Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links

Osman Yağan, *Member, IEEE*, and Armand M. Makowski, *Fellow, IEEE*

***Abstract*—We investigate the secure connectivity of wireless sensor networks under the random pairwise key predistribution scheme of Chan, Perrig, and Song. Unlike recent work carried out under the assumption of *full visibility*, here we assume a (simplified) communication model where unreliable wireless links are represented as independent on/off channels. We present conditions on how to scale the model parameters so that the network 1) has no secure node that is isolated and 2) is securely connected, both with high probability, when the number of sensor nodes becomes large. The results are given in the form of zero-one laws, and exhibit significant differences with corresponding results in the full-visibility case. Through simulations, these zero-one laws are shown to also hold under a more realistic communication model, namely the disk model.**

***Index Terms*—Connectivity, key predistribution, random graphs, security, wireless sensor networks (WSNs).**

I. Introduction

A. Motivation and Background

Wireless sensor networks (WSNs) are distributed collections of sensors with limited capabilities for computations and wireless communications. It is envisioned [1] that WSNs will be used in a wide range of applications areas such as healthcare (e.g., patient monitoring), military operations (e.g., battlefield surveillance), and homes (e.g., home automation and monitoring). These WSNs will often be deployed in hostile environments where communications can be monitored, and nodes are subject to capture and surreptitious use by an adversary. Under such circumstances, cryptographic protection will be needed to ensure secure communications, and to support functions such as sensor-capture detection, key revocation, and sensor disabling.

Unfortunately, many security schemes developed for general network environments do not take into account the unique features of WSNs: Public key cryptography is not feasible computationally because of the severe limitations imposed on the physical memory and power consumption of the individual sensors. Traditional key exchange and distribution protocols are based on trusting third parties, and this makes them inadequate for large-scale WSNs whose topologies are unknown prior to deployment. Some of the challenges specific to WSN settings are discussed in the papers [6], [11], and [20]–[23].

Random key predistribution schemes were introduced to address some of these difficulties. The idea of randomly assigning secure keys to sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor [11]. Since then, many competing alternatives to the Eschenauer and Gligor (EG) scheme have been proposed; see [6], [9], and [20]–[23] (and references therein) for a detailed survey of various key predistribution schemes for WSNs. With so many schemes available, a basic question arises as to how they compare with each other. Answering this question passes through a good understanding of the properties and performance of the schemes under consideration, and this can be achieved in a number of ways. The approach we use here considers random graph models naturally induced by a given scheme, and then develops the scaling laws corresponding to desirable network properties, e.g., absence of secure nodes that are isolated, secure connectivity, etc. This is done with the aim of deriving guidelines to *dimension* the scheme, namely adjust its parameters so that these properties occur with high probability as the number of nodes becomes large.

To date, most of the efforts along these lines have been carried out under the assumption of *full visibility* according to which sensor nodes are all within communication range of each other; more on this later. Under this assumption, the EG scheme gives rise to a class of random graphs known as random key graphs; relevant results are available in [3], [8], [11], [18], and [30]. The q-composite scheme [7], a simple variation of the EG scheme, was investigated by Bloznelis *et al.* [4] through an appropriate extension of the random key graph model. In [7], Chan *et al.* also proposed the random pairwise key predistribution scheme as an alternative to the EG scheme. Yağan and Makowski have recently analyzed various random graphs induced by this scheme; see the papers [28], [29], and [31]–[33].

To be sure, the full-visibility assumption does away with the wireless nature of the communication medium supporting WSNs. In return, this simplification makes it possible to focus on how randomization in the key assignments alone affects the establishment of a secure network in the best of circumstances, i.e., when there are no link failures. A common criticism of this line of work is that by disregarding the unreliability of the wireless links, the resulting dimensioning guidelines are likely to be too *optimistic*: In practice, nodes will have fewer neighbors since some of the communication links may be

Manuscript received October 08, 2010; accepted March 19, 2012. Date of publication September 18, 2012; date of current version February 12, 2013. This work was supported by the National Science Foundation under Grant CCF-0729093. This paper was presented in part at the 2011 IEEE International Conference on Communications.

O. Yağan was with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA. He is now with CyLab, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: osmanyagan@gmail.com).

A. M. Makowski is with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: armand@isr.umd.edu).

Communicated by E. Erkip, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2219578

impaired. As a result, the desired connectivity properties may not be achieved if dimensioning is done according to results derived under full visibility.

B. Summary of Main Contributions

In this paper, in an attempt to go beyond full visibility, we revisit the pairwise key predistribution scheme of Chan *et al.* [7] under more realistic assumptions that account for the possibility that communication links between nodes may not be available—This could occur due to the presence of physical barriers between nodes or because of harsh environmental conditions severely impairing transmission. To study such situations, we introduce a simple communication model where channels are mutually independent, and are either on or off. An overall system model is then constructed by *intersecting* the random graph model of the pairwise key distribution scheme (under full visibility), with an Erdős-Rényi (ER) graph model [5]. For this new random graph structure, we establish zero-one laws for two basic (and related) graph properties, namely graph connectivity and the absence of isolated nodes, when the model parameters are scaled with the number of users. We identify the critical thresholds and show that they coincide. To the best of our knowledge, these full zero-one laws constitute the first *complete* analysis of a key predistribution scheme under *non*full visibility[1]—Contrast this with the partial results by Yi *et al.* [34] for the absence of isolated nodes (under additional conditions) when the communication model is taken to be the disk model.

Although the communication model considered here may be deemed simplistic, it does permit a complete analysis of the issues of interest, with the results already yielding a number of interesting observations: The obtained zero-one laws differ significantly from the corresponding results in the full-visibility case [31], [33]. Thus, the communication model may have a significant impact on the dimensioning of the pairwise distribution algorithm, and this points to the need of possibly reevaluating guidelines developed under the full-visibility assumption. Simulations also suggest that the zero-one laws obtained here under the on/off channel model may still be useful in dimensioning the pairwise scheme under the popular, and more realistic, disk model [13].

We also compare the results established here with well-known zero-one laws for ER graphs [5]. In particular, we show that the connectivity behavior of the model studied here does not in general resemble that of the ER graphs. However, the picture is somewhat more subtle for the results also imply that if the channel is very poor, the model studied here does behave like an ER graph as far as connectivity is concerned. The comparison with ER graphs is particularly relevant to the analysis of key predistribution schemes for WSNs: Indeed, connectivity results for ER graphs have often been used wholesale in the dimensioning and evaluation of key predistribution schemes, e.g., see the papers by Eschenauer and Gligor [11], Chan *et al.* [7], and Hwang and Kim [14]. There it is a common practice to assume that the random graph induced by the particular key predistribution scheme behaves *like* an ER graph (although it is not strictly speaking an ER graph). As pointed out by Di Pietro *et al.* [8] such an assumption is made without any formal justification, and subsequent efforts to confirm its validity have remained limited to this date: The EG scheme has been analyzed by a number of authors [3], [8], [18], [26], [27], [30], and as a result of these efforts, it is now known that the ER *assumption* does yield the correct results for both the absence of isolated nodes and connectivity under the assumption of full visibility. On the other hand, the ER assumption is *not* valid for the pairwise scheme under full visibility; see [12], [31], [33], and the discussion given in Section V-A.

[1]The connectivity of the EG scheme under an on/off channel has also been studied recently by Yağan [24], and zero-one laws analogous to the ones given here were established.

C. Organization of This Paper

The rest of this paper is organized as follows: In Section II, we give precise definitions and implementation details for the pairwise scheme of Chan *et al.*, while Section III is devoted to describing the model of interest. The main results of the paper, namely Theorem 4.1 and Theorem 4.2, are presented in Section IV with an extensive discussion given in Section V. The remaining sections, namely Sections VI–XV, are devoted to establishing the main results of this paper. The proofs of several technical results have been relegated to the Appendix.

D. Notation

A word on notation and conventions in use: All limiting statements, including asymptotic equivalences, are understood with the number n of sensor nodes going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. Also, for any pair of events E and F, we have

$$\mathbf{1}[E \cup F] = \mathbf{1}[E] + \mathbf{1}[F] - \mathbf{1}[E \cap F]. \tag{1}$$

For any discrete set S, we write $|S|$ for its cardinality.

II. Implementing Pairwise Key Predistribution Schemes

Interest in the random pairwise key predistribution scheme of Chan *et al.* [7] stems from the following advantages over the EG scheme: 1) Even if some nodes are captured, the secrecy of the remaining nodes is *perfectly* preserved. 2) Unlike earlier schemes, this pairwise scheme enables both node-to-node authentication and quorum-based revocation.

We parameterize the pairwise key distribution scheme by two positive integers n and K such that $K < n$. There are n nodes, labeled $i = 1, \ldots, n$, with unique ids $\mathrm{Id}_1, \ldots, \mathrm{Id}_n$. Write $\mathcal{N} = \{1, \ldots n\}$ and set $\mathcal{N}_{-i} = \mathcal{N} - \{i\}$ for each $i = 1, \ldots, n$. With node i, we associate a subset $\Gamma_{n,i}(K)$ of nodes selected at *random* from $\mathcal{N}_{-i}$—We say that each of the nodes in $\Gamma_{n,i}(K)$ is paired to node i. Thus, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

$$\mathbb{P}[\Gamma_{n,i}(K) = A] = \begin{cases} \binom{n-1}{K}^{-1} & \text{if } |A| = K \\ 0 & \text{otherwise.} \end{cases}$$

The selection of $\Gamma_{n,i}(K)$ is done *uniformly* amongst all subsets of $\mathcal{N}_{-i}$ which are of size exactly K. The rvs

$\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$ are assumed to be mutually independent so that

$$\mathbb{P}\left[\Gamma_{n,i}(K) = A_i,\ i = 1, \ldots, n\right] = \prod_{i=1}^{n} \mathbb{P}\left[\Gamma_{n,i}(K) = A_i\right]$$

for arbitrary $A_1, \ldots, A_n$ subsets of $\mathcal{N}_{-1}, \ldots, \mathcal{N}_{-n}$, respectively.

Once this *offline* random pairing has been created, we construct the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$, one for each node, as follows: Assumed available is a collection of nK distinct cryptographic keys $\{\omega_{i|\ell},\ i = 1, \ldots, n;\ \ell = 1, \ldots, K\}$. Fix $i = 1, \ldots, n$ and let $\ell_{n,i} : \Gamma_{n,i}(K) \to \{1, \ldots, K\}$ denote a labeling of $\Gamma_{n,i}(K)$. For each node j in $\Gamma_{n,i}(K)$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}(K)$ is realized as $\{j_1, \ldots, j_K\}$ with $1 \leq j_1 < \ldots < j_K \leq n$, then an obvious labeling consists in $\ell_{n,i}(j_k) = k$ for each $k = 1, \ldots, K$ so that key $\omega_{i|k}$ is associated with node j_k. Of course, other labelings are possible, e.g., according to decreasing labels or according to a random permutation. Finally, with node j paired to node i, the pairwise key $\omega^\star_{n,ij} = [\mathrm{Id}_i | \mathrm{Id}_j | \omega_{i|\ell_{n,i}(j)}]$ is constructed and inserted in the memory modules of both nodes i and j. The key $\omega^\star_{n,ij}$ is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise predistribution scheme. The key ring $\Sigma_{n,i}(K)$ of node i is the set

$$\Sigma_{n,i}(K) = \left\{\omega^\star_{n,ij},\ j \in \Gamma_{n,i}(K)\right\} \cup \left\{\omega^\star_{n,ji},\ \begin{array}{c} j = 1, \ldots, n \\ i \in \Gamma_{n,j}(K) \end{array}\right\}. \quad (2)$$

If two nodes, say i and j, are within communication range of each other, then they can establish a secure link if at least one of the events $i \in \Gamma_{n,j}(K)$ or $j \in \Gamma_{n,i}(K)$ is taking place. Both events can take place, in which case the memory modules of node i and j both contain the distinct keys $\omega^\star_{n,ij}$ and $\omega^\star_{n,ji}$. Finally, it is plain by construction that this scheme supports *distributed* node-to-node authentication.

III. Model

Under full visibility, this pairwise predistribution scheme naturally gives rise to the following class of random graphs: With $n = 2, 3, \ldots$ and positive integer $K < n$, we say that the distinct nodes i and j are K-adjacent, written $i \sim_K j$, if and only if they have at least one key in common in their key rings, namely

$$i \sim_K j \quad \text{iff} \quad \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset. \quad (3)$$

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (3); this corresponds to modeling the pairwise distribution scheme under full visibility. We have

$$\mathbb{P}\left[i \sim_K j\right] = \lambda_n(K) \quad (4)$$

where $\lambda_n(K)$ is the link assignment probability in $\mathbb{H}(n; K)$ given by

$$\lambda_n(K) = 1 - \left(\frac{\binom{n-2}{K}}{\binom{n-1}{K}}\right)^2 = 1 - \left(1 - \frac{K}{n-1}\right)^2 = \frac{2K}{n-1} - \left(\frac{K}{n-1}\right)^2. \quad (5)$$

The random graph $\mathbb{H}(n; K)$ is known in the literature on random graphs as the random K-out graph [5], [12]: To each of the n vertices, assign exactly K arcs to K distinct vertices that are selected uniformly at random, and then ignore the orientation of the arcs. In what follows, we sometimes refer to $\mathbb{H}(n; K)$ as the random *pairwise* graph (instead of the random K-out graph) in order to emphasize its connection with the random pairwise scheme of Chan *et al.*

As mentioned earlier, we seek to account for the possibility that communication links between nodes may not be available. To study such situations, we assume a simple communication model that consists of independent channels, each of which can be either on or off. Thus, with p in $(0, 1)$, let $\{B_{ij}(p),\ 1 \leq i < j \leq n\}$ denote i.i.d. $\{0, 1\}$-valued rvs with success probability p. The channel between nodes i and j is available (resp. up) with probability p and unavailable (resp. down) with the complementary probability $1 - p$. Distinct nodes i and j are said to be B-adjacent, written $i \sim_B j$, if $B_{ij}(p) = 1$. B-adjacency defines the standard ER graph $\mathbb{G}(n; p)$ on the vertex set $\{1, \ldots, n\}$. Obviously

$$\mathbb{P}\left[i \sim_B j\right] = p.$$

The random graph model studied here is obtained by *intersecting* the random pairwise graph $\mathbb{H}(n; K)$ with the ER graph $\mathbb{G}(n; p)$. More precisely, the distinct nodes i and j are said to be adjacent, written $i \sim j$, if and only they are both K-adjacent and B-adjacent, namely

$$i \sim j \quad \text{iff} \quad \begin{array}{c} \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset \\ \text{and} \\ B_{ij}(p) = 1. \end{array} \quad (6)$$

The resulting *undirected* random graph defined on the vertex set $\{1, \ldots, n\}$ through this notion of adjacency is denoted $\mathbb{H} \cap \mathbb{G}(n; K, p)$.

Throughout we assume the collections of rvs $\{\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)\}$ and $\{B_{ij}(p),\ 1 \leq i < j \leq n\}$ to be independent, in which case the edge occurrence probability in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is given by

$$\mathbb{P}\left[i \sim j\right] = \mathbb{P}\left[i \sim_K j\right] \mathbb{P}\left[i \sim_B j\right] = p\lambda_n(K). \quad (7)$$

IV. Results

To fix the terminology, we refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* (for random pairwise graphs) provided it satisfies the natural conditions

$$K_n < n, \quad n = 1, 2, \ldots. \quad (8)$$

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

To lighten the notation, we often group the parameters K and p into the ordered pair $\theta \equiv (K,p)$. Hence, a mapping $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ defines a scaling for the intersection graph $\mathbb{H} \cap \mathbb{G}(n;\theta)$ provided the condition (8) holds on the first component mapping.

