Connectivity of Wireless Sensor Networks Secured by Heterogeneous Key Predistribution Under an On/Off Channel Model

Rashad Eletreby, Student Member, IEEE, and Osman Yaşan, Senior Member, IEEE

Abstract—We investigate the connectivity of a wireless sensor network (WSN) secured by the heterogeneous key predistribution scheme under an independent on/off channel model. The heterogeneous scheme induces an inhomogeneous random key graph, denoted by $K(n;\mu,K,P)$ and the on/off channel model induces an Erdős-Rényi graph, denoted by $\mathbb{E}(n,\alpha)$. Hence, the overall random graph modeling the WSN is obtained by the intersection of $K(n;\mu,K,P)$ and $\mathbb{E}(n,\alpha)$. We present conditions on how to scale the parameters of the intersecting graph with respect to the network size $n$ such that the graph i) has no isolated nodes and ii) is connected, both with high probability (whp) as the number of nodes gets large. Our results are supported by a simulation study demonstrating that i) despite their asymptotic nature, our results can in fact be useful in designing finite-node WSNs so that they achieve secure connectivity whp; and ii) despite the simplicity of the on/off communication model, the probability of connectivity in the resulting WSN approximates very well the case where the disk model is used.

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

I. INTRODUCTION

A. Wireless Sensor Networks (WSNs) and Security

WSNs emerged as an enabling platform for a broad range of application areas owing to their low-cost, low-power, small size, and adaptability to the physical environment [1]. These unique features triggered the proliferation and adoption of WSNs in several domains including military, health, and environment, but also gave rise to unique security challenges that cannot be tackled using classical security mechanisms [2]. In particular, asymmetric cryptosystems provide a scalable solution for securing large scale WSNs; however, they are generally slow and lead to excessive energy and memory consumption. On the other hand, symmetric cryptosystems were shown to be superior in terms of speed and energy efficiency, but they demand novel and efficient mechanisms for key-establishment among sensor nodes [3], [4]. In principle, an efficient key-establishment mechanism should result in a securely connected topology, i.e., a network where there exists a secure communication path (possibly multihop) between every pair of nodes allowing the exchange of data and control messages, while conforming to the typical limitations of WSNs. Also, it shall not assume knowledge of postdeployment configuration, since in most cases WSNs are deployed randomly in large numbers.

In their seminal work, Eschenauer and Gligor proposed a random key predistribution protocol as a practical and efficient method for key-establishment in large scale WSNs [3]. Their scheme, hereafter referred to as the EG scheme, operates as follows: before deployment, each node is given a random set of $K$ cryptographic keys, selected uniformly (without replacement) from a large key pool of size $P$. After deployment, two nodes can communicate securely over an existing channel if they share at least one key.\(^1\) The EG scheme is currently regarded as one of the most feasible solutions for key-establishment among sensor nodes, e.g., see [5, Ch. 13], [6], and references therein, and has led the way to several other variants, including the $q$-composite scheme [4], the random pairwise scheme [4], and many others.

The EG scheme inherently assumes that all nodes are homogeneous in terms of their roles and capabilities, hence they are assigned the same number $K$ of keys. However, emerging WSN applications are complex and are envisioned to require the coexistence of different classes of nodes with different roles and capabilities [7]. For instance, a particular class of nodes may act as cluster heads that are used to connect several clusters of nodes together. These cluster heads need to communicate with a large number of nodes in their vicinity and they are also expected to be more powerful than regular nodes. Thus, more keys should be given to the cluster heads to ensure high levels of connectivity and security.

To cope with the expected heterogeneity in WSN topologies, Yaşan proposed a new variation of the EG scheme, referred to as the heterogeneous random key predistribution scheme [8].

\(^1\)There are multiple reasons why node-to-node encryption/decryption is vital to WSNs. First, each node broadcasts an encrypted packet which contains the entire header info; i.e., source and destination addresses are encrypted. Hence, each packet has to be decrypted to be routed. Furthermore, the lack of a trusted third party induces the need for shared-keys between nodes to ensure the authenticity of communication among them [4].
The heterogeneous scheme considers the case when the network includes sensors with varying levels of resources, features, security, or connectivity requirements. The scheme is described as follows. Given \( r \) classes, each sensor is independently classified as a class-\( i \) node with probability \( \mu_i > 0 \) for each \( i = 1, \ldots, r \). Then, sensors in class-\( i \) are each assigned \( K_i \) keys selected uniformly at random from a key pool of size \( P \). Similar to the EG scheme, nodes that share at least one common key (regardless of their class) can communicate securely over an available channel after deployment.

Given the randomness involved in the EG scheme and the heterogeneous scheme, there is a positive probability that a pair of nodes may have no common key, thus cannot establish a secure communication link in between. Moreover, two nodes that share a key may not have a wireless channel in between (possibly because of the limited transmission radius). Hence, it is natural to ask whether the resulting network would be securely connected or not. Specifically, two nodes are securely connected if they share a key and have a communication channel in between. A network is said to be connected if there is a path between every pair of vertices. In essence, one needs to know if it is possible to control the parameters of the scheme (possibly as functions of the network size \( n \)), such that the resulting network is connected with high probability (whp). Indeed, there is a fundamental interplay between the security and connectivity of the resulting network. To see this, consider the classical EG scheme where all nodes receive the same number of keys \( K \) from a key pool of size \( P \). Note that when an adversary captures one node, a \( K/P \) fraction of the key pool is revealed to the adversary allowing her to compromise secure communications. Thus, from a security standpoint, it is better to minimize the fraction \( K/P \) to improve the resiliency of the network against node capture attacks [9]. However, it is clear that from a connectivity standpoint, it is always better to increase \( K \) or decrease \( P \) (thus increasing the fraction \( K/P \)), to make it more likely for two nodes to end up sharing a key. That is why it is crucial to know the exact minimum conditions required to achieve the desired level of connectivity by means of a sharp zero-one law -Only then we can avoid overshooting the parameters and losing from resiliency.

In [8], Yağan considered a WSN secured by the heterogeneous scheme under full-visibility assumption, i.e., all pairs of sensors have a communication channel in between, hence the only condition for two nodes to be connected is to share a key. Therein, they established scaling conditions on the parameters of the heterogeneous scheme as functions of the network size \( n \) such that the resulting network is connected whp as the number of nodes gets large. In particular, they considered a random graph model naturally induced by the heterogeneous scheme and established scaling conditions on the model parameters such that the resulting graph is connected whp as the number of nodes gets large. Specifically, with \( K = \{K_1, K_2, \ldots, K_r\} \), \( \mu = \{\mu_1, \mu_2, \ldots, \mu_r\} \), and \( n \) denoting the network size, we let \( \mathbb{K}(n; \mu, K, P) \) denote the random graph induced by the heterogeneous key predistribution scheme, where any pair of vertices are adjacent as long as they share a key.

The inhomogeneous random key graph models the shared-key connectivity of the WSN under the heterogeneous scheme.

Our paper is motivated by the fact that the full-visibility assumption is not likely to hold in real-world implementations of WSNs. In particular, the randomness of the wireless channel as well as limited transmission ranges would severely limit the availability of wireless channels between nodes, rendering two nodes disconnected even when they share a key. In fact, as wireless connectivity comes into play, an essential question arises: Under a given model for wireless connectivity, is it possible to control the parameters of the heterogeneous scheme to ensure that the resulting network is connected?

The rest of the introduction is devoted to answering the aforementioned question, hence bridging the disconnect between the model developed in [8] and real world implementations of WSNs where wireless channels are scarce and the full-visibility assumption does not hold. In Section 1.B, we start by exploring different random graph models that can be used to model the wireless connectivity of the network. We explain our rationale behind choosing the on/off channel model (that induces an Erdős–Rényi (ER) graph \( \mathbb{H}(n; \alpha) \)) as our model for the wireless connectivity of the network. Then, we show that the overall model for the WSN is given by the intersection of \( \mathbb{K}(n; \mu, K, P) \) with \( \mathbb{H}(n; \alpha) \), namely \( \mathbb{K}(n; \mu, K, P) \cap \mathbb{H}(n; \alpha) \). Finally, in Section 1.C, we summarize our contributions and introduce our notations.

