Designing secure and reliable wireless sensor networks under a pairwise key predistribution scheme

Faruk Yavuz, Jun Zhao, Osman Yağan, and Virgil Gligor
CyLab and Dept. of ECE, Carnegie Mellon University
{fyavuz,junzhao,oyagan,virgil}@andrew.cmu.edu

***Abstract*—We investigate k-connectivity in secure wireless sensor networks under the random pairwise key predistribution scheme with unreliable links; a network is said to be k-connected if it remains connected despite the failure of any of its $(k-1)$ nodes or links. With wireless communication links modeled as independent on-off channels, this amounts to analyzing a *random graph model* formed by *intersecting* a random K-out graph and an Erdős-Rényi graph. We present conditions on how to scale the parameters of this intersection model so that the resulting graph is k-connected with probability approaching to one (resp. zero) as the number of nodes gets large. The resulting zero-one law is shown to improve and sharpen the previous result on the 1-connectivity of the same model. We also provide numerical results to support our analysis and show that even in the finite node regime, our results can provide useful guidelines for designing sensor networks that are secure and reliable.**

***Index Terms*—Wireless sensor networks, key predistribution, random graphs, k-connectivity.**

I. Introduction

Random key predistribution schemes have been extensively studied in the literature over the last decade and they are widely regarded as appropriate solutions to secure communications in resource-constrained wireless sensor networks (WSNs) [3]–[5], [10]–[18]. The idea of randomly assigning cryptographic keys to sensors before deployment has been introduced by Eschenauer and Gligor [5]. Following this seminal work [5], Chan *et al.* [3] proposed the random pairwise key predistribution scheme, which has received much attention over the last decade [11]–[17].

The random pairwise key predisrtibution scheme operates as follows. In a WSN with n sensors, prior to deployment, each sensor is *paired* with K distinct sensors that are selected randomly from all other $(n-1)$ sensors. For each such sensor pair, a unique pairwise key is then generated and loaded into the memory modules of the paired sensors together with their IDs. After deployment, any two sensors can securely communicate over an existing wireless link if and only if they share at least one common key. Precise implementation details are given in Section II-A.

Given the randomness involved in the key predistribution mechanism, as well as in the availability of wireless communication links, there arises a basic question as to how one can adjust the scheme parameter K so that the resulting network is both *securely* and *reliably* connected with high probability. Reliability against the failure of sensors or links is particularly important in WSN applications where sensors are deployed in hostile environments (e.g., battlefield surveillance), or, are unattended for long periods of time (e.g., environmental monitoring), or, are used in life-critical applications (e.g., patient monitoring).

With these in mind, this paper is devoted to finalize our analysis initiated in [16] towards k-connectivity for secure WSNs under the random pairwise key predistribution scheme. A network (or a graph) is said to be k-connected if it remains connected despite the deletion of any $(k-1)$ nodes or links; a graph is simply deemed connected if it is 1-connected. Therefore, k-connectivity provides a guarantee of network reliability against the possible failures of $(k-1)$ sensors or links due to adversarial attacks, battery depletion, harsh environmental conditions, etc. Same with [16], the analysis here is conducted under a wireless communication model comprising independent channels that are either *on* with probability p or *off* with probability $(1-p)$. Such on/off channel model has been extensively used recently [10], [14]–[18] in the context of secure WSNs, and is also shown to well approximate the disk model [10], [15] (whereby any two sensors need to be within a certain distance of each other to have a wireless link in between).

Our main result is a zero-one law for the property of k-connectivity. Namely, we present scaling conditions on the parameters p and K with respect to the number of sensors n, such that the studied WSN is k-connected with probability approaching to zero, or one, as the number of sensors n gets large. This result extends and improves upon the zero-one law for 1-connectivity obtained by Yağan and Makowski [14], [15]. We also

present numerical results for the finite node case under various parameter settings. This extensive simulation study suggests that although asymptotic in nature, our main results can still help design WSNs (in a secure and reliable manner) in practical scenarios.

We organize the rest of the paper as follows. Section II describes the system model in detail. We provide the main results in Section III. Section IV presents some comments and discussion; in particular, we give a comparison with related work and numerical experiments that confirm our analytical findings. We close in Section V with an outline of the proof of our main result.

II. Basic Building Blocks

A. The random pairwise key predistribution scheme

The random pairwise key predistribution scheme of Chan et al. [3] is motivated by the following advantages over the original EG scheme: (i) Even if some nodes are captured, the secrecy of the remaining nodes is *perfectly* preserved; (ii) Unlike earlier schemes, this pairwise scheme enables both node-to-node authentication and quorum-based revocation. See [11] for a detailed comparison of these two classical key predistribution schemes.

