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

Rashad Eletreby, *Student Member, IEEE,* and Osman Yağan, *Senior Member, IEEE,*

Abstract—We investigate the connectivity of a wireless sensor network 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and the on/off channel model induces an Erdős-Rényi graph, denoted by $\mathbb{H}(n, \alpha)$. Hence, the overall random graph modeling the WSN is obtained by the intersection of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and $\mathbb{H}(n, \alpha)$. 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 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 wireless sensor networks so that they achieve secure connectivity with high probability; and ii) despite the simplicity of the on/off communication model, the probability of connectivity in the resulting wireless sensor network approximates very well the case where the disk model is used.

Index Terms—Wireless Sensor Networks, Security, Inhomogeneous Random Key Graphs, Connectivity.

1. INTRODUCTION

A. Wireless Sensor Networks and Security

WIRELESS sensor networks (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 can not 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

R. Eletreby and O. Yağan are with the Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Pittsburgh, PA, 15213 USA. E-mail: reletreby@cmu.edu, oyagan@ece.cmu.edu.

conforming to the typical limitations of WSNs. Also, it shall not assume knowledge of post-deployment 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. The EG scheme is currently regarded as one of the most feasible solutions for key-establishment among sensor nodes, e.g., see [5, Chapter 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, one can reasonably argue that 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, Yağan proposed a new variation of the EG scheme, referred to as the *heterogeneous* random key predistribution scheme [8]. 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 can not 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.

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 the resulting network is connected with high probability 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 with high probability as the number of nodes gets large. Specifically, with $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$, $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$, and n denoting the network size, we let $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ 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. This model was referred to as the *inhomogeneous* random key graph in [8], where zero-one laws for absence of isolated nodes and connectivity were established. 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?*

B. Modeling Wireless Connectivity

Our paper aims to answer this 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 particular, 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ 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 in between. Let $\mathbb{G}$ be the intersecting graph, i.e., $\mathbb{G} := \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{I}(n; \cdot)$. At a high level, our objective is to establish scaling conditions on

the parameters of $\mathbb{G}$ such that the resulting graph is connected with high probability 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* [9] 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 $\mathcal{D}$ of a euclidean plane, nodes v_i and v_j located at $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, respectively, are able to communicate if $\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho$, where ρ denotes the transmission radius. A special case of the disk model when node locations are independently and uniformly distributed over the region $\mathcal{D}$, gives rise to the random geometric graph [10], hereafter denoted $\mathbb{I}(n; \rho)$. Now, let $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \rho)$ be a random graph obtained by intersecting the inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \cdot)$ with a random geometric graph $\mathbb{I}(n; \rho)$. Clearly, $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \rho)$ 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \rho)$ is likely to be very challenging, and may very well be impossible. In fact, the Gupta-Kumar conjecture [9] on the connectivity of $\mathbb{H}(n; \alpha) \cap \mathbb{I}(n; \rho)$ where $\mathbb{H}(n; \alpha)$ represents an Erdős-Rényi (ER) graph, took many years (and several attempts) to be resolved eventually by Penrose [11]; see [12] for a detailed discussion on the difficulties involved in analyzing *intersection* of different types of graphs. The model $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ 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 [12], [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 α) or off (with probability $1 - \alpha$) independently from all other channels. The model induces an ER graph $\mathbb{H}(n; \alpha)$, where an edge exists (respectively does not exist) between two vertices with probability α (respectively $1 - \alpha$) independently from all other edges.

With these in mind, we model the wireless connectivity of the WSN by an ER graph $\mathbb{H}(n; \alpha)$ and study the connectivity of the intersecting graph $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha) := \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$. This approach allows us to i) establish rigorous results concerning the secure 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{I}(n; \rho)$ behaves very similar to that of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$, as we *match* α and ρ 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and the on/off channel model induces an ER graph, denoted by $\mathbb{H}(n, \alpha)$. Hence, the overall random graph modeling the WSN is obtained by the intersection of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and $\mathbb{H}(n, \alpha)$. We denote this intersection by $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$, i.e., $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha) := \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n, \alpha)$. We present conditions on how to scale the parameters of $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$ with respect to the network size n such that i) it has no isolated nodes and ii) it is connected, both with high probability 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 α 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 with high probability; 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 for details).

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 $\mathbf{1}[E]$. We say that an event holds with high probability (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., $a_n = o(b_n)$, $a_n = \omega(b_n)$, $a_n = O(b_n)$, $a_n = \Omega(b_n)$, and $a_n = \Theta(b_n)$. We also use $a_n \sim b_n$ to denote the asymptotic equivalence $\lim_{n \to \infty} a_n/b_n = 1$.

2. THE 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 $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ 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 Σ_x of node v_x is a random variable (rv) with

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

where t_x denotes the class of v_x and $\mathcal{P}_{K_i}$ is the collection of all subsets of $\{1, \ldots, P\}$ with size K_i. 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 $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$ and assume without loss of generality that $K_1 \leq K_2 \leq \ldots \leq K_r$. Consider a random graph $\mathbb{K}$ induced on the vertex set $\mathcal{V} = \{v_1, \ldots, v_n\}$ such that a pair of 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ [8]. This model is also known in the literature as the *general random intersection graph*; e.g., see [15]–[17]. The probability p_{ij} that a class-i node and a class-j node are adjacent is given by

$$p_{ij} = \mathbb{P}[v_x \sim_{\mathbb{K}} v_y \mid t_x = i, t_y = j] = 1 - \frac{\binom{P - K_i}{K_j}}{\binom{P}{K_j}} \tag{2}$$

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we have $p_{ij} = 1$. Let λ_i denote the *mean* probability that a class-i node is connected to another node in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$. We have

$$\lambda_i = \mathbb{P}[v_x \sim_{\mathbb{K}} v_y \mid t_x = i] = \sum_{j=1}^{r} p_{ij} \mu_j. \tag{3}$$

We also find it useful to define the *mean* key ring size by K_{avg}; i.e.,

$$K_{\text{avg}} = \sum_{j=1}^{r} K_j \mu_j. \tag{4}$$

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 α 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 α. 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 $\mathbb{H}(n; \alpha)$ [18], defined on the vertices $\mathcal{V} = \{v_1, \ldots, v_n\}$ 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ with an ER graph $\mathbb{H}(n; \alpha)$. Namely, nodes v_x and v_y are adjacent in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$, if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{H}$. Hence, the edges in the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$ 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 $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$ amounts to studying the secure connectivity of heterogeneous WSNs under the on/off channel model.

Hereafter, we denote the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{H}(n; \alpha)$ by $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$. To simplify the notation, we let $\boldsymbol{\theta} = (\boldsymbol{K}, P)$, and $\boldsymbol{\Theta} = (\boldsymbol{\theta}, \alpha)$. The probability of edge existence between a class-i node v_x and a class-j node v_y in $\mathbb{G}(n; \boldsymbol{\Theta})$ is given by

$$\mathbb{P}[v_x \sim_{\mathbb{G}} v_y \mid t_x = i, t_y = j]$$

$$= \mathbb{P}[v_x \sim_{\mathbb{K}} v_y \cap v_x \sim_{\mathbb{H}} v_y \mid t_x = i, t_y = j]$$
$$= \alpha p_{ij}$$

by independence. Similar to (3), the mean edge probability for a class-i node in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ as Λ_i is given by

$$\Lambda_i = \sum_{j=1}^{r} \mu_j \alpha p_{ij} = \alpha \lambda_i, \quad i = 1, \ldots, r. \tag{5}$$

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.

3. MAIN RESULTS AND DISCUSSION

We refer to a mapping $\boldsymbol{\Theta} = K_1, \ldots, K_r, P, \alpha : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)$ as a *scaling* if

$$1 \leq K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{6}$$

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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$.

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

$$\Lambda_1(n) = \alpha_n \lambda_1(n) \sim c \frac{\log n}{n} \tag{7}$$

for some $c > 0$. *We have*

$$\lim_{n \to \infty} \mathbb{P} \left[\begin{array}{c} \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \text{ has} \\ \text{no isolated nodes} \end{array} \right] = \begin{cases} 0 & \text{if } c < 1 \\ 1 & \text{if } c > 1 \end{cases} \tag{8}$$

The scaling condition (7) will often be used in the form

$$\Lambda_1(n) = c_n \frac{\log n}{n}, \quad n = 2, 3, \ldots \tag{9}$$

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

Next, we present an analogous result for connectivity.

Theorem 3.2. *Consider a probability distribution* $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ *with* $\mu_i > 0$ *for* $i = 1, \ldots, r$ *and a scaling* $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)$ *such that (7) holds for some* $c > 0$. *Then, we have*

$$\lim_{n \to \infty} \mathbb{P}[\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \text{ is connected}] = \begin{cases} 0 & \text{if } c < 1 \\ 1 & \text{if } c > 1 \end{cases} \tag{10}$$

under the additional conditions that

$$P_n \geq \sigma n, \quad n = 1, 2, \ldots \tag{11}$$

for some $\sigma > 0$ *and*

$$p_{11}(n) = \omega \left(\frac{1}{n \alpha_n} \right). \tag{12}$$

The resemblance of the results presented in Theorem 3.1 and Theorem 3.2 indicates that absence of isolated nodes and connectivity are asymptotically equivalent properties for

$\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. Similar observations were made for other well-known random graph models as well; e.g., inhomogeneous random key graphs [8], Erdős-Rényi graphs [18], 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], [19]. 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 [20], [21] 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 non-trivial lower bound on that probability. More specifically, it is easy to see that $\alpha_n p_{11}(n) = O(\Lambda_1) = O(\log n/n)$, but it is not clear if the sequence $\alpha_n p_{11}(n)$ has a non-trivial lower bound. In fact, authors in [22] investigated the connectivity of an inhomogeneous Erdős-Rényi (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 $\log n/n$.

