Zero-one laws for connectivity in inhomogeneous random key graphs
Osman Yağan, Member, IEEE

Abstract—We introduce a new random key predistribution scheme for securing heterogeneous wireless sensor networks. Each of the $n$ sensors in the network is classified into $r$ classes according to some probability distribution $\mu = \{\mu_1, \ldots, \mu_r\}$. Before deployment, a class-$i$ sensor is assigned $K_i$ cryptographic keys that are selected uniformly at random from a common pool of $P$ keys. Once deployed, a pair of sensors can communicate securely if and only if they have a key in common. We model the communication topology of this network by a newly defined inhomogeneous random key graph. We establish scaling conditions on the parameters $P$ and $\{K_1, \ldots, K_r\}$ so that this graph i) has no isolated nodes; and ii) is connected, both with high probability. The results are given in the form of zero-one laws with the number of sensors $n$ growing unboundedly large; critical scalings are identified and shown to coincide for both graph properties. Our results are shown to complement and improve those given by Godehardt et al. and Zhao et al. for the same model, therein referred to as the general random intersection graph.

Keywords: Heterogeneous Wireless Sensor Networks, Security, Key Predistribution, Inhomogeneous Random Key Graphs, Connectivity.

I. INTRODUCTION

A. Motivation and background
Random key graphs are naturally induced by the Eschenauer-Gligor (EG) random key predistribution scheme [9], which is a widely recognized solution for securing wireless sensor network (WSN) communications [4], [8]. Denoted by $G(n, K, P)$, random key graph is constructed on the vertices $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ as follows. Each vertex $v_i$ is assigned independently a set $\Sigma_i$ of $K$ cryptographic keys that are picked uniformly at random from a pool of size $P$. Then, any pair of vertices $v_i, v_j$ are adjacent if they share a key, i.e., if $\Sigma_i \cap \Sigma_j \neq \emptyset$. Random key graphs have recently received attention in a wide range of areas including modeling small world networks [30], recommender systems [16], and clustering and classification analysis [11]. Properties that have been studied include absence of isolated nodes [29], connectivity [31], [19], $k$-connectivity [35], and $k$-robustness [34], among others.

In this paper we propose and study a variation of the EG scheme that is more suitable for heterogeneous WSNs; it is in fact envisioned that many military and commercial WSN applications will consist of heterogeneous nodes [24], [23]. Namely, we assume that the network consists of sensors with varying level of resources (e.g., computational, memory, power) and possibly with varying level of security and connectivity requirements. As a result of this heterogeneity, it may no longer be sensible to assign the same number of keys to all sensors in the network as prescribed by the EG scheme. Instead, we consider a scheme where the number of keys that will be assigned to each sensor is independently drawn from the set $K = \{K_1, \ldots, K_r\}$ according to some probability distribution $\mu = \{\mu_1, \ldots, \mu_r\}$, for some fixed integer $r$. We can think of this as each vertex $v_i$ being assigned to a priority class-$i$ with probability $\mu_i > 0$ and then receiving a key ring with the size $K_i$ associated with this class. As before, we assume that once its size is fixed, the key ring $\Sigma_x$ is constructed by sampling the key pool randomly and without replacement.

Let $G(n; \mu, K, P)$ denote the random graph induced by the heterogeneous key predistribution scheme described above, where again a pair of nodes are adjacent as long as they share a key; see Section II for precise definitions. Inspired by the recently studied inhomogeneous Erdős-Rényi (ER) graphs [3], [5], we refer to this graph as the inhomogeneous random key graph. The main goal of this paper is to study connectivity properties of $G(n; \mu, K, P)$ and to understand how the parameters $n, \mu, K, P$ should behave so that the resulting graph is connected almost surely. Such results can be useful in deriving guidelines for designing heterogeneous WSNs so that they are securely connected. By comparison with the results for the standard random key graph, they can also shed light on the effect of heterogeneity on the connectivity properties of WSNs.

We remark that inhomogeneous random key graphs model the secure connectivity of heterogeneous WSNs under the assumption of full visibility, whereby all sensors are within transmission range of each other. For sure, the assumption of full visibility does away with the wireless nature of the communication infrastructure supporting WSNs. However, in return this simplification allows us to focus on how the randomness and heterogeneity in key predistribution affect the establishment of secure links. In this respect, our work aims to complete a crucial first step towards understanding the feasibility of heterogeneous schemes in securing WSNs.
Future work should incorporate a wireless communication model to the inhomogeneous random key graph with an eye towards revealing how the unreliability of wireless links affects the results presented here. For example, the intersection of inhomogeneous random key graphs with ER graphs (to incorporate the on-off communication model), or with random geometric graphs (to incorporate the disk communication model [12]) might be considered; see for instance [15], [22], [32], [26], [33], [35] for similar approaches on combining a communication graph and a cryptographic graph. We believe that our work will pave the way towards studying these more complicated models as well.

B. Contributions

We establish zero-one laws for the property that \( G(n; \mu, K, P) \) has no isolated nodes (see Theorem 3.1) and for the property that \( G(n; \mu, K, P) \) is connected (see Theorem 3.2). Namely, we scale the parameters \( K \) and \( P \) and provide critical conditions on this scaling such that the resulting graph almost surely has no isolated node (resp. connected) and almost surely has at least one isolated node (resp. connected), respectively, when the number of nodes \( n \) goes to infinity. We show that the critical conditions for the two graph properties coincide, meaning that absence of isolated nodes and connectivity are asymptotically equivalent properties for the inhomogeneous random key graph. Other well-known models that exhibit the same behavior include ER graphs [2], random key graphs [31], and random geometric graphs [18].

Our results are also compared with the existing results by Zhao et al. [34] and Godehardt et al. [11] for the \( k \)-connectivity and connectivity, respectively, of \( G(n; \mu, K, P) \); in those references \( G(n; \mu, K, P) \) was referred to as a general random intersection graph. We show that earlier results are constrained to narrow parameter ranges that are unlikely to be feasible in real world WSN implementations due to excessive memory requirement or very limited resiliency against adversarial attacks. On the contrary, our results cover parameter ranges that are widely regarded as feasible for most WSNs; see Section III-C for details.

The main difficulty in our analysis lies in the fact that edge assignments are correlated in \( G(n; \mu, K, P) \) (even after conditioning on the class of nodes) as opposed to the inhomogeneous ER graph [3], [5] where edges are assigned independently. For example, for nodes \( v_x, v_y, v_z \) with given types, the edge events \( \{v_x \sim v_y, v_x \sim v_z, v_y \sim v_z\} \) are positively correlated in \( G(n; \mu, K, P) \) while independent in the inhomogeneous ER graph; see [30] for a formal proof of edge correlations in homogeneous random key graphs. Prior work [11], [34] attempted to overcome the associated difficulties by indirect approaches that rely on approximating the inhomogeneous random key graph by other well-studied models. In particular, [11] studied hypergraphs generated by \( G(n; \mu, K, P) \) and used known results for models of random hypergraphs. Similarly, [34] used a coupling argument and approximated \( G(n; \mu, K, P) \) by a homogeneous random key graph. Although these approaches lead to relatively simple proofs based on well-known results, they are inherently constrained to parameter ranges where the edge correlations in \( G(n; \mu, K, P) \) become negligible to allow for the approximation arguments to work. Instead, we use a direct approach and analyze the connectivity of \( G(n; \mu, K, P) \) without resorting to its similarity with other well-behaved models. This is done by using a series of judicious bounding arguments to handle the intricate correlations among the edges of \( G(n; \mu, K, P) \); see Sections IV-X for details.

Our main results indicate that the minimum key ring size in the network has a significant impact on the connectivity of \( G(n; \mu, K, P) \), perhaps in a way that would be deemed surprising. In particular, for the standard random key graph \( G(n; K, P) \) the critical threshold for connectivity and absence of isolated nodes is known [31], [19] to be given by \( \frac{K^2}{P} \sim c\log \frac{n}{\mu} \) and the resulting graph is asymptotically almost surely connected (resp. not connected) if \( c > 1 \) (resp. \( c < 1 \)). For the inhomogeneous random key graph \( G(n; \mu, K, P) \) one would be tempted to think that an equivalent result holds under the scaling \( \frac{K^2}{P} \sim c\log \frac{n}{\mu} \), with \( K_{\text{avg}} = \sum_{j=1}^{\mu} K_j \) denoting the mean key ring size. Instead, we show that the zero-one laws for absence of isolated nodes and connectivity hold under \( K_{\text{min}} \frac{c}{P} \sim c\log \frac{n}{\mu} \), where \( K_{\text{min}} \) stands for the minimum of \( \{K_1, \ldots, K_\mu\} \); see Corollary 3.3. This implies that in the heterogeneous key predistribution scheme, the mean number of keys required per sensor node to achieve connectivity can be significantly larger than that required in the homogeneous case. For instance, the expense of allowing an arbitrarily small fraction of sensors to keep half as many keys as in the homogeneous case would be to increase the average key ring size by two-fold.

C. Organization of the paper

The rest of the paper is organized as follows. In Section II, we give detailed description of the heterogeneous random key predistribution scheme and the resulting inhomogeneous random key graph model. Section III is devoted to presenting the main results of the paper, namely the zero-one laws for absence of isolated nodes (see Theorem 3.1) and for connectivity (see Theorem 3.2) in inhomogeneous random key graphs. There, we also compare our results with relevant work from the literature and also comment on the implications of our results on designing secure sensor networks. In Section IV, we present some preliminary technical results that will be useful in proving the main results of the paper. The proof of Theorem 3.1 is outlined in Section V with necessary technical steps completed in Section VI. We start the proof of Theorem 3.2 in Section VII and complete it in Sections VIII through Section X.

D. Notation and conventions

We close with 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 and variance operators by \( E \) and \( \text{var} \), respectively. We use the notation...
II. MODEL DEFINITIONS

Consider a network that consists of \( n \) sensor nodes labeled as \( v_1, \ldots, v_n \). Our key predistribution idea is based on classifying the nodes in this network into \( r \) sets (e.g., depending on their level of importance) and then assigning different numbers of cryptographic keys to sensors based on their class. Assume that each of the \( n \) nodes in the network are independently assigned to a class according to some probability distribution \( \mu : \{1, \ldots, r\} \to (0, 1) \). Namely, with \( t_x \) denoting the class (or, type) of node \( v_x \), we have

\[
P[t_x = i] = \mu_i > 0, \quad i = 1, \ldots, r,
\]

for each \( \ell = 1, \ldots, n \). Then, a class-\( i \)-node is assigned \( K_i \) keys that are selected uniformly at random from a pool of size \( P \), for each \( i = 1, \ldots, r \). More precisely, the key ring \( \Sigma_x \) of a node \( x \) is an \( \mathcal{P}_{K_i} \)-valued random variable (rv) where \( \mathcal{P}_A \) denotes the collection of all subsets of \( \{1, \ldots, P\} \) which contain exactly \( A \) elements. Obviously, we have \( |\mathcal{P}_A| = (P)_A \). It is further assumed that the rvs \( \Sigma_1, \ldots, \Sigma_n \) are independent and identically distributed.

