Absence of isolated nodes in inhomogeneous random key graphs

Osman Yağan
CyLab and Dept. of ECE, Carnegie Mellon University
Moffett Field, CA 94035
Email: oyagan@ece.cmu.edu

***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, for each $i = 1, \ldots, r$. Once deployed, a pair of sensors can establish a *secure* communication channel if and only if they have a key in common. We model the communication topology of this network by an *inhomogeneous* random key graph. We establish scaling conditions on the parameters P and $\{K_1, \ldots, K_r\}$ so that the this graph has no isolated nodes with high probability. The result is given in the form of a zero-one law with the number of sensors n growing unboundedly large. An analogous result is also conjectured for the property of graph connectivity.**

Keywords*—*Heterogeneous wireless sensor networks; key predistribution; random graphs; connectivity.

I. Introduction

Random key graphs are naturally induced by the Eschenauer-Gligor (EG) random key predistribution scheme [8], which is a widely recognized solution for securing wireless sensor network (WSN) communications [4], [7]. Denoted by $\mathbb{G}(n, K, P)$, 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 Σ_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 [19], recommender systems [12], and classification analysis [10]. Properties that have been studied include absence of isolated nodes [18], connectivity [14], [20], k-connectivity [22], and k-robustness [21], 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 [15], [16]. 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 feasible 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 $\boldsymbol{K} = \{K_1, \ldots, K_r\}$ according to some probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$, for some fixed integer r. We can think of this as each vertex v_x 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 Σ_x is constructed by sampling the key pool randomly and without replacement.

Let $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ 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 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and to understand how the parameters $n, \boldsymbol{\mu}, \boldsymbol{K}, P$ should behave so that the resulting graph is connected almost surely. Such results can be useful in deriving guidelines for designing heterogenous 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.

Our main result is a zero-one law for the property that $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ has no *isolated* nodes; see Theorem 1. Namely, we scale the parameters $\boldsymbol{K}$ and P and provide critical conditions on this scaling such that the resulting graph almost surely has no isolated node and almost surely has at least one isolated node, respectively, when the number of nodes n goes to infinity. Although weaker than connectivity, absence of isolated nodes is often a good indicator that the graph is likely to be connected. In fact, in many known random graph models including Erdős-Rényi graphs [2], random key graphs [20], and random geometric graphs [13], absence of isolated nodes and connectivity are known to be asymptotically equivalent properties. Hence, we conjecture that our main result do also hold for the connectivity of $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$.

Our results are also compared with the existing results by Zhao et al. [21] and Godehardt et al. [10] for the k-connectivity and connectivity, respectively, of $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$; in those references $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ was referred to as a *general* random intersection graph. We show that earlier results are constrained to parameter ranges that are unlikely to be feasible in real world 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-B for details.

In addition, our main result indicates that the minimum key ring size in the network has a significant impact on the

connectivity of $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K},P)$, perhaps in a way that would be deemed surprising. In particular, for the standard random key graph $\mathbb{G}(n;K,P)$ the critical threshold for connectivity and absence of isolated nodes is known [14], [20] to be given by $\frac{K^2}{P}\sim c\frac{\log n}{n}$ and the resulting graph is asymptotically almost surely connected (resp. not connected) if $c>1$ (resp. $c<1$). For the inhomogeneous random key graph $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ one would be tempted to think that an equivalent result holds under the scaling $\frac{K_{\text{avg}}^2}{P}\sim c\frac{\log n}{n}$, with $K_{\text{avg}}=\sum_{j=1}^r \mu_j K_j$ denoting the mean key ring size. Instead, we show that the zero-one law for absence of isolated holds under $\frac{K_{\min}K_{\text{avg}}}{P}\sim c\frac{\log n}{n}$, where $K_{\min}$ stands for the minimum of $\{K_1,\ldots,K_r\}$; see Corollary 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.

We close with a word on notation in use. All limiting statements and asymptotic equivalences are understood with the number of sensors 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 the corresponding expectation operator is denoted by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. We say that an even holds *with high probability* (whp) if it holds with probability 1 as $n\to\infty$. In comparing the asymptotic behaviors of the sequences $\{a_n\},\{b_n\}$, we use $a_n=o(b_n)$, $a_n=w(b_n)$, $a_n=O(b_n)$, $a_n=\Omega(b_n)$, and $a_n=\Theta(b_n)$, with their meaning in the standard Landau notation. We also use $a_n\sim b_n$ to denote the asymptotic equivalence $\lim_{n\to\infty}a_n/b_n=1$.

II. Model Definitions

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

$$\mathbb{P}[t_\ell=i]=\mu_i>0,\qquad i=1,\ldots,r,$$

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 Σ_x of a node x is an $\mathcal{P}_{K_{t_x}}$-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 $|\mathcal{P}_A|=\binom{P}{A}$. It is further assumed that the rvs $\Sigma_1,\ldots,\Sigma_n$ are *i.i.d.*.