### B. Modeling Wireless Connectivity

We model the wireless connectivity of the WSN, say using a (possibly random) graph \( \mathbb{I}(n; \cdot) \), whose edges represent pairs of sensors who have a wireless communication channel available in between. The overall model of the WSN will then be an intersection of \( \mathbb{K}(n; \mu, K, P) \) and \( \mathbb{I}(n; \cdot) \) since a pair of sensors can establish a secure communication link if they share a key and have a wireless channel available. Let \( \mathcal{G} \) be the intersecting graph, i.e., \( \mathcal{G} := \mathbb{K}(n; \mu, K, P) \cap \mathbb{I}(n; \cdot) \). At a high level, our objective is to establish scaling conditions on the parameters of \( \mathcal{G} \) such that the resulting graph is connected whp as the number of nodes gets large.

In practice, limited transmission range of sensors significantly impacts the wireless connectivity of a WSN, hence the disk model [10] can be seen as a good candidate model for wireless connectivity among sensor nodes. The disk model is described as follows. Assuming that nodes are distributed over a bounded region \( D \) of a euclidean plane, nodes \( v_i \) and \( v_j \) located at \( x_i \) and \( x_j \), respectively, are able to communicate if \( \| x_i - x_j \| < \rho \), where \( \rho \) denotes the transmission radius. A special case of the disk model when node locations are independently and uniformly distributed over the region \( D \), gives rise to the random geometric graph [11], hereafter denoted \( \mathbb{I}(n; \rho) \). Now, let \( \mathcal{G}(n; \mu, K, P, \rho) \) be a random graph obtained by intersecting the inhomogeneous random key graph \( \mathbb{K}(n; \mu, K, P, \cdot) \) with a random geometric graph \( \mathbb{I}(n; \rho) \). Clearly, \( \mathcal{G}(n; \mu, K, P, \rho) \) represents a reasonably accurate model for a WSN secured by the heterogeneity scheme, where two nodes are connected if they i) share a key, and ii) are within transmission radius.
Unfortunately, analyzing the connectivity of $G(n, \mu, K, P, \rho)$ is likely to be very challenging. In fact, the Gupta–Kumar conjecture [10] on the connectivity of $H(n; \rho) \cap H(n; \rho)$ where $H(n; \rho)$ represents an ER graph, took many years (and several attempts) to be resolved eventually by Penrose [12]; see [13] for a detailed discussion on the difficulties involved in analyzing intersection of different types of graphs. The model $\mathbb{K}(n; \mu, K, P)$ considered here is much more complicated than an ER graph due to edge correlations [8], leading to the following important question: Is there any communication model that provides a good approximation of the classical disk model, but also allows a comprehensive analysis of the resulting intersecting graph?

This question was answered in the affirmative in [13], where it was shown that an independent on/off channel model provides a good approximation of the disk model for understanding the critical scalings of connectivity in settings similar to ones we consider here. In the independent on/off channel model, the wireless channel between any given pair of nodes is either on (with probability $\alpha$) or off (with probability $1 - \alpha$) independently from all other channels. The model induces an ER graph $H(n; \alpha)$, where an edge exists (respectively does not exist) between two vertices with probability $\alpha$ (respectively $1 - \alpha$) independently from all other edges.

With these in mind, we model the wireless connectivity of the WSN by an ER graph $H(n; \alpha)$ and study the connectivity of the intersecting graph $G(n; \mu, K, P, \alpha) := \mathbb{K}(n; \mu, K, P) \cap H(n; \alpha)$. This approach allows us to i) establish rigorous results concerning the connectivity of a WSN albeit using a simplified wireless communication model, and ii) demonstrate via simulations that these results still apply under the more realistic disk model. In Section 4, we provide simulation results indicating that the connectivity of $\mathbb{K}(n; \mu, K, P) \cap H(n; \alpha)$ behaves very similar to that of $\mathbb{K}(n; \mu, K, P) \cap H(n; \rho)$, as we match $\alpha$ and $\rho$ leading to the same probability of wireless channel availability; i.e., $\alpha = \pi \rho^2$.

C. Contributions

We investigate the connectivity of a WSN secured by the heterogeneous key predistribution scheme under an independent on/off channel model. The heterogeneous scheme induces an inhomogeneous random key graph, denoted by $\mathbb{K}(n; \mu, K, P)$ and the on/off channel model induces a random graph, denoted by $H(n, \alpha)$. Hence, the overall random graph modeling the WSN is obtained by the intersection of $\mathbb{K}(n; \mu, K, P)$ and $H(n, \alpha)$. We denote this intersection by $G(n; \mu, K, P, \alpha)$, i.e., $G(n; \mu, K, P, \alpha) := \mathbb{K}(n; \mu, K, P) \cap H(n, \alpha)$. We present conditions on how to scale the parameters of $G(n; \mu, K, P, \alpha)$ with respect to the network size $n$ such that i) it has no isolated nodes and ii) it is connected, both whp as the number of nodes gets large. The results are given in the form of zero-one laws with critical scalings precisely established. This maps to dimensioning the parameters of the heterogeneous scheme with respect to the network size $n$ and the channel parameter $\alpha$ such that the resulting network is securely connected.

Our results are supported by a simulation study (see Section 4) demonstrating that i) despite their asymptotic nature, our results can in fact be useful in designing finite-node WSNs so that they achieve secure connectivity whp; and ii) despite the simplicity of the on/off communication model, the probability of connectivity in the resulting WSN approximates very well the case where the disk model is used. In addition, our results are shown to complement and generalize several previous work in the literature (see Section 3-A).

All limiting statements, including asymptotic equivalences are considered with the number of sensor nodes $n$ going to infinity. The indicator function of an event $E$ is denoted by $1[E]$. We say that an event holds whp if it holds with probability 1 as $n \to \infty$. In comparing the asymptotic behavior of the sequences $\{a_n\}, \{b_n\}$, we use the standard Landau notation, e.g., $a_n = o(b_n)$, $a_n = \omega(b_n)$, $a_n = \Omega(b_n)$, and $a_n = \Theta(b_n)$. We also use $a_n \sim b_n$ to denote the asymptotic equivalence $\lim_{n \to \infty} a_n / b_n = 1$.

II. System Model

The heterogeneous random key predistribution scheme introduced in [8] works as follows. Consider a network of $n$ sensors labeled as $v_1, v_2, \ldots, v_n$. Each sensor node is classified into one of the $r$ classes (e.g., priority levels) according to a probability distribution $\mu = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and $\sum_{i=1}^r \mu_i = 1$. Then, a class-$i$ node is assigned $K_i$ cryptographic keys selected uniformly at random from a key pool of size $P$. It follows that the key ring $\Sigma_x$ of node $v_x$ is a random variable (rv) with

$$P[\Sigma_x = S \mid t_x = i] = \left( \frac{P}{K_i} \right)^{-1}, \quad S \in \mathcal{P}_K,$$

where $t_x$ denotes the class of $v_x$ and $\mathcal{P}_K$ is the collection of all subsets of $\{1, \ldots, P\}$ with size $K$. The classical key predistribution scheme of Eschenauer and Gligor [3] constitutes a special case of this model with $r = 1$, i.e., when all sensors belong to the same class and receive the same number of keys; see also [14].

