Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel

Osman Yağan

Abstract—**We investigate the secure connectivity of wireless sensor networks under the random key distribution scheme of Eschenauer and Gligor. Unlike recent work which was carried out under the assumption of *full visibility*, here we assume a (simplified) communication model where unreliable wireless links are represented as on/off channels. We present conditions on how to scale the model parameters so that the network i) has no secure node which is isolated and ii) is securely connected, both with high probability when the number of sensor nodes becomes large. The results are given in the form of full *zero-one laws*, and constitute the first *complete* analysis of the EG scheme under *non*-full visibility. Through simulations these zero-one laws are shown to be valid also under a more realistic communication model, i.e., the disk model. The relations to the Gupta and Kumar's conjecture on the connectivity of geometric random graphs with randomly deleted edges are also discussed.**

Keywords: Wireless sensor networks, Security, Key predistribution, Random graphs, Connectivity.

I. Introduction

A. Wireless sensor networks and security

Wireless sensor networks (WSNs) are distributed collections of sensors that are envisioned [1] to be used in a wide range of application areas including 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 computationally feasible because of the severe limitations imposed on the physical memory and power consumption of the individual sensors. Traditional key exchange and distribution protocols are also not useful as they are based on trusting third parties while the topologies of large-scale WSNs are unknown prior to deployment. We refer the reader to the papers [6], [11], [19], [21] for more detailed discussions on the security challenges in WSN settings.

Random key predistribution schemes were recently 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]. According to their scheme, here after referred to as the EG scheme, each sensor is independently assigned K distinct cryptographic keys which are selected uniformly at random from a pool of P keys. These K keys constitute the key ring of the node and are inserted into its memory before the network deployment. Two sensor nodes can then establish a secure link between them if they are within transmission range of each other and if their key rings have at least one key in common; see [11] for implementation details.

Since then, many competing alternatives to the EG scheme have been proposed; see [6] for a detailed survey of various key distribution schemes for WSNs. With a number of schemes available, a basic question arises as to how they compare with each other. Answering this question requires a good understanding of the properties and performance of the schemes under consideration, and there are a number of ways to achieve this. 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 which 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. Here, we focus on the connectivity properties since secure connectivity is one of the basic properties required for a successful operation of the WSN.

B. Relevant work

To date, much efforts along the above lines have been carried out under the assumption of *full visibility* according to which sensor nodes are all within communication range of each other. Under this assumption, the EG scheme gives rise to a class of random graphs known as random key graphs; relevant results are available in the references [3], [9], [11], [20], [22]. The q-composite scheme [7], a simple variation of the EG scheme, was investigated by Bloznelis et al. [4] through

Manuscript received November 7, 2011. This work was supported in part by NSF Grant CCF-07290.

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).

an appropriate extension of the random key graph model. Recently, Yağan and Makowski have analyzed various random graphs induced by the random pairwise key predistribution scheme of Chan et al. [7]; see [23].

To be sure, the full visibility assumption does away with the wireless nature of the communication medium supporting WSNs. In fact, a common criticism of the above 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 impaired. As a result, the desired connectivity properties may not be achieved if dimensioning is done according to results derived under full visibility.

With this in mind, there has been a number of efforts to incorporate a wireless communication model to the existing full visibility models of the key distribution schemes. Among them, the most popular one is the so called disk model [13], [2]: Assuming that the sensors are distributed over a bounded region $\mathcal{D}$ of a euclidian plane, two nodes are assumed to have a direct communication link in between as long as they are within transmission range of each other. In other words, with $\rho > 0$ denoting the transmission range, nodes i and j located at $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$ are able to communicate if

$$\parallel \boldsymbol{x_i} - \boldsymbol{x_j} \parallel < \rho. \tag{1}$$

When the node locations are independently and uniformly distributed over the region $\mathcal{D}$, the graph induced under the condition (1) is known as a random geometric graph [13], [18] for which the most well-known result is the following zero-one law for connectivity: If $\mathcal{D}$ is a disk of unit area [13] (or a unit square [17]), ρ is scaled with the number of nodes n, and it holds that

$$\pi \rho_n^2 = \frac{\log n + w_n}{n},$$

then the probability that the resulting geometric random graph is connected tends to 1 (resp. 0) as n gets large if $\lim_{n\to\infty} w_n = \infty$ (resp. $\lim_{n\to\infty} w_n = -\infty$). It was also conjectured by Gupta and Kumar [13] that if each edge of the geometric random graph was to be deleted with probability $1 - \alpha$ independently from all the other edges, then the zero-one law for connectivity would take the following form: If α and ρ are scaled with n and it holds that

$$\pi \rho_n^2 \alpha_n = \frac{\log n + w_n}{n}, \tag{2}$$

then the resulting random graph, which is an *intersection* of the random geometric graph and the Erdős-Rényi graph [5]), is connected with probability tending to 1 (resp. 0) if $\lim_{n\to\infty} w_n = \infty$ (resp. $\lim_{n\to\infty} w_n = -\infty$).

Inspired by these, the studies on the secure connectivity of WSNs have focused [15], [25] on establishing an appropriate analog of the conjecture (2). After all, incorporating the disk model to the EG scheme corresponds to studying a random graph formed by *intersecting* the geometric random graph with the random key graph. As a result, one can conjecture that, with β denoting the probability that two nodes have at least one common key in the EG scheme, and

$$\pi \rho_n^2 \beta_n = \frac{\log n + w_n}{n}, \tag{3}$$

we have connectivity with probability tending to 1 (resp. 0) as n gets large if $\lim_{n\to\infty} w_n = \infty$ (resp. $\lim_{n\to\infty} w_n = -\infty$).

To date, both of the conjectures (2) and (3) remain to be open. In fact, despite several attempts, even the weaker forms of the conjectures have not been established yet. Namely, the conjectures (2) and (3) imply that with

$$\pi \rho_n^2 \alpha_n = c \frac{\log n}{n} \tag{4}$$

$$\pi \rho_n^2 \beta_n = c \frac{\log n}{n}, \tag{5}$$

respectively, the resulting graphs are connected with probability tending to 1 (resp. 0) if $c > 1$ (resp. $c < 1$).

For instance, Di Pietro et al. [8] have shown that under the scaling (5), the one law $\lim_{n\to\infty} \mathbb{P}\left[\text{Corresponding random graph is connected}\right] = 1$ follows if $\rho_n > 0$ and $c > 20\pi$. Very recently, Krzywdziński and Rybarczyk [15] have improved this results and established the one-law under (5) for $c > 8$ without any constraint on ρ_n. In [15], the authors have also established the one-law under (4) for $c > 8$ marking the first connectivity result for the random geometric graph with random edge deletion. Another notable work is due by Yi et al. [25], where the authors have established the strong forms (2) and (3) of the conjectures but *only* for the property of absence of isolated nodes; there, it was also assumed that $\lim_{n\to\infty} \alpha_n \log n = \infty$ and $\lim_{n\to\infty} \beta_n \log n = \infty$. Clearly, absence of isolated nodes is a necessary condition for connectivity but it is not a sufficient one. Hence, for the connectivity property, the results in [25] imply only the zero-laws under the scalings (2) and (3) (and hence under (4) and (5)), leaving the conjectured one-laws under the scalings (2) and (3) open. The weaker forms of the conjectured zero-one laws are also open as there exists no results for the connectivity of the resulting graphs when $1 < c \leq 8$ under the scalings (4) and (5).

C. Contributions

In this paper, we do not attempt to establish either one of the conjectures (4) and (5). Yet, we still would like to establish a precise characterization of the connectivity properties of the EG scheme without the full visibility assumption. With this aim, we study the connectivity properties of the EG scheme under a simple communication model where channels are mutually independent, and are either on or off. This amounts to an overall system model constructed by *intersecting* the random key graph with an Erdős-Rényi (ER) graph [5]. For this random graph structure, we establish zero-one laws for two basic (and related) graph properties, namely graph connectivity and the absence of isolated nodes, as the model parameters are scaled with the number of users – We identify the critical thresholds and show that they coincide. Namely, with the notation introduced so far, we show that if α and β

are scaled with the number of nodes n and it holds that

$$\alpha_n \beta_n = c \frac{\log n}{n} \tag{6}$$

then, the resulting random graph is connected (and has no isolated nodes) with probability approaching to 1 (resp. 0) if $c > 1$ (resp. $c < 1$); see Section III for precise statements of the results. To the best of our knowledge, these *full* zero-one laws constitute the first *complete* analysis of the EG scheme under *non*-full visibility.

Although the communication model considered here may be deemed simplistic, it does permit a complete analysis of the issues of interest with the results providing a *precise* guideline for ensuring the secure connectivity of a WSN. Obtaining such precise guidelines by means of determining the exact threshold of secure connectivity is particularly crucial in a WSN setting due to a number of reasons: First, to increase the chances of connectivity, it is often required to increase the number of keys kept in each sensor's memory. However, since sensor nodes are expected to have very limited memory, it is desirable for practical key distribution schemes to have low memory requirements [10]. Second, in the EG scheme, there is a well known [9] trade-off between security and connectivity meaning that the more connected is the network the less secure it is. These point out the importance of the full zero-one laws established here in dimensioning the EG scheme as compared to the existing results [8], [15], where there is a significant gap between the conditions of the zero-law ($c < 1$) and the one-law ($c > 8$).

Finally, simulations suggest that the connectivity behavior of the EG scheme under the on/off channel model is asymptotically equivalent to that of the EG scheme under the disk model. This suggests that the zero-one laws obtained here can be taken as an indication of the validity of the conjectured zero-one law under the scaling (5).

D. Notation and convention

A word on notation and conventions in use: All limiting statements, including asymptotic equivalences, are understood with the number of sensor nodes n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. Also, we use the notation $=_{st}$ to indicate distributional equality. The indicator function of an event E is denoted by $\mathbf{1}[E]$. We say that an event holds *with high probability* (whp) if it holds with probability 1 as $n \to \infty$. For any discrete set S we write $|S|$ for its cardinality.

E. Structure of the paper

The rest of the paper is organized as follows: In Section II, we give precise definitions and implementation details of the EG scheme along with a description of the model of interest. The main results of the paper, namely Theorem 3.1 and Theorem 3.2, are presented in Section III with an extensive simulation results given in Section IV. The remaining sections, namely Sections V through XIV, are devoted to establishing the main results of the paper.

II. The model

Under full visibility, the random key distribution scheme of Eschenauer and Gligor gives rise to a class of random graphs usually known as random key graphs [22]; some authors [3], [20] refer to them as uniform random intersection graphs. Random key graphs are parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring with $K \leq P$. To lighten the notation we often group the integers P and K into the ordered pair $\theta \equiv (K, P)$.

