On secure and reliable communications in wireless sensor networks: Towards k-connectivity under a random pairwise key predistribution scheme

Faruk Yavuz
Dept. of ECE and CyLab
Carnegie Mellon University
Moffett Field, CA 94035
Email: fyavuz@andrew.cmu.edu

Jun Zhao
Dept. of ECE and CyLab
Carnegie Mellon University
Pittsburgh, PA 15213
Email: junzhao@cmu.edu

Osman Yağan
Dept. of ECE and CyLab
Carnegie Mellon University
Moffett Field, CA 94035
Email: oyagan@ece.cmu.edu

Virgil Gligor
Dept. of ECE and CyLab
Carnegie Mellon University
Pittsburgh, PA 15213
Email: gligor@cmu.edu

***Abstract*—To be considered for an IEEE Jack Keil Wolf ISIT Student Paper Award. We study the secure and reliable connectivity of wireless sensor networks. Security is assumed to be ensured by the random pairwise key predistribution scheme of Chan, Perrig, and Song, and unreliable wireless links are represented by independent on/off channels. Modeling the network by an intersection of a random K-out graph and an Erdős-Rényi graph, we present scaling conditions (on the number of nodes, the scheme parameter K, and the probability of a wireless channel being on) such that the resulting graph contains no nodes with degree less than k with high probability, when the number of nodes gets large. Results are given in the form of zero-one laws and are shown to improve the previous results by Yağan and Makowski on the absence of isolated nodes (i.e., absence of nodes with degree zero). Via simulations, the established zero-one laws are shown to hold also for the property of k-connectivity; i.e., the property that graph remains connected despite the deletion of any $k-1$ nodes or edges.**

Keywords: Random graphs, Connectivity, Zero-one laws, Wireless sensor networks.

I. Introduction

Wireless sensor networks (WSNs) are distributed collection of small sensor nodes that gather security-sensitive data and control security-critical operations in a wide range of industrial, home and business applications [1]. Many applications require deploying sensor nodes in hostile environments where an adversary can eavesdrop sensor communications, and can even capture a number of sensors and surreptitiously use them to compromise the network. Therefore, cryptographic protection is required to secure the sensor communication as well as to detect sensor capture and to revoke the compromised keys. Given the limited communication and computational resources available at each sensor, security is expected to be a key challenge in WSNs [2], [3], [4].

Random key predistribution is one of the approaches proposed in the literature for addressing security challenges in resource constrained WSNs. The idea of randomly assigning secure keys to the sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor [2]. Following their original work, a large number of key predistribution schemes have been proposed; see the survey articles [4], [5] (and references therein).

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 amongst all other nodes. For each sensor and any sensor paired to it, a unique (pairwise) key is generated and stored in their memory modules along with their ids. Two nodes can then secure an existing wireless communication link if at least one of them is paired to the other so that the two nodes have at least one pairwise key in common. Precise implementation details are given in Section II.

Let $\mathbb{H}(n;K)$ denote the undirected random graph on the vertex set $\{1,\ldots,n\}$ where distinct nodes i and j are adjacent if they have a pairwise key in common as described earlier; this random graph models the random pairwise predistribution scheme under *full visibility* (whereby all nodes have a wireless link in between). The random graph $\mathbb{H}(n;K)$ is known in the literature on random graphs as the random K-out graph [6], [7], [8]; several properties of this graph have been recently analyzed by Yağan and Makowski [9], [10], [11], [12].

Recently, there has been a significant interest [13], [14], [15], [16], [17] to drop the full visibility assumption and to model and analyze random key predistribution schemes under more realistic situations that account for the possibility that communication links between nodes may not be available – This could occur due to the presence of physical barriers between nodes or because of harsh environmental conditions severely impairing transmission. With this in mind, several authors [14], [15], [16], [17] have started with a simple communication model where wireless links are represented by independent channels that are either on (with probability p) or off (with probability $1-p$). This suggests an overall modeling framework that is constructed by *intersecting* the random K-out graph $\mathbb{H}(n;K)$, with an Erdős-Rényi (ER) graph model $\mathbb{G}(n;p)$ [6].

