# Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs

Rashad Eletreby and Osman Yağan
Department of Electrical and Computer Engineering and CyLab,
Carnegie Mellon University, Pittsburgh, PA, 15213 USA
reletreby@cmu.edu, oyagan@ece.cmu.edu

***Abstract*—We study the connectivity of a random graph formed by the intersection of an *inhomogeneous random key graph* with an *inhomogeneous Erdős-Rényi graph*. The former graph is naturally induced by a heterogeneous random key predistribution scheme introduced for securing wireless sensor network communications. In this scheme, nodes are divided into $r$ classes according to a probability distribution $\mu = \{\mu_1, \ldots, \mu_r\}$, and a class-$i$ sensor is assigned $K_i$ cryptographic keys that are selected uniformly at random from a common pool of $P$ keys. The latter graph represents a heterogeneous on/off channel model, where the wireless channel between a class-$i$ node and a class-$j$ node is *on* (resp. *off*) with probability $\alpha_{ij}$ (resp. $1-\alpha_{ij}$) independently from others. We present conditions on how to scale the parameters of the intersection model so that it is connected with high probability as the number of nodes gets large. The result is given in the form of a zero-one law and supported by a numerical study in the finite-node regime.**

***Index Terms*—Wireless Sensor Networks, key predistribution, random graphs, connectivity.**

## 1. Introduction

A wireless sensor network (WSN) is a collection of wireless-enabled sensor nodes that are typically of low-cost, low-power, and limited computational capabilities. Such networks are envisioned to have numerous applications in broad areas, such as military, health, environmental monitoring, etc [1]. In most cases, WSNs are deployed in hostile environments (e.g., battlefields) where communications can be eavesdropped by an adversary who might also be able to capture and maliciously use a number of sensor nodes. Therefore, it essential to secure sensors' communications by means of cryptographic protection. However, the energy, complexity, and cost constraints typically render classical cryptographic approaches such as public key cryptography non-feasible for WSNs; see [2], [3] for a detailed discussion on the challenges involved. To date, most promising solution is considered to be (random) key predistribution schemes, introduced originally by Eschenauer and Gligor (EG) [4], which are based on assigning a (possibly random) set of *symmetric* keys to each sensor prior to deployment. Then, sensors that *share* a key can establish a secure link in between (of course, only if they have a wireless communication channel available); see [5], [6] for a review of several key distribution schemes.

Recently, a new modification of the Eschenauer-Gligor (EG) key predistribution scheme was introduced in [7] that accounts for varying level of resources and/or connectivity requirements that the sensors might have; in fact, many WSN applications are likely to have *heterogeneous* nodes, e.g., regular nodes vs. cluster heads [8]. According to this heterogeneous scheme, each sensor node belongs to a specific priority class and is given a number of keys corresponding to its class. More specifically, given $r$ classes, a sensor is classified as class-$i$ with probability $\mu_i > 0$ for each $i = 1, \ldots, r$. Each class-$i$ sensor is assigned $K_i$ keys selected uniformly at random from a pool of size $P$, independently from all other sensors. As with the EG scheme, pairs of sensors that share key(s) can communicate securely over an available channel after deployment.

With $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$, $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$, and $n$ being the number of nodes, let $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ denote the random graph induced by the heterogeneous key predistribution scheme described above; i.e., a pair of nodes are connected by an undirected edge if and only if they have at least one key in common. This model, introduced in [7], is referred to as the *inhomogeneous* random key graph and generalizes the (homogeneous) random key graph $\mathbb{K}(n; K, P)$ where all nodes have the same number $K$ of keys [9], [10]. In [7], zero-one laws for the properties that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ has no isolated nodes and is connected are established under the assumption of *full visibility*. Namely, it was assumed that all wireless channels are reliable and secure communications among participating nodes require only the existence of a shared key.

This paper is motivated by the fact that the full visibility assumption is too optimistic and is not likely to hold in most WSN applications; e.g., the wireless medium of communication is often unreliable and sensors typically have limited communication ranges. To that end, we study the secure connectivity of heterogeneous WSNs under a heterogeneous on/off communication model, where the communication channel between nodes of class-$i$ and class-$j$ is *on* with probability $\alpha_{ij}$ and *off* with probability $1-\alpha_{ij}$ independently from all other channels. The heterogeneous on/off communication model induces the inhomogeneous Erdős-Rényi (ER) graph [11], [12], denoted hereafter by $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$. The overall WSN can then be modeled by a random graph formed by the intersection of an inhomogeneous random key graph and an inhomogeneous ER graph, which we denote by

$\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha}) := \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$.