For each node $i = 1, \ldots, n$, let $K_i(\theta)$ denote the random set of K distinct keys assigned to node i. We can think of $K_i(\theta)$ as an $\mathcal{P}_K$-valued rv where $\mathcal{P}_K$ denotes the collection of all subsets of $\{1, \ldots, P\}$ which contain exactly K elements – Obviously, we have $|\mathcal{P}_K| = \binom{P}{K}$. The rvs $K_1(\theta), \ldots, K_n(\theta)$ are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed over $\mathcal{P}_K$ with

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

for all $i = 1, \ldots, n$. This corresponds to selecting keys randomly and *without* replacement from the key pool.

Distinct nodes $i, j = 1, \ldots, n$ are said to be K-adjacent, written $i \sim_K j$, if they share at least one key in their key rings, namely

$$i \sim_K j \quad \text{iff} \quad K_i(\theta) \cap K_j(\theta) \neq \emptyset. \tag{7}$$

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

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

with

$$q(\theta) = \begin{cases} 0 & \text{if } P < 2K \\ & \\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } 2K \leq P, \end{cases} \tag{8}$$

whence the probability of edge occurrence between any two nodes is equal to $1 - q(\theta)$. The expression (8) and others given later are simple consequences of the often used fact that

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

for every subset S of $\{1, \ldots, P\}$ with $|S| \leq P - K$.

With $n = 2, 3, \ldots$ and positive integers $K < P$, the adjacency notion (7) defines the *random key graph* $\mathbb{K}(n; \theta)$ on the vertex set $\{1, \ldots, n\}$.

As mentioned earlier, in this paper we seek to account for the possibility that communication links between nodes may not be available.[1] To study such situations, we assume a communication model that consists of independent channels each of which can be either on or off. Thus, with α in $(0, 1)$, let $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$ denote i.i.d. $\{0, 1\}$-valued rvs with success probability α. The channel between nodes i and j is available (resp. up) with probability α and unavailable (resp. down) with the complementary probability $1 - \alpha$.

[1] In this work, we only consider link failures and do not account for the possibility that some of the sensor nodes may fail over time due to battery drainage. The interested reader is referred to the references [12], [25] for connectivity results in wireless ad-hoc networks under random node failures.

Distinct nodes i and j are said to be B-adjacent, written $i \sim_B j$, if $B_{ij}(\alpha) = 1$. The notion of B-adjacency defines the standard Erdős-Rényi graph $\mathbb{G}(n;\alpha)$ on the vertex set $\{1,\ldots,n\}$. Obviously,

$$\mathbb{P}\left[i \sim j\right]_B = \alpha.$$

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

$$i \sim j \quad \text{iff} \quad \begin{array}{c} K_i(\theta) \cap K_j(\theta) \neq \emptyset \\ \text{and} \\ B_{ij}(\alpha) = 1. \end{array}$$

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

Throughout the collections of rvs $\{K_1(\theta),\ldots,K_n(\theta)\}$ and $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$ are assumed to be independent, in which case the edge occurrence probability in $\mathbb{K} \cap \mathbb{G}(n;\theta,\alpha)$ is given by

$$\mathbb{P}\left[i \sim j\right] = \alpha \cdot \mathbb{P}\left[i \sim_K j\right] = \alpha(1 - q(\theta)).$$

III. Main results

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

$$K_n \leq P_n, \quad n = 1, 2, \ldots. \tag{9}$$

Similarly, any mapping $\alpha : \mathbb{N}_0 \to (0,1)$ defines a scaling for ER graphs. Finally, a scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ is said to be *admissible* if

$$2 \leq K_n \tag{10}$$

for *all* $n = 1, 2, \ldots$ *sufficiently* large.

To lighten the notation we often group the parameters K, P and α into the ordered triple $\Theta \equiv (K, P, \alpha) = (\theta, \alpha)$. Hence, a mapping $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ defines a scaling for the intersection graph $\mathbb{K} \cap \mathbb{G}(n;\Theta)$ provided the condition (9) holds.

A. Absence of isolated nodes

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

Theorem 3.1: Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ *and a scaling* $\alpha : \mathbb{N}_0 \to (0,1)$ *such that*

$$\alpha_n(1 - q(\theta_n)) \sim c\frac{\log n}{n}, \quad n = 1, 2, \ldots \tag{11}$$

for some $c > 0$*. If* $\lim_{n\to\infty} \alpha_n \log n = \alpha^\star$ *exists, then we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c} \mathbb{K} \cap \mathbb{G}(n;\Theta_n) \textit{ contains} \\ \textit{no isolated nodes} \end{array}\right] = \begin{cases} 0 & \textit{if } c < 1 \\ \\ 1 & \textit{if } c > 1. \end{cases} \tag{12}$$

The condition (11) on the scalings will often be used in the equivalent form

$$\alpha_n(1 - q(\theta_n)) = c_n\frac{\log n}{n}, \quad n = 1, 2, \ldots$$

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

The assumption that $\lim_{n\to\infty} \alpha_n \log n = \alpha^\star$ exists is made due to technical reasons and it is much weaker than the condition $\lim_{n\to\infty} \alpha_n \log n = \infty$ assumed in [25].

B. Connectivity

An analog of Theorem 3.1 also holds for the property of graph connectivity.

Theorem 3.2: Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ *and a scaling* $\alpha : \mathbb{N}_0 \to (0,1)$ *such that (11) holds for some* $c > 0$*. If* $\lim_{n\to\infty} \alpha_n \log n = \alpha^\star$ *exists then we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K} \cap \mathbb{G}(n;\Theta_n) \textit{ is connected}\right] = 0 \quad \textit{if } c < 1 \tag{13}$$

On the other hand, if there exists some $\sigma > 0$ *such that*

$$\sigma n \leq P_n \tag{14}$$

for all $n = 1, 2, \ldots$ *sufficiently large, then we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K} \cap \mathbb{G}(n;\Theta_n) \textit{ is connected}\right] = 1 \quad \textit{if } c > 1. \tag{15}$$

Comparing Theorem 3.2 with Theorem 3.1, 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 [18] or random key graphs [3], [20], [22].

The condition (14) states that the size of the key pool P_n should grow at least linearly with the number of sensor nodes in the network. Although this condition is enforced merely for technical reasons, it is not at all a stringent constraint in a realistic WSN scenario. In fact, it holds trivially for any realization as it is expected [8], [11] that the size of the key pool will be much larger than the number of participating nodes for security purposes.

Theorem 3.2 cannot hold if the condition (10) fails. This is a simple consequence of the fact that if $K_n = 1$ for all n sufficiently large, than the random key graph $\mathbb{K}(n;\theta)$ is disconnected with high probability unless it also holds that $P_n = 1$ for all n sufficiently large; see [24, Lemma 7.1.2, pp. 99].

IV. Numerical Results

We now present numerical results and simulations that show the validity of Theorem 3.1 and Theorem 3.2.

In all experiments, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10,000$. We consider the channel parameters $\alpha = 0.2$, $\alpha = 0.4$, $\alpha = 0.6$ and $\alpha = 0.8$, while varying the parameter K from 1 to 35. For each parameter pair (K, α), we generate 200 independent samples of the graph $\mathbb{K} \cap \mathbb{G}(n;K,P,\alpha)$ and count the number of times (out of a possible 200) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 200, we obtain the (empirical) probabilities for the events

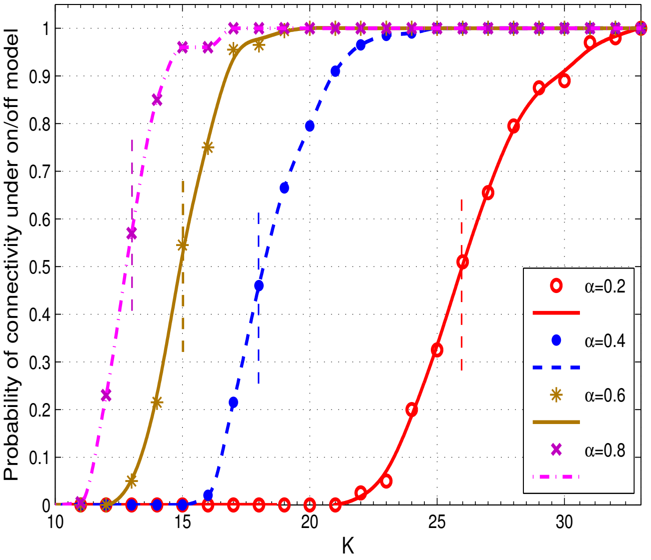

Fig. 1. Empirical probability that $\mathbb{K} \cap \mathbb{G}(n; K, P, \alpha)$ is connected as a function of K for $\alpha = 0.2$, $\alpha = 0.4$, $\alpha = 0.6$, $\alpha = 0.8$ with $n = 500$ and $P = 10,000$; in each case, the empirical probability value is obtained by averaging over 200 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.2. It is clear that the theoretical findings are in perfect agreement with the experimental observations.

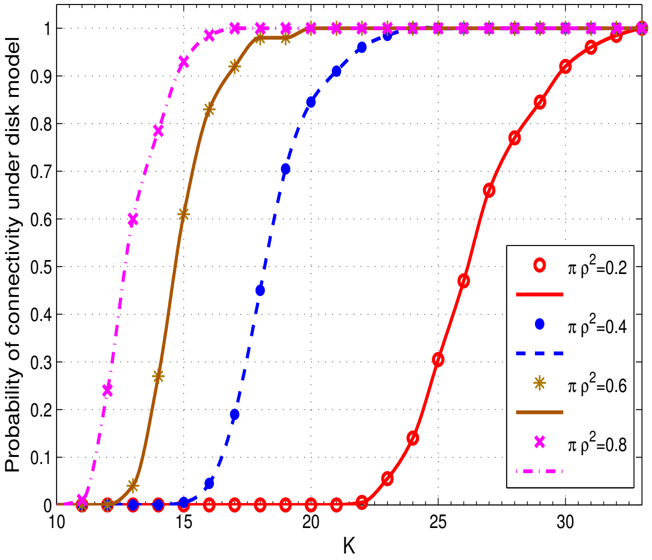

Fig. 2. Empirical probability that $\mathbb{K} \cap \mathbb{H}(n; K, P, \rho)$ is connected as a function of K. The number of nodes is set to $n = 500$ and we take $P = 10,000$. The resemblance of the plots to those of Figure 1 suggests that the connectivity behaviors of the models $\mathbb{K} \cap \mathbb{G}(n; K, P, \alpha)$ and $\mathbb{K} \cap \mathbb{H}(n; K, P, \rho)$ are quite similar under the matching condition $\pi\rho^2 = \alpha$.

of interest. In all cases, we observe that $\mathbb{K} \cap \mathbb{G}(n; K, P, \alpha)$ is connected whenever it has no isolated nodes yielding the same empirical probability for both events. This confirms the asymptotic equivalence of the connectivity and absence of isolated nodes properties in $\mathbb{K} \cap \mathbb{G}(n; \Theta)$ as stated in Proposition 7.1.

