On the Connectivity of Sensor Networks Under Random Pairwise Key Predistribution

Osman Yağan, *Member, IEEE*, and Armand M. Makowski, *Fellow, IEEE*

***Abstract*—We investigate the connectivity of wireless sensor networks under the random pairwise key predistribution scheme of Chan *et al.* Under the assumption of full visibility, this reduces to studying the connectivity in the so-called random K-out graph $\mathbb{H}(n;K)$; here, n is the number of nodes and $K < n$ is an integer parameter affecting the number of keys stored at each node. We show that if $K \geq 2$ (respectively, $K = 1$), the probability that $\mathbb{H}(n;K)$ is a connected graph approaches 1 (respectively, 0) as n goes to infinity. For the one-law this is done by establishing an explicitly computable lower bound on the probability of connectivity. Using this bound, we see that with high probability, network connectivity can already be guaranteed (with $K \geq 2$) by a relatively small number of sensors. This corrects earlier predictions made on the basis of a heuristic transfer of connectivity results available for Erdős–Rényi graphs.**

***Index Terms*—Connectivity, random graphs, zero-one laws.**

I. Introduction

RANDOM key predistribution is an approach proposed in the literature for addressing security challenges in resource-constrained wireless sensor networks (WSNs). The idea of randomly assigning secure keys to the sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor [5]. Following their original work, a large number of key predistribution schemes have been proposed; see the survey articles [2], [16], [17].

Here, we consider the random pairwise key predistribution scheme proposed by Chan *et al.* in [3]: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from among all other nodes. For each such pair of sensors, a unique (pairwise) key is generated and stored in the memory modules of each of the paired sensors together with both their ids. A secure link can then be established between two communicating nodes if they have at least one pairwise key in common. Precise implementation details are given in Section II. The random pairwise predistribution scheme has a number of advantages over the original scheme of Eschenauer and Gligor: 1) It is *perfectly resilient* against node capture attacks [3]; 2) unlike earlier schemes, this pairwise scheme enables both distributed node-to-node authentication and quorum-based node revocation.

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 at least one pairwise key in common. This random graph models the random pairwise key predistribution scheme under full visibility (whereby all nodes are within wireless communication range of each other). In this paper, we seek conditions on n and K under which $\mathbb{H}(n;K)$ is a connected graph with high probability as n grows large. As in the case of the Eschenauer–Gligor scheme [19], such conditions might provide helpful guidelines for dimensioning purposes (although possibly too optimistic given the full visibility assumption used).

We show the following zero-one law: With $K \geq 2$ (respectively, $K = 1$), the probability that $\mathbb{H}(n;K)$ is a connected graph approaches 1 (respectively, 0) as n grows large. For the one-law, this is done by establishing a computable lower bound on the probability of connectivity for each $K \geq 2$. In particular, we see that with $K = 2$ and $n = 20$, the graph is connected with probability larger than 0.98, whereas with only 50 sensors, the probability of connectivity becomes larger than 0.999. Thus, connectivity is achievable with high probability under very small values of K and n. In fact these values are much smaller than the ones predicted by a heuristic transfer of connectivity results from Erdős–Rényi (ER) graphs (as was done in the original paper of Chan *et al.* [3] and in [8]). The results obtained here help correct misleading predictions made in these earlier papers and form the basis for a reappraisal of the scalability of the random pairwise predistribution scheme; see [22] and [23] for details.

The random graph $\mathbb{H}(n;K)$ is known in the literature on random graphs as the random K-out graph [1], [6], [9]: To each of the n vertices, assign exactly K arcs to K distinct vertices that are selected uniformly at random, and then ignore the orientation of the arcs. Fenner and Frieze have established [6, Th. 2.1, p. 348] the zero-one law given here by a completely different approach which focuses on vertex and edge connectivity parameters. While their analysis also leads to a lower bound on the probability of connectivity, the lower bound obtained here is sharper for $K \geq 3$.

This paper is organized as follows: In Section II, we give a formal construction of the random pairwise key predistribution scheme and introduce the induced random K-out graph. The main results of this paper concerning the connectivity of random

Manuscript received February 14, 2012; revised January 07, 2013; accepted March 04, 2013. Date of publication May 30, 2013; date of current version August 14, 2013. This work was supported by the National Science Foundation under Grant CCF-0729093. This paper was presented in part at the 2012 IEEE International Symposium on Information Theory.

O. Yağan was with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA. He is now with the Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: oyagan@andrew.cmu.edu).

A. M. Makowski is with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: armand@isr.umd.edu).

Communicated by M. Franceschetti, Associate Editor for Communication Networks.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2013.2265694

K-out graphs are presented in Section III; there, we also compare them against the earlier results of Fenner and Frieze. Various comments are given in Section IV, and proofs are given in Sections V and VI.

II. Model

All statements involving limits, including asymptotic equivalences, are understood with n going to infinity. The cardinality of any discrete set S is denoted by $|S|$. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$.

A. Random Pairwise Key Predistribution Scheme

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 labeled $i = 1, \ldots, n$ 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 $\Gamma_{n,i}(K)$ of nodes selected at *random* from $\mathcal{N}_{-i}$. Each of the nodes in $\Gamma_{n,i}(K)$ is said to be *paired* to node i. Specifically, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

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

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

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

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

Once this offline random pairing has been created, we construct the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$, 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 $\ell_{n,i} : \Gamma_{n,i}(K) \to \{1, \ldots, K\}$ denote a labeling of $\Gamma_{n,i}(K)$. For each node j in $\Gamma_{n,i}(K)$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}(K)$ is realized as $\{j_1, \ldots, j_K\}$ with $1 \leq j_1 < \ldots < j_K \leq n$, then an obvious labeling consists in $\ell_{n,i}(j_k) = k$ for each $k = 1, \ldots, K$ so that key $\omega_{i|k}$ is associated with node j_k. Of course other labeling are possible, e.g., according to decreasing labels or according to a random permutation. Finally, 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 predistribution scheme. The key ring $\Sigma_{n,i}(K)$ of node i is the set

$$\Sigma_{n,i}(K) = \left\{\omega^{\star}_{n,ij},\ j \in \Gamma_{n,i}(K)\right\} \cup \left\{\omega^{\star}_{n,ji},\ \begin{array}{c} j = 1, \ldots, n \\ i \in \Gamma_{n,j}(K) \end{array}\right\}. \tag{2}$$

As mentioned earlier, under full visibility, two nodes, say i and j, can establish a secure link if at least one of the events $i \in \Gamma_{n,j}(K)$ or $j \in \Gamma_{n,j}(K)$ is taking place. Note that both events can take place, in which case the memory modules of nodes i and j both contain the distinct keys $\omega^{\star}_{n,ij}$ and $\omega^{\star}_{n,ji}$. By construction, this scheme supports node-to-node authentication.