Let $K = \{K_1, K_2, \ldots, K_r\}$ and assume without loss of generality that $K_1 \leq K_2 \leq \cdots \leq K_r$. Consider a random graph $\mathbb{K}$ induced on the vertex set $V = \{v_1, \ldots, v_n\}$ such that a pair of nodes $v_x$ and $v_y$ are adjacent, denoted by $v_x \sim v_y$, if they have at least one cryptographic key in common, i.e.,

$$v_x \sim v_y \quad \text{if} \quad \Sigma_x \cap \Sigma_y \neq \emptyset. \quad (1)$$

The adjacency condition (1) defines the inhomogeneous random key graph denoted by $\mathbb{K}(n; \mu, K, P)$ [8]. This model is also known in the literature as the general random intersection graph; e.g., see [15] and [16]. The probability $p_{ij}$ that a class-$i$ node and a class-$j$ node are adjacent is given by

$$p_{ij} = P[v_x \sim v_y \mid t_x = i, t_y = j] = 1 - \left( \frac{P - K_j}{K_j} \right) \left( \frac{K_i}{K_j} \right) \quad (2)$$

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we have $p_{ij} = 1$. Let $\lambda_i$ denote the mean probability that a class-$i$ node
is connected to another node in $\mathbb{K}(n; \mu, K, P)$. We have
\[
\lambda_i = P[v_x \sim_{\mathbb{K}} v_y \mid t_x = i] = \sum_{j=1}^{r} p_{ij} \mu_j.
\] (3)
We also find it useful to define the mean key ring size by $K_{\text{avg}}$; i.e.,
\[
K_{\text{avg}} = \sum_{j=1}^{r} K_j \mu_j.
\] (4)

We model the wireless connectivity of the WSN by means of an independent on/off channel model. In particular, the channel between any given pair of nodes is either on with probability $\alpha$ or off with probability $1 - \alpha$. More precisely, let $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$ denote i.i.d Bernoulli rvs, each with success probability $\alpha$. The communication channel between two distinct nodes $v_x$ and $v_y$ is on (respectively, off) if $B_{xy}(\alpha) = 1$ (respectively, if $B_{xy}(\alpha) = 0$). The on/off channel model induces a standard ER graph $\mathbb{H}(n; \alpha)$ [17], defined on the vertices $V = \{v_1, \ldots, v_n\}$ such that $v_x$ and $v_y$ are adjacent, denoted by $v_x \sim_{\mathbb{H}} v_y$, if $B_{xy}(\alpha) = 1$.

We model the overall topology of a WSN by the intersection of an inhomogeneous random key graph $\mathbb{K}(n; \mu, K, P)$ with an ER graph $\mathbb{H}(n; \alpha)$. Namely, nodes $v_x$ and $v_y$ are adjacent in $\mathbb{K}(n; \mu, K, P)$ and $\mathbb{H}(n; \alpha)$, if and only if they are adjacent in both $\mathbb{K}$ and $\mathbb{H}$. Hence, the edges in the intersection graph $\mathbb{K}(n; \mu, K, P) \cap \mathbb{H}(n; \alpha)$ represent pairs of sensors that can securely communicate since they have i) a communication link available in between, and ii) a shared cryptographic key. Therefore, studying the connectivity properties of $\mathbb{K}(n; \mu, K, P) \cap \mathbb{H}(n; \alpha)$ amounts to studying the secure connectivity of heterogeneous WSNs under the on/off channel model.

Hereafter, we denote the intersection graph $\mathbb{K}(n; \mu, K, P) \cap \mathbb{H}(n; \alpha)$ by $\mathbb{G}(n; \mu, K, P, \alpha)$. To simplify the notation, we let $\Theta = (K, P)$, and $\Theta = (\theta, \alpha)$. The probability of edge existence between a class-$i$ node $v_x$ and a class-$j$ node $v_y$ in $\mathbb{G}(n; \Theta)$ is given by
\[
P[v_x \sim_{\mathbb{G}} v_y \mid t_x = i, t_y = j] = \frac{\lambda_i}{\lambda_i} \alpha p_{ij}
\] by independence. Similar to (3), the mean edge probability for a class-$i$ node in $\mathbb{G}(n; \mu, \Theta)$ as $\Lambda_i$ is given by
\[
\Lambda_i = \sum_{j=1}^{r} \mu_j \alpha p_{ij} = \alpha \lambda_i, \quad i = 1, \ldots, r.
\] (5)

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 $n$.

### III. MAIN RESULTS AND DISCUSSION

We refer to a mapping $\Theta = K_1, \ldots, K_r, P, \alpha : N_0 \rightarrow N_0^{r+1} \times (0, 1)$ as a scaling if
\[
1 \leq K_{1,n} \leq K_{2,n} \leq \cdots \leq K_{r,n} \leq P_n/2
\] (6)
for all $n = 2, 3, \ldots$. We note that under (6), the edge probability $p_{ij}$ is given by (2).

#### A. Results

We first present a zero-one law for the absence of isolated nodes in $\mathbb{G}(n; \mu, \Theta)$.

**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 $\Theta : N_0 \rightarrow N_0^{r+1} \times (0, 1)$ such that
\[
\Lambda_1(n) = \alpha_n \lambda_1(n) \sim \frac{\log n}{n}
\] (7)
for some $c > 0$. We have
\[
\lim_{n \rightarrow \infty} \mathbb{P}[\mathbb{G}(n; \mu, \Theta_n) \text{ has no isolated nodes}] = \begin{cases} 0 & \text{if } c < 1 \\ 1 & \text{if } c > 1. \end{cases}
\] (8)
The scaling condition (7) will often be used in the form
\[
\Lambda_1(n) = c_n \frac{\log n}{n}, \quad n = 2, 3, \ldots
\] (9)
with $\lim_{n \rightarrow \infty} c_n = c > 0$.

Next, we present an analogous result for 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 $\Theta : N_0 \rightarrow N_0^{r+1} \times (0, 1)$ such that (7) holds for some $c > 0$. Then, we have
\[
\lim_{n \rightarrow \infty} \mathbb{P}[\mathbb{G}(n; \mu, \Theta_n) \text{ is connected}] = \begin{cases} 0 & \text{if } c < 1 \\ 1 & \text{if } c > 1 \end{cases}
\] (10)
under the additional conditions that
\[
P_n = \Omega(n)
\] (11)
\[
p_{11}(n) = \omega\left(\frac{1}{n\alpha_n}\right).
\] (12)

The resemblance of the results presented in Theorems 3.1 and 3.2 indicates that absence of isolated nodes and connectivity are asymptotically equivalent properties for $\mathbb{G}(n; \mu, \Theta_n)$. Similar observations were made for other well-known random graph models as well; e.g., inhomogeneous random key graphs [8], ER graphs [17], and (homogeneous) random key graphs [14].

Conditions (11) and (12) are enforced mainly for technical reasons and they are only needed in the proof of the one-law of Theorem 3.2. In particular, condition (11) is essential for real-world WSN implementations in order to ensure the resilience of the network against node capture attacks; e.g., see [3] and [9]. 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 [18] and would be deemed as vulnerable against adversarial attacks.

Also, condition (12) 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 (7) merely
scales the minimum mean edge probability, not the minimum (or each) edge probability, as $\log n/n$. For instance, the current scaling condition (7) gives us an easy upper bound on the minimum edge probability in the network, but does not specify any nontrivial lower bound on that probability. More specifically, it is easy to see that $\alpha_n p_{11}(n) = O(1)$ and $O(\log n/n)$, but it is not clear if the sequence $\alpha_n p_{11}(n)$ has a nontrivial lower bound. It is generally desirable to provide nontrivial bounds on the edge probabilities of a given random graph to facilitate the proof of the zero-one law for connectivity. For instance, Devroye and Fraiman investigated the connectivity of an inhomogeneous ER graph [19], under the condition that the probability of an edge connecting two nodes of classes $i$ and $j$ scales as $\kappa(i, j) \log n/n$, where $\kappa(i, j)$ returns a positive real number for each pair $(i, j)$, i.e., each individual edge was scaled as $\Theta(\log n/n)$. Finally, we note that $K_{1,n}^2/P_n = \Omega(p_{11}(n))$ by virtue of [14, Lemma 7.1–7.2]. Thus, condition (12) also implies that $\alpha_n K_{1,n}^2 / P_n = o(1/n)$.