In this paper, we initiate an analysis towards the k-connectivity for the resulting intersection graph $\mathbb{H} \cap \mathbb{G}(n; K, p)$. A network (or graph) is said to be k-connected if its connectivity is preserved despite the failure of any $(k-1)$ nodes or links [18]. Therefore, the property of k-connectivity provides a guarantee of network reliability against the possible failures of sensors or links due to adversarial attacks or battery depletion; a much needed property given the key application areas of sensor networks such as health monitoring, battlefield surveillance, and environmental monitoring. Finally, k-connectivity has important benefits in *mobile* wireless sensor networks. For instance, if a network is known to be k-connected, then any $k-1$ nodes in the network are free to move anywhere in the network while the rest of the network remains at least 1-connected.

Our main result is a zero-one law for the property that the minimum node degree of $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is at least k. Namely, we present scaling conditions on the parameters p and K with respect to n, such that the resulting graph contains no nodes with degree less than k with probability approaching to zero, or one, respectively, as the number of nodes n gets large. The established results already imply the zero-law for the k-connectivity, since a graph can not be k-connected unless all nodes have degree at least k. Further, in most (if not all) random graph models in the literature, including ER graphs, random geometric graphs [18], and random key graphs [17], the conditions that ensure k-connectivity coincide with those ensuring minimum node degree to be at least k. This is often established by showing the improbability of a graph being *not* k-connected when all nodes have at least k neighbors. Here, we demonstrate this phenomenon via simulations which indicate that our zero-one laws hold also for the property of k-connectivity. Finally, our results constitute an improvement of the previous results by Yağan and Makowski [19], [14] on the absence of isolated nodes (i.e., absence of nodes with degree zero) in $\mathbb{H} \cap \mathbb{G}(n; K, p)$.

A word on the notation: All statements involving limits are understood with n going to infinity. In comparing the asymptotic behaviors of the sequences $\{a_n\}, \{b_n\}$, we use $a_n = o(b_n)$, $a_n = O(b_n)$, $a_n = \Omega(b_n)$, and $a_n = \Theta(b_n)$, with their meaning in the standard Landau notation.

II. Model

A. The random pairwise key predistribution scheme

We parametrize the pairwise key distribution 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 $\mathcal{N} = \{1, \ldots n\}$ 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 $\mathcal{N}_{-i}$ – We say that each of the nodes in $\Gamma_{n,i}(K)$ is paired to node i. Thus, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

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

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

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 in [12], [10], [14]. In a nutshell, 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 $j \in \Gamma_{n,i}(K)$ take place. In this case node i and j can secure an existing wireless communication link available to 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 they have at least one key in common in their key rings, namely

$$i \sim_K j \quad \text{iff} \quad \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset. \tag{1}$$

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (1); this corresponds to modeling the pairwise distribution scheme under full visibility. We have $\mathbb{P}[i \sim_K j] = \lambda_n(K)$ where $\lambda_n(K)$ is the link assignment probability in $\mathbb{H}(n; K)$ given by (see [10], [12])

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

The random graph $\mathbb{H}(n; K)$ is known in the literature on random graphs as the random K-out graph [6], [7], [8]: 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.

C. Intersection of random 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 i.i.d. $\{0, 1\}$-valued rvs with success probability p. The channel between nodes i and j is available (resp. up) with probability p and unavailable (resp. down) with the complementary 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 $\{1, \ldots, n\}$ [6]. Obviously, $\mathbb{P}[i \sim_B j] = p$.