B. Induced Random Graphs

Under full visibility, the pairwise predistribution scheme naturally gives rise to the following class of random graphs: With $n = 2, 3, \ldots$ and positive integer $K < n$, 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

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

or, equivalently

$$i \sim j \quad \text{iff} \quad i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K). \tag{3}$$

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (3). In the literature on random graphs, the random graph $\mathbb{H}(n; K)$ is usually referred to as a random K-out graph [1], [6].

We close with some notation. Throughout, we write

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

Let $\lambda(n; K)$ denote the probability of edge assignment (between any two nodes) in $\mathbb{H}(n; K)$. Under the enforced independence assumptions, it is plain from (3) that

$$\lambda(n; K) = 1 - \left(1 - \frac{K}{n-1}\right)^2 = \frac{2K}{n-1} - \left(\frac{K}{n-1}\right)^2. \tag{4}$$

III. Results

Throughout, it will be convenient to use the notation

$$Q(n; K) = \left(\frac{K+1}{n}\right)^{K^2-1} + \frac{n}{2}\left(\frac{K+2}{n}\right)^{(K+2)(K-1)}$$

and

$$a(K) = e^{-\frac{1}{2}(K+1)(K-2)} \tag{5}$$

with n and K arbitrary positive integers.

A. Tight Bound and Its Consequences

Our main technical result, given next, is established in Section V; its proof adapts classical arguments used for proving the one-law for connectivity in ER graphs [4, Sec. 3.4.2, p. 42].

Theorem 3.1: For any positive integer $K \geq 2$, the bound

$$P(n;K) \geq 1 - a(K)Q(n;K) \tag{6}$$

holds for all $n \geq n(K)$ with $n(K) = 4(K+2)$.

The bound (6) gives some indication as to how fast the convergence $\lim_{n\to\infty} P(n;K) = 1$ occurs when $K \geq 2$, with the convergence becoming faster with larger K as would be expected; see also (8) below.

For $K = 2$, since $n(2) = 16$, the bound (6) becomes

$$P(n;2) \geq 1 - \frac{155}{n^3}, \quad n \geq 16. \tag{7}$$

For each $n = 2, 3, \ldots$, a simple coupling argument yields the comparison

$$P(n;2) \leq P(n,K), \quad K = 2, \ldots, n-1. \tag{8}$$

Making use of (7), we then conclude

$$P(n;K) \geq 1 - \frac{155}{n^3}, \quad \begin{array}{c} n \geq 16, \\ K = 2, \ldots, n-1. \end{array} \tag{9}$$

A zero-one law for connectivity is presented next.

Theorem 3.2: With any positive integer K, it holds that

$$\lim_{n\to\infty} P(n;K) = \begin{cases} 0, & \text{if } K = 1 \\ \\ 1, & \text{if } K \geq 2. \end{cases} \tag{10}$$

The one-law in Theorem 3.2 is an easy consequence of the bound (6), while the zero-law of Theorem 3.2 is proved separately in Section VI. Theorem 3.2 easily yields the behavior of graph connectivity as the parameter K is scaled with n, but first some terminology: We refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* provided it satisfies the natural conditions

$$K_n < n, \quad n = 2, 3, \ldots. \tag{11}$$

Corollary 3.3: For any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$, we have

$$\lim_{n\to\infty} P(n;K_n) = 1 \tag{12}$$

provided $K_n \geq 2$ for all n sufficiently large.

Proof: Under the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$, it follows from (8) that $P(n;2) \leq P(n,K_n)$ for all n sufficiently large as soon as $K_n \geq 2$. Letting n go to infinity in this last inequality, we get (12) by invoking Theorem 3.2 (with $K = 2$), or equivalently (7). ■

B. Earlier Results of Fenner and Frieze

Related results have appeared earlier: Fix $n = 2, 3, \ldots$ and consider a positive integer $K < n$. We define the *vertex connectivity* $C_v(n;K)$ of $\mathbb{H}(n;K)$ as the minimum number of its vertices whose deletion disconnects $\mathbb{H}(n;K)$. The *edge connectivity* $C_e(n;K)$ is defined similarly in terms of edges. Fenner and Frieze have established the following result in terms of these quantities [6, Th. 2.1, p. 348].

Theorem 3.4: For any positive integer $K \geq 2$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[C_v(n;K) = K\right] = 1 \tag{13}$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[C_e(n;K) = K\right] = 1, \tag{14}$$

while

$$\lim_{n\to\infty} P(n;1) = 0. \tag{15}$$

The one-law in Theorem 3.2 is immediate from either (13) or (14) since $\mathbb{H}(n;K)$ is connected if either $C_v(n;K) \geq 1$ (respectively, $C_e(n;K) \geq 1$). However, as we shall show below, the arguments used here lead to *computable* lower bounds on $P(n;K)$ which are stronger (except for the case $K = 2$) than the bounds that can be inferred from the proof of Theorem 3.4 [6, Th. 2.1, p. 348].

The zero-law in Theorem 3.2 coincides with (15). However, (15) was obtained [6] by completely different arguments based on results by Katz [11] concerning random mappings. Our proof, given in Section VI, uses instead classical enumeration results for the set of undirected graphs on n nodes which are connected and have exactly n edges [7, pp. 133–134].

We now compare the lower bound (on the probability of connectivity in $\mathbb{H}(n;K)$) obtained in Theorem 3.1 with the one (implicitly) given in the proof of Theorem 3.4 [6, Th. 2.1, p. 348]. Inspection of the proof given there [6, p. 348] yields the bound

$$P(n;K) \geq 1 - b(n;K)Q(n;K) \tag{16}$$

for any positive integers n and K such that $K < n$, where we have set

$$b(n;K) = \frac{12n}{12n-1}\sqrt{\frac{n}{n-K-1}} \cdot b(K)$$

with

$$b(K) = \sqrt{\frac{1}{2\pi(K+1)}}.$$

This follows from [6, p. 349, eqn. (2.2)] with $p = 0$; note that the parameter K used here is denoted m in [6].

The lower bound (16) has the same form as the one given in Theorem 3.1, but is *weaker* (i.e., is a smaller lower bound) than (6) except for $K = 2$. Indeed, it is easy to check that

$$a(K) \leq b(K) \leq b(n;K), \quad \begin{array}{c} K = 3, \ldots, n-1 \\ n = 4, 5, \ldots \end{array}$$

with $\lim_{n\to\infty} b(n;K) = b(K)$ monotonically from above.