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 non-trivial 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 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ 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 $(1 + \epsilon) \log n$ for some $\epsilon > 0$. On the other hand, if this minimal mean degree scales as $(1 - \epsilon) \log n$ for some $\epsilon > 0$, then whp $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$.

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* $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ *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*

$$\alpha_n \frac{K_{1,n} K_{\text{avg},n}}{P_n} \sim c \frac{\log n}{n} \qquad (13)$$

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 Lemma A.1, this then leads to $p_{1j}(n) \sim \frac{K_{1,n} K_{j,n}}{P_n}$, whence

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

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 α_n for which the network becomes connected whp is increased by two-fold (see Figure 2 for a numerical example demonstrating this phenomenon).

B. Comparison with related work

Our main results extend the work in [8] and [23], 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 [23] 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 [12] (respectively, [24]) 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 [12] 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 [12].

4. NUMERICAL RESULTS

We now present numerical results to support Theorems 3.1 and Theorem 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 number of nodes at $n = 500$ and the size of the key pool at $P = 10^4$.

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 $\mathbb{I}(n; \rho)$ 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

$$\mathbb{P}\left[\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho\right] = \pi \rho^2, \qquad i \neq j, \quad i, j = 1, \ldots, n$$

whenever $\rho < 0.5$. Thus, in order to match the two communication models we set $\alpha = \pi \rho^2$. Recall that $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\theta}, \alpha) = \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{H}(n; \alpha)$, and let $\widetilde{\mathbb{G}}(n; \boldsymbol{\mu}, \boldsymbol{\theta}, \rho) = \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{I}(n; \rho)$. Next, we present several simulation results comparing the (empirical) probabilities that $\mathbb{G}$ and $\widetilde{\mathbb{G}}$ are connected, respectively.

We start by considering the channel parameter $\alpha = \pi \rho^2 = 0.2$, $\alpha = \pi \rho^2 = 0.4$, $\alpha = \pi \rho^2 = 0.6$, and $\alpha = \pi \rho^2 = 0.8$, while varying the parameter K_1 (i.e., the smallest key ring size) from 5 to 35. The number of classes is fixed at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and we set $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \alpha)$ (respectively, $(\boldsymbol{K}, \pi \rho^2)$), we generate 800 independent samples of the graphs $\mathbb{G}$ (respectively, $\widetilde{\mathbb{G}}$) and count the number of times (out of a possible 800) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 800, we obtain the (empirical) probabilities for the events of interest. We observed that $\mathbb{G}$ is connected whenever it has no isolated nodes yielding the same empirical probability for both events. This is in parallel with the asymptotic equivalence of the two properties as implied by Theorems 3.1 and 3.2.

In Figure 1, we show the empirical probabilities of the connectivity of $\mathbb{G}$ (represented by lines) and $\widetilde{\mathbb{G}}$ (represented by symbols). We observe that the empirical probabilities are almost identical, supporting the claim that the on/off channel model serves as a good approximation of the disk model under the given matching condition. Furthermore, we show the critical threshold of connectivity *predicted* by Theorem 3.2 by a vertical dashed line for each curve. More specifically, for a given α, the vertical dashed lines stand for the minimum integer value of K_1 that satisfies

$$\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left(1 - \frac{\binom{P-K_j}{K_1}}{\binom{P}{K_1}} \right) > \frac{1}{\alpha} \frac{\log n}{n} \qquad (14)$$

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 Figure 1 that even in the finite-node regime ($n = 500$), the critical value of K_1 results in a connected network with high probability.

Figure 2 is generated in a similar manner with Figure 1, this time with an eye towards understanding the impact of the minimum key ring size K_1 on network connectivity. We fix the number of classes at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and consider four different key ring sizes $\boldsymbol{K}$ each with mean 40; we consider $\boldsymbol{K} = \{10, 70\}$, $\boldsymbol{K} = \{20, 50\}$, $\boldsymbol{K} = \{30, 50\}$, and $\boldsymbol{K} = \{40, 40\}$. We compare the probability of connectivity in the
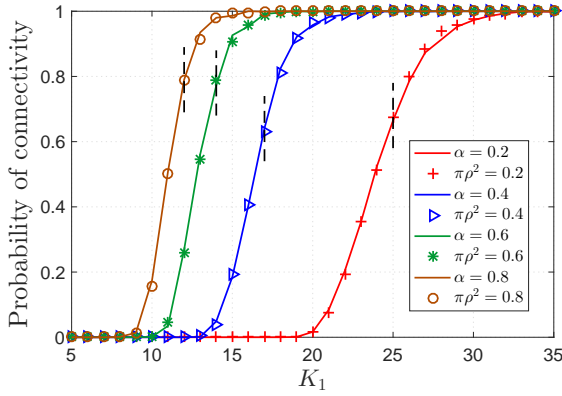
Fig. 1. Empirical probability that $\mathbb{G}$ and $\widetilde{\mathbb{G}}$ are connected as a function of $\boldsymbol{K}$ for $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$ with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 800 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.2.
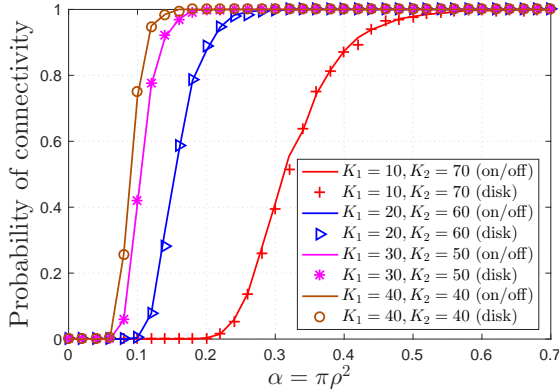

Fig. 2. Empirical probability that $\mathbb{G}$ and $\widetilde{\mathbb{G}}$ are connected as a function of α and $\pi\rho^2$ for four choices of $\boldsymbol{K} = (K_1, K_2)$, each with the same mean.

resulting networks as α (respectively, $\pi\rho^2$) 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.

5. OTHER APPLICATION AREAS: THE SPREAD OF EPIDEMICS AND INFORMATION IN REAL-WORLD SOCIAL NETWORKS

The last decade has witnessed a tremendous advance in our understanding of how information [25], [26], influence [27], [28], and diseases [29], [30] propagate across the globe. A large variety of mathematical models as well as a multitude of data sets paved the way for precise predictions and control of the behavior of such spreading processes on complex networks. In particular, several generative models were proposed to create networks which 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 [31]–[33].

The *homogeneous* random key graph (where all nodes receive the same number K of objects) was shown to generate networks that are clustered and small-world [34]. Indeed, the inhomogeneous counterpart $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ intrinsically exhibits these two properties as well. In addition to that, one can tune the parameters of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ to generate networks with a power-law degree distribution similar to that observed in real-world social networks [35]. Collectively, the inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ 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 [24]. 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$ 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 [30], 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 α being the average transmissibility; If we are to occupy each edge in the graph with probability α, 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 [30]. Typically, one is interested in deriving the threshold value of α for which a *giant* connected component emerges, indicating that the disease has reached a positive fraction of the population.

Intersecting the inhomogeneous random key graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ with an ER graph $\mathbb{H}(n; \alpha)$ is essentially equivalent to *occupying* each edge of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ independently with probability α. Hence, the scaling condition for which the one-law of Theorem 3.2 holds gives us a threshold value of α for which a strain of a disease or a piece of information would infect the entire population. In particular, let $\hat{\alpha}_n := \log n / (n\lambda_1(n))$; if the average transmissibility of a disease α satisfies $\alpha_n > \hat{\alpha}_n$, 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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{K}, P, \alpha)$ 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.

6. PROOF OF THEOREM 3.1

A. Preliminaries

Few technical results are collected here for convenience. A full list of preliminaries is given in Appendix A. The first result follows easily from the scaling condition (6).