Let \( K = (K_1, \ldots, K_r) \) and \( \mu = (\mu_1, \ldots, \mu_r) \). Without loss of generality we assume that \( K_1 \leq K_2 \leq \cdots \leq K_r \). Consider a random graph \( G \) defined on the vertex set \( V = \{v_1, \ldots, v_n\} \) such that two nodes \( v_x \) and \( v_y \) are adjacent, denoted \( v_x \sim v_y \), if they have at least one key in common in their corresponding key rings. Namely, we have

\[
v_x \sim v_y \quad \text{if} \quad \Sigma_x \cap \Sigma_y \neq \emptyset.
\]

The adjacency condition (1) defines the inhomogeneous random key graph, hereafter denoted \( G(n; \mu, K, P) \). The name is reminiscent of the recently studied inhomogeneous random graph [3] model where nodes are again divided into \( r \) classes, and a class \( i \) node and a class \( j \) node are connected with probability \( p_{ij} \) independent of everything else. However, the model adopted here differs from the random intersection graphs discussed by Singer- Cohen et al. in [13], [18] where each node is assigned a key ring, one key at a time according to a Bernoulli-like mechanism (so that each key ring has a random size and has positive probability of being empty). This independence disappears in the inhomogeneous random key graph case, but one can still compute \( p_{ij} \) as

\[
p_{ij} := 1 - \left( \frac{P - K_i}{P} \right)^{K_j}, \quad i, j = 1, \ldots, r.
\]

In view of (2), our key predistribution scheme results in higher priority nodes (i.e., nodes with more assigned keys) connecting with each other with higher probability; see Proposition 4.1. In presenting our results below, we shall make use of the mean probability of edge occurrence for each node class. Namely, we define

\[
\lambda_i := \sum_{j=1}^{r} p_{ij} \mu_j, \quad i = 1, \ldots, r,
\]

where \( p_{ij} \) denotes the probability that a node of class-\( i \) and a node of class-\( j \) have an edge in between; see (2). It is easy to see that the mean number of edges incident on a node (i.e., the degree of a node) of class-\( i \) is given by \( (n - 1)\lambda_i \).

Throughout, we assume that the number of classes \( r \) is fixed and do not scale with \( n \), and so are the probabilities \( \mu_1, \ldots, \mu_r > 0 \). All remaining parameters are assumed to be scaled with \( n \), and we shall be interested in the properties of the resulting inhomogeneous random key graph as \( n \) grows unboundedly large. The dependence of scheme parameters and events on \( n \) will be denoted by a subscript, while that of some variables will be denoted by a parenthesis. For instance, we define

\[
p_{ij}(n) := 1 - \left( \frac{P_n - K_{i,n}}{P_{j,n}} \right), \quad i, j = 1, \ldots, r,
\]

and

\[
\lambda_i(n) := \sum_{j=1}^{r} p_{ij}(n) \mu_j, \quad i = 1, \ldots, r.
\]

III. MAIN RESULTS AND DISCUSSION

A. The results

Our main results are presented next. To fix the terminology, we refer to any mapping \( K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \) as a scaling as long as the conditions

\[
1 \leq K_1, n \leq K_2, n \leq \cdots \leq K_r, n < P_n
\]

are satisfied for all \( n = 2, 3, \ldots \). To simplify the notation, we also let \( K_n = (K_1, n, K_2, n, \ldots, K_r, n) \). We first present a zero-one law for the absence of isolated nodes in inhomogeneous random key graphs.

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

\[
\lambda_1(n) \sim c \frac{\log n}{n}
\]

for some \( c > 0 \). Then, we have

\[
\lim_{n \to \infty} \mathbb{P} \left[ G(n; \mu, K_n, P_n) \text{ has no isolated nodes} \right] = \begin{cases} 0 & \text{if } c < 1 \\ 1 & \text{if } c > 1. \end{cases}
\]

A proof of Theorem 3.1 can be found in Section V. The scaling condition (7) will often be used in the equivalent form

\[
\lambda_1(n) = c_n \frac{\log n}{n}
\]

with \( \lim_{n \to \infty} c_n = c > 0 \).
Next, we present an analogous result for the property of graph connectivity.

**Theorem 3.2:** Consider a probability distribution \( \mu = (\mu_1, \ldots, \mu_r) \) with \( \mu_i > 0 \) for \( i = 1, \ldots, r \), and a scaling \( K_1, \ldots, K_r, P : N_0 \rightarrow N_0^{r+1} \) such that (7) holds for some \( c > 0 \). We have

\[
\lim_{n \to \infty} \mathbb{P} [ G(n; \mu, K_n, P_n) \text{ is connected} ] = \begin{cases} 
0 & \text{if } c < 1 \\
1 & \text{if } c > 1.
\end{cases}
\]

under the additional conditions

\[
P_n \geq \sigma n
\]

for all \( n = 2, 3, \ldots \) sufficiently large and

\[
\left( \frac{K_{1,n}}{P_n} \right)^2 = \omega \left( \frac{1}{n} \right)
\]

(12)

In words, Theorem 3.1 (resp. Theorem 3.2) states that the inhomogeneous random key graph \( G(n; \mu, K_n, P_n) \) has no isolated node (resp. is connected) whp if the mean degree of “the nodes that have the least number of keys” is scaled as \((1 + \epsilon) \log n\) for some \( \epsilon > 0 \); in view of Proposition 4.1, the nodes that are assigned the least number of keys have the minimum mean-degree in the graph. On the other hand, if this minimal mean degree scales like \((1 - \epsilon) \log n\) for some \( \epsilon > 0 \), then whp \( G(n; \mu, K_n, P_n) \) has a node that is isolated, and hence not connected. The additional conditions (11) and (12) are enforced here merely for technical reasons and are required only for the one-law part of the connectivity result, Theorem 3.2. A detailed discussion on these additional conditions is given in Section III-B, where we explain why they are likely to hold in many real-world WSN applications. There, we also discuss how and when these conditions can be relaxed or replaced by milder conditions.

Our results demonstrate that the inhomogeneous random key graph provides one more example random graph model where the properties of absence of isolated nodes and connectivity are asymptotically equivalent. Other well-known examples include Erdős-Rényi graphs [2], random key graphs [31], random geometric graphs [18], and intersection of random key graphs and ER graphs [26]. Our results are also analogous to the recent findings by Levroye and Freiman [5] for the connectivity of inhomogeneous Erdős-Rényi graph model, where nodes are classified into \( r \) classes independently according to a probability distribution \( \mu \) and an edge is drawn between a class-\( i \) and a class-\( j \) node with probability \( p_{ij}(n) \) independent of everything else. With \( \lambda_i(n) \) defined as in (5), their result states that if \( \min_{i=1, \ldots, r} \lambda_i(n) \sim c \log n/n \) then with \( c > 1 \) (resp. \( c < 1 \)) the corresponding graph is connected (resp. not connected) whp, under some additional technical conditions.\(^2\)

We now present a corollary that states the zero-one laws of Theorem 3.1 and Theorem 3.2 under a different scaling condition than (7). This alternative formulation will make it easier to derive design guidelines for *dimensioning* heterogeneous key predistribution schemes, namely in adjusting key ring sizes \( K_1, \ldots, K_r \) and probabilities \( \mu_1, \ldots, \mu_r \) such that the resulting network i) has no isolated nodes and ii) is connected, both whp.

**Corollary 3.3:** Consider a probability distribution \( \mu = (\mu_1, \ldots, \mu_r) \) with \( \mu_i > 0 \) for \( i = 1, \ldots, r \), and a scaling \( K_1, \ldots, K_r, P : N_0 \rightarrow N_0^{r+1} \). Let \( |\Sigma|_n \) denote a rv that takes the value \( K_{1,n} \) with probability \( \mu_1 \) for each \( i = 1, \ldots, r \). If it holds that

\[
\frac{K_{1,n} E [ |\Sigma|_n ]}{P_n} \sim c \log n/n
\]

for some \( c > 0 \), then we have the zero-one law (8) for absence of isolated nodes. If, in addition, the the conditions (11) and (12) are satisfied by this scaling, then we also have the zero-one law (10) for connectivity.

A proof of Corollary 3.3 is given in Appendix A, where we show that the scaling conditions (7) and (13) are indeed equivalent to each other, meaning that one can obtain both Theorem 3.1 and Theorem 3.2 from Corollary 3.3, and vice versa. We remark that \( E [ |\Sigma|_n ] \) gives the mean number of keys assigned to a sensor in the network. With this in mind, Corollary 3.3 provides various design choices to ensure that no sensor is isolated in the network: One just has to set the minimum and average key ring sizes such that their multiplication scales as \((1 + \epsilon) \log n\) for some \( \epsilon > 0 \). We also see from Corollary 3.3 that such a scaling would also ensure connectivity as long as the additional conditions (11)-(12) are also satisfied.

To compare with the homogeneous random key predistribution scheme, set \( r = 1 \) and consider a universal key ring size \( K_n \) in Corollary 3.3. This leads to zero-one laws for the absence of isolated nodes and connectivity in the standard random key graph \( G(n; K_n, P_n) \). Namely, with

\[
\frac{K_n^2}{P_n} \sim c \log n/n, \quad c > 0
\]

(14)

analogs of (8) and (10) are obtained for \( G(n; K_n, P_n) \); these results had already been established [29], [31] by the authors (in stronger forms). An interesting observation is that minimum key ring size has a dramatic impact on the connectivity properties of inhomogeneous random key graph. To provide a simple and concrete example, set \( P_n = n \log n \). In the homogeneous case, we see from (14) that the universal key ring size has to scale as \( K_n = (1 + \epsilon) \log n \) for some \( \epsilon > 0 \) to ensure that the network is free of isolated nodes and is connected. In the heterogeneous case, one gains the flexibility of having a positive fraction of sensors in the network with substantially smaller number of keys. For the absence of isolated nodes, a positive fraction of sensors can be assigned as few as one key per node. However, from Corollary 3.3 we see that this comes at the expense of having to assign a substantially larger key rings to a positive fraction of other sensors in the network. More precisely, if \( K_{1,n} = O(1) \) then we must have \( K_{r,n} = \Omega((\log n)^2) \) to have no isolated nodes under the same setting. For connectivity on the other hand, we see from (15) that the minimum key ring size \( K_{1,n} \) can be kept on the order of \( O(\sqrt{\log n}) \) and connectivity can still be achieved with mean key ring size satisfying \( O((\log n)^{1.5}) \).
B. Comments on the conditions (11)-(12) of Theorem 3.2

We now provide a detailed discussion on the technical conditions (11) and (12) enforced in Theorem 3.2. We will focus on i) the feasibility of these additional conditions for real-world WSN implementations, and ii) when and how they can be replaced with milder conditions.

