Designing securely connected wireless sensor networks in the presence of unreliable links

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

***Abstract*— We investigate the secure connectivity of wireless sensor networks under the pairwise key distribution scheme of Chan et al.. Unlike recent work which was carried out under the assumption of *full visibility*, here we assume a (simplified) communication model where unreliable wireless links are represented as on/off channels. We present conditions on how to scale the model parameters so that the network i) has no isolated secure node and ii) is securely connected, both with high probability when the number of sensor nodes becomes large. The results are given in the form of *zero-one laws*, and exhibit significant differences with corresponding results in the full visibility case.**

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

I. Introduction

It is envisioned that security will constitute a key challenge for wireless sensor networks (WSNs) deployed in hostile environments. Unfortunately, many security schemes developed for general network environments do not take into account the unique features of WSNs: Public key cryptography is not computationally feasible because of the severe limitations imposed on the physical memory and power consumption of the individual sensors. Traditional key exchange and distribution protocols are based on thrusting third parties, and this makes them inadequate for large-scale WSNs whose topologies are unknown prior to deployment. We refer the reader to [5], [8], [13] for discussions of the security challenges in WSN settings.

Random key predistribution schemes were introduced to address some of these difficulties. The idea of randomly assigning secure keys to sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor [8]. Since then, many competing alternatives to the Eschenauer and Gligor (EG) scheme have been proposed; see [5] for a detailed survey of various key distribution schemes for WSNs. With so many schemes available, a basic question arises as to how they compare with each other. Answering this question passes through a good understanding of the properties and performance of the schemes under consideration, and this can be achieved in a number of ways. The approach used here focuses on random graph models naturally induced by a scheme, and develops the scaling laws corresponding to desirable network properties, e.g., absence of secure nodes which are isolated, secure connectivity, etc. We do so with an eye towards deriving guidelines to *dimension* the given scheme, namely help adjust its parameters so that these properties occur with high probability as the number of nodes becomes large.

To date, most of the efforts along these lines have been carried out under the assumption of *full visibility* according to which sensor nodes are all within communication range of each other; more on this later: Under this assumption, the EG scheme gives rise to a class of random graphs known as random key graphs; relevant results can be found in the references [2], [7], [8], [12], [14]. A simple variation of the EG scheme, the so-called q-composite scheme [6], was also investigated by Bloznelis et al. [3] through an appropriate extension of the random key graph model. Recently Yağan and Makowski have analyzed the random graph induced by the random pairwise key predistribution scheme of Chan et al. [6]; a number of its properties were discussed in the conference papers [15], [16].

To be sure, the full visibility assumption does away with the wireless nature of the communication medium supporting WSNs. In return, this simplification makes it possible to focus on how randomization of the key distribution mechanism alone affects the establishment of a secure network in the best of circumstances. However, a common criticism of this line of work is that by disregarding the unreliability of the wireless links, the resulting dimensioning guidelines are likely to be too *optimistic* – Indeed, in practice nodes may turn up to have fewer neighbors (since some of the communication links are impaired some of the time) and the desired connectivity properties may *not* be achieved if dimensioning were to be done according to the results derived under full visibility.

In this paper, in an attempt to go beyond full visibility, we revisit the pairwise key predistribution scheme of Chan et al. [6] under more realistic assumptions 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. To study such situations, we assume a simple communication model where

communication channels are either on or off, independently from one another. The overall system model is then formed by *intersecting* the random graph model of the pairwise key distribution scheme (under full visibility), and an Erdős-Rényi (ER) graph model [4]. For this new random graph structure, we establish zero-one laws for two basic (and related) graph properties, namely graph connectivity and the absence of isolated nodes, once the model parameters are scaled with the number of users. We identify the critical thresholds and show that they coincide. Furthermore, via simulations, we show that the established zero-one laws apply also under a more realistic channel model, i.e., the disk model [9].

The paper is organized as follows: In Section II, we give precise definitions and implementation details of the pairwise scheme of Chan et al. while Section III is devoted to describing the model of interest. The main results of the paper are given in Section IV. Due to space limitations, we omit the proofs here but all the details can be found in [17]. In Section V we close with an extensive discussion of the main results. Among other things, we compare them with well-known zero-one laws for ER graphs and comment on the suitability of ER graphs as proxies of the model studied here.

II. Implementing pairwise key distribution schemes

Interest in the random pairwise key predistribution scheme of Chan et al. [6] stems from the following advantages over the 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.

