On the gradual deployment of random pairwise key distribution schemes

Osman Yağan and Armand M. Makowski
Department of Electrical and Computer Engineering
and the Institute for Systems Research
University of Maryland, College Park
College Park, Maryland 20742
oyagan@umd.edu, armand@isr.umd.edu

***Abstract*— The pairwise key distribution scheme of Chan et al. is a randomized key predistribution scheme which enables cryptographic protection in wireless sensor networks (WSNs). This pairwise scheme has many advantages over other randomized key predistribution schemes but has been deemed *non-*scalable due to (i) the large number of keys required to ensure secure connectivity; and (ii) implementation difficulties when sensors are required to be deployed in multiple stages. Here, we address this issue by proposing an implementation of the pairwise scheme that supports the gradual deployment of sensor nodes in several consecutive phases. We show how the scheme parameter should be adjusted with the number n of sensors so that secure connectivity is maintained in the network throughout all the stages of the deployment. We also discuss briefly the relation between the scheme parameter and the amount of memory that each sensor needs to spare for storing their keys. By showing that $O(\log n)$ many keys per node suffice to achieve secure connectivity at every step of the deployment, we confirm the scalability of the pairwise scheme in the context of WSNs.**

Keywords: Wireless sensor networks, Security, Key predistribution, Random key graphs, Connectivity.

I. Introduction

Providing cryptographic protection has been identified as a serious challenge to the successful deployment of wireless sensor networks (WSNs); see [6], [9], [11] for discussions of some of the obstacles. *Random* key predistribution schemes were recently introduced to address some of these challenges. The idea of randomly assigning secure keys to sensor nodes prior to network deployment was first proposed by Eschenauer and Gligor [6]. The modeling and performance of the EG scheme, as we refer to it hereafter, has been extensively investigated [1], [4], [6], [10], [12], with most of the focus being on the *full visibility* case where nodes are all within communication range of each other. Although the assumption of full visibility does away with the wireless nature of the communication medium supporting WSNs, in return this simplification makes it possible to understand how randomizing the key selections affects the establishment of a secure network in the best of circumstances.

The work of Eschenauer and Gligor has spurred the development of other key distribution schemes, e.g., see [3], [5], [9], [11]. Here we consider the following random *pairwise* key predistribution scheme proposed by Chan et al. [3]: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected amongst all other $n-1$ nodes. For each such pairing, a unique pairwise key is generated and stored in the memory modules of each of the paired sensors along with the id of the other node. A secure link can then be established between two communicating nodes if at least one of them has been paired to the other (in which case they have at least one key in common). See Section II for implementation details.

This scheme has the following advantages over the EG scheme (and others): (i) Even if some nodes are captured, the secrecy of the remaining nodes is *perfectly* preserved; and (ii) Both node-to-node authentication and quorum-based revocation are enabled. Given these advantages, we found it of interest to assess the performance of the pairwise scheme, and in [13] we began a formal investigation along these lines: Let $\mathbb{H}(n;K)$ denote the random graph on the vertex set $\{1,\ldots,n\}$ where distinct nodes i and j are adjacent if they have a pairwise key in common; as in earlier work on the EG scheme this corresponds to modeling the random pairwise distribution scheme under full visibility. In [13] we showed that the probability of $\mathbb{H}(n;K)$ being connected approaches 1 (resp. 0) as n grows large if $K \geq 2$ (resp. if $K = 1$), i.e., $\mathbb{H}(n;K)$ is asymptotically almost surely (a.a.s.) connected whenever $K \geq 2$.

In [14], we revisited the connectivity issue under more realistic assumptions that account for the possibility that communication links between nodes may not be available. This was done in the context of a simple communication model where the communication channels are mutually independent, and are either on or off. For the resulting random graph structure, we established zero-one laws for two basic (and related) graph properties, namely graph connectivity and the absence of isolated nodes, when the model parameters are scaled with the number of users. The critical thresholds were identified and shown to coincide.

In the present paper, we continue our study of connectivity properties for the scheme of Chan et al., still under full visibility, but from a different perspective: We note that in many applications, the sensor nodes are expected to be deployed

gradually over time. Yet, the pairwise key distribution is an *offline* pairing mechanism which simultaneously involves all n nodes. Thus, once the network size n is set, there is no way to add more nodes to the network and still *recursively* expand the pairwise distribution scheme (as is possible for the EG scheme). However, as explained in Section II-B, the gradual deployment of a large number of sensor nodes is nevertheless feasible from a practical viewpoint. In that context we are interested in understanding how the parameter K needs to scale with n large in order to ensure that connectivity is *maintained* a.a.s. throughout gradual deployment.

The main contributions of the paper can be stated as follows: With $0 < \gamma < 1$, we denote by $\mathbb{H}_\gamma(n;K)$ the subgraph of $\mathbb{H}(n;K)$ restricted to the nodes $1,\ldots,\lfloor \gamma n \rfloor$. We first present scaling laws for the absence of isolated nodes in $\mathbb{H}_\gamma(n;K)$ in the form of a full zero-one law, and use these results to formulate conditions under which $\mathbb{H}_\gamma(n;K)$ is a.a.s. *not* connected. Then, with $0 < \gamma_1 < \gamma_2 < \ldots < \gamma_\ell < 1$, we give conditions on n, K and γ_1 so that $\mathbb{H}_{\gamma_i}(n;K)$ is a.a.s. connected for each $i = 1,2,\ldots,\ell$. This corresponds to the network being connected in *each* of the ℓ phases of the gradual deployment.

Since sensor nodes are expected to have very limited memory, it is desirable for practical key distribution schemes to have low memory requirements [5]. In contrast with the EG scheme (and its variants), the key rings produced by the pairwise scheme of Chan et al. have variable size between K and $K+(n-1)$. We have recently shown [15] that the *maximum* key ring size is on the order $\log n$ with very high probability provided $K = O(\log n)$. Using this fact it is possible to conclude that the sensor network can maintain the a.a.s. connectivity through all the phases of its deployment when the number of keys stored in each sensor's memory is $O(\log n)$; this is a key ring size comparable to that of the EG scheme (in realistic WSN scenarios [4]).

As with the results in [13], the assumption of full visibility may yield a dimensioning of the pairwise scheme which is too optimistic. This is due to the fact that the unreliable nature of wireless links has not been incorporated in the model. However the results obtained in this paper already yield a number of interesting observations: The zero-one laws obtained here differ significantly from the corresponding results in the single deployment case [13]. Thus, the gradual deployment may have a significant impact on the dimensioning of the pairwise distribution algorithm. Yet, the required number of keys to achieve secure connectivity being $O(\log n)$, it is still feasible to use the pairwise scheme in the case of gradual deployment; note that the required key ring size in EG scheme is also $O(\log n)$ under full visibility [4].