Let $\boldsymbol{K}=(K_1,\ldots,K_r)$ and $\boldsymbol{\mu}=(\mu_1,\ldots,\mu_r)$. Without loss of generality we assume that $K_1\le K_2\le\cdots\le K_r$. Consider a random graph $\mathbb{G}$ defined on the vertex set $\mathcal{V}=\{v_1,\ldots,v_n\}$ 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

$$v_x\sim v_y\qquad\text{if}\qquad\Sigma_x\cap\Sigma_y\neq\emptyset. \tag{1}$$

The adjacency condition (1) defines the inhomogeneous random key graph, hereafter denoted $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K},P)$. 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. This independence disappears in the inhomogeneous random key graph case, but one can still compute p_{ij} as

$$p_{ij}=1-\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}},\quad i,j=1,\ldots,r. \tag{2}$$

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 6.

Throughout, we assume that the number of classes r is fixed and do not scale with n, and so are the probabilities $\mu_1,\ldots,\mu_r$. 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 gets large. In presenting our results below, we shall make use of the *mean* probability of edge occurrence for each node class. Namely, we define

$$\lambda_i(n):=\sum_{j=1}^r p_{ij}(n)\mu_j,\quad i=1,\ldots,r, \tag{3}$$

where $p_{ij}(n)$ 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 $(n-1)\lambda_i(n)$.

III. Main Results and Discussion

A. The results

Our main result is 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

$$K_{1,n}\le K_{2,n}\le\cdots\le K_{r,n}<P_n \tag{4}$$

are satisfied for all $n=2,3,\ldots$. To simplify the notation, we also let $\boldsymbol{K}_n=(K_{1,n},K_{2,n},\ldots,K_{r,n})$.

Theorem 1. *Consider a scaling $K_1,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$ such that*

$$\lambda_1(n)\sim c\frac{\log n}{n} \tag{5}$$

for some $c>0$. Then, we have

$$\lim_{n\to\infty}\mathbb{P}[\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)\text{ has no isolated nodes}]=\begin{cases}0 & \text{if } c<1\\ 1 & \text{if } c>1.\end{cases} \tag{6}$$

A proof of Theorem 1 can be found in Section V. The scaling condition (5) will often be used in the equivalent form

$$\lambda_1(n)=c_n\frac{\log n}{n} \tag{7}$$

with $\lim_{n\to\infty}c_n=c>0$.

In words, Theorem 1 states that the inhomogeneous random key graph $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)$ has no isolated node 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 6, 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 $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)$ has a node that is isolated. This result is analogous to that established 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 $\boldsymbol{\mu}$ 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 (3), 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.[1]

It can also be inferred from [5] that a similar zero-one law applies also for the property of absence of isolated nodes; i.e., absence of isolated nodes and connectivity are asymptotically equivalent properties. This naturally prompts us to ask whether a similar version of Theorem 1 can be established for the property of graph connectivity in $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)$. After all, we readily get from Theorem 1 that

$$\lim_{n\to\infty}\mathbb{P}\left[\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)\text{ is connected}\right]=0\quad\text{if } c<1$$

under the scaling condition (5); this follows since the existence of isolated nodes automatically implies that the graph is *not* connected. We conjecture below that the one-law holds as well.

Conjecture 2. *Consider a scaling $K_1,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$ such that (5) holds for some $c>0$. Then, we have*

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

Next, we give a corollary of Theorem 1 that states the same zero-one law under a different scaling condition than (5). This alternative formulation will make it easier to derive design guidelines for *dimensioning* 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 has no isolated sensors whp.

Corollary 3. *Consider a probability distribution $\boldsymbol{\mu}=(\mu_1,\ldots,\mu_r)$ with $\mu_i>0$ for $i=1,\ldots,r$ and a scaling $K_1,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$. Let X_n denote a rv that takes the value $K_{i,n}$ with probability μ_i for each $i=1,\ldots,r$. If it holds that*

$$\frac{K_{1,n}\mathbb{E}\left[X_n\right]}{P_n}\sim c\frac{\log n}{n}\tag{8}$$

for some $c>0$, then we have the zero-one law (6).

A proof of Corollary 3 is given in Section VIII. We remark that $\mathbb{E}\left[X_n\right]$ gives the mean number of keys assigned to a sensor in the network. With this in mind, Corollary 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 $(1+\epsilon)\frac{P_n\log n}{n}$ for some $\epsilon>0$.

To compare with the homogeneous random key predistribution scheme, set $r=1$ and consider a universal key ring size K_n in Corollary 3. This leads to a zero-one law for the absence of isolated nodes in the standard random key graph $\mathbb{G}(n;K_n,P_n)$. Namely, with

$$\frac{K_n^2}{P_n}\sim c\frac{\log n}{n},\qquad c>0\tag{9}$$

an analog of (6) is obtained for $\mathbb{G}(n;K_n,P_n)$; a result that has already been established [18], [20] 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 (9) 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. In the heterogeneous case, one gains the flexibility of having a positive fraction of sensors in the network with arbitrarily small number of keys; i.e., they can have as few as one key per node. However, from Corollary 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.

