}$$

Given (178) and (179), we obtain for all $n \ge n^\star(\eta)$,

$$e^{-\mu K_n} \le e^{-p_e r\lambda} \cdot (e^{\eta p_e r\lambda} - 1) = e^{-p_e r\lambda(1-\eta)} - e^{-p_e r\lambda}$$

and thus

$$e^{-p_e r\lambda} + e^{-\mu K_n} \le e^{-p_e r\lambda(1-\eta)}. \tag{180}$$

Recalling (120) and the fact that we have $n - \ell - r \ge n/3$, we now get

$$\begin{aligned} &e^{-p_e r\lambda(1-\eta)(n-r-\ell)} \\ &\le n^{-r\lambda(1-\eta)/3} (\ln n)^{-r\lambda\ell(1-\eta)/3} e^{-r\lambda\beta_{\ell,n}(1-\eta)/3}. \end{aligned} \tag{181}$$

Putting (180) and (181) into (177), and noting that $p_e \le 2\frac{\ln n}{n}$, we get

$$\begin{aligned} f_{n,\ell,r} &\le n^{\ell+r} e^r \left(\frac{2\ln n}{n}\right)^{r-1} \\ &\quad \times n^{-r\lambda(1-\eta)/3} (\ln n)^{-r\lambda\ell(1-\eta)/3} e^{-r\lambda\beta_{\ell,n}(1-\eta)/3} \\ &\le n^{\ell+1-r\lambda(1-\eta)/3} \cdot (2e\ln n)^r \\ &= n^{\ell+1} \cdot (2en^{-\lambda(1-\eta)/3} \ln n)^r. \end{aligned} \tag{182}$$

Given $\lim_{n\to\infty} r_n = +\infty$, then for any arbitrarily large integer $\hat{R}$, we have $r_n \ge \hat{R}$ for all n sufficiently large. From $2en^{-\lambda(1-\eta)/3} \ln n = o(1)$ and (182), we have

$$\begin{aligned} \sum_{r_n+1}^{\hat{r}_n - 1} f_{n,\ell,r} &\le \sum_{\hat{R}+1}^{\infty} n^{\ell+1} \cdot (2en^{-\lambda(1-\eta)/3} \ln n)^r \\ &\sim n^{\ell+1} \cdot \frac{(2en^{-\lambda(1-\eta)/3} \ln n)^{\hat{R}+1}}{1 - 2en^{-\lambda(1-\eta)/3} \ln n} \\ &\sim n^{\ell+1-\lambda(1-\eta)(\hat{R}+1)/3} (2e\ln n)^{\hat{R}+1}. \end{aligned} \tag{183}$$

Since $\hat{R}$ was arbitrary, we pick $\hat{R} \ge \frac{3(\ell+1)}{\lambda(1-\eta)}$. Then

$$\ell + 1 - \lambda(1-\eta)(\hat{R}+1)/3 \le -\lambda(1-\eta)/3.$$

As a result, we have

$$\text{R.H.S. of (183)} = o(1)$$

and thus

$$\sum_{r_n+1}^{\hat{r}_n - 1} f_{n,\ell,r} = o(1).$$

The desired conclusion (167) is now established. ■

Having established (165), (166) and (167), we now get (149) and this completes the proof of Proposition 4. ■

XIV. Applications of Our Results in Other Network Domains

In this section we use properties of random key graphs with physical link constraints to explore k-connectivity in a different network application, namely, in distributed publish-subscribe services for online social networks.

Online social networks interconnect users by symmetric *friend* relations and allow them to define *circles of friends* (viz., `Google+`). We view a user's circle of friends as the group of friends who share a *common interest*. A basic common interest between two friends can be represented by their selection of a number of common objects from a large pool of available objects. For example, two friends may pick the same set of books to read from Amazon's pool, or the same movies to watch from Netflix's pool, or the same hobbies or professional activities from a vast set of possibilities. Of course, a user can belong to multiple circles of friends defined around the same pool of common-interest objects. Identifying friends with common interests in a social network enables the implementation of large-scale, distributed publish-subscribe services which support dissemination of special-interest messages among the users. Such services allow publisher nodes to post interest-specific news, recommendations, warnings, or announcements to subscriber nodes in a wide variety of applications ranging from on-line behavioral advertising (e.g., the message may contain an advertisement targeted to a common-interest group) to social science (e.g., the message may contain a survey request or result directed to a special-interest group).

Assume there are n users. The common-interest relation in the social network induces a graph G_c, where each of the n users represents a node in G_c and two nodes are connected by an edge if and only if the users they represent are common-interest friends. The relevance of the connectivity properties of G_c in the context of large-scale, distributed publish-subscribe services can be seen as follows. Each publisher and each subscriber represents a node in G_c. When publisher v_a posts an interest-specific message `msg`, each node v_b in v_a's circle of common-interest friends receives `msg` and posts `msg` to its own circle of common-interest friends, unless `msg` has already been posted there recently. This process continues iteratively. Obviously, the global dissemination of message `msg` can be achieved if and only if there exists a path between v_a and each subscriber among the other $(n-1)$ nodes of G_c, which happens if G_c is connected. Furthermore, even if at most $(k-1)$ users leave the network, k-connectivity of G_c assures the availability of message-dissemination paths between any two remaining nodes.

A possible way to construct the graph G_c on n users is as follows. Suppose that there exists an *object pool* $\mathcal{P}$ consisting of P_n objects and that each user picks exactly K_n distinct objects uniformly and independently from the object pool; i.e., each user has an *object ring* consisting of K_n objects. Two *friends* are said to have a common-interest relation if they have at least one common object in their object rings. In order to model the friendship network, we use an Erdős-Rényi graph following the prior works [18], [22]. In other words, any two users in the network are friends with each other with probability p_n independently from all other users. As a result, the graph G_c becomes the intersection of an Erdős-Rényi graph $G(n, p_n)$ and a random key graph $G(n, K_n, P_n)$; i.e., G_c is exactly the graph $\mathbb{G}_{on}$ which we have defined in Section III.

Clearly, our zero-one law on k-connectivity in $\mathbb{G}_{on}$ allows us to answer the two key questions for the design of a large-scale, reliable publish-subscribe service: (1) what values should the parameters K_n, P_n, and n take in order to achieve connectivity between publisher and subscriber nodes in the common-interest graph G_c; and (2) how can reliable message dissemination be achieved when some nodes may fail to forward messages. This could happen as a result of discretionary user action (e.g., a node may decide not to forward a particular message, or all messages, of a particular publisher); or voluntary account deletion (e.g., `Facebook` account deletions are not uncommon events); or involuntary account deletion caused by adversary attacks (e.g., Agarwalla [1] shows that clickjacking vulnerability found in Linkedin results in involuntary account deletion).

XV. Conclusion and Future Work

In this paper, we study the k-connectivity of secure wireless sensor networks (WSNs) under an on/off channel model. In particular, we derive zero-one laws for the properties that i) WSN is securely k-connected and ii) each sensor node is securely connected to at least $k-1$ other sensors. The established zero-one laws are shown to improve the existing results on the k-connectivity of random key graphs as well as on the 1-connectivity of the random key graphs when they are intersected with Erdős-Rényi graphs.

A possible extension of our work would be to consider a more realistic communication model than the on/off channel model. One possible candidate is the so-called *disk model* [23], [24] where nodes are distributed over a bounded region of a euclidian plane, and two nodes have a communication link in between if they are within a certain distance (usually referred to as the transmission range) of each other; when nodes are distributed independently and uniformly over this region, the induced random graph is usually referred to as the *random geometric graph* [23], [24]. However, as discussed in [30], the connectivity analysis of such a model (i.e., one obtained by intersecting a random key graph with a random geometric graph) is likely to be challenging and only partial results have been established so far.

Acknowledgements

This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the US Army Research Office and by the MURI grant W 911 NF 0710287 also from the US Army Research Office. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution, the U.S. government or any other entity.

References

[1] http://seclists.org/fulldisclosure/2011/Oct/359.

[2] F. Anjum. Location dependent key management using random key-predistribution in sensor networks. In *Proc. of ACM WiSe*, pages 21–30, 2006.

[3] S. R. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16):5130–5140, 2009.

[4] S. R. Blackburn, D. R. Stinson, and J. Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Cryptology ePrint Archive, Report 2010/030, 2010. http://eprint.iacr.org/.

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

[6] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. of IEEE Symposium on Security and Privacy*, 2003.