The rest of the paper is organized as follows: In Section II we introduce a framework to model the random pairwise distribution scheme; this section also describes an implementation of the scheme which supports gradual network deployment. We present the contributions of the paper in Section III, and Section IV contains some limited simulation results that illustrate the various zero-one laws obtained here. Section V gives some perspectives on these results in light of facts on the size of key rings derived in [15]. We conclude the paper with Sections VI and VII where proofs can be found.

II. The model

A. Implementing pairwise key distribution schemes

The random pairwise key predistribution scheme of Chan et al. is parametrized by two positive integers n and K such that $K < n$. There are n nodes which are labelled $i = 1,\ldots,n$. with unique ids $\mathrm{Id}_1,\ldots,\mathrm{Id}_n$. Write $\mathcal{N} := \{1,\ldots n\}$ and set $\mathcal{N}_{-i} := \mathcal{N} - \{i\}$ for each $i = 1,\ldots,n$. With node i we associate a subset $\Gamma_{n,i}$ of K nodes selected at *random* from $\mathcal{N}_{-i}$ – We say that each of the K nodes in $\Gamma_{n,i}$ is paired to node i. Thus, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

$$\mathbb{P}\left[\Gamma_{n,i} = A\right] = \begin{cases} \binom{n-1}{K}^{-1} & \text{if } |A| = K \\ 0 & \text{otherwise.} \end{cases}$$

The selection of $\Gamma_{n,i}$ is done *uniformly* amongst all subsets of $\mathcal{N}_{-i}$ which are of size exactly K. The rvs $\Gamma_{n,1},\ldots,\Gamma_{n,n}$ are assumed to be mutually independent so that

$$\mathbb{P}\left[\Gamma_{n,i} = A_i,\ i = 1,\ldots,n\right] = \prod_{i=1}^{n} \mathbb{P}\left[\Gamma_{n,i} = A_i\right]$$

for arbitrary $A_1,\ldots,A_n$ subsets of $\mathcal{N}_{-1},\ldots,\mathcal{N}_{-n}$, respectively.

On the basis of this *offline* random pairing, we now construct the key rings $\Sigma_{n,1},\ldots,\Sigma_{n,n}$, one for each node, as follows: Assumed available is a collection of nK *distinct* cryptographic keys $\{\omega_{i|\ell},\ i = 1,\ldots,n;\ \ell = 1,\ldots,K\}$ – These keys are drawn from a very large pool of keys; in practice the pool size is assumed to be much larger than nK, and can be safely taken to be infinite for the purpose of our discussion.

Now, fix $i = 1,\ldots,n$ and let $\ell_{n,i} : \Gamma_{n,i} \to \{1,\ldots,K\}$ denote a labeling of $\Gamma_{n,i}$. For each node j in $\Gamma_{n,i}$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}$ is realized as $\{j_1,\ldots,j_K\}$ with $1 \le j_1 < \ldots < j_K \le n$, then an obvious labeling consists in $\ell_{n,i}(j_k) = k$ for each $k = 1,\ldots,K$ with key $\omega_{i|k}$ associated with node j_k. Of course other labeling are possible. e.g., according to decreasing labels or according to a random permutation. The pairwise key $\omega^\star_{n,ij} = [\mathrm{Id}_i|\mathrm{Id}_j|\omega_{i|\ell_{n,i}(j)}]$ is constructed and inserted in the memory modules of both nodes i and j. Inherent to this construction is the fact that the key $\omega^\star_{n,ij}$ is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise distribution scheme. The key ring $\Sigma_{n,i}$ of node i is the set

$$\Sigma_{n,i} := \{\omega^\star_{n,ij},\ j \in \Gamma_{n,i}\} \cup \{\omega^\star_{n,ji},\ i \in \Gamma_{n,j}\} \qquad (1)$$

as we take into account the possibility that node i may have been paired to some other node j. As mentioned earlier, if two nodes, say i and j, are within wireless range of each other, then they can establish a secure link if at least one of the events $i \in \Gamma_{n,j}$ or $j \in \Gamma_{n,j}$ is taking place. Note that both events can take place, in which case the memory modules of node i and j each contain the distinct keys $\omega^\star_{n,ij}$ and $\omega^\star_{n,ji}$. By construction this scheme supports node-to-node authentication.

B. Gradual deployment

Initially n node identities were generated and the key rings $\Sigma_{n,1}, \ldots, \Sigma_{n,n}$ were constructed as indicated above – Here n stands for the maximum possible network size and should be selected large enough. This key selection procedure does not require the physical presence of the sensor entities and can be implemented completely on the software level. We now describe how this offline pairwise key distribution scheme can accommodate gradual network deployment in consecutive stages. In the initial phase of deployment, with $0 < \gamma_1 < 1$, let $\lfloor \gamma_1 n \rfloor$ sensors be produced and given the labels $1, \ldots, \lfloor \gamma_1 n \rfloor$. The key rings $\Sigma_{n,1}, \ldots, \Sigma_{n,\lfloor \gamma_1 n \rfloor}$ are then inserted into the memory modules of the sensors $1, \ldots, \lfloor \gamma_1 n \rfloor$, respectively. Imagine now that more sensors are needed, say $\lfloor \gamma_2 n \rfloor - \lfloor \gamma_1 n \rfloor$ sensors with $0 < \gamma_1 < \gamma_2 \leq 1$. Then, $\lfloor \gamma_2 n \rfloor - \lfloor \gamma_1 n \rfloor$ additional sensors would be produced, this second batch of sensors would be assigned labels $\lfloor \gamma_1 n \rfloor + 1, \ldots, \lfloor \gamma_2 n \rfloor$, and the key rings $\Sigma_{n,\lfloor \gamma_1 n \rfloor + 1}, \ldots, \Sigma_{n,\lfloor \gamma_2 n \rfloor}$ would be inserted into their memory modules. Once this is done, these $\lfloor \gamma_2 n \rfloor - \lfloor \gamma_1 n \rfloor$ new sensors are added to the network (which now comprises $\lfloor \gamma_2 n \rfloor$ deployed sensors). This step may be repeated a number of times: For some finite integer ℓ, consider positive scalars $0 < \gamma_1 < \ldots < \gamma_\ell \leq 1$ (with $\gamma_0 = 0$ by convention). We can then deploy the sensor network in ℓ consecutive phases, with the kth phase adding $\lfloor \gamma_k n \rfloor - \lfloor \gamma_{k-1} n \rfloor$ new nodes to the network for each $k = 1, \ldots, \ell$.

C. Related work

As already mentioned in Section I, the pairwise distribution scheme naturally gives rise to the following class of well-structured random graphs: With $n = 2, 3, \ldots$ and positive integer K with $K < n$, we say that the distinct nodes i and j are *adjacent*, written $i \sim j$, if and only if they have at least one key in common in their key rings, namely

$$i \sim j \quad \text{iff} \quad \Sigma_{n,i} \cap \Sigma_{n,j} \neq \emptyset. \tag{2}$$

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (2). The following zero-one law for connectivity is the main result established in [13], and is given here for easy reference.