We start with the condition (11) that states the key pool size grows at least linearly with the network size $n$. In terms of applicability in the context of heterogeneous key predistribution schemes in WSNs, this condition is not stringent at all. In fact, it is often needed that key pool size $P_n$ be much larger than the network size $n$ [6], [7], [9] as otherwise the network will be extremely vulnerable against node capture attacks. From a technical point of view, the case where $P_n = \Omega(n)$ is also the more interesting and challenging one as compared to the case where $P_n = o(n)$. For instance, when $P_n = O(n^\delta)$ for some $0 < \delta < 1/2$, the inhomogeneous random key graph $G(n; \mu, K_n, P_n)$ can be shown to be connected for any $\mu$ as long as $K_{1,n} \geq 2$; see [28, Lemma 8.1] for a proof of a similar result for the standard random key graph. This means that if $P_n = O(n^\delta)$ with $\delta < 1/2$, even two keys per sensor node is enough to get network connectivity whp. Finally, we remark that the scaling condition (7) or its equivalent (13) already implies that $P_n = \Omega(n^{1/2+\varepsilon})$ since $K_{1,n}E[|\Sigma_n|] \geq 1$.

Next, we look at the condition (12) and start with discussing possible relaxations. First of all, (12) is stronger than what is possible relaxations. First of all, (12) is stronger than what is often needed for our proof to work; it is enforced to enable a shorter proof and an easier exposition of the main result. By inspection of the arguments in Section X-D, it can be seen that (12) can be replaced with

$$K_{1,n}^2 \geq \frac{2\log 2+\log(1-\mu_r)+\varepsilon}{\mu_r} \quad \text{and} \quad K_{1,n} = \omega(1), \quad \text{if } \mu_r \leq 0.75$$

$$K_{1,n}^2 = \Omega\left(\frac{1}{(\log(\log n))^\beta}\right) \quad \text{and} \quad K_{1,n} = \omega(1), \quad \text{if } \mu_r > 0.75$$

(15)

with some $\beta > 0$ and $\nu > 0$ to be specified, and for any $\varepsilon > 0$ and any finite integer $M$; the details are omitted here for brevity.

As we look at (15), we see that $K_{1,n} = \omega(1)$ is needed for any $\mu_r$. In fact, this condition can easily be satisfied in real-world WSN implementations given that key ring sizes on order of $O(\log n)$ are regarded as feasible for most sensor networks [7]. Considered in combination with (13), other conditions enforced in (15) bounds the variability in the key ring sizes used in the network. In particular, given that

$$\frac{E[|\Sigma_n|]}{K_{1,n}} = K_{1,n}E[|\Sigma_n|] \frac{(K_{1,n})^2}{P_n} = \Theta\left(\frac{1}{n(\log n)^\beta}\right)$$

(15) implies

$$\frac{E[|\Sigma_n|]}{K_{1,n}} = O(\log n) \quad \text{when } \mu_r \leq 0.75 \quad \text{and} \quad \frac{E[|\Sigma_n|]}{K_{1,n}} = O((\log n)^M) \quad \text{when } \mu_r > 0.75.$$
if \( \mathbb{E}[|\Sigma|_n] = \Omega(\sqrt{\log n}) \), \( var[|\Sigma|_n] = o\left(\frac{\mathbb{E}[|\Sigma|_n]^2}{n(\log n)^2}\right) \) and \( |\alpha_n| = o(\log n) \), then

\[
\lim_{n \to \infty} \mathbb{P}[\mathcal{G}(n, D_n, P_n) \text{ is } k\text{-connected}] = 0, \quad \text{if } \lim_{n \to \infty} \alpha_n = -\infty,
\]

\[
1, \quad \text{if } \lim_{n \to \infty} \alpha_n = \infty.
\]

**Theorem 3.5:** [11, Theorem 2] Consider a general random intersection graph \( \mathcal{G}(n, D, P_n) \), where \( D(\ell) = 0 \) for all \( \ell > r \) and \( \ell = 0 \). Namely, all key ring sizes are bound to be on the interval \([1, r]\). Let \( |\Sigma| \) be a random variable following the probability distribution \( D \). Then if \( n P_n (\mathbb{E}[|\Sigma|] - D(1)) - \log P_n \to \infty \) (17) then \( \lim_{n \to \infty} \mathbb{P}[\mathcal{G}(n, D, P_n) \text{ is connected}] = 1 \). Also, if \( D(r) = 1 \) for some \( r \geq 2 \), and it holds that

\[
n = P_n \log P_n + o(\log \log P_n), \quad \text{(18)}
\]

then \( \lim_{n \to \infty} \mathbb{P}[\mathcal{G}(n, D, P_n) \text{ is connected}] = 0 \).

In comparing Theorems 3.1, 3.4 and 3.5, it is worth noting that \( k\)-connectivity is a stronger property than connectivity, which in turn is stronger than absence of isolated nodes. However, although Theorems 3.4 and 3.5 consider strong graph properties, we now argue why the established results come with strict constraints on the parameters of the heterogeneous scheme that are not likely to be applicable for real-world sensor networks. First, Theorem 3.5 focuses on the case where all possible key rings have a finite size that do not scale with \( n \). In addition, with \( \mathbb{E}[|\Sigma|] \) fixed, it is clear that the scaling conditions (17) and (18) both require

\[
P_n = O\left(\frac{n}{\log n}\right). \quad \text{(19)}
\]

Unfortunately, it is often needed that key pool size \( P_n \) be much larger than the network size \( n \) [9], [7] as otherwise the network will be extremely vulnerable against node capture attacks. In fact, one can see that with (19) in effect, an adversary can compromise a significant portion of the key pool (and, hence network communication) by capturing \( o(n) \) nodes.

We now focus on Theorem 3.4, where the major problem arises from the assumption

\[
\text{var}[|\Sigma|_n] = o\left(\frac{\mathbb{E}[|\Sigma|_n]^2}{n(\log n)^2}\right), \quad \text{(20)}
\]

that puts a prohibitively stringent constraint on the variance of the key ring sizes. For instance, (20) precludes using \( K_{2,n} = cK_1,n \), for some \( c > 1 \), and forces key ring sizes to be asymptotically equivalent; i.e., \( K_{r,n} \sim K_1,n \). In fact, for the model to be deemed as inhomogeneous random key graph, the variance of the key ring size should be non-zero. Given that key ring sizes are integer-valued, the simplest possible case would be that \( D(K + 1) = \mu \) and \( D(K) = 1 - \mu \) for some \( 0 < \mu < 1 \) and positive integer \( K \). This would amount to assigning either \( K + 1 \) or \( K \) keys to each node with probabilities \( \mu \) and \( 1 - \mu \), respectively. In this case, we can easily see that \( \text{var}[|\Sigma|] = \mu(1 - \mu) > 0 \) as long as \( 0 < \mu < 1 \). Therefore, for an inhomogeneous random key graph, the condition (20) implies that \( \mathbb{E}[|\Sigma|_n]^2 = \omega(1) \), or, equivalently that

\[
\mathbb{E}[|\Sigma|_n] = o\left(\frac{\sqrt{n \log n}}{\sqrt{n \log n}}\right). \quad \text{(21)}
\]

Put differently, Theorem 3.4 enforces (at the very least) mean key ring size to be much larger than \( \sqrt{n \log n} \). However, a typical wireless sensor network will consist of a very large number of sensors, each with very limited memory and computational capability [9], [7]. As a result, key rings with size \( \omega(\sqrt{n \log n}) \) are unlikely to be implementable in most practical network deployments. In fact, it was suggested by Di Pietro et al. [7] that key rings with size \( O(\log n) \) are acceptable for sensor networks.

In comparison, our results Theorem 3.1 and Theorem 3.2 do not require either of the unrealistic conditions (19) or (21). To see this, note that the enforced scaling condition (9) or its equivalent (13) implies (see also Lemma 4.3)

\[
\frac{K_{1,n} K_{r,n}}{P_n} = \Theta\left(\frac{\log n}{n}\right). \quad \text{(22)}
\]

It is clear that this condition does not require (19), and in fact already enforces \( P_n = \Omega(n/\log n) \). As mentioned earlier, in real-world implementations the key pool size is expected to grow at least linearly with \( n \) so that the additional condition (11) of Theorem 3.2 is automatically satisfied. The second additional condition (12) of our connectivity result (22) can also be satisfied simultaneously without requiring the prohibitively large key ring sizes given at (22). To provide concrete examples, we can use \( P_n = \Theta(n \log n) \), \( K_{1,n} = \Theta(\log n) \) and \( K_{r,n} = \Theta(\log n) \), or \( P_n = \Theta(n \log n) \), \( K_{1,n} = \Theta(\sqrt{n \log n}) \) and \( K_{r,n} = \Theta((\log n)^{3/2}) \). With proper choice of constants in these scalings, we will ensure that i) the resulting WSN is connected almost surely; ii) the key pool size is much larger than the network so that the resulting WSN has good level of resiliency against node capture attacks; and iii) the maximum key ring size used in the network is on the order of the ranges \( \log n \) or \( (\log n)^{3/2} \) that are usually regarded as feasible [9], [7]; these choices also lead to a much smaller mean key ring size than that prescribed in (21).

In conclusion, we showed that our results enable parameter choices that are widely regarded as practical in real-world sensor networks, while previous results given in [34] and [11] do not.

**IV. Preliminaries**

In this section, we establish several preliminary results that will be used in the proof of Theorem 3.1. Recall the definition (2) of edge probabilities \( p_{ij} \) and their mean \( \lambda_i \) given at (3). The first result states that mean edge probabilities are ordered in the same way with the key ring sizes.

**Proposition 4.1:** For any scaling \( K_1, \ldots, K_r, P : N_0 \to N_0^{r+1} \), we have

\[
\lambda_1(n) \leq \lambda_2(n) \leq \cdots \leq \lambda_r(n) \quad \text{(23)}
\]

for each \( n = 2, 3, \ldots \).

**Proof.** In view of (5), the desired result (23) will follow immediately if we show that \( p_{ij}(n) \) is increasing in both \( i \) and
Thus, we readily obtain that $K_i$ increases as $i$ increases. For any $i, j$ such that $K_i + K_j > P$ we see from (2) that $p_{ij}(n) = 1$; otherwise if $K_i + K_j \leq P$ we have $p_{ij}(n) < 1$. Thus, given that $K_i + K_j$ increases with both $i$ and $j$, it will be enough to show that $p_{ij}(n)$ increases with both $i$ and $j$ on the range where $K_i + K_j \leq P$. But, on that range, we have

$$
\frac{(P-K_i)}{K_i} = \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{K_j}{P - \ell} \right) .
$$

(24)

It is now immediate that $(\frac{(P-K_i)}{K_i}) / (\frac{P}{K_i})$ decreases with both $K_i$ and $K_j$, and hence with $i$ and $j$. Hence, $p_{ij}(n)$ is seen to be increasing with $i$ and $j$, and this establishes Proposition 4.1.

A useful consequence of Proposition 4.1 is given next.

**Lemma 4.2:** Consider any scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$. For any $i, j = 1, \ldots, r$, it holds that

$$
\lim_{n \to \infty} p_{ij}(n) = 0 \quad \text{if and only if} \quad \lim_{n \to \infty} \frac{K_{i,n} K_{j,n}}{P_n} = 0,
$$

and under either condition we have the asymptotic equivalence

$$
p_{ij}(n) \sim \frac{K_{i,n} K_{j,n}}{P_n}.
$$

**Proof.** Lemma 4.2 can easily be established by following the same arguments used in [31, Lemma 7.3] or [25, Lemma 7.4.4], namely by applying crude bounds (upper and lower) to the expression (24). The details are omitted here for brevity.