Proposition 6.1 ([8, Proposition 4.1]). *For any scaling* $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, *we have (in view of (6))*

$$\lambda_1(n) \leq \lambda_2(n) \leq \ldots \leq \lambda_r(n) \qquad (15)$$

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

Another useful bound that will be used throughout is

$$(1 \pm x) \leq e^{\pm x}, \quad x \in (0,1) \qquad (16)$$

Finally, we find it useful to write

$$\log(1-x) = -x - \Psi(x) \qquad (17)$$

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

$$\lim_{x \to 0} \frac{\Psi(x)}{x^2} = \frac{-x - \log(1-x)}{x^2} = \frac{1}{2}. \qquad (18)$$

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 $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. Let $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the total number of isolated nodes in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, namely,

$$I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{\ell=1}^n \mathbf{1}[v_\ell \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \qquad (19)$$

The method of first moment [36, Eqn. (3.10), p. 55] gives

$$1 - \mathbb{E}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0]$$

It is clear that in order to establish the one-law, namely that $\lim_{n \to \infty} \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta_n}) = 0] = 1$, we need to show that

$$\lim_{n \to \infty} \mathbb{E}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = 0. \qquad (20)$$

Recalling (19), we have

$$\mathbb{E}\left[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \right]$$
$$= n \sum_{i=1}^r \mu_i \mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) \mid t_1 = i \right]$$
$$= n \sum_{i=1}^r \mu_i \mathbb{P}\left[\cap_{j=2}^n [v_j \not\sim v_1] \mid v_1 \text{ is class i} \right]$$
$$= n \sum_{i=1}^r \mu_i \left(\mathbb{P}[v_2 \not\sim v_1 \mid v_1 \text{ is class i}] \right)^{n-1} \qquad (21)$$

where (21) follows by the independence of the rvs $\{v_j \not\sim v_1\}_{j=1}^n$ given Σ_1. By conditioning on the class of v_2, we find

$$\mathbb{P}[v_2 \not\sim v_1 \mid t_1 = i] = \sum_{j=1}^r \mu_j \mathbb{P}[v_2 \not\sim v_1 \mid t_1 = i, t_2 = j]$$

$$= \sum_{j=1}^r \mu_j (1 - \alpha p_{ij}) = 1 - \Lambda_i \qquad (22)$$

Using (22) in (21), and recalling (15) and (16), we obtain

$$\mathbb{E}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = n \sum_{i=1}^r \mu_i \left(1 - \Lambda_i(n)\right)^{n-1}$$
$$\leq n \left(1 - \Lambda_1(n)\right)^{n-1} \leq e^{\log n \left(1 - c_n \frac{n-1}{n}\right)}.$$

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

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 whp 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 $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the number of nodes that are class-1 and isolated in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, and let

$$x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \mathbf{1}[t_i = 1 \cap v_i \text{ is isolated in } \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)],$$

then we have $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^n x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. By applying the method of second moments [36, Remark 3.1, p. 55] on $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, we get

$$\mathbb{P}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0] \leq 1 - \frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]} \qquad (23)$$

where

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \qquad (24)$$

and

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \qquad (25)$$
$$+ n(n-1)\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]$$

by exchangeability and the binary nature of the rvs $\{x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\}_{i=1}^n$. Using (24) and (25), we get

$$\frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} = \frac{1}{n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}$$
$$+ \frac{n-1}{n} \frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}$$

In order to establish the zero-law, we need to show that

$$\lim_{n \to \infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty, \qquad (26)$$

and

$$\limsup_{n \to \infty} \left(\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} \right) \leq 1. \qquad (27)$$

Proposition 6.2. *Consider a scaling* $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *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*

$$\lim_{n \to \infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty, \quad \text{if } c < 1$$

Proof. We have

$$n\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \right]$$

$$= n\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) \cap t_1 = 1\right]$$

$$= n\mu_1\mathbb{P}\left[\cap_{j=2}^n [v_j \nsim v_1] \mid t_1 = 1\right]$$

$$= n\mu_1\mathbb{P}\left[v_2 \nsim v_1 \mid t_1 = 1\right]^{n-1}$$

$$= n\mu_1\left(\sum_{j=1}^r \mu_j\mathbb{P}\left[v_2 \nsim v_1 \mid t_1 = 1, t_2 = j\right]\right)^{n-1}$$

$$= n\mu_1\left(\sum_{j=1}^r \mu_j(1 - \alpha_n p_{1j})\right)^{n-1} \tag{28}$$

$$= n\mu_1\left(1 - \Lambda_1(n)\right)^{n-1} = \mu_1 e^{\beta_n} \tag{29}$$

where $\beta_n = \log n + (n-1)\log(1 - \Lambda_1(n))$. Recalling (17), we get

$$\beta_n = \log n - (n-1)\left(\Lambda_1(n) + \Psi(\Lambda_1(n))\right)$$

$$= \log n - (n-1)\left(c_n\frac{\log n}{n} + \Psi\left(c_n\frac{\log n}{n}\right)\right)$$

$$= \log n\left(1 - c_n\frac{n-1}{n}\right)$$

$$- (n-1)\left(c_n\frac{\log n}{n}\right)^2 \frac{\Psi\left(c_n\frac{\log n}{n}\right)}{\left(c_n\frac{\log n}{n}\right)^2} \tag{30}$$

Recalling (18), we have

$$\lim_{n\to\infty} \frac{\Psi\left(c_n\frac{\log n}{n}\right)}{\left(c_n\frac{\log n}{n}\right)^2} = \frac{1}{2} \tag{31}$$

since $c_n\frac{\log n}{n} = o(1)$. Thus, $\beta_n = \log n\left(1 - c_n\frac{n-1}{n}\right) - o(1)$. Using (29), (30), (31), and letting n go to infinity, we get

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = \infty$$

whenever $\lim_{n\to\infty} c_n = c < 1$. ∎

Proposition 6.3. *Consider a scaling $K_1,\ldots,K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ 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 (27) if $c < 1$.*

The proof of Proposition 6.3 is given in Appendix C. Collectively, Proposition 6.2 and Proposition 6.3 establish (26) and (27) respectively, which in turn establish the zero-law of Theorem 3.1.

7. PROOF OF THEOREM 3.2

Let $C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{G}(n,\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ is connected, and with a slight abuse of notation, let $I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{G}(n,\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ has no isolated nodes. It is clear that if a random graph is connected then it does not have any isolated node, hence

$$C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) \subseteq I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$$

and we get

$$\mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \tag{32}$$

and

$$\mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c] = \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c] + \mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]. \tag{33}$$

In view of (32), we obtain the zero-law for connectivity, i.e., that

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

immediately from the zero-law part of Theorem 3.1, i.e., from that $\lim_{n\to\infty} \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0$ 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

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

will follow if we show that

$$\lim_{n\to\infty} \mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0. \tag{34}$$

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 towards deriving an upper bound for (34); then in Appendix E we will show that the bound goes to zero as n gets large. Define the event $E_n(\boldsymbol{\mu},\boldsymbol{\theta},\boldsymbol{X})$ via

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

where $\mathcal{N} = \{1,\ldots,n\}$ and $\boldsymbol{X} = [X_1 \cdots X_n]$ is an n-dimensional array of integers. Let

$$L_n := \min\left(\left\lfloor\frac{P}{K_1}\right\rfloor, \left\lfloor\frac{n}{2}\right\rfloor\right) \tag{35}$$

and

$$X_\ell = \begin{cases} \lfloor\beta\ell K_1\rfloor & \ell = 1,\ldots,L_n \\ \lfloor\gamma P\rfloor & \ell = L_n+1,\ldots,n \end{cases} \tag{36}$$

for some β and γ in $(0,\frac{1}{2})$ that will be specified later. In words, $E_n(\boldsymbol{\mu},\boldsymbol{\theta},\boldsymbol{X})$ denotes the event that there exists $\ell = 1,\ldots,n$ such that the number of unique keys stored by at least one subset of ℓ sensors is less than $\lfloor\beta\ell K_1\rfloor \mathbf{1}[\ell \leq L_n] + \lfloor\gamma P\rfloor \mathbf{1}[\ell > L_n]$. Using a crude bound, we get

$$\mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]$$
$$\leq \mathbb{P}[E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)]$$
$$+ \mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] \tag{37}$$

Thus, (34) will be established by showing that

$$\lim_{n\to\infty} \mathbb{P}[E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)] = 0, \tag{38}$$

and

$$\lim_{n\to\infty} \mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] = 0 \tag{39}$$

Proposition 7.1. *Consider scalings $K_1,\ldots,K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$ such that (7) holds for some $c > 1$, (11) and (12) hold. Then, we have (38) where $\boldsymbol{X}_n$ is as specified in (36), $\beta \in (0,\frac{1}{2})$ and $\gamma \in (0,\frac{1}{2})$ are selected such that*

$$\max\left(2\beta\sigma, \beta\left(\frac{e^2}{\sigma}\right)^{\frac{\beta}{1-2\beta}}\right) < 1 \tag{40}$$

$$\max\left(2\left(\sqrt{\gamma}\left(\frac{e}{\gamma}\right)^\gamma\right)^\sigma, \sqrt{\gamma}\left(\frac{e}{\gamma}\right)^\gamma\right) < 1 \tag{41}$$

Proof. The proof is similar to [8, Proposition 7.2]. Results only require conditions (11) and $K_{1,n} = \omega(1)$ to hold. The latter condition is clearly established in Lemma A.4. ∎

The rest of the paper is devoted to establishing (39) under the enforced assumptions on the scalings and with $\boldsymbol{X}_n$ as specified in (36), $\beta \in (0, \frac{1}{2})$ selected small enough such that (40) holds, and $\gamma \in (0, \frac{1}{2})$ selected small enough such that (41) holds. We denote by $\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)(S)$ a subgraph of $\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ whose vertices are restricted to the set S. Define the events

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := [\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)(S) \text{ is connected}]$$
$$B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := [\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)(S) \text{ is isolated}]$$
$$A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$$

In other words, $A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$ encodes the event that $\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)(S)$ 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 $1 \leq |S| \leq \lfloor \frac{n}{2} \rfloor$; note that if vertices S form a component then so do vertices $\mathcal{N} - S$. The event $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ eliminates the possibility of $\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\Theta}_n)(S)$ containing a component of size one (i.e., an isolated node), whence we have

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \subseteq \cup_{S \in \mathcal{N} : 2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$$

and the conclusion

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \sum_{S \in \mathcal{N} : 2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)]$$

follows. By exchangeability, we get

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$
$$\leq \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{S \in \mathcal{N}_{n,\ell}} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \right)$$
$$= \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \quad (42)$$

where $\mathcal{N}_{n,\ell}$ denotes the collection of all subsets of $\{1, \ldots, n\}$ with exactly ℓ elements, and $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that the set $\{1, \ldots, \ell\}$ of nodes form a component. As before we have $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, where $C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that $\{1, \ldots, \ell\}$ is connected and $B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ 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

$$\nu_{\ell,j}(\alpha) := \{i = 1, 2, \ldots, \ell : B_{ij}(\alpha) = 1\} \quad (43)$$

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

$$B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \bigcap_{m=\ell+1}^{n} \left[(\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i) \cap \Sigma_m = \emptyset \right].$$

We have

$$\mathbb{P}[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \mid \Sigma_1, \ldots, \Sigma_\ell]$$
$$= \mathbb{E}\left[\prod_{m=\ell+1}^{n} \frac{\binom{P - |\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell \right]$$
$$= \prod_{m=\ell+1}^{n} \mathbb{E}\left[\frac{\binom{P - |\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell \right]$$
$$= \mathbb{E}\left[\frac{\binom{P - |\cup_{i \in \nu_\ell(\alpha_n)} \Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell \right]^{n-\ell} \quad (44)$$

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, $\nu_\ell(\alpha_n)$ 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_j with probability μ_j.