Theorem 2.1: With K a positive integer, it holds that

$$\lim_{n \to \infty} \mathbb{P}\left[\mathbb{H}(n; K) \text{ is connected}\right] = \begin{cases} 0 & \text{if } K = 1 \\ 1 & \text{if } K \geq 2. \end{cases} \tag{3}$$

Moreover, for any $K \geq 2$, we have

$$\mathbb{P}\left[\mathbb{H}(n; K) \text{ is connected}\right] \geq 1 - \frac{27}{2n^2} \tag{4}$$

for all $n = 2, 3, \ldots$ sufficiently large.

III. The results

With the network deployed gradually over time as described in Section II-B, we are now interested in understanding how the parameter K needs to be scaled with large n to ensure that connectivity is *maintained* a.a.s. throughout gradual deployment. The following terminology will be useful in what follows: A scaling is any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$K_n < n, \quad n = 2, 3, \ldots$$

Consider positive integers $n = 2, 3, \ldots$ and K with $K < n$. With γ in the interval $(0, 1)$, let $\mathbb{H}_\gamma(n; K)$ denote the subgraph of $\mathbb{H}(n; K)$ restricted to the nodes $\{1, \ldots, \lfloor \gamma n \rfloor\}$. The fact that $\mathbb{H}(n; K)$ is connected does *not* imply that $\mathbb{H}_\gamma(n; K)$ is necessarily connected. Indeed, with distinct nodes $i, j = 1, \ldots, \lfloor \gamma n \rfloor$, the path that exists in $\mathbb{H}(n; K)$ between these nodes (as a result of the assumed connectivity of $\mathbb{H}(n; K)$) may comprise edges that are not in $\mathbb{H}_\gamma(n; K)$. We write $P_\gamma(n; K) := \mathbb{P}\left[\mathbb{H}_\gamma(n; K) \text{ is connected}\right] = \mathbb{P}\left[C_{n,\gamma}(K)\right]$ with $C_{n,\gamma}(K)$ denoting the event that $\mathbb{H}_\gamma(n; K)$ is connected. The next result constitutes an analog of Theorem 2.1 in this new setting, and shows that gradual deployment has a significant impact on the dimensioning of the pairwise scheme.

Theorem 3.1: With γ in the unit interval $(0, 1)$ and $c > 0$, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$K_n \sim c \, \frac{\log n}{\gamma}. \tag{5}$$

Then, we have $\lim_{n \to \infty} P_\gamma(n; K_n) = 1$ whenever $c > 1$.

The random graphs $\mathbb{H}(n; K)$ and $\mathbb{H}_\gamma(n; K)$ have very different neighborhood structures. Indeed, any node in $\mathbb{H}(n; K)$ has degree at least K, so that no node is isolated in $\mathbb{H}(n; K)$. However, there is a positive probability that isolated nodes exist in $\mathbb{H}_\gamma(n; K)$. In fact, with $P^\star_\gamma(n; K_n) := \mathbb{P}\left[\mathbb{H}_\gamma(n; K) \text{ contains no isolated nodes}\right]$, we have the following zero-one law.

Theorem 3.2: With γ in the unit interval $(0, 1)$, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that (5) holds for some $c > 0$. Then, we have

$$\lim_{n \to \infty} P^\star_\gamma(n; K_n) = \begin{cases} 0 & \text{if } c < r(\gamma) \\ 1 & \text{if } r(\gamma) < c \end{cases} \tag{6}$$

where the threshold $r(\gamma)$ is given by

$$r(\gamma) := \left(1 - \frac{\log(1 - \gamma)}{\gamma}\right)^{-1}. \tag{7}$$

It is easy to check that $r(\gamma)$ is decreasing on the interval $[0, 1]$ with $\lim_{\gamma \downarrow 0} r(\gamma) = \frac{1}{2}$ and $\lim_{\gamma \uparrow 1} r(\gamma) = 0$. Since a connected graph has no isolated nodes, Theorem 3.2 yields $\lim_{n \to \infty} \mathbb{P}\left[\mathbb{H}_\gamma(n; K_n) \text{ is connected}\right] = 0$ if the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfies (5) with $c < r(\gamma)$. The following corollary is now immediate from Theorem 3.1.

Corollary 3.3: With γ in the unit interval $(0, 1)$, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that (5) holds for some $c > 0$. Then, with $r(\gamma)$ given by (7), we have

$$\lim_{n \to \infty} P_\gamma(n; K_n) = \begin{cases} 0 & \text{if } c < r(\gamma) \\ 1 & \text{if } 1 < c. \end{cases} \tag{8}$$

Corollary 3.3 does not provide a full zero-one law for the connectivity of $\mathbb{H}_\gamma(n; K_n)$ as there is a gap between the

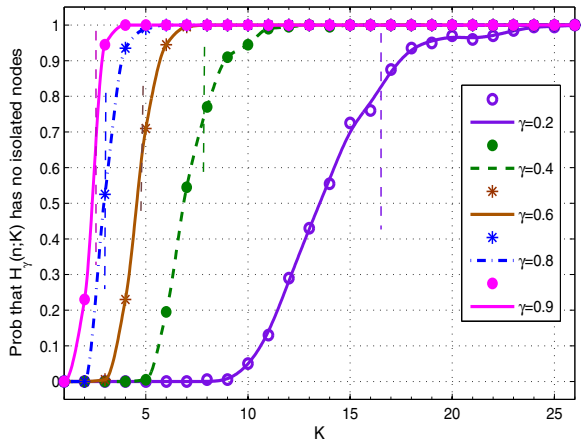

Fig. 1. Probability that $\mathbb{H}_\gamma(n;K)$ contains no isolated for $n = 1000$ obtained through 200 experiments. Vertical dashed lines stand for the critical thresholds asserted by Theorem 3.2. It is clear that the theoretical findings are in perfect agreement with the practical observations.

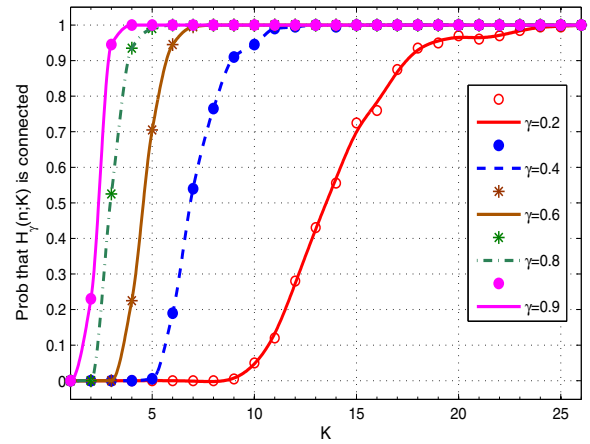

Fig. 2. Probability that $\mathbb{H}_\gamma(n;K)$ is connected for $n = 1,000$ obtained via 200 experiments. Clearly, the curves are almost indistinguishable from the corresponding ones of Figure 1; this supports the claim that absence of isolated nodes and connectivity are asymptotically equivalent properties.

threshold $r(\gamma)$ of the zero-law and the threshold 1 of the one-law. However the gap between the thresholds of the zero-law and the one-law is quite small with $\frac{1}{2} < 1 - r(\gamma) < 1$. More importantly, Corollary 3.3 already implies (via a monotonicity argument) that it is necessary *and* sufficient to keep the parameter K_n on the order of $\log n$ to ensure that the graph $\mathbb{H}_\gamma(n;K_n)$ is a.a.s. connected. It is worth pointing out that the simulation results in Section IV suggest the existence of a full zero-one law for $P_\gamma(n;K_n)$ with a threshold resembling $r(\gamma)$. This would not be surprising since in many known classes of random graphs, the absence of isolated nodes and graph connectivity are asymptotically equivalent properties, e.g., Erdős-Rényi graphs [2], geometric random graphs [8] and random key graphs [10], among others.