B. Comparison with related works

The random graph model $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)$ considered here is also known as *general random intersection graphs* in the literature; e.g., see [1], [9], [21]. To the best of our knowledge this model has been first considered by Godehardt and Jaworski [9] and by Goderhardt et al. [10]. Results for both the existence of isolated nodes and graph connectivity have been established; see below for a comparison of these results with those established here. Later, Bloznelis et al. [1] analyzed the component evolution problem in the general random intersection graph and provided scaling conditions for the existence of a *giant component*. There, they also established that under certain conditions $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{K}_n,P_n)$ behaves very similarly with a standard Erdős-Rényi graph [2]. Taking advantage of this similarity, Zhao et al. [21] established various results for the k-connectivity and k-robustness of the general random intersection graph by means of a coupling argument.

We now compare our results with those established in the literature. Our main argument is that previous results for the connectivity of inhomogeneous random key graphs are constrained to very narrow parameter ranges that are impractical for wireless sensor network applications. In particular, we will argue below that the result by Zhao et al. [21] is restricted to *very large* key ring sizes, rendering them impractical for resource-constrained sensor networks. On the other hand, the results by Godehardt et al. [1], [9] focus on fixed key ring sizes that do not grow with the network size n. As a consequence, in order to ensure connectivity, their result requires a key pool size P_n that is *much smaller* than typically prescribed for security and resiliency purposes.

[1]Results in [5] cover more general cases than presented here; e.g., the case where the number of classes r is not bounded.

To fix the terminology, let $\mathcal{D}_n : \{1, 2, \ldots, P_n\} \to [0, 1]$ be the probability distribution used for drawing the *size* of the key rings $\Sigma_1, \ldots, \Sigma_n$; as before, once its size is fixed a key ring is formed by sampling a key pool with size P_n randomly and without replacement. The graph $\mathbb{G}(n; \mathcal{D}_n, P_n)$ is then defined on the vertices $\{v_1, \ldots, v_n\}$ and contains an edge between any pair of nodes v_x and v_y as long as $\Sigma_x \cap \Sigma_y \neq \emptyset$. The model $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}_n, P_n)$ considered here constitutes a special case of $\mathbb{G}(n; \mathcal{D}_n, P_n)$ under the assumption that the support of $\mathcal{D}_n$ has a fixed size of r.

With these definitions in mind we now state the results by Zhao et al. [21] and by Goderhardt et al. [10], respectively.

Theorem 4. *[21, Theorem 1] Consider a general random intersection graph $\mathbb{G}(n, \mathcal{D}_n, P_n)$. Let X_n be a random variable following the probability distribution $\mathcal{D}_n$. With a sequence α_n for all n defined through*

$$\frac{\mathbb{E}[X_n]^2}{P_n} = \frac{\ln n + (k-1)\log\log n + \alpha_n}{n}, \tag{10}$$

if $\mathbb{E}[X_n] = \Omega\big(\sqrt{\log n}\,\big)$, $var[X_n] = o\Big(\frac{\mathbb{E}[X_n]^2}{n(\log n)^2}\Big)$ and $|\alpha_n| = o(\log n)$, then

$$\lim_{n\to\infty} \mathbb{P}\big[\mathbb{G}(n, \mathcal{D}_n, P_n) \text{ is } k\text{-connected.}\big] = \begin{cases} 0, & \text{if } \lim_{n\to\infty} \alpha_n = -\infty, \\ 1, & \text{if } \lim_{n\to\infty} \alpha_n = \infty, \\ e^{-\frac{e^{-\alpha^*}}{(k-1)!}}, & \text{if } \lim_{n\to\infty} \alpha_n = \alpha^* \in (-\infty, \infty). \end{cases}$$

Theorem 5. *[10, Theorem 2] Consider a general random intersection graph $\mathbb{G}(n, \mathcal{D}, P_n)$, where $\mathcal{D}(\ell) = 0$ for all $\ell > r$ and $\ell = 0$. Namely, all key ring sizes are bound to be on the interval $[1, r]$. Let X be a random variable following the probability distribution $\mathcal{D}$. Then if*

$$\frac{n}{P_n}(\mathbb{E}[X] - \mathcal{D}(1)) - \log P_n \to \infty \tag{11}$$

then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n, \mathcal{D}, P_n) \text{ is connected}\right] = 1.$$

Also, if $\mathcal{D}(r) = 1$ for some $r \geq 2$, and it holds that

$$n = P_n \frac{\log P_n + o(\log\log P_n)}{r^2}, \tag{12}$$

then

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

In comparing Theorems 1, 4 and 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 4 and 5 consider more complicated graph properties, we now argue why the established results are *not* likely to be applicable for real-world sensor networks. First, Theorem 5 focuses on the case where all possible key rings have a finite size that do not scale with n. In addition, with $\mathbb{E}[X]$ fixed, it is clear that the scaling conditions (11) and (12) both require

$$P_n = O\left(\frac{n}{\log n}\right). \tag{13}$$

Unfortunately, it is often needed that key pool size P_n be much larger than the network size n [6], [8] as otherwise the network will be extremely vulnerable against node capture attacks. In fact, one can see that with (13) 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 4, where the major problem arises from the assumption