The results will be expressed in terms of the threshold function $\tau : [0,1] \to [0,1]$ defined by

$$\tau(p) = \begin{cases} 1 & \text{if } p = 0 \\ \frac{2}{1 - \frac{\log(1-p)}{p}} & \text{if } 0 < p < 1 \\ 0 & \text{if } p = 1. \end{cases} \tag{9}$$

It is easy to check that this threshold function is continuous on its entire domain of definition (see Fig. 3).

A. Absence of Isolated Nodes

The first result gives a zero-one law for the absence of isolated nodes.

Theorem 4.1: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that

$$p_n \left(2K_n - \frac{K_n^2}{n-1} \right) \sim c \log n, \quad n = 1,2,\ldots \tag{10}$$

for some $c > 0$. If $\lim_{n\to\infty} p_n = p^\star$ for some $p^\star$ in $[0,1]$, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c} \mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ contains} \\ \text{no isolated nodes} \end{array} \right] = \begin{cases} 0 & \text{if } c < \tau(p^\star) \\ 1 & \text{if } c > \tau(p^\star) \end{cases} \tag{11}$$

where the threshold $\tau(p^\star)$ is given by (9).

The condition (10) on the scaling $\mathbb{N}_0 \to (0,1) \times \mathbb{N}_0$ will often be used in the equivalent form

$$p_n \left(2K_n - \frac{K_n^2}{n-1} \right) = c_n \log n, \quad n = 2,3,\ldots \tag{12}$$

with the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfying $\lim_{n\to\infty} c_n = c$. In view of (5), this amounts to

$$p_n \lambda_n(K_n) = c_n \frac{\log n}{n-1}, \quad n = 2,3,\ldots \tag{13}$$

B. Connectivity

An analog of Theorem 4.1 also holds for the property of graph connectivity.

Theorem 4.2: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that (10) holds for some $c > 0$. If $\lim_{n\to\infty} p_n = p^\star$ for some $p^\star$ in $[0,1]$, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } c < \tau(p^\star) \\ 1 & \text{if } c > \tau(p^\star) \end{cases} \tag{14}$$

where the threshold $\tau(p^\star)$ is given by (9).

Comparing Theorem 4.2 with Theorem 4.1, we see that the class of random graphs studied here provides one more instance where the zero-one laws for absence of isolated nodes and connectivity coincide, viz. ER graphs [5], random geometric graphs [19], or random key graphs [3], [18], [30].

A case of particular interest arises when $p^\star > 0$ since requiring (10) now amounts to

$$\left(2K_n - \frac{K_n^2}{n-1} \right) \sim \frac{c}{p^\star} \log n \tag{15}$$

for some $c > 0$. Any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ that satisfies (15) must necessarily satisfy $K_n = \Theta(\log n) = o(n)$, e.g., see (39) in the proof of Lemma 7.1. Therefore, requiring (10) is equivalent to

$$K_n \sim t \log n \tag{16}$$

for some $t > 0$ with c and t related by $2tp^\star = c$. With this reparameterization, Theorem 4.1 and Theorem 4.2 can be summarized in the following simpler form.

Theorem 4.3: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that $\lim_{n\to\infty} p_n = p^\star > 0$. Under the condition (16) for some $t > 0$, we have

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ contains no isolated nodes}\right] \\ &= \lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected}\right] \\ &= \begin{cases} 0 & \text{if } t < \widehat{\tau}(p^\star) \\ 1 & \text{if } t > \widehat{\tau}(p^\star) \end{cases} \end{aligned} \tag{17}$$

where we have set

$$\widehat{\tau}(p) = \frac{\tau(p)}{2p} = \frac{1}{p - \log(1-p)}, \quad 0 < p \le 1. \tag{18}$$

This alternate formulation is particularly relevant for the case $p_n = p^\star$ (in $(0,1)$) for all $n = 1,2,\ldots$, which captures situations when channel conditions are not affected by the number of users. Such simplifications do not occur in the more realistic case $p^\star = 0$ which corresponds to the situation where channel conditions are indeed influenced by the number of users in the system—The more users in the network, the more likely they will experience interferences from other users.

In Figs. 1 and 2, we present simulation results that support (17). In all these simulations, the number of nodes is fixed at $n = 200$. We consider the channel parameters $p = 0.2$, $p = 0.4$, $p = 0.6$, $p = 0.8$, and $p = 1$ (the full-visibility case), while varying the parameter K from $K = 1$ to $K = 25$. For each parameter pair (K,p), we generate 500 independent samples of the graph $\mathbb{H} \cap \mathbb{G}(n;K,p)$ and count the number of times (out of a possible 500) that the obtained graphs 1) have no isolated nodes and 2) are connected. Dividing the counts by 500, we obtain the (empirical) probabilities for the events of interest. The results for connectivity are given in Fig. 1, where the curve fitting tool of MATLAB is used. It is easy to check that for each value of $p \neq 1$, the connectivity threshold matches the prescription (17), namely $K = \widehat{\tau}(p) \log n$. It is also seen that, if the channel is poor, i.e., if p is close to zero, then the required value for K to ensure connectivity can be much larger than the one in the

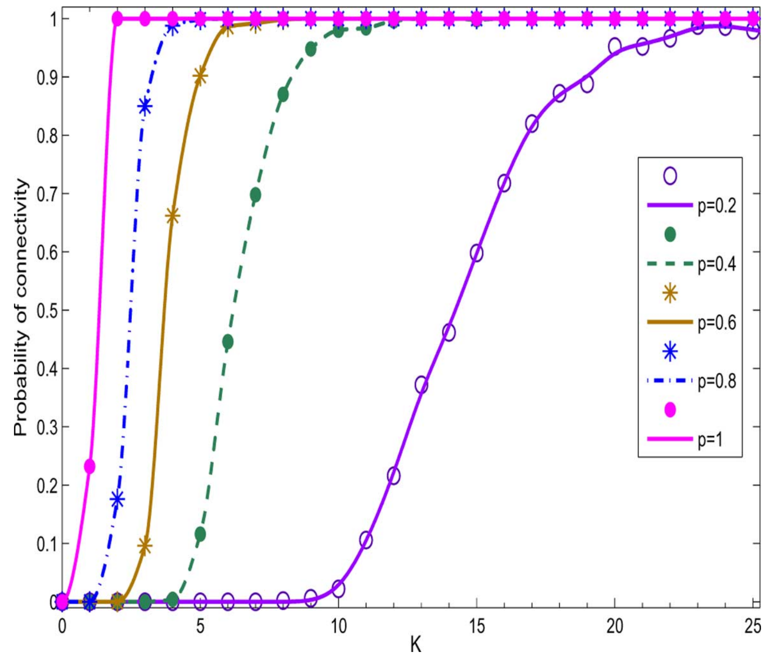

Fig. 1. Probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is connected as a function of K for $p = 0.2$, $p = 0.4$, $p = 0.6$, $p = 0.8$, and $p = 1$ with $n = 200$.

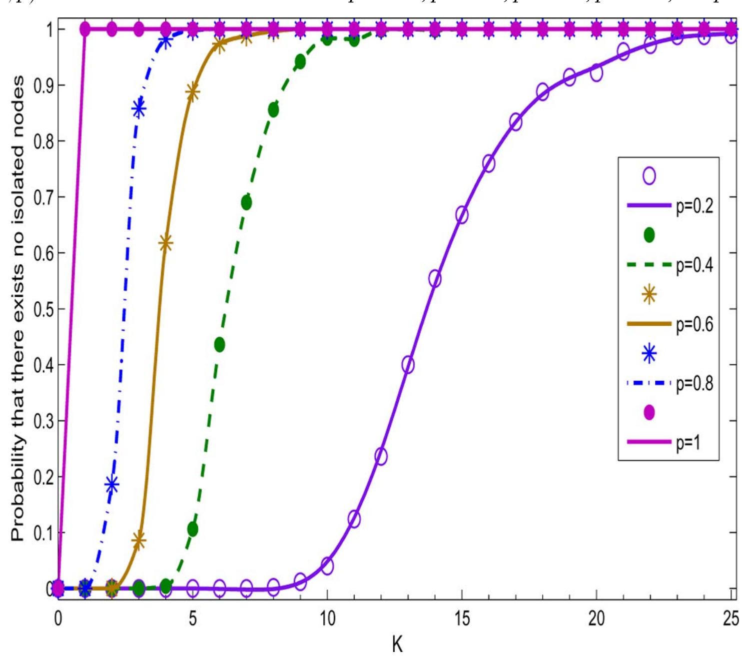

Fig. 2. Probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ has no isolated nodes as a function of K for $p = 0.2$, $p = 0.4$, $p = 0.6$, $p = 0.8$, and $p = 1$ with $n = 200$. This figure clearly resembles Fig. 1 for all $p \neq 1$.

full-visibility case $p = 1$. The results regarding the absence of node isolation are displayed in Fig. 2. For each value of $p \neq 1$, Fig. 2 is indistinguishable from Fig. 1, with the difference between the estimated probabilities of graph connectivity and absence of isolated nodes being quite small, in agreement with (17).

V. Discussion and Comments

A. Comparing With the Full-Visibility Case

At this point, the reader may wonder as to what form would Theorem 4.2 take in the context of full visibility. In the setting developed here, this corresponds to $p = 1$ so that $\mathbb{H} \cap \mathbb{G}(n; \theta)$ coincides with $\mathbb{H}(n; K)$; see the curve for $p = 1$ in Fig. 1. Results for this case were given by Fenner and Frieze [12, Th. 2.1, p. 348], and by the authors in [31] and [33].

Theorem 5.1: For any K a positive integer, it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; K) \text{ is connected}\right] = \begin{cases} 0 & \text{if } K = 1 \\ 1 & \text{if } K \geq 2. \end{cases}$$

The case where the parameter K is scaled with n is an easy corollary of Theorem 5.1.

Corollary 5.2: For any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n \geq 2$ for all n sufficiently large, we have the one-law

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; K_n) \text{ is connected}\right] = 1.$$

Each node in $\mathbb{H}(n;K)$ has degree at least K, so that no node is ever isolated in $\mathbb{H}(n;K)$. This is in sharp contrast with the model studied here, as reflected by the full zero-one law for node isolation given in Theorem 4.1.

Theorem 5.1 and its Corollary 5.2 together show that very small values of K suffice to ensure asymptotically almost sure (a.a.s.) connectivity of the random graph $\mathbb{H}(n;K)$. However, these two results cannot be recovered from Theorem 4.2 whose zero-one law is derived under the assumption $p_n < 1$ for all $n = 1, 2, \ldots$. Furthermore, even if the scaling $p : \mathbb{N}_0 \to (0,1)$ were to satisfy $\lim_{n\to\infty} p_n = 1$, only the one-law in Theorem 4.3 remains since $\tau(p^\star) = 0$ (and $\widehat{\tau}(p^\star) = 0$) at $p^\star = 1$. Although this might perhaps be expected given the aforementioned absence of isolated nodes in $\mathbb{H}(n;K)$, the one-laws for both the absence of isolated nodes and graph connectivity in $\mathbb{H}\cap\mathbb{G}(n;\theta)$ still require conditions on the behavior of the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$, namely (16) (whereas Corollary 5.2 does not).

B. Comparing $\mathbb{H} \cap \mathbb{G}(n;\theta)$ With ER Graphs

In the original paper of Chan *et al.* [7] (as in [14]), the connectivity analysis of the pairwise scheme was based on ER graphs [5]—It was assumed that the random graph induced by the pairwise scheme under a communication model (taken mostly to be the disk model [13]) behaves *like* an ER graph; similar assumptions have been made in [11] and [14] when discussing the connectivity of the EG scheme. However, this assumption was made without any formal justification. Recently, we have shown that the full-visibility model $\mathbb{H}(n;K)$ has major differences with ER graphs. For instance, the edge assignments are (negatively) correlated in $\mathbb{H}(n;K)$ while independent in ER graphs; see [25, Ch. 3.2, pp. 32–35], for a detailed discussion on the differences of $\mathbb{H}(n;K)$ and $\mathbb{G}(n;p)$. It is easy to verify that the edge assignments in $\mathbb{H} \cap \mathbb{G}(n;\theta)$ are also negatively correlated; see Section IX. Therefore, the models $\mathbb{H}(n;K)$ and $\mathbb{H} \cap \mathbb{G}(n;\theta)$ cannot be equated with an ER graph, and the results obtained in [31], [33] and in this paper are *not* mere consequences of classical results for ER graphs.

However, *formal* similarities do exist between $\mathbb{H} \cap \mathbb{G}(n;\theta)$ and ER graphs. Recall the following well-known zero-one law for ER graphs: For any scaling $p : \mathbb{N}_0 \to [0,1]$ satisfying

$$p_n \sim c\,\frac{\log n}{n}$$

for some $c > 0$, it holds that

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

On the other hand, the condition (10) can be rephrased more compactly as

$$p_n \lambda_n(K_n) \sim c\,\frac{\log n}{n}, \qquad c > 0$$

with the results (11) and (14) unchanged. Hence, in both ER graphs and $\mathbb{H} \cap \mathbb{G}(n;\theta)$, the zero-one laws can be expressed as a comparison of the probability of link assignment against the critical scaling $\frac{\log n}{n}$; this is also the case for random geometric graphs [19], and random key graphs [3], [18], [30]. But the condition $c > \tau(p^\star)$ that ensures a.a.s. connectivity in $\mathbb{H}\cap\mathbb{G}(n;\theta)$ is not the same as the condition $c > 1$ for a.a.s. connectivity in ER graphs; see Fig. 3. Thus, the connectivity behavior of the model $\mathbb{H}\cap\mathbb{G}(n;\theta)$ is in general different from that in an ER graph, and a "transfer" of the connectivity results from ER graphs cannot be taken for granted. Yet, the comparison becomes more subtle when the channel is poor: The connectivity behaviors of the two models do match in the practically relevant case for WSNs, i.e., when $\lim_{n\to\infty} p_n = 0$ since then $\tau(p^\star) = \tau(0) = 1$.

C. A More Realistic Communication Model

One possible extension of the work presented here would be to consider a more realistic communication model, e.g., the popular disk model [13] which takes into account the geographical positions of the sensor nodes. For instance, assume that the nodes are distributed over a bounded region $\mathcal{D}$ of the plane. According to the *disk model*, nodes i and j located at $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$, respectively, in $\mathcal{D}$ are able to communicate if

$$\|\boldsymbol{x_i} - \boldsymbol{x_j}\| < \rho \tag{19}$$

where $\rho > 0$ is called the transmission range. When the node locations are independently and uniformly distributed over the region $\mathcal{D}$, the graph induced under the condition (19) is known as a random geometric graph [19], thereafter denoted $\mathbb{G}(n;\rho)$.

Under the disk model, studying the pairwise scheme of Chan *et al.* amounts to analyzing the intersection of $\mathbb{H}(n;K)$ and $\mathbb{G}(n;\rho)$, say $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$. A direct analysis of this model seems to be very challenging; see the following for more on this. However, limited simulations already suggest that the zero-one laws obtained here for $\mathbb{H} \cap \mathbb{G}(n;K,p)$ have an analog for the model $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$. To verify this, consider 200 nodes distributed uniformly and independently over a folded unit square $[0,1]^2$ with toroidal (continuous) boundary conditions. Since there are no border effects, it is easy to check that

$$\mathbb{P}\left[\|\boldsymbol{x_i} - \boldsymbol{x_j}\| < \rho\right] = \pi\rho^2, \qquad \begin{matrix} i \neq j \\ i,j = 1,2,\ldots,n \end{matrix}$$

whenever $\rho < 0.5$. We match the two communication models $\mathbb{G}(n;p)$ and $\mathbb{G}(n;\rho)$ by requiring $\pi\rho^2 = p$. Then, we use the same procedure that produced Fig. 1 to obtain the empirical probability that $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ is connected for various values of K and p. The results are depicted in Fig. 4 whose resemblance with Fig. 1 suggests that the connectivity behaviors of the models $\mathbb{H} \cap \mathbb{G}(n;K,p)$ and $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ are quite similar. This raises the possibility that the results obtained here for the on/off communication model can also be used for dimensioning the pairwise scheme under the disk model.