Our main contribution is as follows. We present conditions (in the form of a zero-one law) on how to scale the parameters of the intersection model $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ so that it is connected with high probability when the number $n$ of nodes gets large. Our result generalizes several results in literature, including the zero-one laws for connectivity for inhomogeneous random key graphs intersecting (homogeneous) ER graphs [13], and for (homogeneous) random key graphs intersecting (homogeneous) ER graphs [14].

All limiting statements, including asymptotic equivalence are considered 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 $\mathbb{P}$. We say that an event holds with high probability (whp) if it holds with probability 1 as $n \to \infty$. For any discrete set $S$, we write $|S|$ for its cardinality. In comparing the asymptotic behaviors of the sequences $\{a_n\},\{b_n\}$, we use $a_n = o(b_n)$, $a_n = \omega(b_n)$, $a_n = O(b_n)$, $a_n = \Omega(b_n)$, 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 $\lim_{n\to\infty} a_n/b_n = 1$.

## 2. The Model

Consider a network consisting of $n$ sensor nodes (labeled as $v_1, v_2, \ldots, v_n$) and $r$ possible classes. Each node is independently assigned to one of the $r$ possible classes according to a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$. We clearly have $\mu_i > 0$ for $i = 1,\ldots,r$ and $\sum_{i=1}^r \mu_i = 1$. Put differently, an arbitrary node $v_x$ belongs to class-$i$ with probability $\mu_i$ for $i = 1,\ldots,r$. Then, a class-$i$ node is given $K_i$ cryptographic keys selected uniformly at random from a pool of size $P$. More specifically, the key ring $\Sigma_x$ of node $v_x$ is an $\mathcal{P}_{K_{t_x}}-$valued random variable where $\mathcal{P}_{K_{t_x}}$ denotes the collection of all subsets of $\{1,\ldots,P\}$ with exactly $K_{t_x}$ elements and $t_x$ denotes the class of node $v_x$. It follows that the rvs $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ are i.i.d. with

$$\mathbb{P}[\Sigma_x = S \mid t_x = i] = \binom{P}{K_i}^{-1}, \quad S \in \mathcal{P}_{K_i}.$$

Let $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$ and consider a random graph $\mathbb{K}$ induced on the vertex set $\mathcal{V} = \{v_1,\ldots,v_n\}$ such that a pair of distinct nodes $v_x$ and $v_y$ are adjacent, denoted by $v_x \sim_{\mathbb{K}} v_y$, if they have at least one cryptographic key in common, i.e.,

$$v_x \sim_{\mathbb{K}} v_y \quad \text{if} \quad \Sigma_x \cap \Sigma_y \neq \emptyset. \tag{1}$$

The adjacency condition (1) defines the inhomogeneous random key graph denoted by $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ [7], [13]. This model is also known in the literature as the *general random intersection graph*; e.g., see [15], [16]. Let $p_{ij}$ denote the probability that a class-$i$ node and a class-$j$ node are adjacent. It is easy to check that

$$p_{ij} = 1 - \frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} \tag{2}$$

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we have $p_{ij} = 1$. Then, the *mean* probability of edge occurrence for a class-$i$ node in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ is given by