Finally we turn to gradual network deployment in several phases as discussed in Section II-B. Given scalars $0 < \gamma_1 < \ldots < \gamma_\ell \leq 1$, we give conditions on how to scale K as a function of n such that $\mathbb{H}_{\gamma_i}(n;K)$ is a.a.s. connected for each $i = 1, 2, \ldots, \ell$.

Theorem 3.4: With $0 < \gamma_1 < \gamma_2 < \ldots < \gamma_\ell \leq 1$, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$K_n \sim c\,\frac{\log n}{\gamma_1} \tag{9}$$

for some $c > 1$. Then we have

$$\lim_{n\to\infty} \mathbb{P}\left[C_{n,\gamma_1}(K_n) \cap \ldots \cap C_{n,\gamma_\ell}(K_n)\right] = 1. \tag{10}$$

The event $C_{\gamma_1,n}(K_n) \cap \ldots \cap C_{\gamma_\ell,n}(K_n)$ corresponds to the network in *each* of its ℓ phases being connected as more nodes get added – In other words, on that event the sensors do form a connected network at each phase of deployment. Theorem 3.4 shows that the condition (9) (with $c > 1$) is enough to ensure that the network remains a.a.s. connected as more sensors are deployed over time.

Proof. With the notation in the statement of Theorem 3.4, it is plain that (10) will hold provided

$$\lim_{n\to\infty} \mathbb{P}\left[C_{n,\gamma_k}(K_n)\right] = 1, \quad k = 1, \ldots, \ell. \tag{11}$$

For each $k = 1, 2, \ldots, \ell$, we note that

$$c\,\frac{\log n}{\gamma_1} = c_k\,\frac{\log n}{\gamma_k} \quad \text{with } c_k := c\,\frac{\gamma_k}{\gamma_1}$$

for all $n = 1, 2, \ldots$. But $c > 1$ implies $c_k > 1$ since $\gamma_1 < \ldots < \gamma_\ell$. As a result, $\mathbb{H}_{\gamma_k}(n;K_n)$ is a.a.s. connected by virtue of Theorem 3.1 applied to $\mathbb{H}_{\gamma_k}(n;K)$, and (11) indeed holds. ■

IV. A LIMITED SIMULATION STUDY

We now present experimental results in support of the theoretical findings discussed earlier. In each set of experiments, we fix n and γ. Then, we generate random graphs $\mathbb{H}_\gamma(n;K)$ for each $K = 1, \ldots, K_{\max}$ where the maximal value $K_{\max}$ is selected large enough. In each case, we check whether the generated random graph has isolated nodes and is connected. We repeat the process 200 times for each pair of values γ and K in order to estimate the probabilities of the events of interest. For various values of γ, Figure 1 depicts the estimated probability $P^\star_\gamma(n;K)$ that $\mathbb{H}_\gamma(n;K)$ has no isolated nodes as a function of K. Here, n is taken to be $1,000$. The plots in Figure 1 clearly confirm the claims of Theorem 3.2: In each case $P^\star_\gamma(n;K)$ exhibits a threshold behavior and the transitions from $P^\star_\gamma(n;K) = 0$ to $P^\star_\gamma(n;K) = 1$ take place around $K_n(\gamma) = r(\gamma)\frac{\log n}{\gamma}$ as dictated by Theorem 3.2; the critical value $K_n(\gamma)$ is shown by a vertical dashed line in each plot.

Similarly, Figure 2 shows the estimated probability $P_\gamma(n;K)$ vs. K for various values of γ with $n = 1000$. For each specified γ, we see that the variation of $P_\gamma(n;K)$ with K is almost indistinguishable from that of $P^\star_\gamma(n;K)$ supporting the claim that $P_\gamma(n;K)$ exhibits a full zero-one law similar to that of Theorem 3.2 with a threshold behaving like $r(\gamma)$. We can also conclude by monotonicity that $P_\gamma(n;K) = 1$

whenever (5) holds with $c > 1$; this verifies Theorem 3.1. Furthermore, it is evident from Figure 2 that for given K and n, $P_\gamma(n;K)$ increases as γ increases supporting Theorem 3.4.

V. Discussion

Theorem 2.1 shows that very small values of K suffice for a.a.s. connectivity of the random graph $\mathbb{H}(n;K)$. However the mere fact that $\mathbb{H}(n;K)$ becomes connected even with very small K values does not imply that the *number* of keys needed to achieve connectivity is necessarily small. This is so because the pairwise scheme produces key rings of variable size between K and $K+(n-1)$.

In [15] we investigated how key ring sizes behave under scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ for which $\lim_{n\to\infty} K_n = \infty$. In that case we showed that the quantity $|\Sigma_{n,1}(K_n)|$, which can fluctuate from K_n to $K_n+(n-1)$, has a propensity to hover about its expected value $2K_n$. A sharper concentration result is available for the maximal key ring size when the scaling satisfies a condition similar to the very condition (5) appearing in Theorem 3.1. To give a precise statement of this result, define the maximal key ring size by

$$M_n(K) := \max_{i=1,\ldots,n} |\Sigma_{n,i}(K)|, \quad n = 2,3,\ldots$$

where the dependence on the parameter K has been explicitly indicated. Also set $\lambda^\star := (2\log 2 - 1)^{-1}$.

Theorem 5.1: Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ of the form $K_n \sim \lambda \log n$ with $\lambda > 0$. If $\lambda > \lambda^\star$, then there exists $c(\lambda)$ in the interval $(0,\lambda)$ such that

$$\lim_{n\to\infty} \mathbb{P}\left[|M_n(K_n) - 2K_n| \geq c\log n\right] = 0 \tag{12}$$

whenever $c(\lambda) < c < \lambda$.

A proof of Theorem 5.1 can be found in [15], [16]. In the course of this proof we also show that

$$\mathbb{P}\left[|M_n(K_n) - 2K_n| \geq c\log n\right] \leq 2n^{-h(\lambda;c)}$$

for all $n = 1,2,\ldots$ whenever $c(\lambda) < c < \lambda$ with $h(\lambda;c) > 0$ specified in [15], [16].

