

# On the gradual deployment of random pairwise key distribution schemes

Osman Yagan  
Armand M. Makowski

The  
Institute for  
**Systems**  
Research



A. JAMES CLARK  
SCHOOL OF ENGINEERING

ISR develops, applies and teaches advanced methodologies of design and analysis to solve complex, hierarchical, heterogeneous and dynamic problems of engineering technology and systems for industry and government.

ISR is a permanent institute of the University of Maryland, within the A. James Clark School of Engineering. It is a graduated National Science Foundation Engineering Research Center.

[www.isr.umd.edu](http://www.isr.umd.edu)

# 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**—In the context of wireless sensor networks, the pairwise key distribution scheme of Chan et al. has several advantages over other key distribution schemes including the original scheme of Eschenauer and Gligor. However, this offline pairwise key distribution mechanism requires that the network size be set in advance, and involves all sensor nodes simultaneously. Here, we address this issue by describing an implementation of the pairwise scheme that supports the gradual deployment of sensor nodes in several consecutive phases. We discuss the key ring size needed to maintain the secure connectivity throughout all the deployment phases. In particular we show that the number of keys at each sensor node can be taken to be  $O(\log n)$  in order to achieve secure connectivity (with high probability).

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

## I. INTRODUCTION

Wireless sensor networks (WSNs) are distributed collections of sensors with limited capabilities for computations and wireless communications. Such networks will likely be deployed in hostile environments where cryptographic protection will be needed to enable secure communications, sensor-capture detection, key revocation and sensor disabling. However, traditional key exchange and distribution protocols based on trusting third parties have been found inadequate for large-scale WSNs, e.g., see [6, 9, 11] for discussions of some of the challenges.

Random key predistribution schemes were recently proposed 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, 13, 14], with most of the focus being on the *full visibility* case where nodes are all within communication range of each other. Under full visibility, the EG scheme induces so-called *random key graphs* [12] (also known in the literature as *uniform random intersection graphs* [1]). Conditions on the graph parameters to ensure the absence of isolated nodes have been obtained independently in [1, 12] while the papers

[1, 4, 10, 13, 14] are concerned with zero-one laws for connectivity. Although the assumption of full visibility does away with the wireless nature of the communication infrastructure supporting WSNs, in return this simplification makes it possible to focus on how randomizing the key selections affects the establishment of a secure network; the connectivity results for the underlying random key graph then provide helpful (though optimistic) guidelines to dimension the EG scheme.

The work of Eschenauer and Gligor has spurred the development of other key distribution schemes which perform better than the EG scheme in some aspects, e.g., [3, 5, 9, 11]. Although these schemes somewhat improve resiliency, they fail to provide *perfect* resiliency against node capture attacks. More importantly, they do not provide a node with the ability to authenticate the identity of the neighbors with which it communicates. This is a major drawback in terms of network security since *node-to-node authentication* may help detect node misbehavior, and provides resistance against node replication attacks [3].

To address this issue Chan et al. [3] have proposed the following random *pairwise* key predistribution scheme: 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 assigned to the other, i.e., if 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) Unlike earlier schemes, this scheme enables both node-to-node authentication and quorum-based revocation without involving a base station. Given these advantages, we found it of interest to model the pairwise scheme of Chan et al. and to assess its performance. In the companion paper [15] we began a formal investigation along these lines. Let  $\mathbb{H}(n; K)$  denote the random graph on the vertex set  $\{1, \dots, n\}$  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 [15] 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 the present paper, we continue our study of connectivity properties 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. We also discuss the number of keys needed in the memory module of each sensor to achieve secure connectivity at every step of the gradual deployment. Since sensor nodes are expected to have very limited memory, it is crucial for a key distribution scheme to have *low* memory requirements [5].

The key contributions of the paper can be stated as follows: Let  $\mathbb{H}_\gamma(n; K)$  denote the subgraph of  $\mathbb{H}(n; K)$  restricted to the nodes  $1, \dots, \lfloor \gamma n \rfloor$ . We first present scaling laws for the absence of isolated nodes 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  $0 < \gamma_1 < \gamma_2 < \dots < \gamma_\ell < 1$ , we give conditions on  $n$ ,  $K$  and  $\gamma_1$  so that  $\mathbb{H}_{\gamma_i}(n; K)$  is a.a.s. connected for each  $i = 1, 2, \dots, \ell$ . As with the EG scheme, such conditions can be helpful for dimensioning the pairwise key distribution in the case of gradual deployment. We show that connectivity can be achieved a.a.s. when the number of keys to be stored in the memory modules is  $O(\log n)$ ; this is a key ring size comparable to that of the EG scheme (in realistic WSN scenarios [4]). Thus, if key ring sizes are somewhat larger than in the full deployment case, it is feasible to gradually deploy an a.a.s. connected WSN.

These results may help dimension the pairwise scheme when the network is deployed gradually over time. However, as with the results in [15], 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. This issue could be addressed, as was done for the original pairwise scheme in [16], by considering a simplified communication model where unreliable wireless links are represented as on/off channels. The study of the corresponding model for gradual deployment would provide a better understanding of how the vagaries of the channel affect the performance of the pairwise distribution scheme; this will be carried out elsewhere.

The rest of the paper is organized as follows: In Section II we present the model introduced in [15] for the random

pairwise distribution scheme, and in Section III we summarize the relevant work from the companion paper [15]. Section IV presents the main results of the paper; proofs are given in Section VI and Section VII. Section V contains some simulation results.