$$\lambda_i = \sum_{j=1}^r p_{ij}\mu_j, \quad i = 1,\ldots,r.$$

In order to account for the possibility that communication channels between nodes may not be available, e.g., due to deep fading, interference, etc., we consider a *heterogeneous* on/off channel model, where the channel between a node of type-$i$ and a node of type-$j$ is *on* with probability $\alpha_{ij}$ or *off* with probability $1-\alpha_{ij}$ independently from others. By allowing the probability of channel existence to vary with the class of the participating nodes, this model captures the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. The heterogeneous on/off channel model can be represented by a random graph $\mathbb{G}$ induced on the same vertex set $\mathcal{V} = \{v_1,\ldots,v_n\}$, where arbitrary nodes $v_x$ and $v_y$ are adjacent, denoted $v_x \sim_{\mathbb{G}} v_y$, if $B_{xy}(\alpha_{t_x t_y}) = 1$ with $B_{xy}(\alpha_{ij})$ denoting a Bernoulli rv with success probability $\alpha_{ij}$. The resulting graph $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is known as the inhomogeneous ER graph and has received significant attention recently [11], [12]. Although the on/off representation of a channel may be deemed too simplistic, we point out that it allows a comprehensive analysis of the properties of interest and such analyses were shown to provide useful guidelines when more realistic channel models is considered; e.g., see [14] that suggest that the connectivity behavior of the EG scheme under the on/off channel model is asymptotically equivalent to that under the disk model [17].

Let $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ denote the random graph obtained by the intersection of the inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ and the inhomogeneous ER graph $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$; i.e., $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha}) := \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$. Namely, a class-$i$ node $v_x$ is adjacent to a distinct class-$j$ node $v_y$ in $\mathbb{H}$ if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{G}$. In words, the edges in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ represent pairs of sensors that share cryptographic key(s) *and* have a communication channel in between that is on, and hence can communicate securely. Therefore, studying the connectivity properties of $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ amounts to studying the secure connectivity of heterogeneous WSNs under the heterogeneous on/off channel model.

To simplify the notation, we let $\boldsymbol{\theta} = (\boldsymbol{K},P)$, and $\boldsymbol{\Theta} = (\boldsymbol{\theta},\boldsymbol{\alpha})$. By independence, we see that the probability of edge assignment between a class-$i$ node $v_x$ and a class-$j$ node $v_y$ in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ is given by $\mathbb{P}[v_x \sim v_y \mid t_x = i, t_y = j] = \alpha_{ij}p_{ij}$. We denote the mean edge probability for a class-$i$ node in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ as $\Lambda_i$. It is clear that

$$\Lambda_i = \sum_{j=1}^r \mu_j \alpha_{ij} p_{ij}, \quad i = 1,\ldots,r. \tag{3}$$

Let $m(n) := \arg\min_i \Lambda_i(n)$ for $n = 1,2,\ldots$ and assume that $\lim_{n\to\infty} m(n) = m$. In other words, for all $n$ sufficiently large, there exists a particular class $m$ such that $\Lambda_m(n) \leq \Lambda_i(n)$ for $i = 1,\ldots,r$. We also let $d(n) := \arg\max_j \alpha_{mj}(n)$

for $n = 1, 2, \ldots$ and $j = 1, \ldots, r$, and assume that $\lim_{n\to\infty} d(n) = d$; i.e., for all $n$ sufficiently large, we have $\alpha_{md} = \max\{\alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{mr}\}$. Throughout, we assume that the number of classes $r$ is fixed and does not scale with $n$, and so are the probabilities $\mu_1, \ldots, \mu_r$. All of the remaining parameters are assumed to be scaled with $n$.

## 3. Main Results and Discussion

We refer to a mapping $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ as a *scaling* for the inhomogeneous random key graph if

$$1 \leq K_{1,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{4}$$

hold for all $n = 2, 3, \ldots$. Similarly any mapping $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ defines a scaling for the inhomogeneous ER graphs. A mapping $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)^{r\times r}$ defines a scaling for the intersection graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ given that condition (4) holds. We remark that under (4), the edge probabilities $p_{ij}$ will be given by (2).

We now present a zero-one law for the property that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected.

**Theorem 3.1.** *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ such that*

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

*holds for some $c > 0$.*

*i) We have*

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

*If $\lim_{n\to\infty} \alpha_{md}(n) \log n = 0$, or $\lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^* > 0$*

*ii) If $P_n = \Omega(n)$, $\frac{\alpha_{\max}}{\alpha_{\min}} = o(\log n)$, $\frac{K_r}{K_1} = o(\log n)$, and $\alpha_{\min} p_{1r}(n) = \Omega\left(\frac{\log n}{n}\right)$, then, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \text{ is connected}\right] = 1 \quad \text{if } c > 1$$

Theorem 3.1 states that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ is connected whp if the minimum mean degree, i.e., $n\Lambda_m$, is scaled as $(1 + \epsilon)\log n$ for some $\epsilon > 0$. On the other hand, if this minimum mean degree scales as $(1-\epsilon)\log n$ for some $\epsilon > 0$, then whp $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ is not connected. The proof of Theorem 3.1 is lengthy and technically involved. Due to space limitation, we omit the proof of Theorem 3.1 from this conference version. All details can be found in [18].