In order to better understand how these lower bounds compare with each other, observe that

$$\sup_{n=K+1,\ldots} \left(\frac{a(K)}{b(n;K)}\right) = \frac{a(K)}{b(K)}, \quad K = 3, 4, \ldots$$

with

$$\lim_{K\to\infty} \frac{a(K)}{b(K)} = 0.$$

Thus, the lower bound given in Theorem 3.1 for the probability of network connectivity approaches one much faster than the bound (16) inferred from [6].

To illustrate this fact, with $n = 50$, we have plotted the behavior of $a(K)$, $b(K)$ and $b(n;K)$ as a function of K in Fig. 1. As expected from the remarks above, $a(K)$ approaches zero

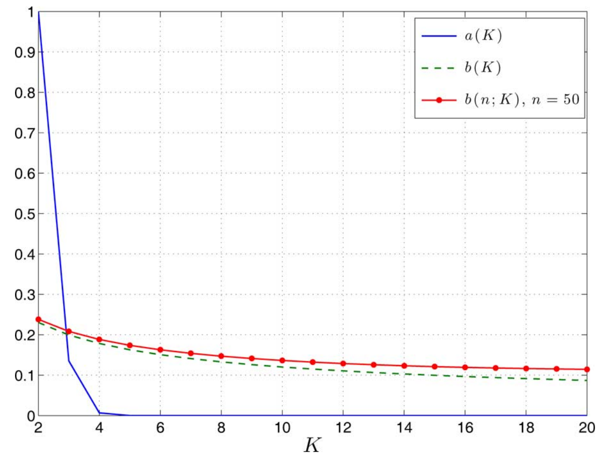

Fig. 1. For $n = 50$, we compare the coefficients $a(K)$, $b(K)$ and $b(n; K)$. It is clear that $a(K) < b(K) < b(n; K)$ for all $K = 3, 4, \ldots$, so that the lower bound $1 - a(K)Q(n; K)$ obtained here is stronger (i.e., larger) than the lower bound $1 - b(n; K)Q(n; K)$ derived in [6].

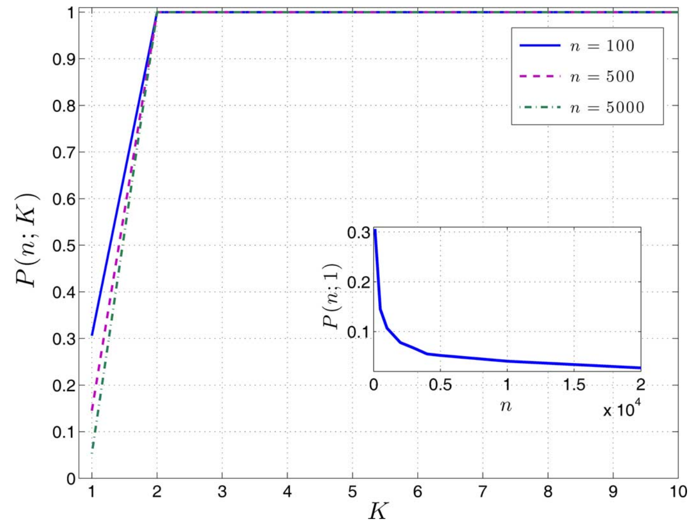

Fig. 2. Empirical probability $P(n; K)$ versus K for $n = 100$, $n = 500$ and $n = 5000$. (Inset) The empirical probability $P(n; 1)$ versus n.

much faster (in fact, exponentially fast) than $b(n; K)$ as K increases. This confirms that the upper bound given in Theorem 3.1 for the probability of connectivity is much sharper than the bound available in [6]. Although $K = 2$ is already enough to ensure connectivity with high probability, in a realistic WSN setting, we expect K to take larger values in order to accommodate other network requirements and to ensure connectivity under severe channel conditions [21].

C. Simulation Study

We now explore the main result of the paper via computer simulations. First, for three typical network sizes, i.e., for $n = 100$, $n = 500$, and $n = 5000$, we look at the probability that $\mathbb{H}(n; K)$ is connected as the parameter K varies from $K = 1$ to $K = 10$. For each pair of (n, K) values, we generate 10^6 independent samples of the graph $\mathbb{H}(n; K)$ and count the number of times (out of a possible 10^6) that the obtained graph is connected. Dividing this count by 10^6, we obtain the (empirical) probability that $\mathbb{H}(n; K)$ is connected. The results, depicted in Fig. 2, readily confirm Theorem 3.1 and the bound (9). In fact, with $K = 2$, we have observed only two (out of a possible 10^6) instances where the generated graph was disconnected; for $K > 2$, all instantiations of $\mathbb{H}(n; K)$ were connected. In the inset of Fig. 2, we focus on the case $K = 1$ and plot the variations of $P(n; 1)$ with respect to network size n. Here, each estimate is constructed on the basis of 2000 independent samples. We see that $P(n; 1)$ approaches zero as n gets large, confirming the zero-law in Theorem 3.2.

IV. Comments

Before giving proofs in Sections V and VI, we pause for some comments concerning the results.

A. Correlated Edge Assignments

For each p in $[0, 1]$ and $n = 2, 3, \ldots$, let $\mathbb{G}(n; p)$ denote the Erdős–Rényi graph on the vertex set $\{1, \ldots, n\}$ with edge probability p. While edge assignments are mutually independent in $\mathbb{G}(n; p)$, they are strongly correlated in $\mathbb{H}(n; K)$, namely *negatively associated* in the sense of Joag-Dev and Proschan [10]; details are available in [18] and [21]. Thus, $\mathbb{H}(n; K)$ cannot be equated with $\mathbb{G}(n; p)$ even when the parameters p and K are selected so that the edge assignment probabilities in these two graphs coincide, say $\lambda(n; K) = p$. As a result, neither Theorem 3.1 nor Corollary 3.3 are consequences of classical results for ER graphs [1]. See also the discussion in Section IV-C.

B. Connectivity Versus Absence of Isolated Nodes

To drive the point further, note the following: In many known classes of random graphs, the absence of isolated nodes and graph connectivity are asymptotically equivalent properties, e.g., ER graphs [1], [4], geometric random graphs [13], and random key graphs [14], [19], [20]. This equivalence, when it holds, is used to advantage by first establishing the zero-one law for the absence of isolated nodes, a step which is usually much simpler to complete with the help of the method of first and second moments [9, p. 55]. However, there are no isolated nodes in $\mathbb{H}(n; K)$ since each node is of degree at least K. Thus, the class of random graphs studied here provides an example where graph connectivity and the absence of isolated nodes are not asymptotically equivalent properties; in fact, this is what makes the proof of the zero-law more intricate.