## 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  $i = 1, \dots, n$ , with unique ids  $\text{Id}_1, \dots, \text{Id}_n$ . Write  $\mathcal{N} := \{1, \dots, n\}$  and set  $\mathcal{N}_{-i} := \mathcal{N} - \{i\}$  for each  $i = 1, \dots, n$ . With node  $i$  we associate a subset  $\Gamma_{n,i}$  nodes selected at *random* from  $\mathcal{N}_{-i}$  – We say that each of the nodes in  $\Gamma_{n,i}$  is paired to node  $i$ . Thus, for any subset  $A \subseteq \mathcal{N}_{-i}$ , we require

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

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

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

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

On the basis of this *offline* random pairing, we now construct the key rings  $\Sigma_{n,1}, \dots, \Sigma_{n,n}$ , one for each node, as follows: Assumed available is a collection of  $nK$  distinct cryptographic keys  $\{\omega_{i|\ell}, i = 1, \dots, n; \ell = 1, \dots, K\}$  – 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  $i = 1, \dots, n$  and let  $\ell_{n,i} : \Gamma_{n,i} \rightarrow \{1, \dots, K\}$  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  $\{j_1, \dots, j_K\}$  with  $1 \leq j_1 < \dots < j_K \leq n$ , then an obvious labeling consists in  $\ell_{n,i}(j_k) = k$  for each  $k = 1, \dots, K$  with key  $\omega_{i|k}$  associated with node  $j_k$ . Of course other labelings are possible, e.g., according to decreasing labels or according to a random permutation. The pairwise key

$$\omega_{n,ij}^* = [\text{Id}_i | \text{Id}_j | \omega_{i|\ell_{n,i}(j)}]$$

is constructed and inserted in the memory modules of both nodes  $i$  and  $j$ . Inherent to this construction is the fact that the key  $\omega_{n,ij}^*$  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

$$\Sigma_{n,i} := \{\omega_{n,ij}^*, j \in \Gamma_{n,i}\} \cup \{\omega_{n,ji}^*, i \in \Gamma_{n,j}\} \quad (1)$$

as we take into account the possibility that node  $i$  was paired to some other node  $j$ . As mentioned earlier, under full visibility,

two node, say  $i$  and  $j$ , can establish a secure link if at least one of the events  $i \in \Gamma_{n,j}$  or  $j \in \Gamma_{n,i}$  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  $\omega_{n,i,j}^*$  and  $\omega_{n,j,i}^*$ . It is also plain that by construction this scheme supports node-to-node authentication.

### B. Gradual deployment

Initially  $n$  node identities were generated and the key rings  $\Sigma_{n,1}, \dots, \Sigma_{n,n}$  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 support 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  $1, \dots, \lfloor \gamma_1 n \rfloor$ . The key rings  $\Sigma_{n,1}, \dots, \Sigma_{n,\lfloor \gamma_1 n \rfloor}$  are then inserted into the memory modules of the sensors  $1, \dots, \lfloor \gamma_1 n \rfloor$ , 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  $\lfloor \gamma_1 n \rfloor + 1, \dots, \lfloor \gamma_2 n \rfloor$ , and the key rings  $\Sigma_{n,\lfloor \gamma_1 n \rfloor + 1}, \dots, \Sigma_{n,\lfloor \gamma_2 n \rfloor}$  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 times: In fact, for some finite integer  $\ell$ , consider positive scalars  $0 < \gamma_1 < \dots < \gamma_\ell \leq 1$  (with  $\gamma_0 = 0$  by convention). We can then deploy the sensor network in  $\ell$  consecutive phases, with the  $k^{\text{th}}$  phase adding  $\lfloor \gamma_k n \rfloor - \lfloor \gamma_{k-1} n \rfloor$  new nodes to the network for each  $k = 1, \dots, \ell$ .

## III. RELATED WORK

The pairwise distribution scheme naturally gives rise to the following class of random graphs: With  $n = 2, 3, \dots$  and positive integer  $K$  with  $K < n$ , the distinct nodes  $i$  and  $j$  are said to be *adjacent*, written  $i \sim j$ , if and only if they have at least one key in common in their key rings, namely

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

Let  $\mathbb{H}(n; K)$  denote the undirected random graph on the vertex set  $\{1, \dots, n\}$  induced through the adjacency notion (2). To keep the notation simple we have omitted the dependence on  $K$  for most of the quantities introduced so far. In what follows we largely abide by this practice, although we shall make the dependence on  $K$  explicit in a few places when scaling  $K$  with the number  $n$  of users.

Below we summarize results obtained in the companion paper [15]. We set

$$P(n; K) := \mathbb{P}[\mathbb{H}(n; K) \text{ is connected}].$$

In [15] we have shown the following zero-one law.