### A. Comments on the additional technical conditions

In establishing the zero-law of Theorem 3.1, it is required that either $\lim_{n\to\infty} \alpha_{md}(n) \log n = 0$, or $\lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^* \in (0, \infty]$ hold. This condition is enforced mainly for technical reasons for the proof of the zero-law to work. A similar condition was also required in [14, Theorem 3.2] for establishing the zero-law for connectivity in the *homogeneous* random key graph [9] intersecting the *homogeneous* ER graph. There, it was required that $\lim_{n\to\infty} \alpha(n) \log n = [0, \infty]$ for the proof of the zero-law to work. We remark that the condition needed for our zero-law of connectivity is not required if $\alpha_{ii} = \max_j \alpha_{ij}$ for $i, j = 1, \ldots, r$; i.e., intra-class links are more reliable than inter-class links. In particular, if $\alpha_{mm} := \alpha_{md}$, the condition can indeed be eliminated by virtue of the subsubsequence principle [19], [20, p. 12].

Next, we consider the conditions needed for the one-law of Theorem 3.1. We remark that having $P_n = \Omega(n)$ is essential for real-world WSN implementations in order to ensure the *resilience* of the network against node capture attacks; e.g., see [4], [21]. For instance, assume that an adversary captures a number of sensors, compromising all the keys that belong to the captured nodes. If $P_n = o(n)$, then it would be possible for the adversary to compromise $\Omega(P_n)$ keys by capturing only $o(n)$ sensors (whose type does not matter in this case). In this case, the WSN would fail to exhibit the *unassailability* property [22], [23] and would be deemed as vulnerable against adversarial attacks. We also remark that this condition was required in [7], [10] to establish results in the same vein as ours.

Condition $\alpha_{min}(n)p_{1r}(n) = \Omega(\log n/n)$ is enforced mainly for technical reasons for the proof of the one-law to work. The need of such a lower bound arises from the fact that our scaling condition (5) merely scales the minimum *mean* edge probability, not the minimum (or each) edge probability, as $\log n/n$. For instance, the current scaling condition (5) gives us an easy upper bound on the minimum edge probability in the network, but does not specify any non-trivial lower bound on that probability. More specifically, it is easy to see that $\alpha_{min}(n)p_{11}(n) = O(\Lambda_m) = O(\log n/n)$, but it is not clear if the sequence $\alpha_{min}(n)p_{11}(n)$ has a non-trivial lower bound. In fact, authors in [11] investigated the connectivity of the inhomogeneous ER graph, while setting the probability of an edge connecting two nodes of classes $i$ and $j$ to $\kappa(i,j)\log n/n$, where $\kappa(i,j)$ returns a positive real number for each pair $(i,j)$; i.e., each individual edge was scaled as $\log n/n$. Condition $\alpha_{min}(n)p_{1r}(n) = \Omega(\log n/n)$ is itself a lower bound on a particular edge probability, but combined with $K_{r,n} = o(\log n) K_{1,n}$ it gives a non-trivial lower bound on the minimum edge probability of the network. In particular, combining those two conditions gives us $\alpha_{min}(n)p_{11}(n) = w(1/n)$ (see [18] for a proof).

Finally, conditions $\alpha_{max}(n) = o(\log n)\alpha_{min}(n)$, and $K_{r,n} = o(\log n) K_{1,n}$ limit the flexibility of assigning very large values to the maximum key ring size and the maximum channel probability compared to their respective minima. These two conditions are required to obtain efficient bounds for various expressions that involve $K_{r,n}$ or $\alpha_{max}(n)$. In particular, it is always easy to derive a lower bound on those variables from the existing conditions, but the existing conditions alone are not sufficient in obtaining non-trivial upper bounds.