C. Earlier Analysis via Transfers

In the original paper of Chan *et al.* [3] (as in [8]), the connectivity of $\mathbb{H}(n; K)$ was analyzed through the following two-step process: 1) First, the random graph $\mathbb{H}(n; K)$ was equated with an ER graph so that the edge assignment probabilities are asymptotically equivalent; 2) Next, well-known connectivity results for ER graphs were formally transferred to $\mathbb{H}(n; K)$ under this constraint. We now revisit this transfer argument in some details.

Recall that in ER graphs, the property of graph connectivity exhibits the following zero-one law [1]: There is no loss of generality in writing any scaling $p : \mathbb{N}_0 \to [0, 1]$ for the edge assignment probability in the form

$$p_n = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{17}$$

for some deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$. We then have the zero-one law

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p_n) \text{ is connected}\right] = \begin{cases} 0, & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1, & \text{if } \lim_{n\to\infty} \alpha_n = +\infty. \end{cases} \tag{18}$$

It is tempting to take advantage of this zero-one law as follows: A given scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ is said to be *asymptotically matched* to a scaling $p : \mathbb{N}_0 \to [0,1]$ for ER graphs provided $\lambda(n;K_n) \sim p_n$. This requirement ensures that the expected degrees (per node) in the random graphs $\mathbb{G}(n;p_n)$ and $\mathbb{H}(n;K_n)$ are asymptotically equivalent. In view of (4), this amounts to

$$p_n \sim \frac{2K_n}{n-1} - \left(\frac{K_n}{n-1}\right)^2. \tag{19}$$

If the scaling $p : \mathbb{N}_0 \to [0,1]$ is put in the form (17) for some deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, then (19) becomes

$$\frac{2K_n}{n-1} - \left(\frac{K_n}{n-1}\right)^2 \sim \frac{\log n + \alpha_n}{n}. \tag{20}$$

With this identification, one might possibly expect that the random graphs $\mathbb{G}(n;p_n)$ and $\mathbb{H}(n;K_n)$ behave in tandem, at least asymptotically, so that by analogy, the following zero-one law

$$\lim_{n\to\infty} P(n;K_n) = \begin{cases} 0, & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1, & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{21}$$

should hold owing to (18). This approach, though appealing for its simplicity, leads to incorrect conclusions as we now show.

Indeed, if the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ is such that $K_n = K^\star$ for some positive integer $K^\star$ for all n sufficiently large, then on that range, (20) gives the corresponding deviation function as

$$\alpha_n = \frac{n}{t_n}\left(\frac{2K^\star}{n-1} - \left(\frac{K^\star}{n-1}\right)^2\right) - \log n$$

for some sequence $t : \mathbb{N}_0 \to \mathbb{R}_+$ with $\lim_{n\to\infty} t_n = 1$. Note that $\lim_{n\to\infty} \alpha_n = -\infty$ regardless of the value of $K^\star$, and according to (21), we would conclude that $\lim_{n\to\infty} P(n;K^\star) = 0$ for *all* positive integers $K^\star$, in clear contradiction with Theorem 3.2.

We could also have used a weaker version of the zero-one law (18) which considers scalings $p : \mathbb{N}_0 \to [0,1]$ of the form

$$p_n \sim c\,\frac{\log n}{n} \tag{22}$$

for some $c > 0$. It easily follows from (18) that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p_n) \text{ is connected}\right] = \begin{cases} 0, & \text{if } 0 < c < 1 \\ 1, & \text{if } 1 < c. \end{cases} \tag{23}$$

This time, (19) requires

$$2K_n \sim c\,\log n \tag{24}$$

under (22), and a formal transfer of (23) suggests the validity of

$$\lim_{n\to\infty} P(n;K_n) = \begin{cases} 0, & \text{if } 0 < c < 1 \\ 1, & \text{if } 1 < c. \end{cases} \tag{25}$$

In particular, from (24) and (25), we read off that K_n should behave like $\gamma \log n$ with $\gamma > \frac{1}{2}$ (respectively, $\gamma < \frac{1}{2}$) in order for $\mathbb{H}(n;K_n)$ to be connected (respectively, disconnected) with a probability approaching 1 for n large. Not only does this conclusion fall short from the result given in Corollary 3.3, but it also leads to incorrect design decisions: For instance, the maximum supportable network size evaluated in [3] and [8] leads to the conclusion that the random pairwise key predistribution scheme is *not* scalable in the context of WSNs. The results given here form the basis for a reevaluation of these conclusions; see [22] and [23] for details.

D. Numerical Comparisons

We close with a numerical example that illustrates the difference between the random K-out graph $\mathbb{H}(n;K)$ and its matched ER graph $\mathbb{G}(n;p)$. For that purpose, we take $n = 75$ and $K = 2$, and select $p = \lambda(75;2) = 0.0533$ so that the matching condition (19) is satisfied exactly. For this setting, we show instantiations of the random K-out [see Fig. 3(a)] and of the corresponding ER graph [see Fig. 3(b)]. The random K-out graph is seen to be connected, while the ER graph is *not* as it has two isolated nodes (shown by a star symbol). In fact, out of 1000 independent realizations of the two graphs (with the same parameters), we observed that the random K-out graph is always connected, while the ER graph is connected only 28% of the time (even with 75 nodes). Thus, the difference in connectivity between the two graphs is present not only in the asymptotic regime, further highlighting the usefulness of Theorem 3.1 for tuning the parameters of the pairwise scheme.

V. Proof of Theorem 3.1

Fix $n = 2, 3, \ldots$ and consider a positive integer K. The conditions

$$2 \le K \quad \text{and} \quad e(K+2) < n \tag{26}$$

are assumed enforced throughout; the second condition automatically implies $K < n$.