In Figure 1, we depict the resulting empirical probability of connectivity in $\mathbb{K} \cap \mathbb{G}(n; K, P, \alpha)$ versus K for several α values. For a better visualization of the data, we use the curve fitting tool of MATLAB. For each α value, we show the critical threshold of connectivity asserted by Theorem 3.2 by a vertical dashed line. Namely, the vertical dashed lines stand for the minimum integer value of K that satisfies

$$1 - q(\theta) = 1 - \frac{\binom{P-K}{K}}{\binom{P}{K}} > \frac{1}{\alpha} \frac{\log n}{n}. \tag{16}$$

Even with $n = 500$, the threshold behavior of the probability of connectivity is evident from the plots. Of course, as n gets large, we expect the curves to look more like a *shifted unit step* function with a jump discontinuity (i.e., a threshold) at around the K value that gives $\mathbb{P}[\text{Connectivity}] = \frac{1}{2}$ in the current plots. Thus, for each value of α, we see that the connectivity threshold prescribed by (16) is in perfect agreement with the experimentally observed threshold of connectivity.

One possible extension of the work presented here would be to consider a more realistic communication model; e.g., the popular disk model [13] instead of the on/off channel model. As discussed in the Introduction, the disk model induces random geometric graphs [18] denoted by $\mathbb{H}(n; \rho)$, where n is the number of nodes and ρ is the transmission range. Under the disk model, studying the EG scheme amounts to analyzing the intersection of $\mathbb{K}(n; \theta)$ and $\mathbb{H}(n; \rho)$, say $\mathbb{K} \cap \mathbb{H}(n; K, P, \rho)$. To compare the connectivity behavior of the EG scheme under the disk model with that of the on-off channel model, 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

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

whenever $\rho < 0.5$. Thus, we can match the two communication models $\mathbb{G}(n; \alpha)$ and $\mathbb{H}(n; \rho)$ by requiring $\pi\rho^2 = \alpha$. Using the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{K} \cap \mathbb{H}(n; K, P, \rho)$ is connected versus K for various ρ values. The results are depicted in Figure 2 whose resemblance with Figure 1 suggests that the connectivity behaviors of the models $\mathbb{K} \cap \mathbb{G}(n; K, P, \alpha)$ and $\mathbb{K} \cap \mathbb{H}(n; K, P, \rho)$ are quite similar under the matching condition $\pi\rho^2 = \alpha$. This raises the possibility that the results obtained here for the on/off communication model can be taken as an indication of the validity of the conjectured zero-one law given under the scaling (5) for the disk model.

V. Preliminaries

Before we give a proof of Theorem 3.1 and Theorem 3.2, we give some preliminary results that will help establish them.

The following inequality will prove useful in a number of places.

Lemma 5.1: For any $\theta = (K, P)$ with positive integers K, P and any scalar $a \geq 1$, we have

$$\frac{\binom{P-\lceil aK \rceil}{K}}{\binom{P}{K}} \leq q(\theta)^a \tag{17}$$

Proof. Observe that under the enforced assumptions it always holds that $q(\theta) \geq 0$, so that (17) holds trivially if $K + \lceil aK \rceil > P$. On the other hand, if $K + \lceil aK \rceil \leq P$, we can use the relation [24, Lemma 5.4.1, pp. 79]

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} = \prod_{\ell=0}^{K-1} \left(1 - \frac{L}{P-\ell} \right)$$

valid for any L such that $L + K \leq P$. Substituting we find

$$\begin{aligned} \frac{\binom{P-\lceil aK \rceil}{K}}{\binom{P}{K}} &= \prod_{\ell=0}^{K-1} \left(1 - \frac{\lceil aK \rceil}{P-\ell} \right) \\ &\leq \prod_{\ell=0}^{K-1} \left(1 - \frac{aK}{P-\ell} \right) \end{aligned} \tag{18}$$

and

$$q(\theta) = \prod_{\ell=0}^{K-1} \left(1 - \frac{K}{P-\ell} \right) \tag{19}$$

In view of (18) and (19), the desired inequality (17) will follow if we show that

$$1 - \frac{aK}{P-\ell} \leq \left(1 - \frac{K}{P-\ell} \right)^a, \quad \ell = 0, 1, \ldots, K-1$$

For each $\ell = 0, 1, \ldots, K-1$, this is immediate once we note that

$$1 - \left(1 - \frac{K}{P-\ell} \right)^a = \int_{1-\frac{K}{P-\ell}}^{1} a t^{a-1} dt \leq \frac{aK}{P-\ell}$$

by a crude bounding argument and (17) follows. ■

We also find it useful to make use of the next result:

Lemma 5.2: Consider $\theta = (K, P)$ with positive integers K, P such that $2K \leq P$. For any $0 < \lambda < 1$, we have

$$1 - q(\theta)^\lambda \geq \lambda (1 - q(\theta)) \tag{20}$$

Proof.

Since $\lambda < 1$, we have

$$1 - q(\theta)^\lambda = \int_{q(\theta)}^{1} \lambda t^{\lambda - 1} dt \geq \int_{q(\theta)}^{1} \lambda dt = \lambda (1 - q(\theta)).$$

■

In the proof of Theorem 3.2, we will make use of a result that is a direct consequence of the condition (14).

Lemma 5.3: Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 0$ and (14) holds for some $\sigma > 0$. Then, for any $\delta > 0$, there exists a finite integer $n^\star = n^\star(\delta)$ such that for all $n \geq n^\star$ sufficiently large, we have

$$K_n \geq \sqrt{(1-\delta)\, \sigma c \log n} \tag{21}$$

for all $n \geq n^\star$ sufficiently large.

Proof. Under the enforced assumptions it can be seen [24, Lemma 7.4.3, pp. 118] from (19) that

$$1 - q(\theta_n) \leq \frac{K_n^2}{P_n - K_n}.$$

Multiplying the above inequality by α_n and using the scaling condition (11), we find

$$c_n \frac{\log n}{n} \leq \alpha_n \frac{K_n^2}{P_n} \frac{1}{1 - \frac{K_n}{P_n}},$$

or equivalently

$$\alpha_n \frac{K_n^2}{P_n} \geq c_n \frac{\log n}{n} \left(1 - \frac{K_n}{P_n} \right)$$

where the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfies $\lim_{n\to\infty} c_n = c$. Invoking (14), we get

$$K_n^2 \geq \frac{1}{\alpha_n} c_n \sigma \log n \left(1 - \frac{K_n}{P_n} \right) \geq c_n \sigma \log n \left(1 - \frac{K_n}{\sigma n} \right)$$

upon using the fact that $\alpha_n \leq 1$ for each $n = 1, 2, \ldots$. This is equivalent to having

$$K_n^2 + K_n \frac{c_n \log n}{n} \geq c_n \sigma \log n$$

which yields

$$K_n^2 (1 + o(1)) \geq c_n \sigma \log n$$

The desired conclusion (21) is now immediate. ■

VI. A proof of Theorem 3.1

We prove Theorem 3.1 by the method of first and second moments [14, p. 55] applied to the total number of isolated nodes in $\mathbb{K} \cap \mathbb{G}(n; \Theta)$. First some notation: Fix $n = 2, 3, \ldots$ and consider $\Theta = (K, P, \alpha)$ with α in $(0,1)$ and positive integers K, P such that $K \leq P$. With

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

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

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

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

The method of first moment [14, Eqn (3.10), p. 55] relies on the well-known bound

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

while the method of second moment [14, 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

$$\begin{aligned}\frac{\mathbb{E}\left[I_n(\Theta)^2\right]}{\mathbb{E}\left[I_n(\Theta)\right]^2} &= \frac{1}{n\mathbb{E}\left[\chi_{n,1}(\Theta)\right]} \\ &\quad + \frac{n-1}{n}\cdot\frac{\mathbb{E}\left[\chi_{n,1}(\Theta)\chi_{n,2}(\Theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\Theta)\right]\right)^2}. \quad (25)\end{aligned}$$

From (22) and (24) we see 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

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

It is also plain from (23) and (25) that the zero-law $\lim_{n\to\infty}\mathbb{P}\left[I_n(\Theta_n)=0\right] = 0$ holds if

$$\lim_{n\to\infty} n\mathbb{E}\left[\chi_{n,1}(\Theta_n)\right] = \infty \quad (27)$$

and

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

The proof of Theorem 3.1 passes through the next two technical propositions which establish (26), (27) and (28) under the appropriate conditions on the scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$.

Proposition 6.1: Consider a scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$ such that (11) holds for some $c > 0$. Then, we have

$$\lim_{n\to\infty} n\mathbb{E}\left[\chi_{n,1}(\Theta_n)\right] = \begin{cases} 0 & \textit{if } c > 1 \\ \\ \infty & \textit{if } c < 1 \end{cases} \quad (29)$$

A proof of Proposition 6.1 is given in Section VI-A.

Proposition 6.2: Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$ such that (11) holds for some $c > 0$. If $\lim_{n\to\infty}\alpha_n \log n = \alpha^\star$ exists, then we have (28) whenever $c < 1$.

A proof of Proposition 6.2 can be found in Section VI-B.