Combining Theorem 5.1 with Theorem 3.4 allows us to reach the following conclusions: With $0 < \gamma_1 < \gamma_2 < \ldots < \gamma_\ell \leq 1$, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n = O(\log n)$ with

$$K_n \geq \max\left(\lambda^\star, \frac{1}{\gamma_1}\right) \cdot \log n, \quad n = 2,3,\ldots.$$

Then the following statements hold true: (i) The maximum number of keys kept in the memory module of each sensor will be a.a.s. less than $3K_n$; (ii) The network deployed gradually in ℓ steps (as in Section II) will be a.a.s. connected in each of the ℓ phases of deployment.

VI. A proof of Theorem 3.1

Fix $n = 2,3,\ldots$ and γ in the interval $(0,1)$, and consider a positive integer $K \geq 2$. Throughout the discussion, n is sufficiently large so that the conditions

$$2(K+1) < n, \quad K+1 \leq n - \lfloor \gamma n \rfloor \quad \text{and} \quad 2 < \gamma n \tag{13}$$

are all enforced; these conditions are made in order to avoid degenerate situations which have no bearing on the final result. There is no loss of generality in doing so as we eventually let n go to infinity.

For any non-empty subset R contained in $\{1,\ldots,\lfloor\gamma n\rfloor\}$, we define the graph $\mathbb{H}_\gamma(n;K)(R)$ (with vertex set R) as the subgraph of $\mathbb{H}_\gamma(n;K)$ restricted to the nodes in R. We say that R is *isolated* in $\mathbb{H}_\gamma(n;K)$ if there are no edges (in $\mathbb{H}_\gamma(n;K)$) between the nodes in R and the nodes in its complement $R^{c|\gamma} := \{1,\ldots,\lfloor\gamma n\rfloor\} - R$. This is characterized by the event $B_{n,\gamma}(K;R)$ given by

$$B_{n,\gamma}(K;R) := \left[i \notin \Gamma_{n,j}, j \notin \Gamma_{n,i},\ i \in R,\ j \in R^{c|\gamma}\right].$$

Also, let $C_{n,\gamma}(K;R)$ denote the event that the induced subgraph $\mathbb{H}_\gamma(n;K)(R)$ is itself connected. Finally, we set

$$A_{n,\gamma}(K;R) := C_{n,\gamma}(K;R) \cap B_{n,\gamma}(K;R).$$

The discussion starts with the following basic observation: If $\mathbb{H}_\gamma(n;K)$ is *not* connected, then there must exist a non-empty subset R of nodes contained in $\{1,\ldots,\lfloor\gamma n\rfloor\}$, such that $\mathbb{H}_\gamma(n;K)(R)$ is itself connected while R is isolated in $\mathbb{H}_\gamma(n;K)$. This is captured by the inclusion

$$C_{n,\gamma}(K)^c \subseteq \cup_{R\in\mathcal{N}_{n,\gamma}} A_{n,\gamma}(K;R) \tag{14}$$

with $\mathcal{N}_{n,\gamma}$ denoting the collection of all non-empty subsets of $\{1,\ldots,\lfloor\gamma n\rfloor\}$. This union need only be taken over all non-empty subsets R of $\{1,\ldots,\lfloor\gamma n\rfloor\}$ with $1 \leq |R| \leq \lfloor\frac{\lfloor\gamma n\rfloor}{2}\rfloor$, and it is useful to note that $\lfloor\frac{\lfloor\gamma n\rfloor}{2}\rfloor = \lfloor\frac{\gamma n}{2}\rfloor$. Then, a standard union bound argument immediately gives

$$\begin{aligned}\mathbb{P}\left[C_{n,\gamma}(K)^c\right] &\leq \sum_{R\in\mathcal{N}_{n,\gamma}:\ 1\leq|R|\leq\lfloor\frac{\gamma n}{2}\rfloor} \mathbb{P}\left[A_{n,\gamma}(K;R)\right] \\ &= \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}\left(\sum_{R\in\mathcal{N}_{n,\gamma,r}} \mathbb{P}\left[A_{n,\gamma}(K;R)\right]\right) \end{aligned} \tag{15}$$

where $\mathcal{N}_{n,\gamma,r}$ denotes the collection of all subsets of $\{1,\ldots,\lfloor\gamma n\rfloor\}$ with exactly r elements.

For each $r = 1,\ldots,\lfloor\gamma n\rfloor$, when $R = \{1,\ldots,r\}$, we simplify the notation by writing $A_{n,\gamma,r}(K) := A_{n,\gamma}(K;R)$, $B_{n,\gamma,r}(K) := B_{n,\gamma}(K;R)$ and $C_{n,\gamma,r}(K) := C_{n,\gamma}(K;R)$. For $r = \lfloor\gamma n\rfloor$, the notation $C_{n,\gamma,\lfloor\gamma n\rfloor}(K)$ coincides with $C_{n,\gamma}(K)$ as defined earlier. Under the enforced assumptions, it is a simple matter to check by exchangeability that

$$\mathbb{P}\left[A_{n,\gamma}(K;R)\right] = \mathbb{P}\left[A_{n,\gamma,r}(K)\right], \quad R \in \mathcal{N}_{n.\gamma,r}$$

and the expression

$$\sum_{R\in\mathcal{N}_{\gamma,r}} \mathbb{P}\left[A_{n,\gamma}(K;R)\right] = \binom{\lfloor\gamma n\rfloor}{r} \mathbb{P}\left[A_{n,\gamma,r}(K)\right]$$

follows since $|\mathcal{N}_{n,\gamma,r}| = \binom{\lfloor\gamma n\rfloor}{r}$. Substituting into (15) we obtain the bounds

$$\mathbb{P}\left[C_{n,\gamma}(K)^c\right] \leq \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}\binom{\lfloor\gamma n\rfloor}{r} \mathbb{P}\left[B_{n,\gamma,r}(K)\right] \tag{16}$$

as we make use of the obvious inclusion $A_{n,\gamma,r}(K) \subseteq B_{n,\gamma,r}(K)$. Under the enforced assumptions, we get

$$\mathbb{P}\left[B_{n,\gamma,r}(K)\right] = \left(\frac{\binom{n-\lfloor\gamma n\rfloor+r-1}{K}}{\binom{n-1}{K}}\right)^r \left(\frac{\binom{n-r-1}{K}}{\binom{n-1}{K}}\right)^{\lfloor\gamma n\rfloor-r} \tag{17}$$

To see why this last relation holds, recall that for the set $\{1,\ldots,r\}$ to be isolated *in* $\mathbb{H}_\gamma(n;K)$ we need that (i) each of the nodes $r+1,\ldots,\lfloor\gamma n\rfloor$ are adjacent only to nodes *outside* the set of nodes $\{1,\ldots,r\}$; and (ii) none of the nodes $1,\ldots,r$ are adjacent with any of the nodes $r+1,\ldots,\lfloor\gamma n\rfloor$ – This last requirement does not preclude adjacency with any of the nodes $\lfloor\gamma n\rfloor+1,\ldots,n$. Reporting (17) into (16), we conclude that

$$\begin{aligned}&\mathbb{P}\left[C_{n,\gamma}(K)^c\right] \qquad (18)\\ &\leq \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}\binom{\lfloor\gamma n\rfloor}{r}\left(\frac{\binom{n-\lfloor\gamma n\rfloor+r-1}{K}}{\binom{n-1}{K}}\right)^r\cdot\left(\frac{\binom{n-r-1}{K}}{\binom{n-1}{K}}\right)^{\lfloor\gamma n\rfloor-r}\end{aligned}$$

with conditions (13) ensuring that the binomial coefficients are well defined.