In summary, condition (11) is needed to ensure the resilience of the network against node capture attacks, while condition (12) is needed to provide a nontrivial lower bound on the minimum edge probability of the network. To provide a concrete example, one can set $P_n = n \log n$ and have $K_{1,n} = (\log n)^{1/2+\varepsilon}$ with any $\varepsilon > 0$ to satisfy (12) for any $\alpha_n \geq 1/(\log n)^\varepsilon$ (see [20, Lemma A.1]). In this case, setting $K_{\text{avg},n} = (\log n)^{3/2}$ ensures that the resulting network is connected whp (see Corollary 3.3).

Theorem 3.1 (resp. Theorem 3.2) states that $\mathbb{G}(n; \mu, \Theta_n)$ has no isolated node (resp. is connected) whp if the mean degree of class-1 nodes (that receive the smallest number $K_{1,n}$ of keys) is scaled as $(1 + \varepsilon) \log n$ for some $\varepsilon > 0$. On the other hand, if this minimal mean degree scales as $(1 - \varepsilon) \log n$ for some $\varepsilon > 0$, then whp $\mathbb{G}(n; \mu, \Theta_n)$ has an isolated node, and hence not connected. These results indicate that the minimum key ring size in the network has a significant impact on the connectivity of $\mathbb{G}(n; \mu, \Theta_n)$.

The importance of the minimum key ring size on connectivity can be seen more explicitly under a mild condition on the scaling, as shown in the next corollary.

**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 $\Theta : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1]$ such that $\lambda_1(n) = o(1)$ and

$$\alpha_n \frac{K_{1,n}}{P_n} \sim c \frac{\log n}{n}$$

for some $c > 0$, where $K_{\text{avg},n}$ is as defined at (4). Then, we have the zero-one law (8) for absence of isolated nodes. If, in addition, the conditions (11) and (12) are satisfied, then we also have the zero-one law (10) for connectivity.

**Proof:** In view of (3), we see that $\lambda_1(n) = o(1)$ implies $p_{1j}(n) = o(1)$ for $j = 1, \ldots, r$. From [20, Lemma A.1], this then leads to $p_{1j}(n) \sim K_{1,n} K_{1,n} / P_n$,

$$\lambda_1(n) = \sum_{j=1}^r \mu_j p_{1j}(n) \sim \frac{K_{1,n}}{P_n} \sum_{j=1}^r \mu_j = \frac{K_{1,n} K_{\text{avg},n}}{P_n}.$$ 

Thus, the scaling conditions (7) and (13) are equivalent under $\lambda_1(n) = o(1)$ and Corollary 3.3 follows from Theorem 3.1 and Theorem 3.2.

We see from Corollary 3.3 that for a fixed mean number $K_{\text{avg},n}$ of keys per sensor, network connectivity is directly affected by the minimum key ring size $K_{1,n}$. For example, reducing $K_{1,n}$ by half means that the smallest $\alpha_n$ for which the network becomes connected whp is increased by two-fold (see Fig. 2 for a numerical example demonstrating this phenomenon).

### B. Comparison With Related Work

Our main results extend the work in [8] and [21], where authors established zero-one laws for the connectivity of a WSN secured by the heterogeneous key predistribution scheme under the full-visibility assumption. Although a crucial first step in the study of heterogeneous key predistribution schemes, the assumption that all pairs of sensors have a communication channel in between is not likely to hold in most practical settings. In this regard, our work extends the results in [8] and [21] to more practical WSN scenarios where the wireless connectivity of the network is taken into account. By setting $\alpha_n = 1$ for each $n = 1, 2, \ldots$ (i.e., by assuming that all links are available), our results reduce to those given in [8].

Authors in [13] (respectively, [22]) investigated the connectivity (respectively, $k$-connectivity) of WSNs secured by the classical EG scheme under an independent on/off channel model. However, when the network consists of sensors with varying level of resources (e.g., computational, memory, power), and with varying level of security and connectivity requirements, it may no longer be sensible to assign the same number of keys to all sensors. Our work addresses this issue by generalizing [13] to the cases where nodes can be assigned different number of keys. When $r = 1$, i.e., when all nodes belong to the same class and receive the same number of keys, our result recovers the main result in [13].

### IV. Numerical Results

We now present numerical results to support Theorems 3.1 and 3.2 in the finite node regime. Furthermore, we show by simulations that the on/off channel model serves as a good approximation of the disk model. In our simulations, we fix the size of the key pool at $P = 10^4$ and fix $n = 500$ for Figs. 1 and 2.

The first step in comparing the on/off channel model to the disk model is to propose a matching between ER graph $\mathbb{H}(n; \alpha)$ and the random geometric graph $\mathbb{G}(n; \rho)$ in a way that leads to the same probability of link availability. In particular, consider 500 nodes distributed uniformly and independently over a folded unit square $[0, 1]^2$ with toroidal (continuous) boundary conditions. Since there are no border effects, we get

$$P[\|x_i - x_j\| < \rho] = \pi \rho^2, \quad i \neq j, \quad i, j = 1, \ldots, n$$

whenever $\rho < 0.5$. Thus, in order to match the two communication models we set $\alpha = \pi \rho^2$. Recall that $\mathbb{G}(n; \mu, \rho) = \mathbb{H}(n; \rho) \cap \mathbb{H}(n; \alpha)$, and let $\mathbb{G}(n; \mu, \rho) = \mathbb{H}(n; \rho) \cap \mathbb{H}(n; \alpha)$. Next, we present several simulation results...
Empirical probability that \( \pi \rho \) (represented by lines) and by Theorem 3.2 by a vertical dashed line for \( \pi \rho = \alpha \) (respectively, \( K \)). For each parameter \( \alpha = \tilde{\alpha} = 0 \) \( \alpha \) and we set \( \alpha \) (respectively, \( G-K \)).

\[
\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left( 1 - \frac{(\mu - K_1)}{(K_1)} \right) > \frac{1}{\alpha} \frac{\log n}{n}. \tag{14}
\]

According to Theorem 3.2, at this critical value of \( K_1 \) the network would be connected with probability 1 as the number of nodes tends to infinity. We see from Fig. 1 that even in the finite-node regime \( \alpha = 500 \), the critical value of \( K_1 \) results in a connected network whp.

Fig. 2 is generated in a similar manner with Fig. 1, this time with an eye toward understanding the impact of the minimum key ring size \( K_1 \) on network connectivity. We fix the number of classes at 2 with \( \mu = 0.5, 0.5 \) and consider four different key ring sizes \( K \) each with mean 40; we consider \( K = 10, 70, K = 20, 50, K = 30, 50, \) and \( K = 40, 40 \). We compare the probability of connectivity in the resulting networks as \( \alpha \) (respectively, \( \pi \rho \)) varies from zero to one. Although the average number of keys per sensor is kept constant in all four cases, network connectivity improves dramatically as the minimum key ring size \( K_1 \) increases; e.g., with \( \alpha = \pi \rho^2 = 0.2 \) the probability of connectivity is one when \( K_1 = K_2 = 40 \) while it drops to zero if we set \( K_1 = 10 \) and \( K_2 = 70 \) so that the mean key ring size is still 40. This confirms the observations made via Corollary 3.3.

Finally, we investigate the effect of the network size \( n \) on the probability of connectivity. Recall that our scaling condition is equivalent to

\[
\frac{K_{1,n} K_{\text{avg},n}}{P} \sim c \frac{\log n}{n}
\]

by virtue of Corollary 3.3. Thus, as we increase \( n \) for fixed \( P \) and \( \alpha \), the fraction \( \log n/n \) decreases, leading to a decrease on the critical value of \( K_{1,n} K_{\text{avg},n} \) needed to ensure that \( c > 1 \). We would also expect the probability of connectivity to exhibit a sharper transition between 0 and 1 as we increase \( n \) by virtue of Theorem 3.2. This is illustrated in Fig. 3.