[7] R. Di Pietro, L. V. Mancini, and A. Mei. Random key-assignment for secure wireless sensor networks. In *Proc. of ACM SASN*, 2003.

[8] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Connectivity properties of secure wireless sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, SASN '04, pages 53–58, New York, NY, USA, 2004. ACM.

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

[10] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *Proc. of INFOCOM*, 2004.

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

[12] P. Erdős and A. Rényi. On the strength of connectedness of random graphs. *Acta Math. Acad. Sci. Hungar*, pages 261–267, 1961.

[13] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of ACM CCS*, 2002.

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

[15] E. N. Gilbert. Random graphs. *The Annals of Mathematical Statistics*, 30:1141–1144, 1959.

[16] V. Gligor and P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In *Fast Software Encryption*, pages 92–108, 2001.

[17] V. Gligor, A. Perrig, and J. Zhao. Brief encounters with a random key graph. In *Proc. of the 17th Security Protocols Workshop (SPW 17)*, Cambridge, U.K, April 2009. Lecture Notes in Computer Science (LNCS), volume 7028. Springer Verlag.

[18] M. O. Jackson and B. W. Rogers. Meeting strangers and friends of friends: How random are socially generated networks? *American Economic Review*, 97(3):890–915, 2007.

[19] C. S. Jutla. Encryption modes with almost free message integrity. In *Proc. of Eurocrypt*, pages 529–544, 2001.

[20] X. Li, P. Wan, Y. Wang, and C. Yi. Fault tolerant deployment and topology control in wireless networks. In *Proc. of ACM MobiHoc*. Annapolis (MD), 2003.

[21] P. Marbach. A lower-bound on the number of rankings required in recommender systems using collaborativ filtering. In *Proc. IEEE CISS*, 2008.

[22] M. E. J. Newman, D. J. Watts, and S. H. Strogatz. Random graph models of social networks. *Proc. of the National Academy of Sciences of the United States of America*, 99(Suppl 1):2566–2572, Feb. 2002.

[23] M. Penrose. *Random Geometric Graphs*. Oxford University Press, July 2003.

[24] M. D. Penrose. On k-connectivity for a geometric random graph. *Random Struct. Algorithms*, 15:145–164, 1999.

[25] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In *Proc. of ACM CCS*, pages 196–205, 2001.

[26] K. Rybarczyk. Diameter, connectivity and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311, 2011.

[27] K. Rybarczyk. Sharp threshold functions for the random intersection graph via a coupling method. *Electr. Journal of Combinatorics*, 18:36–47, 2011.

[28] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, pages 172–194, London, UK, UK, 2000. Springer-Verlag.

[29] O. Yağan. *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*. PhD thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011. Available online at http://hdl.handle.net/1903/11910.

[30] O. Yağan. Performance of the Eschenauer-Gligor key distribution scheme under an on/off channel. *IEEE Transactions on Information Theory*, 58(6), June 2012. Available online at arXiv:1112.3415v1 [cs.IT].

[31] O. Yağan and A. Makowski. Random key graphs – can they be small worlds? In *Proc. of International Conference on Networks and Communications (NETCOM)*, pages 313 –318, December 2009.

[32] O. Yağan and A. Makowski. Zero-one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, May 2012.

[33] H. Zhang and S. Sundaram. Robustness of complex networks: Reaching consensus despite adversaries. 2012. Available online at arXiv:1203.6119v1 [cs.SI]. http://arxiv.org/abs/1203.6119v1.

Appendix A
Additional Facts and Lemmas

A. Facts

We introduce additional facts below. The proofs of all the following facts are deferred to Appendix B.

Fact 2. *For $0 \leq x < 1$, the following properties hold.*
(a) If $0 < y < 1$, then

$$(1-x)^y \leq 1 - xy.$$

(b) If $y = 0, 1, 2, \ldots$, then

$$1 - xy \leq (1-x)^y \leq 1 - xy + \frac{1}{2}x^2y^2.$$

Fact 2 is used in the proof of the one-law (12) of Theorem 1 as well as in the proofs of Fact 4, Fact 5, Lemma 9, and Lemma 12.

Fact 3. *Let x and y be both positive functions of n. If $x = o(1)$, then for any given constant $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for any $n > N$, the following properties hold.*
(a)

$$e^{-xy-(\frac{1}{2}+\varepsilon)x^2y} \leq (1-x)^y \leq e^{-xy-\frac{1}{2}x^2y}. \tag{184}$$

(b) If $x^2y = o(1)$ further holds, then

$$(1-x)^y \sim e^{-xy}. \tag{185}$$

Fact 3 is used in the proofs of Lemma 2 and Lemma 4.

Fact 4. *Let integers x and y be both positive functions of n, where $y \geq 2x$. For $z = 0, 1, \ldots, x$, we have*

$$\frac{\binom{y-z}{x}}{\binom{y}{x}} \geq 1 - \frac{zx}{y-z}, \tag{186}$$

and

$$\frac{\binom{y-z}{x}}{\binom{y}{x}} = 1 - \frac{xz}{y} \pm O\left(\frac{x^4}{y^2}\right). \tag{187}$$

Fact 4 is used in the proof of Lemma 8.

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

$$\frac{\binom{y-ax}{x}}{\binom{y}{x}} \geq \left[\frac{\binom{y-x}{x}}{\binom{y}{x}}\right]^{2a} \tag{188}$$

Fact 5 is used in the proof of the one-law (12) of Theorem 1.

B. Lemmas

We introduce additional lemmas below. The proofs of all the following lemmas are deferred to Appendix C.

Lemma 7. *Let ℓ be a non-negative constant integer. If $P_n = \Omega(n)$ and (120) holds with $\beta_{\ell,n} > 0$, then $K_n = \Omega\left(\sqrt{\ln n}\right)$.*

Lemma 7 is used in the proof of the one-law (12) of Theorem 1.

Lemma 8. *In $\mathbb{G}_{on}$, given $P_n \geq 2K_n$, then the following properties hold.*

(a) $p_s = \frac{K_n^2}{P_n} \pm O\left(\frac{K_n^4}{P_n^2}\right)$.

(b) ([29, Lemma 7.4.3, pp. 118]) $p_s \leq \frac{K_n^2}{P_n - K_n}$.

(c) $p_s = o(1)$ *if and only if* $\frac{K_n^2}{P_n} = o(1)$.

(d) If $p_s = o(1)$ *or* $\frac{K_n^2}{P_n} = o(1)$*, then* $\frac{K_n^2}{P_n} = p_s \pm O\left(p_s^2\right)$.

Lemma 8 is used in the proof of the zero-law (11) of Theorem 1, as well as in the proofs of Lemma 7 and Lemma 9.

Lemma 9. *Consider K_n and P_n such that $K_n \leq P_n$. The following two properties hold for any three distinct nodes v_x, v_y and v_j.*

(a) We have

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}\right] \leq p_s^2. \tag{189}$$

(b) If $p_s = o(1)$, then for any $u = 0, 1, 2, \ldots, K_n$, we have

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)\right] = \frac{u}{K_n} p_s \pm O\left(p_s^2\right), \tag{190}$$

$$\mathbb{P}[E_{xj \cup yj} \mid (|S_{xy}| = u)] = 2p_e - \frac{p_n u}{K_n} \cdot p_e \pm O({p_e}^2). \tag{191}$$

Lemma 9 is used in the proof of the zero-law (11) of Theorem 1 as well as in the proof of Lemma 4.

Lemma 10. *If $P_n \geq 2K_n$, then we have*

$$\mathbb{P}[|S_{xy}| = u] \leq \frac{1}{u!}\left(\frac{K_n^2}{P_n - K_n}\right)^u.$$

Lemma 10 is used in the proof of the zero-law (11) of Theorem 1.

Lemma 11 ([30, Lemma 10.2] via the argument of [29, Lemma 7.4.5, pp. 124])**.** *For each $r = 2, \ldots, n$, we have*

$$\mathbb{P}\left[\mathcal{C}_r\right] \leq r^{r-2} \left(p_e\right)^{r-1}. \tag{192}$$

Lemma 11 is used in the proof of the one-law (12) of Theorem 1.