Next, we give a result that collects several useful consequences of the scaling condition (7) under (12).

**Lemma 4.3:** Consider any scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds for some $c > 0$. We have

$$
\frac{K_{1,n} K_{r,n}}{P_n} = \Theta \left( \frac{\log n}{n} \right).
$$

(25)

If in addition (12) holds, we have

$$
p_{rr}(n) \sim \frac{K_{r,n}^2}{P_n} = o \left( \frac{(\log n)^2}{n} \right).
$$

(26)

**Proof.** The scaling condition (9) states that

$$
\lambda_1(n) = \sum_{j=1}^{r} \mu_j p_{1j}(n) = c_n \log n / n
$$

with $\lim_{n \to \infty} c_n = c > 0$. From the proof of Proposition (4.1) we know that $p_{ij}(n)$ increases with $i$ and $j$ under any scaling. Thus, we readily obtain that

$$
c_n \log n / n \leq p_{1r}(n) \leq c_n \log n / n .
$$

(27)

Since $\mu_r > 0$ this gives $p_{1r}(n) = \Theta \left( \frac{\log n}{n} \right) = o(1)$, whence we get $\frac{K_{1,n} K_{r,n}}{P_n} \sim p_{1r}(n)$ from Lemma 4.2 and (25) is readily established. We also find it useful to state the more detailed bounds

$$
\frac{c_n \log n / n}{2} \leq \frac{K_{1,n} K_{r,n}}{P_n} \leq \frac{2c_n \log n / n}{\mu_r} .
$$

(28)

This easily seen to be valid for any $n = 2, 3, \ldots$ sufficiently large in view of (27).

We now turn to establishing (26). Comparing (25) with (12), we get

$$
\frac{K_{r,n}}{K_{1,n}} = \frac{K_{1,n} K_{r,n}}{P_n} = \Theta \left( \frac{\log n}{\omega(1)} \right) = o(\log n).
$$

(29)

Next, we multiply (25) with (29) to get

$$
\frac{K_{2,n}}{P_n} = o \left( \frac{(\log n)^2}{n} \right) = o(1).
$$

Invoking Lemma 4.2 with $i = j = r$, we obtain (26).

The following inequality will also be useful in our proof.

**Proposition 4.4:** For any set of positive integers $K_1, \ldots, K_r, P$, and any scalar $a \geq 1$, we have

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

(30)

**Proof.** Fix $i, j = 1, 2, \ldots , r$. Observe that $(\frac{P-K_i}{K_i}) / (\frac{P}{K_i}) \geq 0$ so that (30) holds trivially if $K_j + [aK_i] > P$. Assume here onwards that $K_j + [aK_i] \leq P$. Recalling (24), we find

$$
\frac{P-aK_i}{P} = \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{[aK_i]}{P - \ell} \right) \leq \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{aK_i}{P - \ell} \right) .
$$

(31)

and

$$
\frac{P-aK_i}{P} = \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{K_i}{P - \ell} \right) .
$$

(32)

In view of (31) and (32), the desired inequality (30) will follow if we show that

$$
1 - \frac{aK_i}{P - \ell} \leq \left( 1 - \frac{K_i}{P - \ell} \right)^a , \quad \ell = 0, 1, \ldots , K_j - 1 .
$$

(33)

For each $\ell = 0, 1, \ldots , K_j - 1$, (33) follows as we note that

$$
1 - \frac{K_i}{P - \ell} = \int_0^{1 - \frac{K_i}{P - \ell}} x^{a-1} dx \leq \frac{aK_i}{P - \ell}
$$

and (30) is now established.

In the course of proving Theorem 3.1 we often make use of the decomposition

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

(34)

with $\Psi(x) := \int_0^x \frac{t}{1-t} dt$, and repeatedly use the fact that

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

(35)

Finally, we find it useful to derive a bound on $p_{ij}$. Starting with (24) we write

$$
\frac{(P-K_i)}{K_i} \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{K_j}{P - \ell} \right) \leq \prod_{\ell=0}^{K_i-1} \left( 1 - \frac{K_j}{P} \right) \leq e^{-\frac{K_j}{P}} .
$$

(36)
V. A Proof of Theorem 3.1 – Establishing the Zero-One Law for Absence of Isolated Nodes

The proof of Theorem 3.1 passes through applying the method of first and second moments [13, p. 55] to the number of isolated nodes in $\mathbb{G}(n; \mu, K, P)$. To simplify the notation, let $\theta = (K, P)$. Let $I_n(\mu, \theta)$ denote the total number of isolated nodes in $\mathbb{G}(n; \mu, \theta)$; i.e.,

$$I_n(\mu, \theta) = \sum_{i=1}^{n} 1_{\{v_i \text{ is isolated in } \mathbb{G}(n; \mu, \theta)\}}. \tag{37}$$

A. Establishing the one-law

Consider now a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds with $c > 1$. The random graph $\mathbb{G}(n; \mu, \theta_n)$ has no isolated nodes if and only if $I_n(\mu, \theta_n) = 0$. The method of first moment [13, Eqn. (3.10), p. 55] gives

$$1 - \mathbb{E} [I_n(\mu, \theta_n)] \leq \mathbb{P} [I_n(\mu, \theta_n) = 0], \tag{38}$$

whence the one-law $\lim_{n \to \infty} \mathbb{P} [I_n(\mu, \theta_n) = 0] = 1$ will follow if we show that

$$\lim_{n \to \infty} \mathbb{E} [I_n(\mu, \theta_n)] = 0. \tag{39}$$

By exchangeability of the indicator functions appearing at (37), we find

$$\mathbb{E} [I_n(\mu, \theta_n)] = n \mathbb{P} [v_1 \text{ is isolated in } \mathbb{G}(n; \mu, \theta_n)]. \tag{40}$$

Conditioning on the class of $v_1$, we further get

$$n \mathbb{P} [v_1 \text{ is isolated in } \mathbb{G}(n; \mu, \theta_n)] = n \sum_{i=1}^{r} \mu_i \mathbb{P} [v_1 \text{ is isolated } | v_1 \text{ is class } i]$$

$$= n \sum_{i=1}^{r} \mu_i \mathbb{P} [\cap_{j=2}^{n} v_j \neq v_1] | v_1 \text{ is class } i]$$

$$= n \sum_{i=1}^{r} \mu_i (\mathbb{P} [v_1 \neq v_2 | v_1 \text{ is class } i])^{n-1} \tag{41}$$

where (41) follows from the fact that rvs $\{v_1 \neq v_j\}_{j=2}^{n}$ are conditionally independent given the key ring $\Sigma_1$ of node $v_1$. Conditioning further on the class of $v_2$, we find

$$\mathbb{P} [v_1 \neq v_2 | v_1 \text{ is class } i]$$

$$= \sum_{j=1}^{r} \mu_j \mathbb{P} [v_1 \neq v_2 | v_1 \text{ is class } i, v_2 \text{ is class } j]$$

$$= \sum_{j=1}^{r} \mu_j (1 - p_{ij}(n))$$

$$= 1 - \lambda_i(n). \tag{42}$$

Using (42) in (41), and recalling (23) we get

$$n \mathbb{P} [v_1 \text{ is isolated in } \mathbb{G}(n; \mu, \theta_n)]$$

$$= n \sum_{i=1}^{r} \mu_i (1 - \lambda_i(n))^{n-1}$$

$$\leq n (1 - \lambda_1(n))^{n-1}$$

$$\leq e^{\log n - c_{\alpha} \log n^{-1/\alpha}} \tag{43}$$

as we also use (9). Letting $n$ go to infinity in this last expression we immediately get

$$\lim_{n \to \infty} n \mathbb{P} [v_1 \text{ is isolated in } \mathbb{G}(n; \mu, \theta_n)] = 0$$

since $\lim_{n \to \infty} 1 - c_n n^{-1} = 1 - c < 0$ under the enforced assumptions. Invoking (40) we now get (39) and the one-law is established.

B. Establishing the zero-law

This section is devoted to establishing the zero-law in Theorem 3.1, namely the fact that inhomogeneous random key graph contains at least one isolated node when the scaling condition (7) is satisfied with $c < 1$. We will establish this by applying the method of second moment [13, Remark 3.1, p. 55] to a variable that counts nodes that are class-1 and isolated. Clearly, if we show that what there exists at least one class-1 node that is isolated, then the desired zero-law will follow.

Let $Y_n(\mu, \theta)$ denote the number of isolated nodes in $\mathbb{G}(n; \mu, \theta_n)$ that are class-1. Namely, with $\chi_{n,i}(\mu, \theta)$ denoting the indicator function that node $v_i$ is isolated and belongs to class-1, we have $Y_n(\mu, \theta) = \sum_{i=1}^{n} \chi_{n,i}(\mu, \theta)$. The second moment method states the inequality

$$\mathbb{P} [Y_n(\mu, \theta) = 0] \leq 1 - \frac{\mathbb{E} [Y_n(\mu, \theta)]^2}{\mathbb{E} [Y_n(\mu, \theta)^2]} \tag{44}.$$
\textbf{Proposition 5.1:} Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (9) holds with $\lim_{n \to \infty} c_n = c > 0$. Then, we have
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta)] = (1 + o(1))\mu_1n^{1-c_n} \tag{50}
\end{equation}
so that
\begin{equation}
\lim_{n \to \infty} n\mathbb{E}[\chi_{n,1}(\mu, \theta)] = \infty \quad \text{if} \quad c < 1. \tag{51}
\end{equation}

\textbf{Proposition 5.2:} Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (9) holds with $\lim_{n \to \infty} c_n = c > 0$. Then, we have (49).

A Proof of Proposition 5.1 is given in Section VI-A, while Proposition 5.2 is established in Section VI-B.

\section{VI. PROOFS OF PROPNS. 5.1 AND 5.2}
\subsection{A. A proof of Proposition 5.1}
Fix $n = 2, 3, \ldots$, and pick $u$ and $\theta$. We have
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta)] = n\mathbb{P}[v_1 \text{ is isolated and class-1}] = n\mu_1\mathbb{P}[v_1 \text{ is isolated | } v_1 \text{ is class-1}] = n\mu_1\mathbb{P}[v_1 \sim v_j | v_1 \text{ is class-1}] = n\mu_1(1 - \lambda_1)^{n-1} \tag{52}
\end{equation}
by virtue of the fact that the events $\{v_1 \sim v_j \text{ and } v_1 \text{ is class-1}\}$ are independent conditionally on $\Sigma_1$. Invoking (42), we then get
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta)] = n\mu_1(1 - \lambda_1)^{n-1}. \tag{53}
\end{equation}

Now, consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (9) holds with $\lim_{n \to \infty} c_n = c > 0$. Using this scaling in (53) and recalling (34) we get
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta, \theta)] = n\mu_1(1 - c_n \log n/n) n^{-1} = n\mu_1 e^{-c_n \log n/n} (n-1)(\log n/n)^2 \tag{54}
\end{equation}
The desired result (50) is now immediate as we recall (35) and note that $\lim_{n \to \infty} c_n \log n/n = 0$,
\begin{equation}
\lim_{n \to \infty} \left( \frac{\psi((c_n \log n/n)^2)}{(c_n \log n/n)^2} \right) = 1/2 \quad \text{and} \quad \lim_{n \to \infty} (n-1)(\log n/n)^2 = 0
\end{equation}
in view of $\lim_{n \to \infty} c_n = c > 0$. From (50), we readily get (51) upon noting that $\mu_1 > 0$.