$$var[X_n] = o\left(\frac{\mathbb{E}[X_n]^2}{n(\log n)^2}\right). \tag{14}$$

For the model to be deemed as *inhomogeneous* random key graph, the variance of the key ring size should be non-zero. In fact, given that key ring sizes are integer valued, the simplest possible case would be that $\mathcal{D}(K+1) = \mu$ and $\mathcal{D}(K) = 1 - \mu$ 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 μ and $1-\mu$, respectively. In this case, we can easily see that $var[X] = \mu(1-\mu) > 0$ as long as $0 < \mu < 1$. Therefore, for an inhomogeneous random key graph, the condition (14) implies that $\frac{\mathbb{E}[X_n]^2}{n(\log n)^2} = w(1)$, or, equivalently that

$$\mathbb{E}[X_n] = w\left(\sqrt{n}\log n\right). \tag{15}$$

Put differently, Theorem 4 enforces *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 [6], [8]. As a result, key rings with size $w(\sqrt{n}\log n)$ are unlikely to be implementable in most practical network deployments. In fact, it was suggested by Di Pietro et al. [6] that key rings with size $O(\log n)$ are acceptable for sensor networks.

In comparison, our main result Theorem 1 do not require either of the conditions (13) or (15). To see this, note that we only enforce the scaling condition (7), which implies that

$$\lambda_1(n) = \sum_{j=1}^{r} \mu_j p_{1j}(n) = \Theta\left(\frac{\log n}{n}\right).$$

With r fixed, $\mu_j > 0$ for all $j = 1, \ldots, r$, and p_{1j} increasing with j as shown in the proof of Proposition 6 below, this is equivalent to

$$p_{1r}(n) = \Theta\left(\frac{\log n}{n}\right). \tag{16}$$

In view of Lemma 10 presented in Section VIII, our condition (16) is equivalent to

$$\frac{K_{1,n}K_{r,n}}{P_n} = \Theta\left(\frac{\log n}{n}\right). \tag{17}$$

It is clear that this condition does not require (13) or (15). More importantly, it enables parameter choices that are widely regarded as practical in real-world sensor networks. To provide a concrete example, one can set $P_n = \Theta(n\log n)$ and $K_{r,n} = \Theta(\log n)$. With these choices, in addition to network being free of isolated nodes, i) the key pool will be much larger than the network size ensuring a good level resiliency against node capture attacks, and ii) the maximum key ring size will be on the order of the practical value $\log n$.

IV. Preliminaries

In this section, we establish several preliminary results that will be used in the proof of Theorem 1. The first result states that mean edge probabilities are ordered in the same way with the key ring sizes.

Proposition 6. *For any scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, we have*

$$\lambda_1(n) \leq \lambda_2(n) \leq \cdots \leq \lambda_r(n) \tag{18}$$

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

Proof. In view of (3), the desired result (18) will follow immediately if we show that $p_{ij}(n)$ is increasing in both i and j. Fix $n = 2, 3, \ldots$ and recall 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

$$\begin{aligned}
\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} &= \frac{(P-K_i)!}{(P-K_i-K_j)!K_j!}\frac{(P-K_j)!K_j!}{P!} \\
&= \frac{(P-K_i)!}{P!}\frac{(P-K_j)!}{(P-K_i-K_j)!} \\
&= \frac{(P-K_j)(P-K_j-1)\cdots(P-K_j-K_i+1)}{P(P-1)\cdots(P-K_i+1)} \\
&= \prod_{\ell=0}^{K_i-1}\left(1-\frac{K_j}{P-\ell}\right).
\end{aligned} \tag{19}$$

It is now immediate that $\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}}$ 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 6. ■

The following inequality will also be useful in our proof.

Proposition 7. *For any set of positive integers $K_1, \ldots, K_r$, P, and any scalar $a \geq 1$, we have*

$$\frac{\binom{P-\lceil aK_i\rceil}{K_j}}{\binom{P}{K_j}} \leq \left(\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}}\right)^a, \quad i, j = 1, \ldots, r. \tag{20}$$

Proof. Fix $i, j = 1, 2, \ldots, r$. Observe that $\binom{P-K_i}{K_j}/\binom{P}{K_j} \geq 0$ so that (20) holds trivially if $K_j + \lceil aK_i\rceil > P$. Assume here onwards that $K_j + \lceil aK_i\rceil \leq P$. Recalling (19), we find

$$\begin{aligned}
\frac{\binom{P-\lceil aK_i\rceil}{K_j}}{\binom{P}{K_j}} &= \prod_{\ell=0}^{K_j-1}\left(1-\frac{\lceil aK_i\rceil}{P-\ell}\right) \\
&\leq \prod_{\ell=0}^{K_j-1}\left(1-\frac{aK_i}{P-\ell}\right),
\end{aligned} \tag{21}$$

and

$$\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} = \prod_{\ell=0}^{K_j-1}\left(1-\frac{K_i}{P-\ell}\right). \tag{22}$$