Lemma 12. *With $\boldsymbol{J}$ defined in (131) for some ϵ, λ and μ in $(0, \frac{1}{2})$, if $\frac{K_n}{P_n} = o(1)$ and $p_e = o(1)$, then we have*

$$\mathbb{E}\left[\frac{\binom{P_n - L(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right] \leq \min\left\{e^{-p_e(1+\epsilon/2)}, e^{-p_e \lambda r} + e^{-K_n \mu}\mathbf{1}\left[r > r_n\right]\right\} \tag{193}$$

for all n sufficiently large and for each $r = 2, 3, \ldots, n$.

Lemma 12 is used in the proof of the one-law (12) of Theorem 1.

Appendix B
Proofs of Facts

A. Proof of Fact 1 (Section V-C)

1) Proof of property (a): Clearly, event $[\delta = \ell]$ implies event $[X_\ell \geq 1]$. Then

$$\mathbb{P}[\delta = \ell] \leq \mathbb{P}\left[X_\ell \geq 1\right]. \tag{194}$$

Since X_ℓ is a non-negative integer, then

$$\mathbb{E}[X_\ell] = \sum_{i=0}^{+\infty} \left(i \cdot \mathbb{P}\left[X_\ell = i\right]\right) \geq \sum_{i=1}^{+\infty} \mathbb{P}\left[X_\ell = i\right] = \mathbb{P}\left[X_\ell \geq 1\right]. \tag{195}$$

From (194) and (195), it follows that $\mathbb{P}[\delta = \ell] \leq \mathbb{E}[X_\ell]$. Then for $\ell = 0, 1, \ldots, k-1$, given condition $\mathbb{E}[X_\ell] = o(1)$, we obtain $\mathbb{P}[\delta = \ell] = o(1)$.

2) Proof of property (b): For constant k, given $\mathbb{P}[\delta = \ell] = o(1)$ for $\ell = 0, 1, \ldots, k-1$, we obtain

$$\mathbb{P}[\delta \geq k] = 1 - \sum_{\ell=0}^{k-1} \mathbb{P}[\delta = \ell] \to 1, \text{ as } n \to +\infty.$$

3) Proof of property (c): Fix $\ell = 0, 1, \ldots, k-1$ and let $\text{Var}[X_\ell]$ be the variance of random variable X_ℓ. First, it holds that

$$\text{Var}[X_\ell] = \mathbb{E}\big[\big(X_\ell\big)^2\big] - \big\{\mathbb{E}\big[X_\ell\big]\big\}^2. \tag{196}$$

Given (196) and condition $\mathbb{E}\left[\big(X_\ell\big)^2\right] \sim \big\{\mathbb{E}\big[X_\ell\big]\big\}^2$, we obtain

$$\frac{\text{Var}[X_\ell]}{\big\{\mathbb{E}\big[X_\ell\big]\big\}^2} = \frac{\mathbb{E}\big[\big(X_\ell\big)^2\big]}{\big\{\mathbb{E}\big[X_\ell\big]\big\}^2} - 1 = o(1). \tag{197}$$

Then from Chebyshev's inequality,

$$\mathbb{P}\left[\big|X_\ell - \mathbb{E}\big[X_\ell\big]\big| \geq \frac{\mathbb{E}\big[X_\ell\big]}{2}\right] \leq \frac{4\text{Var}\big[X_\ell\big]}{\big\{\mathbb{E}\big[X_\ell\big]\big\}^2} = o(1).$$

Therefore, we get

$$\mathbb{P}\left[X_\ell < \frac{\mathbb{E}\left[X_\ell\right]}{2}\right] = o(1). \tag{198}$$

Clearly, the event $[\delta > \ell]$ implies $[X_\ell = 0]$. Then

$$\begin{aligned}\mathbb{P}[\delta > \ell] &\leq \mathbb{P}\left[X_\ell = 0\right] \\ &= \mathbb{P}\left[\left[X_\ell = 0\right] \cap \left[X_\ell \geq \frac{\mathbb{E}\left[X_\ell\right]}{2}\right]\right] \\ &\quad + \mathbb{P}\left[\left[X_\ell = 0\right] \cap \left(X_\ell < \frac{\mathbb{E}\left[X_\ell\right]}{2}\right)\right] \\ &\leq \mathbf{1}\left[\mathbb{E}\left[X_\ell\right] = 0\right] + \mathbb{P}\left[X_\ell < \frac{\mathbb{E}\left[X_\ell\right]}{2}\right].\end{aligned} \tag{199}$$

Given condition $\lim_{n \to +\infty} \mathbb{E}\big[X_\ell\big] = +\infty$, we have $\mathbf{1}\left[\mathbb{E}\left[X_\ell\right] = 0\right] = 0$ for all n sufficiently large. Using this and (198) in (199), we get $\lim_{n\to\infty} \mathbb{P}[\delta > \ell] = 0$. The desired result $\lim_{n\to\infty} \mathbb{P}[\delta \geq k] = 0$ also follows since $\ell \leq k-1$. ■

B. Proof of Fact 2

1) Proof of property (a): From the Taylor series expansion with Lagrange remainder, there exist $0 < \theta_1 < 1$ such that

$$(1-x)^y = 1 - xy + \frac{y(y-1)(1-\theta_1 x)^{y-2}}{2}x^2. \tag{200}$$

Using $0 \le x < 1$ and $0 < y < 1$ in (200),

$$(1-x)^y \le 1 - xy.$$

2) Proof of property (b): Note that both inequalities follow trivially for $y = 0, 1$. For $y \ge 2$, we use (200) to obtain

$$(1-x)^y \ge 1 - xy \tag{201}$$

as we also note that $0 \le x < 1$. From the Taylor series expansion with Lagrange remainder, there exist $0 < \theta_2 < 1$ such that

$$\begin{aligned}(1-x)^y = 1 - xy + \frac{y(y-1)}{2}x^2 \\ - \frac{y(y-1)(y-2)(1-\theta_2 x)^{y-3}}{6}x^3.\end{aligned} \tag{202}$$

Using $0 \le x < 1$ and $y \ge 2$ in (202),

$$(1-x)^y \le 1 - xy + \frac{y(y-1)}{2}x^2 \le 1 - xy + \frac{x^2y^2}{2}. \tag{203}$$

Combining (201) and (203), the result follows. ■

C. Proof of Fact 3

1) Proof of property (a): Taking the natural logarithm of $(1-x)^y$ and using the Taylor series expansion, we have

$$\ln(1-x)^y = y\ln(1-x) = -y\sum_{i=1}^{+\infty}\frac{x^i}{i}.$$

Defining Ψ as $\sum_{i=3}^{+\infty}\frac{x^i}{i}$, we obtain

$$\ln(1-x)^y = y\Big(-x - \frac{x^2}{2} - \Psi\Big), \tag{204}$$

and

$$\Psi = \sum_{i=3}^{+\infty}\frac{x^i}{i} \le \frac{1}{3}\int_2^{+\infty} x^t dt = \frac{x^2}{-3\ln x}. \tag{205}$$

Given $x = o(1)$, then for any given constant $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for any $n > N$, we have $x \le e^{-\frac{1}{3\varepsilon}}$. Applying $x \le e^{-\frac{1}{3\varepsilon}}$ to (205), we obtain

$$\Psi = -\frac{x^2}{3\ln x} \le -\frac{x^2}{3\ln e^{-\frac{1}{3\varepsilon}}} = \varepsilon x^2.$$

Using $0 \le \Psi \le \varepsilon x^2$ in (204),

$$e^{-xy-(\frac{1}{2}+\varepsilon)x^2y} \le (1-x)^y \le e^{-xy-\frac{1}{2}x^2y}. \tag{206}$$

2) Proof of property (b): Using $x^2y = o(1)$ in (206), clearly $(1-x)^y \sim e^{-xy}$ follows. ■

D. Proof of Fact 4

From $\binom{y-z}{x} = \frac{(y-z)!}{x!(y-z-x)!}$ and $\binom{y}{x} = \frac{(y)!}{x!(y-x)!}$, we get

$$\frac{\binom{y-z}{x}}{\binom{y}{x}} = \frac{(y-z)!}{y!}\cdot\frac{(y-x)!}{(y-z-x)!} = \prod_{t=0}^{z-1}\frac{y-x-t}{y-t}.$$

We define $g(t) = \frac{y-x-t}{y-t} = 1 - \frac{x}{y-t}$, where $t = 0, 1, 2, \ldots, z$. Clearly, $g(t)$ decreases as t increases for $t = 0, 1, 2, \ldots, z$, so $g(z) \le g(t) \le g(0)$. As a result, we have

$$\left(1 - \frac{x}{y-z}\right)^z \le \frac{\binom{y-z}{x}}{\binom{y}{x}} \le \left(1 - \frac{x}{y}\right)^z. \tag{207}$$

Given the above expressions, we use Fact 2 and obtain

$$\left(1 - \frac{x}{y-z}\right)^z \ge 1 - \frac{zx}{y-z} \tag{208}$$

$$\left(1 - \frac{x}{y}\right)^z \le 1 - \frac{zx}{y} + \frac{1}{2}\left(\frac{zx}{y}\right)^2. \tag{209}$$

From (207) and (208), we get (186).