A. Basic Bound

For any nonempty subset S of nodes, i.e., $S \subseteq \mathcal{N}$, we say that S is *isolated* in $\mathbb{H}(n;K)$ if there are no edges (in $\mathbb{H}(n;K)$) between the nodes in S and the nodes in the complement $S^c = \mathcal{N} - S$. This is characterized by the event $B_n(K;S)$ given by

$$B_n(K;S) = \bigcap_{i\in S}\bigcap_{j\in S^c}\left([i \notin \Gamma_{n,j}(K)] \cap [j \notin \Gamma_{n,i}(K)]\right).$$

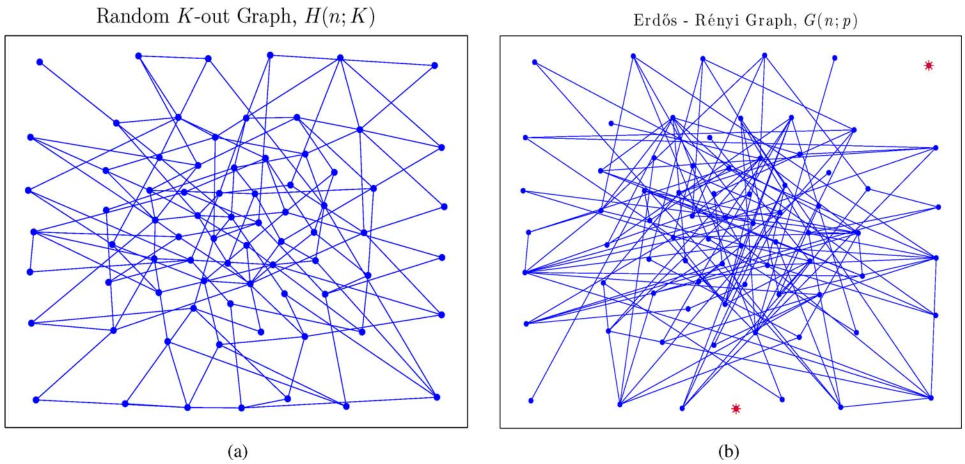

Fig. 3. Instantiation of the random K-out graph $\mathbb{H}(n;K)$ (a) and of the matched ER graph $\mathbb{G}(n;p)$ (b). Both graphs are defined for $n = 75$ nodes with $K = 2$ and $p = \lambda(75;2) = 0.0533$ so that the matching condition (19) is satisfied exactly. While the random K-out graph is connected, the ER graph is *not* connected with two isolated nodes (each indicated by a star symbol).

The discussion starts with the following basic observations: If the realization of $\mathbb{H}(n;K)$ is *not* connected, then there must exist a nonempty subset S of nodes which is isolated in $\mathbb{H}(n;K)$. Since each node in $\mathbb{H}(n;K)$ is connected to at least K other nodes, such an isolated set S in $\mathbb{H}(n;K)$ must necessarily contain at least $K+1$ elements, i.e., $|S| \geq K+1$. Thus, with $C_n(K)$ denoting the event that $\mathbb{H}(n;K)$ is connected, we have the inclusion

$$C_n(K)^c \subseteq \cup_{S \in \mathcal{P}_n : |S| \geq K+1} B_n(K;S) \tag{27}$$

where $\mathcal{P}_n$ stands for the collection of all nonempty subsets of $\mathcal{N}$. A moment of reflection should convince the reader that this union need only be taken over all subsets S of $\mathcal{N}$ with $K+1 \leq |S| \leq \lfloor \frac{n}{2} \rfloor$, a nonvacuous condition under (26). A standard union bound argument immediately gives

$$\begin{aligned}\mathbb{P}\left[C_n(K)^c\right] &\leq \sum_{S \in \mathcal{P}_n : K+1 \leq |S| \leq \lfloor \frac{n}{2} \rfloor} \mathbb{P}\left[B_n(K;S)\right] \\ &= \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\sum_{S \in \mathcal{P}_{n,r}} \mathbb{P}\left[B_n(K;S)\right] \right) \end{aligned} \tag{28}$$

where $\mathcal{P}_{n,r}$ denotes the collection of all subsets of $\mathcal{N}$ with exactly r elements.

For each $r = 1, \ldots, n$, we simplify the notation by writing $B_{n,r}(K) = B_n(K;\{1,\ldots,r\})$. Under the enforced assumptions, exchangeability implies

$$\mathbb{P}\left[B_n(K;S)\right] = \mathbb{P}\left[B_{n,r}(K)\right], \quad S \in \mathcal{P}_{n,r}$$

and the expression

$$\sum_{S \in \mathcal{P}_{n,r}} \mathbb{P}\left[B_n(K;S)\right] = \binom{n}{r} \mathbb{P}\left[B_{n,r}(K)\right] \tag{29}$$

follows since $|\mathcal{P}_{n,r}| = \binom{n}{r}$. Substituting into (28), we obtain the bounds

$$\mathbb{P}\left[C_n(K)^c\right] \leq \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[B_{n,r}(K)\right]. \tag{30}$$

For each $r = K+1, \ldots, n$, it is easy to check that

$$\mathbb{P}\left[B_{n,r}(K)\right] = \left(\frac{\binom{r-1}{K}}{\binom{n-1}{K}} \right)^r \cdot \left(\frac{\binom{n-r-1}{K}}{\binom{n-1}{K}} \right)^{n-r}. \tag{31}$$

To see why this last relation holds, recall that for nodes $\{1,\ldots,r\}$ to be isolated in $\mathbb{H}(n;K)$, we need that 1) none of the sets $\Gamma_{n,1}(K),\ldots,\Gamma_{n,r}(K)$ contains an element from the set $\{r+1,\ldots,n\}$; and 2) none of the sets $\Gamma_{n,r+1}(K),\ldots,\Gamma_{n,n}(K)$ contains an element from $\{1,\ldots,r\}$. More precisely, we must have

$$\Gamma_{n,i}(K) \subseteq \{1,\ldots,r\} - \{i\}, \quad i = 1,\ldots,r$$

and

$$\Gamma_{n,j}(K) \subseteq \{r+1,\ldots,n\} - \{j\}, \quad j = r+1,\ldots,n.$$

The validity of (31) is now immediate from (1) and the mutual independence of the rvs $\Gamma_{n,1}(K),\ldots,\Gamma_{n,n}(K)$.