V. OTHER APPLICATION AREAS: THE SPREAD OF EPIDEMICS AND INFORMATION IN SOCIAL NETWORKS

The last decade has witnessed a tremendous advance in our understanding of how information [23]–[25], influence [26], [27], and diseases [28], [29] propagate across the globe. A large variety of mathematical models as well as a multitude of datasets paved the way for predictions and control of the behavior of such spreading processes on complex networks. In particular, several generative models were proposed to create networks that resemble the structure of real-world complex networks, allowing for large-scale simulations and precise predictions of how a spreading process would behave in real-life. Three structural properties in particular, the power-law degree distribution, small-world, and clustering were shown to be prevalent in real-world social networks [30], [31].
The homogeneous random key graph (where all nodes receive the same number $K$ of objects) was shown to generate networks that are highly-clustered and of small diameter, hence small-world [32]. Indeed, the inhomogeneous counterpart $\mathbb{K}(n; \mu, K, P)$ intrinsically exhibits these two properties as well. In addition to that, one can tune the parameters of $\mathbb{K}(n; \mu, K, P)$ to generate networks with a power-law degree distribution similar to that observed in real-world social networks [33]. Collectively, the inhomogeneous random key graph $\mathbb{K}(n; \mu, K, P)$ generates networks that are small-world and have tunable degree distribution and clustering, hence it can be considered as a useful model for real-world social networks. In fact, the inhomogeneous random key graph is a natural model for common-interest social networks. A common interest relationship between two friends manifests from their selection of common interests or hobbies from a large pool [22]. Clearly, this can be modeled by an inhomogeneous random key graph, where each individual has a set of interests (possibly of different sizes) sampled from a large pool of interests and two individuals are connected if they happen to share an interest.

In addition, the intersection model $\mathbb{G}(n; \mu, K, P, \alpha)$ considered here can be useful in studying the propagation of epidemics or information on complex networks. A simple model for the spread of epidemics (or information) on complex networks is the so-called susceptible-infected-recovered (SIR) model. Therein, a disease is transmitted to a susceptible individual upon contact with an infected individual. Later on, infected individuals recover from the disease and gain immunity from it. The outbreak size is precisely the number of recovered individuals at the steady state. This model results in reasonable predictions for the cases where recovery grants lasting resistance. In [29], it was shown that under some conditions, the dynamics of the SIR model on a given network maps to a bond-percolation problem with the average transmissibility of the disease as the percolation parameter. Namely, with $\alpha$ being the average transmissibility; if we are to occupy each edge in the graph with probability $\alpha$, the final outbreak size would be the size of the cluster of vertices that can be reached from the initial infected vertex by traversing the occupied edges only [29]. Typically, one is interested in deriving the threshold value of $\alpha$ for which a giant connected component emerges, indicating that the disease has reached a positive fraction of the population. It would also be interesting to determine (in a computationally-efficient manner) whether or not a particular pair of vertices is connected [24], [25] in the bond-percolated network. Clearly, showing that a given pair of vertices is connected implies that a piece of information can propagate from one of these two vertices to the other, and reveals that they both belong to a single component of the underlying graph.

Intersecting the inhomogeneous random key graph $\mathbb{K}(n; \mu, K, P)$ with an ER graph $\mathbb{H}(n; \alpha)$ is essentially equivalent to occupying each edge of $\mathbb{K}(n; \mu, K, P)$ independently with probability $\alpha$. Hence, the scaling condition for which the one-law of Theorem 3.2 holds gives us a threshold value of $\alpha$ for which a strain of a disease or a piece of information would infect the entire population. In particular, let $\alpha_n := \log n / (n\lambda_1(n))$; if the average transmissibility of a disease $\alpha$ satisfies $\alpha_n > \alpha_n$, a single giant component containing all of the vertices emerge (because in this case the network is connected by virtue of Theorem 3.2), allowing the disease to infect each single vertex. Therefore, our results on the connectivity of $\mathbb{G}(n; \mu, K, P, \alpha)$ provide a threshold on the average transmissibility a disease should have (possibly through evolution) in order to persist in a given population modeled by the inhomogeneous random key graph.

VI. PROOF OF THEOREM 3.1

A. Preliminaries

Few technical results are collected here for convenience. A full list of preliminaries is given in [20, Appendix A]. The first result follows easily from the scaling condition (6). Proposition 6.1 ([8, Proposition 4.1]): For any scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^+$, we have [in view of (6)]

$$\lambda_1(n) \leq \lambda_2(n) \leq \cdots \leq \lambda_r(n)$$

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

Another useful bound that will be used throughout is

$$(1 \pm x) e^{\pm x}, \quad x \in [0, 1]$$

Finally, we find it useful to write

$$\log(1 - x) = -x - \Psi(x)$$

where $\Psi(x) = \int_0^x \frac{1}{1 - t} dt$. From L’Hôpital’s Rule, we have

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

B. Establishing the One-Law

The proof of Theorem 3.1 relies on the method of first and second moments applied to the number of isolated nodes in $\mathbb{G}(n; \mu, \Theta_n)$. Let $I_n(\mu, \Theta_n)$ denote the total number of isolated nodes in $\mathbb{G}(n; \mu, \Theta_n)$, namely,

$$I_n(\mu, \Theta_n) = \sum_{\ell=1}^n 1[\nu_\ell \text{ is isolated in } \mathbb{G}(n; \mu, \Theta_n)].$$
The method of first moment [34, eq. (3.10), p. 55] gives
\[ 1 - \mathbb{E}[\mathcal{I}_n(\mu, \Theta_n)] \leq \mathbb{P}[\mathcal{I}_n(\mu, \Theta_n) = 0]. \]

It is clear that in order to establish the one-law, namely that
\[ \lim_{n \to \infty} \mathbb{P}[\mathcal{I}_n(\mu, \Theta_n) = 0] = 1, \]
we need to show that
\[ \lim_{n \to \infty} \mathbb{E}[\mathcal{I}_n(\mu, \Theta_n)] = 0. \] (20)

Recalling (19), we have
\[
\mathbb{E}[\mathcal{I}_n(\mu, \Theta_n)] = n \sum_{i=1}^{r} \mu_i \mathbb{P}[v_1 \text{ is isolated in } \mathcal{G}(n; \mu, \Theta_n) | t_1 = i]
= n \sum_{i=1}^{r} \mu_i \mathbb{P} [\cap_{j=2}^{n} [v_j \sim v_1] | t_1 = i]
= n \sum_{i=1}^{r} \mu_i (\mathbb{P}[v_2 \sim v_1 | t_1 = i])^{n-1} \tag{21}
\]
where (21) follows by the independence of the rvs \( \{v_j \sim v_1\}_{j=1}^{n} \) given \( \Sigma_1 \). By conditioning on the class of \( v_2 \), we find
\[ \mathbb{P}[v_2 \sim v_1 | t_1 = i] = \sum_{j=1}^{r} \mu_j (1 - \alpha p_{ij}) = 1 - \Lambda_i \] (22)

Using (22) in (21), and recalling (15) and (16), we obtain
\[
\mathbb{E}[\mathcal{I}_n(\mu, \Theta_n)] = n \sum_{i=1}^{r} \mu_i (1 - \Lambda_i(n))^{n-1}
\leq n (1 - \Lambda_1(n))^{n-1} \leq e^{\log n (1 - c_n \frac{1}{n})}.
\]

Taking the limit as \( n \) goes to infinity, we immediately get (20) since \( \lim_{n \to \infty} (1 - c_n \frac{1}{n}) = 1 - c < 0 \) under the enforced assumptions (with \( c > 1 \)) and the one-law is established. \( \square \)

### C. Establishing the Zero-Law

Our approach in establishing the zero-law relies on the method of second moment applied to a variable that counts the number of nodes that are class-1 and isolated. Clearly, if we can show that when there exists at least one class-1 node that is isolated under the enforced assumptions (with \( c < 1 \)) then the zero-law would immediately follow.