Using $0 \le z \le x$ in the R.H.S. of (209), we also have

$$\left(1 - \frac{x}{y}\right)^z \le 1 - \frac{zx}{y} + O\left(\frac{x^4}{y^2}\right). \tag{210}$$

To evaluate R.H.S. of (208), we have

$$\text{R.H.S. of (208)} - \left(1 - \frac{zx}{y}\right) = -\frac{z^2x}{y\,(y-z)}. \tag{211}$$

Given $y > 2x$ and $0 \le z \le x$, it follows that $z \le \frac{y}{2}$ and thus $y - z \ge y/2$. Note that $x \ge 1$. Then, we have

$$\frac{z^2x}{y\,(y-z)} \le \frac{x^3}{y^2/2} = \frac{2}{x}\cdot\frac{x^4}{y^2} = O\left(\frac{x^4}{y^2}\right). \tag{212}$$

Applying (211) and (212) into (208), we get

$$\left(1 - \frac{x}{y-z}\right)^z \ge 1 - \frac{zx}{y} - O\left(\frac{x^4}{y^2}\right). \tag{213}$$

Using (210) and (213) in (207), we obtain (187). ■

E. Proof of Fact 5

The proof is similar to that of Lemma 5.1 in Yağan [30]. First, given positive integer a, it holds that

$$\frac{\binom{y-ax}{x}}{\binom{y}{x}} = \frac{\prod_{\ell=0}^{x-1}(y-ax-\ell)}{\prod_{\ell=0}^{x-1}(y-\ell)} = \prod_{\ell=0}^{x-1}\left(1 - \frac{ax}{y-\ell}\right). \tag{214}$$

Letting $a = 1$ in (214), we obtain

$$\frac{\binom{y-x}{x}}{\binom{y}{x}} = \prod_{\ell=0}^{x-1}\left(1 - \frac{x}{y-\ell}\right). \tag{215}$$

From property (b) of Fact 2, it follows that

$$\left(1 - \frac{x}{y-\ell}\right)^{2a} \le 1 - \frac{2ax}{y-\ell} + \frac{1}{2}\left(\frac{2ax}{y-\ell}\right)^2 \le 1 - \frac{ax}{y-\ell}, \tag{216}$$

where, in the last step we used the fact that $a \le \frac{y-x}{2x}$ since $y \ge (2a+1)x$ by assumption.

From (214), (215) and (216), we get (188). ■

Appendix C
Proofs of Lemmas

A. Proof of Lemma 1 (Section VI)

1) Proof of (48): We define $\mathrm{I}_{i,\ell}$ as the indicator function of the event that node v_i has degree ℓ, where $i = 1, 2, \ldots, n$; i.e., we have

$$\mathrm{I}_{i,\ell} = \begin{cases} 1, & \text{if node } v_i \text{ has degree } \ell, \\ 0, & \text{otherwise.} \end{cases}$$

Clearly, $\mathbb{E}[\mathrm{I}_{i,\ell}] = \mathbb{P}[D_{x,\ell}]$ and $X_\ell = \sum_{i=1}^{n} \mathrm{I}_{i,\ell}$. Also note that the values of $\mathbb{P}[D_{i,\ell}]$ are the same for all i. Then

$$\mathbb{E}[X_\ell] = \sum_{i=1}^{n} \mathbb{E}[\mathrm{I}_{i,\ell}] = \sum_{i=1}^{n} \mathbb{P}[D_{i,\ell}] = n\mathbb{P}[D_{i,\ell}]. \quad (217)$$

2) Proof of (49): From $X_\ell = \sum_{i=1}^{n} \mathrm{I}_{i,\ell} = \sum_{i=1}^{n} (\mathrm{I}_{i,\ell})^2$, we get

$$\begin{aligned} (X_\ell)^2 &= \left(\sum_{i=1}^{n} \mathrm{I}_{i,\ell}\right)^2 = \sum_{i=1}^{n} (\mathrm{I}_{i,\ell})^2 + 2 \sum_{1 \le i_1 < i_2 \le n} \mathrm{I}_{i_1,\ell}\mathrm{I}_{i_2,\ell} \\ &= X_\ell + 2 \sum_{1 \le i_1 < i_2 \le n} \mathrm{I}_{i_1,\ell}\mathrm{I}_{i_2,\ell}. \end{aligned}$$

Therefore,

$$\begin{aligned} \mathbb{E}\left[(X_\ell)^2\right] &= \mathbb{E}[X_\ell] + 2 \sum_{1 \le i_1 < i_2 \le n} \mathbb{E}[\mathrm{I}_{i_1,\ell}\mathrm{I}_{i_2,\ell}] \\ &= \mathbb{E}[X_\ell] + 2 \sum_{1 \le i_1 < i_2 \le n} \mathbb{P}\left[D_{i_1,\ell} \bigcap D_{i_2,\ell}\right]. \quad (218) \end{aligned}$$

Note that the value of $\mathbb{P}[D_{i_1,\ell} \bigcap D_{i_2,\ell}]$ is the same for $1 \le i_1 < i_2 \le n$. Using this fact and (217) in (218), we obtain

$$\mathbb{E}\left[(X_\ell)^2\right] = n\mathbb{P}[D_{x,\ell}] + n(n-1)\mathbb{P}\left[D_{x,\ell} \bigcap D_{y,\ell}\right]$$

for any two distinct nodes v_x and v_y. ■

B. Proof of Lemma 2 (Section VI)

Note that in $\mathbb{G}_{on}$, the events $E_{1i}, E_{2i}, \ldots, E_{i-1,i}, E_{i+1,i} \ldots, E_{ni}$ are mutually independent for any particular node v_i. Also, the probability that there exists a link between two distinct nodes is p_e. Thus, for each $i = 1, 2, \ldots, n$, the degree of node v_i follows a Binomial distribution $\text{Bin}(n-1, p_e)$. As a result, we have

$$\mathbb{P}[D_{i,\ell}] = \binom{n-1}{\ell} {p_e}^{\ell} (1-p_e)^{n-\ell-1}. \quad (219)$$

Given $p_e = o\left(\frac{1}{\sqrt{n}}\right)$ and constant ℓ, it follows that $p_e = o(1)$ and ${p_e}^2(n-\ell-1) = o(1)$. Then from property (b) of Fact 3, $(1-p_e)^{n-\ell-1} \sim e^{-p_e(n-\ell-1)}$ holds. Then given $p_e = o(1)$ and constant ℓ, we further get

$$(1-p_e)^{n-\ell-1} \sim e^{-p_e n}. \quad (220)$$

Using (220) and $\binom{n-1}{\ell} \sim (\ell!)^{-1} n^\ell$ in (219), we obtain

$$\mathbb{P}[D_{i,\ell}] \sim (\ell!)^{-1} (p_e n)^\ell e^{-p_e n}.$$

■

C. Proof of Lemma 4 (Section VII-A)

In graph $\mathbb{G}_{on}$, besides v_x and v_y, there are $(n-2)$ nodes, denoted by $v_{j_1}, v_{j_2}, \ldots, v_{j_{n-2}}$ below. The $(n-2)$ nodes are split into the four sets N_{xy}, $N_{x\overline{y}}$, $N_{\overline{x}y}$ and $N_{\overline{x}\,\overline{y}}$. According to the definition of event $\mathcal{F}$ in (75), $\mathcal{F}$ means that N_{xy} consists of m_1 nodes, each of which is a neighbor of both v_x and v_y; $N_{x\overline{y}}$ consists of m_2 nodes, each of which is a neighbor of v_x, but is not a neighbor of v_y; $N_{\overline{x}y}$ consists of m_3 nodes, each of which is not a neighbor of v_x, but is a neighbor of v_y; and $N_{\overline{x}\,\overline{y}}$ consists of the remaining $(n-m_1-m_2-m_3-2)$ nodes, each of which is neither a neighbor of v_x nor a neighbor of v_y. Therefore, given non-negative constant integers m_1, m_2 and m_3, the constraints $0 \le |N_{xy}|, |N_{x\overline{y}}|, |N_{\overline{x}y}|, |N_{\overline{x}\,\overline{y}}| \le n-2$ are satisfied. In each instance of event $\mathcal{F}$, the nodes in sets N_{xy}, $N_{x\overline{y}}$, $N_{\overline{x}y}$ and $N_{\overline{x}\,\overline{y}}$ are all determined. Then it is clear that the number of instances for event $\mathcal{F}$ is

$$\binom{n-2}{m_1} \cdot \binom{n-m_1-2}{m_2} \cdot \binom{n-m_1-m_2-2}{m_3}. \quad (221)$$