We conclude by providing a concrete example that demonstrates how all the conditions required by Theorem 3.1 can be met in a real-world implementation. Consider any number $r$ of sensor types, and pick any probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for all $i = 1, \ldots, r$. Set

$P_n = n \log n$, and use

$$K_{1,n} = \frac{(\log n)^{1/2+\varepsilon}}{\sqrt{\alpha_{min}(n)}} \quad \text{and} \quad K_{r,n} = \frac{(1+\varepsilon)(\log n)^{3/2-\varepsilon}}{\mu_r \sqrt{\alpha_{min}(n)}}$$

with any $\varepsilon > 0$. Other key ring sizes $K_{1,n} \leq K_{2,n}, \ldots, K_{r-1,n} \leq K_{r,n}$ can be picked arbitrarily. For simplicity, assume that $\lambda_1(n) = o(1)$; thus, we have $p_{1j}(n) \sim \frac{K_{1,n}K_{j,n}}{P_n}$ [7, Lemma 4.2]. It follows from Theorem 3.1 that the resulting network will be connected whp. Of course, there are many other parameter scalings that one can choose.

### B. Comparison with related work

Theorem 3.1 complements the zero-one law established in [24, Thm. 3.1] for the property that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ has no *isolated* node. In particular, Theorem 3.1 establishes the conjecture appeared in [24] which states that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ would admit a zero-one law for connectivity with the critical scaling given by (5), possibly under additional conditions than needed for the property of absence of isolated nodes. Our result confirms the validity of the conjecture and specifies the additional conditions required for $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ to be connected whp.

Theorem 3.1 also generalizes the results established in [13] concerning the connectivity of the inhomogeneous random key graph intersecting the *homogeneous* (i.e., the standard) ER graph. There, authors considered a homogeneous channel model, wherein the communication channel between any two nodes (regardless of their respective classes) is on with probability $\alpha$ or off with probability $1 - \alpha$. In particular, authors considered a random graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$ formed by the intersection of the inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ with the standard ER graph $\mathbb{G}(n; \alpha)$ [25] and presented conditions on how to scale the parameters of $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$ so that it is connected whp. Our paper considers a more general channel model, namely a *heteregenous* channel model, where the channel between a node of class-$i$ and a node of class-$j$ is *on* with probability $\alpha_{ij}$ or *off* with probability $1 - \alpha_{ij}$ independently from others. Indeed, by setting $\alpha_{ij}(n) = \alpha(n)$ for $i, j = 1, 2, \ldots, r$ and $n = 1, 2, \ldots$, our results cover the results established in [13] regarding the connectivity of $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$. By allowing the probability of channel existence to vary with the class of the participating nodes, our model captures the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics.

The inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ was introduced by Yağan in [7]. There, zero-one laws for the property that the graph has no isolated nodes and the property that the graph is connected were established assuming that all communication links are reliable; i.e., *on*. Such an assumption fails to capture the cases when communication links between nodes fail due to battery depletion, jamming attacks, or deep fading. In fact, by setting $\alpha_{ij}(n) = 1$ for $i, j = 1, \ldots, r$ and each $n = 1, 2, \ldots$, our results reduce to those given in [7].

We remark that our results are not limited in scope to the secure connectivity problem of WSNs, but they can be useful in a diverse set of network applications where multiple conditions are required for participating agents to communicate; e.g., see [18] for specific examples.

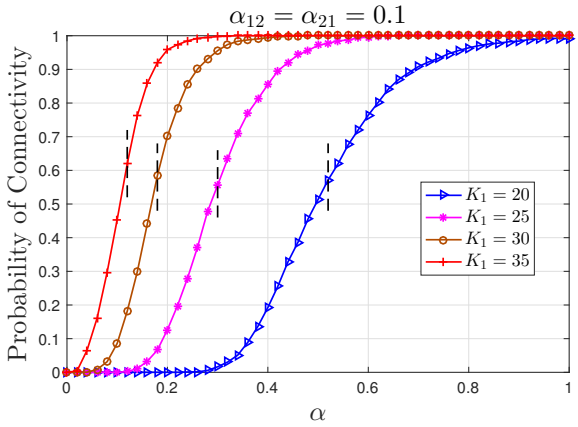


Fig. 1. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected for with $n = 500$, $P = 10^4$, $\alpha_{12} = \alpha_{21} = 0.1$, and $\alpha_{11} = \alpha_{22} = \alpha$. The empirical probability is obtained by averaging over 400 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.1.