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

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

Put differently, $\Gamma_{n,i}(K)$ is selected *uniformly* at random among all subsets of $\mathcal{V}_{-i}$ with size K and, random variables $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$ are mutually independent.

After this *offline* random pairing process, we construct the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$, one for each node, as in [13]–[15]. In essence, key rings are constructed such that two nodes i and j share a pairwise key (that is assigned *exclusively* to the pair of nodes i and j) if at least one of the events $i \in \Gamma_{n,j}(K)$ or $j \in \Gamma_{n,i}(K)$ takes place. In this case, nodes i and j can securely communicate over an *existing* wireless communication link between them.

B. Random K-out graphs

The pairwise key 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 K-adjacent, written $i \sim_K j$, if and only if (iff) they have at least one key in common in their key rings, namely

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

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (2). This ensures that edges in $\mathbb{H}(n; K)$ represent pairs of sensors that have at least one cryptographic key in common, and thus that can securely communicate over an *existing* communication channel. Let $\lambda_n(K)$ define the edge assignment probability in $\mathbb{H}(n; K)$; i.e., we have $\mathbb{P}\left[i \sim_K j\right] = \lambda_n(K)$ for any distinct $i, j \in \mathcal{V}$. It is easy to check that [13]

$$\lambda_n(K) = 2K/(n-1) - K^2/(n-1)^2. \tag{3}$$

The random graph $\mathbb{H}(n; K)$ is known in the literature as the random K-out graph [2], or random K-orientable graph [7]. In some references, $\mathbb{H}(n; K)$ is defined in the following manner that is easily seen to be equivalent to the adjacency condition (2): To each of the n vertices assign exactly K arcs towards K distinct vertices that are selected uniformly at random, and then ignore the orientation of the arcs.

C. Intersection of $\mathbb{H}(n; K)$ with Erdős-Rényi graphs

As mentioned earlier, we assume a simple wireless communication model that consists of independent channels, each of which can be either on or off. Thus, with p in $(0, 1)$, let $\{B_{ij}(p), 1 \leq i < j \leq n\}$ denote independent and identically distributed $\{0, 1\}$-valued random variables with success probability p. The channel between nodes i and j is available (resp. on) with probability p and unavailable (resp. off) with probability $1 - p$. Distinct nodes i and j are said to be B-adjacent, written $i \sim_B j$, if $B_{ij}(p) = 1$. B-adjacency defines the standard Erdős-Rényi (ER) graph $\mathbb{G}(n; p)$ on the vertex set $\{1, \ldots, n\}$ [2]. Obviously, $\mathbb{P}\left[i \sim_B j\right] = p$.

The random graph model studied here is obtained by *intersecting* the random graphs induced by the pairwise key predistribution scheme, and by the on-off communication model, respectively. Namely, we consider the intersection of $\mathbb{H}(n; K)$ with the ER graph $\mathbb{G}(n; p)$. In this case, distinct nodes i and j are said to be adjacent, written $i \sim j$, if and only if they are both K-adjacent and B-adjacent, namely

$$i \sim j \quad \text{iff} \quad \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset \text{ and } B_{ij}(p) = 1. \tag{4}$$

The resulting *undirected* random graph defined on the vertex set $\{1, \ldots, n\}$ through this notion of adjacency is denoted $\mathbb{H} \cap \mathbb{G}(n; K, p)$. The relevance of

$\mathbb{H} \cap \mathbb{G}(n; K, p)$ in the context of secure WSNs is now clear. Two nodes that are connected by an edge in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ share at least one cryptographic key *and* have a wireless link available to them, so that they can establish a *secure communication link*.

Throughout we assume the collections of random variables $\{\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)\}$ and $\{B_{ij}(p), 1 \leq i < j \leq n\}$ to be independent, in which case the edge occurrence probability in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is given by

$$\mathbb{P}[i \sim j] = \mathbb{P}[i \sim_K j]\, \mathbb{P}[i \sim_B j] = p\lambda_n(K). \tag{5}$$