We will leverage the expression (44) in (42) in the following manner. Note that on the event $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c$, we have

$$\left| \cup_{i \in \nu_\ell(\alpha_n)} \Sigma_i \right| \geq \left(X_{n,\nu_\ell(\alpha_n)} + 1 \right) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0] \quad (45)$$

while the crude bound

$$\left| \cup_{i \in \nu_\ell(\alpha_n)} \Sigma_i \right| \geq K_{1,n} \mathbf{1}[|\nu_\ell(\alpha_n)| > 0] \quad (46)$$

always holds. These bounds lead to

$$\mathbb{P}[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \mid \Sigma_1, \ldots, \Sigma_\ell]$$
$$\leq \mathbb{E}\left[\frac{\binom{P - \max(K_{1,n}, X_{n,\nu_\ell(\alpha_n)} + 1) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0]}{|\Sigma|}}{\binom{P}{|\Sigma|}} \right]^{n-\ell} \quad (47)$$

Conditioning on $\Sigma_1, \ldots, \Sigma_\ell$ and $\{B_{ij}(\alpha_n), 1 \leq i < j \leq \ell\}$, we then get

$$\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$
$$= \mathbb{E}[\mathbf{1}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \mathbf{1}[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]]$$
$$\leq \mathbb{E}\Bigg[\mathbf{1}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \cdot$$
$$\cdot \mathbb{E}\left[\left(\frac{\binom{P - \max(K_{1,n}, X_{n,\nu_\ell(\alpha_n)} + 1) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0]}{|\Sigma|}}{\binom{P}{|\Sigma|}} \right) \right]^{n-\ell} \Bigg]$$
$$= \mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \mathbb{E}\left[\frac{\binom{P - \max(K_{1,n}, X_{n,\nu_\ell(\alpha_n)} + 1) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0]}{|\Sigma|}}{\binom{P}{|\Sigma|}} \right]^{n-\ell} \quad (48)$$

since $C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ is fully determined by $\Sigma_1, \ldots, \Sigma_\ell$ and $\{B_{ij}(\alpha_n), 1 \leq i < j \leq \ell\}$, and $B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ and $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)$ are independent from $\{B_{ij}(\alpha_n), 1 \leq i, j \leq \ell\}$.

The next result establishes bounds for both terms at (48).

Lemma 7.2. *Consider a distribution* $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_r)$, *integers* $K_1 \leq \cdots \leq K_r \leq P/2$, *and* $\alpha \in (0, 1)$. *With* $\boldsymbol{X}_n$ *as specified in (36),* $\beta \in (0, \frac{1}{2})$ *and* $\gamma \in (0, \frac{1}{2})$, *we have*

$$\mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \leq \min\left\{ 1, \ell^{\ell-2} (\alpha p_{rr})^{\ell-1} \right\} \quad (49)$$

and

$$\mathbb{E}\left[\frac{\binom{P-\max(K_1, X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \min\left\{1 - \alpha\lambda_1,\right.$$

$$\left. \min\{1 - \mu_r + \mu_r e^{-\alpha p_{1r}\beta\ell}, e^{-\alpha p_{11}\beta\ell}\} + e^{-\gamma K_1}\mathbf{1}[\ell > L_n]\right\} \tag{50}$$

The proof of Lemma 7.2 is given in Appendix D.

Our proof of (39) will be completed (see (42)) upon establishing

$$\lim_{n\to\infty}\sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0 \tag{51}$$

by means of (48), (49), and (50). These steps are taken in Appendix E. This establishes the one-law.

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] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 8, no. 2, pp. 2–23, Second 2006.

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

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of IEEE S&P 2003*, May, pp. 197–213.

[5] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds., *Wireless Sensor Networks*. Norwell, MA, USA: Kluwer Academic Publishers, 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] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proc. of IEEE INFOCOM 2005*, March, pp. 878–890 vol. 2.

[8] 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.

[9] 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.

[10] M. D. Penrose, *Random Geometric Graphs*. Oxford University Press, Jul. 2003.

[11] M. D. Penrose *et al.*, "Connectivity of soft random geometric graphs," *The Annals of Applied Probability*, vol. 26, no. 2, pp. 986–1028, 2016.

[12] 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.

[13] O. Yağan and A. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1740–1760, March 2013.

[14] 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.

[15] J. Zhao, O. Yağan, and V. Gligor, "On the strengths of connectivity and robustness in general random intersection graphs," in *Proc. of IEEE CDC 2014*, 2014, pp. 3661–3668.

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

[17] E. Godehardt and J. Jaworski, "Two models of random intersection graphs for classification," in *Exploratory data analysis in empirical research*. Springer, 2003, pp. 67–81.

[18] B. Bollobás, *Random graphs*. Cambridge university press, 2001, vol. 73.

[19] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *Proc. of ACM TISSEC 2008*, vol. 11, no. 3, pp. 13:1–13:22, Mar. 2008.

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

[21] 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.

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

[23] J. Zhao, "Analyzing connectivity of heterogeneous secure sensor networks," *IEEE Transactions on Control of Network Systems*, vol. PP, no. 99, pp. 1–1, 2016.

[24] J. Zhao, O. Yağan, and V. Gligor, "On connectivity and robustness in random intersection graphs," *IEEE Transactions on Automatic 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 Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1038–1048, June 2013.

[26] E. Bakshy, I. Rosenn, C. Marlow, and L. Adamic, "The role of social networks in information diffusion," in *Proc. of WWW 2012*. New York, NY, USA: ACM, pp. 519–528.

[27] O. Yağan and V. Gligor, "Analysis of complex contagions in random multiplex networks," *Phys. Rev. E*, vol. 86, p. 036103, Sep 2012.

[28] D. Kempe, J. Kleinberg, and E. Tardos, "Maximizing the spread of influence through a social network," in *Proc. of ACM SIGKDD 2003*. ACM, pp. 137–146.

[29] S. Eubank, H. Guclu, V. Anil Kumar, M. V. Marathe, and e. al, "Modeling disease outbreaks in realistic urban social networks," *Nature*, vol. 429, no. 6988, pp. 180–4, May 13 2004.

[30] M. E. J. Newman, "Spread of epidemic disease on networks," *Phys. Rev. E*, vol. 66, p. 016128, Jul 2002.

[31] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[32] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *nature*, vol. 393, no. 6684, p. 440, 1998.

[33] L. A. N. Amaral, A. Scala, M. Barthelemy, and H. E. Stanley, "Classes of small-world networks," *Proceedings of the National Academy of Sciences*, vol. 97, no. 21, pp. 11 149–11 152, 2000.

[34] O. Yağan and A. M. Makowski, "Counting triangles, tunable clustering and the small-world property in random key graphs (Extended version)," *ArXiv e-prints*, Jan. 2017.

[35] M. Deijfen and W. Kets, "Random intersection graphs with tunable degree distribution and clustering," *Probability in the Engineering and Informational Sciences*, vol. 23, no. 4, p. 661674, 2009.

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

[37] S. T. Jensen, "The laguerre-samuelson inequality with extensions and applications in statistics and matrix theory," Ph.D. dissertation, Department of Mathematics and Statistics, McGill University, 1999.

[38] O. Yağan, "Random graph modeling of key distribution scheme in wireless sensor networks," Ph.D. dissertation, University of Maryland, College Park (MD), 2011.

[39] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key distribution schemes," in *Proc. of WiOpt 2011*, May 2011, pp. 257–264.

[40] G. E. Martin, *Counting: The art of enumerative combinatorics*. Springer Science & Business Media, 2013.

APPENDIX A
PRELIMINARIES

Lemma A.1 ([8, Lemma 4.2]). *Consider any scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$. For any $i, j = 1, \ldots, r$,*

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

and we have the asymptotic equivalence

$$p_{ij}(n) \sim \frac{K_{i,n} K_{j,n}}{P_n}. \tag{A.1}$$

Proposition A.2 ([8, Proposition 4.4]). *For any set of positive integers $K_1, \ldots, K_r, P$ and any scalar $a \geq 1$, we have*

$$\frac{\binom{P - \lceil a K_i \rceil}{K_j}}{\binom{P}{K_j}} \leq \left(\frac{\binom{P - K_i}{K_j}}{\binom{P}{K_j}} \right)^a, \quad i, j = 1, \ldots, r. \tag{A.2}$$

Lemma A.3. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7) holds. We have*

$$c_n \frac{\log n}{n \alpha_n} \leq p_{1r}(n) \leq \frac{c_n}{\mu_r} \frac{\log n}{n \alpha_n} \tag{A.3}$$

If in addition (12) holds, we have

$$p_{rr}(n) = o\left(\frac{(\log n)^2}{n \alpha_n} \right). \tag{A.4}$$

A proof of Lemma A.3 is given in Appendix B.