## 4. Numerical Results

In this section, we present numerical results that support Theorem 3.1 in the finite node regime. In all experiments, we fix the number of nodes at $n = 500$, the size of the key pool at $P = 10^4$, and let $r = 2$ with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For better visualization, we use the curve fitting tool of MATLAB.

In Figure 1, we set the channel probability matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha & 0.1 \\ 0.1 & \alpha \end{bmatrix},$$

and consider four different values for $K_1$ while setting $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \boldsymbol{\alpha})$, we generate 400 independent samples of the graph $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ and count the number of times (out of a possible 400) that the obtained graphs are connected. Dividing the counts by 400, we obtain the (empirical) probabilities for the event of interest. For each value of $K_1$, we show the critical threshold of connectivity "predicted" by Theorem 3.1 by a vertical dashed line. More specifically, the vertical dashed lines stand for the minimum value of $\alpha$ that satisfies

$$\Lambda_m(n) = \sum_{j=1}^{2} \mu_j \alpha_{mj} \left( 1 - \frac{\binom{P-K_j}{K_m}}{\binom{P}{K_m}} \right) > \frac{\log n}{n}. \qquad (6)$$

We see that critical values of $\alpha$ obtained by (6) lie near the middle of the probability transition interval. We note that for each parameter pair $(\boldsymbol{K}, \boldsymbol{\alpha})$ in Fig 1, we have $\Lambda_m = \Lambda_1$.

In Figure 2, we set the channel probability matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & \alpha \\ \alpha & 0.2 \end{bmatrix},$$

and consider $\alpha = 0.3$, $\alpha = 0.5$, and $\alpha = 0.7$. We vary the parameter $K_1$ from 10 to 35, and set $K_2 = K_1 + 5$. Using the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected. As before, the critical threshold of connectivity asserted by Theorem 3.1 is shown by a vertical dashed line in each curve.

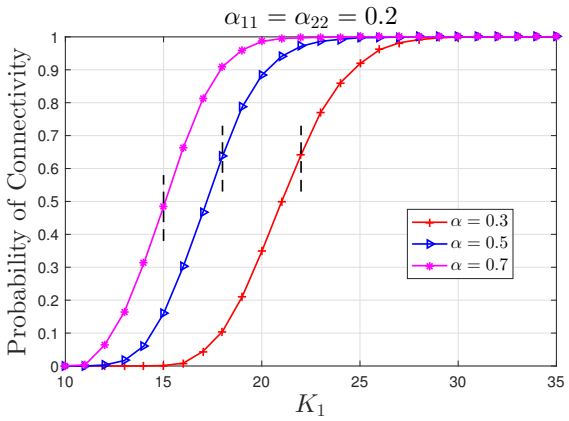


Fig. 2. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected as a function of $\boldsymbol{K}$ for $\alpha = 0.3$, $\alpha = 0.5$, and $\alpha = 0.7$ with $n = 500$ and $P = 10^4$; in each case, $\alpha_{11} = \alpha_{22} = 0.2$, and $\alpha_{12} = \alpha_{21} = \alpha$. The empirical probability value is obtained by averaging over 400 experiments.

In Figure 3, we set the channel probability matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{11} & 0.15 \\ 0.15 & 0.15 \end{bmatrix}$$

and consider four different $K_1$ values where $K_2 = K_1 + 5$ in each case. Varying $\alpha_{11}$ from 0 to 1 and using the same procedure with Figure 1, we obtain the empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected. An interesting observation about Figure 3 is how the probability of connectivity behaves as $\alpha_{11}$ increases. For instance, we see that the probability of connectivity is monotonically increasing with $\alpha_{11}$ until a certain point is reached, then it stays relatively constant afterwards. This can be explained by the fact that when $\alpha_{11}$ exceeds a certain value (while $\alpha_{12}$, $\alpha_{21}$, and $\alpha_{22}$ are fixed), the minimum mean degree changes from being $\Lambda_1$ to $\Lambda_2$ (see (3)); i.e., $\Lambda_m$ changes from $\Lambda_1$ to $\Lambda_2$. From that point onward, $\Lambda_m$ is independent of the specific value of $\alpha_{11}$ and the probability of connectivity remains constant, confirming the form of the critical scaling condition (5).