A complete analysis of $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ is likely to be very challenging given the difficulties already encountered in the analysis of related problems. For example, the intersection of random geometric graphs with ER graphs was considered in [2] and [34]. Although zero-one laws for graph connectivity are available for each component random graph, results for the intersection model given in these references were limited only to the absence of isolated nodes; the connectivity problem is still open for that model. Yi *et al.* [34] also consider the intersection of random key graphs with random geometric graphs, but these results are again limited to the property of node isolation. To the best of our knowledge, Theorem 4.2 reported here constitutes the *first* zero-one law for graph connectivity in a model formed by intersecting multiple random graphs! (Except of course the

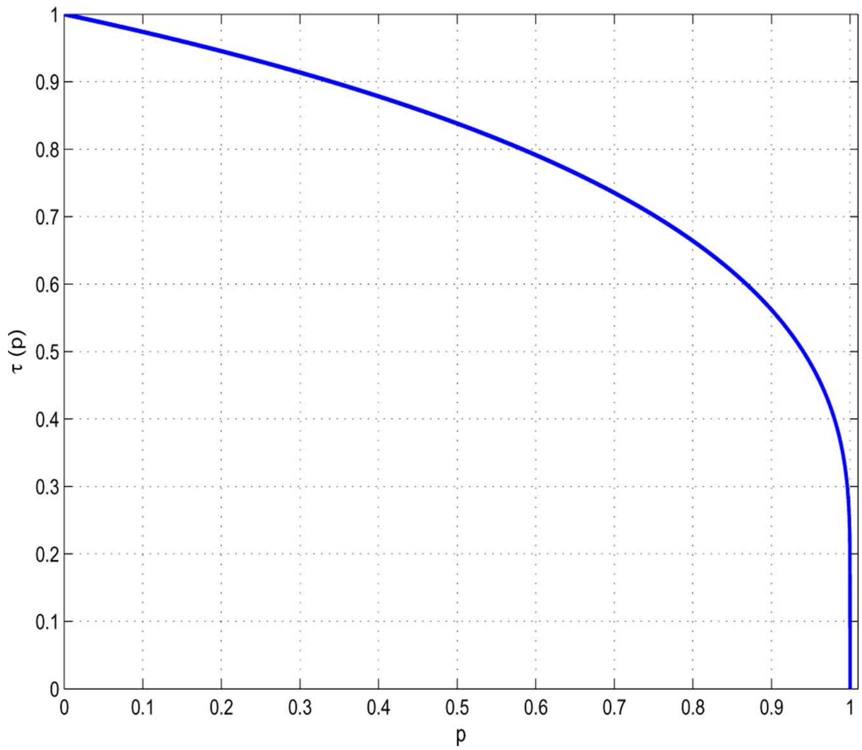

Fig. 3. $\tau(p)$ versus p. Clearly, $\tau(p^\star) = 1$ only if $p^\star = 0$.

trivial case where an ER graph intersects another ER graph.) As mentioned previously, Yağan [24] has recently established analogous zero-one laws for the connectivity of random key graphs intersecting ER graphs.

D. Intersection of Random Graphs

When using random graph models to study networks, situations arise where the notion of adjacency between nodes reflects multiple constraints. This can be so even when dealing with networks other than WSNs. As was the case here, such circumstances call for studying models that are constructed by taking the intersection of multiple random graphs. However, the availability of results for each component model does not necessarily imply such results for the intersection of these models; see the examples provided in the previous section.

Figs. 5–7 can help better understand the relevant issues as to why this is so: Fig. 5 provides a sample of an ER graph $\mathbb{G}(n,p)$ with $n = 200$ and $p = 0.2$. As would be expected from the classical results, the obtained graph is very densely connected. Similarly, Fig. 6 provides a sample of the pairwise random graph $\mathbb{H}(n;K)$ with $n = 200$ and $K = 5$. In line with Theorem 5.1, the obtained graph is connected. On the other hand, the graph formed by intersecting these graphs turns out to be *disconnected* as shown in Fig. 7.

To drive this point further, consider the constant parameter case for the models $\mathbb{H}(n;K)$ and $\mathbb{G}(n;p)$, a case which cannot be recovered from either Theorem 4.1 or Theorem 4.2. Nevertheless, Theorem 5.1 yields

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n;K) \text{ is connected}\right] = 1, \quad K \geq 2$$

while it is well known [5] that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p) \text{ is connected}\right] = 1, \quad 0 < p < 1.$$

However, it can be shown that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta) \text{ contains no isolated nodes}\right] = 0 \quad (20)$$

whence

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta) \text{ is connected}\right] = 0. \quad (21)$$

For details, see the discussion at the end of Section X. This clearly provides a *nontrivial* example (one that is not for an ER intersecting an ER graph) where the intersection of two random graphs is indeed a.a.s. *not* connected although each of the components is a.a.s. connected.

VI. A Proof of Theorem 4.1

We prove Theorem 4.1 by the method of first and second moments [15, p. 55] applied to the total number of isolated nodes in $\mathbb{H} \cap \mathbb{G}(n;\theta)$. First some notation: Fix $n = 2, 3, \ldots$ and consider $\theta = (K, p)$ with p in $(0,1)$ and positive integer K such that $K < n$. With

$$\chi_{n,i}(\theta) = \mathbf{1}\left[\text{Node } i \text{ is isolated in } \mathbb{H} \cap \mathbb{G}(n;\theta)\right]$$

for each $i = 1, \ldots, n$, the number of isolated nodes in $\mathbb{H} \cap \mathbb{G}(n;\theta)$ is simply given by

$$I_n(\theta) = \sum_{i=1}^{n} \chi_{n,i}(\theta).$$

The random graph $\mathbb{H} \cap \mathbb{G}(n;\theta)$ has no isolated nodes if and only if $I_n(\theta) = 0$.

The method of first moment [15, eq. (3.10), p. 55] relies on the well-known bound

$$1 - \mathbb{E}\left[I_n(\theta)\right] \leq \mathbb{P}\left[I_n(\theta) = 0\right] \quad (22)$$

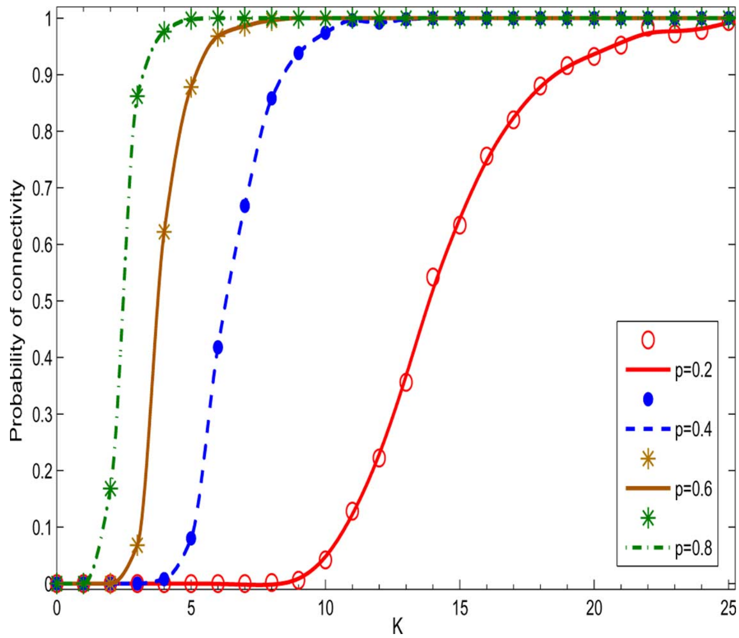

Fig. 4. Probability that $\mathbb{H} \cap \mathbb{G}(n; K, \rho)$ is connected as a function of K. The number of nodes is set to $n = 200$ and ρ is given by $\pi\rho^2 = p$.

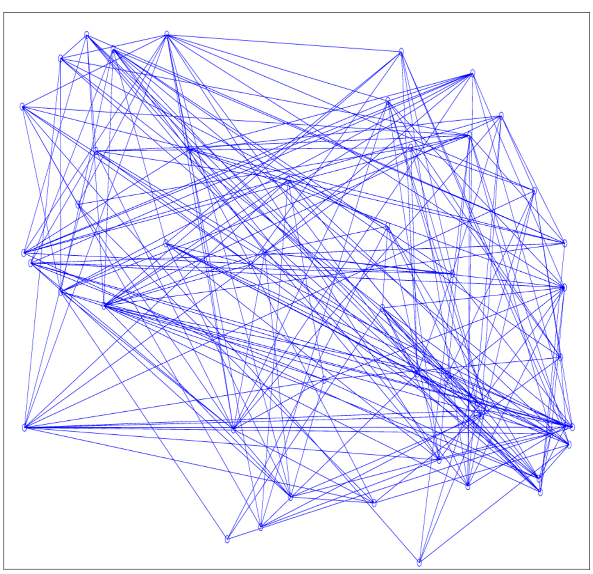

Fig. 5. Instantiation of ER graph $\mathbb{G}(n; p)$ with $n = 50$ and $p = 0.2$.—The graph is connected.

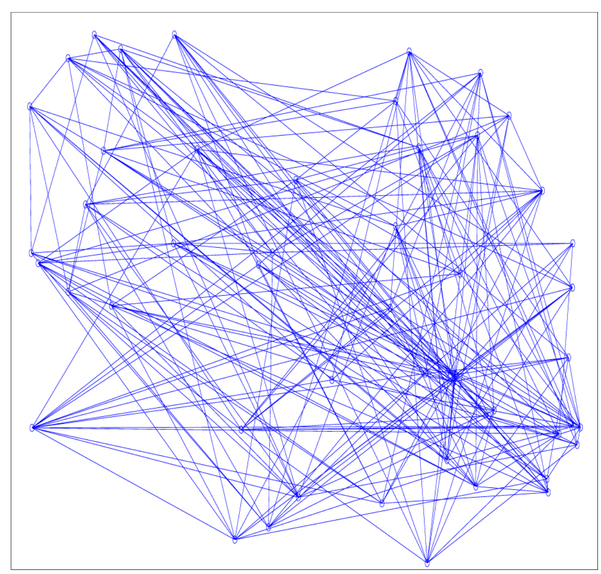

Fig. 6. Instantiation of $\mathbb{H}(n; K)$ with $n = 50$ and $K = 5$.—The graph is connected.

while the method of second moment [15, Remark 3.1, p. 55] has its starting point in the inequality

$$\mathbb{P}\left[I_n(\theta) = 0\right] \leq 1 - \frac{\mathbb{E}\left[I_n(\theta)\right]^2}{\mathbb{E}\left[I_n(\theta)^2\right]}. \tag{23}$$

The rvs $\chi_{n,1}(\theta), \ldots, \chi_{n,n}(\theta)$ being exchangeable, we find

$$\mathbb{E}\left[I_n(\theta)\right] = n\mathbb{E}\left[\chi_{n,1}(\theta)\right] \tag{24}$$

and

$$\mathbb{E}\left[I_n(\theta)^2\right] = n\mathbb{E}\left[\chi_{n,1}(\theta)\right] + n(n-1)\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]$$

by the binary nature of the rvs involved. It then follows that

$$\frac{\mathbb{E}\left[I_n(\theta)^2\right]}{\mathbb{E}\left[I_n(\theta)\right]^2} = \frac{1}{n\mathbb{E}\left[\chi_{n,1}(\theta)\right]} + \frac{n-1}{n} \cdot \frac{\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\theta)\right]\right)^2}. \tag{25}$$

From (22) and (24), it is plain that the one-law $\lim_{n\to\infty} \mathbb{P}\left[I_n(\theta_n) = 0\right] = 1$ will be established if we show that

$$\lim_{n\to\infty} n\mathbb{E}\left[\chi_{n,1}(\theta_n)\right] = 0. \tag{26}$$

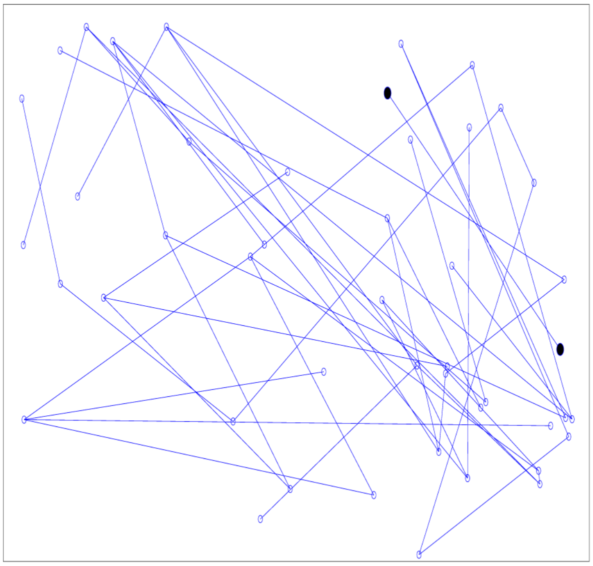

Fig. 7. Intersection $\mathbb{H} \cap \mathbb{G}(n;\theta)$ of the graphs in Figs. 5 and 6—The graph is disconnected as the marked nodes form a component!

From (23) and (25), we see that the zero-law $\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n) = 0] = 0$ holds if

$$\lim_{n\to\infty} n\mathbb{E}[\chi_{n,1}(\theta_n)] = \infty \tag{27}$$

and

$$\limsup_{n\to\infty} \left(\frac{\mathbb{E}[\chi_{n,1}(\theta_n)\chi_{n,2}(\theta_n)]}{(\mathbb{E}[\chi_{n,1}(\theta_n)])^2} \right) \le 1. \tag{28}$$

The proof of Theorem 4.1 passes through the next two technical propositions which establish (26)–(28) under the appropriate conditions on the scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$.

Proposition 6.1: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that (10) holds for some $c > 0$. Assume also that $\lim_{n\to\infty} p_n = p^\star$ exists. Then, we have

$$\lim_{n\to\infty} n\mathbb{E}[\chi_{n,1}(\theta_n)] = \begin{cases} 0 & \text{if } c > \tau(p^\star) \\ \infty & \text{if } c < \tau(p^\star) \end{cases} \tag{29}$$

where the threshold $\tau(p^\star)$ is given by (9).

A proof of Proposition 6.1 is given in Section VIII.

Proposition 6.2: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that (10) holds for some $c > 0$. Assume also that $\lim_{n\to\infty} p_n = p^\star$ exists. Then, we have (28) whenever $p^\star < 1$.

A proof of Proposition 6.2 can be found in Section X. To complete the proof of Theorem 4.1, pick a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ such that (10) holds for some $c > 0$ and $\lim_{n\to\infty} p_n = p^\star$ exists. Under the condition $c > \tau(p^\star)$ we get (26) from Proposition 6.1, and the one-law $\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n) = 0] = 1$ follows. Next, assume that $c < \tau(p^\star)$—This case is possible only if $p^\star < 1$ since $\tau(1) = 0$ as seen at (9). When $p^\star < 1$, we obtain (27) and (28) with the help of Propositions 6.1 and 6.2, respectively. The conclusion $\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n) = 0] = 0$ is now immediate.