The event $\mathcal{J}$ defined below is an instance of $\mathcal{F}$.

$$\begin{aligned} \mathcal{J} := &\left(N_{xy} = \left\{v_{j_1}, v_{j_2}, \ldots, v_{j_{m_1}}\right\}\right) \\ &\bigcap \left(N_{x\overline{y}} = \left\{v_{j_{m_1+1}}, v_{j_{m_1+2}}, \ldots, v_{j_{m_1+m_2}}\right\}\right) \\ &\bigcap \left(N_{\overline{x}y} = \left\{v_{j_{m_1+m_2+1}}, v_{j_{m_1+m_2+2}}, \ldots, v_{j_{m_1+m_2+m_3}}\right\}\right) \\ &\bigcap \left(N_{\overline{x}\,\overline{y}} = \left\{v_{j_{m_1+m_2+m_3+1}}, v_{j_{m_1+m_2+m_3+2}}, \ldots, v_{j_{n-2}}\right\}\right). \end{aligned} \quad (222)$$

It is clear that all instances of $\mathcal{F}$ happen with the same probability. Let node v_j be any given node other than v_x and v_y in graph $\mathbb{G}_{on}$. Then

$$E_{xj \cap yj} \Leftrightarrow (v_j \in N_{xy}); \; E_{xj \cap \overline{yj}} \Leftrightarrow (v_j \in N_{x\overline{y}}); \quad (223)$$

$$E_{\overline{xj} \cap yj} \Leftrightarrow (v_j \in N_{\overline{x}y}); \text{ and } E_{\overline{xj} \cap \overline{yj}} \Leftrightarrow (v_j \in N_{\overline{x}\,\overline{y}}). \quad (224)$$

Applying the above equivalences (223) and (224) to the definition of $\mathcal{J}$ in (222), we obtain

$$\begin{aligned} \mathcal{J} = &\left(\bigcap_{i=1}^{m_1} E_{xj_i \cap yj_i}\right) \bigcap \left(\bigcap_{i=m_1+1}^{m_1+m_2} E_{xj_i \cap \overline{yj_i}}\right) \\ &\bigcap \left(\bigcap_{i=m_1+m_2+1}^{m_1+m_2+m_3} E_{\overline{xj_i} \cap yj_i}\right) \bigcap \left(\bigcap_{i=m_1+m_2+m_3+1}^{n-2} E_{\overline{xj_i} \cap \overline{yj_i}}\right). \end{aligned} \quad (225)$$

Given

$$E_{xj} = C_{xj} \cap K_{xj} \text{ and } E_{yj} = C_{yj} \cap K_{yj}, \quad (226)$$

we have

$$E_{xj \cap yj} = (C_{xj} \cap C_{yj}) \cap (K_{xj} \cap K_{yj}). \quad (227)$$

For any node v_j distinct from v_x and v_y, we have the following observations: (a) events $C_{xj}, C_{yj}, C_{xj} \cap C_{yj}, K_{xj}, K_{yj}$ and thus E_{xj}, E_{yj} given by (226) do not depend on any nodes other than v_x, v_y and v_j; (b) given $(|S_{xy}| = u)$, event $K_{xj} \cap K_{yj}$ does not depend on any nodes other than v_x, v_y and v_j; (c) from (227), and observations (a) and (b) above, event $E_{xj \cap yj}$ does not depend on any nodes other than v_x, v_y and

v_j given that $(|S_{xy}| = u)$; (d) since the relative complement of event $E_{xj\cap yj}$ with respect to event E_{xj} is event $E_{xj\cap\overline{yj}}$, given observations (a) and (c) above, event $E_{xj\cap\overline{yj}}$ and then similarly, events $E_{\overline{xj}\cap yj}$ and $E_{\overline{xj}\cap\overline{yj}}$ do not depend on any nodes other than v_x, v_y and v_j.

From observations (c) and (d) above, we conclude that

$$\begin{aligned}&E_{xj_1\cap yj_1}, \ldots, E_{xj_{m_1}\cap yj_{m_1}},\\&E_{xj_{m_1+1}\cap\overline{yj_{m_1+1}}}, \ldots, E_{xj_{m_1+m_2}\cap\overline{yj_{m_1+m_2}}},\\&E_{\overline{xj_{m_1+m_2+1}}\cap yj_{m_1+m_2+1}}, \ldots, E_{\overline{xj_{m_1+m_2+m_3}}\cap yj_{m_1+m_2+m_3}},\\&E_{\overline{xj_{m_1+m_2+m_3+1}}\cap\overline{yj_{m_1+m_2+m_3+1}}}, \ldots, E_{\overline{xj_{n-2}}\cap\overline{yj_{n-2}}}\end{aligned}$$

are mutually independent given that $(|S_{xy}| = u)$.

Then from (221) and (225), we finally get

$$\begin{aligned}&\mathbb{P}\left[\mathcal{F} \mid |S_{xy}| = u\right]\\&= \binom{n-2}{m_1}\binom{n-m_1-2}{m_2}\binom{n-m_1-m_2-2}{m_3}\\&\quad\times\{\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)]\}^{m_1}\\&\quad\times\{\mathbb{P}[E_{xj\cap\overline{y}j} \mid (|S_{xy}| = u)]\}^{m_2}\\&\quad\times\{\mathbb{P}[E_{\overline{xj}\cap yj} \mid (|S_{xy}| = u)]\}^{m_3}\\&\quad\times\{\mathbb{P}[E_{\overline{xj}\cap\overline{yj}} \mid (|S_{xy}| = u)]\}^{n-m_1-m_2-m_3-2}. \end{aligned}\tag{228}$$

upon using exchangeability.

Now, observe that for any constant integers c_1 and c_2, we have

$$\binom{n-c_1}{c_2} = \frac{(n-c_1)!}{c_2!(n-c_1-c_2)!} \sim \frac{n^{c_2}}{c_2!}. \tag{229}$$

Consequently, for constants m_1, m_2 and m_3, we get

$$\begin{aligned}&\binom{n-2}{m_1}\binom{n-m_1-2}{m_2}\binom{n-m_1-m_2-2}{m_3}\\&\sim \frac{n^{m_1}}{m_1!}\cdot\frac{n^{m_2}}{m_2!}\cdot\frac{n^{m_3}}{m_3!} = \frac{n^{m_1+m_2+m_3}}{m_1!m_2!m_3!}.\end{aligned}\tag{230}$$

Now, we evaluate the probability

$$\{\mathbb{P}[E_{\overline{xj}\cap\overline{yj}} \mid (|S_{xy}| = u)]\}^{n-m_1-m_2-m_3-2}. \tag{231}$$

It is clear that

$$(231) = (1 - \mathbb{P}[E_{xj\cup yj} \mid (|S_{xy}| = u)])^{n-m_1-m_2-m_3-2}. \tag{232}$$

From Lemma 9 and the fact that $p_e \leq \frac{\ln n + (k-1)\ln\ln}{n}$ for all n sufficiently large, we find

$$\begin{aligned}\mathbb{P}[E_{xj\cup yj} \mid (|S_{xy}| = u)] &= 2p_e - \frac{p_n u}{K_n}\cdot p_e \pm O({p_e}^2)\\&= 2p_e - \frac{p_n u}{K_n}\cdot p_e \pm o\left(\frac{1}{n}\right) \qquad (233)\\&= O\left(\frac{\ln n}{n}\right) \qquad (234)\\&= o(1).\end{aligned}$$