Let \( Y_n(\mu, \Theta_n) \) denote the number of nodes that are class-1 and isolated in \( \mathcal{G}(n; \mu, \Theta_n) \), and let
\[ x_{n,i}(\mu, \Theta_n) = 1 | t_i = 1 \cap v_i \text{ is isolated in } \mathcal{G}(n; \mu, \Theta_n) \]
then we have \( Y_n(\mu, \Theta_n) = \sum_{i=1}^{r} x_{n,i}(\mu, \Theta_n) \). By applying the method of second moments [34, Remark 3.1, p. 55] on \( Y_n(\mu, \Theta_n) \), we get
\[ \mathbb{P}[Y_n(\mu, \Theta_n) = 0] \leq 1 - \frac{\mathbb{E}[Y_n(\mu, \Theta_n)]^2}{\mathbb{E}[Y_n(\mu, \Theta_n)]^2} \] (23)

where
\[ \mathbb{E}[Y_n(\mu, \Theta_n)] = n \mathbb{E}[x_{n,1}(\mu, \Theta_n)] \] (24)

and
\[ \mathbb{E}[Y_n(\mu, \Theta_n)]^2 = n \mathbb{E}[x_{n,1}(\mu, \Theta_n)]^2 + n(n-1) \mathbb{E}[x_{n,1}(\mu, \Theta_n)x_{n,2}(\mu, \Theta_n)] \]

by exchangeability and the binary nature of the rvs \( \{x_{n,i}(\mu, \Theta_n)\}_{i=1}^{r} \). Using (24) and (25), we get
\[
\frac{\mathbb{E}[Y_n(\mu, \Theta_n)]^2}{\mathbb{E}[Y_n(\mu, \Theta_n)]^2} = \frac{1}{n} \mathbb{E}[x_{n,1}(\mu, \Theta_n)] + \frac{n-1}{n} \frac{\mathbb{E}[x_{n,1}(\mu, \Theta_n)x_{n,2}(\mu, \Theta_n)]}{\mathbb{E}[x_{n,1}(\mu, \Theta_n)]^2}.
\]

In order to establish the zero-law, we need to show that
\[ \lim_{n \to \infty} n \mathbb{E}[x_{n,1}(\mu, \Theta_n)] = \infty \] (26)

and
\[ \limsup_{n \to \infty} \left( \frac{\mathbb{E}[x_{n,1}(\mu, \Theta_n)x_{n,2}(\mu, \Theta_n)]}{\mathbb{E}[x_{n,1}(\mu, \Theta_n)]^2} \right) \leq 1. \] (27)

**Proposition 6.2:** Consider a scaling \( K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{+1} \) and a scaling \( \alpha : \mathbb{N}_0 \to (0, 1) \) such that (7) holds with \( \lim_{n \to \infty} c_n = c > 0 \). Then, we have
\[ \lim_{n \to \infty} n \mathbb{E}[x_{n,1}(\mu, \Theta_n)] = \infty, \quad \text{if } c < 1. \]

**Proof:** We have
\[
n \mathbb{E}[x_{n,1}(\mu, \Theta_n)] = n \mathbb{P}[v_1 \text{ is isolated in } \mathcal{G}(n; \mu, \Theta_n) \cap t_1 = 1]
= n \mu_1 \mathbb{P}[\cap_{j=2}^{n} [v_j \sim v_1] | t_1 = 1]
= n \mu_1 \mathbb{P}[v_2 \sim v_1 | t_1 = 1]^{n-1}
= n \mu_1 \left( \sum_{j=1}^{r} \mu_j (1 - \alpha p_{ij}) \right)^{n-1} \tag{28}
= n \mu_1 (1 - \Lambda_1(n))^{n-1} \mu_1 e^{\beta_n} \tag{29}
\]
where \( \beta_n = \log n + (n-1) \log(1 - \Lambda_1(n)) \). Recalling (17), we get
\[ \beta_n = \log n - (n-1) (\Lambda_1(n) + \Psi(\Lambda_1(n)) \tag{30} \]
\[ = \log n - (n-1) \left( c_n \log n + \Psi \left( c_n \log n \right) \right) \tag{30} \]
\[ = \log n \left( 1 - c_n \frac{n-1}{n} \right) \tag{30} \]
\[ - (n-1) \left( c_n \log n \right)^2 \left( \frac{1}{c_n \log n} \right)^2 \tag{30} \]

Recalling (18), we have
\[ \lim_{n \to \infty} \frac{\Psi \left( c_n \log n \right)^2}{\left( c_n \log n \right)^2} = \frac{1}{2} \tag{21} \]
since $c_n \log n - n - 1 \neq o(1)$. Thus, $\beta_n = \log n(1 - c_n^{-1}) - o(1)$.
Using (29)–(31), and letting $n$ go to infinity, we get
$$\lim_{n \to \infty} nE[x_n,1](\mu,\Theta_n)] = \infty$$
whenever $\lim_{n \to \infty} c_n = c < 1$.

Due to space limitations, the proof of (27) (under the enforced assumptions of the zero-law of Theorem 3.1) is given in [20, Appendix C]. Collectively, Proposition 6.2 and (27) establish the zero-law of Theorem 3.1.

VII. PROOF OF THEOREM 3.2

Let $C_n(\mu,\Theta_n)$ denote the event that the graph $G(n,\mu,\Theta_n)$
is connected, and with a slight abuse of notation, let $I_n(\mu,\Theta_n)$
denote the event that the graph $G(n,\mu,\Theta_n)$ has no isolated
nodes. It is clear that if a random graph is connected then it does
not have any isolated node, hence
$$C_n(\mu,\Theta_n) \subseteq I_n(\mu,\Theta_n)$$
and we get
$$P[C_n(\mu,\Theta_n)] \leq P[I_n(\mu,\Theta_n)] \quad (32)$$
and
$$P[C_n(\mu,\Theta_n)^c] = P[I_n(\mu,\Theta_n)^c] + P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n)]. \quad (33)$$

In view of (32), we obtain the zero-law for connectivity, i.e., that
$$\lim_{n \to \infty} P[G(n,\mu,\Theta_n) \text{ is connected}] = 0 \quad \text{if} \quad c < 1$$
immediately from the zero-law part of Theorem 3.1, i.e., from
that $\lim_{n \to \infty} P[I_n(\mu,\Theta_n)] = 0$ if $c < 1$. It remains to establish
the one-law for connectivity. In the remainder of this section,
we assume that (7) holds for some $c > 1$. From Theorem 3.1
and (33), we see that the one-law for connectivity, i.e., that
$$\lim_{n \to \infty} P[G(n,\mu,\Theta_n) \text{ is connected}] = 1 \quad \text{if} \quad c > 1$$
will follow if we show that
$$\lim_{n \to \infty} P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n)] = 0. \quad (34)$$
Our approach will be to find a suitable upper bound for (34) and
prove that it goes to zero as $n$ goes to infinity with $c > 1$.