VII. A Preparatory Result

Fix $n = 2, 3, \ldots$ and consider $\theta = (K, p)$ with p in $(0,1)$ and positive integer K such that $K < n$. Under the enforced assumptions, for each $i = 1, \ldots, n$, we easily get

$$\mathbb{E}[\chi_{n,i}(\theta)] = \mathbb{E}\left[(1-p)^{D_{n,i}(K)}\right] \tag{30}$$

where $D_{n,i}(K)$ denotes the degree of node i in $\mathbb{H}(n;K)$. Note that

$$D_{n,i}(K) = K + \sum_{j=1, j\notin \Gamma_{n,i}(K)\cup\{i\}}^{n} \mathbf{1}[i \in \Gamma_{n,j}(K)]. \tag{31}$$

By independence, since

$$|\{j = 1, \ldots, n : j \notin \Gamma_{n,i}(K) \cup \{i\}\}| = n - K - 1$$

the second term in (31) is a binomial rv with $n - K - 1$ trials and success probability given by

$$\mathbb{P}[i \in \Gamma_{n,j}(K)] = \frac{\binom{n-2}{K-1}}{\binom{n-1}{K}} = \frac{K}{n-1} \tag{32}$$

whence

$$\mathbb{E}[\chi_{n,i}(\theta)] = (1-p)^K \cdot \left(1 - \frac{pK}{n-1}\right)^{n-K-1}. \tag{33}$$

The proof of Proposition 6.1 uses a somewhat simpler form of the expression (33) which we develop next.

Lemma 7.1: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that (10) holds for some $c > 0$. It holds that

$$n\mathbb{E}[\chi_{n,1}(\theta_n)] = e^{\alpha_n + o(1)}, \quad n = 1, 2, \ldots \tag{34}$$

with

$$\alpha_n = (1 - c_n)\log n + K_n(p_n + \log(1 - p_n)) \tag{35}$$

where the sequence $c : \mathbb{N}_0 \to \mathbb{R}$ is the one appearing in the form (12) of the condition (10).

In what follows, we make use of the decomposition

$$\log(1 - x) = -x - \Psi(x), \quad 0 \le x < 1 \tag{36}$$

with

$$\Psi(x) = \int_0^x \frac{t}{1-t} dt$$

on that range. Note that

$$\lim_{x\downarrow 0} \frac{\Psi(x)}{x^2} = \frac{1}{2}.$$

Proof: Consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ such that (10) holds for some $c > 0$ and assume the existence of the limit $\lim_{n\to\infty} p_n = p^\star$. Replacing θ by θ_n in (33) for each $n = 2, 3, \ldots$, we get

$$n\mathbb{E}\left[\chi_{n,1}(\theta_n)\right] = e^{\beta_n} \tag{37}$$

with β_n given by

$$\beta_n = \log n + K_n \log(1 - p_n) - \gamma_n$$

where

$$\gamma_n = -(n - K_n - 1)\log\left(1 - \frac{p_n K_n}{n-1}\right).$$

The decomposition (36) now yields

$$\begin{aligned}
\gamma_n &= (n - K_n - 1)\left(\frac{p_n K_n}{n-1} + \Psi\left(\frac{p_n K_n}{n-1}\right)\right) \\
&= p_n K_n\left(1 - \frac{K_n}{n-1}\right) + (n - K_n - 1)\Psi\left(\frac{p_n K_n}{n-1}\right) \\
&= -\, p_n K_n + p_n K_n\left(2 - \frac{K_n}{n-1}\right) \\
&\qquad + (n - K_n - 1)\Psi\left(\frac{p_n K_n}{n-1}\right) \\
&= -\, p_n K_n + c_n \log n + (n - K_n - 1)\Psi\left(\frac{p_n K_n}{n-1}\right)
\end{aligned}$$

where the last step used the form (12) of the condition (10) on the scaling. Reporting this calculation into the expression for β_n, we find

$$\beta_n = \alpha_n - (n - K_n - 1)\Psi\left(\frac{p_n K_n}{n-1}\right).$$

Lemma 7.1 will be established if we show that

$$\lim_{n\to\infty} (n - K_n - 1)\Psi\left(\frac{p_n K_n}{n-1}\right) = 0. \tag{38}$$

To that end, for each $n = 2, 3, \ldots$, we note the inequalities

$$p_n K_n \le p_n\left(2K_n - \frac{K_n^2}{n-1}\right) \le 2p_n K_n$$

by virtue of the fact that $K_n < n$. The condition (12) implies

$$\frac{c_n}{2}\log n \le p_n K_n \le c_n \log n \tag{39}$$

hence

$$\lim_{n\to\infty} \frac{p_n K_n}{n-1} = 0 \tag{40}$$

and

$$\lim_{n\to\infty} (n - K_n - 1)\frac{p_n^2 K_n^2}{(n-1)^2} = 0.$$

Invoking the behavior of $\Psi(x)$ at $x = 0$ mentioned earlier, we conclude from these facts that

$$\lim_{n\to\infty}\left((n - K_n - 1)\frac{p_n^2 K_n^2}{(n-1)^2}\right)\left(\frac{\Psi\left(\frac{p_n K_n}{n-1}\right)}{\left(\frac{p_n K_n}{n-1}\right)^2}\right) = 0. \tag{41}$$

This establishes (38) and the proof of Lemma 7.1 is completed. ■

VIII. A Proof of Proposition 6.1

In view of Lemma 7.1, Proposition 6.1 will be established if we show

$$\lim_{n\to\infty} \alpha_n = \begin{cases} -\infty & \text{if } c > \tau(p^\star) \\ +\infty & \text{if } c < \tau(p^\star). \end{cases} \tag{42}$$

To see this, first note from (36) that for each $n = 1, 2, \ldots$, we have $p_n + \log(1 - p_n) \le 0$ and the lower bound in (39) implies

$$\begin{aligned}
\alpha_n &\le (1 - c_n)\log n + c_n\left(\frac{\log n}{2p_n}\right)\cdot(p_n + \log(1 - p_n)) \\
&= \left(1 - \frac{c_n}{2}\left(1 - \frac{\log(1 - p_n)}{p_n}\right)\right)\cdot \log n.
\end{aligned} \tag{43}$$

Letting n go to infinity in this last expression yields $\lim_{n\to\infty} \alpha_n = -\infty$ whenever

$$c > \lim_{n\to\infty} \frac{2}{1 - \frac{\log(1-p_n)}{p_n}} = \tau(p^\star) \tag{44}$$

since $\lim_{n\to\infty} c_n = c$.

Next, we show that if $c < \tau(p^\star)$, then $\lim_{n\to\infty} \alpha_n = +\infty$. We only need to consider the case $0 \le p^\star < 1$ since $\tau(1) = 0$ and the constraint $c < \tau(1)$ is then vacuous. We begin by assuming $p^\star = 0$, in which case for each $n = 2, 3, \ldots$, we have

$$\begin{aligned}
\alpha_n &= (1 - c_n)\log n + K_n(p_n + (-p_n - \Psi(p_n))) \\
&= (1 - c_n)\log n - K_n \Psi(p_n) \\
&= (1 - c_n)\log n - \left(\frac{\Psi(p_n)}{p_n^2}\right)\cdot K_n p_n^2 \\
&\ge (1 - c_n)\log n - c_n \log n \cdot \left(\frac{\Psi(p_n)}{p_n^2}\right) p_n \\
&= \left(1 - c_n\left(1 + \left(\frac{\Psi(p_n)}{p_n^2}\right) p_n\right)\right)\cdot \log n
\end{aligned} \tag{45}$$

with the inequality following from the upper bound in (39). Let n grow large in the last expression. Since we have assumed $\lim_{n\to\infty} p_n = 0$, we get

$$\lim_{n\to\infty} p_n\left(\frac{\Psi(p_n)}{p_n^2}\right) = 0$$

and the desired conclusion $\lim_{n\to\infty} \alpha_n = +\infty$ is obtained whenever $c < 1 = \tau(0)$ because $\lim_{n\to\infty} c_n = c$.

Finally, we assume $0 < p^\star < 1$. For each $\varepsilon > 0$, there exists a finite positive integer $n^\star(\varepsilon)$ such that $p_n \ge (1 - \varepsilon)p^\star$ when $n \ge n^\star(\varepsilon)$. On that range, the upper bound in (39) yields

$$K_n \le \frac{c}{(1 - \varepsilon)p^\star}\cdot \log n$$

and the conclusions $K_n^2 = o(n)$ and

$$p_n\left(2K_n - \frac{K_n^2}{n-1}\right) = 2p_n K_n + o(1)$$

follow. Comparing this last fact against the left-hand side of (12) yields

$$p_nK_n = \frac{c_n}{2}\log n + o(1)$$

so that

$$p_nK_n \sim \frac{c_n}{2}\log n. \tag{46}$$

From (35), it follows that

$$\frac{\alpha_n}{\log n} = (1-c_n) + \left(1+\frac{\log(1-p_n)}{p_n}\right)\cdot\frac{p_nK_n}{\log n}$$

for all n sufficiently large. Letting n go to infinity in this last expression and using (46) with earlier remarks, we readily conclude

$$\lim_{n\to\infty}\frac{\alpha_n}{\log n} = (1-c) + \frac{c}{2}\left(1+\frac{\log(1-p^\star)}{p^\star}\right) = 1-\frac{c}{\tau(p^\star)}$$

by direct inspection. It is now clear that $\lim_{n\to\infty}\alpha_n = \infty$ when $c < \tau(p^\star)$ with $0 < p^\star < 1$. The proof of Proposition 6.1 is now completed. ■

IX. Negative Dependence and Consequences

Fix positive integers $n = 2, 3, \ldots$ and K with $K < n$. Several properties of the $\{0,1\}$-valued rvs

$$\left\{\mathbf{1}\left[j\in\Gamma_{n,i}(K)\right], \quad \begin{array}{c} i\neq j \\ i,j=1,\ldots,n\end{array}\right\} \tag{47}$$

and

$$\left\{\mathbf{1}\left[j\in\Gamma_{n,i}(K)\vee i\in\Gamma_{n,j}(K)\right], \quad \begin{array}{c} i\neq j \\ i,j=1,\ldots,n\end{array}\right\} \tag{48}$$

will play a key role in some of the forthcoming arguments.

A. Negative Association

The properties of interest can be couched in terms of *negative association*, a form of negative correlation introduced by Joag-Dev and Proschan [16]. We first develop the needed definitions and properties: Let $\{X_\lambda,\ \lambda\in\Lambda\}$ be a collection of $\mathbb{R}$-valued rvs indexed by the finite set Λ. For any nonempty subset A of Λ, we write X_A to denote the $\mathbb{R}^{|A|}$-valued $X_A = (X_\lambda,\ \lambda\in A)$. The rvs $\{X_\lambda,\ \lambda\in\Lambda\}$ are then said to be negatively associated if for any nonoverlapping subsets A and B of Λ and for any monotone increasing mappings $\varphi : \mathbb{R}^{|A|}\to\mathbb{R}$ and $\psi:\mathbb{R}^{|B|}\to\mathbb{R}$, the covariance inequality

$$\mathbb{E}\left[\varphi(X_A)\psi(X_B)\right] \le \mathbb{E}\left[\varphi(X_A)\right]\mathbb{E}\left[\psi(X_B)\right] \tag{49}$$

holds whenever the expectations in (49) are well defined and finite. Note that φ and ψ need only be monotone increasing on the support of X_A and X_B, respectively.

This definition has some easy consequences to be used repeatedly in what follows: The negative association of $\{X_\lambda,\ \lambda\in\Lambda\}$ implies the negative association of the collection $\{X_\lambda,\ \lambda\in\Lambda'\}$ where Λ' is any subset of Λ. It is also well known [16, P2, p. 288] that the negative association of the rvs $\{X_\lambda,\ \lambda\in\Lambda\}$ implies the inequality

$$\mathbb{E}\left[\prod_{\lambda\in A} f_\lambda(X_\lambda)\right] \le \prod_{\lambda\in A}\mathbb{E}\left[f_\lambda(X_\lambda)\right] \tag{50}$$

where A is a subset of Λ and the collection $\{f_\lambda,\ \lambda\in A\}$ of mappings $\mathbb{R}\to\mathbb{R}_+$ are all monotone increasing; by nonnegativity, all the expectations exist and finiteness is moot.

We can apply these ideas to collections of indicator rvs, namely for each λ in Λ, $X_\lambda = \mathbf{1}\left[E_\lambda\right]$ for some event E_λ. From the definitions, it is easy to see that if the rvs $\{\mathbf{1}\left[E_\lambda\right],\ \lambda\in\Lambda\}$ are negatively associated, so are the rvs $\{\mathbf{1}\left[E_\lambda^c\right],\ \lambda\in\Lambda\}$. Moreover, for any subset A of Λ, we have

$$\mathbb{P}\left[E_\lambda,\ \lambda\in A\right] \le \prod_{\lambda\in A}\mathbb{P}\left[E_\lambda\right]. \tag{51}$$

This follows from (50) by taking $f_\lambda(x) = x^+$ on $\mathbb{R}$ for each λ in Λ.

B. Useful Consequences

A key observation for our purpose is as follows: For each $i = 1,\ldots,n$, the rvs

$$\{\mathbf{1}\left[j\in\Gamma_{n,i}(K)\right],\ j\in\mathcal{N}_{-i}\} \tag{52}$$

form a collection of negatively associated rvs. This is a consequence of the fact that the random set $\Gamma_{n,i}(K)$ represents a random sample (without replacement) of size K from $\mathcal{N}_{-i}$; see [16, Example 3.2(c)] for details.

The n collections (52) are mutually independent, so that by the "closure under products" property of negative association [16, P7, p. 288] [10, p. 35], the rvs (47) also form a collection of negatively associated rvs.

By taking complements, we see that the rvs

$$\left\{\mathbf{1}\left[j\notin\Gamma_{n,i}(K)\right], \quad \begin{array}{c} i\neq j \\ i,j=1,\ldots,n\end{array}\right\} \tag{53}$$

also form a collection of negatively associated rvs. With distinct $i,j = 1,\ldots,n$, we note that

$$\begin{aligned}&\mathbf{1}\left[i\notin\Gamma_{n,j}(K), j\notin\Gamma_{n,i}(K)\right]\\ &\quad = g\left(\mathbf{1}\left[i\notin\Gamma_{n,j}(K)\right], \mathbf{1}\left[j\notin\Gamma_{n,i}(K)\right]\right)\end{aligned}$$

with mapping $g:\mathbb{R}^2\to\mathbb{R}$ given by $g(x,y) = x^+y^+$ for all x,y in $\mathbb{R}$. This mapping being nondecreasing on $\mathbb{R}^2$, it follows [16, P6, p. 288] that the rvs

$$\left\{\mathbf{1}\left[j\notin\Gamma_{n,i}(K), i\notin\Gamma_{n,j}(K)\right], \quad \begin{array}{c} i\neq j \\ i,j=1,\ldots,n\end{array}\right\} \tag{54}$$

are also negatively associated. Taking complements one more time, we see that the rvs (48) are also negatively associated.

For each $k = 1, 2$ and $j = 3,\ldots,n$, we shall find it useful to define

$$u_{n,j,k}(\theta) = \mathbb{E}\left[(1-p)^{\mathbf{1}[k\in\Gamma_{n,j}(K)]}\right]$$

and

$$b_{n,j}(\theta) = \mathbb{E}\left[(1-p)^{\mathbf{1}[1\in\Gamma_{n,j}(K)]+\mathbf{1}[2\in\Gamma_{n,j}(K)]}\right].$$

Under the enforced assumptions, we have $b_{n,3}(\theta) = \cdots = b_{n,n}(\theta) \equiv b_n(\theta)$ and $u_{n,3,1}(\theta) = \cdots = u_{n,n,1}(\theta) = u_{n,3,2}(\theta) = \cdots = u_{n,n,2}(\theta) \equiv u_n(\theta)$.

Before computing either one of the quantities $u_n(\theta)$ and $b_n(\theta)$, we note that

$$b_n(\theta) \le u_n(\theta)^2. \tag{55}$$

This is a straightforward consequence of the negative association of the rvs (47)—In (49), with A and B singletons, use the increasing functions $\varphi, \psi : \mathbb{R} \to \mathbb{R} : x \to -(1-p)^x$.