In view of (21) and (22), the desired inequality (20) will follow if we show that

$$1-\frac{aK_i}{P-\ell} \leq \left(1-\frac{K_i}{P-\ell}\right)^a, \quad \ell = 0, 1, \ldots, K_j-1. \tag{23}$$

For each $\ell = 0, 1, \ldots, K_j - 1$, (23) follows as we note that

$$1-\left(1-\frac{K_i}{P-\ell}\right)^a = \int_{1-\frac{K_i}{P-\ell}}^1 at^{a-1}dt \leq \frac{aK_i}{P-\ell}$$

and (20) is now established. ■

In the course of proving Theorem 1 we also make use of the decomposition

$$\log(1-x) = -x - \Psi(x), \quad 0 \leq x < 1 \tag{24}$$

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

$$\lim_{x\downarrow 0}\frac{\Psi(x)}{x^2} = \frac{1}{2}. \tag{25}$$

V. A proof of Theorem 1

The proof of Theorem 1 passes through applying the method of first and second moments [11, p. 55] to the number of isolated nodes in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$. To simplify the notation, we let $\boldsymbol{\theta} = (\boldsymbol{K}, P)$. Let $I_n(\boldsymbol{\mu}, \boldsymbol{\theta})$ denote the total number of isolated nodes in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta})$; i.e.,

$$I_n(\boldsymbol{\mu}, \boldsymbol{\theta}) = \sum_{\ell=1}^n \mathbf{1}\left[v_\ell \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta})\right]. \tag{26}$$

A. Establishing the one-law

Consider now a scaling $\boldsymbol{\theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (5) holds with $c > 1$. The random graph $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta}_n)$ has no isolated nodes if and only if $I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) = 0$. The method of first moment [11, Eqn (3.10), p. 55] gives

$$1 - \mathbb{E}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] \leq \mathbb{P}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) = 0\right], \tag{27}$$

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

$$\lim_{n\to\infty}\mathbb{E}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] = 0. \tag{28}$$

By exchangeability of the indicator functions appearing at (26), we find

$$\mathbb{E}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] = n\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta}_n)\right]. \tag{29}$$

Conditioning on the class of v_1, we further get

$$\begin{aligned}
&n\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] \\
&= n\sum_{i=1}^r \mu_i \mathbb{P}\left[v_1 \text{ is isolated} \mid v_1 \text{ is class } i\right] \\
&= n\sum_{i=1}^r \mu_i \mathbb{P}\left[\cap_{j=2}^n [v_1 \not\sim v_j] \mid v_1 \text{ is class } i\right] \\
&= n\sum_{i=1}^r \mu_i \left(\mathbb{P}\left[v_1 \not\sim v_2 \mid v_1 \text{ is class } i\right]\right)^{n-1}
\end{aligned} \tag{30}$$

where (30) follows from the fact that rvs $\{v_1 \not\sim v_j\}_{j=2}^n$ are conditionally independent given the key ring Σ_1 of node v_1. Conditioning further on the class of v_2, we find

$$\begin{aligned}
&\mathbb{P}\left[v_1 \not\sim v_2 \mid v_1 \text{ is class } i\right] \\
&= \sum_{j=1}^{r} \mu_j \mathbb{P}\left[v_1 \not\sim v_2 \mid v_1 \text{ is class } i, v_2 \text{ is class } j\right] \\
&= \sum_{j=1}^{r} \mu_j (1 - p_{ij}(n)) \\
&= 1 - \lambda_i(n). \qquad (31)
\end{aligned}$$

Using (31) in (30), and recalling (18) we get

$$\begin{aligned}
&n\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] \\
&= n \sum_{i=1}^{r} \mu_i (1 - \lambda_i(n))^{n-1} \\
&\leq n(1 - \lambda_1(n))^{n-1} \\
&\leq e^{\log n - c_n \log n \frac{n-1}{n}} \qquad (32)
\end{aligned}$$

as we recall (7). Letting n go to infinity in this last expression we immediately get

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

since $\lim_{n\to\infty} 1 - c_n \frac{n-1}{n} = 1 - c < 0$ under the enforced assumptions. Invoking (29) we now get (28) and the one-law is established. ∎

B. Establishing the zero-law

This section is devoted to establishing the zero-law in Theorem 1, namely the fact that inhomogeneous random key graph contains at least one isolated node when the scaling condition (5) is satisfied with $c < 1$. We will establish this by applying the method of second moment [11, Remark 3.1, p. 55] to a variable that counts nodes that are class-1 and isolated. Clearly, if we show that whp there exists at least one class-1 node that is isolated, then the desired zero-law will follow.