To complete the proof of Theorem 3.1, pick a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 0$ and $\lim_{n\to\infty}\alpha_n = \alpha^\star$ exists. Under the condition $c > 1$ we get (26) from Proposition 6.1, and the one-law $\lim_{n\to\infty}\mathbb{P}\left[I_n(\Theta_n)=0\right] = 1$ follows. Next, assume that $c < 1$. We obtain (27) and (28) with the help of Propositions 6.1 and 6.2, respectively. The conclusion $\lim_{n\to\infty}\mathbb{P}\left[I_n(\Theta_n)=0\right] = 0$ follows and Theorem 3.1 is now established. ■

A. A proof of Proposition 6.1

In the course of proving Proposition 6.1 we make use of the decomposition

$$\log(1-x) = -x - \Psi(x), \quad 0 \leq x < 1 \quad (30)$$

with

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

on that range. Note that

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

Fix $n = 2, 3, \ldots$ and consider $\Theta = (K, P, \alpha)$ with α in $(0,1)$ and positive integers K, P such that $K \leq P$. It is easy to see that $\chi_{n,1}(\Theta) = 1$, meaning that node 1 is isolated, if and only if

$$B_{1j}(\alpha) = 0 \ \vee \ K_1(\theta) \cap K_j(\theta) = \emptyset, \quad j = 2, \ldots, n.$$

Conditioning on $K_1(\theta)$, we get by independence that

$$\mathbb{E}\left[\chi_{n,1}(\Theta)\right] = \left(1 - \alpha(1 - q(\theta))\right)^{n-1}. \quad (31)$$

Now consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 0$ and replace Θ by Θ_n in (31) according to this scaling. Using decomposition (30) we get

$$n\mathbb{E}\left[\chi_{n,1}(\Theta_n)\right] = e^{\beta_n} \quad (32)$$

with

$$\begin{aligned}\beta_n & \\ &= \log n - (n-1)\left(\alpha_n(1-q(\theta_n)) + \psi\left(\alpha_n(1-q(\theta_n))\right)\right) \\ &= \log n - (n-1)\left(c_n\frac{\log n}{n} + \psi\left(c_n\frac{\log n}{n}\right)\right) \\ &= \log n\left(1 - c_n\frac{n-1}{n}\right) \\ &\quad - (n-1)\left(c_n\frac{\log n}{n}\right)^2 \frac{\psi\left(c_n\frac{\log n}{n}\right)}{\left(c_n\frac{\log n}{n}\right)^2}\end{aligned}$$

where the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfies $\lim_{n\to\infty} c_n = c$. Let n go to infinity in this last expression and recall the behavior of $\Psi(x)$ at $x = 0$ mentioned earlier. We have

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

Noting also that

$$\lim_{n\to\infty}\left(1 - c_n\frac{n-1}{n}\right) = 1 - c,$$

we get $\lim_{n\to\infty}\beta_n = \infty$ (resp. $-\infty$) whenever $c < 1$ (resp. $c > 1$). The desired condition (29) is now immediate via (32). ■

B. 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 $\Theta = (K, P, \alpha)$ with α in $(0,1)$ and positive integers K, P such that $K \leq P$. Define the $\{0,1\}$-valued rv $u(\theta)$ by

$$u(\theta) := \mathbf{1}\left[K_1(\theta) \cap K_2(\theta) \neq \emptyset\right].$$

Next, with $r = 1, 2, \ldots, n-1$ define $v_{r,j}(\alpha)$ by

$$v_{r,j}(\alpha) := \{i = 1, 2, \ldots, r : B_{ij}(\alpha) = 1\} \tag{33}$$

for each $j = r+1, \ldots, n$. In other words, $v_{r,j}(\alpha)$ is the set of nodes in $1, \ldots, r$ that have an edge with the node j in the communication graph $\mathbb{G}(n;\alpha)$. Conditioning in $K_1(\theta)$ and $K_2(\theta)$, it is now a simple matter to check that

$$\mathbb{E}\left[\chi_{n,1}(\Theta)\chi_{n,2}(\Theta)\right] = \mathbb{E}\left[(1-\alpha)^{u(\theta)} \prod_{j=3}^{n} \frac{\binom{P - |\cup_{i \in v_{2,j}} K_i(\theta)|}{K}}{\binom{P}{K}}\right]$$

In order to efficiently bound this term, we first observe that under the event $u(\theta) = 0$ (which happens with probability $q(\theta)$), we have

$$|\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)| = |v_{2,j}(\alpha)|K, \quad j = 3, \ldots, n$$

and it is plain by direct inspection and (17) that

$$\frac{\binom{P - |v_{2,j}(\alpha)|K}{K}}{\binom{P}{K}} \leq q(\theta)^{|v_{2,j}(\alpha)|}$$

As a result, we find

$$\begin{aligned}
&\mathbb{E}\left[(1-\alpha)^{u(\theta)} \prod_{j=3}^{n} \frac{\binom{P - |\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)|}{K}}{\binom{P}{K}} \,\middle|\, u(\theta) = 0\right] \\
&\leq \mathbb{E}\left[\prod_{j=3}^{n} q(\theta)^{|v_{2,j}(\alpha)|}\right] \\
&= \mathbb{E}\left[q(\theta)^{|v_{2,3}(\alpha)|}\right]^{n-2} \\
&= \left(\sum_{i=0}^{2} \binom{2}{i} \alpha^i (1-\alpha)^{2-i} q(\theta)^i\right)^{n-2} \\
&= (1 - \alpha(1 - q(\theta)))^{2(n-2)}
\end{aligned} \tag{34}$$

as we note that $\{|v_{r,j}(\alpha)|\}_{j=r+1}^{n}$ are i.i.d. random variables with

$$|v_{r,j}(\alpha)| =_{\text{st}} \text{Bin}(r, \alpha), \quad j = r+1, \ldots, n.$$

On the other hand if $u(\theta) = 1$ (which happens with probability $1 - q(\theta)$) we get

$$\begin{aligned}
&|\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)| \\
&= \begin{cases} 0 & \text{if } |v_{2,j}(\alpha)| = 0 \\ K & \text{if } |v_{2,j}(\alpha)| = 1 \\ 2K - |K_1(\theta) \cap K_2(\theta)| & \text{if } |v_{2,j}(\alpha)| = 2 \end{cases}
\end{aligned}$$

for each $j = 3, \ldots, n$. Therefore, crude bounding argument gives

$$|\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)| \geq K \mathbf{1}\left[|v_{2,j}(\alpha)| > 0\right]$$

yielding

$$\frac{\binom{P - |\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)|}{K}}{\binom{P}{K}} \leq q(\theta)^{\mathbf{1}[|v_{2,j}(\alpha)| > 0]}$$

With these in mind we obtain

$$\begin{aligned}
&\mathbb{E}\left[(1-\alpha)^{u(\theta)} \prod_{j=3}^{n} \frac{\binom{P - |\cup_{i \in v_{2,j}(\alpha)} K_i(\theta)|}{K}}{\binom{P}{K}} \,\middle|\, u(\theta) = 1\right] \\
&\leq (1-\alpha)\mathbb{E}\left[\prod_{j=3}^{n} q(\theta)^{\mathbf{1}[|v_{2,j}(\alpha)| > 0]}\right] \\
&= (1-\alpha)\mathbb{E}\left[q(\theta)^{\mathbf{1}[|v_{2,3}(\alpha)| > 0]}\right]^{n-2} \\
&= (1-\alpha)\left((1-\alpha)^2 + \left(1 - (1-\alpha)^2\right) q(\theta)\right)^{n-2} \\
&= (1-\alpha)\left((1 - \alpha(1 - q(\theta)))^2 + \alpha^2 q(\theta)(1 - q(\theta))\right)^{n-2} \\
&\leq \left((1 - \alpha(1 - q(\theta)))^2 + \alpha^2 q(\theta)(1 - q(\theta))\right)^{n-2}
\end{aligned} \tag{35}$$

Recalling (31), (34) and (35) we find

$$\begin{aligned}
&\frac{\mathbb{E}\left[\chi_{n,1}(\Theta)\chi_{n,2}(\Theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\Theta)\right]\right)^2} \qquad (36) \\
&\leq q(\theta)\frac{(1 - \alpha(1 - q(\theta)))^{2(n-2)}}{(1 - \alpha(1 - q(\theta)))^{2(n-1)}} + (1 - q(\theta)) \times \\
&\qquad \times \frac{\left((1 - \alpha(1 - q(\theta)))^2 + \alpha^2 q(\theta)(1 - q(\theta))\right)^{n-2}}{(1 - \alpha(1 - q(\theta)))^{2(n-1)}} \\
&= \frac{q(\theta)}{(1 - \alpha(1 - q(\theta)))^2} \\
&\qquad + \frac{1 - q(\theta)}{(1 - \alpha(1 - q(\theta)))^2}\left(1 + \frac{\alpha^2 q(\theta)(1 - q(\theta))}{(1 - \alpha(1 - q(\theta)))^2}\right)^{n-2} \\
&\leq \frac{q(\theta) + (1 - q(\theta))\exp\{\frac{\alpha^2(1 - q(\theta))n}{(1 - \alpha(1 - q(\theta)))^2}\}}{(1 - \alpha(1 - q(\theta)))^2}
\end{aligned}$$

Now consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c < 1$ and replace Θ by Θ_n in (36) according to this scaling. Invoking (11) it is immediate that

$$\lim_{n \to \infty} (1 - \alpha_n(1 - q(\theta_n)))^2 = 1$$

and the desired condition (28) will follow if we show that

$$\limsup_{n \to \infty} \left(q(\theta_n) + (1 - q(\theta_n))\exp\left\{\frac{\alpha_n c_n \log n}{\left(1 - c_n \frac{\log n}{n}\right)^2}\right\}\right) \leq 1 \tag{37}$$

with $\lim_{n\to\infty} c_n = c < 1$. As in the statement of Proposition 6.2 assume that $\lim_{n\to\infty} \alpha_n \log n = \alpha^\star$ exists. We consider the cases $\alpha^\star = 0$ and $\alpha^\star \in (0, \infty]$ separately. Firstly, if $\alpha^\star = 0$ we get

$$\lim_{n \to \infty} \exp\left\{\frac{\alpha_n c_n \log n}{\left(1 - c_n \frac{\log n}{n}\right)^2}\right\} = 1$$

and (37) readily follows.

Next, assume that $\alpha^\star > 0$. Recalling the scaling condition (11), we write

$$\begin{aligned}
& q(\theta_n) + (1 - q(\theta_n)) \exp\left\{ \frac{\alpha_n c_n \log n}{\left(1 - c_n \frac{\log n}{n}\right)^2} \right\} \\
= \quad & q(\theta_n) + (1 - q(\theta_n)) \alpha_n \log n \frac{\exp\left\{ \frac{\alpha_n c_n \log n}{\left(1 - c_n \frac{\log n}{n}\right)^2} \right\}}{\alpha_n \log n} \\
= \quad & q(\theta_n) + c_n \log n^2 \cdot \frac{n^{-1 + \frac{\alpha_n c_n}{\left(1 - c_n \frac{\log n}{n}\right)^2}}}{\alpha_n \log n} \\
\leq \quad & q(\theta_n) + c_n \log n^2 \cdot \frac{n^{-1 + \frac{c_n}{\left(1 - c_n \frac{\log n}{n}\right)^2}}}{\alpha_n \log n}
\end{aligned}$$

upon using the fact that $\alpha_n \leq 1$ in the last step. Under the enforced assumptions, we clearly have

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

and we find

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

upon recalling the assumption that $\lim_{n \to \infty} \alpha_n \log n = \alpha^\star > 0$. The desired condition (37) follows as we note that $q(\theta_n) \leq 1$. ■

VII. A proof of Theorem 3.2 (Outline)

Fix $n = 2, 3, \ldots$ and consider $\Theta = (K, P, \alpha)$ with α in $(0, 1)$ and positive integers K, P such that $K \leq P$. We define the events

$$C_n(\Theta) := [\mathbb{K} \cap \mathbb{G}(n; \Theta) \text{ is connected}]$$

and

$$I(n; \Theta) := [\mathbb{K} \cap \mathbb{G}(n; \Theta) \text{ contains no isolated nodes}] .$$

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

$$\mathbb{P}\left[C_n(\Theta)\right] \leq \mathbb{P}\left[I(n; \Theta)\right] \tag{38}$$

and

$$\mathbb{P}\left[C_n(\Theta)^c\right] = \mathbb{P}\left[C_n(\Theta)^c \cap I(n; \theta)\right] + \mathbb{P}\left[I(n; \Theta)^c\right] \tag{39}$$

obtain.