Using (32), we get

$$\begin{aligned} u_n(\theta) &= (1-p)\frac{K}{n-1} + \left(1 - \frac{K}{n-1}\right) \\ &= 1 - \frac{pK}{n-1}. \end{aligned} \tag{56}$$

An expression for $b_n(\theta)$ is available but will not be needed due to the availability of (55).

X. A Proof of Proposition 6.2

As expected, the first step in proving Proposition 6.2 consists in evaluating the cross moment appearing in the numerator of (28). Fix $n = 2, 3, \ldots$ and consider $\theta = (K, p)$ with p in $(0, 1)$ and positive integer K such that $K < n$. Define the $\mathbb{N}_0$-valued rvs $B_n(\theta)$ and $U_n(\theta)$ by

$$B_n(\theta) = \sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,1}(K)]\,\mathbf{1}[j \notin \Gamma_{n,2}(K)] \tag{57}$$

and

$$\begin{aligned} U_n(\theta) = &\sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,1}(K)]\,\mathbf{1}[j \in \Gamma_{n,2}(K)] \\ &+ \sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,2}(K)]\,\mathbf{1}[j \in \Gamma_{n,1}(K)]. \end{aligned} \tag{58}$$

Proposition 10.1: Fix $n = 2, 3, \ldots$. For any p in $(0, 1)$ and positive integer K such that $K < n$, we have

$$\begin{aligned} &\mathbb{E}[\chi_{n,1}(\theta)\chi_{n,2}(\theta)] \\ &\quad = (1-p)^{2K}\mathbb{E}\left[\frac{b_n(\theta)^{B_n(\theta)} \cdot u_n(\theta)^{U_n(\theta)}}{(1-p)^{\mathbf{1}[2\in\Gamma_{n,1}(K),1\in\Gamma_{n,2}(K)]}}\right] \end{aligned} \tag{59}$$

where the rvs $B_n(\theta)$ and $U_n(\theta)$ are given by (57) and (58), respectively.

A proof of Proposition 10.1 is available in Appendix A. Still in the setting of Proposition 10.1, we use (55) in conjunction with (59) to get

$$\begin{aligned} &\mathbb{E}[\chi_{n,1}(\theta)\chi_{n,2}(\theta)] \\ &\quad \le (1-p)^{2K}\mathbb{E}\left[\frac{u_n(\theta)^{2B_n(\theta)+U_n(\theta)}}{(1-p)^{\mathbf{1}[2\in\Gamma_{n,1}(K),1\in\Gamma_{n,2}(K)]}}\right] \end{aligned} \tag{60}$$

where we find

$$\begin{aligned} &2B_n(\theta) + U_n(\theta) \\ &\quad = \sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,1}(K)] + \sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,2}(K)]. \end{aligned}$$

We note that

$$\begin{aligned} &\sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,1}(K)] \\ &\quad = \sum_{j=2}^{n} \mathbf{1}[j \notin \Gamma_{n,1}(K)] - \mathbf{1}[2 \notin \Gamma_{n,1}(K)] \\ &\quad = (n-1-K) - (1 - \mathbf{1}[2 \in \Gamma_{n,1}(K)]) \\ &\quad = (n-2-K) + \mathbf{1}[2 \in \Gamma_{n,1}(K)] \end{aligned}$$

and

$$\sum_{j=3}^{n} \mathbf{1}[j \notin \Gamma_{n,2}(K)] = (n-2-K) + \mathbf{1}[1 \in \Gamma_{n,2}(K)]$$

by similar arguments. The expression

$$\begin{aligned} &2B_n(\theta) + U_n(\theta) \\ &\quad = 2(n-2-K) + \mathbf{1}[2 \in \Gamma_{n,1}(K)] + \mathbf{1}[1 \in \Gamma_{n,2}(K)] \end{aligned}$$

readily follows, and the inequality

$$\mathbb{E}[\chi_{n,1}(\theta)\chi_{n,2}(\theta)] \le (1-p)^{2K} u_n(\theta)^{2(n-2-K)} \cdot R_n(\theta)$$

is obtained upon using (60), with $R_n(\theta)$ given by

$$R_n(\theta) = \mathbb{E}\left[\frac{u_n(\theta)^{\mathbf{1}[2\in\Gamma_{n,1}(K)]+\mathbf{1}[1\in\Gamma_{n,2}(K)]}}{(1-p)^{\mathbf{1}[2\in\Gamma_{n,1}(K),1\in\Gamma_{n,2}(K)]}}\right].$$

Next, with the help of (33) and (56), we conclude that

$$\begin{aligned} &\frac{\mathbb{E}[\chi_{n,1}(\theta)\chi_{n,2}(\theta)]}{(\mathbb{E}[\chi_{n,1}(\theta)])^2} \\ &\quad \le \frac{(1-p)^{2K} \cdot u_n(\theta)^{2(n-2-K)}}{((1-p)^K \cdot u_n(\theta)^{n-1-K})^2} \cdot R_n(\theta) \\ &\quad = u_n(\theta)^{-2} R_n(\theta) \\ &\quad = \mathbb{E}\left[\frac{u_n(\theta)^{\mathbf{1}[2\in\Gamma_{n,1}(K)]+\mathbf{1}[1\in\Gamma_{n,2}(K)]-2}}{(1-p)^{\mathbf{1}[2\in\Gamma_{n,1}(K),1\in\Gamma_{n,2}(K)]}}\right]. \end{aligned} \tag{61}$$

Direct inspection readily yields

$$\begin{aligned} &\frac{u_n(\theta)^{\mathbf{1}[2\in\Gamma_{n,1}(K)]+\mathbf{1}[1\in\Gamma_{n,2}(K)]-2}}{(1-p)^{\mathbf{1}[2\in\Gamma_{n,1}(K),1\in\Gamma_{n,2}(K)]}} \\ &\quad = \begin{cases} \frac{1}{1-p} & \text{if } 2 \in \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,2}(K) \\ \left(1 - \frac{pK}{n-1}\right)^{-2} & \text{if } 2 \notin \Gamma_{n,1}(K),\ 1 \notin \Gamma_{n,2}(K) \\ \left(1 - \frac{pK}{n-1}\right)^{-1} & \text{otherwise.} \end{cases} \end{aligned}$$

Taking expectation and recalling (32), we conclude from (61) that

$$\begin{aligned}
&\frac{\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\theta)\right]\right)^2}\\
&\le \left(1-\frac{pK}{n-1}\right)^{-2}\left(1-\mathbb{P}\left[2\in\Gamma_{n,1}(K), 1\in\Gamma_{n,2}(K)\right]\right)\\
&\quad + \frac{1}{1-p}\mathbb{P}\left[2\in\Gamma_{n,1}(K), 1\in\Gamma_{n,2}(K)\right]\\
&= \left(\frac{K}{n-1}\right)^2\left(\frac{1}{1-p}-\left(1-\frac{pK}{n-1}\right)^{-2}\right)\\
&\quad + \left(1-\frac{pK}{n-1}\right)^{-2}\\
&\le \left(\frac{K}{n-1}\right)^2\left(\frac{1}{1-p}-\frac{1}{1-\frac{pK}{n-1}}\right)+\left(1-\frac{pK}{n-1}\right)^{-2}\\
&\le \frac{K}{n-1}\cdot\frac{p(1-\frac{K}{n-1})}{(1-p)(1-\frac{pK}{n-1})}+\left(1-\frac{pK}{n-1}\right)^{-2}\\
&\le \frac{pK}{n-1}\cdot\frac{1}{(1-p)(1-\frac{pK}{n-1})}+\left(1-\frac{pK}{n-1}\right)^{-2} \qquad (62)
\end{aligned}$$

by crude bounding arguments.

Now, consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ such that (10) holds for some $c > 0$ and $\lim_{n\to\infty} p_n = p^\star < 1$. Replace θ by θ_n in the bound (62) according to this scaling, and let n go to infinity in the resulting inequality. From (39), we get both (40) and

$$\lim_{n\to\infty}\frac{1}{1-p_n}\left(\frac{p_nK_n}{n-1}\right)\left(1-\frac{p_nK_n}{n-1}\right)^{-1}=0$$

since $\lim_{n\to\infty} p_n = p^\star < 1$. This completes the proof of (28). ■

We close with a proof of (20): Consider $\theta = (K,p)$ with p in $(0,1)$ and positive integer K. It follows from (33) that

$$\lim_{n\to\infty}\mathbb{E}\left[\chi_{n,1}(\theta)\right]=(1-p)^K e^{-pK}$$

whence $\lim_{n\to\infty}\mathbb{E}\left[I_n(\theta)\right]=\infty$. It also immediate from (62) that

$$\limsup_{n\to\infty}\frac{\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\theta)\right]\right)^2}\le 1.$$

The arguments outlined in Section VI now yield

$$\lim_{n\to\infty}\mathbb{P}\left[I_n(\theta)=0\right]=0$$

and this establishes (20). The conclusion (21) immediately follows; see discussion at (63).

XI. A Proof of Theorem 4.2 (Part I)

Fix $n = 2,3,\ldots$ and consider $\theta = (K,p)$ with p in $(0,1)$ and positive integer K such that $K < n$. We define the events

$$C_n(\theta) = \left[\mathbb{H}\cap\mathbb{G}(n;\theta) \text{ is connected}\right]$$

and

$$I(n;\theta) = \left[\mathbb{H}\cap\mathbb{G}(n;\theta) \text{ contains no isolated nodes}\right].$$

If the random graph $\mathbb{H}\cap\mathbb{G}(n;\theta)$ is connected, then it does not contain any isolated node, whence $C_n(\theta)$ is a subset of $I(n;\theta)$, and the conclusions

$$\mathbb{P}\left[C_n(\theta)\right]\le\mathbb{P}\left[I(n;\theta)\right] \qquad (63)$$

and

$$\mathbb{P}\left[C_n(\theta)^c\right]=\mathbb{P}\left[C_n(\theta)^c\cap I(n;\theta)\right]+\mathbb{P}\left[I(n;\theta)^c\right] \qquad (64)$$

are obtained.

Taken together with Theorem 4.1, the relations (63) and (64) pave the way to proving Theorem 4.2. Indeed, pick a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0\times(0,1)$ such that (10) holds for some $c > 0$ and $\lim_{n\to\infty} p_n = p^\star$ exists. If $c < \tau(p^\star)$, then $\lim_{n\to\infty}\mathbb{P}\left[I(n;\theta_n)\right] = 0$ by the zero-law for the absence of isolated nodes, whence $\lim_{n\to\infty}\mathbb{P}\left[C_n(\theta_n)\right]=0$ with the help of (63). If $c > \tau(p^\star)$, then $\lim_{n\to\infty}\mathbb{P}\left[I(n;\theta_n)\right]=1$ by the one-law for the absence of isolated nodes, and the desired conclusion $\lim_{n\to\infty}\mathbb{P}\left[C_n(\theta_n)\right]=1$ (or equivalently, $\lim_{n\to\infty}\mathbb{P}\left[C_n(\theta_n)^c\right]=0$) will follow via (64) if we show the following.

Proposition 11.1: For any scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0\times(0,1)$ such that $\lim_{n\to\infty} p_n = p^\star$ exists and (10) holds for some $c > \tau(p^\star)$, we have

$$\lim_{n\to\infty}\mathbb{P}\left[C_n(\theta_n)^c\cap I(n;\theta_n)\right]=0. \qquad (65)$$

The proof of Proposition 11.1 starts below and runs through Sections XII–XV. The basic idea is to find a sufficiently tight upper bound on the probability in (65) and then to show that this bound goes to zero as n becomes large. This approach is similar to the one used for proving the one-law for connectivity in ER graphs [5, p. 164] and in random key graphs [3], [8], [30].

We begin by finding the needed upper bound: Fix $n = 2,3,\ldots$ and consider $\theta = (K,p)$ with p in $(0,1)$ and positive integer K such that $K < n$. For any nonempty subset S of nodes, i.e., $S\subseteq\{1,\ldots,n\}$, we define the graph $\mathbb{H}\cap\mathbb{G}(n;\theta)(S)$ (with vertex set S) as the subgraph of $\mathbb{H}\cap\mathbb{G}(n;\theta)$ restricted to the nodes in S. We also say that S is *isolated* in $\mathbb{H}\cap\mathbb{G}(n;\theta)$ if there are no edges (in $\mathbb{H}\cap\mathbb{G}(n;\theta)$) between the nodes in S and the nodes in the complement $S^c = \{1,\ldots,n\}-S$. This is characterized by

$$\Sigma_{n,i}(K)\cap\Sigma_{n,j}(K)=\emptyset\vee B_{ij}(p)=0,\quad i\in S,\ j\in S^c.$$

With each nonempty subset S of nodes, we associate several events of interest: Let $C_n(\theta;S)$ denote the event that the subgraph $\mathbb{H}\cap\mathbb{G}(n;\theta)(S)$ is itself connected. The event $C_n(\theta;S)$ is completely determined by the rvs $\{\Gamma_{n,i}(K),\ i\in S\}$ and $\{B_{ij}(p),\ i,j\in S\}$. We also introduce the event $B_n(\theta;S)$ to capture the fact that S is isolated in $\mathbb{H}\cap\mathbb{G}(n;\theta)$, i.e.,

$$B_n(\theta;S) = \left[\begin{array}{c}\Sigma_{n,i}(K)\cap\Sigma_{n,j}(K)=\emptyset\vee B_{ij}(p)=0,\\ i\in S,\ j\in S^c\end{array}\right].$$

Finally, we set

$$A_n(\theta;S) = C_n(\theta;S) \cap B_n(\theta;S).$$

The starting point of the discussion is the following basic observation: If $\mathbb{H} \cap \mathbb{G}(n;\theta)$ is *not* connected and yet has *no* isolated nodes, then there must exist a subset S of nodes with $|S| \geq 2$ such that $\mathbb{H} \cap \mathbb{G}(n;\theta)(S)$ is connected while S is isolated in $\mathbb{H} \cap \mathbb{G}(n;\theta)$. This fact is captured by the inclusion

$$C_n(\theta)^c \cap I(n;\theta) \subseteq \bigcup_{S \subseteq \mathcal{N}: |S| \geq 2} A_n(\theta;S). \tag{66}$$

A moment of reflection should convince the reader that this union need only be taken over all subsets S of $\{1,\ldots,n\}$ with $2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor$. A standard union bound argument immediately gives

$$\begin{aligned}\mathbb{P}\left[C_n(\theta)^c \cap I(n;\theta)\right] &\leq \sum_{S \subseteq \mathcal{N}: 2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} \mathbb{P}\left[A_n(\theta;S)\right] \\ &= \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{S \in \mathcal{N}_{n,r}} \mathbb{P}\left[A_n(\theta;S)\right] \right) \end{aligned} \tag{67}$$

where $\mathcal{N}_{n,r}$ denotes the collection of all subsets of $\{1,\ldots,n\}$ with exactly r elements.

For each $r = 1,\ldots,n$, we simplify the notation by writing $A_{n,r}(\theta) = A_n(\theta;\{1,\ldots,r\})$, $B_{n,r}(\theta) = B_n(\theta;\{1,\ldots,r\})$, and $C_{n,r}(\theta) = C_n(\theta;\{1,\ldots,r\})$. With a slight abuse of notation, we use $C_n(\theta)$ for $r = n$ as defined earlier. Under the enforced assumptions, exchangeability yields

$$\mathbb{P}\left[A_n(\theta;S)\right] = \mathbb{P}\left[A_{n,r}(\theta)\right], \quad S \in \mathcal{N}_{n,r}$$

and the expression

$$\sum_{S \in \mathcal{N}_{n,r}} \mathbb{P}\left[A_n(\theta;S)\right] = \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta)\right] \tag{68}$$

follows since $|\mathcal{N}_{n,r}| = \binom{n}{r}$. Substituting into (67), we obtain the key bound

$$\mathbb{P}\left[C_n(\theta)^c \cap I(n;\theta)\right] \leq \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta)\right]. \tag{69}$$

Consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ as in the statement of Proposition 11.1. Substitute θ by θ_n according to this scaling in the right-hand side of (69). The proof of Proposition 11.1 will be completed once we show

$$\lim_{n\to\infty} \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0. \tag{70}$$

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

XII. Bounding Probabilities

Fix $n = 2,3,\ldots$ and consider $\theta = (K,p)$ with p in $(0,1)$ and positive integer K such that $K < n$.