**Theorem 3.1:** *With  $K$  a positive integer, it holds that*

$$\lim_{n \rightarrow \infty} P(n; K) = \begin{cases} 0 & \text{if } K = 1 \\ 1 & \text{if } K \geq 2. \end{cases} \quad (3)$$

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

$$P(n; K) \geq 1 - \frac{27}{2n^2} \quad (4)$$

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

As an immediate corollary of Theorem 3.1, Yağan and Makowski also obtained the behavior of graph connectivity as the parameter  $K$  is scaled with  $n$  [15]. First some terminology: Any mapping  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  is called a *scaling* provided the condition  $K_n < n$  holds for all  $n = 1, 2, \dots$

**Corollary 3.2:** *For any scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that  $K_n \geq 2$  for all  $n$  sufficiently large, we have the one-law  $\lim_{n \rightarrow \infty} P(n; K_n) = 1$ .*

Theorem 3.1 and its Corollary 3.2 together show that very small values of  $K$  suffice for a.a.s. connectivity of the random graph  $\mathbb{H}(n; K)$ . The mere fact that  $\mathbb{H}(n; K)$  becomes connected even with very small  $K$  values does not imply that the *number* of keys (i.e., the size  $|\Sigma_{n,i}|$ ) to achieve connectivity is necessarily small. This is because in contrast with the EG scheme and its variants, the pairwise scheme produces key rings of variable size between  $K$  and  $K + (n - 1)$ . To explore this issue further we first recall minimal conditions on a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  which ensure that the key ring of a node has size roughly of the order (of its mean)  $2K_n$  when  $n$  is large [15].

**Lemma 3.3:** *For any scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ , we have*

$$\frac{|\Sigma_{n,1}(K_n)|}{2K_n} \xrightarrow{P} 1$$

as soon as  $\lim_{n \rightarrow \infty} K_n = \infty$ .

Thus, when  $n$  is large  $|\Sigma_{n,1}(K_n)|$  fluctuates from  $K_n$  to  $K_n + (n - 1)$  with a propensity to hover about  $2K_n$  under the conditions of Lemma 3.3. This result is sharpened with the help of a concentration result for the maximal key ring size under an appropriate class of scalings. We define the maximal key ring size by

$$M_n := \left( \max_{i=1, \dots, n} |\Sigma_{n,i}| \right), \quad n = 2, 3, \dots$$

**Theorem 3.4:** *Consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  of the form*

$$K_n \sim \lambda \log n \quad (5)$$

with  $\lambda > 0$ . If  $\lambda > \lambda^* := (2 \log 2 - 1)^{-1} \simeq 2.6$ , then there exists  $c(\lambda)$  in the interval  $(0, \lambda)$  such that

$$\lim_{n \rightarrow \infty} \mathbb{P}[|M_n(K_n) - 2K_n| \geq c \log n] = 0 \quad (6)$$

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

#### IV. THE RESULTS

With the network deployed gradually over time as described in Section II-B, we are 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. Consider positive integers  $n = 2, 3, \dots$  and  $K$  with  $K < n$ . With  $\gamma$  in the interval  $(0, 1)$ , let  $\mathbb{H}_\gamma(n; K)$  denote the subgraph of  $\mathbb{H}(n; K)$  restricted to the nodes  $\{1, \dots, \lfloor \gamma n \rfloor\}$ . Given scalars  $0 < \gamma_1 < \dots < \gamma_\ell \leq 1$ , we seek conditions on the parameters  $K$  and  $n$  such that  $\mathbb{H}_{\gamma_i}(n; K)$  is a.a.s. connected for each  $i = 1, 2, \dots, \ell$ .

First we write

$$P_\gamma(n; K) := \mathbb{P}[\mathbb{H}_\gamma(n; K) \text{ is connected}] = \mathbb{P}[C_{n,\gamma}(K)]$$

where  $C_{n,\gamma}(K)$  denote the event that  $\mathbb{H}_\gamma(n; K)$  is connected. 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  $i, j = 1, \dots, \lfloor \gamma n \rfloor$ , 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  $\mathbb{H}_\gamma(n; K)$ . The next result provides an analog of Corollary 3.2 in this new setting.

**Theorem 4.1:** *With  $\gamma$  in the unit interval  $(0, 1)$  and  $c > 0$ , consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that*

$$K_n \sim c \frac{\log n}{\gamma}. \quad (7)$$

*Then, we have  $\lim_{n \rightarrow \infty} P_\gamma(n; K_n) = 1$  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

$$P_\gamma^*(n; K_n) := \mathbb{P}[\mathbb{H}_\gamma(n; K) \text{ contains no isolated nodes}],$$

we have the following zero-one law.

**Theorem 4.2:** *With  $\gamma$  in the unit interval  $(0, 1)$ , consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . Then, we have*

$$\lim_{n \rightarrow \infty} P_\gamma^*(n; K_n) = \begin{cases} 0 & \text{if } c < r(\gamma) \\ 1 & \text{if } c > r(\gamma) \end{cases} \quad (8)$$

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

$$r(\gamma) := \left(1 - \frac{\log(1-\gamma)}{\gamma}\right)^{-1}. \quad (9)$$

As can be seen from Figure 1,  $r(\gamma)$  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 4.2 yields  $\lim_{n \rightarrow \infty} \mathbb{P}[\mathbb{H}_\gamma(n; K_n) \text{ is connected}] = 0$  if the scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  satisfies (7) with  $c < r(\gamma)$ . The following corollary is now immediate from Theorem 4.1.