Taken together with Theorem 3.1, the relations (38) and (39) pave the way to proving Theorem 3.2. Indeed, pick a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0, 1)$ such that (11) holds for some $c > 0$ and $\lim_{n \to \infty} \alpha_n \log n = \alpha^\star$ exists. If $c < 1$, 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 (38). If $c > 1$, 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 (39) if we show the following:

Proposition 7.1: For any scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0, 1)$ *such that (11) holds for some* $c > 1$, *we have*

$$\lim_{n \to \infty} \mathbb{P}\left[C_n(\Theta_n)^c \cap I(n; \Theta_n)\right] = 0. \tag{40}$$

as long as the condition (14) is satisfied.

The basic idea in establishing Proposition 7.1 is to find a sufficiently tight upper bound on the probability in (40) 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].

We begin by finding the needed upper bound: Fix $n = 2, 3, \ldots$ and consider $\Theta = (K, P, \alpha)$ with α in $(0, 1)$ and positive integers K, P such that $K \leq P$. For the reasons that will later become apparent we find it useful to introduce the event $E_n(\boldsymbol{X}_n(\theta))$ in the following manner:

$$E_n(\boldsymbol{X}_n(\theta)) = \bigcup_{S \subseteq \mathcal{N}:\ |S| \geq 1} \left[\left| \cup_{i \in S} K_i(\theta) \right| \ \leq \ X_{n, |S|}(\theta) \right]$$

where $\boldsymbol{X}_n(\theta) = [X_{n,1}(\theta) \ \ X_{n,2}(\theta) \ \ \cdots \ \ X_{n,n}(\theta)]$ is an n-dimensional integer valued array. Let

$$r_n(\theta) := \min\left(r(\theta), \left\lfloor \frac{n}{2} \right\rfloor \right) \quad \text{with} \quad r(\theta) := \left\lfloor \frac{P}{K} \right\rfloor .$$

In due course, we always set

$$X_{n,i}(\theta) = \begin{cases} \lfloor \lambda K i \rfloor & i = 1, 2, \ldots, r_n(\theta) \\ \\ \lfloor \mu P \rfloor & i = r_n(\theta) + 1, \ldots, n \end{cases} \tag{41}$$

for some λ, μ in $(0, \frac{1}{2})$ that will be specified later. For convention, we also take $X_{n,0} = 0$.

By a crude bounding argument we now get

$$\begin{aligned}
& \mathbb{P}\left[C_n(\Theta)^c \cap I(n; \Theta)\right] \\
& \quad \leq \ \mathbb{P}\left[E_n(\boldsymbol{X}_n(\theta))\right] + \mathbb{P}\left[C_n(\Theta)^c \cap I(n; \Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right]
\end{aligned}$$

Hence, a proof of Proposition 7.1 consists of establishing the following two results.

Proposition 7.2: Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0, 1)$ *such that (11) holds for some* $c > 1$, *and (14) is satisfied for some* $\sigma > 0$. *We have*

$$\lim_{n \to \infty} \mathbb{P}\left[E_n(\boldsymbol{X}_n(\theta_n))\right] = 0, \tag{42}$$

where $\boldsymbol{X}_n(\theta_n) = [X_{n,1}(\theta_n) \ \cdots \ X_{n,n}(\theta_n)]$ *is as specified in (41) with* λ *in* $(0, \frac{1}{2})$ *is selected small enough to ensure*

$$\max\left(2\lambda\sigma, \lambda \left(\frac{e^2}{\sigma} \right)^{\frac{\lambda}{1 - 2\lambda}} \right) < 1, \tag{43}$$

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

$$\max\left(2 \left(\sqrt{\mu} \left(\frac{e}{\mu} \right)^{\mu} \right)^{\sigma}, \sqrt{\mu} \left(\frac{e}{\mu} \right)^{\mu} \right) < 1. \tag{44}$$

A proof of Proposition 7.2 can be found in Section VIII. Note that for any $\sigma > 0$, $\lim_{\lambda \downarrow 0} \lambda \left(\frac{e^2}{\sigma}\right)^{\frac{\lambda}{1-2\lambda}} = 0$ so that the condition (43) can always be met by suitably selecting $\lambda > 0$ small enough. Also, we have $\lim_{\mu \downarrow 0} \left(\frac{e}{\mu}\right)^{\mu} = 1$, whence $\lim_{\mu \downarrow 0} \sqrt{\mu} \left(\frac{e}{\mu}\right)^{\mu} = 0$, and (44) can be made to hold for any $\sigma > 0$ by taking $\mu > 0$ sufficiently small.

Proposition 7.3: Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 1$, and (14) is satisfied for some $\sigma > 0$. We have

$$\lim_{n \to \infty} \mathbb{P}\left[C_n(\Theta_n)^c \cap I(n;\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] = 0,$$

where $\boldsymbol{X}_n(\theta_n) = [X_{n,1}(\theta_n) \ \cdots \ X_{n,n}(\theta_n)]$ is as specified in (41) with μ in $(0, \frac{1}{2})$ selected small enough to ensure (44) and $\lambda \in (0, \frac{1}{2})$ selected such that it satisfies (43).

A proof of Proposition 7.3 is given in Section IX.

VIII. A PROOF OF PROPOSITION 7.2

The arguments that will lead to (42) are taken mostly from [24]. First observe by a standard union bound that

$$\begin{aligned}
&\mathbb{P}\left[E_n(\boldsymbol{X}_n(\theta))\right] \\
&\quad \leq \sum_{S \subseteq \mathcal{N} : 1 \leq |S| \leq n} \mathbb{P}\left[|\cup_{i \in S} K_i(\theta)| \ \leq \ X_{n,|S|}(\theta)\right] \\
&\quad = \sum_{r=1}^{n} \left(\sum_{S \in \mathcal{N}_{n,r}} \mathbb{P}\left[|\cup_{i \in S} K_i(\theta)| \ \leq \ X_{n,r}(\theta)\right] \right)
\end{aligned}$$

where $\mathcal{N}_{n,r}$ denotes the collection of all subsets of $\{1, \ldots, n\}$ with exactly r elements. By using exchangeability and the fact that $|\mathcal{N}_{n,r}| = \binom{n}{r}$, we get

$$\begin{aligned}
\mathbb{P}\left[E_n(\boldsymbol{X}_n(\theta))\right] &\leq \sum_{r=1}^{n} \binom{n}{r} \mathbb{P}\left[U_r(\theta) \ \leq \ X_{n,r}(\theta)\right] \\
&= \sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[U_r(\theta) \ \leq \ \lfloor \lambda r K \rfloor\right] \qquad (45) \\
&\quad + \sum_{r=r_n(\theta)+1}^{n} \binom{n}{r} \mathbb{P}\left[U_r(\theta) \ \leq \ \lfloor \mu P \rfloor\right]
\end{aligned}$$

where $U_r(\theta)$ matches the definition given in [22], i.e.,

$$U_r(\theta) = | \cup_{i=1}^{r} K_i(\theta)|.$$

Now, consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 1$ and assume that the condition (14) is satisfied for some $\sigma > 0$. Replace θ by θ_n in (45) with respect to this scaling. It was shown in [24, Proposition 7.4.14] that for any scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0$ such that (14) holds for some $\sigma > 0$, we have

$$\lim_{n \to \infty} \sum_{r=r_n(\theta_n)+1}^{n} \binom{n}{r} \mathbb{P}\left[U_r(\theta_n) \leq \lfloor \mu P_n \rfloor\right] = 0$$

whenever μ in $(0, \frac{1}{2})$ is selected so that (44) holds. Hence, the desired conclusion (42) will follow if we show that

$$\lim_{n \to \infty} \sum_{r=1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[U_r(\theta_n) \leq \lfloor \lambda r K_n \rfloor\right] = 0 \qquad (46)$$

under the condition (43). Under the enforced assumptions, one can easily deduce from [24, Proposition 7.4.13] that for any λ in $(0, \frac{1}{2})$ small enough to ensure (43) we have (46) and this establishes Proposition 7.2. ■

IX. A PROOF OF PROPOSITION 7.3

Fix $n = 2, 3, \ldots$ and consider $\Theta = (K, P, \alpha)$ with α in $(0,1)$ and positive integers K, P such that $K \leq P$. For any non-empty subset S of nodes, i.e., $S \subseteq \{1, \ldots, n\}$, we define the graph $\mathbb{K} \cap \mathbb{G}(n;\Theta)(S)$ (with vertex set S) as the subgraph of $\mathbb{K} \cap \mathbb{G}(n;\Theta)$ restricted to the nodes in S. We also say that S is *isolated* in $\mathbb{K} \cap \mathbb{G}(n;\Theta)$ if there are no edges (in $\mathbb{K} \cap \mathbb{G}(n;\Theta)$) between the nodes in S and the nodes in the complement $S^c = \{1, \ldots, n\} - S$. This is characterized by

$$K_i(\theta) \cap K_j(\theta) = \emptyset \ \vee \ B_{ij}(\alpha) = 0, \quad i \in S, \ j \in S^c.$$

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

$$\begin{aligned}
&D_n(\Theta; S) \\
&\ := \ \left[K_i(\theta) \cap K_j(\theta) = \emptyset \ \vee \ B_{ij}(p) = 0, \quad i \in S, \ j \in S^c\right].
\end{aligned}$$