We now work toward deriving an upper bound for (34); then
we will show that the bound goes to zero as $n$ gets large. Define
the event $E_n(\mu,\theta,X)$ via
$$E_n(\mu,\theta,X) := \bigcup_{S \in \cal N} \left\{ \sum_{i \in S} \Sigma_i | \leq X[S]\right\}$$
where $\cal N = \{1, \ldots, n\}$ and $X = [X_1 \cdots X_n]$ is an $n$-dimensional array of integers. Let
$$L_n := \min \left( \left\lfloor \frac{P}{K_1} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor \right) \quad (35)$$
and
$$X_\ell = \begin{cases} \lfloor \beta \ell K_1 \rfloor & \ell = 1, \ldots, L_n \\ \lfloor \gamma P \ell \rfloor & \ell = L_n + 1, \ldots, n \end{cases} \quad (36)$$
for some $\beta$ and $\gamma$ in $(0, \frac{1}{2})$ (specified in [20, Proposition 7.1]).
In words, $E_n(\mu,\theta,X)$ denotes the event that there exists
\( \ell = 1, \ldots, n \) such that the number of unique keys stored by
at least one subset of $\ell$ sensors is less than $\lfloor \beta \ell K_1 \rfloor$.
Using a crude bound, we get
$$P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n)] \leq P[E_n(\mu,\theta,X)] + P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n) \cap E_n(\mu,\theta,X)^c]. \quad (37)$$
Thus, (34) will be established by showing that
$$\lim_{n \to \infty} P[E_n(\mu,\theta,X)] = 0 \quad (38)$$
and
$$\lim_{n \to \infty} P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n) \cap E_n(\mu,\theta,X)^c] = 0. \quad (39)$$

The proof of (38) (under the enforced assumptions of the one-law
of Theorem 3.2) is similar to [8, Proposition 7.2]. Results
only require conditions (11) and $K_{1,n} = o(1)$ to hold. The latter
condition is clearly established in [20, Lemma A.4].

It now remains to establish (39) under the enforced assumptions
of the one-law of Theorem 3.2. Let $G(n,\mu,\Theta_n)(S)$ denotes
a subgraph of $G(n,\mu,\Theta_n)$ whose vertices are restricted
to the set $S$. Define the events
$$C_n(\mu,\Theta_n,S) := \{ G(n,\mu,\Theta_n)(S) \text{ is connected} \}$$
$$B_n(\mu,\Theta_n,S) := \{ G(n,\mu,\Theta_n)(S) \text{ is isolated} \}$$
$$A_n(\mu,\Theta_n,S) := C_n(\mu,\Theta_n,S) \cup B_n(\mu,\Theta_n,S).$$
In other words, $A_n(\mu,\Theta_n,S)$ encodes the event that
$G(n,\mu,\Theta_n)(S)$ is a component, i.e., a connected subgraph
that is isolated from the rest of the graph. The key observation
is that a graph is not connected if and only if it has a component
on vertices $S$ with $1 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor$; note that vertices $S$ form
a component then so do vertices $N \setminus S$. The event $I_n(\mu,\Theta_n)$
eliminates the possibility of $G(n,\mu,\Theta_n)(S)$ containing a component
of size one (i.e., an isolated node), whence we have
$$C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n) \subseteq \bigcup_{S \in \cal N:2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} A_n(\mu,\Theta_n,S)$$
and the conclusion
$$\sum_{S \in \cal N:2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} P[A_n(\mu,\Theta_n,S)] \leq \sum_{S \in \cal N:2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} P[A_n(\mu,\Theta_n,S)]$$
follows. By exchangeability, we get
$$P[C_n(\mu,\Theta_n)^c \cap I_n(\mu,\Theta_n) \cap E_n(\mu,\theta,X)^c]$$
$$\leq \sum_{\ell = 2}^{\left\lfloor \frac{n}{2} \right\rfloor} \left( \sum_{S \in \cal N_{n,\ell}} P[A_n(\mu,\Theta_n,S) \cap E_n(\mu,\theta,X)^c] \right)$$
$$= \sum_{\ell = 2}^{\left\lfloor \frac{n}{2} \right\rfloor} \left( \left( \begin{array}{c} n \\ \ell \end{array} \right) \right) P[A_n(\mu,\Theta_n) \cap E_n(\mu,\theta,X)^c] \quad (40)$$
where $\cal N_{n,\ell}$ denotes the collection of all subsets of $\{1, \ldots, n\}$
with exactly $\ell$ elements, and $A_n(\mu,\Theta_n)$ denotes the event
that the set \( \{1, \ldots, \ell\} \) of nodes form a component. As before we have \( A_{n,\ell}(\mu, \Theta_n) = C_{\ell}(\mu, \Theta_n) \cap B_{n,\ell}(\mu, \Theta_n) \), where \( C_{\ell}(\mu, \Theta_n) \) denotes the event that \( \{1, \ldots, \ell\} \) is connected and \( B_{n,\ell}(\mu, \Theta_n) \) denotes the event that \( \{1, \ldots, \ell\} \) is isolated from the rest of the graph.

Next, with \( \ell = 1, 2, \ldots, n-1 \), define \( \nu_{\ell,j}(\alpha) \) by
\[
\nu_{\ell,j}(\alpha) := \{i = 1, 2, \ldots, \ell : B_{\ell,j}(\alpha) = 1\}
\]
for each \( j = \ell + 1, \ldots, n \). Namely, \( \nu_{\ell,j}(\alpha) \) is the set of nodes in \( \{v_1, \ldots, v_\ell\} \) that are adjacent to node \( v_j \) in the ER graph \( \mathbb{H}(n; \alpha_n) \). For each \( \ell = 1, \ldots, n-1 \), we have
\[
B_{n,\ell}(\mu, \Theta_n) = \bigcap_{m = \ell+1}^{n} \left( \{v_j : j \in \nu_{\ell,j}(\alpha)\} \cap \Sigma_m = \emptyset \right).
\]
We have
\[
P \left[ B_{n,\ell}(\mu, \Theta_n) \mid \Sigma_1, \ldots, \Sigma_\ell \right] = \prod_{m = \ell+1}^{n} E \left[ \left( \frac{P - |\nu_{\ell,m}(\alpha_n)\mid}{|\Sigma_m|} \right) \left( \frac{\Sigma_1, \ldots, \Sigma_\ell}{\Sigma_m} \right) \right]
\]
\[
= \prod_{m = \ell+1}^{n} \left[ \frac{P - |\nu_{\ell,m}(\alpha_n)\mid}{|\Sigma_m|} \right] \left( \frac{\Sigma_1, \ldots, \Sigma_\ell}{\Sigma_m} \right)^{n-\ell}
\]
noting the fact that the collection of rvs \( \{\nu_{\ell,m}, \Sigma_m : m = \ell + 1, \ldots, n\} \) are mutually independent and identically distributed. Here, \( \nu_{\ell,m}(\alpha_n) \) denotes a generic rv distributed identically with \( \nu_{\ell,m}(\alpha_n) \) for any \( m = \ell + 1, \ldots, n \). Similarly, \( \Sigma \) denotes a rv that takes the value \( K_\ell \) with probability \( \mu_\ell \).

We will leverage the expression (42) in (40) in the following manner. Note that on the event \( E_n(\mu, \theta_n, X_n^\ell) \), we have
\[
\left| \cup_{j \in \nu_{\ell}(\alpha_n)} \Sigma_i \right| \geq (X_{n,\nu_{\ell}(\alpha_n)} + 1) \mid \nu_{\ell}(\alpha_n) > 0 \right]
\]
while the crude bound
\[
\left| \cup_{j \in \nu_{\ell}(\alpha_n)} \Sigma_i \right| \geq K_1, \mathbb{1}[\nu_{\ell}(\alpha_n) > 0]
\]
always holds. These bounds lead to
\[
P \left[ B_{n,\ell}(\mu, \Theta_n) \cap E_n(\mu, \theta_n, X_n^\ell) \mid \Sigma_1, \ldots, \Sigma_\ell \right] \leq \mathbb{E} \left[ \left( \frac{P - \max(K_1, \Sigma, X_{n,\nu_{\ell}(\alpha_n)} + 1) \mid \nu_{\ell}(\alpha_n) > 0 \right)}{\Sigma_m} \right]^{n-\ell}
\]
Conditioning on \( \Sigma_1, \ldots, \Sigma_\ell \) and \( \{B_{\ell,j}(\alpha_n), 1 \leq i < j \leq \ell\} \), we then get
\[
P \left[ A_{n,\ell}(\mu, \Theta_n) \cap E_n(\mu, \theta_n, X_n^\ell) \right] = \mathbb{E} \left[ \mathbb{1}[C_{\ell}(\mu, \Theta_n)] \mathbb{1}[B_{n,\ell}(\mu, \Theta_n) \cap E_n(\mu, \theta_n, X_n^\ell)] \right]
\]
\[
\leq \mathbb{P}[C_{\ell}(\mu, \Theta_n)] \mathbb{E} \left[ \left( \frac{P - \max(K_1, X_{n,\nu_{\ell}(\alpha_n)} + 1) \mid \nu_{\ell}(\alpha_n) > 0 \right)}{\Sigma_m} \right]^{n-\ell}
\]
since \( C_{\ell}(\mu, \Theta_n) \) is fully determined by \( \Sigma_1, \ldots, \Sigma_\ell \) and \( \{B_{\ell,j}(\alpha_n), 1 \leq i < j \leq \ell\} \), and \( B_{n,\ell}(\mu, \Theta_n) \) and \( E_n(\mu, \theta_n, X_n^\ell) \) are independent from \( \{B_{\ell,j}(\alpha_n), 1 \leq i < j \leq \ell\} \). Our proof of (39) will be completed [see (40)] upon establishing
\[
\lim_{n \to \infty} \sum_{\ell=2}^{n} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\mu, \Theta_n) \cap E_n(\mu, \theta_n, X_n^\ell)] = 0
\]
by means of deriving upper bounds on the terms appearing in (46) and showing that these bounds tend to zero as \( n \) tends to infinity. Due to space limitations, these steps are taken in [20, Appendix E]. This establishes the one-law.