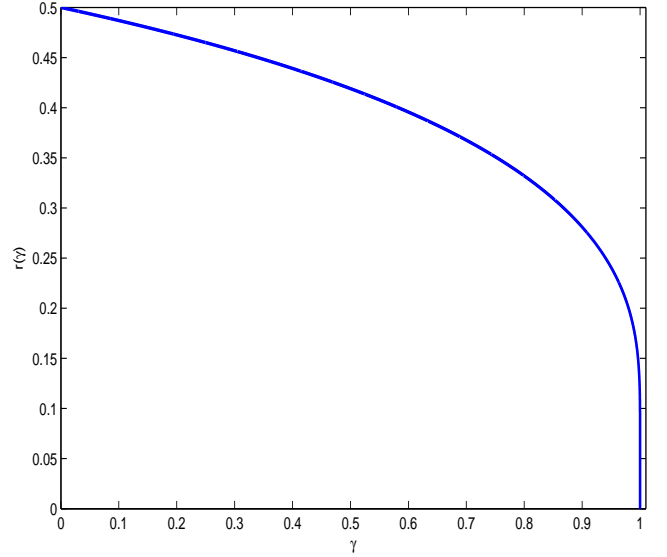


Fig. 1.  $r(\gamma)$  vs  $\gamma$ .

**Corollary 4.3:** *With  $\gamma$  in the unit interval  $(0, 1)$ , consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . Then, we have*

$$\lim_{n \rightarrow \infty} P_\gamma(n; K_n) = \begin{cases} 0 & \text{if } c < r(\gamma) \\ 1 & \text{if } c > 1 \end{cases} \quad (10)$$

where  $r(\gamma)$  is given by (9).

Corollary 4.3 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 threshold  $r(\gamma)$  of the zero-law and the threshold 1 of the one-law. Yet, as can be seen from Figure 1, 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 4.3 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 V 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] and random key graphs [10, 12], among others.

Finally we turn to gradual network deployment as discussed in Section II-A.

**Theorem 4.4:** *With  $0 < \gamma_1 < \gamma_2 < \dots < \gamma_\ell \leq 1$ , consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that*

$$K_n \sim c \frac{\log n}{\gamma_1} \quad (11)$$

for some  $c > 1$ . Then we have

$$\lim_{n \rightarrow \infty} \mathbb{P}[C_{n,\gamma_1}(K_n) \cap \dots \cap C_{n,\gamma_\ell}(K_n)] = 1. \quad (12)$$

The event  $[C_{\gamma_1,n}(K_n) \cap \dots \cap C_{\gamma_\ell,n}(K_n)]$  corresponds to the network in *each* of its  $\ell$  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. As a result, we infer via Theorem 4.4 that the condition (11) (with  $c > 1$ ) is enough to ensure that the network remains a.s. connected as more sensors are deployed over time.

The main conclusions of the paper, obtained by combining Theorem 3.4 and Theorem 4.4, can now be summarized as follows:

**Corollary 4.5:** *With  $0 < \gamma_1 < \gamma_2 < \dots < \gamma_\ell \leq 1$ , consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that  $K_n = O(\log n)$  with*

$$K_n \geq \max\{(\gamma_1)^{-1}, \lambda^*\} \cdot \log n, \quad n = 2, 3, \dots \quad (13)$$

Then, the following holds:

- 1) *The maximum number of keys kept in the memory module of each sensor will be a.s. less than  $3K_n$ ;*
- 2) *The network deployed gradually in  $\ell$  steps (as in Section II-B) will be a.s. connected in each of the  $\ell$  phases of deployment.*

## V. SIMULATION STUDY

We now present experimental results in support of Theorem 4.1 and Theorem 4.2. In each set of experiments, we fix  $n$  and  $\gamma$ . Then, we generate random graphs  $\mathbb{H}_\gamma(n; K)$  for each  $K = 1, \dots, K_{\max}$  where the maximal value  $K_{\max}$  is selected large enough to ensure that the range of  $c$  computed through

$$K = c \cdot \frac{\log n}{\gamma} \quad (14)$$

exceeds 1. In each case, we check whether the generated random graph has isolated nodes and is connected. We repeat the process 500 times for each pair of values  $\gamma$  and  $K$  in order to estimate the probabilities of the events of interest. Due to the integer constraint on  $K$ , the values of  $c$  cannot be varied arbitrarily and the number of data points that can be obtained in the range  $(0, 1)$  is therefore *limited*. Thus, to better assess the dependence of  $P_\gamma^*(n; K_n)$  and  $P_\gamma(n; K_n)$  on  $c$  in the figures, we make use of the curve-fitting tool of MATLAB.

For various values of  $\gamma$ , Figure 2 and Figure 3 display the estimated probability  $P_\gamma^*(n; K_n)$  that  $\mathbb{H}_\gamma(n; K)$  has no isolated nodes as a function of  $c$ . Here,  $n$  is taken to be 1,000 and  $c$  is computed through (14) for various values of  $K$ . The plots in Figure 2 clearly confirm the claims of Theorem 4.2: In each case  $P_\gamma^*(n; K_n)$  exhibits a threshold behavior and the transitions from  $P_\gamma^*(n; K_n) = 0$  to  $P_\gamma^*(n; K_n) = 1$  take place around  $c = r(\gamma)$ . Also, it is evident from Figure 3 that the value of  $c$  at which the transition occurs decreases as  $\gamma$  increases, while the rate of decrease is much faster for larger values of  $\gamma$ . This is compatible with the behavior of  $r(\gamma)$  given in Figure 1.