D. k-connectivity vs. minimum node degree

Consider an undirected graph $\mathbb{G}$ defined on the vertices $1, \ldots, n$. The degree of a node i, denoted d_i, is defined as the total number of links incident on it. Let δ be the *minimum* node degree in $\mathbb{G}$, i.e., $\delta = \min\{d_1, \ldots, d_n\}$. We also let κ_v denote the *vertex connectivity* of $\mathbb{G}$ defined as the minimum number of vertices whose deletion renders $\mathbb{G}$ disconnected; if $\mathbb{G}$ is not connected we clearly have $\kappa_v = 0$. The *edge connectivity* κ_e is defined similarly in terms of edges, as the minimum number of edges that needs to be deleted to make $\mathbb{G}$ disconnected. For any graph $\mathbb{G}$, it is not difficult to see that [6]

$$\kappa_v \leq \kappa_e \leq \delta. \tag{6}$$

For each $k = 0, 1, 2, \ldots$, we say that the graph $\mathbb{G}$ is k-vertex-connected if it holds that $\kappa_v \geq k$, whereas it is said to be k-edge-connected if $\kappa_e \geq k$. It is immediate from (6) that if a graph is k-vertex-connected, then it is also k-edge-connected, and its minimum degree is at least k. With this in mind, throughout we shall say that a graph is k-connected (without referring to vertex-connectivity) to refer to the fact that it is k-vertex-connected, and hence k-edge-connected. The terminology that has been in use thus far is now clear. If a graph is k-connected, then we have $\kappa_v, \kappa_e \geq k$, meaning that the graph can not be made disconnected even if any $k-1$ vertices or links are deleted. This is what makes the study of the property of k-connectivity appealing in seeking secure and reliable WSN designs.

III. The results

Our main technical result is given next. Let $\mathbb{N}_0$ be the set of all positive integers and $\mathbb{R}$ be the set of all real numbers. Throughout, we refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* (for random K-out graphs) provided it satisfies the natural condition

$$K_n < n, \quad n = 1, 2, \ldots. \tag{7}$$

Similarly, we let any mapping $p : \mathbb{N}_0 \to (0, 1)$ define a scaling for Erdős-Rényi graphs. We often group the parameters K and p into the ordered pair $\theta \equiv (K, p)$.

Theorem 3.1: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0, 1)$ such that $\lim_{n\to\infty}(n - 2K_n) = \infty$ and $\limsup_{n\to\infty} p_n < 1$. With a sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ defined through

$$\begin{aligned} & p_n K_n \left(1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}\right) \\ = \;& \log n + (k-1)\log\log n + \gamma_n \end{aligned} \tag{8}$$

we have

$$\begin{aligned} & \lim_{n\to\infty} \mathbb{P}[\mathbb{H} \cap \mathbb{G}(n; \theta_n) \text{ is } k\text{-connected}] \\ = \;& \begin{cases} 0 & \text{if } \lim_{n\to\infty} \gamma_n = -\infty, \\ 1 & \text{if } \lim_{n\to\infty} \gamma_n = +\infty. \end{cases} \end{aligned} \tag{9}$$

Theorem 3.1 establishes a zero-one law of k-connectivity for random K-out graphs intersecting Erdős-Rényi graphs, i.e., for $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$, and it resolves a conjecture by the authors that appeared in [16], [17, Conjecture 4.1]. It also complements an analogous result, established by the authors in [16], [17], for the property that minimum node degree in $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$ is at least k; see Theorem 5.1 in Section V. Thus, the main result of this paper shows that the model $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$ provides one more instance where the zero-one laws for k-connectivity and minimum node degree being at least k coincide; other examples include ER graphs [6], random key graphs [18], certain classes of random geometric graphs [9].

The proof of Theorem 3.1 is technically involved and is omitted here given the space limitations. Some basic steps and main ideas are provided in Section V, with full details deferred to [1]. The proof is based on arguments that are reminiscent of those used in the proof of the k-connectivity result for ER graphs [6]. However, the proof of our main result is much more involved than that of the analogous result for ER graphs. This is mainly due to intricate dependencies that exist between the edge occurrence events $\{[i \sim j]\}_{1 \leq i \leq j \leq n}$ in $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$; see [1, Section 7.1] for details.

We now argue that the extra conditions enforced by Theorem 5.1 are mild and do not preclude their application in practical WSNs. First, the condition $\limsup_{n\to\infty} p_n < 1$ enforces that wireless communication channels between nodes do not become available with probability one as n gets large. The situation $\limsup_{n\to\infty} p_n = 1$ that is not covered by our result is reminiscent of the *full visibility* case considered in [13], and is not likely to hold in practice. In fact, as the number of nodes gets large, one may expect p_n to approach zero given the interference associated with a large number of nodes communicating simultaneously. Second, the condition $\lim_{n\to\infty}(n - 2K_n) = \infty$ will

already follow if $2K_n \leq cn$ for some $c < 1$. Given that $2K_n$ gives the *mean* number of keys stored per sensor in the pairwise scheme [12], this condition will already be dictated in any practical WSN implmentation due to limited memory and computational capability of the sensors. In fact, Di Pietro et al. [4] stated that a feasible key ring size should be on the order of $\log n$.