Then using the above relation, given constants m_1, m_2 and m_3, we obtain

$$\begin{aligned}&(n-m_1-m_2-m_3-2)\{\mathbb{P}[E_{xj\cup yj} \mid (|S_{xy}| = u)]\}^2\\&= (n-m_1-m_2-m_3-2)\cdot\left[O\left(\frac{\ln n}{n}\right)\right]^2 = o(1).\end{aligned}\tag{235}$$

Given (234) and (235), we use property (b) of Fact 3 to evaluate R.H.S. of (232) (i.e., (231)). We get

$$(231) \sim e^{-(n-m_1-m_2-m_3-2)\mathbb{P}[E_{xj\cup yj}|(|S_{xy}|=u)]}. \tag{236}$$

Substituting (233) and (234) into (236), given constants m_1, m_2 and m_3, we find

$$\begin{aligned}(231) &\sim e^{-n[2p_e - \frac{p_n u}{K_n}\cdot p_e \pm o(\frac{1}{n})]}\cdot e^{(m_1+m_2+m_3+2)\cdot o(1)}\\&\sim e^{-2p_e n + \frac{p_n u}{K_n}\cdot p_e n}.\end{aligned}\tag{237}$$

Applying (230) and (237) into (228), we obtain (76) and this establishes Lemma 4. ■

D. *Proof of Lemma 7*

The proof is similar to Lemma 5.3 of Yağan [30]. Given non-negative ℓ, $\beta_{\ell,n} > 0$ and (120), we obtain $p_e = pp_s \geq \frac{\ln n}{n}$. Then from the fact that $p_n \leq 1$, we get $p_s \geq \frac{\ln n}{n}$. Then using $p_s \leq \frac{K_n^2}{P_n - K_n}$ given in property (b) of Lemma 8, $\frac{K_n^2}{P_n-K_n} \geq \frac{\ln n}{n}$ holds. Using this and $P_n = \Omega(n)$, we get

$$\begin{aligned}K_n^2 &= \frac{K_n^2}{P_n - K_n}\cdot(P_n - K_n)\\&\geq \frac{\ln n}{n}\cdot(P_n - K_n) = \Omega(\ln n) - \frac{K_n \ln n}{n}.\end{aligned}\tag{238}$$

Given $K_n \geq 1$, then $\frac{K_n \ln n}{n} < K_n^2$. Applying this into (238), we find

$$K_n > \sqrt{\frac{K_n^2 + \frac{K_n \ln n}{n}}{2}} = \sqrt{\Omega(\ln n)} = \Omega\left(\sqrt{\ln n}\right).$$

■

E. *Proof of Lemma 8*

1) Proof of property (a): Recall from (5) that given $P_n \geq 2K_n$, we have

$$p_s = 1 - \mathbb{P}[S_i \cap S_j = \emptyset] = 1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}. \tag{239}$$

We use Fact 4 (in particular (187)) to evaluate R.H.S. of (239) and obtain

$$p_s = \frac{K_n^2}{P_n} \pm O\left(\left(\frac{K_n^2}{P_n}\right)^2\right). \tag{240}$$

2) Proof of property (b): Property (b) is proved in [29, Lemma 7.4.3, pp. 118].

3) Proof of property (c): From (240), $p_s = o(1)$ if and only if $\frac{K_n^2}{P_n} = o(1)$; namely, property (b) holds.

4) Proof of property (d): From property (c), given $p_s = o(1)$ or $\frac{K_n^2}{P_n} = o(1)$, we use property (b) and have $\frac{K_n^2}{P_n} = o(1)$. From (240) and $\frac{K_n^2}{P_n} = o(1)$, it follows that $p_s \sim \frac{K_n^2}{P_n}$. Therefore,

$$p_s - \frac{K_n^2}{P_n} = \pm O\left(\left(\frac{K_n^2}{P_n}\right)^2\right) = \pm O\left((p_s)^2\right).$$

Then, we get $\frac{K_n^2}{P_n} = p_s \pm O\left((p_s)^2\right)$. ■

F. Proof of Lemma 9

1) Proof of property (a): We start by computing the probability $\mathbb{P}[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)]$ for each $u = 0, 1, 2, \ldots, K_n$. First, note that

$$\begin{aligned}&\mathbb{P}[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)] \\ &= 1 - \mathbb{P}\left[\left(\overline{K_{xj}} \cup \overline{K_{yj}}\right) \mid (|S_{xy}| = u)\right]. \end{aligned} \tag{241}$$

From the inclusion-exclusion principle, this yields

$$\begin{aligned}&\mathbb{P}[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)] \\ &= 1 - \mathbb{P}\left[\overline{K_{xj}} \mid (|S_{xy}| = u)\right] - \mathbb{P}\left[\overline{K_{yj}} \mid (|S_{xy}| = u)\right] \\ &\quad + \mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid (|S_{xy}| = u)\right]. \end{aligned} \tag{242}$$

Note that for each $u = 0, 1, 2, \ldots, K_n$, events $\overline{K_{xj}}$ and $\overline{K_{yj}}$ are both independent of $(|S_{xy}| = u)$; however, $\overline{K_{xj}} \cap \overline{K_{yj}}$ is not independent of $(|S_{xy}| = u)$. Thus, we get

$$\mathbb{P}\left[\overline{K_{xj}} \mid \overline{K_{xy}}\right] = \mathbb{P}\left[\overline{K_{xj}}\right] = 1 - p_s \tag{243}$$
$$\mathbb{P}\left[\overline{K_{yj}} \mid \overline{K_{xy}}\right] = \mathbb{P}\left[\overline{K_{yj}}\right] = 1 - p_s. \tag{244}$$

Substituting (243) and (244) into (242), it follows that

$$\begin{aligned}&\mathbb{P}[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)] \\ &= 2p_s - 1 + \mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid (|S_{xy}| = u)\right]. \end{aligned} \tag{245}$$

Given that the events $\overline{K_{xy}}$ and $(|S_{xy}| = 0)$ are equivalent, letting $u = 0$ in (245), we obtain

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}\right] = 2p_s - 1 + \mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid \overline{K_{xy}}\right]. \tag{246}$$

Since events $\overline{K_{xj}}$ and $\overline{K_{yj}}$ are equivalent to $[(S_x \cap S_j) = \emptyset]$ and $[(S_y \cap S_j) = \emptyset]$, respectively, we have

$$(\overline{K_{xj}} \cap \overline{K_{yj}}) \Leftrightarrow \Big\{S_j \subseteq [\mathcal{P}_n \setminus (S_x \cup S_y)]\Big\}. \tag{247}$$

Therefore, from (247), $(\overline{K_{xj}} \cap \overline{K_{yj}})$ equals the event that the K_n keys forming S_j are all from $[\mathcal{P}_n \setminus (S_x \cup S_y)]$. From $|\mathcal{P}_n| = P_n$, $|S_x| = K_n$ and $|S_y| = K_n$, we get

$$|\mathcal{P}_n \setminus (S_x \cup S_y)| = P_n - 2K_n + |S_{xy}|. \tag{248}$$

Under $\overline{K_{xy}}$ we have $|S_{xy}| = 0$ so that $|\mathcal{P}_n \setminus (S_x \cup S_y)| = P_n - 2K_n$. Clearly, if $P_n < 3K_n$, then $\mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid \overline{K_{xy}}\right] = 0 \leq (1-p_s)^2$. Below we consider the case of $P_n \geq 3K_n$. We have

$$\mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid \overline{K_{xy}}\right] = \frac{\binom{P_n - 2K_n}{K_n}}{\binom{P_n}{K_n}}. \tag{249}$$

Applying Lemma 5.1 in Yağan [30] to R.H.S. of (249), we get

$$\mathbb{P}\left[\left(\overline{K_{xj}} \cap \overline{K_{yj}}\right) \mid \overline{K_{xy}}\right] \leq (1-p_s)^2. \tag{250}$$

Using (250) in (246), we obtain

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid \overline{K_{xy}}\right] \leq 1 - 2(1-p_s) + (1-p_s)^2 = p_s^2.$$