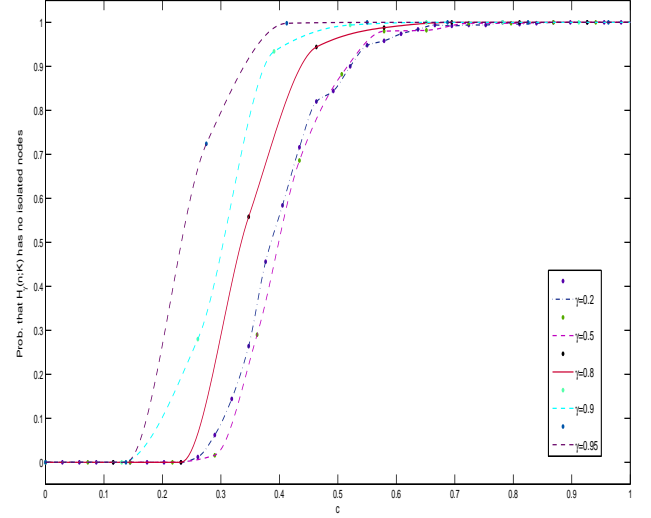


Fig. 2. Probability that  $\mathbb{H}_\gamma(n; K)$  contains no isolated nodes estimated via 500 experiments with  $n = 1,000$  and  $K = c \cdot \frac{\log n}{\gamma}$ .

Similarly, Figure 4 shows the estimated probability  $P_\gamma(n; K_n)$  for various values of  $\gamma$  with  $n = 500$  as  $c$  ranges over the interval  $(0, 1)$ . For each specified  $\gamma$ , we can conclude by monotonicity that  $P_\gamma(n; K_n) = 1$  whenever  $c > 1$ , in agreement with Theorem 4.1. As pointed out earlier, Figure 4 suggests that  $P_\gamma(n; K_n)$  exhibits a full zero-one law similar to that of Theorem 4.2 with a threshold behaving like  $r(\gamma)$ . More work is in progress on this issue.

## VI. A PROOF OF THEOREM 4.1

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

$$2(K+1) < n, \quad K+1 \leq n - \lfloor \gamma n \rfloor \quad \text{and} \quad 2 < \gamma n \quad (15)$$

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  $\{1, \dots, \lfloor \gamma n \rfloor\}$ , 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  $R^{c|\gamma} := \{1, \dots, \lfloor \gamma n \rfloor\} - R$ . 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

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

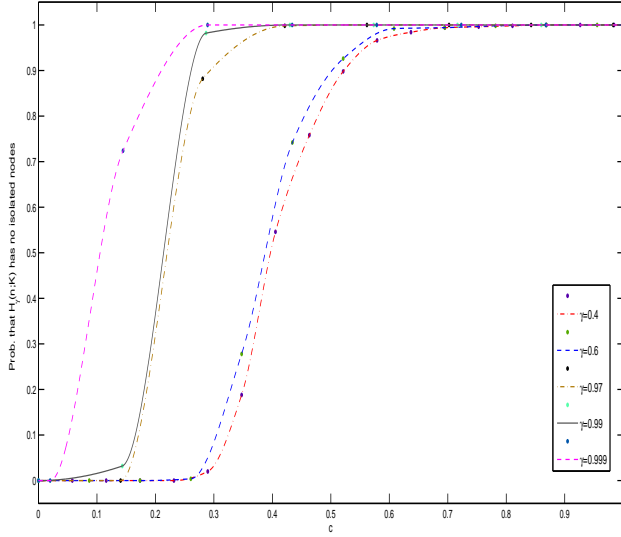


Fig. 3. Probability that  $\mathbb{H}_\gamma(n; K)$  contains no isolated nodes estimated via 500 experiments with  $n = 1,000$  and  $K = c \cdot \frac{\log n}{\gamma}$ .

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  $\{1, \dots, \lfloor \gamma n \rfloor\}$ , 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

$$C_{n,\gamma}(K)^c \subseteq \cup_{R \in \mathcal{N}_{n,\gamma}} A_{n,\gamma}(K; R) \quad (16)$$

with  $\mathcal{N}_{n,\gamma}$  denoting the collection of all non-empty subsets of  $\{1, \dots, \lfloor \gamma n \rfloor\}$ . This union need only be taken over all non-empty subsets  $R$  of  $\{1, \dots, \lfloor \gamma n \rfloor\}$  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

$$\begin{aligned} \mathbb{P}[C_{n,\gamma}(K)^c] &\leq \sum_{R \in \mathcal{N}_{n,\gamma}; 1 \leq |R| \leq \lfloor \frac{\gamma n}{2} \rfloor} \mathbb{P}[A_{n,\gamma}(K; R)] \\ &= \sum_{r=1}^{\lfloor \frac{\gamma n}{2} \rfloor} \left( \sum_{R \in \mathcal{N}_{n,\gamma,r}} \mathbb{P}[A_{n,\gamma}(K; R)] \right) \end{aligned} \quad (17)$$

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

For each  $r = 1, \dots, \lfloor \gamma n \rfloor$ , when  $R = \{1, \dots, r\}$ , 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