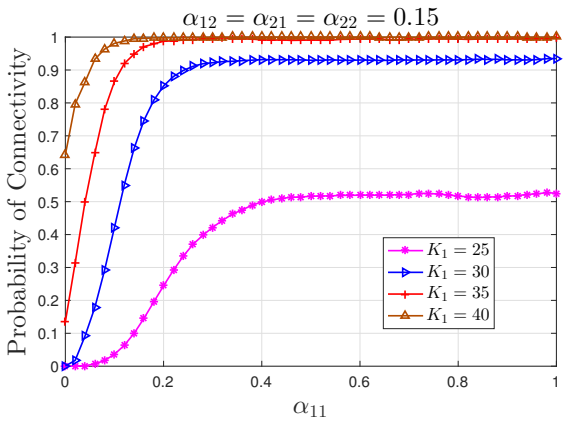


Fig. 3. Empirical probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected as a function of $\alpha_{11}$ for $K_1 = 25$, $K_1 = 30$, $K_1 = 35$, and $K_1 = 40$, with $n = 500$ and $P = 10^4$; in each case, $\alpha_{12} = \alpha_{21} = \alpha_{22} = 0.15$ . The empirical probability value is obtained by averaging over 1000 experiments.

## ACKNOWLEDGMENT

This work has been supported in part by National Science Foundation through grant CCF-1617934.

## REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004. [Online]. Available: http://doi.acm.org/10.1145/990680.990707

[3] X. Du and H.-H. Chen, "Security in wireless sensor networks," *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60–66, Aug 2008.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of ACM CCS 2002*, pp. 41–47.

[5] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds., *Wireless Sensor Networks*, Norwell, MA, USA, 2004.

[6] S. A. Çamtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, pp. 05–07, 2005.

[7] O. Yağan, "Zero-one laws for connectivity in inhomogeneous random key graphs," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4559–4574, Aug 2016.

[8] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proc. of IEEE INFOCOM 2005*, vol. 2, March 2005, pp. 878–890.

[9] O. Yağan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2983–2999, 2012.

[10] J. Zhao, O. Yağan, and V. Gligor, "k-connectivity in random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3810–3836, July 2015.

[11] L. Devroye and N. Fraiman, "Connectivity of inhomogeneous random graphs," *Random Structures & Algorithms*, vol. 45, no. 3, pp. 408–420, 2014.

[12] B. Bollobás, S. Janson, and O. Riordan, "The phase transition in inhomogeneous random graphs," *Random Structures and Algorithms*, vol. 33, no. 1, pp. 3–122, 2007.

[13] R. Eletreby and O. Yağan, "Reliability of wireless sensor networks under a heterogeneous key predistribution scheme," April 2016, available online at https://arxiv.org/abs/1604.00460.

[14] O. Yağan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3821–3835, June 2012.

[15] J. Zhao, O. Yağan, and V. Gligor, "On the strengths of connectivity and robustness in general random intersection graphs," in *53rd Annual Conference on Decision and Control*. IEEE, 2014, pp. 3661–3668.

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

[17] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic analysis, control, optimization and applications*. Springer, 1999, pp. 547–566.

[18] R. Eletreby and O. Yağan, "Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs," available online at http://www.andrew.cmu.edu/user/reletreb/papers/ISIT17Full.pdf.

[19] A. M. Makowski and O. Yağan, "On the eschenauer-gligor key predistribution scheme under on-off communication channels: The absence of isolated nodes," in *53rd Annual Allerton Conference on Communication, Control, and Computing*, Sept 2015, pp. 1494–1501.

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

[21] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 3, pp. 13:1–13:22, Mar. 2008.

[22] A. Mei, A. Panconesi, and J. Radhakrishnan, "Unassailable sensor networks," in *Proceedings of ACM SecureComm*, 2008, pp. 1–10.

[23] O. Yağan and A. M. Makowski, "Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?" *IEEE/ACM Transactions on Networking*, vol. 24, no. 6, pp. 3383–3396, December 2016.

[24] R. Eletreby and O. Yağan, "Node isolation of secure wireless sensor networks under a heterogeneous channel model," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2016.

[25] B. Bollobás, *Random Graphs*, 2nd ed. Cambridge University Press, 2001, cambridge Books Online. [Online]. Available: http://dx.doi.org/10.1017/CBO9780511814068