2) Proof of property (b): We first establish (190). Given $p_s = o(1)$, from property (c) of Lemma 8, $\frac{K_n^2}{P_n} = o(1)$ follows. Then $P_n > 3K_n$ holds for all n sufficiently large. We first compute $\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid (|S_{xy}| = u)]$ to derive $\mathbb{P}[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)]$ from (245). As presented in (247), event $(\overline{K_{xj}} \cap \overline{K_{yj}})$ is equivalent to event $\Big\{S_j \subseteq [\mathcal{P}_n \setminus (S_x \cup S_y)]\Big\}$. Given $|S_{xy}| = u$ and (248), it follows that $|\mathcal{P}_n \setminus (S_x \cup S_y)| = P_n - 2K_n + u$. Also, for $0 \leq u \leq K_n$, it holds that $P_n - 2K_n + u \geq K_n$ since $P_n > 3K_n$. Then for all n sufficiently large, we have

$$\begin{aligned}\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] &= \frac{\binom{P_n - 2K_n + u}{K_n}}{\binom{P_n}{K_n}} \\ &= \prod_{t=0}^{K_n - 1}\left(1 - \frac{2K_n - u}{P_n - t}\right). \end{aligned} \tag{251}$$

Now, it is a simple matter to check that

$$\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] \leq \left(1 - \frac{2K_n - u}{P_n}\right)^{K_n} \tag{252}$$

and

$$\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] \geq \left(1 - \frac{2K_n - u}{P_n - K_n}\right)^{K_n}. \tag{253}$$

We first evaluate R.H.S. of (252). It is clear that $0 < \frac{2K_n - u}{P_n} < 1$ for all sufficiently large since $P_n > 3K_n$ and $u \leq K_n$. We utilize Fact 2 to get

$$\begin{aligned}&\text{R.H.S. of (252)} \\ &\leq 1 - \frac{K_n(2K_n - u)}{P_n} + \frac{1}{2}\left[\frac{K_n(2K_n - u)}{P_n}\right]^2. \end{aligned} \tag{254}$$

Applying (254) to (252), we obtain

$$\begin{aligned}&\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] \\ &\leq 1 - \frac{2K_n^2}{P_n} + \frac{uK_n}{P_n} + O\left(\frac{K_n^4}{P_n^2}\right). \end{aligned} \tag{255}$$

Then we evaluate R.H.S. of (253). With $0 \leq u \leq K_n$ and $P_n > 3K_n$, it follows that $0 < \frac{2K_n - u}{P_n - K_n} < 1$ for all n sufficiently large. We utilize Fact 2 and (253) to get

$$\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] \geq 1 - \frac{K_n(2K_n - u)}{P_n - K_n}. \tag{256}$$

We now write

$$\frac{K_n(2K_n - u)}{P_n - K_n} - \frac{K_n(2K_n - u)}{P_n} = \frac{K_n^2(2K_n - u)}{P_n(P_n - K_n)} \tag{257}$$

so that

$$\frac{K_n(2K_n - u)}{P_n - K_n} = \frac{K_n(2K_n - u)}{P_n} + O\left(\frac{K_n^4}{P_n^2}\right). \tag{258}$$

Applying (258) to (256) and using (255) it follows that

$$\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] = 1 - \frac{2K_n^2}{P_n} + \frac{uK_n}{P_n} \pm O\left(\frac{K_n^4}{P_n^2}\right).$$

Given $p_s = o(1)$, from property (d) of Lemma 8, we have that $\frac{K_n^2}{P_n} = p_s \pm O\left(p_s^2\right) \sim p_s$. Given $0 \le u \le K_n$, this yields

$$\begin{aligned}
&\mathbb{P}[(\overline{K_{xj}} \cap \overline{K_{yj}}) \mid |S_{xy}| = u] \\
&= 1 - 2\left[p_s \pm O\left(p_s^2\right)\right] + \frac{u}{K_n}\left[p_s \pm O\left(p_s^2\right)\right] \pm O\left(p_s^2\right) \\
&= 1 - 2p_s + \frac{u}{K_n} \cdot p_s \pm O({p_s}^2). \qquad (259)
\end{aligned}$$

Applying (259) to (245), we obtain

$$\mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)\right] = \frac{u}{K_n} \cdot p_s \pm O({p_s}^2) \qquad (260)$$

and this establishes (190).

We now turn to the proof of (191). First, note that

$$\begin{aligned}
&\mathbb{P}[E_{xj\cup yj} \mid (|S_{xy}| = u)] \\
&= \mathbb{P}[E_{xj} \mid (|S_{xy}| = u)] + \mathbb{P}[E_{yj} \mid (|S_{xy}| = u)] \\
&\quad - \mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)]. \qquad (261)
\end{aligned}$$

Given $E_{xj} = K_{xj} \cap C_{xj}$ and $E_{yj} = K_{yj} \cap C_{yj}$, it is clear that E_{xj} and E_{yj} are both independent of $(|S_{xy}| = u)$. Thus

$$\mathbb{P}[E_{xj} \mid (|S_{xy}| = u)] = \mathbb{P}[E_{yj} \mid (|S_{xy}| = u)] = p_e. \qquad (262)$$

Note that $E_{xj\cap yj} = (K_{xj} \cap C_{xj}) \cap (K_{yj} \cap C_{yj})$ and that $C_{xj} \cap C_{yj}$ is independent of $(|S_{xy}| = u)$. Then from (260) and $\mathbb{P}[C_{xj}] = \mathbb{P}[C_{yj}] = p_n$, it follows that

$$\begin{aligned}
&\mathbb{P}[E_{xj\cap yj} \mid (|S_{xy}| = u)] \\
&= \mathbb{P}[C_{xj}] \cdot \mathbb{P}[C_{yj}] \cdot \mathbb{P}\left[(K_{xj} \cap K_{yj}) \mid (|S_{xy}| = u)\right] \\
&= {p_n}^2 \cdot \left[\frac{u}{K_n} p_s \pm O\left({p_s}^2\right)\right] \\
&= \frac{p_n u}{K_n} \cdot p_e \pm O({p_e}^2). \qquad (263)
\end{aligned}$$

Substituting (263) and (262) into (261), we obtain (191). ∎

G. Proof of Lemma 10

It is not difficult to see that

$$\begin{aligned}
&\mathbb{P}[|S_{xy}| = u] \\
&= \frac{\binom{K_n}{u} \cdot \binom{P_n - K_n}{K_n - u}}{\binom{P_n}{K_n}}. \\
&= \frac{1}{u!} \cdot \left[\frac{K_n!}{(K_n - u)!}\right]^2 \cdot \frac{(P_n - K_n)!}{(P_n - 2K_n + u)!} \cdot \frac{(P_n - K_n)!}{P_n!} \\
&\le \frac{1}{u!} \cdot K_n^{2u} \cdot (P_n - K_n)^{K_n - u} \cdot (P_n - K_n)^{-K_n} \\
&= \frac{1}{u!}\left(\frac{K_n^2}{P_n - K_n}\right)^u.
\end{aligned}$$

∎

H. Proof of Lemma 12

Recall J_i defined in (131). Here we still use Y_i defined in (136) for $j \ge 2$. Then (137) follows. We define $M(|\nu_r|)$ and $Q(|\nu_r|)$ as follows:

$$M(\nu_r) = \mathbf{1}\left[|\nu_r| > 0\right] \cdot \max\{K_n, Y_{n,|\nu_r|} + 1\} \qquad (264)$$

$$Q(\nu_r) = K_n \mathbf{1}\left[|\nu_r| = 1\right] + (\lfloor (1+\varepsilon)K_n \rfloor + 1)\mathbf{1}\left[|\nu_r| > 1\right] \qquad (265)$$

Lemma 12 is an extension of a similar result established in [30, Lemma 10.1, pp. 11]. There, it was shown that for $r = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$,

$$\mathbb{E}\left[\frac{\binom{P_n - M(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right] \le e^{-p_e \lambda r} + e^{-K_n \mu}\mathbf{1}\left[r > r_n\right]. \qquad (266)$$

Recalling the definition of $L(\nu_r)$ in (157) and using the definitions of $M(\nu_r)$ and $Q(\nu_r)$ in (264) and (265), we have the following cases.

(a) If $|\nu_r| = 0$, then $L(\nu_r) = M(\nu_r) = Q(\nu_r) = 0$.
(b) If $|\nu_r| = 1$, then $L(\nu_r) = M(\nu_r) = Q(\nu_r) = K_n$.
(c) If $|\nu_r| \ge 2$, then

$$L(\nu_r) = \max\left\{K_n, J_{n,|\nu_r|} + 1\right\} \qquad (267)$$

$$M(\nu_r) = \max\left\{K_n, Y_{n,|\nu_r|} + 1\right\} \qquad (268)$$

$$Q(\nu_r) = \lfloor (1+\varepsilon)K_n \rfloor + 1. \qquad (269)$$

Then for case (c), we further have the following two subcases.