The remainder of the proof consists in bounding each of the terms in (18). To do so we make use of several standard bounds. First we recall the well-known bound

$$\binom{\lfloor\gamma n\rfloor}{r} \leq \left(\frac{\lfloor\gamma n\rfloor e}{r}\right)^r, \quad r=1,\ldots,\lfloor\gamma n\rfloor.$$

Next, for $0\leq K\leq x\leq y$, we note that

$$\frac{\binom{x}{K}}{\binom{y}{K}} = \prod_{\ell=0}^{K-1}\left(\frac{x-\ell}{y-\ell}\right) \leq \left(\frac{x}{y}\right)^K$$

since $\frac{x-\ell}{y-\ell}$ decreases as ℓ increases from $\ell=0$ to $\ell=K-1$.

Now pick $r=1,\ldots,\lfloor\gamma n\rfloor$. Under (13) we can apply these bounds to obtain

$$\begin{aligned}&\binom{\lfloor\gamma n\rfloor}{r}\left(\frac{\binom{n-\lfloor\gamma n\rfloor+r-1}{K}}{\binom{n-1}{K}}\right)^r\cdot\left(\frac{\binom{n-r-1}{K}}{\binom{n-1}{K}}\right)^{\lfloor\gamma n\rfloor-r}\\ &\leq \left(\frac{\lfloor\gamma n\rfloor e}{r}\right)^r\cdot\left(\frac{n-\lfloor\gamma n\rfloor+r-1}{n-1}\right)^{rK}\\ &\quad\times\left(\frac{n-r-1}{n-1}\right)^{K(\lfloor\gamma n\rfloor-r)}\\ &\leq \left(\frac{\gamma ne}{r}\right)^r\left(1-\frac{\lfloor\gamma n\rfloor-r}{n-1}\right)^{rK}\left(1-\frac{r}{n-1}\right)^{K(\lfloor\gamma n\rfloor-r)}\\ &\leq (\gamma ne)^r\cdot\left(1-\frac{\lfloor\gamma n\rfloor-r}{n}\right)^{rK}\cdot\left(1-\frac{r}{n}\right)^{K(\lfloor\gamma n\rfloor-r)}\\ &\leq (\gamma ne)^r\cdot e^{-\left(\frac{\lfloor\gamma n\rfloor-r}{n}\right)rK}\cdot e^{-\left(\frac{r}{n}\right)(\lfloor\gamma n\rfloor-r)K}.\end{aligned}$$

It is plain that

$$\begin{aligned}\mathbb{P}\left[C_{n,\gamma}(K)^c\right] &\leq \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}(\gamma ne)^r\cdot e^{-2\left(\frac{\lfloor\gamma n\rfloor-r}{n}\right)rK}\\ &\leq \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}\left(\gamma ne\cdot e^{-2\left(\frac{\lfloor\gamma n\rfloor-\lfloor\frac{\gamma n}{2}\rfloor}{n}\right)K}\right)^r \qquad (19)\end{aligned}$$

Next, consider a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that (5) holds for some $c>1$, and replace K by K_n in (19) according to this scaling. Using the form (5) of the scaling we get,

$$a_n := \gamma ne\cdot e^{-2\left(\frac{\lfloor\gamma n\rfloor-\lfloor\frac{\gamma n}{2}\rfloor}{n}\right)K_n} = (\gamma e)\cdot n^{1-2c_n\left(\frac{\lfloor\gamma n\rfloor-\lfloor\frac{\gamma n}{2}\rfloor}{\gamma n}\right)}$$

for each $n=1,2,\ldots$, with $\lim_{n\to\infty}c_n=c$. It is a simple matter to check that

$$\lim_{n\to\infty}\left(2c_n\left(\frac{\lfloor\gamma n\rfloor-\lfloor\frac{\gamma n}{2}\rfloor}{\gamma n}\right)\right)=c,$$

so that by virtue of the fact that $c>1$, we get $\lim_{n\to\infty}a_n=0$.

From (19) we conclude that

$$\mathbb{P}\left[C_{n,\gamma}(K_n)^c\right] \leq \sum_{r=1}^{\lfloor\frac{\gamma n}{2}\rfloor}(a_n)^r \leq \sum_{r=1}^{\infty}(a_n)^r = \frac{a_n}{1-a_n} \tag{20}$$

where for n sufficiently large the summability of the geometric series is guaranteed by the fact that $\lim_{n\to\infty}a_n=0$. This fact also yields the conclusion $\lim_{n\to\infty}\mathbb{P}\left[C_{n,\gamma}(K)^c\right]=0$ via (20).

VII. A PROOF OF THEOREM 3.2

Fix $n=2,3,\ldots$ and consider γ in $(0,1)$ and positive integer K such that $K<n$. We write

$$\chi_{n,\gamma,i}(K) := \mathbf{1}\left[\text{Node } i \text{ is isolated in } \mathbb{H}_\gamma(n;K)\right]$$

for each $i=1,\ldots,\lfloor\gamma n\rfloor$. The number of isolated nodes in $\mathbb{H}_\gamma(n;K)$ is simply given by $I_{n,\gamma}(K):=\sum_{i=1}^{\lfloor\gamma n\rfloor}\chi_{n,\gamma,i}(K)$, whence the random graph $\mathbb{H}_\gamma(n;K)$ has no isolated nodes if $I_{n,\gamma}(K)=0$. The method of first moment [7, Eqn (3.10), p. 55] and second moment [7, Remark 3.1, p. 55] yield the useful bounds

$$1-\mathbb{E}\left[I_{n,\gamma}(K)\right] \leq \mathbb{P}\left[I_{n,\gamma}(K)=0\right] \leq 1-\frac{\mathbb{E}\left[I_{n,\gamma}(K)\right]^2}{\mathbb{E}\left[I_{n,\gamma}(K)^2\right]}. \tag{21}$$