We now present a simple corollary of Theorem 3.1, that will help us compare our main result with the classical result of Erdős-Rényi graph [6]. A proof is available in [1].

Corollary 3.2: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that $\lim_{n\to\infty}(n - 2K_n) = \infty$ and $\limsup_{n\to\infty} p_n < 1$. With a sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ defined through

$$\begin{aligned} &\frac{p_n K_n}{n-1}\left(1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}\right) \qquad (10)\\ &= \frac{\log n + (k-1)\log\log n + \gamma_n}{n}, \end{aligned}$$

we have

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is } k\text{-connected}\right] \qquad (11)\\ &= \begin{cases} 0 & \text{if } \lim_{n\to\infty} \gamma_n = -\infty, \\ 1 & \text{if } \lim_{n\to\infty} \gamma_n = +\infty. \end{cases} \qquad (12) \end{aligned}$$

The main advantage of Corollary 3.2 is that it presents the zero-one law for k-connectivity under the scaling (10), where the left-hand side is easily comparable with the link probability $p_n\lambda_n(K_n)$ in $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$; from (3) we easily see that

$$\mathbb{P}[i \sim j] = p_n\lambda_n(K_n) = \frac{p_n K_n}{n-1}\left(2 - \frac{K_n}{n-1}\right). \quad (13)$$

IV. Comments and Discussion

A. Comparison with Erdős-Rényi (ER) Graphs

For each p in $(0,1)$ and $n = 2,3,\ldots$, let $\mathbb{G}(n;p)$ denote the ER graph on the vertex set $\{1,\ldots,n\}$ with an edge assigned between any pair of nodes independently with probability p. Although edge assignment events are mutually independent in $\mathbb{G}(n;p)$, they can be shown to be *negatively associated* in $\mathbb{H}(n;K)$ in the sense of Joag-Dev and Proschan [8]; see [1, Section 7.1] and [15] for details. Therefore neither the random K-out graph $\mathbb{H}(n;K)$ nor the intersection model $\mathbb{H} \cap \mathbb{G}(n;\theta)$ can be equated with $\mathbb{G}(n;p)$. This is true even when the parameters p and K are selected so that the edge assignment *probabilities* in these graphs coincide.

However, some similarities do exist between $\mathbb{H} \cap \mathbb{G}(n;\theta)$ and ER graphs. For instance, consider the following well-known zero-one law for k-connectivity in ER graphs [6]: Given any scaling $p : \mathbb{N}_0 \to (0,1)$, define a sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ through

$$p_n = \frac{\log n + (k-1)\log\log n + \gamma_n}{n}. \qquad (14)$$

It holds that

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p_n) \text{ is } k\text{-connected}\right] \\ &= \begin{cases} 0 & \text{if } \lim_{n\to\infty} \gamma_n = -\infty, \\ 1 & \text{if } \lim_{n\to\infty} \gamma_n = +\infty. \end{cases} \qquad (15) \end{aligned}$$

In words, this result indicates that for ER graphs, the threshold of k-connectivity appears when the link probability p_n is compared against $(\log n + (k-1)\log\log n)/n$.

We now compare this result with our main finding by means of Corollary 3.2. Notice that the right-hand sides of the scalings (10) and (14) are exactly the same, and so are the corresponding zero-one laws (12) and (15), respectively. In the case of the ER graph $\mathbb{G}(n;p_n)$, the left-hand side of (14) coincides with the edge probability p_n. In exploring how the left-hand side of (10) is related to the edge probability $p_n\lambda_n(K_n)$ (viz. (13)) of the graph $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$, we recall (3) and use the fact that $\log(1-p_n) < -p_n$ for $p_n > 0$ to get

$$\frac{p_n K_n}{n-1}\left(1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}\right) > p_n\lambda_n(K_n).$$

Hence, our result shows that in $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ the threshold of k-connectivity appears when a quantity that is always larger than the link probability $p_n\lambda_n(K_n)$ is compared against $(\log n + (k-1)\log\log n)/n$. This indicates that $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ tends to exhibit k-connectivity *easier* than ER graphs; i.e., k-connectivity can be ensured by a smaller link probability between nodes (which leads to a smaller average node degree).