A. Bounding the Probabilities $\mathbb{P}\left[B_{n,r}(\theta)\right]$

The following two results will be used to efficiently bound the probability $\mathbb{P}\left[B_{n,r}(\theta)\right]$; proofs are available in Appendix B.

Lemma 12.1: For each $r = 2,\ldots,n-1$, the inequality

$$\mathbb{P}\left[B_{n,r}(\theta) \;\middle|\; \begin{array}{l} B_{ij}(p),\ 1 \leq i < j \leq r \\ \Gamma_{n,1}(K),\ldots,\Gamma_{n,n}(K) \end{array}\right] \leq (1-p)^{E^\star_{n,r}(K)} \tag{71}$$

holds with the rv $E^\star_{n,r}(K)$ given by

$$E^\star_{n,r}(K) = \sum_{i=1}^{r} \sum_{k=r+1}^{n} \mathbf{1}\left[i \in \Gamma_{n,k}(K)\right]. \tag{72}$$

The arguments leading to (71) can be modified to obtain the next bound.

Lemma 12.2: For each $r = 2,\ldots,n-1$, the inequality

$$\begin{aligned}&\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \leq i < j \leq r \\ \Gamma_{n,1}(K),\ldots,\Gamma_{n,r}(K) \end{array}\right] \\ &\quad \leq (1-p)^{E^{\star\star}_{n,r}(K)} \cdot u_n(\theta)^{r(n-r)-E^{\star\star}_{n,r}(K)} \end{aligned} \tag{73}$$

holds with $u_n(\theta)$ defined by (56) and the rv $E^{\star\star}_{n,r}(K)$ given by

$$E^{\star\star}_{n,r}(K) = \sum_{i=1}^{r} \sum_{k=r+1}^{n} \mathbf{1}\left[k \in \Gamma_{n,i}(K)\right]. \tag{74}$$

The tail of the rv $E^\star_{n,r}(K)$ is controlled through the following result.

Lemma 12.3: Fix $r = 2,\ldots,n-1$. For any t in $(0,1)$, we have

$$\mathbb{P}\left[E^\star_{n,r}(K) \leq (1-t) rK \cdot \frac{n-r}{n-1}\right] \leq e^{-\frac{t^2}{2} rK \cdot \frac{n-r}{n-1}}. \tag{75}$$

Proof: Consider a positive integer K such that $K < n$. From the facts reported in Section IX, the negative association of the rvs (52) implies that of the rvs $\{\mathbf{1}\left[i \in \Gamma_{n,k}(K)\right],\ i = 1,\ldots,r;\ k = r+1,\ldots,n\}$. We are now in a position to apply the Chernoff–Hoeffding bound to the sum (72) as given for negatively associated rvs [10, Th. 3.1, p. 35]. This bound takes the form

$$\mathbb{P}\left[E^\star_{n,r}(K) \leq (1-t)\mathbb{E}\left[E^\star_{n,r}(K)\right]\right] \leq e^{-\frac{t^2}{2} \cdot \mathbb{E}\left[E^\star_{n,r}(K)\right]}$$

and the conclusion (75) follows upon noting that

$$\mathbb{E}\left[E^\star_{n,r}(K)\right] = \sum_{i=1}^{r} \sum_{k=r+1}^{n} \mathbb{P}\left[i \in \Gamma_{n,k}(K)\right] = r(n-r)\frac{K}{n-1}$$

as we use (32). ■

B. Bounding the Probabilities $\mathbb{P}[C_{n,r}(\theta)]$

For each $r = 2, \ldots, n$, let $\mathbb{H}\cap\mathbb{G}_r(n;\theta)$ stand for the subgraph $\mathbb{H}\cap\mathbb{G}(n;\theta)(S)$ when $S = \{1, \ldots, r\}$. Also let $\mathcal{T}_r$ denote the collection of all spanning trees on the vertex set $\{1, \ldots, r\}$.

Lemma 12.4: Fix $r = 2, \ldots, n$. For each T in $\mathcal{T}_r$, we have

$$\mathbb{P}[T \subseteq \mathbb{H}\cap\mathbb{G}_r(n;\theta)] \le (p\lambda_n(K))^{r-1} \tag{76}$$

where the notation $T \subseteq \mathbb{H}\cap\mathbb{G}_r(n;\theta)$ indicates that the tree T is a subgraph spanning $\mathbb{H}\cap\mathbb{G}_r(n;\theta)$.

Since $p\lambda_n(K)$ is the probability of link assignment, the situation is reminiscent of the one found in ER graphs [5] and random key graphs [30], where in each of these cases the bound (76) holds with equality.

Proof: Fix $r = 2, 3, \ldots, n$ and pick a tree T in $\mathcal{T}_r$. Let $\mathcal{E}(T)$ be the set of edges that appear in T. It is plain that $T \subseteq \mathbb{H}\cap\mathbb{G}_r(n,;\theta)$ occurs if and only if the set of conditions

$$\begin{array}{c} \Sigma_{n,i}(K)\cap\Sigma_{n,j}(K) \neq \emptyset \\ \text{and} \\ B_{ij}(p) = 1 \end{array}, \quad \{i,j\} \in \mathcal{E}(T)$$

holds. Therefore, under the enforced independence assumptions, since $|\mathcal{E}(T)| = r-1$, we get

$$\begin{aligned} &\mathbb{P}[T \subset \mathbb{H}\cap\mathbb{G}_r(n;\theta)] \\ &= p^{r-1}\mathbb{E}\left[\prod_{\{i,j\}\in\mathcal{E}(T)} \mathbf{1}[\Sigma_{n,i}(K)\cap\Sigma_{n,j}(K)\neq\emptyset]\right] \\ &= p^{r-1}\mathbb{E}\left[\prod_{\{i,j\}\in\mathcal{E}(T)} \mathbf{1}[i\in\Gamma_{n,j}(K)\vee j\in\Gamma_{n,i}(K)]\right] \\ &\le p^{r-1}\prod_{\{i,j\}\in\mathcal{E}(T)} \mathbb{P}[i\in\Gamma_{n,j}(K)\vee j\in\Gamma_{n,i}(K)] \end{aligned}$$

by making use of (51) with the negatively associated rvs (48). The desired result (76) is now immediate from (5) and the relation $|\mathcal{E}(T)| = r-1$. ■

As for ER graphs [5] and random key graphs [30], we have the following bound.

Lemma 12.5: For each $r = 2, \ldots, n$, we have

$$\mathbb{P}[C_{n,r}(\theta)] \le r^{r-2}(p\lambda_n(K))^{r-1}. \tag{77}$$

Proof: Fix $r = 2, \ldots, n$. If $\mathbb{H}\cap\mathbb{G}_r(n;\theta)$ is a connected graph, then it must contain a spanning tree on the vertex set $\{1, \ldots . r\}$, and a union bound argument yields

$$\mathbb{P}[C_{n,r}(\theta)] \le \sum_{T\in\mathcal{T}_r} \mathbb{P}[T \subset \mathbb{H}\cap\mathbb{G}_r(n;\theta)].$$

By Cayley's formula [17], there are r^{r-2} labeled trees on r vertices, i.e., $|\mathcal{T}_r| = r^{r-2}$, and (77) follows upon making use of (76). ■

XIII. A Proof of Proposition 11.1 (Part II)

Consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ as in the statement of Proposition 11.1. Pick integers $R \ge 2$ and $n^\star(R) \ge 2(R+1)$ (to be specified in Section XV). On the range $n \ge n^\star(R)$, we consider the decomposition

$$\begin{aligned} &\sum_{r=2}^{\lfloor \frac{n}{2}\rfloor} \binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] \\ &\quad = \sum_{r=2}^{R}\binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] + \sum_{r=R+1}^{\lfloor \frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] \end{aligned}$$

and let n go to infinity. The desired convergence (70) will be established if we show

$$\lim_{n\to\infty}\binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] = 0 \tag{78}$$

for *each* $r = 2, 3, \ldots$ and

$$\lim_{n\to\infty}\sum_{r=R+1}^{\lfloor \frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] = 0. \tag{79}$$

We establish (78) and (79) in turn in Sections XIV and XV, respectively. Throughout, we shall make use of several bounds. The following bounds

$$\binom{n}{r} \le \left(\frac{en}{r}\right)^r, \quad \begin{array}{l} r = 1, \ldots, n \\ n = 2, 3, \ldots \end{array} \tag{80}$$

are standard.

Furthermore, fix $r = 2, 3, \ldots$ and consider $n = 2, 3, \ldots$ such that $r < n$. With (72) in mind, for each $i = 1, \ldots, r$, we note that

$$\begin{aligned} &\sum_{k=r+1}^{n}\mathbf{1}[k\in\Gamma_{n,i}(K)] \\ &\quad = \sum_{k=1}^{n}\mathbf{1}[k\in\Gamma_{n,i}(K)] - \sum_{k=1}^{r}\mathbf{1}[k\in\Gamma_{n,i}(K)] \\ &\quad = K - \sum_{k=1}^{r}\mathbf{1}[k\in\Gamma_{n,i}(K)] \end{aligned}$$

since $|\Gamma_{n,i}(K)| = K$. The bounds

$$(K-r)^+ \le \sum_{k=r+1}^{n}\mathbf{1}[k\in\Gamma_{n,i}(K)] \le K$$

follow, whence

$$r(K-r)^+ \le E^{\star\star}_{n,r}(K) \le rK. \tag{81}$$

It is also easy to see that

$$r(n-r) = E^{\star\star}_{n,r}(K) + \sum_{i=1}^{r}\sum_{k=r+1}^{n}\mathbf{1}[k\notin\Gamma_{n,i}(K)]$$

where for each $i = 1, \ldots, r$, we have

$$\begin{aligned} \sum_{k=r+1}^{n}\mathbf{1}[k\notin\Gamma_{n,i}(K)] &= n - r - \sum_{k=r+1}^{n}\mathbf{1}[k\in\Gamma_{n,i}(K)] \\ &\ge (n-r-K)^+ \end{aligned}$$

since $|\Gamma_{n,i}(K)| = K$, and the bounds

$$r(n-r-K)^+ \leq r(n-r) - E^{\star\star}_{n,r}(K) \tag{82}$$

follow.

XIV. Establishing (78)

Fix $r = 2, 3, \ldots$ and consider $n = 2, 3, \ldots$ such that $r < n$. Also let $\theta = (K, p)$ with p in $(0,1)$ and positive integer K such that $K < n$.

Using the lower bounds at (81) and (82) into (73), we get

$$\begin{aligned}\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \leq i < j \leq r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K)\end{array}\right] \\ \leq (1-p)^{r(K-r)} \cdot u_n(\theta)^{r(n-r-K)^+}\end{aligned} \tag{83}$$

since $0 < p, u_n(\theta) < 1$. The event $C_{n,r}(\theta)$ depends only on the rvs $\Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K)$ and $\{B_{ij}(p),\ 1 \leq i < j \leq r\}$. Write

$$F_{n,r}(\theta) = (1-p)^{(K-r)} \cdot u_n(\theta)^{(n-r-K)^+}$$

and use a straightforward conditioning argument to conclude that

$$\begin{aligned}&\mathbb{P}[A_{n,r}(\theta)] \\ &= \mathbb{E}\left[\mathbf{1}[C_{n,r}(\theta)]\, \mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \leq i < j \leq r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K)\end{array}\right]\right] \\ &\leq \mathbb{P}[C_{n,r}(\theta)] \cdot F_{n,r}(\theta)^r\end{aligned} \tag{84}$$

upon applying the bound (83). By Lemma 12.5, we get

$$\begin{aligned}\binom{n}{r}\mathbb{P}[A_{n,r}(\theta)] &\leq \left(\frac{en}{r}\right)^r \mathbb{P}[C_{n,r}(\theta)] \cdot F_{n,r}(\theta)^r \\ &\leq \frac{(en)^r}{r^2}\left(p\lambda_n(K)\right)^{r-1} F_{n,r}(\theta)^r\end{aligned} \tag{85}$$

as we make use of (80). With the help of (36), we also note from (56) that

$$F_{n,r}(\theta) \leq e^{F^\star_{n,r}(\theta)} \tag{86}$$

with

$$\begin{aligned}&F^\star_{n,r}(\theta) \\ &= (K-r)\log(1-p) - (n-r-K)\frac{pK}{n-1} \\ &= (K-r)\log(1-p) - \left(1 - \frac{K}{n-1} - \frac{r-1}{n-1}\right)pK \\ &= (K-r)\log(1-p) - p\left(K - \frac{K^2}{n-1}\right) + \frac{r-1}{n-1}pK \\ &= K\left(p + \log(1-p)\right) - r\log(1-p) \\ &\quad - p\left(2K - \frac{K^2}{n-1}\right) + \frac{r-1}{n-1}pK.\end{aligned} \tag{87}$$

Now, pick any given positive integer $r = 2, 3, \ldots$ and consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ such that $\lim_{n\to\infty} p_n = p^\star$ exists and (10) holds for some $c > \tau(p^\star)$. Replace θ by θ_n in (85) according to this scaling.

For n sufficiently large, upon using (12), (85), and (86), we get

$$\begin{aligned}&\binom{n}{r}\mathbb{P}[A_{n,r}(\theta_n)] \\ &\leq (en)^r \left(p_n\lambda_n(K_n)\right)^{r-1} F_{n,r}(\theta_n)^r \\ &= (en)^r \left(c_n \frac{\log n}{n-1}\right)^{r-1} \cdot F_{n,r}(\theta_n)^r \\ &= e^r \left(c_n \frac{\log n}{n-1}\right)^{r-1} \cdot \left(nF_{n,r}(\theta_n)\right)^r \\ &\leq e^r \left(c_n \frac{\log n}{n-1}\right)^{r-1} \cdot e^{r\left(\log n + F^\star_{n,r}(\theta_n)\right)}\end{aligned} \tag{88}$$

with the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfying $\lim_{n\to\infty} c_n = c$.