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

$$\mathbb{P}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta}) = 0\right] \leq 1 - \frac{\mathbb{E}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta})\right]^2}{\mathbb{E}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta})^2\right]}. \qquad (33)$$

Also, by exchangeability and the binary nature of the rvs $\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}), \ldots, \chi_{n,n}(\boldsymbol{\mu}, \boldsymbol{\theta})$, we have

$$\begin{aligned}
&\mathbb{E}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta})^2\right] \qquad (34) \\
&= n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\right] + n(n-1)\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\chi_{n,2}(\boldsymbol{\mu}, \boldsymbol{\theta})\right]
\end{aligned}$$

It then follows that

$$\begin{aligned}
\frac{\mathbb{E}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta})^2\right]}{\mathbb{E}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta})\right]^2} &= \frac{1}{n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\right]} \\
&\quad + \frac{n-1}{n} \cdot \frac{\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\chi_{n,2}(\boldsymbol{\mu}, \boldsymbol{\theta})\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\right]\right)^2}. \qquad (35)
\end{aligned}$$

From (33) and (34) we see that

$$\lim_{n\to\infty} \mathbb{P}\left[Y_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) = 0\right] = 0 \qquad (36)$$

holds if

$$\lim_{n\to\infty} n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] = \infty \qquad (37)$$

and

$$\limsup_{n\to\infty} \left(\frac{\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\chi_{n,2}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right]\right)^2} \right) \leq 1. \qquad (38)$$

However, since $I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) \geq Y_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)$, (36) immediately implies the desired the zero-law $\lim_{n\to\infty} \mathbb{P}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) = 0\right] = 0$.

The next two technical propositions establish the needed results (37) and (38) under the appropriate conditions on the scaling $\boldsymbol{\theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$.

Proposition 8. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds with $\lim_{n\to\infty} c_n = c > 0$. Then, we have*

$$n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] = (1 + o(1))\mu_1 n^{1-c_n} \qquad (39)$$

so that

$$\lim_{n\to\infty} n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] = \infty \quad \text{if } c < 1. \qquad (40)$$

Proposition 9. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds with $\lim_{n\to\infty} c_n = c > 0$. Then, we have (38).*

A proof of Proposition 8 is given in Section VI, while Proposition 9 is established in Section VII.

VI. A proof of Proposition 8

Fix $n = 2, 3, \ldots$, and pick $\boldsymbol{u}$ and $\boldsymbol{\theta}$. We have

$$\begin{aligned}
&n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\right] \\
&= n\mathbb{P}\left[v_1 \text{ is isolated and class-1}\right] \\
&= n\mu_1 \mathbb{P}\left[v_1 \text{ is isolated} \mid v_1 \text{ is class-1}\right] \\
&= n\mu_1 \mathbb{P}\left[\cap_{j=2}^{n} [v_1 \not\sim v_j] \mid v_1 \text{ is class-1}\right] \\
&= n\mu_1 \left(\mathbb{P}\left[v_1 \not\sim v_2 \mid v_1 \text{ is class-1}\right]\right)^{n-1} \qquad (41)
\end{aligned}$$

by virtue of the fact that the events $\{v_1 \not\sim v_j\}_{j=2}^n$ are independent conditionally on Σ_1. Invoking (31), we then get

$$n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta})\right] = n\mu_1 \left(1 - \lambda_1\right)^{n-1}. \qquad (42)$$

Now, consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds with $\lim_{n\to\infty} c_n = c > 0$. Using this scaling in (42) and recalling (24) we get

$$\begin{aligned}
&n\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu}, \boldsymbol{\theta}_n)\right] \\
&= n\mu_1 \left(1 - c_n \frac{\log n}{n}\right)^{n-1} \\
&= n\mu_1 e^{-c_n \log n \frac{n-1}{n} - (n-1)\psi\left(c_n \frac{\log n}{n}\right)} \\
&= \mu_1 n^{1-c_n} e^{c_n \frac{\log n}{n}} e^{-(n-1)c_n^2 \frac{(\log n)^2}{n^2} \left(\frac{\psi\left(c_n \frac{\log n}{n}\right)}{\left(c_n \frac{\log n}{n}\right)^2} \right)}. \qquad (43)
\end{aligned}$$

The desired result (39) is now immediate as we recall (25) and note that

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

and

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

since $\lim_{n\to\infty} c_n = c > 0$.

From (39), we readily get (40) upon noting that $\mu_1 > 0$. ■

VII. A PROOF OF PROPOSITION 9

We start by obtaining an expression for the probability that nodes v_1 and v_2 are isolated in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta})$. We get

$$\begin{aligned}
&\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu},\boldsymbol{\theta})\chi_{n,2}(\boldsymbol{\mu},\boldsymbol{\theta})\right] \\
&= \mu_1^2 \mathbb{P}\left[v_1 \text{ and } v_2 \text{ are isolated} \mid v_1 \text{ and } v_2 \text{ are class-1}\right] \\
&= \mu_1^2 \mathbb{P}\left[\Sigma_1 \cap \Sigma_2 = \emptyset \;\middle|\; |\Sigma_1| = |\Sigma_2| = K_1\right] \\
&\quad \times \mathbb{P}\left[\cap_{j=3}^n [\Sigma_j \cap (\Sigma_1 \cup \Sigma_2) = \emptyset] \;\middle|\; \begin{array}{l} \Sigma_1 \cap \Sigma_2 = \emptyset, \\ |\Sigma_1| = |\Sigma_2| = K_1 \end{array}\right] \\
&= \mu_1^2 \frac{\binom{P-K_1}{K_1}}{\binom{P}{K_1}} \\
&\quad \times \mathbb{P}\left[\Sigma_3 \cap (\Sigma_1 \cup \Sigma_2) = \emptyset \;\middle|\; \begin{array}{l} \Sigma_1 \cap \Sigma_2 = \emptyset, \\ |\Sigma_1| = |\Sigma_2| = K_1 \end{array}\right]^{n-2} \\
&= \mu_1^2 \frac{\binom{P-K_1}{K_1}}{\binom{P}{K_1}} \left(\sum_{j=1}^r \mu_j \frac{\binom{P-2K_1}{K_j}}{\binom{P}{K_j}} \right)^{n-2} \qquad (44)
\end{aligned}$$