The situation is more intricate if $\lim_{n\to\infty} p_n = 0$ (this is possible even $p_n > 0$ for all n; e.g., $p_n = \frac{1}{n}$). There, we have $\log(1-p_n) = -p_n - \frac{{p_n}^2}{2}(1+o(1))$, leading to

$$\begin{aligned} &\frac{p_n K_n}{n-1}\left(1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}\right) \\ &= \frac{p_n K_n}{n-1}\left(2 - \frac{K_n}{n-1} + \frac{p_n}{2}(1+o(1))\right) \\ &= \frac{p_n K_n}{n-1}\left(2 - \frac{K_n}{n-1}\right)\left(1 + \frac{p_n}{2}\cdot\frac{1+o(1)}{2 - \frac{K_n}{n-1}}\right) \\ &= p_n\lambda_n(K_n)(1 + \Theta(p_n)) \qquad (16)\\ &= p_n\lambda_n(K_n)(1 + o(1)), \qquad (17) \end{aligned}$$

where in (16), we used the fact that $1 \leq 2 - \frac{K_n}{n-1} \leq 2$ since $K_n \leq n-1$. This shows that, in the practically relevant case where wireless channels become weaker as n gets large, the threshold for the k-connectivity of

$\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ appears when a quantity that is asymptotically equivalent to the link probability is compared against $(\log n + (k-1)\log\log n)/n$; a situation that is reminiscent of the ER graphs. It is worth mentioning that the dichotomy between the cases $\lim_{n\to\infty} p_n = 0$ and $\lim_{n\to\infty} p_n > 0$ was also observed in [14], [15] for the thresholds of 1-connectivity and absence of isolated nodes in the same model $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$.

It is also important to realize that even under $\lim_{n\to\infty} p_n = 0$, the zero-one laws for the k-connectivity in ER graphs and $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ are *not* exactly analogous. This is because, the $(1+o(1))$ term appearing in (17) may change the limit behavior of the sequence γ_n appearing in (10). In particular, using (16) in (10), we get

$$\begin{aligned}
&\gamma_n \\
&= np_n\lambda_n(K_n)(1+\Theta(p_n)) - \log n - (k-1)\log\log n \\
&= np_n\lambda_n(K_n) - \log n - (k-1)\log\log n \\
&\quad + \Theta(np_n{}^2\lambda_n(K_n)) \\
&= np_n\lambda_n(K_n) - \log n - (k-1)\log\log n + \Theta(K_n p_n{}^2)
\end{aligned}$$

as we note from (3) that $\lambda_n(K_n) = \Theta(K_n/n)$. It is now clear that, even under $\lim_{n\to\infty} p_n = 0$, the two results, (15) under (14) and (12) under (10), may be deemed analogous if and only if the last term $K_n p_n{}^2$ is bounded, i.e., $K_n p_n{}^2 = O(1)$; note that only then this last term is guaranteed to not affect whether $\lim_{n\to\infty} \gamma_n = \pm\infty$. Finally, we conclude that for the two graphs $\mathbb{G}(n;p_n)$ and $\mathbb{H} \cap \mathbb{G}(n;K_n,p_n)$ to exhibit asymptotically the same behavior for the property of k-connectivity, the parameter scalings should satisfy

$$p_n = o(1) \qquad \text{and} \qquad K_n p_n{}^2 = O(1).$$

B. Comparison with results by Yağan and Makowski for $k = 1$

We now compare our results with those by Yağan and Makowski [15] who established zero-one laws for 1-connectivity and for the absence of isolated nodes (i.e., absence of nodes with degree zero) in $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$. Here, we present their result in a slightly different form: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that

$$p_n K_n \left(2 - \frac{K_n}{n-1}\right) \left(\frac{1 - \frac{\log(1-p_n)}{p_n}}{2}\right) \sim c \log n, \tag{18}$$

for some $c > 0$. Assume also that $\lim_{n\to\infty} p_n = p^\star$ exists. Then, we have

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected }\right] \\
&\quad = \begin{cases} 0 & \text{if } \ c < 1 \\ 1 & \text{if } \ c > 1. \end{cases}
\end{aligned} \tag{19}$$

To better compare this result with ours, we set $k = 1$ and rewrite our scaling condition (8) as

$$\begin{aligned}
&p_n K_n \left(2 - \frac{K_n}{n-1}\right) \left(\frac{1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2 - \frac{K_n}{n-1}}\right) \\
&\quad = \log n + \gamma_n
\end{aligned} \tag{20}$$

under which Theorem 3.1 gives

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected }\right] \\
&\quad = \begin{cases} 0 & \text{if } \ \lim\limits_{n\to\infty} \gamma_n = -\infty, \\ 1 & \text{if } \ \lim\limits_{n\to\infty} \gamma_n = +\infty. \end{cases}
\end{aligned} \tag{21}$$