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 they are both K-adjacent and B-adjacent, namely

$$i \sim j \quad \text{iff} \quad \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset \text{ and } B_{ij}(p) = 1. \tag{3}$$

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 rvs $\{\Gamma_{n,1}(K),\ldots,\Gamma_{n,n}(K)\}$ and $\{B_{ij}(p), 1\le i<j\le n\}$ to be independent, in which case the edge occurrence probability in $\mathbb{H}\cap\mathbb{G}(n;K,p)$ is given by

$$\mathbb{P}\left[i\sim j\right]=\mathbb{P}\left[i\sim_K j\right]\mathbb{P}\left[i\sim_B j\right]=p\lambda_n(K). \tag{4}$$

III. Main Result

Our main technical result is given next. To fix the terminology, 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 conditions $K_n<n$ for each $n=1,2,\ldots$. Similarly, we let any mapping $p:\mathbb{N}_0\to[0,1]$ define a scaling for Erdős-Rényi graphs. To lighten the notation 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 the sequence $\gamma:\mathbb{N}_0\to\mathbb{R}$ defined through

$$\begin{aligned} p_nK_n\left(1-\frac{\log(1-p_n)}{p_n}-\frac{K_n}{n-1}\right) \\ =\ \log n+(k-1)\log\log n+\gamma_n, \end{aligned} \tag{5}$$

we have

$$\lim_{n\to\infty}\mathbb{P}\left[\begin{array}{c}\textit{Min node degree of}\\ \mathbb{H}\cap\mathbb{G}(n;\theta_n)\ \textit{is no less than } k\end{array}\right] \tag{6}$$

$$=\begin{cases}0 & \textit{if}\ \lim_{n\to\infty}\gamma_n=-\infty\\ 1 & \textit{if}\ \lim_{n\to\infty}\gamma_n=+\infty.\end{cases} \tag{7}$$

The proof of Theorem 3.1 passes through the method of first and second moments [8], applied to the random variable counting the number of nodes with degree ℓ, with $\ell=0,1,\ldots,k-1$. Although this technique is standard in the literature, its application to the intersection graph $\mathbb{H}\cap\mathbb{G}(n;\theta)$ is far from being straightforward due to intricate dependencies amongst the degrees of nodes. Due to space limitations, we refer the reader to [20] for a proof of Theorem 3.1.

The extra conditions enforced by Theorem 3.1 are required for technical reasons; i.e., for the method of moments to be applied successfully to the aforementioned count variables. However, we remark that these conditions are mild and do no preclude their application in realistic WSN scenarios. 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 $\limsup_{n\to\infty}p_n=1$ is reminiscent of the *full visibility* case considered in [12], and is not likely to hold in practice. In fact, as the number of nodes gets large, it may be expected that p_n goes to zero due to 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 $2K_n\le cn$ for some $c<1$. Given that $2K_n$ is equal to the mean number of keys stored per sensor in the pairwise scheme [11], this condition needs to hold in any practical WSN scenario due to limited memory and computational capability of the sensors. In fact, Di Pietro et al. [21] noted that key ring sizes on the order of $\log n$ are feasible for WSNs.

IV. Comments and Discussion

A. Comparison with Erdős-Rényi Graphs

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. It is known that edge assignments are mutually independent in $\mathbb{G}(n;p)$, whereas they are strongly correlated in $\mathbb{H}(n;K)$ in that they are *negatively associated* in the sense of Joag-Dev and Proschan [22]; see [14] for details. 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 $\lambda(n;K)=p$. Therefore, $\mathbb{H}\cap\mathbb{G}(n;\theta)$ cannot be equated with an ER graph either, and the results obtained here are *not* mere consequences of classical results for ER graphs.

However, some similarities do exist between $\mathbb{H}\cap\mathbb{G}(n;\theta)$ and ER graphs. We start by presenting the following well-known zero-one law for k-connectivity in ER graphs [23]: For any scaling $p:\mathbb{N}_0\to[0,1]$ satisfying

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

for some $\gamma:\mathbb{N}_0\to\mathbb{R}$, it holds that

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

The same result also holds for the property that minimum node degree is at least k. On the other hand, the condition (5) can be rephrased as

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

with the result (7) unchanged. Since $\log(1-p_n)\le-p_n$, we get from (2) that

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

Hence, in ER graphs the threshold of k-connectivity, and of minimum node degree being at least k, appears when the link probability is compared against $(\log n+(k-1)\log\log n)/n$. In $\mathbb{H}\cap\mathbb{G}(n;\theta)$, our result shows that the threshold 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 $\mathbb{H}\cap\mathbb{G}(n;\theta)$ tends to exhibit the property that all nodes have at least k neighbors *easier* than ER graphs;

i.e., this property can be ensured by a smaller link probability between nodes (which leads to smaller average node degree).