\subsection{B. A proof of Proposition 5.2}
We start by obtaining an expression for the probability that nodes $v_1$ and $v_2$ are class-1 and isolated in $G(n; \mu, \theta)$. We get
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta)\chi_{n,2}(\mu, \theta)] = \mu_1^2\mathbb{P}[v_1 \text{ and } v_2 \text{ are isolated | } v_1 \text{ and } v_2 \text{ are class-1}]
\end{equation}

\textbf{Combining (55) and (56), we find}
\begin{equation}
\mathbb{E}[\chi_{n,1}(\mu, \theta)] = \mu_1 \left( \sum_{j=1}^r \mu_j \frac{\left(P_{K_j} - K_j\right)}{K_j} \right)^{n-1}. \tag{56}
\end{equation}

Consider a scaling $\theta : \mathbb{N}_0 \to \mathbb{N}^{r+1}$ such that (7) holds with $c < 1$. Reporting this scaling into the last expression, we see that
\begin{equation}
\sum_{j=1}^r \mu_j \left(\frac{P_{K_j} - K_j}{K_j}\right) = (1 - \lambda_1(1/n))^{-2} = \left(1 - \frac{c_n \log n/n}{n}\right)^{-2} = 1 + o(1). \tag{58}
\end{equation}

With $p_{ij}(n)$ increasing with $i$ and $j$ as shown in Proposition 4.1, it is also clear that
\begin{equation}
1 \geq \frac{P_{K_{j,n}}}{P_{K_{j,n}}} = 1 - \frac{p_{ij}(n) \geq 1 - \lambda_1(1/n) = 1 - \frac{c_n \log n/n}{n},
\end{equation}
leading to
\begin{equation}
\frac{P_{K_{j,n}}}{P_{K_{j,n}}} = 1 - o(1). \tag{59}
\end{equation}

Finally, we note from Proposition 4.4 that
\begin{equation}
\left(\frac{P_{K_{j,n}} - K_{j,n}}{P_{K_{j,n}}}ight)^2 \leq \left(\frac{P_{K_{j,n}} - K_{j,n}}{P_{K_{j,n}}}ight)^2, \quad j = 1, \ldots, r. \tag{60}
\end{equation}

Let $Z_n(\mu, \theta) = \frac{P_{K_{j,n}}}{K_{j,n}}$ denote a rv such that
\begin{equation}
Z_n(\mu, \theta) = \frac{P_{K_{j,n}}}{K_{j,n}} \quad \text{with probability } \mu_j, \quad j = 1, \ldots, r.
\end{equation}
Applying (58), (59), and (60) in (57) we see that the desired result (49) will follow upon showing

\[
\limsup_{n \to \infty} \left( \frac{\mathbb{E}[Z_n(\mu, \theta)]^2}{\mathbb{E}[Z_n(\mu, \theta)]} \right)^{n-2} \leq 1. \tag{61}
\]

We note that

\[
\left( \frac{\mathbb{E}[Z_n(\mu, \theta)]^2}{\mathbb{E}[Z_n(\mu, \theta)]} \right)^{n-2} = \left( 1 + \frac{\text{var}[Z_n(\mu, \theta)]}{\mathbb{E}[Z_n(\mu, \theta)]} \right)^{n-2}
\]

\[
\leq e^{\frac{\text{var}[Z_n(\mu, \theta)]}{\mathbb{E}[Z_n(\mu, \theta)]}}(n-2)
\]

and that

\[
\mathbb{E}[Z_n(\mu, \theta)] = 1 - \lambda_1(n) = 1 - o(1).
\]

Hence, we will obtain (61) if we show that

\[
\lim_{n \to \infty} n \cdot \text{var}[Z_n(\mu, \theta)] = 0. \tag{63}
\]

In order to bound the variance of \(Z_n(\mu, \theta)\), we use Popoviciu’s inequality [14, p. 9]. Namely, for any bounded rv \(X\) with maximum value of \(M\) and minimum value of \(m\), we have

\[
\text{var}[X] \leq \frac{1}{4}(M - m)^2.
\]

It is clear from the discussion given in the proof of Proposition 4.1 that

\[
\frac{(P_n - K_{1,n})}{(P_n - K_{r,n})} \leq Z_n(\mu, \theta) \leq \frac{(P_n - K_{1,n})}{(P_n - K_{r,n})}
\]

holds for any scaling. Applying Popoviciu’s inequality, we then get

\[
\text{var}[Z_n(\mu, \theta)] \leq \frac{1}{4} \left( \frac{(P_n - K_{1,n})}{(P_n - K_{r,n})} + \frac{(P_n - K_{1,n})}{(P_n - K_{r,n})} \right)^2 \leq \frac{1}{4} \left( 1 - \frac{(P_n - K_{1,n})}{(P_n - K_{r,n})} \right)^2 = \frac{1}{4} (P_{nr}(n))^2. \tag{64}
\]

Reporting the upper bound in (27) into (64) we now find

\[
n \cdot \text{var}[Z_n(\mu, \theta)] \leq \frac{n}{4} \left( \frac{c n \log n}{\mu r} \right)^2. \tag{65}
\]

Letting \(n\) go to infinity in this last expression, we immediately get (63) as we note that \(\mu r > 0\) and \(\lim_{n \to \infty} c n = c > 0\). This establishes (61) and the desired result (49) now follows.

VII. A PROOF OF THEOREM 3.2 – ESTABLISHING THE ZERO-ONE LAW FOR CONNECTIVITY

The proof of Theorem 3.2 is technically more involved than that of Theorem 3.1. To that end, we outline the main arguments leading to the proof in this section and complete the remaining steps in several sections that follow.

Fix \(n = 2, 3, \ldots\) and consider \(u\) and \(\theta = (K, P)\). We define the event

\[
C_n(u, \theta) := \{G(n; \mu, \theta) \text{ is connected}\}\]

and recall that

\[
[I_n(u, \theta) = 0] = \mathbb{G}(n; \mu, \theta) \text{ contains no isolated nodes}. \]

If the random graph \(G(n; \mu, \theta)\) is connected, then it does not contain any isolated node, whence \(C_n(\mu, \theta)\) is a subset of \([I_n(u, \theta) = 0]\), and the conclusions

\[
\mathbb{P}[C_n(\mu, \theta)] \leq \mathbb{P}[I_n(u, \theta) = 0] \tag{66}
\]

and

\[
\mathbb{P}[C_n(\mu, \theta)^c] = \mathbb{P}[C_n(\mu, \theta)^c \cap (I_n(u, \theta) = 0)] + \mathbb{P}[(I_n(u, \theta) = 0)^c] = 0 \tag{67}
\]

follow. Taken together with Theorem 3.1, the relations (66) and (67) pave the way to proving Theorem 3.2. To see this, pick any scaling \(K_1, \ldots, K_r, P : N_0 \to N_0^{r+1}\) such that (7) holds for some \(c > 0\). If \(c < 1\), then \(\lim_{n \to \infty} \mathbb{P}[I_n(u, \theta_n) = 0] = 0\) by the zero-law for the absence of isolated nodes (see Theorem 3.1), whence \(\lim_{n \to \infty} \mathbb{P}[C_n(\mu, \theta_n)] = 0\) with the help of (66). If \(c > 1\), then \(\lim_{n \to \infty} \mathbb{P}[I_n(u, \theta_n) = 0] = 1\) by the one-law for the absence of isolated nodes, and the desired conclusion \(\lim_{n \to \infty} \mathbb{P}[C_n(\mu, \theta_n)^c] = 1\) (equivalently, \(\lim_{n \to \infty} \mathbb{P}[C_n(\mu, \theta_n)^c] = 0\) will follow via (67) if we show the following:

**Proposition 7.1**: For any scaling \(K_1, \ldots, K_r, P : N_0 \to N_0^{r+1}\) such that (7) holds for some \(c > 1\), we have

\[
\lim_{n \to \infty} \mathbb{P}[C_n(\mu, \theta)^c \cap (I_n(u, \theta_n) = 0)] = 0. \tag{68}
\]

as long as the conditions (11) and (12) are satisfied.

In words, Proposition 7.1 states that the probability of the inhomogeneous random key graph being not connected despite having no isolated nodes diminishes asymptotically under the enforced assumptions. In fact, the asymptotic equivalence of graph connectivity and absence of isolated nodes is a well-known phenomenon in many classes of random graphs; e.g., ER graphs [2], random key graphs [31], and intersection of random key graphs and ER graphs [26].

The basic idea in establishing Proposition 7.1 is to find a sufficiently tight upper bound on the probability in (68) and then to show that this bound goes to zero as \(n\) becomes large. Our approach is in the same vein with the one used for proving the one-law for connectivity in ER graphs [2, p. 164]. This approach has already proved useful in establishing one-laws for connectivity in the standard random key graph [31] and its intersection with an ER graph [26]. Throughout the proof of the one-law for connectivity in inhomogeneous random key graphs, several intermediate results will be borrowed directly from [31], [26] to avoid duplication.

We begin by deriving the needed upper bound on the term (68). Fix \(n = 2, 3, \ldots\) and consider \(u\) and \(\theta = (K, P)\). For reasons that will later become apparent we will need bounds on the number of distinct keys held by a specific set \(S\) of sensors; just to give a hint, this will help us efficiently bound the probability that the sensors in \(S\) are isolated from the rest of the network. To that end, we define the event \(E_n(\mu, \theta; X)\) via

\[
E_n(\mu, \theta; X) = \bigcup_{S \subseteq N: |S| \geq 1} \{\bigcup_{i \in S} \Sigma_i \leq X_{|S|}\} \tag{69}
\]
where \( \mathcal{N} = \{1, \ldots, n\} \) and \( X = [X_1, X_2, \ldots, X_n] \) is an \( n \)-dimensional integer-valued array.