upon conditioning on the class of v_3. Similarly, it is easy to see that

$$\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu},\boldsymbol{\theta})\right] = \mu_1 \left(\sum_{j=1}^r \mu_j \frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} \right)^{n-1}. \qquad (45)$$

Combining (44) and (45), we find

$$\begin{aligned}
&\frac{\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu},\boldsymbol{\theta})\chi_{n,2}(\boldsymbol{\mu},\boldsymbol{\theta})\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\boldsymbol{\mu},\boldsymbol{\theta})\right]\right)^2} \\
&= \frac{\binom{P-K_1}{K_1}}{\binom{P}{K_1}} \left(\frac{\sum_{j=1}^r \mu_j \frac{\binom{P-2K_1}{K_j}}{\binom{P}{K_j}}}{\left(\sum_{j=1}^r \mu_j \frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}}\right)^2} \right)^{n-2} \left(\sum_{j=1}^r \mu_j \frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} \right)^{-2} \qquad (46)
\end{aligned}$$

Consider a scaling $\boldsymbol{\theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (5) holds with $c < 1$. Reporting this scaling into the last expression, we see that

$$\begin{aligned}
\left(\sum_{j=1}^r \mu_j \frac{\binom{P_n-K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \right)^{-2} &= (1-\lambda_1(n))^{-2} = \left(1 - c_n \frac{\log n}{n}\right)^{-2} \\
&= 1 + o(1). \qquad (47)
\end{aligned}$$

With $p_{ij}(n)$ increasing with i and j as shown in Proposition 6, it is also clear that

$$1 \geq \frac{\binom{P_n-K_{1,n}}{K_{1,n}}}{\binom{P_n}{K_{1,n}}} = 1 - p_{11}(n) \geq 1 - \lambda_1(n) = 1 - c_n \frac{\log n}{n},$$

leading to

$$\frac{\binom{P_n-K_{1,n}}{K_{1,n}}}{\binom{P_n}{K_{1,n}}} = 1 - o(1). \qquad (48)$$

Finally, we note from Proposition 7 that

$$\frac{\binom{P_n-2K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \leq \left(\frac{\binom{P_n-K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \right)^2, \qquad j = 1, \ldots, r. \qquad (49)$$

Let $Z_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)$ denote a rv such that

$$Z_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n) = \frac{\binom{P_n-K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \quad \text{with probability } \mu_j, \quad j = 1, \ldots, r.$$

Applying (47), (48), and (49) in (46) we see that the desired result (38) will follow upon showing

$$\limsup_{n\to\infty} \left(\frac{\mathbb{E}\left[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)^2\right]}{\mathbb{E}\left[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)\right]^2} \right)^{n-2} \leq 1. \qquad (50)$$

We note that

$$\begin{aligned}
\left(\frac{\mathbb{E}\left[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)^2\right]}{\mathbb{E}\left[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)\right]^2} \right)^{n-2} &= \left(1 + \frac{var[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)]}{\mathbb{E}\left[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)\right]^2} \right)^{n-2} \\
&\leq e^{\frac{var[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)]}{\mathbb{E}[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)]^2}(n-2)} \qquad (51)
\end{aligned}$$

and that

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

Hence, we will obtain (50) if we show that

$$\lim_{n\to\infty} n \cdot var[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)] = 0. \qquad (52)$$

In order to bound the variance of $Z_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)$, we use Popoviciu's inequality. Namely, for any bounded rv X with maximum value of M and minimum value of m, we have

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

It is clear from the discussion given in the proof of Proposition 6 that

$$\frac{\binom{P_n-K_{1,n}}{K_{r,n}}}{\binom{P_n}{K_{r,n}}} \leq Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n) \leq \frac{\binom{P_n-K_{1,n}}{K_{1,n}}}{\binom{P_n}{K_{1,n}}}$$

always holds. Applying Popoviciu's inequality, we then get

$$\begin{aligned}
var[Z_n(\boldsymbol{\mu},\boldsymbol{\theta}_n)] &\leq \frac{1}{4} \left(\frac{\binom{P_n-K_{1,n}}{K_{1,n}}}{\binom{P_n}{K_{1,n}}} - \frac{\binom{P_n-K_{1,n}}{K_{r,n}}}{\binom{P_n}{K_{r,n}}} \right)^2 \\
&\leq \frac{1}{4} \left(1 - \frac{\binom{P_n-K_{1,n}}{K_{r,n}}}{\binom{P_n}{K_{r,n}}} \right)^2 \\
&= \frac{1}{4} \left(p_{1r}(n) \right)^2. \qquad (53)
\end{aligned}$$