Substituting (31) into (30) readily yields

$$\begin{aligned}&\mathbb{P}\left[C_n(K)^c\right] \\ &\leq \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \left(\frac{\binom{r-1}{K}}{\binom{n-1}{K}} \right)^r \left(\frac{\binom{n-r-1}{K}}{\binom{n-1}{K}} \right)^{n-r}. \end{aligned} \tag{32}$$

B. Simplifying (32)

Next we seek a computable upper bound to the right handside of (32). 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 $\ell = K-1$. Using this fact in (32) together with the standard bound

$$\binom{n}{r} \leq \left(\frac{ne}{r} \right)^r, \quad r = 1,\ldots,n,$$

we conclude that

$$\begin{aligned}
&\mathbb{P}\left[C_n(K)^c\right] \\
&\leq \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{ne}{r}\right)^r \left(\frac{r-1}{n-1}\right)^{rK} \left(1 - \frac{r}{n-1}\right)^{K(n-r)} \\
&\leq \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{ne}{r}\right)^r \left(\frac{r}{n}\right)^{rK} \left(1 - \frac{r}{n}\right)^{K(n-r)} \\
&\leq \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{ne}{r}\right)^r \left(\frac{r}{n}\right)^{rK} e^{-rK\frac{(n-r)}{n}} \\
&= \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{r}{n}\right)^{r(K-1)} \left(e^{1-K\frac{(n-r)}{n}}\right)^r. \qquad (33)
\end{aligned}$$

On the range $r = K+1, \ldots, \lfloor \frac{n}{2} \rfloor$, we note that

$$K\,\frac{n-r}{n} \geq K\,\frac{n - \lfloor \frac{n}{2} \rfloor}{n} \geq \frac{K}{2}$$

so that

$$\left(e^{1-K\frac{n-r}{n}}\right)^r \leq e^{(1-\frac{K}{2})r} \leq e^{-\frac{1}{2}(K+1)(K-2)}$$

where the last inequality used the fact that $K \geq 2$. Using this bound into (33), we find

$$\begin{aligned}
\mathbb{P}\left[C_n(K)^c\right] &\leq a(K) \sum_{r=K+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{r}{n}\right)^{r(K-1)} \\
&= a(K) \left(\frac{K+1}{n}\right)^{K^2-1} \qquad (34) \\
&\quad + a(K) \sum_{r=K+2}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{r}{n}\right)^{r(K-1)}
\end{aligned}$$

with $a(K)$ given by (5).

C. Bounding the Sum in (34)

Under the constraint (26), we necessarily have $K+2 \leq \lfloor \frac{n}{2} \rfloor$, and the sum in (34) is, therefore, not empty. To bound it further, we proceed as follows: Write

$$\left(\frac{x}{n}\right)^{x(K-1)} = e^{(K-1)f_n(x)}, \quad x \geq 1 \qquad (35)$$

with

$$f_n(x) = x \log\left(\frac{x}{n}\right) = x\left(\log x - \log n\right).$$

It is easy to see that $r \to f_n(r)$ is monotone decreasing on the range $r = 1, \ldots, \lfloor \frac{n}{e} \rfloor$ and monotone increasing on the range $r = \lfloor \frac{n}{e} \rfloor + 1, \ldots, \lfloor \frac{n}{2} \rfloor$; hence

$$\begin{aligned}
&\max\left(f_n(r),\ r = K+2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right) \\
&\quad = \max\left(f_n(K+2), f_n\left(\left\lfloor \frac{n}{2} \right\rfloor\right)\right). \qquad (36)
\end{aligned}$$

While $K+2 \leq \lfloor \frac{n}{e} \rfloor$ by virtue of (26), we now show that

$$f_n\left(\left\lfloor \frac{n}{2} \right\rfloor\right) \leq f_n(K+2) \qquad (37)$$

for all n large enough, say $n \geq n(K)$ for some finite integer $n(K)$ which depends on K. Indeed, (37) is equivalent to

$$\left\lfloor \frac{n}{2} \right\rfloor \log\left(\frac{\lfloor \frac{n}{2} \rfloor}{n}\right) \leq (K+2)\left(\log(K+2) - \log n\right),$$

a condition which we rewrite as

$$n\left(\frac{\lfloor \frac{n}{2} \rfloor}{n}\right) \log\left(\frac{\lfloor \frac{n}{2} \rfloor}{n}\right) \leq (K+2)\left(\log(K+2) - \log n\right).$$

The mapping $t \to t\log t$ is monotone increasing on the interval (e^{-1}, ∞). Therefore, since $\lfloor \frac{n}{2} \rfloor \leq \frac{n}{2}$, the inequality (37) will hold as soon as

$$-\left(\frac{n}{2}\right)\log 2 \leq (K+2)\left(\log(K+2) - \log n\right) \qquad (38)$$

whenever n satisfies the constraint

$$\frac{1}{e} < \frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor.$$

A straightforward analysis shows that this occurs for all $n > 4$, a range automatically guaranteed under (26). Condition (38) simplifies to read

$$\log n \leq \left(\frac{\log 2}{2(K+2)}\right) \cdot n + \log(K+2). \qquad (39)$$

It is easy to check that (39) holds as an equality for $n = 4(K+2)$ and as a strict inequality for all $n > 4(K+2)$. The choice $n(K) = 4(K+2)$ is, therefore, acceptable for (38) (hence (37)) to hold.

Using (35)–(37), we get

$$\begin{aligned}
&\max\left(\left(\frac{r}{n}\right)^{r(K-1)} : r = K+2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right) \\
&\quad = \left(\frac{K+2}{n}\right)^{(K+2)(K-1)}
\end{aligned}$$

for all $n \geq n(K)$ so that

$$\sum_{r=K+2}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{r}{n}\right)^{r(K-1)} \leq \left\lfloor \frac{n}{2} \right\rfloor \cdot \left(\frac{K+2}{n}\right)^{(K+2)(K-1)}.$$

Using this fact in (34), we readily obtain the conclusion (6) since $P(n;K) = 1 - \mathbb{P}\left[C_n(K)^c\right]$. ■

VI. Proof of the Zero-Law in Theorem 3.2

Fix $n = 2, 3, \ldots$. When $K = 1$, the random sets $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$ are now singletons, and can be interpreted as $\mathcal{N}$-valued rvs $\Gamma_{n,1}, \ldots, \Gamma_{n,n}$ (as we do from now on) such that $\Gamma_{n,i} \neq i$ for each $i = 1, \ldots, n$. Thus, the rv $\Gamma_{n,i}$ denotes the node randomly associated (paired) with node i; it is distributed according to

$$\mathbb{P}\left[\Gamma_{n,i} = j\right] = \frac{1}{n-1}, \quad \begin{array}{c} j \neq i \\ j = 1, \ldots, n. \end{array} \qquad (40)$$

A *formation* (on $\mathcal{N}$) is any sequence $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n)$ such that for each $i = 1, \ldots, n$, the component γ_i is an element of $\mathcal{N}$ with $\gamma_i \neq i$. In other words, $\boldsymbol{\gamma}$ is one of the $(n-1)^n$ possible realizations of the rv vector $(\Gamma_{n,1}, \ldots, \Gamma_{n,n})$. If $\mathcal{F}_n$ denotes the collection of all formations on $\mathcal{N}$, then

$$\mathbb{P}\left[\Gamma_{n,i} = \gamma_i,\ i = 1, \ldots, n\right] = \frac{1}{(n-1)^n}, \quad \boldsymbol{\gamma} \in \mathcal{F}_n$$

since the rvs $\Gamma_{n,1}, \ldots, \Gamma_{n,n}$ are i.i.d. rvs, each distributed according to (40).