We now explain how our result on 1-connectivity constitutes an improvement on this result of [15]. The assumption that limit $\lim_{n\to\infty} p_n = p^\star$ exists was instrumental in establishing (19) under (18) and our results in this paper explains why. First, it is clear that if $p^\star = 0$, then

$$\begin{aligned}
&\lim_{n\to\infty} \left(\frac{1 - \frac{\log(1-p_n)}{p_n}}{2}\right) = 1 \\
&\quad = \lim_{n\to\infty} \left(\frac{1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2 - \frac{K_n}{n-1}}\right)
\end{aligned} \tag{22}$$

so that the left hand sides of (20) and (18) are asymptotically equivalent. Next, if $p^\star > 0$, then it follows that $K_n = O(\log n)$ (see [15]) under (18). This again yields the asymptotical equivalence of the left hand sides of (20) and (18) under $p^\star > 0$. Therefore, under the assumption that p_n has a limit, a scaling condition that is *equivalent* to (18) is given by

$$p_n K_n \left(2 - \frac{K_n}{n-1}\right) \left(\frac{1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2 - \frac{K_n}{n-1}}\right) \sim c \log n, \tag{23}$$

with the corresponding result (19) unchanged.

Comparing (20)-(21) and (19)-(23), we see that our 1-connectivity result is more fine-grained than the one given in [15]. In particular, the scaling condition (23) enforced in [15] requires a deviation of $(c-1)\log n = \pm\Omega(\log n)$ from the threshold $\log n$ to get the zero-one law (with $c < 1$, or $c > 1$, respectively). On the other hand, in our formulation (20), it suffices to have an unbounded deviation; e.g., even $\gamma_n = \pm \log\log\cdots\log n$ will do. Put differently, we cover the case $c = 1$ that is not covered by the zero-one law (19) under (23). In fact, we show that if $c = 1$ in (23), then $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ could be almost surely connected or almost surely not connected depending on the limit of γ_n defined in (20). Furthermore, Theorem 3.1 indicates that if (23) holds

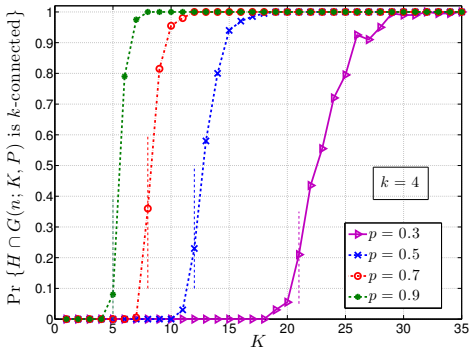

Fig. 1. *Probability that* $\mathbb{H} \cap \mathbb{G}(n; K, p)$ *is* 4*-connected as a function of* K *with* $p = 0.3, 0.5, 0.7, 0.9$ *and* $n = 2000$.

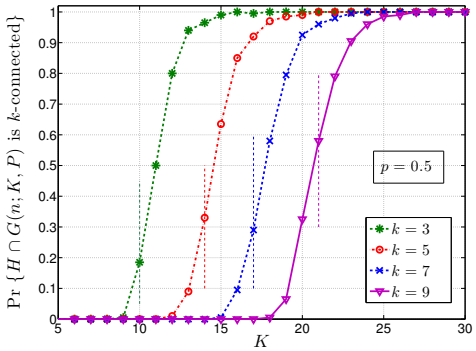

Fig. 2. *Probability that* $\mathbb{H} \cap \mathbb{G}(n; K, p)$ *is* k*-connected as a function of* K *with* $p = 0.5$ *and* $n = 2000$.

with $c > 1$, then $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$ will be not only 1-connected, but also k-connected (almost surely) for all $k = 1, 2, \ldots$.

Collecting, our contributions in this paper improve the results in [15] two directions. First, we extend the results on the 1-connectivity of the model $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$ to k-connectivity with arbitrary $k = 1, 2, \ldots$. As discussed before, the k-connectivity property quantifies the reliability of the network against node or edge removals, and is desirable in a number of applications including wireless sensor networks. Second, with $k = 1$, our main result sharpens and improves the zero-one law for 1-connectivity of $\mathbb{H} \cap \mathbb{G}(n; \theta_n)$. In particular, our result does not require the unnatural condition that limit $\lim_{n\to\infty} p_n$ should exist, and does establish a sharper *phase transition* result with deviation functions of the form $\gamma_n = \pm o(\log n)$ being able to change the phase of the graph from being disconnected to connected.