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

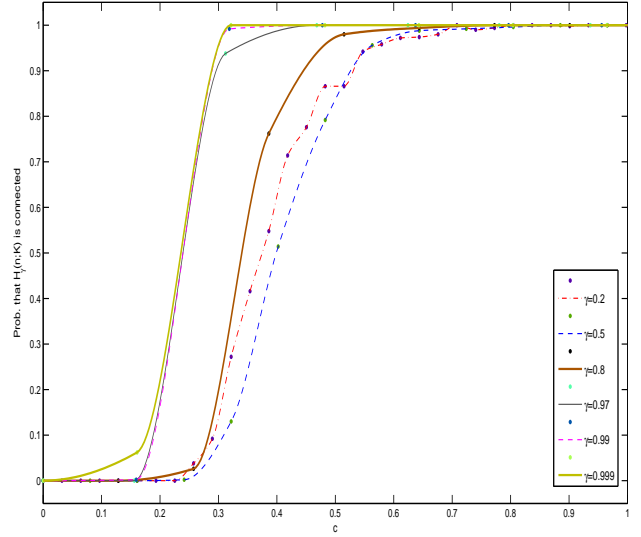


Fig. 4. Probability that  $\mathbb{H}_\gamma(n; K)$  is connected estimated via 500 experiments with  $n = 500$  and  $K = c \cdot \frac{\log n}{\gamma}$ .

and the expression

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

follows since  $|\mathcal{N}_{n,\gamma,r}| = \binom{\lfloor \gamma n \rfloor}{r}$ . Substituting into (17) we obtain the bounds

$$\mathbb{P}[C_{n,\gamma}(K)^c] \leq \sum_{r=1}^{\lfloor \frac{\gamma n}{2} \rfloor} \binom{\lfloor \gamma n \rfloor}{r} \mathbb{P}[B_{n,\gamma,r}(K)] \quad (18)$$

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

$$\begin{aligned} \mathbb{P}[B_{n,\gamma,r}(K)] &= \left( \frac{\binom{n - \lfloor \gamma n \rfloor + r - 1}{K}}{\binom{n-1}{K}} \right)^r \cdot \left( \frac{\binom{n-r-1}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - r} \end{aligned} \quad (19)$$

To see why this last relation holds, recall that for the set  $\{1, \dots, r\}$  to be isolated in  $\mathbb{H}_\gamma(n; K)$  we need that (i) each of the nodes  $r+1, \dots, \lfloor \gamma n \rfloor$  are adjacent only to nodes *outside* the set of nodes  $\{1, \dots, r\}$ ; and (ii) none of the nodes  $1, \dots, r$  are adjacent with any of the nodes  $r+1, \dots, \lfloor \gamma n \rfloor$  – This last requirement does not preclude adjacency with any of the nodes  $\lfloor \gamma n \rfloor + 1, \dots, n$ . Reporting (19) into (18), we conclude that

$$\begin{aligned} \mathbb{P}[C_{n,\gamma}(K)^c] &\leq \sum_{r=1}^{\lfloor \frac{\gamma n}{2} \rfloor} \binom{\lfloor \gamma n \rfloor}{r} \left( \frac{\binom{n - \lfloor \gamma n \rfloor + r - 1}{K}}{\binom{n-1}{K}} \right)^r \cdot \left( \frac{\binom{n-r-1}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - r} \end{aligned} \quad (20)$$

with conditions (15) ensuring that the binomial coefficients are well defined.

The remainder of the proof consists in bounding each of the terms in (20). To do so we make use of several standard bounds. First we recall the well-known bound

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

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  $\ell$  increases from  $\ell = 0$  to  $\ell = K - 1$ .

Now pick  $r = 1, \dots, \lfloor \gamma n \rfloor$ . Under (15) we can apply these bounds to obtain

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

It is plain that

$$\begin{aligned} \mathbb{P}[C_{n,\gamma}(K)^c] & \leq \sum_{r=1}^{\lfloor \frac{\gamma n}{2} \rfloor} (\gamma n e)^r \cdot e^{-2\left(\frac{\lfloor \gamma n \rfloor - r}{n}\right)rK} \\ & \leq \sum_{r=1}^{\lfloor \frac{\gamma n}{2} \rfloor} \left( \gamma n e \cdot e^{-2\left(\frac{\lfloor \gamma n \rfloor - \lfloor \frac{\gamma n}{2} \rfloor}{n}\right)K} \right)^r \end{aligned} \quad (21)$$

as we note that

$$\frac{\lfloor \gamma n \rfloor - r}{n} \geq \frac{\lfloor \gamma n \rfloor - \lfloor \frac{\gamma n}{2} \rfloor}{n}, \quad r = 1, \dots, \lfloor \frac{\gamma n}{2} \rfloor.$$

Next, consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 1$ , and replace  $K$  by  $K_n$  in (21) according to this scaling. Using the form (7) of the scaling we get,

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

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

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

so that by virtue of the fact that  $c > 1$ , we have

$$\lim_{n \rightarrow \infty} a_n = 0. \quad (22)$$

From (21) we conclude that

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

where for  $n$  sufficiently large the summability of the geometric series is guaranteed by (22). The conclusion  $\lim_{n \rightarrow \infty} \mathbb{P}[C_{n,\gamma}(K)^c] = 0$  is now a straightforward consequence of the last bound, again by virtue of (22).