With each formation $\boldsymbol{\gamma}$ in $\mathcal{F}_n$, we associate two graphs on the vertex set $\{1, \ldots, n\}$: We first define a *directed* graph on these vertices by creating a directed edge from node i to node j whenever $\gamma_i = j$; let $H_{\boldsymbol{\gamma}}(n)$ denote this directed graph. Next, we introduce the *undirected* graph $H^\star_{\boldsymbol{\gamma}}(n)$ naturally induced by $H_{\boldsymbol{\gamma}}(n)$—Just turn all directed edges into undirected ones. It is plain that $H^\star_{\boldsymbol{\gamma}}(n)$ realizes the random graph $\mathbb{H}(n;1)$ when $(\Gamma_{n,1}, \ldots, \Gamma_{n,n}) = \boldsymbol{\gamma}$.

In what follows, we use the conventional notion of connectivity for directed graphs [1]: A directed graph is connected if and only if the underlying *undirected* graph is connected—This is to be distinguished from the notion of *strong* connectivity defined for directed graphs. With this in mind, it follows from the discussion so far that

$$P(n;1) = \frac{N_n}{(n-1)^n} \tag{41}$$

where N_n counts the number of formations in $\mathcal{F}_n$ whose directed graphs are connected, namely

$$N_n = \sum_{\boldsymbol{\gamma} \in \mathcal{F}_n} \mathbf{1}\left[\, H_{\boldsymbol{\gamma}}(n) \text{ is connected } \right]. \tag{42}$$

The proof now proceeds by obtaining the asymptotic behavior of N_n for large n. This will be done with the help of the following easily validated facts:

1) By definition, $H^\star_{\boldsymbol{\gamma}}(n)$ is connected if and only if $H_{\boldsymbol{\gamma}}(n)$ is connected.
2) The undirected graph $H^\star_{\boldsymbol{\gamma}}(n)$ can have *at most* n edges since $H_{\boldsymbol{\gamma}}(n)$ has *exactly* n directed edges (as each of the n nodes has out-degree 1).
3) If $H^\star_{\boldsymbol{\gamma}}(n)$ *is* connected, then basic principles force $H^\star_{\boldsymbol{\gamma}}(n)$ to have *at least* $n-1$ edges.

It follows that there are two distinct types of formations which yield (undirected) connected graphs:

A) If $H^\star_{\boldsymbol{\gamma}}(n)$ is connected with $n-1$ edges, then $H^\star_{\boldsymbol{\gamma}}(n)$ is necessarily a *tree*, and $H_{\boldsymbol{\gamma}}(n)$ has exactly one bidirectional edge.

B) If $H^\star_{\boldsymbol{\gamma}}(n)$ is connected with n edges (and so cannot be a tree), then the graph $H_{\boldsymbol{\gamma}}(n)$ is also connected, has no bidirectional edge and must contain exactly one directed *cycle*. This can easily be validated upon noting that each node in $H_{\boldsymbol{\gamma}}(n)$ has out-degree 1; see Fig. 4.

This dichotomy leads to decomposing N_n as

$$N_n = A_n + B_n \tag{43}$$

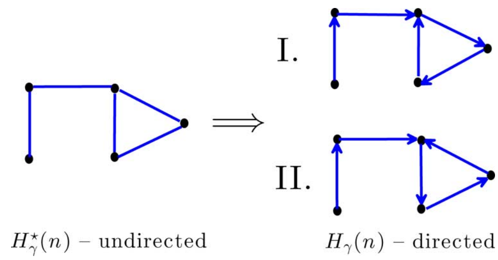

Fig. 4. Case B is illustrated with $n = 5$ nodes. On the left, we show an example where $H^\star_{\boldsymbol{\gamma}}(n)$ is connected and has 5 edges. On the right, we show the corresponding possibilities for the directed graph $H_{\boldsymbol{\gamma}}(n)$. Since $H_{\boldsymbol{\gamma}}(n)$ needs to have five edges with each node having out-degree 1, there are only two such possibilities, one for the clockwise (I) and one for the counter clockwise (II) orientation of the cycle.

with the counts A_n and B_n given by

$$A_n = \sum_{\boldsymbol{\gamma} \in \mathcal{F}_n} \mathbf{1}\left[\, H^\star_{\boldsymbol{\gamma}}(n) \text{ is a tree } \right]$$

and

$$B_n = \sum_{\boldsymbol{\gamma} \in \mathcal{F}_n} \mathbf{1}\left[\begin{array}{c} H^\star_{\boldsymbol{\gamma}}(n) \text{ is connected and} \\ \text{has } n \text{ edges} \end{array}\right],$$

respectively. We take each count in turn.

Case A

The count A_n tallies all formations $\boldsymbol{\gamma}$ in $\mathcal{F}_n$ such that $H^\star_{\boldsymbol{\gamma}}(n)$ is a tree with $n-1$ edges. With $\mathcal{T}_n$ denoting the collection of labeled trees on the set of vertices $\{1, \ldots, n\}$, we recall that $|\mathcal{T}_n| = n^{n-2}$ by Cayley's formula [12]. Any such labeled tree can be the underlying undirected graph for $n-1$ different formations (each corresponding to one of the $n-1$ possible locations for the single bidirectional edge). Therefore, we have

$$\begin{aligned} A_n &= \sum_{T \in \mathcal{T}_n} \left(\sum\nolimits_{\boldsymbol{\gamma} \in \mathcal{F}_n} \mathbf{1}\left[H^\star_{\boldsymbol{\gamma}}(n) = T \right] \right) \\ &= n^{n-2} \cdot (n-1), \end{aligned}$$

so that

$$\frac{A_n}{(n-1)^n} = \frac{1}{n} \cdot \left(\frac{n}{n-1} \right)^{n-1} \sim \frac{e}{n}. \tag{44}$$

Case B

Recall that B_n counts all formations $\boldsymbol{\gamma}$ in $\mathcal{F}_n$ such that $H^\star_{\boldsymbol{\gamma}}(n)$ is connected with n edges and thus has exactly one undirected cycle. For each such formation, the corresponding directed graph $H_{\boldsymbol{\gamma}}(n)$ has exactly one directed cycle, and cannot have any bidirectional edge (since the number of edges in $H^\star_{\boldsymbol{\gamma}}(n)$ and $H_{\boldsymbol{\gamma}}(n)$ are both n). It is plain that a connected graph $H^\star_{\boldsymbol{\gamma}}(n)$ with n edges can be the underlying undirected graph of two different formations (each corresponding to one of the two possible orientations of the directed cycle); see Fig. 4 for an illustration of this fact.