Under the enforced assumptions, we have

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

so that

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

Reporting this into (53) we now find

$$n \cdot var[Z_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n)] \leq \frac{n}{4} \left(\frac{c_n}{\mu_r} \frac{\log n}{n} \right)^2. \tag{54}$$

Letting n go to infinity in this last expression, we immediately get (52) as we note that $\mu_r > 0$ and $\lim_{n\to\infty} c_n = c > 0$. This establishes (50) and the desired result (38) now follows. ■

VIII. A PROOF OF COROLLARY 3

In this section, we will show that under the enforced assumptions Theorem 1 and Corollary 3 are equivalent results. Consider a probability distribution $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_r)$ with $\mu_i > 0$ for all $i = 1, \ldots, r$ and a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$. The equivalence of these results will follow upon showing the equivalence of the conditions (5) and (8), namely that for any $c > 0$ we have

$$\lambda_1(n) \sim c \frac{\log n}{n} \quad \text{if and only if} \quad \frac{K_{1,n}\mathbb{E}[X_n]}{P_n} \sim c \frac{\log n}{n}.$$

In order to establish this, we will show that either of the conditions (5) or (8) imply $\lambda_1(n) \sim \frac{K_{1,n}\mathbb{E}[X_n]}{P_n}$, or equivalently

$$\sum_{j=1}^{r} p_{1j}(n)\mu_j \sim \sum_{j=1}^{r} \frac{K_{1,n}K_{j,n}}{P_n} \mu_j.$$

Noting that $\mu_i > 0$ for all $i = 1, \ldots, r$, this will follow upon showing that

$$p_{1j}(n) \sim \frac{K_{1,n}K_{j,n}}{P_n}, \qquad j = 1, \ldots, r, \tag{55}$$

under either (5) or (8). We readily get (55) from Lemma 10 below upon noting that for all $j = 1, \ldots, r$, (5) implies $p_{1j}(n) = o(1)$ while (8) implies $\frac{K_{1,n}K_{j,n}}{P_n} = o(1)$.

Lemma 10. *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*

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

and under either condition we have the asymptotic equivalence

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

Lemma 10 can easily be established by following the same arguments used in [20, Lemma 7.3] or [17, Lemma 7.4.4], namely by applying crude bounds to the expression (19). The details are committed here for brevity. The equivalence of Theorem 1 and Corollary 3 is now established. ■

ACKNOWLEDGEMENTS

This work has been supported in part by the Department of Electrical and Computer Engineering at Carnegie Mellon University. The author also thanks Prof. A. M. Makowski from UMD for insightful comments concerning this work.

REFERENCES

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

[2] B. Bollobás. *Random graphs*, volume 73. Cambridge university press, 2001.

[3] B. Bollobás, S. Janson, and O. Riordan. The phase transition in inhomogeneous random graphs. *Random Structures and Algorithms*, 33(1):3–122, 2007.

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

[5] L. Devroye and N. Fraiman. Connectivity of inhomogeneous random graphs. *Random Structures & Algorithms*, 45(3):408–420, 2014.

[6] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Redoubtable sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(3):13:1–13:22, 2008.

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

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

[9] E. Godehardt and J. Jaworski. Two models of random intersection graphs for classification. In *Exploratory Data Analysis in Empirical Research*, pages 67–81. Springer Berlin Heidelberg, 2003.

[10] E. Godehardt, J. Jaworski, and K. Rybarczyk. Random intersection graphs and classification. In *Advances in Data Analysis*, pages 67–74. Springer Berlin Heidelberg, 2007.

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

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

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

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

[15] C.-H. Wu and Y.-C. Chung. Heterogeneous wireless sensor network deployment and topology control based on irregular sensor model. In *Advances in Grid and Pervasive Computing*, volume 4459, pages 78–88. Springer Berlin Heidelberg, 2007.

[16] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh. Exploiting heterogeneity in sensor networks. In *Proceedings IEEE INFOCOM 2005*, volume 2, pages 878–890 vol. 2, March 2005.

[17] O. Yağan. *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*. PhD thesis, Dept. of ECE, College Park (MD), June 2011. Available online at http://hdl.handle.net/1903/11910.

[18] O. Yağan and A. M. Makowski. On the random graph induced by a random key predistribution scheme under full visibility. In *IEEE International Symposium on Information Theory*, pages 544–548, 2008.

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

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

[21] J. Zhao, O. Yağan, and V. Gligor. On the strengths of connectivity and robustness in general random intersection graphs. In *IEEE Annual Conference on Decision and Control*, pages 3661–3668, Dec 2014.

[22] J. Zhao, O. Yağan, and V. Gligor. k -connectivity in random key graphs with unreliable links. *Information Theory, IEEE Transactions on*, 61(7):3810–3836, July 2015.