Finally, we set

$$A_n(\Theta; S) := C_n(\Theta; S) \cap D_n(\Theta; S).$$

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

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

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

By a standard union bound argument, we immediately get

$$\begin{aligned}
&\mathbb{P}\left[C_n(\Theta)^c \cap I(n;\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\
&\quad \leq \sum_{S \subseteq \mathcal{N} : 2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} \mathbb{P}\left[A_n(\Theta; S) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\
&\quad = \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{S \in \mathcal{N}_{n,r}} \mathbb{P}\left[A_n(\Theta; S) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \right) \qquad (47)
\end{aligned}$$

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 $A_{n,r}(\Theta) := A_n(\Theta; \{1, \ldots, r\})$, $D_{n,r}(\Theta) := D_n(\Theta; \{1, \ldots, r\})$ 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 before. 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

$$\begin{aligned} \sum_{S \in \mathcal{N}_{n,r}} & \mathbb{P}\left[A_n(\Theta; S) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ = & \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \end{aligned}$$

follows since $|\mathcal{N}_{n,r}| = \binom{n}{r}$. Substituting into (47) we obtain the key bound

$$\begin{aligned} & \mathbb{P}\left[C_n(\Theta)^c \cap I(n; \Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ & \leq \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right]. \end{aligned} \tag{48}$$

Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ as in the statement of Proposition 7.1. Substitute Θ by Θ_n by means of this scaling in the right hand side of (48). The proof of Proposition 7.1 will be completed once we show

$$\lim_{n \to \infty} \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] = 0. \tag{49}$$

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

X. Bounding the probabilities $\mathbb{P}\left[A_{n,r}(\Theta)\right]$ $(r = 1, \ldots, n)$

Consider α in $(0,1)$ and positive integers K and P such that $K \leq P$. Fix $n = 2, 3, \ldots$ and pick $r = 1, \ldots, n-1$. First, observe the equivalence

$$D_{n,r}(\Theta) = \left[\left(\cup_{i \in v_{r,j}(\alpha)} K_i(\theta)\right) \cap K_j(\theta) = \emptyset, \ j = r+1, \ldots n\right]$$

where $v_{r,j}(\alpha)$ is as defined in (33). Hence, under the enforced assumptions on the rvs $K_1(\theta), \ldots, K_n(\theta)$, we readily obtain the expression

$$\begin{aligned} & \mathbb{P}\left[D_{n,r}(\Theta) \;\middle|\; \begin{array}{c} K_i(\theta), \ i = 1, \ldots, r \\ B_{ij}(\alpha), \ i = 1, \ldots, r, j = r+1, \ldots, n \end{array}\right] \\ & = \prod_{j=r+1}^{n} \left(\frac{\binom{P - |\cup_{i \in v_{r,j}(\alpha)} K_i(\theta)|}{K}}{\binom{P}{K}}\right) \end{aligned}$$

It is clear that the distributional properties of the term $|\cup_{i \in v_{r,j}(\alpha)} K_i(\theta)|$ will play an important role in efficiently bounding $\mathbb{P}\left[D_{n,r}(\Theta)\right]$. Note that it is always the case that

$$|\cup_{i \in v_{r,j}(\alpha)} K_i(\theta)| \geq K \mathbf{1}\left[|v_{r,j}(\alpha)| > 0\right]. \tag{50}$$

Also, on the event $E_n(\boldsymbol{X}_n(\theta))^c$, we have

$$|\cup_{i \in v_{r,j}(\alpha)} K_i(\theta)| \geq \left(X_{n,|v_{r,j}(\alpha)|}(\theta) + 1\right) \cdot \mathbf{1}\left[|v_{r,j}(\alpha)| > 0\right] \tag{51}$$

for each $j = r+1, \ldots, n$. Conditioning on the rvs $K_1(\theta), \ldots, K_r(\theta)$ and $\{B_{ij}(\alpha), \ i,j = 1, \ldots, r\}$ (which determine the event $C_r(\Theta)$), we conclude via (50)-(51) that

$$\begin{aligned} & \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ = & \ \mathbb{P}\left[C_r(\Theta) \cap D_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ \leq & \ \mathbb{E}\left[\begin{array}{l} \mathbf{1}\left[C_r(\Theta)\right] \times \\ \times \prod_{j=r+1}^{n} \frac{\binom{P - \max\{K, X_{n,|v_{r,j}(\alpha)|}(\theta)+1\} \cdot \mathbf{1}[|v_{r,j}(\alpha)|>0]}{K}}{\binom{P}{K}} \end{array}\right] \end{aligned}$$

Observe that the event $C_r(\Theta)$ is independent from the set-valued random variables $v_{r,j}(\alpha)$ for each $j = r+1, \ldots, n$. Also, as noted before $\{|v_{r,j}(\alpha)|\}_{j=r+1}^{n}$ are i.i.d.. Invoking these we obtain

$$\begin{aligned} & \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ \leq & \ \mathbb{E}\left[\frac{\binom{P - \max\{K, X_{n,|v_r(\alpha)|}(\theta)+1\} \mathbf{1}[|v_r(\alpha)|>0]}{K}}{\binom{P}{K}}\right]^{n-r} \\ & \times \mathbb{P}\left[C_r(\Theta)\right] \end{aligned} \tag{52}$$

with $v_r(\alpha)$ denoting a generic random variable identically distributed with $v_{r,j}(\alpha)$, $j = r+1, \ldots, n$, i.e.,

$$v_r(\alpha) =_{\text{st}} \text{Bin}(r, \alpha). \tag{53}$$

We now compute the expectation appearing at (52) by using the definition (41).

Lemma 10.1: Consider $\theta = (K, P)$ with positive integers K and P such that $K \leq P$. With $\boldsymbol{X}_n(\theta)$ defined as in (41) for some λ and μ in $(0, \frac{1}{2})$, we have

$$\begin{aligned} & \mathbb{E}\left[\frac{\binom{P - \max\{K, X_{n,|v_r(\alpha)|}(\theta)+1\} \mathbf{1}[|v_r(\alpha)|>0]}{K}}{\binom{P}{K}}\right] \\ & \qquad \leq e^{-\alpha(1-q(\theta))\lambda r} + e^{-K\mu} \mathbf{1}\left[r > r_n(\theta)\right] \end{aligned} \tag{54}$$

for each $r = 1, \ldots, \lfloor \frac{n}{2} \rfloor$.

Proof: Fix $r = 1, \ldots, r_n(\theta)$ and recall (17). On that range, we have

$$\left(X_{n,|v_r(\alpha)|}(\theta) + 1\right) \cdot \mathbf{1}\left[|v_r(\alpha)| > 0\right] \geq \lceil \lambda |v_r(\alpha)| K \rceil.$$

Thus, in view of (17), we get

$$\begin{aligned} & \frac{\binom{P - \max\{K, X_{n,|v_r(\alpha)|}(\theta)+1\} \mathbf{1}\left[|v_r(\alpha)| > 0\right]}{K}}{\binom{P}{K}} \\ \leq & \ \frac{\binom{P - \max\{\lceil \lambda |v_r(\alpha)| K \rceil, K \mathbf{1}[|v_r(\alpha)|>0]\}}{K}}{\binom{P}{K}} \\ \leq & \ q(\theta)^{\lambda |v_r(\alpha)| \mathbf{1}[\lambda |v_r(\alpha)| \geq 1] + \mathbf{1}[|v_r(\alpha)|>0] \mathbf{1}[\lambda |v_r(\alpha)| < 1]} \\ \leq & \ q(\theta)^{\lambda |v_r(\alpha)| \mathbf{1}[\lambda |v_r(\alpha)| \geq 1] + \lambda |v_r(\alpha)| \mathbf{1}[\lambda |v_r(\alpha)| < 1]} & (55) \\ = & \ q(\theta)^{\lambda |v_r(\alpha)|} & (56) \end{aligned}$$

where in (55) we used the facts that

$$\mathbf{1}\left[|v_r(\alpha)| > 0\right] \mathbf{1}\left[\lambda |v_r(\alpha)| < 1\right] \geq \lambda |v_r(\alpha)| \mathbf{1}\left[\lambda |v_r(\alpha)| < 1\right]$$

and $q(\theta) < 1$.

Now, direct computation via (53) yields

$$\begin{aligned}\mathbb{E}\left[q(\theta)^{\lambda|v_r(\alpha)|}\right] &= \sum_{j=0}^{r}\binom{r}{j}\alpha^j(1-\alpha)^{r-j}q(\theta)^{\lambda j} \\ &= \left(1-\alpha\left(1-q(\theta)^{\lambda}\right)\right)^r \\ &\leq (1-\alpha\lambda(1-q(\theta)))^r \qquad (57) \\ &\leq e^{-\alpha(1-q(\theta))\lambda r}, \qquad (58)\end{aligned}$$

upon using (20) in (57), and the first term in (54) is established.

On the range $r = r_n(\theta)+1, \ldots, \lfloor \frac{n}{2} \rfloor$, we use

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} \leq e^{-\frac{K}{P}\cdot L}$$

that holds [24, Lemma 5.4.1, pp. 79] for any positive integer L. Thus, in view of (56), we have

$$\begin{aligned}&\mathbb{E}\left[\frac{\binom{P-\max\{K,X_{n,|v_r(\alpha)|}(\theta)+1\}\mathbf{1}[|v_r(\alpha)|>0]}{K}}{\binom{P}{K}}\right] \\ &\leq \mathbb{E}\left[q(\theta)^{\lambda|v_r(\alpha)|}\mathbf{1}\left[|v_r(\alpha)| \leq r_n(\theta)\right]\right] \qquad (59) \\ &\quad + \mathbb{E}\left[e^{-\frac{K}{P}\cdot(\lfloor \mu P\rfloor+1)}\mathbf{1}\left[|v_r(\alpha)| > r_n(\theta)\right]\right]\end{aligned}$$

upon using the fact that

$$\max\{K, X_{n,|v_r(\alpha)|}(\theta)+1\}\mathbf{1}\left[|v_r(\alpha)|>0\right] \geq \lfloor \mu P \rfloor + 1$$

whenever $|v_r(\alpha)| > r_n(\theta)$.