## VII. A PROOF OF THEOREM 4.2

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

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

for each  $i = 1, \dots, \lfloor \gamma n \rfloor$ . 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 [8, Eqn (3.10), p. 55] and second moment [8, Remark 3.1, p. 55] yield the useful bounds

$$1 - \mathbb{E}[I_{n,\gamma}(K)] \leq \mathbb{P}[I_{n,\gamma}(K) = 0] \leq 1 - \frac{\mathbb{E}[I_{n,\gamma}(K)]^2}{\mathbb{E}[I_{n,\gamma}(K)]}. \quad (23)$$

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

$$\mathbb{E}[I_{n,\gamma}(K)] = \lfloor \gamma n \rfloor \mathbb{E}[\chi_{n,\gamma,1}(K)] \quad (24)$$

and

$$\begin{aligned} & \mathbb{E}[I_{n,\gamma}(K)^2] \\ & = \lfloor \gamma n \rfloor \mathbb{E}[\chi_{n,\gamma,1}(K)] \\ & \quad + \lfloor \gamma n \rfloor (\lfloor \gamma n \rfloor - 1) \mathbb{E}[\chi_{n,\gamma,1}(K) \chi_{n,\gamma,2}(K)] \end{aligned} \quad (25)$$

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

$$\begin{aligned} \frac{\mathbb{E}[I_{n,\gamma}(K)^2]}{\mathbb{E}[I_{n,\gamma}(K)]^2} & = \frac{1}{\lfloor \gamma n \rfloor \mathbb{E}[\chi_{n,\gamma,1}(K)]} \\ & \quad + \frac{\lfloor \gamma n \rfloor - 1}{\lfloor \gamma n \rfloor} \frac{\mathbb{E}[\chi_{n,\gamma,1}(K) \chi_{n,\gamma,2}(K)]}{(\mathbb{E}[\chi_{n,\gamma,1}(K)])^2}. \end{aligned} \quad (26)$$

From (23) and (24) we conclude that the one-law  $\lim_{n \rightarrow \infty} \mathbb{P}[I_{n,\gamma}(K_n) = 0] = 1$  holds if we show that

$$\lim_{n \rightarrow \infty} \lfloor \gamma n \rfloor \mathbb{E}[\chi_{n,\gamma,1}(K_n)] = 0. \quad (27)$$

On the other hand, it is plain from (23) and (26) that the zero-law  $\lim_{n \rightarrow \infty} \mathbb{P}[I_{n,\gamma}(K_n) = 0] = 0$  will be established if

$$\lim_{n \rightarrow \infty} \lfloor \gamma n \rfloor \mathbb{E}[\chi_{n,1}(K_n)] = \infty \quad (28)$$

and

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

The next two technical lemmas establish (27), (28) and (29) under the appropriate conditions on the scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ .



**Lemma 7.1:** Consider  $\gamma$  in  $(0, 1)$  and a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . We have

$$\lim_{n \rightarrow \infty} n \mathbb{E}[\chi_{n,\gamma,1}(K_n)] = \begin{cases} 0 & \text{if } c > r(\gamma) \\ \infty & \text{if } c < r(\gamma) \end{cases} \quad (30)$$

with  $r(\gamma)$  specified via (9).

**Lemma 7.2:** Consider  $\gamma$  in  $(0, 1)$  and a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . We have

$$\limsup_{n \rightarrow \infty} \left( \frac{\mathbb{E}[\chi_{n,\gamma,1}(K_n)\chi_{n,\gamma,2}(K_n)]}{(\mathbb{E}[\chi_{n,\gamma,1}(K_n)])^2} \right) \leq 1. \quad (31)$$

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 4.2, pick a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . Under the condition  $c > r(\gamma)$  we get (27) from Lemma 7.1 and the one-law  $\lim_{n \rightarrow \infty} \mathbb{P}[I_{n,\gamma}(K_n) = 0] = 1$  follows. Next, assume the condition  $c < r(\gamma)$ . We obtain (28) and (29) with the help of Lemmas 7.1 and 7.2, respectively, and the conclusion  $\lim_{n \rightarrow \infty} \mathbb{P}[I_{n,\gamma}(K_n) = 0] = 0$  is now immediate.

#### A. A proof of Lemma 7.1

Fix  $n = 2, 3, \dots$  and  $\gamma$  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

$$\begin{aligned} \mathbb{E}[\chi_{n,\gamma,1}(K)] &= \frac{\binom{n-\lfloor \gamma n \rfloor}{K}}{\binom{n-1}{K}} \left( \frac{\binom{n-2}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - 1} \\ &= a(n; K) \cdot \left( 1 - \frac{K}{n-1} \right)^{\lfloor \gamma n \rfloor - 1} \end{aligned} \quad (32)$$

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  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$  and replace  $K$  by  $K_n$  in (32) with respect to this scaling. Applying Stirling's formula

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

to the factorials appearing in (32), we readily get

$$\begin{aligned} a(n; K_n) &\sim \sqrt{\frac{(n - \lfloor \gamma n \rfloor)(n - 1 - K_n)}{(n - \lfloor \gamma n \rfloor - K_n)(n - 1)}} \cdot \alpha_n \beta_n \\ &\sim \alpha_n \beta_n \end{aligned} \quad (33)$$

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 (33) we rely on the following technical fact: For any sequence  $m : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  with  $m_n = O(n)$ , we have

$$\left( 1 - \frac{K_n}{m_n} \right)^{m_n} \sim e^{-K_n}. \quad (34)$$

To see why (34) holds, recall the elementary decomposition

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

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

$$\left( 1 - \frac{K_n}{m_n} \right)^{m_n} = e^{-K_n} \cdot e^{-m_n \Psi\left(\frac{K_n}{m_n}\right)} \quad (35)$$

for all  $n = 1, 2, \dots$

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

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

It is now plain that

$$\lim_{n \rightarrow \infty} m_n \Psi\left(\frac{K_n}{m_n}\right) = 0$$

as we note that  $\lim_{x \downarrow 0} \frac{\Psi(x)}{x^2} = \frac{1}{2}$ . This establishes (34) via (35).