C. Numerical results

We now present numerical results to check the validity of Theorem 5.1, particularly in the non-asymptotic regime, i.e., when parameter values are set in accordance with real-world wireless sensor network scenarios. In all experiments, we fix the number of nodes at $n = 2000$. Then for a given parameter pair (K, p), we generate 200 independent samples of the graph $\mathbb{H} \cap \mathbb{G}(n; K, p)$ and count the number of times (out of a possible 200) that the obtained graph is k-connected for $k = 1, 2, \ldots$. Dividing the counts by 200, we obtain the (empirical) probabilities for k-connectivity.

For brevity, we display only three figures, namely Figures 1, 2, and 3. Each time, one of the parameters (k, p, K) is fixed at a typical value, another is varied through a wide range, while the third one is set to four different values of interest. In doing so, our goal is to understand the sensitivity of the reliability of the network (as quantified by the probability of k-connectivity) to the variations in the network parameters p and K.

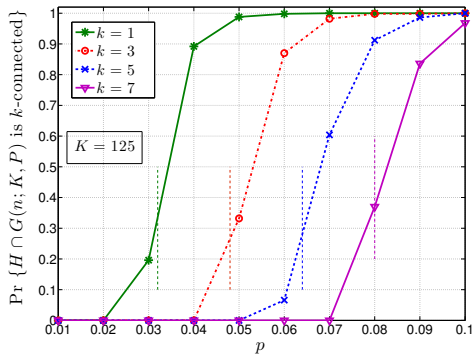

Fig. 3. *Probability that* $\mathbb{H} \cap \mathbb{G}(n; K, p)$ *is* k*-connected as a function of* p *with* $K = 125$ *and* $n = 2000$.

In particular, we want to check whether the observed sensitivity is in parallel with our analytical results given in Theorem 3.1. To that end, in each curve, we include a vertical dashed line that stands for the *critical* value of the varying parameter (i.e., of K in Figures 1 and 2, and of p in Figure 3) that results in a change of sign in the sequence γ_n given via (8). As an example, in Figure 1, vertical dashed lines stand for the minimum integer value of K that satisfies

$$pK\left(1 - \frac{\log(1-p)}{p} - \frac{K}{n-1}\right) > \log n + 3\log\log n. \tag{24}$$

Our main conclusions from the numerical results are twofold. First, we see that the the sharp phase transition behavior suggested by Theorem 3.1 is already observable with $n = 2000$ nodes. Namely, the probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is k-connected transitions from *zero* to *one* as the parameter K (or, p) varies very slightly from a certain value. Second, we see that those critical values match well the vertical dashed lines obtained from Theorem 5.1. This prompts us to conclude that simulation outcomes are in good agreement with the analytical results.

V. Basic Ideas for Proving Theorem 3.1

We give a brief overview of the proof of Theorem 3.1. As mentioned before, all details are given in [1]. The proof of Theorem 3.1 takes advantage of the relationship between minimum node degree and k-connectivity (viz. (6)) in the following way. First, observe from (6) that $[\kappa_v \geq k\,] \subseteq [\,\delta \geq k\,]$. This implies

$$\mathbb{P}\,[\kappa_v \geq k\,] \leq \mathbb{P}\,[\,\delta \geq k\,] \tag{25}$$

and

$$\begin{aligned}\mathbb{P}[\kappa_v \geq k] &= \mathbb{P}[\delta \geq k] - \mathbb{P}[(\kappa_v < k) \cap (\delta \geq k)] \\ &\geq \mathbb{P}[\delta \geq k] - \sum_{\ell=0}^{k-1} \mathbb{P}[(\kappa_v = \ell) \cap (\delta > \ell)].\end{aligned} \tag{26}$$

Let $\kappa_v(n;\theta_n)$ and $\delta(n;\theta_n)$ denote the vertex connectivity and minimum node degree in $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$, respectively. The bounds (25)-(26) pave the way to establishing the zero-one law for k-connectivity (i.e., for the property that $\kappa_v(n;\theta_n) \geq k$) in $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$. Of particular importance will be the following zero-one law for the minimum node degree of $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ established by us in [16].