In view of (58) and (59), we now obtain

$$\begin{aligned}&\mathbb{E}\left[\frac{\binom{P-\max\{K,X_{n,|v_r(\alpha)|}(\theta)+1\}\mathbf{1}[|v_r(\alpha)|>0]}{K}}{\binom{P}{K}}\right] \\ &\leq e^{-\alpha(1-q(\theta))\lambda r} \\ &\quad + \mathbb{E}\left[e^{-\frac{K}{P}\cdot(\lfloor \mu P\rfloor+1)}\mathbf{1}\left[|v_r(\alpha)| > r_n(\theta)\right]\right] \\ &\leq e^{-\alpha(1-q(\theta))\lambda r} + \mathbb{E}\left[e^{-\frac{K}{P}\cdot(\lfloor \mu P\rfloor+1)}\right] \\ &\leq e^{-\alpha(1-q(\theta))\lambda r} + e^{-\mu K}\end{aligned}$$

and the desired conclusion (54) follows. ■

We also find it useful to note the crude bound

$$\begin{aligned}&\mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\ &\leq \mathbb{P}\left[C_r(\Theta)\right]\mathbb{E}\left[\frac{\binom{P-K\cdot\mathbf{1}[|v_r(\alpha)|>0]}{K}}{\binom{P}{K}}\right]^{n-r} \\ &= \mathbb{P}\left[C_r(\Theta)\right]\mathbb{E}\left[q(\theta)^{\mathbf{1}[|v_r(\alpha)|>0]}\right]^{n-r} \qquad (60)\end{aligned}$$

immediate by direct inspection from (52).

The next result shows that for each $r = 2.\ldots,n$, the probability of the event $C_r(\Theta)$ can be provided an upper bound in terms of known quantities.

Lemma 10.2: For each $r = 2,\ldots,n$, we have

$$\mathbb{P}\left[C_r(\Theta)\right] \leq r^{r-2}\left(\alpha\left(1-q(\theta)\right)\right)^{r-1}. \qquad (61)$$

Proof. First some notation: For each $r = 2,\ldots,n$, let $\mathbb{K}_r(n;\theta)$ and $\mathbb{G}_r(n;\alpha)$ define the subgraphs $\mathbb{K}(S)$ and $\mathbb{G}(S)$, respectively, when $S = \{1,\ldots,r\}$. Similarly let $\mathbb{K}_r \cap \mathbb{G}_r(n;\Theta)$ stand for the subgraph $\mathbb{K} \cap \mathbb{G}(S)$. Finally, let $\mathcal{T}_r$ denote the collection of all spanning trees on the vertex set $\{1,\ldots,r\}$. It was shown [24, Lemma 7.4.5, pp. 124] that

$$\mathbb{P}\left[T \subset \mathbb{K}_r(n;\theta)\right] = (1-q(\theta))^{r-1}, \quad T \in \mathcal{T}_r \qquad (62)$$

where the notation $T \subset \mathbb{K}_r(n;\theta)$ indicates that the tree T is a subgraph spanning $\mathbb{K}_r(n;\theta)$. It is also well known [5] that

$$\mathbb{P}\left[T \subset \mathbb{G}_r(n;\alpha)\right] = \alpha^{r-1}, \quad T \in \mathcal{T}_r \qquad (63)$$

By independence we find

$$\mathbb{P}\left[T \subset \mathbb{K}_r \cap \mathbb{G}_r(n;\Theta)\right] = \left(\alpha\left(1-q(\theta)\right)\right)^{r-1}, \quad T \in \mathcal{T}_r, \qquad (64)$$

upon combining (62) and (63).

By Cayley's formula [16] there are r^{r-2} trees on r vertices, i.e., $|\mathcal{T}_r| = r^{r-2}$, and (61) follows (via (64)) upon making use of a union bound. ■

XI. Establishing (49)

It is now clear how to proceed: Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$ as in the statement of Proposition 7.1. For the time being, pick an integer $R \geq 2$ (to be specified in Section XIII), and for n sufficiently large consider the decomposition

$$\begin{aligned}&\sum_{r=2}^{\lfloor \frac{n}{2} \rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &= \sum_{r=2}^{R}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad + \sum_{r=R+1}^{\max\{R,r_n(\theta)\}}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad + \sum_{r=\max\{R,r_n(\theta)\}+1}^{\lfloor \frac{n}{2} \rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right].\end{aligned}$$

Let n go to infinity: The desired convergence (49) will be established if we show

$$\lim_{n\to\infty}\sum_{r=2}^{R}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] = 0, \qquad (65)$$

$$\lim_{n\to\infty}\sum_{r=R+1}^{\max\{R,r_n(\theta_n)\}}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] = 0 \qquad (66)$$

and

$$\begin{aligned}&\lim_{n\to\infty}\sum_{r=\max\{R,r_n(\theta_n)\}+1}^{\lfloor \frac{n}{2} \rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &= 0 \qquad (67)\end{aligned}$$

The next sections are devoted to proving the validity of (65), (66) and (67) by repeated applications of the inequalities (52) and Lemmas 10.1-10.2. Throughout, we also make repeated use of the standard bounds

$$\binom{n}{r} \leq \left(\frac{en}{r}\right)^r \tag{68}$$

valid for all $r, n = 1, 2, \ldots$ with $r \leq n$. Finally, we note by convexity that the inequality

$$(x+y)^p \leq 2^{p-1}(x^p + y^p), \qquad \begin{matrix} x, y \geq 0 \\ p \geq 1 \end{matrix} \tag{69}$$

holds.

XII. Establishing (65)

For any arbitrary integer $R \geq 2$, it is clear that (65) will follow upon showing

$$\lim_{n\to\infty} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] = 0, \quad r = 2, 3, \ldots$$

Fix $r = 2, 3, \ldots$ and recall (60), (61) together with (68). We get

$$\begin{aligned}
&\binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\
&\leq \binom{n}{r} \mathbb{P}\left[C_r(\Theta)\right] \mathbb{E}\left[q(\theta)^{\mathbf{1}[|v_r(\alpha)|>0]}\right]^{n-r} \\
&\leq \left(\frac{en}{r}\right)^r r^{r-2} \left(\alpha\left(1-q(\theta)\right)\right)^{r-1} \mathbb{E}\left[q(\theta)^{\mathbf{1}[|v_r(\alpha)|>0]}\right]^{n-r}
\end{aligned}$$

while we find

$$\begin{aligned}
\mathbb{E}\left[q(\theta)^{\mathbf{1}[|v_r(\alpha)|>0]}\right] &= (1-\alpha)^r + \left(1-(1-\alpha)^r\right) q(\theta) \\
&\leq 1 - \alpha(1-q(\theta))
\end{aligned}$$

upon using (53) and the fact that $q(\theta) \leq 1$. This yields

$$\begin{aligned}
&\binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta) \cap E_n(\boldsymbol{X}_n(\theta))^c\right] \\
&\quad \leq (en)^r \left(\alpha\left(1-q(\theta)\right)\right)^{r-1} \left(1-\alpha(1-q(\theta))\right)^{n-r}
\end{aligned} \tag{70}$$

Now consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ such that (11) holds for some $c > 1$ and replace Θ by Θ_n in (70) according to this scaling. We find

$$\begin{aligned}
&\binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\
&\leq (en)^r \left(\alpha_n\left(1-q(\theta_n)\right)\right)^{r-1} \left(1-\alpha_n(1-q(\theta_n))\right)^{n-r} \\
&= (en)^r \left(c_n \frac{\log n}{n}\right)^{r-1} \left(1 - c_n \frac{\log n}{n}\right)^{n-r} \\
&\leq n \left(ec_n \log n\right)^r e^{-c_n \log n \frac{n-r}{n}} \\
&= \left(ec_n \log n\right)^r n^{1-c_n \frac{n-r}{n}}
\end{aligned}$$

with the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfying $\lim_{n\to\infty} c_n = c > 1$. Now let n grow large in this last inequality. We obtain

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

and the desired conclusion (65) follows for any $r = 2, 3, \ldots$. ■

XIII. Establishing (66)

Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ and positive scalars λ, μ as in the statement of Proposition 7.3. Since R can be taken to be arbitrarily large by virtue of the previous section, the desired relation (66) follows immediately if $\limsup r_n(\theta_n) < \infty$. Assume now that $\limsup r_n(\theta_n) = \infty$ and on the range $r = R+1, \ldots, r_n(\theta_n)$, recall (52), (54), (61), and (68). We get

$$\begin{aligned}
&\binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\
&\leq \left(\frac{en}{r}\right)^r r^{r-2} \left(\alpha_n(1-q(\theta_n))\right)^{r-1} e^{-\alpha_n(1-q(\theta_n))r\lambda(n-r)} \\
&= \left(\frac{en}{r}\right)^r r^{r-2} \left(c_n \frac{\log n}{n}\right)^{r-1} e^{-c_n \frac{\log n}{n} r\lambda(n-r)} \\
&\leq n \left(ec_n \log n\right)^r e^{-c_n \log n \cdot r\lambda \frac{n-r}{n}}.
\end{aligned}$$

Now, observe that on the range $r = R+1, \ldots, r_n(\theta_n)$, we have $r \leq \lfloor \frac{n}{2} \rfloor$ so that $\frac{n-r}{n} \geq \frac{1}{2}$. This yields

$$\begin{aligned}
&\sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\
&\leq \sum_{r=R+1}^{r_n(\theta_n)} n \left(ec_n \log n \; e^{-\lambda \frac{c_n}{2} \log n}\right)^r \\
&\leq \sum_{r=R+1}^{\infty} n \left(ec_n \log n \; e^{-\lambda \frac{c_n}{2} \log n}\right)^r.
\end{aligned} \tag{71}$$

Observe that

$$\lim_{n\to\infty} ec_n \log n \; e^{-\frac{c_n}{2}\lambda \log n} = 0 \tag{72}$$

so that the infinite series appearing at (71) is summable. Indeed, for n sufficiently large to ensure that $ec_n \log n \; e^{-\frac{c_n}{2}\lambda \log n} < 1$, we find

$$\begin{aligned}
&\sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\
&\leq n \frac{\left(ec_n \log n \; e^{-\frac{c_n}{2}\lambda \log n}\right)^{R+1}}{1 - ec_n \log n \; e^{-\frac{c_n}{2}\lambda \log n}} \\
&= \frac{\left(ec_n \log n\right)^{R+1} n^{1-\frac{c_n}{2}\lambda(R+1)}}{1 - ec_n \log n \; e^{-\frac{c_n}{2}\lambda \log n,}}
\end{aligned}$$

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

Now let n go to infinity in this last expression. In view of (72), we get (66) whenever R is selected large enough to satisfy

$$\frac{c}{2}\lambda(R+1) > 1. \tag{73}$$

Note that we have $c > 1$ and $\lambda > 0$. Thus, (73) can always be satisfied by selecting

$$R \geq \frac{2}{\lambda} \tag{74}$$

and (66) is now established. ■

XIV. Establishing (67)

Consider a scaling $\Theta : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 \times (0,1)$ and positive scalars λ, μ as in the statement of Proposition 7.3. On the range $r = \max\{R, r_n(\theta_n)\} + 1, \ldots, \lfloor \frac{n}{2} \rfloor$, recall (52), (54), and (61). We get

$$\begin{aligned} &\binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad\leq \binom{n}{r} \mathbb{P}\left[C_r(\Theta_n)\right] \left(e^{-\alpha_n(1-q(\theta_n))r\lambda} + e^{-K_n\mu}\right)^{n-r} \\ &\quad\leq \binom{n}{r} \mathbb{P}\left[C_r(\Theta_n)\right] \left(e^{-c_n \frac{\log n}{n} r\lambda} + e^{-K_n\mu}\right)^{\frac{n}{2}} \end{aligned} \tag{75}$$

where the sequence $c : \mathbb{N}_0 \to \mathbb{R}_+$ satisfies $\lim_{n\to\infty} c_n = c > 1$.