On the other hand, upon making repeated use of the bounds (39), we find from (87) that

$$\begin{aligned}F^\star_{n,r}(\theta_n) &\leq K_n\left(p_n + \log(1-p_n)\right) - r\log(1-p_n) \\ &\quad - p_n\left(2K_n - \frac{K_n^2}{n-1}\right) + \frac{r}{n}p_nK_n \\ &= K_n\left(p_n + \log(1-p_n)\right) - r\log(1-p_n) \\ &\quad - c_n\log n + \frac{r}{n}p_nK_n \\ &\leq K_n\left(p_n + \log(1-p_n)\right) - c_n\log n \\ &\quad - r\log(1-p_n) + \frac{r}{n}c_n\log n \\ &= p_nK_n\left(1 + \frac{\log(1-p_n)}{p_n}\right) - c_n\log n \\ &\quad - r\log(1-p_n) + \frac{r}{n}c_n\log n \\ &\leq \frac{c_n}{2}\log n \cdot \left(1 + \frac{\log(1-p_n)}{p_n}\right) - c_n\log n \\ &\quad - r\log(1-p_n) + \frac{r}{n}c_n\log n \\ &= -\frac{c_n}{2}\cdot\left(1 - \frac{\log(1-p_n)}{p_n}\right)\cdot\log n \\ &\quad - r\log(1-p_n) + \frac{r}{n}c_n\log n. \\ &= -\frac{1}{2}\left(c_n - \frac{2rp_n}{\log n}\right)\left(1 - \frac{\log(1-p_n)}{p_n}\right)\cdot\log n \\ &\quad - rp_n + \frac{r}{n}c_n\log n.\end{aligned}$$

Therefore, with an eye toward the last factor in (88), we obtain

$$\log n + F^\star_{n,r}(\theta_n) \leq \gamma_{n,r}\cdot\log n \tag{89}$$

with

$$\gamma_{n,r} = 1 - \frac{1}{2}\left(c_n - \frac{2rp_n}{\log n}\right)\left(1 - \frac{\log(1-p_n)}{p_n}\right) + \frac{r}{n}c_n.$$

To conclude, let n go to infinity in (88): The assumptions of Proposition 11.1 yield

$$\begin{aligned}\lim_{n\to\infty}\gamma_{n,r} &= 1 - \frac{c}{2}\cdot\left(1 - \frac{\log(1-p^\star)}{p^\star}\right) \\ &= 1 - \frac{c}{\tau(p^\star)} < 0\end{aligned} \tag{90}$$

since here we have assumed $c = \tau(p^\star)$, and the desired conclusion (78) follows from (88) as a consequence of (89) and (90). ■

XV. Establishing (79)

Fix $n = 2, 3, \ldots$ and consider $\theta = (K, p)$ with p in $(0,1)$, and positive integer K such that $K < n$. Pick $r = 1, 2, \ldots, n-1$. Recall that the event $C_{n,r}(\theta)$ depends only on $\Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K)$ and $\{B_{ij}(p),\ 1 \le i < j \le r\}$. A straightforward conditioning argument with respect to these rvs yields

$$\begin{aligned}
&\mathbb{P}\left[A_{n,r}(\theta)\right] \\
&= \mathbb{E}\left[\mathbf{1}\left[C_{n,r}(\theta)\right]\mathbb{P}\left[B_{n,r}(\theta) \,\middle|\, \begin{array}{c} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K) \end{array}\right]\right] \\
&\le \mathbb{E}\left[\mathbf{1}\left[C_{n,r}(\theta)\right](1-p)^{E^\star_{n,r}(\theta)}\right] \qquad (91)
\end{aligned}$$

as we use the bound (71). By the observation made earlier, the event $C_{n,r}(\theta)$ is independent of the rvs $\Gamma_{n,r+1}(K), \ldots, \Gamma_{n,n}(K)$, hence is independent of the rv $E^\star_{n,r}(\theta)$, and we conclude

$$\mathbb{P}\left[A_{n,r}(\theta)\right] \le \mathbb{P}\left[C_{n,r}(\theta)\right]\mathbb{E}\left[(1-p)^{E^\star_{n,r}(K)}\right]. \qquad (92)$$

Pick t arbitrary in $(0,1)$ and recall Lemma 12.3. A simple decomposition argument shows that

$$\begin{aligned}
&\mathbb{E}\left[(1-p)^{E^\star_{n,r}(K)}\right] \\
&\le \mathbb{E}\left[(1-p)^{E^\star_{n,r}(K)}\mathbf{1}\left[E^\star_{n,r}(K) > (1-t)rK \cdot \frac{n-r}{n-1}\right]\right] \\
&\quad + \mathbb{P}\left[E^\star_{n,r}(K) \le (1-t)rK \cdot \frac{n-r}{n-1}\right] \\
&\le (1-p)^{(1-t)rK\cdot\frac{n-r}{n-1}} + e^{-\frac{t^2}{2}rK\cdot\frac{n-r}{n-1}} \\
&\le e^{-(1-t)rpK\cdot\frac{n-r}{n-1}} + e^{-\frac{t^2}{2}rK\cdot\frac{n-r}{n-1}} \\
&\le e^{-(1-t)rpK\cdot\frac{n-r}{n-1}} + e^{-\frac{t^2}{2}rpK\cdot\frac{n-r}{n-1}} \\
&\le 2e^{-a(t)rpK\cdot\frac{n-r}{n-1}}
\end{aligned}$$

where

$$a(t) = \min\left(1-t, \frac{t^2}{2}\right).$$

Whenever $r = 2, 3, \ldots, \lfloor\frac{n}{2}\rfloor$, we have

$$\mathbb{E}\left[(1-p)^{E^\star_{n,r}(K)}\right] \le 2e^{-\frac{a(t)}{2}\cdot rpK} \qquad (93)$$

since on that range, we have

$$\frac{n-r}{n-1} \ge \frac{n/2}{n-1} \ge \frac{1}{2}.$$

Next, combine (92) with (77) and (93). By arguments similar to the ones leading to (85), we obtain

$$\begin{aligned}
&\binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta)\right] \\
&\le 2\binom{n}{r}r^{r-2}\left(p\lambda_n(K)\right)^{r-1}e^{-\frac{a(t)}{2}\cdot rpK} \\
&\le 2\frac{(en)^r}{r^2}\left(p\lambda_n(K)\right)^{r-1}e^{-\frac{a(t)}{2}\cdot rpK} \qquad (94)
\end{aligned}$$

with the help of (80).

Now, consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ such that $\lim_{n\to\infty} p_n = p^\star$ exists and (10) holds for some $c > \tau(p^\star)$. Replace θ by θ_n in (94) according to this scaling, and use (12). With integer $R \ge 2$ (to be further specified shortly) for $n \ge 2(R+1)$, we now get

$$\begin{aligned}
&\sum_{r=R+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta_n)\right] \\
&\le 2\sum_{r=R+1}^{\lfloor\frac{n}{2}\rfloor}\frac{(en)^r}{r^2}\left(c_n\frac{\log n}{n-1}\right)^{r-1}e^{-\frac{a(t)}{2}\cdot rp_nK_n} \\
&\le \frac{2(n-1)}{c_n\log n}\sum_{r=R+1}^{\lfloor\frac{n}{2}\rfloor}\left(c_n\frac{en}{n-1}\log n\cdot e^{-\frac{a(t)}{2}\cdot p_nK_n}\right)^r \\
&\le \frac{2(n-1)}{c_n\log n}\sum_{r=R+1}^{\lfloor\frac{n}{2}\rfloor}\rho_n(t)^r \qquad (95)
\end{aligned}$$

with

$$\rho_n(t) = c_n\frac{en}{n-1}\log n\cdot e^{-\frac{a(t)}{4}\cdot c_n\log n}$$

for each $n = 2, 3, \ldots$—The last step made use of the lower bound at (39). It is plain that $\lim_{n\to\infty}\rho_n(t) = 0$ since $\lim_{n\to\infty} c_n = c > 0$. Hence, there exists a positive integer $n^\star(R) > 2(R+1)$ such that $\rho_n(t) < 1$ for all $n \ge n^\star(R)$. Thus, on that range

$$\begin{aligned}
\sum_{r=R+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta_n)\right] &\le \frac{2(n-1)}{c_n\log n}\sum_{r=R+1}^{\infty}\rho_n(t)^r \\
&= \frac{2(n-1)}{c_n\log n}\cdot\frac{\rho_n(t)^{R+1}}{1-\rho_n(t)}
\end{aligned}$$

by standard results on convergent geometric series. Note that

$$\begin{aligned}
&\frac{2(n-1)}{c_n\log n}\cdot\rho_n(t)^{R+1} \\
&= \frac{2(n-1)}{c_n\log n}\cdot\left(c_n\frac{en}{n-1}\log n\right)^{R+1}\cdot e^{-(R+1)\frac{a(t)}{4}\cdot c_n\log n} \\
&= 2e\cdot\left(c_n\frac{en}{n-1}\log n\right)^R\cdot n^{1-(R+1)\frac{a(t)}{4}\cdot c_n}
\end{aligned}$$

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

Finally, let n go to infinity in the last inequality: If we select R such that

$$\lim_{n\to\infty}\left(1-(R+1)\frac{a(t)}{4}\cdot c_n\right) = 1-(R+1)\frac{a(t)}{4}\cdot c < 0$$

then

$$\lim_{n\to\infty}\frac{2(n-1)}{c_n\log n}\cdot\rho_n(t)^{R+1} = 0$$

and the desired conclusion (79) follows. For each t in $(0,1)$, since $a(t) > 0$, this choice of R is always feasible by taking R sufficiently large, specifically

$$\frac{4}{ca(t)} < R+1.$$

■

APPENDIX A
A PROOF OF PROPOSITION 10.1

The basis for deriving (59) lies in the observation that nodes 1 and 2 are both isolated in $\mathbb{H} \cap \mathbb{G}(n;\theta)$ if and only if each edge in $\mathbb{H}(n;K)$ incident to one of these nodes is *not* present in $\mathbb{G}(n;p)$. Thus, $\chi_{n,1}(\theta) = \chi_{n,2}(\theta) = 1$ if and only if both sets of conditions

$$B_{1j}(p) = 0 \quad \text{if} \quad \Sigma_{n,1}(K) \cap \Sigma_{n,j}(K) \neq \emptyset,\ j \in \mathcal{N}_{-1}$$

and

$$B_{2k}(p) = 0 \quad \text{if} \quad \Sigma_{n,2}(K) \cap \Sigma_{n,k}(K) \neq \emptyset,\ k \in \mathcal{N}_{-2}$$

hold.

To formalize this observation, we introduce the random sets $N_{n,1}(\theta)$ and $N_{n,2}(\theta)$ defined by

$$N_{n,1}(\theta) = \{j = 3, \ldots, n : j \in \Gamma_{n,1}(K) \vee 1 \in \Gamma_{n,j}(K)\}$$

and

$$N_{n,2}(\theta) = \{k = 3, \ldots, n : k \in \Gamma_{n,2}(K) \vee 2 \in \Gamma_{n,k}(K)\}.$$

Thus, node j in $N_{n,1}(\theta)$ is neither node 1 nor node 2, and is K-adjacent to node 1. Similarly, node k in $N_{n,2}(\theta)$ is neither node 1 nor node 2, and is K-adjacent to node 2. Let $Z_n(\theta)$ denote the total number of edges in $\mathbb{H}(n;K)$ that are incident to either node 1 or node 2. It is plain that

$$\begin{aligned} Z_n(\theta) &= |N_{n,1}(\theta)| + |N_{n,2}(\theta)| \\ &\quad + \mathbf{1}\left[2 \in \Gamma_{n,1}(K) \vee 1 \in \Gamma_{n,2}(K)\right] \end{aligned} \tag{96}$$

with the last term accounting for the possibility that nodes 1 and 2 are K-adjacent. By conditioning on the rvs $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$, we readily conclude from the earlier observation that

$$\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right] = \mathbb{E}\left[(1-p)^{Z_n(\theta)}\right] \tag{97}$$

under the enforced independence on the collections of rvs $\{\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)\}$ and $\{B_{ij}(p),\ 1 \leq i < j \leq n\}$.

To proceed, we need to assess the various contributions to $Z_n(\theta)$: Using (1), we find

$$\begin{aligned} |N_{n,1}(\theta)| &= \sum_{j=3}^{n} \mathbf{1}\left[j \in \Gamma_{n,1}(K) \vee 1 \in \Gamma_{n,j}(K)\right] \\ &= \sum_{j=3}^{n} \mathbf{1}\left[j \in \Gamma_{n,1}(K)\right] + \sum_{j=3}^{n} \mathbf{1}\left[1 \in \Gamma_{n,j}(K)\right] \\ &\quad - \sum_{j=3}^{n} \mathbf{1}\left[j \in \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,j}(K)\right] \\ &= \sum_{j=3}^{n} \mathbf{1}\left[j \in \Gamma_{n,1}(K)\right] \\ &\quad + \sum_{j=3}^{n} \mathbf{1}\left[j \notin \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,j}(K)\right] \\ &= K - \mathbf{1}\left[2 \in \Gamma_{n,1}(K)\right] \\ &\quad + \sum_{j=3}^{n} \mathbf{1}\left[j \notin \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,j}(K)\right] \end{aligned} \tag{98}$$

where the last step made use of fact $|\Gamma_{n,1}(K)| = K$. Similar arguments show that

$$\begin{aligned} |N_{n,2}(\theta)| &= \sum_{k=3}^{n} \mathbf{1}\left[k \in \Gamma_{n,2}(K) \vee 2 \in \Gamma_{n,k}(K)\right] \\ &= K - \mathbf{1}\left[1 \in \Gamma_{n,2}(K)\right] \\ &\quad + \sum_{k=3}^{n} \mathbf{1}\left[k \notin \Gamma_{n,2}(K),\ 2 \in \Gamma_{n,k}(K)\right]. \end{aligned}$$

By the definition of $Z_n(\theta)$, we now get

$$Z_n(\theta) = 2K - \mathbf{1}\left[2 \in \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,2}(K)\right] + Z_n^\star(\theta) \tag{99}$$

upon using (1) one more time, where

$$\begin{aligned} Z_n^\star(\theta) &= \sum_{j=3}^{n} \mathbf{1}\left[j \notin \Gamma_{n,1}(K),\ 1 \in \Gamma_{n,j}(K)\right] \\ &\quad + \sum_{j=3}^{n} \mathbf{1}\left[j \notin \Gamma_{n,2}(K),\ 2 \in \Gamma_{n,j}(K)\right]. \end{aligned}$$

In order to evaluate the expression (97), we first compute the conditional expectation

$$\mathbb{E}\left[(1-p)^{Z_n(\theta)} \,\middle|\, \Gamma_{n,1}(K),\ \Gamma_{n,2}(K)\right]. \tag{100}$$

From (99), this quantity can be evaluated as the product of the two terms

$$(1-p)^{2K - \left(\mathbf{1}\left[2 \in \Gamma_{n,1}(K), 1 \in \Gamma_{n,2}(K)\right]\right)} \tag{101}$$

and

$$\mathbb{E}\left[(1-p)^{Z_n^\star(\theta)} \,\middle|\, \Gamma_{n,1}(K),\ \Gamma_{n,2}(K)\right]. \tag{102}$$

To evaluate this last conditional expectation, for each $j = 3, \ldots, n$, we set

$$\begin{aligned} &V_{n,j}(\theta; S, T) \\ &\quad = \mathbb{E}\left[(1-p)^{\mathbf{1}[j \notin S,\ 1 \in \Gamma_{n,j}(K)] + \mathbf{1}[j \notin T,\ 2 \in \Gamma_{n,j}(K)]}\right] \end{aligned}$$

with S and T elements of $\mathcal{N}_{n,K}$. It is straightforward to check that

$$\begin{aligned} &V_{n,j}(\theta; S, T) \\ &\quad = \mathbf{1}\left[j \notin S\right] \mathbf{1}\left[j \notin T\right] \mathbb{E}\left[(1-p)^{\mathbf{1}[1 \in \Gamma_{n,j}(K)] + \mathbf{1}[2 \in \Gamma_{n,j}(K)]}\right] \\ &\qquad + \mathbf{1}\left[j \notin S\right] \mathbf{1}\left[j \in T\right] \mathbb{E}\left[(1-p)^{\mathbf{1}[1 \in \Gamma_{n,j}(K)]}\right] \\ &\qquad + \mathbf{1}\left[j \in S\right] \mathbf{1}\left[j \notin T\right] \mathbb{E}\left[(1-p)^{\mathbf{1}[2 \in \Gamma_{n,j}(K)]}\right] \\ &\qquad + \mathbf{1}\left[j \in S\right] \mathbf{1}\left[j \in T\right]. \end{aligned}$$