Let

\[
L_n := \min \left( \frac{P}{K_1}, \left\lfloor \frac{n}{2} \right\rfloor \right)
\]

and set

\[
X_\ell = \begin{cases} 
\left\lfloor \beta \ell K_1 \right\rfloor & \ell = 1, 2, \ldots, L_n \ \\
\left\lfloor \gamma P \right\rfloor & \ell = L_n + 1, \ldots, n
\end{cases}
\]  

(70)

for some \( \beta, \gamma \in (0, \frac{1}{2}) \) that will be specified later. With this setting, \( E_n(\mu, \theta; X) \) encodes the event that for at least one \( \ell = 1, 2, \ldots, n \), the total number of distinct keys held by at least one set of \( \ell \) sensors is less than \( \beta \ell K_1 \left[ \ell \leq L_n \right] + \gamma P \left[ \ell > L_n \right] \). Below, we will show that by a careful selection of \( \beta \) and \( \gamma \), we can have the complement of \( E_n(\mu, \theta; X) \) take place whp under the enforced assumptions on the scaling \( \theta : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \); i.e., for all \( \ell = 1, 2, \ldots, n \), the total number of keys held by any set of \( \ell \) sensors will be at least \( \beta \ell K_1 \left[ \ell \leq L_n \right] + \gamma P \left[ \ell > L_n \right] \). The relevance of this is easily seen as we use a simple bounding argument to write

\[
\mathbb{P} \left[ C_n(\mu, \theta)^c \cap (I_n(u, \theta) = 0) \right] 
\leq \mathbb{P} \left[ E_n(\mu, \theta; X) \right] 
+ \mathbb{P} \left[ C_n(\mu, \theta)^c \cap (I_n(u, \theta) = 0) \cap E_n(\mu, \theta; X)^c \right].
\]

It is now clear that the proof of Proposition 7.1 and hence that of Theorem 3.2 will consist of establishing the following two results.

**Proposition 7.2:** Consider a scaling \( K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \) such that (7) holds for some \( c > 1 \), (11) is satisfied for some \( \sigma > 0 \), and (12) hold. We have

\[
\lim_{n \to \infty} \mathbb{P} \left[ E_n(\mu, \theta_n; X_n) \right] = 0.
\]  

(71)

where \( X_n = [X_{1,n}, \ldots, X_{n,n}] \) is as specified in (70) with \( \beta \) in \( (0, \frac{1}{2}) \) is selected small enough to ensure

\[
\max \left( 2 \beta \sigma, \beta \left( \frac{c^2}{\sigma} \right)^{\frac{\beta}{\beta + \sigma}} \right) < 1,
\]

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

\[
\max \left( 2 \sqrt{\gamma} \left( \frac{c}{\gamma} \right)^{\gamma}, \sqrt[\gamma]{\frac{c}{\gamma}}^{\gamma} \right) < 1.
\]  

(73)

A proof of Proposition 7.2 can be found in Section VIII. Note that for any \( \sigma > 0 \), \( \lim_{\beta \to 0} \beta \left( \frac{c^2}{\sigma} \right)^{\frac{\beta}{\beta + \sigma}} = 0 \) so that the condition (72) can always be met by suitably selecting \( \beta > 0 \) small enough. Also, we have \( \lim_{\gamma \to 0} \sqrt[\gamma]{\frac{c}{\gamma}}^{\gamma} = 1 \), whence \( \lim_{\gamma \to 0} \sqrt{\gamma} \left( \frac{c}{\gamma} \right)^{\gamma} = 0 \), and (73) can be made to hold for any \( \sigma > 0 \) by taking \( \gamma > 0 \) sufficiently small.

**Proposition 7.3:** Consider a scaling \( K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \) such that (7) holds for some \( c > 1 \), (11) is satisfied for some \( \sigma > 0 \), and (12) hold. We have

\[
\lim_{n \to \infty} \mathbb{P} \left[ C_n(\mu, \theta_n)^c \cap (I_n(u, \theta_n) = 0) \cap E_n(\mu, \theta_n; X_n)^c \right] = 0.
\]  

(74)

where \( X_n = [X_{1,n}, \ldots, X_{n,n}] \) is as specified in (70) with \( \gamma \) in \( (0, \frac{1}{2}) \) is selected small enough to ensure (73) and \( \beta \in (0, \frac{1}{2}) \) is selected such that (72) is satisfied.

The proof of Proposition 7.3 is outlined in Section IX with several steps completed in the sections that follow.

**VIII. A PROOF OF PROPOSITION 7.2**

The proof of Proposition 7.2 will follow similar steps to [26, Proposition 7.2] and rely heavily on the results obtained by the author in [25]. Using a standard union bound we first write

\[
\mathbb{P} \left[ E_n(\mu, \theta; X) \right] \leq \sum_{S \subseteq \mathcal{N} \leq |S| \leq n} \mathbb{P} \left[ \cup_{i \in S} \Sigma_i \leq X_{|S|} \right]
\]

\[
= \sum_{\ell=1}^{n} \left( \sum_{S \subseteq \mathcal{N}_n, |S| = \ell} \mathbb{P} \left[ \cup_{i \in S} \Sigma_i \leq X_{\ell} \right] \right)
\]  

(75)

where \( \mathcal{N}_n, \ell \) denotes the collection of all subsets of \( \{1, \ldots, n\} \) with exactly \( \ell \) elements. Let \( U_{\ell}(\mu, \theta) \) be given by

\[
U_{\ell}(\mu, \theta) = \cup_{i=1}^{\ell} \Sigma_i, \quad \ell = 1, 2, \ldots, n.
\]

By using exchangeability and the fact that \( |\mathcal{N}_n, \ell| = \binom{n}{\ell} \), we get

\[
\mathbb{P} \left[ E_n(\mu, \theta; X) \right] \leq \sum_{\ell=1}^{n} \binom{n}{\ell} \mathbb{P} \left[ U_{\ell}(\mu, \theta) \leq X_{\ell} \right]
\]

\[
= \sum_{\ell=1}^{n} \binom{n}{\ell} \mathbb{P} \left[ U_{\ell}(\mu, \theta) \leq \beta \ell K_1 \right]
\]

\[
+ \sum_{\ell=L_n+1}^{n} \binom{n}{\ell} \mathbb{P} \left[ U_{\ell}(\mu, \theta) \leq \gamma P \right].
\]  

(76)

Now, consider any scaling \( K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \) and recall the ordering (6) of the key ring sizes. For all \( \ell = 1, 2, \ldots, n \) define \( U_\ell(K_{1,n}, P_n) \) as

\[
U_\ell(K_{1,n}, P_n) = \min \left\{ 1, 0, 0, \ldots, 0 \right\}, \theta_n).
\]

In other words, \( U_\ell(K_{1,n}, P_n) \) stands for the rv that has the same distribution with \( U_\ell(\mu, \theta_n) \) when \( \mu \) is degenerate with \( \mu_1 = 1 \) and \( \mu_j = 0 \) for all \( j = 2, \ldots, r \); i.e., when all key ring sizes are equal to \( K_1 \). With this setting, \( U_\ell(K_{1,n}, P_n) \) is equivalent to the rv defined similarly for the standard random key graph in [31], [26], [25], where it was often denoted by \( U_{\ell}(\theta_n) = (K_n, P_n) \). Given (6), it is a simple matter to check that

\[
U_\ell(K_{1,n}, P_n) \leq U_\ell(\mu, \theta_n), \quad \mu = (\mu_1, \ldots, \mu_r)
\]

with \( \leq \) denoting the usual stochastic ordering; i.e., \( A \preceq B \) if \( \mathbb{P} \left[ A > x \right] \leq \mathbb{P} \left[ B > x \right] \) for all \( x \in (-\infty, \infty) \). This can be seen by an easy coupling argument where all sensors first receive \( K_{1,n} \) keys and then an additional \( K_{\ell,n} = K_{1,n} \) keys are assigned to each sensor independently with probability \( \mu_\ell \). Since additionally distributed keys can only increase the variable \( U_{\ell} \), we obtain (77).

Reporting (77) into (76) we now get

\[
\mathbb{P} \left[ E_n(\mu, \theta_n; X_n) \right] \leq \sum_{\ell=1}^{L_n} \binom{n}{\ell} \mathbb{P} \left[ U_{\ell}(K_{1,n}, P_n) \leq \beta \ell K_1 \right]
\]
It is also clear that this union need only be taken over all subsets $S$ of $\{v_1, \ldots, v_n\}$ with $2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor$.

We now apply a standard union bound argument to (81) and get
\[
\Pr[C_n(\mu, \theta)^c \cap (I_n(u, \theta) = 0) \cap E_n(\mu, \theta; X)^c] \\
\leq \sum_{S \subseteq V: 2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} \Pr[A_{n, \ell}(\mu, \theta; S) \cap E_n(\mu, \theta; X)^c] \\
= \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \left( \sum_{S \subseteq V, \ell} \Pr[A_{n, \ell}(\mu, \theta; S) \cap E_n(\mu, \theta; X)^c] \right)^{\ell-1} \tag{82}
\]

where $V_{n, \ell}$ denotes the collection of all subsets of $\{v_1, \ldots, v_n\}$ with exactly $\ell$ elements.

For each $\ell = 1, \ldots, n$, we simplify the notation by writing $A_{n, \ell}(\mu, \theta) := A_{n, \ell}(\mu, \theta; \{v_1, \ldots, v_\ell\})$, $B_{n, \ell}(\mu, \theta) := B_{n, \ell}(\mu, \theta; \{v_1, \ldots, v_\ell\})$, and $C_{n, \ell}(\mu, \theta) := C_{n, \ell}(\mu, \theta; \{v_1, \ldots, v_\ell\})$. With a slight abuse of notation, we use $C_{n, \ell}(\mu, \theta)$ for $\ell = n$ as defined before. Under the enforced assumptions, exchangeability yields
\[
\Pr[A_n(\mu, \theta; S)] = \Pr[A_{n, \ell}(\mu, \theta)], \; S \in V_{n, \ell}
\]
and the expression
\[
\sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \Pr[A_{n, \ell}(\mu, \theta) \cap E_n(\mu, \theta; X)^c] \\
= \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \left( \Pr[A_{n, \ell}(\mu, \theta) \cap E_n(\mu, \theta; X)^c] \right)^{\ell-1} \tag{83}
\]
follows since $|V_{n, \ell}| = \binom{n}{\ell}$. Substituting into (82) we obtain the key bound
\[
\Pr[C_n(\mu, \theta)^c \cap (I_n(u, \theta) = 0) \cap E_n(\mu, \theta; X)^c] \\
\leq \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \left( \Pr[A_{n, \ell}(\mu, \theta) \cap E_n(\mu, \theta; X)^c] \right)^{\ell-1} \tag{84}
\]

Next, we derive bounds for the probabilities appearing at (84). Recall the definitions (2) and (3).

**Proposition 9.1**: Consider $\theta = (K, P)$ and $\mu = (\mu_1, \ldots, \mu_r)$ such that $K_1 \leq K_2 \leq \cdots \leq K_r$. We have
\[
\Pr[A_{n, \ell}(\mu, \theta) \cap E_n(\mu, \theta; X)^c] \\
\leq \min\left\{1, \ell^{t-2}(prr)^{\ell-1}\left(\min\left\{1 - \lambda_1, \mathbb{E}\left[e^{-(X_{j+1}+|\Sigma|)/\rho}\right]\right]\right)^{n-\ell}\right\} \tag{85}
\]
where $|\Sigma|$ denotes a rv such that $|\Sigma| = K_j$ with probability $\mu_j$, $j = 1, \ldots, r$.