Using (34), 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

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

whence

$$\alpha_n \beta_n \sim \left( \frac{n - \lfloor \gamma n \rfloor - K_n}{n - K_n - 1} \right)^{K_n}. \quad (36)$$

With the help of (32) and (33) we now conclude that

$$\begin{aligned} n \mathbb{E}[\chi_{n,\gamma,1}(K_n)] & \\ &\sim n \left( 1 - \frac{K_n}{n - 1} \right)^{\lfloor \gamma n \rfloor - 1} \cdot \left( \frac{n - \lfloor \gamma n \rfloor - K_n}{n - K_n - 1} \right)^{K_n}. \end{aligned} \quad (37)$$

A final application of (34), this time with  $m_n = n - 1$ , gives

$$\begin{aligned} \left( 1 - \frac{K_n}{n - 1} \right)^{\lfloor \gamma n \rfloor - 1} &= \left( \left( 1 - \frac{K_n}{n - 1} \right)^{n - 1} \right)^{\frac{\lfloor \gamma n \rfloor - 1}{n - 1}} \\ &\sim e^{-\frac{\lfloor \gamma n \rfloor - 1}{n - 1} K_n} \end{aligned} \quad (38)$$

since  $\lim_{n \rightarrow \infty} \frac{\lfloor \gamma n \rfloor - 1}{n-1} = \gamma$ . Reporting (38) into (37) we obtain

$$n \mathbb{E} [\chi_{n,\gamma,1}(K_n)] \sim e^{\zeta_n} \quad (39)$$

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  $n = 1, 2, \dots$ . Finally, from the condition (7) on the scaling, we see that

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

Thus,  $\lim_{n \rightarrow \infty} \zeta_n = -\infty$  (resp.  $\infty$ ) if  $r(\gamma) > c$  (resp.  $r(\gamma) < c$ ) and the desired result follows upon using (39).

### B. A proof of Lemma 7.2

Fix positive integers  $n = 3, 4, \dots$  and  $K$  with  $K < n$ . With  $\gamma$  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

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

and invoking (32) we readily conclude that

$$\begin{aligned} & \frac{\mathbb{E} [\chi_{n,\gamma,1}(K) \chi_{n,\gamma,2}(K)]}{(\mathbb{E} [\chi_{n,\gamma,1}(K)])^2} \\ &= \left( \frac{\binom{n-3}{K}}{\binom{n-1}{K}} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left( \frac{\binom{n-1}{K}}{\binom{n-2}{K}} \right)^{2(\lfloor \gamma n \rfloor - 1)} \\ &= \left( \left( \frac{n-1-K}{n-1} \right) \left( \frac{n-2-K}{n-2} \right) \right)^{\lfloor \gamma n \rfloor - 2} \\ & \quad \times \left( \frac{n-1}{n-1-K} \right)^{2(\lfloor \gamma n \rfloor - 1)} \\ &= \left( \frac{n-2-K}{n-2} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left( \frac{n-1}{n-1-K} \right)^{\lfloor \gamma n \rfloor} \\ &= \left( 1 - \frac{K}{n-2} \right)^{\lfloor \gamma n \rfloor - 2} \cdot \left( 1 + \frac{K}{n-1-K} \right)^{\lfloor \gamma n \rfloor} \\ &\leq e^{-K \cdot E(n;K)} \end{aligned} \quad (40)$$

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  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that (7) holds for some  $c > 0$ . It is plain that  $\lim_{n \rightarrow \infty} K_n E(n; K_n) = 0$  and the conclusion (31) follows from (40).

## VIII. A PROOF OF THEOREM 4.4

Pick  $0 < \gamma_1 < \gamma_2 < \dots < \gamma_\ell \leq 1$  and consider a scaling  $K : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  such that

$$K_n \sim c \frac{\log n}{\gamma_1}$$

for some  $c > 1$ . It is plain that (12) will hold provided

$$\lim_{n \rightarrow \infty} \mathbb{P} [C_{n,\gamma_k}(K_n)] = 1, \quad k = 1, \dots, \ell. \quad (41)$$

For each  $k = 1, 2, \dots, \ell$ , 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  $n = 1, 2, \dots$ . But  $c > 1$  implies  $c_k > 1$  since  $\gamma_1 < \dots < \gamma_\ell$ . As a result,  $\mathbb{H}_{\gamma_k}(n; K_n)$  will be a.a.s. connected by virtue of Theorem 4.1 applied to  $\mathbb{H}_{\gamma_k}(n; K)$ , and (41) indeed holds.

### 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*, Second Edition, 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] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in Proceedings of the SASN 2004, Washington (DC), October 2004.
- [8] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.
- [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 to *Discrete Mathematics*, July 2009.
- [11] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica* **12** (2006), pp. 900-906.
- [12] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," in Proceedings of the ISIT 2008, Toronto (ON), June 2008.
- [13] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," in Proceedings of the ISIT 2009, Seoul (Korea), June 2009.
- [14] 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.
- [15] O. Yağan and A. M. Makowski, "On random graphs associated with a pairwise key distribution scheme for wireless sensor networks," submitted for inclusion in the program of Infocom 2011. Available online at <http://www.lib.umd.edu/drum/>.
- [16] O. Yağan and A. M. Makowski, "Modeling the pairwise key distribution scheme in the presence of unreliable links," submitted for inclusion in the program of Infocom 2011. Available online at <http://www.lib.umd.edu/drum/>.