Lemma A.4. *Under (12), we have*

$$\frac{K_{1,n}^2}{P_n} = \omega\left(\frac{1}{n \alpha_n} \right), \tag{A.5}$$

and

$$K_{1,n} = \omega(1). \tag{A.6}$$

Proof. It is a simple matter to check that $p_{11}(n) \leq \frac{K_{1,n}^2}{P_n - K_{1,n}}$; see [14, Proposition 7.1-7.2] for a proof. In view of (6) this gives $p_{11}(n) \leq 2 \frac{K_{1,n}^2}{P_n}$. Thus, we have

$$\frac{K_{1,n}^2}{P_n} = \Omega\left(p_{11}(n) \right) = \omega\left(\frac{1}{n \alpha_n} \right).$$

From (11), (A.5), and $\alpha_n \leq 1$, we readily obtain (A.6). ∎

Other useful bounds that will be used throughout are

$$\binom{n}{\ell} \leq \left(\frac{en}{\ell} \right)^\ell, \quad \ell = 1, \ldots, n, \quad n = 1, 2, \ldots \tag{A.7}$$

$$\sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \leq 2^n \tag{A.8}$$

APPENDIX B
A PROOF OF LEMMA A.3

We know from (9) that

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

Since p_{1j} is monotone increasing in $j = 1, \ldots, r$ by virtue of (15), we readily obtain the bounds

$$c_n \frac{\log n}{n \alpha_n} \leq p_{1r}(n) \leq \frac{c_n}{\mu_r} \frac{\log n}{n \alpha_n} \tag{B.9}$$

which establishes (A.3).

In view of (B.9) that implies $p_{1r}(n) = \Theta(\frac{\log n}{\alpha_n n})$, we will obtain (A.4) if we show that $p_{rr}(n) = o(\log n) p_{1r}(n)$. Here this will be established by showing that

$$p_{rr}(n) \leq \max\left(2, \frac{8 c_n}{\mu_r} \frac{\log n}{w_n} \right) p_{1r}(n), \quad n = 2, 3, \ldots \tag{B.10}$$

for some sequence w_n such that $\lim_{n \to \infty} w_n = \infty$. Fix $n = 2, 3, \ldots$. We have either $p_{1r}(n) > \frac{1}{2}$, or $p_{1r}(n) \leq \frac{1}{2}$. In the former case, it automatically holds that

$$p_{rr}(n) \leq 2 p_{1r}(n) \tag{B.11}$$

by virtue of the fact that $p_{rr}(n) \leq 1$.

Assume now that $p_{1r}(n) \leq \frac{1}{2}$. We know from [14, Lemmas 7.1-7.2] that

$$1 - e^{-\frac{K_{j,n} K_{r,n}}{P_n}} \leq p_{jr}(n) \leq \frac{K_{j,n} K_{r,n}}{P_n - K_{j,n}}, \quad j = 1, \ldots, r \tag{B.12}$$

and it follows that

$$\frac{K_{1,n} K_{r,n}}{P_n} \leq \log\left(\frac{1}{1 - p_{1r}(n)} \right) \leq \log 2 < 1. \tag{B.13}$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ with x in $(0, 1)$, we then get

$$p_{1r}(n) \geq \frac{K_{1,n} K_{r,n}}{2 P_n}. \tag{B.14}$$

In addition, using the upper bound in (B.12) with $j = r$ gives

$$p_{rr}(n) \leq \frac{K_{r,n}^2}{P_n - K_{r,n}} \leq 2 \frac{K_{r,n}^2}{P_n}$$

as we invoke (6). Combining the last two bounds we obtain

$$\frac{p_{rr}(n)}{p_{1r}(n)} \leq 4 \frac{K_{r,n}}{K_{1,n}} \tag{B.15}$$

In order to bound the term $K_{r,n}/K_{1,n}$, we recall from Lemma A.4 that (12) implies (A.5), i.e., that $\frac{K_{1,n}^2}{P_n} = \frac{w_n}{n \alpha_n}$, for some sequence w_n satisfying $\lim_{n \to \infty} w_n = \infty$. Using this together with (B.14) and (B.9) we then get

$$\frac{K_{r,n}}{K_{1,n}} = \frac{\frac{K_{1,n} K_{r,n}}{P_n}}{\frac{K_{1,n}^2}{P_n}} \leq \frac{2 p_{1r}(n)}{\frac{w_n}{n \alpha_n}} \leq \frac{2 \frac{c_n}{\mu_r} \frac{\log n}{n \alpha_n}}{\frac{w_n}{n \alpha_n}} = \frac{2 c_n}{\mu_r} \frac{\log n}{w_n}$$

Reporting this into (B.15) we get

$$p_{rr}(n) \leq \frac{8 c_n}{\mu_r} \frac{\log n}{w_n} p_{1r}(n). \tag{B.16}$$

Combining (B.11) and (B.16), we readily obtain (B.10).

APPENDIX C
PROOF OF PROPOSITION 6.3

Consider fixed $\boldsymbol{\Theta}$.

$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]$

$= \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated} \cap t_1 = 1, t_2 = 1]\right]$

$= \mu_1^2 \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated}] \,\Big|\, t_1 = 1, t_2 = 1\right]$

$= \mu_1^2 \mathbb{E}\left[\mathbf{1}[v_1 \nsim v_2] \prod_{m=3}^{n} \mathbf{1}[v_m \nsim v_1, v_m \nsim v_2] \,\Big|\, t_1 = t_2 = 1\right]$

Now we condition on Σ_1 and Σ_2 and note that i) Σ_1 and Σ_2 determine t_1 and t_2; and ii) the events $[v_1 \nsim v_2]$, $\{[v_m \nsim v_1 \cap v_m \nsim v_2]\}_{m=3}^n$ are mutually independent given Σ_1 and Σ_2. Thus, we have

$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]$

$= \mu_1^2 \mathbb{E}\Bigg[\mathbb{P}\left[v_1 \nsim v_2 \,\Big|\, \Sigma_1, \Sigma_2\right] \cdot$ (C.17)

$\prod_{m=3}^{n} \mathbb{P}\left[v_m \nsim v_1 \cap v_m \nsim v_2 \,\Big|\, \Sigma_1, \Sigma_2\right] \,\Big|\, t_1 = t_2 = 1\Bigg]$

Define the $\{0,1\}$-valued rv $u(\boldsymbol{\theta})$ by

$$u(\boldsymbol{\theta}) := \mathbf{1}[\Sigma_1 \cap \Sigma_2 \neq \emptyset].$$ (C.18)

Recalling (43), (C.17) gives

$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]$

$= \mu_1^2 \mathbb{E}\left[(1-\alpha)^{u(\boldsymbol{\theta})} \prod_{m=3}^{n} \frac{\binom{P-\left|\cup_{i \in \nu_{2,m}(\alpha)}\Sigma_i\right|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \,\Big|\, t_1 = t_2 = 1\right]$

Conditioned on $u(\boldsymbol{\theta}) = 0$ and v_1, v_2 being class-1, we have

$$\left|\cup_{i \in \nu_{2,m}(\alpha)}\Sigma_i\right| = |\nu_{2,m}(\alpha)| \, K_1.$$

Also, we have

$$\mathbb{P}[u(\boldsymbol{\theta_n}) = 0 \mid t_1 = t_2 = 1] = 1 - p_{11}.$$

Thus, we get

$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\,\mathbf{1}[u(\boldsymbol{\theta}) = 0]]$

$= \mu_1^2(1-p_{11})\mathbb{E}\left[\prod_{m=3}^{n} \frac{\binom{P-|\nu_{2,m}(\alpha)K_1|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}}\right]$

$= \mu_1^2(1-p_{11})\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}}\right]^{n-2}$

$= \mu_1^2(1-p_{11})\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}} \,\Big|\, t_3 = j\right]\right)^{n-2}$

$= \mu_1^2(1-p_{11})\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{K_j}}{\binom{P}{K_j}}\right]\right)^{n-2}$

$\leq \mu_1^2(1-p_{11})\mathbb{E}\left[\sum_{j=1}^{r}\mu_j\left(\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}}\right)^{|\nu_{2,3}(\alpha)|}\right]^{n-2}$

where we use (A.2) in the last step.