**Proof.** We start by observing the equivalence
\[
B_{n, \ell}(\mu, \theta) = \left(\bigcup_{j=1}^{\ell} \Sigma_j\right) \cap \Sigma_j = \emptyset, \; j = \ell + 1, \ldots, n.
\]

Hence, under the enforced assumptions on the rvs $\Sigma_1, \ldots, \Sigma_n$, we readily obtain the expression
\[
\Pr\left[B_{n, \ell}(\mu, \theta) \mid \Sigma_1, \ldots, \Sigma_{\ell}\right] = \prod_{j=\ell+1}^{n} \mathbb{E}\left[\frac{\left(\rho^{-|\Sigma_j|}\right)^{\ell-1}}{\left(|\Sigma_j|\right)^{\ell}}\right] \\
= \mathbb{E}\left[\left(\rho^{-|\Sigma_j|}\right)^{\ell-1}\right]^{n-\ell} \tag{86}
\]
where \(|\Sigma|\) denotes a rv that takes the value \(K_j\) with probability \(\mu_j\) for each \(j = 1, \ldots, r\). Note that we always have \(|\cup_{i=1}^{\ell} \Sigma_i| \geq K_1\), while it holds that \(|\cup_{i=1}^{\ell} \Sigma_i| \geq X_1 + 1\) on the event \(E_n(\mu, \theta; X)^c\). Combining, we get
\[
P \left[ B_{n, \ell}(\mu, \theta) \cap E(\mu, \theta; X)^c \right| \Sigma_1, \ldots, \Sigma_\ell \right] \\
\leq \left( \min \left\{ \frac{\left(\frac{P(K_1)}{|\Sigma|}\right)}{\left(\frac{P-1}{|\Sigma|}\right)} \right\} \right)^{-\ell} \\
\leq \left( \min \left\{ 1 - \lambda_1, \mathbb{E} \left[ e^{-\frac{X_1+1}{n}} \right] \right\} \right)^{n-\ell},
\] (87)
where in the last step we also used (36).

Conditioning on the rvs \(\Sigma_1, \ldots, \Sigma_\ell\) which fully determine the event \(C_{n, \ell}(\mu, \theta)\), we conclude via (87) that
\[
P \left[ A_{n, \ell}(\mu, \theta) \cap E(\mu, \theta; X)^c \right] \\
= \mathbb{E} \left[ 1 \left| C_{n, \ell}(\mu, \theta) \right| \right] \\
\cdot \mathbb{P} \left[ B_{n, \ell}(\mu, \theta) \cap E(\mu, \theta; X)^c \right| \Sigma_1, \ldots, \Sigma_\ell \right] \\
\leq \mathbb{P} \left[ C_{n, \ell}(\mu, \theta) \right] \left( \min \left\{ 1 - \lambda_1, \mathbb{E} \left[ e^{-\frac{X_1+1}{n}} \right] \right\} \right)^{n-\ell}.
\]

In view of this last bound, Proposition 9.1 will be established if we show that
\[
P \left[ C_{n, \ell}(\mu, \theta) \right] \leq (p_{rr})^{\ell-1}. \tag{88}
\]

To see why (88) holds, observe that the subgraph of \(G(n; \mu, \theta)\) on the vertices \(v_1, \ldots, v_r\), hereafter denoted \(G_r(\mu, \theta)\), is connected if and only if it contains a spanning tree. Let \(T_\ell\) denote the collection of all spanning trees on the vertex set \(\{v_1, \ldots, v_r\}\). Then, we have
\[
C_{n, \ell}(\mu, \theta) = \cup_{T \in T_\ell} [T \subseteq G(n; \mu, \theta)]
\]
By Cayley’s formula [17] there are \(\ell^{\ell-2}\) trees on \(\ell\) vertices, i.e., \(|T_\ell| = \ell^{\ell-2}\). In addition, for any \(T\) in \(T_\ell\), it is clear that
\[
P \left[ T \subseteq G(n; \mu, \theta) \right] \leq \mathbb{P} \left[ T \subseteq G_r(n; \{0, \ldots, 0, 1\}, \theta) \right]
\]
since \(K_r \geq K_j\) for any \(j = 1, 2, \ldots, r-1\); i.e., probability that the tree \(T\) is contained in this subgraph is maximized when all the nodes in the subgraph belong to class-\(r\) that are assigned the largest number of keys. With \(\mu_r = 1\), \(G_r(\mu, \theta)\) becomes equivalent to the standard random key graph \(G_{\ell}(n; K_r, P)\) for which it is known [31, Lemma 9.1] that
\[
P \left[ T \subseteq G_r(n; \mu, \theta) \right] = (p_{rr})^{\ell-1}, \quad T \in T_\ell, \quad \ell = 2, 3, \ldots
\]
This follows from the fact that a tree on \(\ell\) nodes consists of \(\ell-1\) edges and that edge events in the random key graph are pairwise independent. Collecting, we obtain via a union bound that
\[
P \left[ C_{n, \ell}(\mu, \theta) \right] \leq \sum_{T \in T_\ell} \mathbb{P} \left[ T \subseteq G_r(n; \mu, \theta) \right] \\
\leq \sum_{T \in T_\ell} \mathbb{P} \left[ T \subseteq G_r(n; \{0, \ldots, 0, 1\}, \theta) \right] \\
\leq (p_{rr})^{\ell-1}. \tag{89}
\]
This establishes (88) and the proof of Proposition 9.1 is now completed.

Now, consider a scaling \(\theta : \mathbb{N}_0 \to \mathbb{N}_{r+1}\) as in the statement of Proposition 7.3. Using this scaling in (84) together with (85) we see that the proof of Proposition 7.3 will be completed once we show
\[
\lim_{n \to \infty} \sum_{\ell \geq 2} \frac{n}{\ell} f_{n, \ell}(\mu, \theta) = 0 \tag{90}
\]
where for convenience we define
\[
f_{n, \ell}(\mu, \theta) := \min \left\{ \frac{1}{\ell} \left( (p_{rr})^{\ell-1} \right) \right\} \cdot \left( \min \left\{ 1 - \lambda_1, \mathbb{E} \left[ e^{-\frac{(X_1+1)}{n}} \right] \right\} \right)^{n-\ell} \tag{91}
\]
Combined with Proposition 7.2, this will lead to Proposition 7.1 and hence to Theorem 3.2. To that end, we devote the rest of the paper to establishing (90). Throughout, we make repeated use of the standard bounds
\[
\left( \frac{n}{\ell} \right) \leq \left( \frac{en}{\ell} \right)^\ell, \quad \ell = 1, \ldots, n \tag{92}
\]
and
\[
\sum_{\ell = 2}^{[n/2]} \left( \frac{n}{\ell} \right) \leq 2^n, \tag{93}
\]
where the latter follows from the Binomial formula.

X. Establishing (90)

We will establish (90) in several steps with each step focusing on a specific range of the summation over \(\ell\). Throughout this section, we consider a scaling \(K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_{r+1}\) such that (7) holds for some \(c > 1\), (11) holds for some \(\sigma > 0\) and (12) is satisfied. The desired result (90) follows from (95), (100), (106), (109), and (112) that are established in Sections X-A-X-E, respectively.

A. The case where \(2 \leq \ell \leq R\)

The first range considers fixed values of \(\ell\). For the moment, fix an integer \(R\) that will be specified later in Section X-B; see (101). For each \(\ell = 2, \ldots, R\) we use (92), (26), and (7) to get
\[
\left( \frac{n}{\ell} \right) f_{n, \ell}(\mu, \theta) \leq \left( \frac{en}{\ell} \right)^{\ell-1} (1 - \lambda_1(n))^{n-\ell} \\
\leq (c \ell)^{\ell-1} (p_{rr}(n))^{\ell-1} e^{-cn \log n \frac{n\ell}{\ell^2}} \\
= o(1) n^{\ell} \left( \frac{\log n}{n} \right)^{\ell-1} n^{-cn \frac{n\ell}{\ell^2}} \\
= o(1) n^{1-cn \frac{n\ell}{\ell^2}} \left( \log n \right)^{2\ell-2} \\
= o(1) \tag{94}
\]
only LaTeX
B. The case where $R + 1 \leq \ell \leq \left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil$

Next, we handle the range where $R + 1 \leq \ell \leq \left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil$. Noting that $K_{1,n} \leq K_{r,n}$, we realize from (25) that $\frac{K_{r,n}^2}{P_n} = O\left( \frac{n}{\log n} \right)$, or equivalently that $\frac{P_n}{K_{r,n}^2} = \Omega\left( \frac{\log n}{n} \right)$. Also, (11) and (12) imply together that $K_{1,n} = \omega(1)$, leading to $\frac{P_n}{K_{1,n}} = \omega\left( \frac{n}{\log n} \right)$. Hence, on the range under consideration here, we have $\ell \leq L_n = \min\left( \left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil, \left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil \right)$ so that $X_{\ell,n} = [\beta \ell K_{1,n}]$. With this in mind, we get

$$
\mathbb{E}\left[ e^{-\frac{X_{\ell,n+1}}{P_n}} \right] \leq \mathbb{E}\left[ e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}} \right] = \sum_{j=1}^{r} \mu_j e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}} \leq 1 - \mu_r + \mu_r e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}}. \tag{96}
$$

In view of (28),

$$
\beta \ell \frac{K_{1,n} K_{r,n}}{P_n} \leq \beta \ell \frac{2 \log n}{\mu_r} \leq 1.
$$

holds for all $n$ sufficiently large and $\ell \leq \frac{\mu_r n}{2 \log \log n}$. Hence, on the same range we have

$$
1 - e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}} \geq \frac{\beta \ell K_{1,n} K_{r,n}}{2 P_n}.
$$

Reporting these into (96) we get

$$
\mathbb{E}\left[ e^{-\frac{X_{\ell,n+1}}{P_n}} \right] \leq 1 - \mu_r \left( 1 - e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}} \right) \leq 1 - \mu_r \beta \ell K_{1,n} K_{r,n} \leq e^{-\frac{\mu_r \beta c}{2 \log \log n} (n-\ell)} \tag{97}
$$

for all $n$ sufficiently large, where the last inequality follows from the lower bound in (28).