**ACKNOWLEDGMENT**

The authors would like to thank Philip and M. Dowd for their financial support and encouragement.

**REFERENCES**

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” IEEE Commun. Surv. Tutus., vol. 8, no. 2, pp. 2–23, Apr.–Jun. 2006.

[3] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. 9th ACM Conf. Comput. Commun. Security, 2002, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. IEEE Symp. Security Privacy, May 2003, pp. 197–213.

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

[6] S. A. Çamtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: A survey,” Rensselaer Polytech. Inst., Troy, NY, USA, Tech. Rep. TR-05-07, 2005.

[7] M. Varis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, “Exploiting heterogeneity in sensor networks,” in Proc. IEEE INFOCOM, Mar. 2005, vol. 2, pp. 878–890.

[8] O. Yağan, “Zero-one laws for connectivity in inhomogeneous random key graphs,” IEEE Trans. Inf. Theory, vol. 62, no. 8, pp. 4559–4574, Aug. 2016.

[9] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, “Redoubleable sensor networks,” ACM Trans. Inf. Syst. Security, vol. 11, no. 3, pp. 13:1–13:22, Mar. 2008.

[10] P. Gupta and P. R. Kumar, “Critical power for asymptotic connectivity in wireless networks,” in Stochastic Analysis, Control, Optimization and Applications. New York, NY, USA: Springer-Verlag, 1999, pp. 547–566.

[11] M. D. Penrose, Random Geometric Graphs. London, UK.: Oxford Univ. Press, Jul. 2003.

[12] M. D. Penrose et al., “Connectivity of soft random geometric graphs,” Ann. Appl. Probab., vol. 26, no. 2, pp. 986–1028, 2016.

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

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

[15] M. Bloznelis, J. Jaworski, and K. Rybarczyk, “Component evolution in a secure wireless sensor network,” Networks, vol. 53, pp. 19–26, Jan. 2009.

[16] E. Goderhardt and J. Jaworski, “Two models of random intersection graphs for classification,” in Exploratory Data Analysis in Empirical Research. New York, NY, USA: Springer-Verlag, 2003, pp. 67–81.

[17] B. Bollobás, Random Graphs. Cambridge, U.K.: Cambridge Univ. Press, 2001, vol. 73.

[18] A. Mei, A. Panconesi, and J. Radhakrishnan, “Unasailable sensor networks,” in Proc. 4th Int. Conf. Security Privacy Commun. Netw., 2008, pp. 1–10.
[19] L. Devroye and N. Fraiman, “Connectivity of inhomogeneous random graphs,” *Random Struct. Algorithms*, vol. 45, no. 3, pp. 408–420, 2014.

[20] R. Eletreby and O. Yağan, “Connectivity of wireless sensor networks secured by heterogeneous key predistribution under an on/off channel model,” arXiv:1604.00460, Oct. 2017. [Online]. Available: https://arxiv.org/abs/1604.00460

[21] J. Zhao, “Analyzing connectivity of heterogeneous secure sensor networks,” *IEEE Trans. Control Netw. Syst.*, vol. PP, no. 99, pp. 1–1, 2016, doi: 10.1109/TCNS.2016.2641799.

[22] J. Zhao, O. Yağan, and V. Gligor, “On connectivity and robustness in random intersection graphs,” *IEEE Trans. Automat. Control*, vol. 62, no. 5, pp. 2121–2136, May 2017.

[23] O. Yağan, D. Qian, J. Zhang, and D. Cochran, “Conjoining speeds up information diffusion in overlaying social-physical networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 6, pp. 1038–1048, Jun. 2013.

[24] J. Zhang, O. Yağan, and V. Gligor, “On connectivity and robustness in random intersection graphs,” *IEEE Trans. Automat. Control*, vol. 62, no. 5, pp. 2121–2136, May 2017.

[25] O. Yağan, D. Qian, J. Zhang, and D. Cochran, “Conjoining speeds up information diffusion in overlaying social-physical networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 6, pp. 1038–1048, Jun. 2013.

[26] L. Fu, X. Fu, Z. Xu, Q. Peng, X. Wang, and S. Lu, “Determining source-destination connectivity in uncertain networks: Modeling and solutions,” *IEEE/ACM Trans. Netw.*, vol. 25, no. 6, pp. 3237–3252, Dec. 2017.

[27] L. Fu, X. Wang, and P. R. Kumar, “Are we connected? Optimal determination of source-destination connectivity in random networks,” *IEEE/ACM Trans. Netw.*, vol. 25, no. 2, pp. 751–764, Apr. 2017.

[28] D. J. Watts, “A simple model of global cascades on random networks,” *Proc. Nat. Acad. Sci.*, vol. 99, no. 9, pp. 5766–5771, 2002.

[29] D. Kempe, J. Kleinberg, and E. Tardos, “Maximizing the spread of influence through a social network,” in *Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2003, pp. 137–146.

[30] S. Eubank et al., “Modeling disease outbreaks in realistic urban social networks,” *Nature*, vol. 429, no. 6988, pp. 180–4, May 13, 2004.

[31] M. E. J. Newman, “Spread of epidemic disease on networks,” *Phys. Rev. E*, vol. 66, Jul. 2002, Art. no. 016128.

[32] A.-L. Barabási and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[33] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks,” *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[34] O. Yağan and A. M. Makowski, “Counting triangles, tunable clustering and the small-world property in random key graphs (Extended version),” arXiv:1701.03758, Jan. 2017.

[35] M. Deijfen and W. Kets, “Random intersection graphs with tunable degree distribution and clustering,” *Probab. Eng. Inf. Sci.*, vol. 23, no. 4, pp. 661–674, 2009.

[36] S. Janson, T. Łuczak, and A. Ruciński, *Random Graphs*. Wiley–Intersc. Ser. Discrete Math. Optim. Hoboken, NJ, USA: Wiley, 2000.

**Rashad Eletreby (S’10)*** received the B.Sc. degree (with honors) in electronics and electrical communications engineering from Cairo University, Giza, Egypt, in 2012. He is currently working toward the Ph.D. degree in structure and dynamics on random graphs at the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. His research interests include network science, random graph theory, and wireless communications.

**Osman Yağan (S’07–M’12–SM’17)** 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, USA, in 2011. He is an Assistant Research Professor with the Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. His research interests include wireless network security, dynamical processes in complex networks, percolation theory, random graphs, and their applications.

Mr. Eletreby was the recipient of multiple prestigious fellowships including Dowd Fellowship, Carnegie Mellon University Presidential Fellowship, William J. Happel Fellowship, and Carnegie Institute of Technology Dean's Fellowship.