Theorem 5.1 ([16], [17]): Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that $\lim_{n\to\infty}(n - 2K_n) = \infty$ and $\limsup_{n\to\infty} p_n < 1$. With the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ defined through (8), we have

$$\lim_{n\to\infty} \mathbb{P}\,[\delta(n;\theta_n) \geq k] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \gamma_n = -\infty, \\ 1 & \text{if } \lim_{n\to\infty} \gamma_n = +\infty. \end{cases} \tag{27}$$

It is now clear how to proceed. Pick any scaling $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ as in the statements of Theorems 3.1 and 5.1. If it holds that $\lim_{n\to\infty} \gamma_n = -\infty$, then we get from Theorem 5.1

$$\lim_{n\to\infty} \mathbb{P}\,[\delta(n;\theta_n) \geq k] = 0.$$

From (25), this already establishes the zero-law for k-connectivity, namely that

$$\lim_{n\to\infty} \mathbb{P}\,[\kappa_v(n;\theta_n) \geq k] = 0 \quad \text{if } \lim_{n\to\infty} \gamma_n = -\infty,$$

Hence, we only need to establish the one-law of Theorem 3.1. With $\lim_{n\to\infty} \gamma_n = +\infty$, we have from Theorem 5.1 that

$$\lim_{n\to\infty} \mathbb{P}\,[\delta(n;\theta_n) \geq k] = 1. \tag{28}$$

Reporting this in to (26), we see that the desired one-law

$$\lim_{n\to\infty} \mathbb{P}\,[\kappa_v(n;\theta_n) \geq k] = 1 \quad \text{if } \lim_{n\to\infty} \gamma_n = +\infty$$

will follow if we show that $\lim_{n\to\infty} \gamma_n = +\infty$ implies

$$\lim_{n\to\infty} \mathbb{P}\,[(\kappa_v(n;\theta_n) = \ell) \cap (\delta(n;\theta_n) > \ell)] = 0 \tag{29}$$

for each $\ell = 0, 1, \ldots, k-1$.

The rest of the proof deals with establishing (29), i.e., the fact that almost surely $\mathbb{H} \cap \mathbb{G}(n;\theta_n)$ can not be made disconnected by deleting ℓ vertices when all of its nodes have degree larger than ℓ. This is done by finding a sufficiently tight upper bound on the probability $\mathbb{P}\,[(\kappa_v(n;\theta_n) = \ell) \cap (\delta(n;\theta_n) > \ell)]$ and then showing that it goes to zero as $n \to \infty$. The approach is similar to the one used for proving the one-law for k-connectivity in Erdős-Rényi graphs [2, p. 164].

References

[1] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "A zero-one law for k-connectivity in random K-out graphs intersecting Erdős-Rényi Graphs." Available online at www.ece.cmu.edu/∼oyagan/Journals/ICC15Long.pdf

[2] B. Bollobás, *Random Graphs*, Cambridge University Press, 2001.

[3] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy, 2003.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security*, 2008.

[5] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in ACM CCS, 2002.

[6] P. Erdős and A. Rényi, "On the Strength of Connectedness of Random Graphs," *Acta Math. Acad. Sci. Hungar* **12**, 1961, pp. 261–267.

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

[8] K. Joag-Dev and F. Proschan, "Negative association of random variables, with applications," *The Annals of Statistics* 11 (1983), pp. 266-295

[9] M.D. Penrose, *Random geometric graphs*, Oxford Studies in Probability 5, Oxford University Press, New York (NY), 2003.

[10] O. Yağan, "Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel," *IEEE Transactions on Information Theory*, IT-58 (2012), pp. 3821-3835.

[11] O. Yağan, *Random graph modeling of key distribution schemes in wireless sensor networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, 2011.

[12] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key distribution scheme: Gradual deployment and key ring sizes." *Performance Evaluation*, 70(7-8) (2013).

[13] O. Yağan and A. M. Makowski, "On the connectivity of sensor networks under random pairwise key predistribution," *IEEE Transcations on Information Theory*, IT-59 (2013).

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

[15] O. Yağan and A.M. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *IEEE Transactions on Information Theory*, IT-59 (2013).

[16] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "On secure and reliable communications in wireless sensor networks: Towards k-connectivity under a random pairwise key predistribution scheme," in IEEE International Symposium on Information Theory (ISIT), 2014.

[17] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "Towards k-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links," Available online at `arXiv:1405.5193 [cs.DM]`.

[18] J. Zhao, O. Yağan and V. Gligor, "Secure k-Connectivity in Wireless Sensor Networks under an On/Off Channel Model," in IEEE IEEE International Symposium on Information Theory (ISIT), 2013.