Now, let $Z(\boldsymbol{\theta})$ denote a rv that takes the value

$$\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} \quad \text{with probability} \quad \mu_j, \quad j = 1,\dots,r. \quad \text{(C.19)}$$

In other words, $Z(\boldsymbol{\theta}) = 1 - p_{1j}$ with probability μ_j so that $\mathbb{E}[Z(\boldsymbol{\theta})] = 1 - \lambda_1$. Then,

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta}) = 0]]$$
$$\leq \mu_1^2(1-p_{11})\mathbb{E}\left[Z(\boldsymbol{\theta})^{|\nu_{2,3}(\alpha)|}\right]^{n-2} \quad \text{(C.20)}$$

Under the independent on/off channel model, we have that $|\nu_{2,3}(\alpha)|$ is a Binomial rv, i.e., $|\nu_{2,3}(\alpha)| =_{st} \text{Bin}(2,\alpha)$. Hence,

$$\mu_1^2(1-p_{11})\mathbb{E}\left[Z(\boldsymbol{\theta})^{|\nu_{2,3}(\alpha)|}\right]^{n-2} \quad \text{(C.21)}$$

$$= \mathbb{E}\left[\sum_{i=0}^{2}\binom{2}{i}\alpha^i(1-\alpha)^{2-i}Z(\boldsymbol{\theta})^i\right]^{n-2}$$

$$= \mu_1^2(1-p_{11})\mathbb{E}\left[(1-\alpha)^2 + 2\alpha(1-\alpha)Z(\boldsymbol{\theta}) + \alpha^2 Z(\boldsymbol{\theta})^2\right]^{n-2}$$

Conditioning on $u(\boldsymbol{\theta}) = 1$ and $t_1 = t_2 = 1$, we have

$$\left|\cup_{i \in \nu_{2,m}(\alpha)}\Sigma_i\right| = \begin{cases} 0 & \text{if } |\nu_{2,m}(\alpha)| = 0 \\ K_1 & \text{if } |\nu_{2,m}(\alpha)| = 1 \\ 2K_1 - |\Sigma_1 \cap \Sigma_2| & \text{if } |\nu_{2,m}(\alpha)| = 2 \end{cases}$$

and by a crude bounding argument, we have

$$\left|\cup_{i \in \nu_{2,m}(\alpha)}\Sigma_i\right| \geq K_1\mathbf{1}[|\nu_{2,m}(\alpha)| > 0] \quad \text{(C.22)}$$

Using (C.22) and recalling the analysis for $\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta}) = 0]]$, we obtain

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta}) = 1]]$$
$$\leq \mu_1^2 p_{11}(1-\alpha)\mathbb{E}\left[Z(\boldsymbol{\theta})^{\mathbf{1}[|\nu_{2,3}(\alpha)|>0]}\right]^{n-2}$$
$$= \mu_1^2 p_{11}(1-\alpha)\mathbb{E}\left[(1-\alpha)^2 + \left(1 - (1-\alpha)^2\right)Z_n\right]^{n-2}$$ (C.23)

Combining (C.20), (C.21), and (C.23), we get

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]$$
$$= \mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\left(\mathbf{1}[u(\boldsymbol{\theta}) = 0] + \mathbf{1}[u(\boldsymbol{\theta}) = 1]\right)]$$
$$\leq \mu_1^2(1-p_{11})\Big((1-\alpha)^2 + 2\alpha(1-\alpha)\mathbb{E}[Z(\boldsymbol{\theta})]$$
$$+ \alpha^2\mathbb{E}\left[Z(\boldsymbol{\theta})^2\right]\Big)^{n-2} + \mu_1^2 p_{11}(1-\alpha)\Big((1-\alpha)^2$$
$$+ \left(1 - (1-\alpha)^2\right)\mathbb{E}[Z(\boldsymbol{\theta})]\Big)^{n-2}$$ (C.24)

It is clear from (28) and the definition of $Z(\boldsymbol{\theta})$ that

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})] = \mu_1\left(\sum_{j=1}^{r}\mu_j(1-\alpha p_{1j})\right)^{n-1}$$
$$= \mu_1\left((1-\alpha) + \alpha\mathbb{E}[Z(\boldsymbol{\theta})]\right)^{n-1} \quad \text{(C.25)}$$

Combining (C.24) and (C.25), we get

$$\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]}{\mathbb{E}[x_{n,1}(\boldsymbol{\theta})]^2}$$

$$\leq (1-p_{11})\frac{\left((1-\alpha)^2 + 2\alpha(1-\alpha)\mathbb{E}[Z(\boldsymbol{\theta})] + \alpha^2\mathbb{E}[Z(\boldsymbol{\theta})^2]\right)^{n-2}}{\left((1-\alpha) + \alpha\mathbb{E}\left[Z(\boldsymbol{\theta})\right]\right)^{2(n-1)}}$$

$$+ p_{11}\frac{\left((1-\alpha)^2 + \left(1 - (1-\alpha)^2\right)\mathbb{E}[Z(\boldsymbol{\theta})]\right)^{n-2}}{\left((1-\alpha) + \alpha\mathbb{E}\left[Z(\boldsymbol{\theta})\right]\right)^{2(n-1)}}$$

$$:= A + B \tag{C.26}$$

where we use the fact that $1 - \alpha \leq 1$.

We now consider a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ as stated in Proposition 6.3 and bound the terms A and B in turn. Our goal is to show that

$$\limsup_{n\to\infty}(A+B) \leq 1. \tag{C.27}$$

First, we write $\mathbb{E}[Z(\boldsymbol{\theta}_n)^2] = \mathbb{E}[Z(\boldsymbol{\theta}_n)]^2 + var[Z(\boldsymbol{\theta}_n)]$, where $var[Z(\boldsymbol{\theta}_n)]$ can be bounded by the Popoviciu's inequality [37, p. 9] as follows

$$var[Z(\boldsymbol{\theta}_n)] \leq \frac{1}{4}\left(\max(Z(\boldsymbol{\theta}_n)) - \min(Z(\boldsymbol{\theta}_n))\right)^2$$

$$= \frac{1}{4}\left(\frac{\binom{P_n - K_{1,n}}{K_{1,n}}}{\binom{P_n}{K_{1,n}}} - \frac{\binom{P_n - K_{1,n}}{K_{r,n}}}{\binom{P_n}{K_{r,n}}}\right)^2$$

$$\leq \frac{1}{4}\left(1 - \frac{\binom{P_n - K_{1,n}}{K_{r,n}}}{\binom{P_n}{K_{r,n}}}\right)^2 = \frac{1}{4}\left(p_{1r}(n)\right)^2.$$

Then, we get from the scaling condition (9) and (B.9) that

$$\mathbb{E}[Z(\boldsymbol{\theta}_n)^2] \leq \mathbb{E}[Z(\boldsymbol{\theta}_n)]^2 + \frac{1}{4}\left(\frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n}\right)^2$$

Reporting this into (C.26) we get

$$A \leq (1-p_{11})\frac{\left(((1-\alpha_n) + \alpha_n\mathbb{E}[Z(\boldsymbol{\theta}_n)])^2 + \left(\frac{c_n}{2\mu_r}\frac{\log n}{n}\right)^2\right)^{n-2}}{\left((1-\alpha_n) + \alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right]\right)^{2(n-1)}}$$

$$= (1 + o(1))(1-p_{11})\left(1 + \left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1 - \alpha_n + \alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n\right]}\right)^2\right)^{n-2}$$

where we used the fact that

$$\left((1-\alpha_n) + \alpha_n\mathbb{E}[Z(\boldsymbol{\theta}_n)]\right)^2 = (1 - \alpha_n\lambda_1(n))^2 = 1 - o(1) \tag{C.28}$$

since $\alpha_n\lambda_1(n) = c_n\log n/n$. Finally, we have

$$\left(1 + \left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1 - \alpha_n + \alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n\right]}\right)^2\right)^{n-2}$$

$$\leq \exp\left\{n\left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1 - c_n\frac{\log n}{n}}\right)^2\right\} = o(1)$$

since $\lim_{n\to\infty} c_n = c > 0$ and $\mu_r > 0$. Thus, we obtain the bound

$$A \leq (1 - p_{11})(1 + o(1)). \tag{C.29}$$

We now consider the second term in (C.26). Recall (C.28) and that $\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right] = 1 - \lambda_1(n) = 1 - c_n\log n/n$. We have

$$B = \frac{p_{11}}{(1 - \alpha_n + \alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right])^2}.$$

$$\cdot\left(1 + \frac{\alpha_n^2\mathbb{E}[Z(\boldsymbol{\theta}_n)](1 - \mathbb{E}[Z(\boldsymbol{\theta}_n)])}{(1 - \alpha_n + \alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right])^2}\right)^{n-2}$$

$$\leq p_{11}(1 + o(1))\exp\left\{n\frac{\alpha_n^2 c_n\frac{\log n}{n\alpha_n}(1 - c_n\frac{\log n}{n\alpha_n})}{(1 - c_n\frac{\log n}{n})^2}\right\}$$

$$\leq p_{11}(1 + o(1))\exp\left\{\frac{c_n\alpha_n\log n}{\left(1 - c_n\frac{\log n}{n}\right)^2}\right\} \tag{C.30}$$

We will now establish the desired result (C.27) by using (C.29) and (C.30). Our approach is based on the subsubsequence principle [36, p. 12] and considering the cases $\lim_{n\to\infty}\alpha_n\log n = 0$ and $\lim_{n\to\infty}\alpha_n\log n \in (0, \infty]$ separately.

a) Assume that $\lim_{n\to\infty}\alpha_n\log n = 0$: From (C.30) we get $B \leq (1 + o(1))p_{11}$ and upon using (C.29) we see that $A + B \leq (1 + o(1))$ establishing (C.27) along subsequences with $\lim_{n\to\infty}\alpha_n\log n = 0$.

b) Assume that $\lim_{n\to\infty}\alpha_n\log n \in (0, \infty]$: Since p_{1j} is monotonically increasing in $j = 1, \ldots, r$ (see (15)), we have

$$\lambda_1 = \sum_{j=1}^{r}\mu_j p_{1j} \geq p_{11}\sum_{j=1}^{r}\mu_j = p_{11}$$

Thus, $p_{11} \leq \lambda_1(n) = c_n\log n/(\alpha_n n)$. Then, (C.30) gives

$$B \leq (1 + o(1))\frac{c_n\log n}{\alpha_n n}\exp\left\{\frac{c_n\alpha_n\log n}{(1 - c_n\log n/n)^2}\right\}$$

$$= (1 + o(1))\frac{c_n(\log n)^2}{\alpha_n\log n}n^{-1 + \frac{c_n\alpha_n}{(1 - c_n\log n/n)^2}}$$

$$= o(1)$$

since $\lim_{n\to\infty}\alpha_n\log n > 0$ along this subsequence and

$$\lim_{n\to\infty} -1 + \frac{c_n\alpha_n}{(1 - c_n\log n/n)^2} < 0$$

given that $\lim_{n\to\infty} c_n = c < 1$. From (C.29) and the fact that $p_{11} \leq 1$, we have $A \leq 1 + o(1)$, and (C.27) follows.