Consider now the range of $n$ sufficiently large that (97) is valid. Using (97), (92), and (26), we get

$$
\sum_{\ell=R+1}^{\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil} \binom{n}{\ell} f_{n,\ell}(\mu, \theta_n) \leq \sum_{\ell=R+1}^{\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil} \left( \frac{\log n}{n} \right) \ell \left( 1 - e^{-\frac{\mu_r \beta c}{2 \log \log n} (n-\ell)} \right) \leq n \sum_{\ell=R+1}^{\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil} \left( \frac{\log n}{n} \right)^{\ell - 1} e^{-\frac{\mu_r \beta c}{2 \log \log n} \left( n - \ell \right)} \leq n \sum_{\ell=R+1}^{\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil} \left( \frac{\log n}{n} \right)^{\ell} e^{-\frac{\mu_r \beta c}{2 \log \log n} \left( n - \ell \right)} \leq n \sum_{\ell=R+1}^{\infty} \left( \frac{\log n}{n} \right)^{\ell} e^{-\frac{\mu_r \beta c}{2 \log \log n} n} \tag{98}
$$

for all $n$ sufficiently large. Since $\mu_r$, $\beta$, $c$ are all positive scalars, we have

$$
\lim_{n \to \infty} e^{\left( \frac{c}{n} \right)^{\nu n}} = 0
$$

so that the infinite series appearing at (98) is summable. In fact, we have

$$
n \sum_{\ell=R+1}^{\infty} \left( e^{\log n} \right)^{\ell} e^{-\frac{\mu_r \beta c}{2 \log \log n} \log n} \leq (1 + o(1)) n \left( e^{\log n} \right)^{2 \log \log n} R+1 = O(1) n^{1-(R+1)\frac{\mu_r \beta c}{8 \log (n)^{2 R+2}}}. \tag{99}
$$

It is now clear that we get

$$
\lim_{n \to \infty} \sum_{\ell=R+1}^{\infty} \binom{n}{\ell} f_{n,\ell}(\mu, \theta_n) = 0 \tag{100}
$$

as long as $R$ satisfies

$$
R \geq \left\lceil \frac{8}{\mu_r \beta c} \right\rceil. \tag{101}
$$

Since $\mu_r, \beta, c > 0$, such a selection is permissible given that (95) holds for any positive integer $R$.

C. The case where $\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil + 1 \leq \ell \leq \min\{L_n, \lfloor \nu n \rfloor \}$

We now consider the range where $\frac{\mu_r n}{2 \log \log n} < \ell \leq \min\{L_n, \lfloor \nu n \rfloor \}$ for some $0 < \nu < 1/2$ to be specified later; see (105). From (70), we see that $X_{\ell,n} = [\beta \ell K_{1,n}]$ so that (96) still holds. Using (96) and (28) on the given range, we get

$$
\mathbb{E}\left[ e^{-\frac{X_{\ell,n+1}}{P_n}} \right] \leq \left( 1 - \mu_r + \mu_r e^{-\frac{\beta K_{1,n} K_{r,n}}{P_n}} \right) n^{-\ell} \leq \left( 1 - \mu_r + \mu_r e^{-\frac{\mu_r n}{2 \log \log n} \frac{2 \log n}{n}} \right) n^{n/2} \leq \left( 1 - \mu_r + \mu_r e^{-\frac{\mu_r n}{2 \log \log n} \frac{2 \log n}{n}} \right) n^{n/2} \tag{102}
$$

for all $n$ sufficiently large. Also, since $\binom{n}{\ell}$ is monotone increasing in $\ell$ over the range $0 \leq \ell \leq \lfloor n/2 \rfloor$ we have

$$
\binom{n}{\ell} \leq \binom{n}{\lfloor n/2 \rfloor} \leq \left( \frac{e}{\nu} \right)^{\nu n} \tag{103}
$$

by means of (92).

Using (102) and (103) we now find

$$
\min\{L_n, \lfloor \nu n \rfloor \} \sum_{\ell=R+1}^{\left\lceil \frac{\mu_r n}{2 \log \log n} \right\rceil + 1} \binom{n}{\ell} f_{n,\ell}(\mu, \theta_n) \leq n \left( \frac{e}{\nu} \right)^{\nu n} \left( 1 - \mu_r + \mu_r e^{-\frac{\mu_r n}{2 \log \log n} \frac{2 \log n}{n}} \right) n^{n/2} = n \left( \frac{e}{\nu} \right)^{\nu n} \left( 1 - \mu_r + \mu_r e^{-\frac{\mu_r n}{2 \log \log n} \frac{2 \log n}{n}} \right) 1/2 \right)^n, \tag{104}
$$

for all $n$ sufficiently large. With $\mu_r > 0$, it always holds that

$$
\left( 1 - \mu_r + \mu_r e^{-\frac{\mu_r n}{2 \log \log n} \frac{2 \log n}{n}} \right)^{1/2} < 1,
$$

while we have

$$
\lim_{\nu \to 0} \left( \frac{e}{\nu} \right)^{\nu n} = 1.
Therefore, for any $\mu_r > 0$, $\nu$ can be selected small enough to ensure that,
\[
\left( \frac{e}{\nu} \right)^{n - \ell} \left( 1 - \mu_r + \mu_r e^{-\frac{\nu}{\ell}} \right)^{1/2} < 1.
\]  \hspace{1cm} (105)

With $\nu$ selected according to (105), we immediately obtain
\[
\lim_{n \to \infty} \sum_{\ell = \min \{L_n, \lfloor vn \rfloor \} + 1} (n \ell) f_{n, \ell}(\mu, \theta_n) = 0
\]  \hspace{1cm} (106)
in view of (104).

**D. The case where $\min \{L_n, \lfloor vn \rfloor \} + 1 \leq \ell \leq L_n$**

Our next goal is to handle the range $\min \{L_n, \lfloor vn \rfloor \} + 1 \leq \ell \leq L_n$, where it still holds that $X_{\ell,n} = \lfloor \beta \ell K_{1,n} \rfloor$. This range will become obsolete if $L_n \leq \lfloor vn \rfloor$, so we only consider the case where $\lfloor vn \rfloor < L_n$, and hence the range $\lfloor vn \rfloor + 1 \leq \ell \leq L_n$. On this range, we use the crude bound $|\Sigma|_n \geq K_{1,n}$ to get
\[
\mathbb{E} \left[ e^{-\frac{(X_{\ell,n} + 1)|\Sigma|_n}{\ell}} \right]^{n - \ell} \leq e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n} \leq e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n^2} \leq 2 e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n^2},
\]  \hspace{1cm} (107)

where we also note that $n - \ell \geq \frac{n}{2}$. Using (107) and (93) we now get
\[
\sum_{\ell = \min \{L_n, \lfloor vn \rfloor \} + 1}^{L_n} \binom{n}{\ell} f_{n, \ell}(\mu, \theta_n) \leq \left( \sum_{\ell = \min \{L_n, \lfloor vn \rfloor \} + 1}^{L_n} \binom{n}{\ell} e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n^2} \right) \leq \left( 2 e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n^2} \right)^n.
\]  \hspace{1cm} (108)

Under the enforced condition (12) on the scaling we have that $\frac{K_{1,n}^2}{\ell} n = \omega(1)$, so that
\[
2 e^{-\frac{\beta \ell K_{1,n}^2}{\ell} n^2} = o(1)
\]  \hspace{1cm} since $\beta, \nu > 0$. Reporting this into (108), we immediately obtain
\[
\lim_{n \to \infty} \sum_{\ell = \min \{L_n, \lfloor vn \rfloor \} + 1}^{L_n} \binom{n}{\ell} f_{n, \ell}(\mu, \theta_n) = 0.
\]  \hspace{1cm} (109)

**E. The case where $L_n + 1 \leq \ell \leq \lfloor \frac{2}{\theta} \rfloor$**

Finally, we consider the range $L_n + 1 \leq \ell \leq \lfloor \frac{2}{\theta} \rfloor$, where we have $X_{\ell,n} = \lfloor \gamma P_n \rfloor$ as stated in (70). Using once again the crude bound $|\Sigma|_n \geq K_{1,n}$ we get
\[
\mathbb{E} \left[ e^{-\frac{(X_{\ell,n} + 1)|\Sigma|_n}{\ell}} \right]^{n - \ell} \leq e^{-\gamma K_{1,n} \frac{n}{\ell}} \leq e^{-\gamma K_{1,n} \frac{n}{2}}.
\]  \hspace{1cm} (110)

In view of (110) and (93) we find
\[
\sum_{\ell = L_n + 1}^{\lfloor \frac{2}{\theta} \rfloor} \binom{n}{\ell} f_{n, \ell}(\mu, \theta_n) \leq \left( \sum_{\ell = L_n + 1}^{\lfloor \frac{2}{\theta} \rfloor} \binom{n}{\ell} \right) e^{-\gamma K_{1,n} \frac{n}{2}}.
\]

As before, we have under (11) and (12) that $K_{1,n} = \omega(1)$ leading to
\[
2 e^{-\gamma K_{1,n} \frac{n}{2}} = o(1).
\]

Reporting this into (111), we immediately obtain
\[
\lim_{n \to \infty} \sum_{\ell = L_n + 1}^{\lfloor \frac{2}{\theta} \rfloor} \binom{n}{\ell} f_{n, \ell}(\mu, \theta_n) = 0.
\]  \hspace{1cm} (112)

**ACKNOWLEDGEMENTS**

This work has been supported in part by the Department of Electrical and Computer Engineering at Carnegie Mellon University. The author thanks Prof. A. M. Makowski from UMD and R. Eletreby from CMU for insightful comments concerning this work. Finally, we thank the anonymous reviewers whose comments helped improve the paper.

**APPENDIX**

In this section, we will show that combined together Theorem 3.1 and Theorem 3.2 is equivalent to Corollary 3.3 under the enforced assumptions. Consider a probability distribution $\mu = (\mu_1, \ldots, \mu_r)$ with $\mu_i > 0$ for all $i = 1, \ldots, r$ and a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to [0, 1]$ of the aforementioned equivalence of the results will follow upon showing the equivalence of the conditions (7) and (13), namely that for any $c > 0$ we have
\[
\lambda_1(n) \sim c \frac{\log n}{n} \text{ if and only if } K_{1,n} \mathbb{E} \left[ |\Sigma|_n \right] \sim c \frac{\log n}{P_n}.
\]

In order to establish this, we will show that either of the conditions (7) or (13) individually imply $\lambda_1(n) \sim K_{1,n} \mathbb{E} \left[ |\Sigma|_n \right]$, or equivalently that
\[
\sum_{j=1}^{r} p_{1,j}(n) \mu_j \sim \sum_{j=1}^{r} K_{1,n} \frac{K_{1,j,n}}{P_n} \mu_j.
\]  \hspace{1cm} (A.1)

Since $\mu_j > 0$ for all $j = 1, \ldots, r$, (A.1) will follow immediately if we show under either (7) or (13) that
\[
p_{1,j}(n) \sim \frac{K_{1,1,n} K_{1,j,n}}{P_n}, \quad j = 1, \ldots, r.
\]  \hspace{1cm} (A.2)

Lemma 4.2 readily gives (A.2) as we note that for all $j = 1, \ldots, r$, (7) implies $p_{1,j}(n) = o(1)$ while (13) implies $K_{1,j,n}^2 / P_n = o(1)$. The equivalence of Theorem 3.1-Theorem 3.2 with Corollary 3.3 is now established.

**REFERENCES**


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, College Park, MD in 2011. He is an Assistant Research Professor of Electrical and Computer Engineering (ECE) at Carnegie Mellon University (CMU) with an appointment in the Silicon Valley Campus. Prior to joining the faculty of the ECE department in August 2013, he was a Postdoctoral Research Fellow in CyLab at CMU. He has also held a visiting Postdoctoral Scholar position at Arizona State University during Fall 2011. He has served as a Technical Program Committee member of several international conferences including SECRYPT 2012, IEEE GLOBECOM 2013-2015, IEEE GlobalSIP 2013, IEEE PIMRC 2014. His research interests include wireless network security, dynamical processes in complex networks, percolation theory, random graphs and their applications.