The situation is more intricate if it holds that $\lim_{n\to\infty} p_n = 0$, whence we have

$$\log(1-p_n) = -p_n - \frac{p_n^2}{2}(1+o(1)).$$

This leads

$$\frac{p_n K_n}{n-1}\left(1 - \frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}\right) = p_n\lambda_n(K_n)(1+o(1)) \tag{9}$$

The $o(1)$ term in this last expression can be written more precisely as $\Theta(p_n)$. Thus, in the practically relevant case when the wireless channels become weaker as n gets large, the threshold for minimum node degree of $\mathbb{H}\cap\mathbb{G}(n;\theta)$ to be at least k appears when a quantity that is asymptotically equivalent to link probability is compared against $(\log n + (k-1)\log\log n)/n$; a situation that is reminiscent of the ER graphs. A similar observation was made in [14] for the threshold of 1-connectivity and absence of isolated nodes.

Nevertheless, it is worth mentioning that even under $\lim_{n\to\infty} p_n = 0$, the zero-one laws for the minimum node degree being at least k in ER graphs and $\mathbb{H}\cap\mathbb{G}(n;\theta)$ are *not* exactly analogous. This is because, the term $o(1)$ in (9) may change the behavior of the sequence γ_n appearing in (8) since γ_n will be given by

$$\gamma_n = np_n\lambda_n(K_n)(1+o(1)) - \log n - (k-1)\log\log n.$$

Replacing $o(1)$ with the more precise term $\Theta(p_n)$, and noting that that $\lambda_n(K_n) = \Theta(K_n/n)$, we conclude that the two results will be exactly analogous if and only if $K_n p_n^2$ is bounded; i.e., it does not approach to infinity as n gets large.

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

We now compare our results with those by Yağan and Makowski [14] who established zero-one laws for 1-connectivity, and for the absence of isolated nodes (i.e., nodes with degree zero) in $\mathbb{H}\cap\mathbb{G}(n;\theta)$. 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

$$p_n K_n\left(2 - \frac{K_n}{n-1}\right)\left(\frac{1-\frac{\log(1-p_n)}{p_n}}{2}\right) \sim c\log n, \tag{10}$$

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

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}\cap\mathbb{G}(n;\theta_n) \text{ contains no isolated nodes}\right] \\
&= \lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}\cap\mathbb{G}(n;\theta_n) \text{ is connected}\right] \\
&= \begin{cases} 0 & \text{if } c<1 \\ 1 & \text{if } c>1. \end{cases}
\end{aligned} \tag{11}$$

To better compare this result with ours, we set $k=1$ and rewrite our scaling condition (5) as

$$p_n K_n\left(2 - \frac{K_n}{n-1}\right)\left(\frac{1-\frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2-\frac{K_n}{n-1}}\right) = \log n + \gamma_n \tag{12}$$

under which Theorem 3.1 gives

$$\lim_{n\to\infty}\mathbb{P}\left[\begin{array}{c}\mathbb{H}\cap\mathbb{G}(n;\theta_n)\\ \text{has no isolated nodes}\end{array}\right] = \begin{cases} 0 & \text{if } \gamma_n\to-\infty \\ 1 & \text{if } \gamma_n\to+\infty. \end{cases}$$

We now argue how our result on absence of isolated nodes constitutes an improvement on the result of [14]. The assumption that limit $\lim_{n\to\infty} p_n = p^\star$ exists was the key in establishing (11) under (10) and our results in this paper explains why. First, it is clear that if $p^\star = 0$, then

$$\lim_{n\to\infty}\left(\frac{1-\frac{\log(1-p_n)}{p_n}}{2}\right) = 1 = \lim_{n\to\infty}\left(\frac{1-\frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2-\frac{K_n}{n-1}}\right)$$

so that the left hand sides of (12) and (10) are asymptotically equivalent. Next, if $p^\star>0$, then it follows that $K_n = O(\log n)$ (see [14]) under (10). This again yields the asymptotical equivalence of the left hand sides of (12) and (10). Therefore, under the assumption that p_n has a limit, a scaling condition that is *equivalent* to (10) is given by

$$p_n K_n\left(2 - \frac{K_n}{n-1}\right)\left(\frac{1-\frac{\log(1-p_n)}{p_n} - \frac{K_n}{n-1}}{2-\frac{K_n}{n-1}}\right) \sim c\log n, \tag{13}$$

with the results (11) unchanged.