The two cases considered cover all the possibilities for the limit of $\alpha_n\log n$. By virtue of the subsubsequence principle [36, p. 12], we get (C.27) without any condition on the sequence $\alpha_n\log n$; i.e., we obtain (C.27) even when the sequence $\alpha_n\log n$ does not have a limit!

APPENDIX D
ESTABLISHING LEMMA 7.2

The bounds given at Lemma 7.2 are valid irrespective of how the parameters involved scale with n. Thus, we consider fixed $\boldsymbol{\Theta}$ with constraints given in the statement of Lemma 7.2.

We first establish (50) starting with the first bound. Recall that $|\nu_\ell(\alpha)|$ is a Binomial rv with ℓ trials and success probability α. Recall also the rv $Z(\boldsymbol{\theta})$ defined at (C.19). Using a crude bound and then (A.2) we get

$$\mathbb{E}\left[\frac{\binom{P - \max(K_1, X_{n,\nu_\ell(\alpha)} + 1)}{|\Sigma|}\mathbf{1}[|\nu_\ell(\alpha)| > 0]}{\binom{P}{|\Sigma|}}\right]$$

$$\leq \mathbb{E}\left[\frac{\binom{P-K_1 \mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$$

$$\leq \mathbb{E}\left[Z(\boldsymbol{\theta})^{\mathbf{1}[|\nu_\ell(\alpha)|>0]}\right]$$

$$= (1-\alpha)^\ell + \left(1 - (1-\alpha)^\ell\right)\mathbb{E}[Z(\boldsymbol{\theta})]$$

$$\leq 1 - \alpha + \alpha\mathbb{E}[Z(\boldsymbol{\theta})] = 1 - \alpha\lambda_1(n). \qquad \text{(D.31)}$$

upon noting that $\mathbb{E}[Z(\boldsymbol{\theta})] = 1 - \lambda_1 \leq 1$.

Next, consider range $\ell = 1, \ldots, L_n$, where we have

$$\left(X_{n,\nu_\ell(\alpha)} + 1\right)\mathbf{1}[|\nu_\ell(\alpha)| > 0] \geq \lceil \beta|\nu_\ell(\alpha)|K_1 \rceil$$

Recalling (A.2), we get

$$\mathbb{E}\left[\frac{\binom{P-\max(K_1, X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$$

$$\leq \mathbb{E}\left[\frac{\binom{P-\beta|\nu_\ell(\alpha)|K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$$

$$= \mathbb{E}\left[Z(\boldsymbol{\theta})^{\beta|\nu_\ell(\alpha)|}\right]$$

$$= \mathbb{E}\left[\sum_{j=0}^\ell \binom{\ell}{j}\alpha^j(1-\alpha)^{\ell-j}Z(\boldsymbol{\theta})^{\beta j}\right]$$

$$= \mathbb{E}\left[\left(1 - \alpha\left(1 - Z(\boldsymbol{\theta})^\beta\right)\right)^\ell\right]$$

$$\leq \mathbb{E}\left[\left(1 - \alpha\beta\left(1 - Z(\boldsymbol{\theta})\right)\right)^\ell\right] \leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] \quad \text{(D.32)}$$

using the fact that $1 - Z(\boldsymbol{\theta})^\beta \geq \beta(1 - Z(\boldsymbol{\theta}))$ with $Z(\boldsymbol{\theta}) \leq 1$ and $0 \leq \beta \leq 1$; a proof is available at [12, Lemma 5.2]. On the range $\ell = L_n + 1, \ldots, \lfloor\frac{n}{2}\rfloor$, $|\nu_\ell(\alpha)|$ can be less than or greater than L_n. In the latter case, we have

$$\max(K_1, X_{n,\nu_\ell(\alpha)} + 1)\mathbf{1}[|\nu_\ell(\alpha)| > 0] \geq \lfloor \gamma P \rfloor + 1$$

Using (D.32) and the fact that (see [38, Lemma 5.4.1] for a proof)

$$\binom{P-K_1}{K_2}\Big/\binom{P}{K_2} \leq e^{-\frac{K_2}{P}K_1}$$

for $K_1 + K_2 \leq P$, we have

$$\mathbb{E}\left[\frac{\binom{P-\max(K_1, X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$$

$$\leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\mathbf{1}[|\nu_\ell(\alpha)| \leq L_n]\right]$$

$$+ \mathbb{E}\left[e^{-\frac{|\Sigma|}{P}(\lfloor\gamma P\rfloor+1)}\mathbf{1}[|\nu_\ell(\alpha)| > L_n]\right]$$

$$\leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] + e^{-\gamma K_1}\mathbf{1}[\ell > L_n] \qquad \text{(D.33)}$$

by virtue of the fact that $|\Sigma| \geq K_1$.

Finally, we get (50) from (D.31) and (D.33) by noting that

$$\mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] = \sum_{j=1}^r \mu_j e^{-\alpha p_{1j}\beta\ell} \leq (1-\mu_r) + \mu_r e^{-\alpha p_{1r}\beta\ell}$$

and that

$$\mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] = \sum_{j=1}^r \mu_j e^{-\alpha p_{1j}\beta\ell} \leq e^{-\alpha p_{11}\beta\ell} \qquad \text{(D.34)}$$

The last step used the fact that p_{ij} is monotone increasing in both i and j.

Next, we establish (49). This is a version of a fairly standard bound derived previously for various other random graph models including ER graphs [18], random key graphs [14], and random K-out graphs [13], [39]. The proof is very similar to that of [8, Proposition 9.1] and [12, Lemma 10.2]. We give it below for completeness.

Let $\mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ denote the subgraph of $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ induced on the vertices $\{v_1, \ldots, v_\ell\}$. $\mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is connected if and only if it contains a spanning tree; i.e., we have

$$C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}) = \cup_{T\in\mathcal{T}_\ell}\left[T \subseteq \mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})\right]$$

where $\mathcal{T}_\ell$ denotes the collection of all spanning trees on the vertices $\{v_1, \ldots, v_\ell\}$. Thus,

$$\mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \leq \sum_{T\in\mathcal{T}_\ell}\mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})\right]. \qquad \text{(D.35)}$$

Given that $K_1 \leq K_2 \leq \ldots \leq K_r$, the probability of T being contained in $\mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})$ is maximized when all nodes receive the largest possible number K_r of keys. Thus, for any $T \in \mathcal{T}$ and distribution $\boldsymbol{\mu}$ we have

$$\mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta})\right] \leq \mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n; \boldsymbol{\mu} = \{0, 0, \ldots, 1\}, \boldsymbol{\Theta})\right]$$

$$= (\alpha p_{rr})^{\ell-1} \qquad \text{(D.36)}$$

where the last equality follows from the facts that i) a tree on ℓ vertices contain $\ell - 1$ edges, and ii) since all nodes have the same key ring size, edges in $\mathbb{G}_\ell(n; \boldsymbol{\mu} = \{0, 0, \ldots, 1\}, \boldsymbol{\Theta})$ are *pairwise* independent; see [14, Lemma 9.1] and [12, Eq. 64]. We obtain (49) upon using (D.36) in (D.35) and noting by Cayley's formula [40] that there are $\ell^{\ell-2}$ trees on ℓ vertices, i.e., $|\mathcal{T}_\ell| = \ell^{\ell-2}$.

APPENDIX E
ESTABLISHING (51)

We will establish (51) in several steps with each step focusing on a specific range of the summation over ℓ. Throughout, we consider a scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0, 1)$ such that (7) holds with $c > 1$, (12), and (11) hold.