(c1) If $|\nu_r| = 2, 3, \ldots, r_n$, given (267), (268) and $J_{|\nu_r|} = \max\{(1+\varepsilon)K_n, Y_{|\nu_r|}\}$ from (137), it follows that

$$L(\nu_r) = \max\left\{\lfloor (1+\varepsilon)K_n \rfloor + 1, Y_{n,|\nu_r|} + 1\right\} \qquad (270)$$

resulting in $L(\nu_r) = \max\{M(\nu_r), Q(\nu_r)\}$ from (268) and (269).

(c2) If $|\nu_r| = r_n + 1, r_n + 2, \ldots, n$, given (267), (268) and $J_{|\nu_r|} = Y_{|\nu_r|}$ from (137), it follows that

$$L(\nu_r) = M(\nu_r) = \max\{K_n, \lfloor \mu P_n \rfloor + 1\}. \qquad (271)$$

Given $\frac{K_n}{P_n} = o(1)$, then $\lfloor \mu P_n \rfloor \ge \lfloor (1+\varepsilon)K_n \rfloor$ for all n sufficiently large. Consequently, from (269) and (271), it follows that $L(\nu_r) = \max\{M(\nu_r), Q(\nu_r)\}$.

Summarizing cases (a), (b), and (c1)-(c2) above, given any $|\nu_r|$, we have $L(\nu_r) = \max\{M(\nu_r), Q(\nu_r)\}$ for all n sufficiently large. This yields

$$\frac{\binom{P_n - L(\nu_r)}{K_n}}{\binom{P_n}{K_n}} = \min\left\{\frac{\binom{P_n - M(\nu_r)}{K_n}}{\binom{P_n}{K_n}}, \frac{\binom{P_n - Q(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right\}$$

and

$$\begin{aligned}
&\mathbb{E}\left[\frac{\binom{P_n - L(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right] \\
&\le \min\left\{\mathbb{E}\left[\frac{\binom{P_n - M(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right], \mathbb{E}\left[\frac{\binom{P_n - Q(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right]\right\}. \qquad (272)
\end{aligned}$$

We will show the following result: for all n sufficiently large and for any $r = 2, 3, \ldots, n$,

$$\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right] \le e^{-p_e(1+\varepsilon/2)}. \qquad (273)$$

Clearly, if (273) holds, we can substitute (266) and (273) into (272) and obtain (193), which establishes Lemma 12.

For any given n and any given r, from (265), we get

$$\begin{aligned}
&\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_r)}{K_n}}{\binom{P_n}{K_n}}\right] \\
&\le \mathbb{E}\left[\frac{\binom{P_n - \lceil K_n\{\mathbf{1}[|\nu_r|=1] + (1+\varepsilon)\mathbf{1}[|\nu_r|>1]\}\rceil}{K_n}}{\binom{P_n}{K_n}}\right]. \qquad (274)
\end{aligned}$$

From Lemma 5.1 in Yağan [30], it follows that

$$\text{R.H.S. of (274)} \leq \mathbb{E}\left[(1-p_s)^{\mathbf{1}[|\nu_r|=1]+(1+\varepsilon)\mathbf{1}[|\nu_r|>1]}\right]. \tag{275}$$

Then from (156), we obtain

$$\begin{aligned}
&\text{R.H.S. of (275)} \\
&= \mathbb{P}[|\nu_r|=0] + (1-p_s)\mathbb{P}[|\nu_r|=1] \\
&\quad + (1-p_s)^{1+\varepsilon}\mathbb{P}[|\nu_r|\geq 2] \\
&= (1-p_n)^r + rp_n(1-p_n)^{r-1}(1-p_s) \\
&\quad + [1-(1-p_n)^r - rp_n(1-p_n)^{r-1}](1-p_s)^{1+\varepsilon}. \qquad (276)
\end{aligned}$$

We introduce a continuous variable γ and define $f(\gamma, p_n, p_s)$ as follows, where $\gamma \geq 1$.

$$\begin{aligned}
f(\gamma, p_n, p_s) &= (1-p_n)^\gamma + \gamma p_n(1-p_n)^{\gamma-1}(1-p_s) \\
&\quad + [1-(1-p_n)^\gamma - \gamma p_n(1-p_n)^{\gamma-1}](1-p_s)^{1+\varepsilon}.
\end{aligned} \tag{277}$$

From (276) and (277), we obtain

$$\text{R.H.S. of (275)} = f(r, p_n, p_s). \tag{278}$$

Note that since r is an integer, we cannot take the partial derivative of $f(r, p_n, p_s)$ with respect to r. We have introduced continuous variable γ and hence can take the partial derivative of $f(\gamma, p_n, p_s)$ with respect to γ. We get

$$\begin{aligned}
&\frac{\partial f(\gamma, p_n, p_s)}{\partial \gamma} \\
&= (1-p_n)^\gamma[1-(1-p_s)^{1+\varepsilon}]\ln(1-p_n) \\
&\quad + p_n(1-p_n)^{\gamma-1}[1-p_s-(1-p_s)^{1+\varepsilon}][1+\gamma\ln(1-p_n)] \\
&\leq (1-p_n)^\gamma[1-p_s-(1-p_s)^{1+\varepsilon}]\ln(1-p_n) \\
&\quad + p_n(1-p_n)^{\gamma-1}[1-p_s-(1-p_s)^{1+\varepsilon}][1+\gamma\ln(1-p_n)],
\end{aligned}$$

where, in the last step, we used the fact that $\ln(1-p_n) \leq 0$. Therefore, it's clear that

$$\begin{aligned}
&\frac{1}{(1-p_n)^{\gamma-1}[1-p_s-(1-p_s)^{1+\varepsilon}]}\frac{\partial f(\gamma, p_n, p_s)}{\partial \gamma} \\
&\leq (1-p_n)\ln(1-p_n) + p_n[1+\gamma\ln(1-p_n)] \\
&= (1-p_n+p_n\gamma)\ln(1-p_n) + p_n
\end{aligned}$$

with $(1-p_n)^{\gamma-1}[1-p_s-(1-p_s)^{1+\varepsilon}] \geq 0$. Using $\ln(1-p_n) \leq -p_n < 0$ and $\gamma \geq 1$, we get

$$\begin{aligned}
&\frac{1}{(1-p_n)^{\gamma-1}[1-p_s-(1-p_s)^{1+\varepsilon}]}\frac{\partial f(\gamma, p_n, p_s)}{\partial \gamma} \\
&\leq -p_n(1-p_n+p_n\gamma) + p_n \\
&= p_n^2(1-\gamma) \leq 0.
\end{aligned} \tag{279}$$

Given p_n and p_s, then $f(\gamma, p_n, p_s)$ is decreasing with respect to γ for $\gamma \geq 1$. Then given $r \geq 2$, (275) and (278), we have

$$\begin{aligned}
&\text{R.H.S. of (274)} \\
&\leq f(2, p_n, p_s) \\
&= (1-p_n)^2 + 2p_n(1-p_n)(1-p_s) + p_n^2(1-p_s)^{1+\varepsilon} && (280) \\
&\leq (1-p_n)^2 + 2p_n(1-p_n)(1-p_s) + p_n^2(1-p_s)(1-\varepsilon p_s) && (281) \\
&= 1 - p_e[2-\varepsilon p_e - (1-\varepsilon)p_n] && (282) \\
&\leq \exp\{-p_e[2-\varepsilon p_e-(1-\varepsilon)p_n]\} && (283)
\end{aligned}$$

where in (280) we use $0 < p_s < 1$, $0 < \varepsilon < 1$ and Fact 2 to obtain $(1-p_s)^\varepsilon \leq 1-\varepsilon p_s$; and in (281) we use $p_e = p_n p_s$; and in (282) we use the simple inequality that $1-x \leq e^{-x}$ holds for any $x \geq 0$.

Given $p_e = o(1)$, then $p_e \leq \frac{1}{2}$ for all n sufficiently large. Using this and $0 < p_n \leq 1$, we obtain

$$2-\varepsilon p_e-(1-\varepsilon)p_n \geq 2-\frac{\varepsilon}{2}-(1-\varepsilon) = 1+\frac{\varepsilon}{2}$$

for all n sufficiently large. Applying the above result to (283), we obtain

$$\text{R.H.S. of (274)} \leq e^{-p_e(1+\varepsilon/2)}. \tag{284}$$

Applying (284) to (274), we get (273) and Lemma 12 is now established. ■