The rvs $\chi_{n,\gamma,1}(K),\ldots,\chi_{n,\gamma,\lfloor\gamma n\rfloor}(K)$ being exchangeable, we find

$$\mathbb{E}\left[I_{n,\gamma}(K)\right] = \lfloor\gamma n\rfloor\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right] \tag{22}$$

and

$$\begin{aligned}\mathbb{E}\left[I_{n,\gamma}(K)^2\right] &= \lfloor\gamma n\rfloor\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right] \qquad (23)\\ &\quad+\lfloor\gamma n\rfloor(\lfloor\gamma n\rfloor-1)\mathbb{E}\left[\chi_{n,\gamma,1}(K)\chi_{n,\gamma,2}(K)\right]\end{aligned}$$

by the binary nature of the rvs involved. It then follows in the usual manner that

$$\begin{aligned}\frac{\mathbb{E}\left[I_{n,\gamma}(K)^2\right]}{\mathbb{E}\left[I_{n,\gamma}(K)\right]^2} &= \frac{1}{\lfloor\gamma n\rfloor\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right]} \qquad (24)\\ &\quad+\frac{\lfloor\gamma n\rfloor-1}{\lfloor\gamma n\rfloor}\frac{\mathbb{E}\left[\chi_{n,\gamma,1}(K)\chi_{n,\gamma,2}(K)\right]}{\left(\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right]\right)^2}.\end{aligned}$$

From (21) and (22) we conclude that the one-law $\lim_{n\to\infty}\mathbb{P}\left[I_{n,\gamma}(K_n)=0\right]=1$ holds if we show that

$$\lim_{n\to\infty}\lfloor\gamma n\rfloor\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right]=0. \tag{25}$$

On the other hand, it is plain from (21) and (24) that the zero-law $\lim_{n\to\infty}\mathbb{P}\left[I_{n,\gamma}(K_n)=0\right]=0$ will be established if

$$\lim_{n\to\infty}\lfloor\gamma n\rfloor\mathbb{E}\left[\chi_{n,1}(K_n)\right]=\infty \tag{26}$$

and

$$\limsup_{n\to\infty}\left(\frac{\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\chi_{n,\gamma,2}(K_n)\right]}{\left(\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right]\right)^2}\right)\leq 1. \tag{27}$$

The next two technical lemmas establish (25), (26) and (27) under the appropriate conditions on the scaling $K:\mathbb{N}_0\to\mathbb{N}_0$.

Lemma 7.1: Consider γ in $(0,1)$ and a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that (5) holds for some $c>0$. We have

$$\lim_{n\to\infty}n\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right]=\begin{cases}0 & \text{if } r(\gamma)<c\\ \infty & \text{if } c<r(\gamma)\end{cases} \tag{28}$$

with $r(\gamma)$ specified via (7).

Lemma 7.2: Consider γ in $(0,1)$ and a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that (5) holds for some $c>0$. We have

$$\limsup_{n\to\infty}\left(\frac{\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\chi_{n,\gamma,2}(K_n)\right]}{\left(\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right]\right)^2}\right)\leq 1. \tag{29}$$

Proofs of Lemma 7.1 and Lemma 7.2 can be found in Section VII-A and Section VII-B, respectively. To complete the proof of Theorem 3.2, pick a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that (5) holds for some $c>0$. Under the condition $c>r(\gamma)$ we get (25) from Lemma 7.1 and the one-law $\lim_{n\to\infty}\mathbb{P}\left[I_{n,\gamma}(K_n)=0\right]=1$ follows. Next, assume the condition $c<r(\gamma)$. We obtain (26) and (27) with the help of Lemmas 7.1 and 7.2, respectively, and the conclusion $\lim_{n\to\infty}\mathbb{P}\left[I_{n,\gamma}(K_n)=0\right]=0$ is now immediate.

A. A proof of Lemma 7.1

Fix $n=2,3,\ldots$ and γ in $(0,1)$, and consider a positive integer K such that $K<n$. Here as well there is no loss of generality in assuming $n-\lfloor\gamma n\rfloor\geq K$ and $\lfloor\gamma n\rfloor>1$. Under the enforced assumptions, we get

$$\begin{aligned}\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right] &= \frac{\binom{n-\lfloor\gamma n\rfloor}{K}}{\binom{n-1}{K}}\left(\frac{\binom{n-2}{K}}{\binom{n-1}{K}}\right)^{\lfloor\gamma n\rfloor-1}\\ &= a(n;K)\cdot\left(1-\frac{K}{n-1}\right)^{\lfloor\gamma n\rfloor-1}\end{aligned} \tag{30}$$

with

$$a(n;K):=\frac{(n-\lfloor\gamma n\rfloor)!}{(n-\lfloor\gamma n\rfloor-K)!}\cdot\frac{(n-1-K)!}{(n-1)!}.$$

Now pick a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that (5) holds for some $c>0$ and replace K by K_n in (30) with respect to this scaling. Applying Stirling's formula

$$m!\sim\sqrt{2\pi m}\left(\frac{m}{e}\right)^m\qquad(m\to\infty)$$

to the factorials appearing in (30), we readily get

$$\begin{aligned}a(n;K_n) &\sim \sqrt{\frac{(n-\lfloor\gamma n\rfloor)(n-1-K_n)}{(n-\lfloor\gamma n\rfloor-K_n)(n-1)}}\cdot\alpha_n\beta_n\\ &\sim \alpha_n\beta_n\end{aligned} \tag{31}$$

under the enforced assumptions on the scaling with

$$\begin{aligned}\alpha_n &:= \frac{(n-K_n-1)^{n-K_n-1}}{(n-1)^{n-1}}\\ &= \left(1-\frac{K_n}{n-1}\right)^{n-1}\cdot(n-K_n-1)^{-K_n}\end{aligned}$$

and

$$\begin{aligned}\beta_n &:= \frac{(n-\lfloor\gamma n\rfloor)^{n-\lfloor\gamma n\rfloor}}{(n-\lfloor\gamma n\rfloor-K_n)^{n-\lfloor\gamma n\rfloor-K_n}}\\ &= \left(1-\frac{K_n}{n-\lfloor\gamma n\rfloor}\right)^{-(n-\lfloor\gamma n\rfloor)}\cdot(n-\lfloor\gamma n\rfloor-K_n)^{K_n}.\end{aligned}$$

In obtaining the asymptotic behavior of (31) we rely on the following technical fact: For any sequence $m:\mathbb{N}_0\to\mathbb{N}_0$ with $m_n=O(n)$, we have

$$\left(1-\frac{K_n}{m_n}\right)^{m_n}\sim e^{-K_n}. \tag{32}$$

To see why (32) holds, recall the elementary decomposition

$$\log(1-x)=-x-\Psi(x)\ \text{ with }\ \Psi(x):=\int_0^x\frac{t}{1-t}\,dt$$

valid for $0\leq x<1$. Using this fact, we get

$$\left(1-\frac{K_n}{m_n}\right)^{m_n}=e^{-K_n}\cdot e^{-m_n\Psi\left(\frac{K_n}{m_n}\right)},\quad n=1,2,\ldots. \tag{33}$$

Under the enforced assumptions we have $m_n=O(n)$ and $K_n=O(\log n)$, so that

$$\lim_{n\to\infty}\frac{K_n}{m_n}=0\quad\text{and}\quad\lim_{n\to\infty}m_n\left(\frac{K_n}{m_n}\right)^2=0.$$

It is now plain that $\lim_{n\to\infty}m_n\Psi\left(\frac{K_n}{m_n}\right)=0$ as we note that $\lim_{x\downarrow 0}\frac{\Psi(x)}{x^2}=\frac{1}{2}$. This establishes (32) via (33).