We will establish (67) in two steps. First set

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

Obviously, the range $r = \max\{R, r_n(\theta_n)\} + 1, \ldots, \lfloor \frac{n}{2} \rfloor$ is intersecting the range $r = \hat{r}_n, \ldots, \lfloor \frac{n}{2} \rfloor$. For the latter range, we invoke (75) to get

$$\begin{aligned} &\sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad\leq \sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \left(e^{-c_n \frac{\log n}{n} r\lambda} + e^{-K_n\mu}\right)^{\frac{n}{2}} \\ &\quad\leq \sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \left(e^{-3} + e^{-K_n\mu}\right)^{\frac{n}{2}} \end{aligned}$$

for n sufficiently large since $\lim_{n\to\infty} c_n = c > 1$. Using the binomial formula

$$\sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \leq 2^n,$$

this yields

$$\begin{aligned} &\sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad\leq 2^n \left(e^{-3} + e^{-K_n\mu}\right)^{\frac{n}{2}} \\ &\quad\leq (2\sqrt{2})^n \left(e^{-\frac{3}{2}n} + e^{-\frac{K_n\mu}{2}n}\right) \end{aligned}$$

upon also invoking (69). Now, let n go to infinity and recall from (21) that $\lim_{n\to\infty} K_n = \infty$. We immediately get

$$\lim_{n\to\infty} \sum_{r=\hat{r}_n}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] = 0 \tag{76}$$

since $2\sqrt{2} \cdot e^{-\frac{3}{2}} < 1$.

If $\hat{r}_n \leq r_n(\theta_n) + 1$ for all n sufficiently large, then the desired condition (67) is automatically satisfied via (76). On the other hand, if $r_n(\theta_n) + 1 < \hat{r}_n$, we should still consider the range $r = \max\{R, r_n(\theta_n)\} + 1, \ldots, \hat{r}_n$. But, on that range we have

$$\begin{aligned} &e^{-c_n \frac{\log n}{n} r\lambda} + e^{-\mu K_n} \\ &\quad= e^{-c_n \frac{\log n}{n} r\lambda} \left(1 + e^{-\mu K_n + c_n \frac{\log n}{n} r\lambda}\right) \\ &\quad\leq \exp\left\{-c_n \frac{\log n}{n} r\lambda + e^{-\mu K_n + c_n \frac{\log n}{n} r\lambda}\right\} \\ &\quad= \exp\left\{-c_n \frac{\log n}{n} r\lambda \left(1 - \frac{e^{-\mu K_n + c_n \frac{\log n}{n} r\lambda}}{c_n \frac{\log n}{n} r\lambda}\right)\right\} \\ &\quad\leq \exp\left\{-c_n \frac{\log n}{n} r\lambda \left(1 - \frac{e^{-\mu K_n + 3c_n}}{c_n \frac{\log n}{n} r\lambda}\right)\right\} \end{aligned} \tag{77}$$

while it also holds that

$$\begin{aligned} \frac{e^{-\mu K_n}}{c_n \frac{\log n}{n} r\lambda} &\leq \frac{e^{-\mu K_n}}{c_n \frac{\log n}{n} \min\{\frac{P_n}{K_n}, \frac{n}{2}\}\lambda} \\ &\leq \max\left\{\frac{K_n e^{-\mu K_n}}{c_n \sigma\lambda}, \frac{2e^{-\mu K_n}}{c_n \lambda}\right\} \end{aligned}$$

in view of (14). Invoking the consequence (21) yields

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

whence we get

$$\lim_{n\to\infty} \frac{e^{-\mu K_n + 3c_n}}{c_n \frac{\log n}{n} r\lambda} = 0.$$

It is now immediate via (77) that for any given $\epsilon > 0$, there exists a finite integer $n^\star$ such that if $n \geq n^\star$, we have

$$e^{-c_n \frac{\log n}{n} r\lambda} + e^{-\mu K_n} \leq e^{-c_n \frac{\log n}{n} r\lambda(1-\epsilon)}.$$

Thus, on the range $n = n^\star + 1, \ldots$, we use (75) to get

$$\begin{aligned} &\sum_{\max\{R.r_n(\theta_n)\}+1}^{\hat{r}_n} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad\leq \sum_{\max\{R,r_n(\theta_n)\}+1}^{\hat{r}_n} \binom{n}{r} \mathbb{P}\left[C_r(\Theta_n)\right] e^{-c_n \frac{\log n}{n} r\lambda(1-\epsilon)\frac{n}{2}} \end{aligned}$$

Arguments leading to (71) give

$$\begin{aligned} &\sum_{\max\{R,r_n(\theta_n)\}+1}^{\hat{r}_n} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\Theta_n) \cap E_n(\boldsymbol{X}_n(\theta_n))^c\right] \\ &\quad\leq \sum_{r=\max\{R,r_n(\theta_n)\}+1}^{\infty} n \left(ec_n \log n \; e^{-c_n \frac{(1-\epsilon)}{2}\lambda \log n}\right)^r \end{aligned}$$

and via similar arguments it is easy to see that

$$\lim_{n\to\infty} \sum_{r=\max\{R,r_n(\theta_n)\}+1}^{\infty} n \left(ec_n \log n \; e^{-\frac{c_n(1-\epsilon)}{2}\lambda \log n}\right)^r = 0$$

as long as

$$\liminf_{n\to\infty} \frac{(1-\epsilon)}{2} c\lambda \max\{R, r_n(\theta_n)\} > 1$$

The above relation can be guaranteed by choosing R such that

$$R \geq \frac{2}{\lambda}$$

as in (74). The desired conclusion (67) is now established. ■

Acknowledgment

The author would like to thank the anonymous reviewers for their careful reading of the original manuscript; their comments helped improve the final version of this paper. We also thank Prof. A. M. Makowski from the Department of Electrical and Computer Engineering at the University of Maryland for insightful comments concerning this work and his warm encouragement.

References

[1] I. F. Akyildiz, Y. Sankarsubramaniam, W. Su and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks* **38**, pp. 393-422.

[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,” Proceedings of IEEE Infocom 2010, San Diego (CA), March 2010.

[3] S.R. Blackburn and S. Gerke, “Connectivity of the uniform random intersection graph,” *Discrete Mathematics* **309** (2009), pp. 5130-5140.

[4] M. Bloznelis, J. Jaworski and K. Rybarczyk, “Component evolution in a secure wireless sensor network,” *Networks* **53** (2009), pp. 19-26.

[5] B. Bollobás, *Random Graphs*, Second Edition, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[6] S. A. Çamtepe and B. Yener, “Key Distribution Mechanisms for Wireless Sensor Networks: a Survey,” Technical Report TR-05-07, Computer Science Department, Rensselaer Polytechnic Institute, Troy (NY), March 2005.

[7] H. Chan, A. Perrig and D. Song, “Random key predistribution schemes for sensor networks,” Proceedings of the 2003 IEEE Symposium on Research in Security and Privacy (SP 2003), Oakland (CA), May 2003, pp. 197-213.

[8] R. Di Pietro, A. Mei, L. V. Mancini, A. Panconesi, and J. Radhakrishnan, “Connectivity Properties of Secure Wireless Sensor Networks,” Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004), October 2004, Washington DC, pp. 53-68.

[9] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, “Redoubtable sensor networks,” *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[10] W. Du, J. Deng, Y.S. Han and P.K. Varshney, “A pairwise key predistribution scheme for wireless sensor networks,” Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003), Washington (DC), October 2003, pp. 42-51.

[11] L. Eschenauer and V.D. Gligor, “A key-management scheme for distributed sensor networks,” Proceedings of the ACM Conference on Computer and Communications Security (CSS 2002), Washington (DC), November 2002, pp. 41-47.

[12] M. Franceschetti and R. Meester, “Critical node lifetimes in random networks via the Chen-Stein method,” *IEEE Transactions on Information Theory* **52** (2006), pp. 2831–2837.

[13] P. Gupta and P. R. Kumar, “Critical power for asymptotic connectivity in wireless networks, Chapter in *Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, Edited by W.M. McEneany, G. Yin and Q. Zhang, Birkhauser, Boston (MA), 1998.

[14] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

[15] K. Krzywdziński and K. Rybarczyk, “Geometric Graphs with Randomly Deleted Edges - Connectivity and Routing Protocols,” Proceedings of the 36th international conference on Mathematical foundations of computer science, Warsaw (Poland), 2011, pp. 544–555.

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

[17] M. D. Penrose “The longest edge of the random minimal spanning tree,” *Annals of Applied Probability* **7** (1997), pp. 340–361.

[18] M.D. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability **5**, Oxford University Press, New York (NY), 2003.

[19] A. Perrig, J. Stankovic and D. Wagner, “Security in wireless sensor networks,” *Communications of the ACM* **47** (2004), pp. 53–57.

[20] K. Rybarczyk, “Diameter, connectivity and phase transition of the uniform random intersection graph,” *Discrete Mathematics* **311**:17 (2011), pp. 1998-2019.

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

[22] O. Yağan and A.M. Makowski, “Zero-one laws for connectivity in random key graphs.” *IEEE Transactions on Information Theory*. Accepted for publication (2011). Available online at arXiv:0908.3644v1 [math.CO], August 2009.

[23] O. Yağan and A. M. Makowski, “Designing securely connected wireless sensor networks in the presence of unreliable links,” Proceedings of the IEEE International Conference on Communications (ICC 2011), Tokyo (Japan), June 2011.

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

[25] 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,” *Discrete Mathematics, Algorithms, and Applications* **2**:1 (2010), pp. 107–124.

Osman Yağan (S’07) 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, College Park, MD 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 the Cyber Security Laboratory (CyLab) at the Carnegie Mellon University. His research interests include wireless network security, dynamical processes in complex networks, percolation theory, random graphs and their applications.