Then, with the notation introduced earlier in Section IX, we can write

$$\begin{aligned} &V_{n,j}(\theta; S, T) \\ &\quad = \mathbf{1}\left[j \notin S\right] \mathbf{1}\left[j \notin T\right] b_n(\theta) \\ &\qquad + \left(\mathbf{1}\left[j \notin S\right] \mathbf{1}\left[j \in T\right] + \mathbf{1}\left[j \in S\right] \mathbf{1}\left[j \notin T\right]\right) u_n(\theta) \\ &\qquad + \mathbf{1}\left[j \in S\right] \mathbf{1}\left[j \in T\right]. \end{aligned}$$

Next, the two rvs $\Gamma_{n,1}(K)$ and $\Gamma_{n,2}(K)$ being jointly independent of the rvs $\Gamma_{n,3}(K), \ldots, \Gamma_{n,n}(K)$, we find

$$\begin{aligned} &\mathbb{E}\left[(1-p)^{Z_n^\star(\theta)} \middle| \Gamma_{n,1}(K),\ \Gamma_{n,2}(K)\right] \\ &= \prod_{j=3}^{n} V_{n,j}(\theta; \Gamma_{n,1}(K), \Gamma_{n,2}(K)) \\ &= b_n(\theta)^{B_n(\theta)} \cdot u_n(\theta)^{U_n(\theta)} \end{aligned} \tag{103}$$

where the rvs $B_n(\theta)$ and $U_n(\theta)$ are given by (57) and (58), respectively. Therefore, since

$$\mathbb{E}\left[(1-p)^{Z_n(\theta)}\right] = \mathbb{E}\left[\mathbb{E}\left[(1-p)^{Z_n(\theta)} \middle| \Gamma_{n,1}(K), \Gamma_{n,2}(K)\right]\right]$$

by a standard preconditioning argument, the expression (59) is obtained upon writing (100) as the product of the quantities (101) and (102), and using (103). ■

Appendix B
Proofs of Lemmas 12.1 and 12.2

The defining conditions for $B_{n,r}(\theta)$ lead to the representation

$$B_{n,r}(\theta) = \cap_{i=1}^{r} \cap_{k=r+1}^{n} E_{n,ik}(\theta)$$

where we have set

$$\begin{aligned} &E_{n,ik}(\theta) \\ &= ([k \notin \Gamma_{n,i}(K)] \cap [i \notin \Gamma_{n,k}(K)]) \cup [B_{ik}(p) = 0] \end{aligned}$$

with $i = 1, \ldots, r$ and $k = r+1, \ldots, n$. In terms of indicator functions, with the help of (1), this definition reads

$$\begin{aligned} &\mathbf{1}\left[E_{n,ik}(\theta)\right] \\ &= \mathbf{1}\left[k \notin \Gamma_{n,i}(K)\right] \mathbf{1}\left[i \notin \Gamma_{n,k}(K)\right] + (1 - B_{ik}(p)) \\ &\quad - \mathbf{1}\left[k \notin \Gamma_{n,i}(K)\right] \mathbf{1}\left[i \notin \Gamma_{n,k}(K)\right](1 - B_{ik}(p)) \\ &= (1 - B_{ik}(p)) + \mathbf{1}\left[k \notin \Gamma_{n,i}(K)\right] \mathbf{1}\left[i \notin \Gamma_{n,k}(K)\right] B_{ik}(p). \end{aligned}$$

The three collection of rvs $\{B_{ij}(p),\ 1 \le i < j \le r\}$, $\{B_{ik}(p),\ i = 1, \ldots, r,\ k = r+1, \ldots, n\}$, and $\{\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)\}$ are mutually independent. It is then elementary to see that

$$\begin{aligned} &\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K) \end{array}\right] \\ &= \mathbb{E}\left[\prod_{i=1}^{r} \prod_{k=r+1}^{n} \mathbf{1}\left[E_{n,ik}(\theta)\right] \middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K) \end{array}\right] \\ &= \prod_{i=1}^{r} \prod_{k=r+1}^{n} W\left(\mathbf{1}\left[k \notin \Gamma_{n,i}(K)\right] \mathbf{1}\left[i \notin \Gamma_{n,k}(K)\right]; p\right) \end{aligned}$$

under the enforced independence assumptions, where

$$W(x;p) = 1 - p + px, \quad x \in \mathbb{R}.$$

Since $W(x,p) = (1-p)^{1-x}$ for $x = 0, 1$, we obtain

$$\begin{aligned} &\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K) \end{array}\right] \\ &= \prod_{i=1}^{r} \prod_{k=r+1}^{n} (1-p)^{1 - \mathbf{1}[k \notin \Gamma_{n,i}(K)] \mathbf{1}[i \notin \Gamma_{n,k}(K)]}. \end{aligned} \tag{104}$$

A. A Proof of Lemma 12.1

It is plain from (104) that

$$\begin{aligned} &\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K) \end{array}\right] \\ &\le \prod_{i=1}^{r} \prod_{k=r+1}^{n} (1-p)^{1 - \mathbf{1}[i \notin \Gamma_{n,k}(K)]} \end{aligned}$$

and (71) immediately follows upon noting that

$$\begin{aligned} &\sum_{i=1}^{r} \sum_{k=r+1}^{n} (1 - \mathbf{1}\left[i \notin \Gamma_{n,k}(K)\right]) \\ &= \sum_{i=1}^{r} \sum_{k=r+1}^{n} \mathbf{1}\left[i \in \Gamma_{n,k}(K)\right] = E_{n,r}^\star(\theta). \end{aligned}$$

■

B. A Proof of Lemma 12.2

We start at (104). Conditioning on the rvs $\{B_{ij}(p),\ 1 \le i < j \le r\}$ and $\Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K)$ (rather than $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$), we find that

$$\begin{aligned} &\mathbb{P}\left[B_{n,r}(\theta) \middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K) \end{array}\right] \\ &= (1-p)^{r(n-r)} G_{n,r}(\Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K); \theta) \end{aligned} \tag{105}$$

where we have set

$$\begin{aligned} &G_{n,r}(S_1, \ldots, S_r; \theta) \\ &= \mathbb{E}\left[\prod_{i=1}^{r} \prod_{k=r+1}^{n} (1-p)^{-\mathbf{1}[k \notin S_i] \mathbf{1}[i \notin \Gamma_{n,k}(K)]}\right] \end{aligned}$$

with subsets $S_1, \ldots, S_r$ of $\mathcal{N}$, each of size K.

Next, we find

$$\begin{aligned} &G_{n,r}(S_1, \ldots, S_r; \theta) \\ &= \mathbb{E}\left[\prod_{k=r+1}^{n} \prod_{i=1}^{r} (1-p)^{-\mathbf{1}[k \notin S_i] \mathbf{1}[i \notin \Gamma_{n,k}(K)]}\right] \\ &= \mathbb{E}\left[\prod_{k=r+1}^{n} (1-p)^{-\sum_{i=1}^{r} \mathbf{1}[k \notin S_i] \mathbf{1}[i \notin \Gamma_{n,k}(K)]}\right] \\ &= \prod_{k=r+1}^{n} \mathbb{E}\left[(1-p)^{-\sum_{i=1}^{r} \mathbf{1}[k \notin S_i] \mathbf{1}[i \notin \Gamma_{n,k}(K)]}\right] \end{aligned}$$

under the enforced independence assumptions. Fix $k = r+1, \ldots, n$ and note that

$$\begin{aligned}
&\mathbb{E}\left[(1-p)^{-\sum_{i=1}^{r}\mathbf{1}[k\notin S_i]\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right] \\
&= \mathbb{E}\left[\prod_{i=1}^{r}\left((1-p)^{-\mathbf{1}[k\notin S_i]}\right)^{\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right] \\
&\le \prod_{i=1}^{r}\mathbb{E}\left[\left((1-p)^{-\mathbf{1}[k\notin S_i]}\right)^{\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right] \qquad (106) \\
&= \prod_{i=1}^{r}\mathbb{E}\left[(1-p)^{-\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right]^{\mathbf{1}[k\notin S_i]}
\end{aligned}$$

where (106) follows from the negative association of the rvs (53)—Use (50) and note that

$$(1-p)^{-\mathbf{1}[k\notin S_i]} \ge 1, \quad i = 1, \ldots, r.$$

Next, for each $i = 1, \ldots, r$, we have

$$\begin{aligned}
&\mathbb{E}\left[(1-p)^{-\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right] \\
&= (1-p)^{-1}\,\mathbb{P}\left[i \notin \Gamma_{n,k}(K)\right] + \mathbb{P}\left[i \in \Gamma_{n,k}(K)\right] \\
&= (1-p)^{-1}\left(1 - \frac{K}{n-1}\right) + \frac{K}{n-1} \\
&= \frac{u_n(\theta)}{1-p}
\end{aligned}$$

whence

$$\prod_{i=1}^{r}\mathbb{E}\left[(1-p)^{-\mathbf{1}[i\notin\Gamma_{n,k}(K)]}\right]^{\mathbf{1}[k\notin S_i]} = \left(\frac{u_n(\theta)}{1-p}\right)^{\sum_{i=1}^{r}\mathbf{1}[k\notin S_i]}.$$

Combining these observations readily leads to

$$\begin{aligned}
&G_{n,r}(S_1, \ldots, S_r; \theta) \\
&\le \prod_{k=r+1}^{n}\left(\frac{u_n(\theta)}{1-p}\right)^{\sum_{i=1}^{r}\mathbf{1}[k\notin S_i])]} \\
&= \left(\frac{u_n(\theta)}{1-p}\right)^{\sum_{i=1}^{r}\sum_{k=r+1}^{n}\mathbf{1}[k\notin S_i]}.
\end{aligned}$$

From (105), we finally obtain

$$\begin{aligned}
&\mathbb{P}\left[B_{n,r}(\theta)\middle| \begin{array}{l} B_{ij}(p),\ 1 \le i < j \le r \\ \Gamma_{n,1}(K), \ldots, \Gamma_{n,r}(K) \end{array}\right] \\
&\le (1-p)^{r(n-r)}\left(\frac{u_n(\theta)}{1-p}\right)^{\sum_{i=1}^{r}\sum_{k=r+1}^{n}\mathbf{1}[k\notin\Gamma_{n,i}(K)]}
\end{aligned}$$

and the desired conclusion (73) follows. ∎

References

[1] I. F. Akyildiz, Y. Sankarasubramaniam, W. Su, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, pp. 393–422, 2002.

[2] N. P. Anthapadmanabhan and A. M. Makowski, "On the absence of isolated nodes in wireless ad-hoc networks with unreliable links—A curious gap," in *Proc. IEEE Infocom*, San Diego, CA, Mar. 2010, pp. 1–9.

[3] S. R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discr. Math.*, vol. 309, pp. 5130–5140, 2009.

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

[5] B. Bollobás, *Random Graphs*, ser. Cambridge Studies in Advanced Mathematics, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[6] S. A. Çamtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: A survey." Dept. Comput. Sci., Rensselaer Polytechnic Inst., Troy, NY, 2005, Tech. Rep. TR-05-07.

[7] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Res. Security Privacy*, Oakland, CA, May 2003, pp. 197–213.

[8] R. D. Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Inf. Syst. Security*, vol. TISSEC 11, pp. 1–22, 2008.

[9] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Security*, Washington, DC, Oct. 2003, pp. 42–51.

[10] D. Dubhashi and A. Panconesi, *Concentration of Measure for the Analysis of Randomized Algorithms*. New York: Cambridge Univ. Press, 2009.

[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Security (CSS 2002)*, Washington, DC, Nov. 2002, pp. 41–47.

[12] T. I. Fenner and A. M. Frieze, "On the connectivity of random m-orientable graphs and digraphs," *Combinatorica*, vol. 2, pp. 347–359, 1982.

[13] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Analysis, Control, Optimization and Applications: A Volume in Honor of W. H. Fleming*, W. M. McEneany, G. Yin, and Q. Zhang, Eds. Cambridge, MA: Birkhäuser, 1998.

[14] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in *Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw.*, Washington, DC, Oct. 2004, pp. 43–52.

[15] S. Janson, T. Łuczak, and A. Ruciński, *Random graphs*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization. New York: Wiley, 2000.

[16] K. Joag-Dev and F. Proschan, "Negative association of random variables, with applications," *Ann. Statist.*, vol. 11, pp. 266–295, 1983.

[17] G. E. Martin, *Counting: The Art of Enumerative Combinatorics*. New York: Springer-Verlag, 2001.

[18] K. Rybarczyk, "Diameter, connectivity and phase transition of the uniform random intersection graph," *Discr. Math.*, vol. 311, pp. 1998–2019, 2011.

[19] M. D. Penrose, *Random Geometric Graphs, Oxford Studies in Probability*. New York: Oxford Univ. Press, 2003, vol. 5.

[20] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, pp. 53–57, 2004.

[21] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica*, vol. 12, pp. 900–906, 2006.

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

[23] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, pp. 2314–2341, 2007.

[24] O. Yağan, "Performance of the Eschenauer–Gligor key distribution scheme under an ON/OFF channel," *IEEE Trans. Inf. Theory*, vol. IT-58, no. 6, pp. 3821–3835, Jun. 2012.

[25] O. Yağan, "Random graph modeling of key distribution schemes in wireless sensor networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., University of Maryland, College Park, MD, 2011.

[26] O. Yağan and A. M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Jun. 2008, pp. 544–548.

[27] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 2403–2407.

[28] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key distribution schemes," in *Proc. 9th Int. Symp. Model. Optim. Mobile, Ad Hoc, Wireless Netw.*, Princeton, NJ, May 2011, pp. 257–264.

[29] O. Yağan and A. M. Makowski, "Designing securely connected wireless sensor networks in the presence of unreliable links," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[30] O. Yağan and A. M. Makowski, "Zero-one laws for connectivity in random key graphs," *IEEE Trans. Inf. Theory*, vol. IT-58, no. 5, pp. 2983–2999, May 2012.

[31] O. Yağan and A. M. Makowski, "Connectivity results for sensor networks under a random pairwise key predistribution scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Boston, MA, Jul. 2012, pp. 1797–1801.

[32] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key distribution scheme: Gradual deployment and key ring sizes," *Perform. Eval.*, 2013, to be published.

[33] O. Yağan and A. M. Makowski, "On the connectivity of sensor networks under random pairwise key predistribution," *IEEE Trans. Inf. Theory*, Feb. 2012, to be published.

[34] C.-W. Yi, P.-J. Wan, K.-W. Lin, and C.-H. Huang, "Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with unreliable nodes and links," in *Proc. IEEE Global Telecommun. Conf.*, San Francisco, CA, Nov. 2006, pp. 1–5.

Osman Yağan (S'07–M'12) received the B.S. degree in Electrical and Electronics Engineering from the Middle East Technical University, Ankara (Turkey) in 2007, and the Ph.D. degree in Electrical and Computer Engineering from the University of Maryland at College Park in 2011.

He was a visiting Postdoctoral Scholar at Arizona State University during Fall 2011. Since December 2011, he has been a Postdoctoral Research Fellow in CyLab at Carnegie Mellon University. His research interests include wireless communications, security, dynamical processes in complex networks, percolation theory, random graphs and their applications.

Armand M. Makowski (M'83–SM'94–F'06) received the Licence en Sciences Mathématiques from the Université Libre de Bruxelles in 1975, the M.S. degree in Engineering-Systems Science from U.C.L.A. in 1976 and the Ph.D. degree in Applied Mathematics from the University of Kentucky in 1981. In August 1981, he joined the faculty of the Electrical Engineering Department at the University of Maryland College Park, where he is Professor of Electrical and Computer Engineering. He has held a joint appointment with the Institute for Systems Research since its establishment in 1985.

Dr. Makowski was a C.R.B. Fellow of the Belgian-American Educational Foundation (BAEF) for the academic year 1975–76; he is also a 1984 recipient of the NSF Presidential Young Investigator Award and became an IEEE Fellow in 2006.

His research interests lie in applying advanced methods from the theory of stochastic processes to the modeling, design and performance evaluation of engineering systems, with particular emphasis on communication systems and networks.