Comparing (12) with (13), we see that our absence of isolated nodes result is more fine-grained than the one given in [14]. In a nutshell, the scaling condition (13) enforced in [14] requires a deviation of $\gamma_n = \pm\Omega(\log n)$ (from the threshold $\log n$) to get the zero-one law, whereas in our formulation (12), 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 of $c=1$ in (11) under (13) and show that $\mathbb{H}\cap\mathbb{G}(n;\theta_n)$ could be almost surely free of or not free of isolated nodes, depending on the limit of γ_n; in fact, if (13) holds with $c>1$, we see from Theorem 3.1 that $\mathbb{H}\cap\mathbb{G}(n;\theta_n)$ is not only free of isolated nodes but also all of its nodes will have degree larger than k for all $k=1,2,\ldots$.

C. Numerical results and a conjecture

We now present some numerical results to check the validity of Theorem 3.1, 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 graphs have minimum node degree no less than k and ii) are k-connected, for $k=1,2,\ldots$. Dividing the counts by 200, we obtain the (empirical) probabilities for the events of interest.

Due to space limitations, we only provide a small subset of the numerical results we have obtained; see [20] for a complete discussion. In Figure 1, we depict the resulting empirical probability that each node in $\mathbb{H}\cap\mathbb{G}(n;K,p)$ has degree at least 2 as a function of K for various p values. For each p value, we also show the critical threshold of having minimum degree at least 2 asserted by Theorem 3.1 (viz. (5)) by a

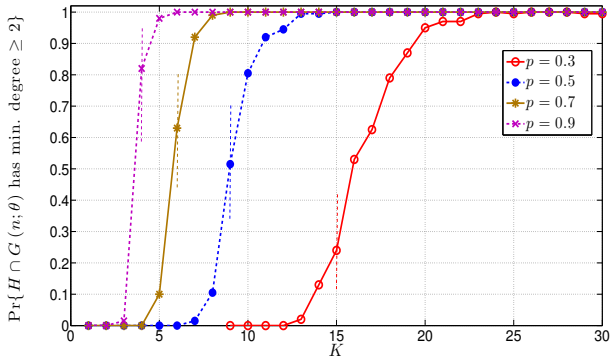

Fig. 1. *Probability that all nodes in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ have degree at least 2 as a function of K for $p = 0.3$, $p = 0.5$, $p = 0.7$, and $p = 0.9$ with $n = 2000$.*

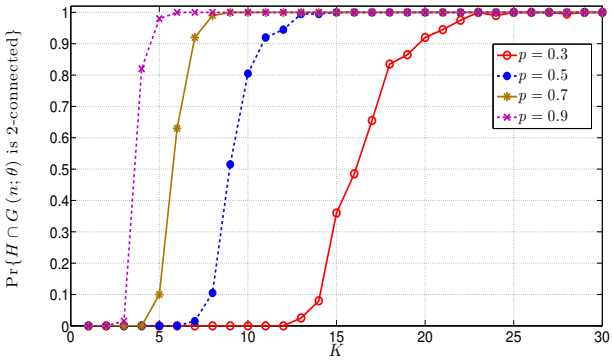

Fig. 2. *Probability that all nodes in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is 2-connected as a function of K for $p = 0.3$, $p = 0.5$, $p = 0.7$, and $p = 0.9$ with $n = 2000$. Its resemblance with Figure 2 suggests that an analog of Theorem 3.1 holds also for the property of k-connectivity.*

vertical dashed line. Namely, the vertical dashed lines stand for the minimum integer value of K that satisfies

$$pK\left(1 - \frac{\log(1-p)}{p} - \frac{K}{n-1}\right) > \log n + \log\log n \quad (14)$$