1) The case where $2 \leq \ell \leq R$: This range considers fixed values of ℓ. Pick an integer R to be specified later at (E.42). Use (7), (A.4), (A.7), (48), (49), and the first bound in (50) to get

$$\sum_{\ell=2}^R \binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq \sum_{\ell=2}^R \left(\frac{en}{\ell}\right)^\ell \ell^{\ell-2}\left(\alpha_n p_{rr}(n)\right)^{\ell-1}\left(1 - \alpha_n\lambda_1(n)\right)^{n-\ell}$$

$$\leq \sum_{\ell=2}^R (en)^\ell\left(\frac{(\log n)^2}{n}\right)^{\ell-1}\left(1 - c_n\frac{\log n}{n}\right)^{n-\ell}$$

$$\leq \sum_{\ell=2}^R n\left(e(\log n)^2\right)^\ell e^{-c_n\log n\frac{n-\ell}{n}}$$

$$= \sum_{\ell=2}^{R} \left(e(\log n)^2\right)^{\ell} n^{1-c_n \frac{n-\ell}{n}}$$

With $c > 1$, we have $\lim_{n\to\infty} \left(1 - c_n \frac{n-\ell}{n}\right) = 1 - c < 0$. Thus, for each $\ell = 2, 3, \ldots$, we have

$$\left(e(\log n)^2\right)^{\ell-1} n^{1-c_n \frac{n-\ell}{n}} = o(1),$$

whence we get

$$\lim_{n\to\infty} \sum_{\ell=2}^{R} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0.$$

2) The case where $R+1 \leq \ell \leq \min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}$: Our goal in this and the next subsubsection is to cover the range $R + 1 \leq \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$. Since the bound given at (50) takes a different form when $\ell > L_n$, we first consider the range $R + 1 \leq \ell \leq \min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}$. Using (A.4), (A.7), (48), (49), and the second bound in (50) we get

$$\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq \sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \left(\frac{en}{\ell}\right)^{\ell} \ell^{\ell-2} \left(\frac{(\log n)^2}{n}\right)^{\ell-1} \cdot \quad \text{(E.37)}$$

$$\cdot \left(1 - \mu_r \left(1 - e^{-\alpha_n \beta \ell p_{1r}(n)}\right)\right)^{n-\ell}$$

From the upper bound in (A.3) and $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$, we have

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

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ for all $0 \leq x \leq 1$, we get

$$1 - \mu_r \left(1 - e^{-\alpha_n \beta \ell p_{1r}(n)}\right) \leq 1 - \frac{\mu_r \alpha_n \beta \ell p_{1r}(n)}{2} \leq e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} \quad \text{(E.38)}$$

using the lower bound in (A.3). Reporting this last bound in to (E.37) and noting that

$$n - \ell \geq \frac{n}{2}, \qquad \ell = 2, 3, \ldots, \left\lfloor \frac{n}{2} \right\rfloor, \quad \text{(E.39)}$$

we get

$$\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq \sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} n \left(e(\log n)^2\right)^{\ell} e^{-\beta \ell c_n \mu_r \frac{\log n}{2n} \frac{n}{2}}$$

$$\leq n \sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \left(e(\log n)^2 e^{-\beta c_n \frac{\mu_r}{4} \log n}\right)^{\ell}$$

$$\leq n \sum_{\ell=R+1}^{\infty} \left(e(\log n)^2 e^{-\beta c_n \frac{\mu_r}{4} \log n}\right)^{\ell} \quad \text{(E.40)}$$

Given that $\beta, \mu_r > 0$ and $\lim_{n\to\infty} c_n = c > 0$ we clearly have

$$e(\log n)^2 e^{-\beta c_n \log n \frac{\mu_r}{4}} = o(1). \quad \text{(E.41)}$$

Thus, the geometric series in (E.40) is summable, and we have

$$\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq (1 + o(1)) n \left(e(\log n)^2 e^{-\beta c_n \log n \frac{\mu_r}{4}}\right)^{R+1}$$

$$= (1 + o(1)) n^{1-(R+1)\beta c_n \frac{\mu_r}{4}} \left(e(\log n)^2\right)^{R+1}$$

$$= o(1)$$

for any positive integer R with

$$R > \frac{8}{\beta c \mu_r}. \quad \text{(E.42)}$$

This choice is permissible given that $c, \beta, \mu_r > 0$.

3) The case where $\min\{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor, \max(R, L_n)\} < \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$: Clearly, this range becomes obsolete if $\max(R, L_n) \geq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$. Thus, it suffices to consider the subsequences for which the range $\max(R, L_n) + 1 \leq \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$ is non-empty. There, we use (A.4), (A.7), (48), (49), and the second bound in (50) to get

$$\sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \quad \text{(E.43)}$$

$$\leq \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \left(\frac{en}{\ell}\right)^{\ell} \ell^{\ell-2} \left(\frac{(\log n)^2}{n}\right)^{\ell-1} \cdot$$

$$\left(1 - \mu_r \left(1 - e^{-\beta \ell \alpha_n p_{1r}(n)}\right) + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \cdot$$

$$\leq \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{2\beta c \log n} \rfloor} n \left(e(\log n)^2\right)^{\ell} \left(e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

where in the last step we used (E.38) in view of $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$.

Next, we write

$$e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}$$

$$= e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} \left(1 + e^{-\gamma K_{1,n} + \beta \ell c_n \mu_r \frac{\log n}{2n}}\right)$$

$$\leq \exp\left\{-\beta \ell c_n \mu_r \frac{\log n}{2n} + e^{-\gamma K_{1,n} + \beta \ell c_n \mu_r \frac{\log n}{2n}}\right\}$$

$$\leq \exp\left\{-\beta \ell c_n \mu_r \frac{\log n}{2n} \left(1 - \frac{e^{-\gamma K_{1,n} + \frac{\mu_r^2}{2}}}{\beta \ell c_n \mu_r \frac{\log n}{2n}}\right)\right\} \quad \text{(E.44)}$$

where the last inequality is obtained from $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$. Using the fact that $\ell > L_n = \min\{\lfloor \frac{P_n}{K_{1,n}} \rfloor, \lfloor \frac{n}{2} \rfloor\}$ and (11) we have

$$\frac{e^{-\gamma K_{1,n}}}{\beta \ell c_n \mu_r \frac{\log n}{2n}} \leq \max\left\{\frac{K_{1,n}}{P_n}, \frac{2}{n}\right\} 2n \frac{e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \log n}$$

$$\leq \max\left\{\frac{2 K_{1,n} e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \sigma \log n}, \frac{4 e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \log n}\right\}$$

$$= o(1)$$

by virtue of (A.6) and the facts that $\beta, \mu_r, \sigma, c_n > 0$. Reporting this into (E.44), we see that for for any $\epsilon > 0$, there exists a finite integer $n^*(\epsilon)$ such that

$$\left(e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right) \leq e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}(1-\epsilon)} \quad \text{(E.45)}$$

for all $n \geq n^*(\epsilon)$. Using (E.45) in (E.43), we get

$$\sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq n \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \left(e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{2n}(1-\epsilon)\frac{n}{2}} \right)^{\ell}$$

$$\leq n \sum_{\ell=\max(R,L_n)+1}^{\infty} \left(e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{4}(1-\epsilon)} \right)^{\ell} \quad \text{(E.46)}$$

Similar to (E.41), we have $e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{4}(1-\epsilon)} = o(1)$ so that the sum in (E.46) converges. Following a similar approach to that in Section E-2, we then see that

$$\lim_{n\to\infty} \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{2\beta c \log n} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

with R selected according to (E.42) and $\epsilon < 1/2$.

4) The case where $\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$: We consider $\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$ for some $\nu \in (0, \frac{1}{2})$ to be specified later. Recall (A.3), (A.7), (48), the first bound in (49), and the second bound in (50). Noting that $\binom{n}{\ell}$ is monotone increasing in ℓ when $0 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$ and using (E.39) we get

$$\sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\lfloor \nu n \rfloor} \left(1 - \mu_r + \mu_r e^{-\alpha_n \beta \ell p_{1r}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

$$\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\alpha_n \beta \frac{\mu_r n}{\beta c_n \log n} \frac{c_n \log n}{n \alpha_n}} \right.$$

$$\left. + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

$$\leq n \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\mu_r} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

$$= n \left(\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\mu_r} + e^{-\gamma K_{1,n}}\right)\right)^{\frac{n}{2}} \quad \text{(E.47)}$$

We have $1 - \mu_r + \mu_r e^{-\mu_r} < 1$ from $\mu_r > 0$ and $e^{-\gamma K_{1,n}} = o(1)$ from (A.6). Also, it holds that $\lim_{\nu \to 0} \left(\frac{e}{\nu}\right)^{2\nu} = 1$. Thus, if we pick ν small enough to ensure that

$$\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\mu_r}\right) < 1, \quad \text{(E.48)}$$

then for any $0 < \epsilon < 1 - (e/\nu)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\mu_r}\right)$ there exists a finite integer $n^*(\epsilon)$ such that

$$\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\mu_r} + e^{-\gamma K_{1,n}}\right) \leq 1-\epsilon, \quad \forall n \geq n^*(\epsilon).$$

Reporting this into (E.47), we get

$$\lim_{n\to\infty} \sum_{\ell=\lfloor \frac{\mu_r n}{2\beta c \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

since $\lim_{n\to\infty} n(1 - \epsilon)^{n/2} = 0$.

5) The case where $\lfloor \nu n \rfloor + 1 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$: In this range, we use (A.8), (48), the first bound in (49), the last bound in (50), and (E.39) to get

$$\sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c]$$

$$\leq \sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \left(e^{-\beta \ell \alpha_n p_{11}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

$$\leq \left(\sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \right) \left(e^{-\beta \nu n \alpha_n p_{11}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

$$\leq \left(4 e^{-\beta \nu n \alpha_n p_{11}(n)} + 4 e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}$$

With $\beta, \nu, \gamma > 0$ have $e^{-\beta \nu n \alpha_n p_{11}(n)} = o(1)$ from (12) and $e^{-\gamma K_{1,n}} = o(1)$ from (A.6). The conclusion

$$\lim_{n\to\infty} \sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

immediately follows and the proof of one-law is completed. ∎