Now let $\mathcal{T}_n^+$ denote the set of undirected graphs on n nodes which are connected and have exactly n edges. We find

$$\begin{aligned} B_n &= \sum_{G \in \mathcal{T}_n^+} \left(\sum_{\gamma \in \mathcal{F}_n} \mathbf{1}\left[H_\gamma^\star(n) = G \right] \right) \\ &= 2 \cdot |\mathcal{T}_n^+|, \end{aligned}$$

whence

$$\frac{B_n}{(n-1)^n} = \frac{2}{(n-1)^n} \cdot |\mathcal{T}_n^+|.$$

However, it is known [7, pp. 133–134] that

$$|\mathcal{T}_n^+| \sim \frac{1}{4}\sqrt{2\pi} n^{n-\frac{1}{2}},$$

so that

$$\begin{aligned} \frac{B_n}{(n-1)^n} &\sim \frac{\sqrt{2\pi}}{2}\left(\frac{n}{n-1}\right)^n n^{-\frac{1}{2}} \\ &\sim \frac{\sqrt{2\pi}e}{2} n^{-\frac{1}{2}}. \end{aligned} \tag{45}$$

Letting n go to infinity in (41), we readily get $\lim_{n\to\infty} P(n;1) = 0$ as we make use of (43)–(45). ■

Acknowledgment

We thank the following individuals: Dr. H. Chan of CyLab at Carnegie Mellon University for some insightful comments concerning this work; Prof. A. Barg from the Department of Electrical and Computer Engineering at the University of Maryland for reference [7]; Prof. A. Srinivasan from the Department of Computer Science at the University of Maryland for making us aware of the work by Fenner and Frieze [6]; and the anonymous reviewers for their careful reading of the manuscript and for their constructive comments.

References

[1] B. Bollobás, *Random Graphs*, ser. Cambridge Studies in Advanced Mathematics, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[2] S. A. Çamtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: A survey," Comput. Sci. Dept., Rensselaer Polytechnic Inst.. Troy, NY, USA, Mar. 2005, Tech. Rep. TR-05-07.

[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Res. Security Privacy*, Oakland, CA, USA, May 2003, pp. 197–213.

[4] M. Draief and L. Massoulié, *Epidemics and Rumours in Complex Networks*, ser. London Mathematical Society Lecture Notes Series. Cambridge, U.K.: Cambridge Univ. Press, 2010, vol. 369.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Security*, Washington, DC, USA, Nov. 2002, pp. 41–47.

[6] T. I. Fenner and A. M. Frieze, "On the connectivity of random m-orientable graphs and digraphs," *Combinatorica*, vol. 2, pp. 347–359, 1982.

[7] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, Jan. 2009.

[8] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in *Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw.*, Washington, DC, USA, Oct. 2004, pp. 43–52.

[9] S. Janson, T. Łuczak, and A. Ruciński, *Random Graphs*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization. New York, NY, USA: Wiley, 2000.

[10] K. Joag-Dev and F. Proschan, "Negative association of random variables, with applications," *Ann. Statist.*, vol. 11, pp. 266–295, 1983.

[11] L. Katz, "Probability of indecomposability of a random mapping function," *Ann. Math. Statist.*, vol. 25, pp. 512–517, 1955.

[12] G. E. Martin, *Counting: The Art of Enumerative Combinatorics*. New York, NY, USA: Springer-Verlag, 2001.

[13] M. D. Penrose, *Random Geometric Graphs*, ser. Oxford Studies in Probability. New York, NY, USA: Oxford Univ. Press, 2003, vol. 5.

[14] K. Rybarczyk, "Diameter of the uniform random intersection graph with a note on the connectivity and the phase transition," *Discr. Math.*, vol. 311, pp. 1998–2019, 2011.

[15] J. Spencer, "Nine lectures on random graphs," in *École d'Été de Probabilités de Saint Flour XXI – 1991*, ser. Springer Lecture Notes in Mathematics, P. L. Hennequin, Ed. Berlin, Germany: Springer-Verlag, 1993, vol. 1541, pp. 293–347.

[16] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta. Autom. Sinica*, vol. 12, pp. 900–906, 2006.

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

[18] O. Yağan, "Random graph modeling of key distribution schemes in wireless sensor networks," Ph.D. dissertation, Dept. Electr. Comput. Eng., Univ. Maryland, College Park, MD, USA, Jun. 2011.

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

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

[21] O. Yağan and A. M. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1740–1760, Mar. 2013.

[22] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key predistribution schemes," in *Proc. 9th Int. Symp. Model. Optim. Mobile, Ad Hoc, Wireless Netw.*, Princeton, NJ, USA, May 2011, pp. 257–264.

[23] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key distribution scheme: Gradual deployment and key ring sizes," *Perform. Eval.*, vol. 70, no. 7-8, pp. 493–512, Jul. 2013.

Osman Yağan (S'07–M'12) received the B.S. degree in Electrical and Electronics Engineering from Middle East Technical University, Ankara (Turkey) in 2007, and the Ph.D. degree in Electrical and Computer Engineering from University of Maryland, College Park, MD in 2011.

He was a visiting Postdoctoral Scholar at Arizona State University during Fall 2011 and then a Postdoctoral Research Fellow in the Cyber Security Laboratory (CyLab) at Carnegie Mellon University until July 2013. In August 2013, he joined the faculty of the Department of Electrical and Computer Engineering at Carnegie Mellon University as an Assistant Research Professor.

Dr. Yağan's research interests include wireless communications, security, random graphs, social and information networks, and cyber-physical systems.

Armand M. Makowski (M'83–SM'94–F'06) received the Licence en Sciences Mathématiques from the Université Libre de Bruxelles in 1975, the M.S. degree in Engineering-Systems Science from U.C.L.A. in 1976 and the Ph.D. degree in Applied Mathematics from the University of Kentucky in 1981. In August 1981, he joined the faculty of the Electrical Engineering Department at the University of Maryland College Park, where he is Professor of Electrical and Computer Engineering. He has held a joint appointment with the Institute for Systems Research since its establishment in 1985.

Armand Makowski was a C.R.B. Fellow of the Belgian-American Educational Foundation (BAEF) for the academic year 1975–76; he is also a 1984 recipient of the NSF Presidential Young Investigator Award and became an IEEE Fellow in 2006.

His research interests lie in applying advanced methods from the theory of stochastic processes to the modeling, design and performance evaluation of engineering systems, with particular emphasis on communication systems and networks.