Even with $n = 2000$, we can observe the threshold behavior suggested by Theorem 3.1; i.e., the probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ has minimum node degree at least k transitions from *zero* to *one* as K varies very slightly from a certain value. For larger n, we would expect the curves to look more like a *shifted unit step* function with a jump discontinuity (i.e., a threshold) at around the K value that gives $\mathbb{P}[\text{min node degree is at least k}] = \frac{1}{2}$ in the current plots. Those K values match well the vertical dashed lines suggested by Theorem 3.1, leading to the conclusion that numerical experiments are in good agreement with our theoretical results.

Figure 2 is obtained in the same way with Figure 1, this time for the probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is 2-connected. It is clear that two figures show a strong similarity with curves corresponding to each p value being almost indistinguishable. In fact, we ran numerous experiments with different parameter pairs, and each time observed that the empirical probabilities of $\mathbb{H} \cap \mathbb{G}(n; K, p)$ being k-connected and having minimum node degree at least k are almost equal. This suggests that in $\mathbb{H} \cap \mathbb{G}(n; K, p)$ as well, the properties of k-connectivity and the minimum node degree being at least k are asymptotically equivalent, leading us to cast the following conjecture.

Conjecture 4.1: 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 $\limsup_{n\to\infty} p_n < 1$, and a sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ defined through (5). Then,

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

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, 2002.

[2] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of ACM CCS*, 2002.

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

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

[5] Y. Xiao and V. K. Rayi and B. Sun and X. Du and F. Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, pp. 2314 – 2341, 2007.

[6] B. Bollobás, *Random graphs*. Cambridge university press, 2001.

[7] T. I. Fenner and A. M. Frieze, "On the connectivity of random m-orientable graphs and digraphs," *Combinatorica*, vol. 2, no. 4, 1982.

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

[9] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key distribution schemes," in *Proc. of WiOpt*, 2011.

[10] ——, "Connectivity results for sensor networks under a random pairwise key predistribution scheme," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, 2012, pp. 1797–1801.

[11] ——, "On the scalability of the random pairwise key predistribution scheme: Gradual deployment and key ring sizes," *Performance Evaluation*, vol. 70, no. 78, pp. 493 – 512, 2013.

[12] ——, "On the connectivity of sensor networks under random pairwise key predistribution," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5754–5762, 2013.

[13] B. Krishnan, A. Ganesh, and D. Manjunath, "On connectivity thresholds in superposition of random key graphs on random geometric graphs," in *Proc. of IEEE ISIT*, 2013, pp. 2389–2393.

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

[15] O. Yağan, "Performance of the Eschenauer-Gligor key distribution scheme under an on/off channel," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3821–3835, June 2012.

[16] J. Zhao, O. Yağan, and V. Gligor, "Secure k-connectivity in wireless sensor networks under an on/off channel model," in *Proc. of IEEE Intl. Symp. Info. Theory (ISIT)*, 2013, pp. 2790–2794.

[17] ——, "k-connectivity in secure wireless sensor networks with physical link constraints - the on/off channel model," *Arxiv*, June 2012, submitted to *IEEE Transactions on Information Theory*. Available online at `arXiv:1206.1531 [cs.IT]`.

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

[19] O. Yağan and A. M. Makowski, "Designing securely connected wireless sensor networks in the presence of unreliable links," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1–5.

[20] F. Yavuz, J. Zhao, O. Yağan, and V. Gligor, "On the k-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links," to be submitted. [Online]. Available: http://users.ece.cmu.edu/~oyagan/Journals/k_con_PER.pdf

[21] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 3, pp. 13:1–13:22, March 2008.

[22] K. Joag-Dev and F. Proschan, "Negative association of random variables with applications," *The Annals of Statistics*, no. 1, pp. 286–295, 1983.

[23] P. Erdős and A. Rényi, "On the strength of connectedness of random graphs," *Acta Math. Acad. Sci. Hungar*, pp. 261–267, 1961.