Using (32), first with $m_n=n-1$, then with $m_n=n-\lfloor\gamma n\rfloor$, we obtain $\left(1-\frac{K_n}{n-1}\right)^{n-1}\sim e^{-K_n}$ and

$$\left(1-\frac{K_n}{n-\lfloor\gamma n\rfloor}\right)^{-(n-\lfloor\gamma n\rfloor)}\sim\left(e^{-K_n}\right)^{-1}=e^{K_n},$$

whence

$$\alpha_n\beta_n\sim\left(\frac{n-\lfloor\gamma n\rfloor-K_n}{n-K_n-1}\right)^{K_n}. \tag{34}$$

With the help of (30) and (31) we now conclude that

$$\begin{aligned}&n\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right]\\ &\sim n\left(1-\frac{K_n}{n-1}\right)^{\lfloor\gamma n\rfloor-1}\cdot\left(\frac{n-\lfloor\gamma n\rfloor-K_n}{n-K_n-1}\right)^{K_n}.\end{aligned} \tag{35}$$

A final application of (32), this time with $m_n=n-1$, gives

$$\begin{aligned}\left(1-\frac{K_n}{n-1}\right)^{\lfloor\gamma n\rfloor-1} &= \left(\left(1-\frac{K_n}{n-1}\right)^{n-1}\right)^{\frac{\lfloor\gamma n\rfloor-1}{n-1}}\\ &\sim e^{-\frac{\lfloor\gamma n\rfloor-1}{n-1}K_n}\end{aligned} \tag{36}$$

since $\lim_{n\to\infty} \frac{\lfloor \gamma n \rfloor - 1}{n-1} = \gamma$. Reporting (36) into (35) we obtain

$$n\mathbb{E}\left[\chi_{n,\gamma,1}(K_n)\right] \sim e^{\zeta_n} \tag{37}$$

with

$$\zeta_n := \log n - \left(\frac{\lfloor \gamma n \rfloor - 1}{n-1} + \log\left(\frac{n - \lfloor \gamma n \rfloor - K_n}{n - K_n - 1} \right) \right) K_n$$

for all $n = 1, 2, \ldots$. Finally, from the condition (5) on the scaling, we see that

$$\lim_{n\to\infty} \frac{\zeta_n}{\log n} = 1 - c + c\frac{\log(1-\gamma)}{\gamma} = 1 - \frac{c}{r(\gamma)}.$$

Thus, $\lim_{n\to\infty} \zeta_n = -\infty$ (resp. ∞) if $c < r(\gamma)$ (resp. $r(\gamma) < c$) and the desired result follows upon using (37).

B. A proof of Lemma 7.2

Fix positive integers $n = 3, 4, \ldots$ and K with $K < n$. With γ in $(0, 1)$, we again assume that $n - \lfloor \gamma n \rfloor \geq K$ and $\lfloor \gamma n \rfloor > 1$. It is a simple matter to check that

$$\mathbb{E}\left[\chi_{n,\gamma,1}(K)\chi_{n,\gamma,2}(K)\right] = \left(\frac{\binom{n-\lfloor \gamma n \rfloor}{K}}{\binom{n-1}{K}} \right)^2 \left(\frac{\binom{n-3}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - 2}$$

and invoking (30) we readily conclude that

$$\begin{aligned}
&\frac{\mathbb{E}\left[\chi_{n,\gamma,1}(K)\chi_{n,\gamma,2}(K)\right]}{\left(\mathbb{E}\left[\chi_{n,\gamma,1}(K)\right]\right)^2} \\
&= \left(\frac{\binom{n-3}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left(\frac{\binom{n-1}{K}}{\binom{n-2}{K}} \right)^{2(\lfloor \gamma n \rfloor - 1)} \\
&= \left(\left(\frac{n-1-K}{n-1} \right) \left(\frac{n-2-K}{n-2} \right) \right)^{\lfloor \gamma n \rfloor - 2} \\
&\quad \times \left(\frac{n-1}{n-1-K} \right)^{2(\lfloor \gamma n \rfloor - 1)} \\
&= \left(\frac{n-2-K}{n-2} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left(\frac{n-1}{n-1-K} \right)^{\lfloor \gamma n \rfloor} \\
&= \left(1 - \frac{K}{n-2} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left(1 + \frac{K}{n-1-K} \right)^{\lfloor \gamma n \rfloor} \\
&\leq e^{-K \cdot E(n;K)}
\end{aligned} \tag{38}$$

where we have set $E(n;K) := \frac{\lfloor \gamma n \rfloor - 2}{n-2} - \frac{\lfloor \gamma n \rfloor}{n-1-K}$. Elementary calculations show that

$$-K \cdot E(n;K) = \frac{\lfloor \gamma n \rfloor}{n-2} \cdot \frac{K(K-1)}{n-1-K} + \frac{2K}{n-2}.$$

Now pick a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that (5) holds for some $c > 0$. It is plain that $\lim_{n\to\infty} K_n E(n; K_n) = 0$ and the conclusion (29) follows from (38).

Acknowledgment

This work was supported by NSF Grant CCF-07290.

References

[1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics* **309** (2009), pp. 5130-5140.

[2] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[3] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the SP 2003, Oakland (CA), May 2003, pp. 197-213.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[5] W. Du, J. Deng, Y.S. Han and P.K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proceedings of the CCS 2003, Washington (DC), October 2004.

[6] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the CSS 2002, Washington (DC), November 2002, pp. 41-47.

[7] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

[8] M. D. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability **5**, Oxford University Press, New York (NY), 2003.

[9] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM* **47** (2004), pp. 53–57.

[10] K. Rybarczyk "Diameter, connectivity and phase transition of the uniform random intersection graph," Submitted, July 2009.

[11] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica* **12** (2006).

[12] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Available online at arXiv:0908.3644v1 [math.CO], August 2009.

[13] O. Yağan and A. M. Makowski, "On random pairwise graphs," submitted to *Discrete Mathematics*. Available online at `http://www.ece.umd.edu/~oyagan/Journals/Pairwise-DM.pdf`.

[14] O. Yağan and A. M. Makowski, "Designing securely connected wireless sensor networks in the presence of unreliable links," in Proceedings of the IEEE International Conference on Communications (ICC 2011), Kyoto (Japan), June 2011.

[15] O. Yağan and A. M. Makowski, "Key ring sizes in the random pairwise key distribution scheme," submitted for inclusion in the program of the Twenty-second Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2011), Toronto (ON, Canada), September 2011.

[16] O. Yağan, *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011.