As in the conference papers [15], [16], we parametrize the random pairwise key predistribution scheme of Chan et al. by two positive integers n and K such that $K < n$. There are n nodes which are labelled $i = 1, \ldots, n$. with unique ids $\mathrm{Id}_1, \ldots, \mathrm{Id}_n$. Write $\mathcal{N} := \{1, \ldots n\}$ and set $\mathcal{N}_{-i} := \mathcal{N} - \{i\}$ for each $i = 1, \ldots, n$. With node i we associate a subset $\Gamma_{n,i}$ of nodes selected at *random* from $\mathcal{N}_{-i}$ – We say that each of the nodes in $\Gamma_{n,i}$ is paired to node i. Thus, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

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

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

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

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

Once this *offline* random pairing has been created, we construct the key rings $\Sigma_{n,1}, \ldots, \Sigma_{n,n}$, one for each node, as follows: Assumed available is a collection of nK distinct cryptographic keys $\{\omega_{i|\ell},\ i = 1, \ldots, n;\ \ell = 1, \ldots, K\}$. Fix $i = 1, \ldots, n$ and let $\ell_{n,i} : \Gamma_{n,i} \to \{1, \ldots, K\}$ denote a labeling of $\Gamma_{n,i}$. For each node j in $\Gamma_{n,i}$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}$ is realized as $\{j_1, \ldots, j_K\}$ with $1 \leq j_1 < \ldots < j_K \leq n$, then an obvious labeling consists in $\ell_{n,i}(j_k) = k$ for each $k = 1, \ldots, K$ with key $\omega_{i|k}$ associated with node j_k. Of course other labeling are possible, e.g., according to decreasing labels or according to a random permutation. 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. The key $\omega^{\star}_{n,ij}$ is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise distribution scheme. The key ring $\Sigma_{n,i}$ of node i is the set

$$\Sigma_{n,i} := \{\omega^{\star}_{n,ij},\ j \in \Gamma_{n,i}\} \cup \{\omega^{\star}_{n,ji},\ i \in \Gamma_{n,j}\}.$$

If two nodes, say i and j, are within communication range of each other, they can establish a secure link if at least one of the events $i \in \Gamma_{n,j}$ or $j \in \Gamma_{n,j}$ is taking place– Both events can take place, in which case the memory modules of node i and j both contain the distinct keys $\omega^{\star}_{n,ij}$ and $\omega^{\star}_{n,ji}$. Finally, it is plain by construction that this scheme supports node-to-node authentication without involving a base station.

III. The model

Under full visibility, this pairwise distribution 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

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

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 modelling the pairwise distribution scheme under full visibility. We have

$$\mathbb{P}\left[i \sim_K j\right] = \lambda_n(K)$$

where $\lambda_n(K)$ is the link assignment probability in $\mathbb{H}(n; K)$ given by

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

As mentioned earlier, in this paper we seek to account for the possibility that communication links between nodes may not be available. To study such situations, we assume a 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 $B_{ij}(p) = 1$. The notion of B-adjacency defines

the standard ER graph $\mathbb{G}(n;p)$ on the vertex set $\{1,\ldots,n\}$. Obviously,

$$\mathbb{P}\left[i \sim j\right]_B = p.$$

Although this communication model may be deemed simplistic, it does permit a complete analysis of the issues of interest, thereby already pointing out the impact that the communication model may have on the dimensioning guidelines for the pairwise distribution algorithm and forcing a reevaluation of the ones developed under the full visibility assumption.

The random graph model studied here is obtained by *intersecting* the random pairwise graph $\mathbb{H}(n;K)$ with the ER graph $\mathbb{G}(n;p)$. More precisely, the 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

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

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

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

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

IV. Main results

Next we present the main results concerning the random graph model introduced in Section III. Due to space limitations the proofs are omitted; see [17] for all details. To fix the terminology, we refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* (for random pairwise graphs) provided it satisfies the natural conditions

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

Similarly, any mapping $p : \mathbb{N}_0 \to (0,1)$ defines a scaling for ER graphs.

To lighten the notation we often group the parameters K and p into the ordered pair $\theta \equiv (K,p)$. Hence, a mapping $\theta : \mathbb{N}_0 \to \mathbb{N}_0 \times (0,1)$ defines a scaling for the intersection graph $\mathbb{H} \cap \mathbb{G}(n;\theta)$ provided the condition (2) holds on the first component mapping.

The results will be expressed in terms of the threshold function $\tau : [0,1] \to [0,1]$ defined by

$$\tau(p) = \begin{cases} 1 & \text{if } \ p = 0 \\ \frac{2}{1-\frac{\log(1-p)}{p}} & \text{if } \ 0 < p < 1 \\ 0 & \text{if } \ p = 1. \end{cases} \tag{3}$$

With this notation, the main results discussed in [17] can be summarized as follows:

Theorem 4.1: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that

$$p_n \left(2K_n - \frac{K_n^2}{n-1}\right) \sim c \, \log n, \quad n = 1,2,\ldots \tag{4}$$

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

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ contains no isolated nodes}\right] \\ &= \lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected}\right] \\ &= \begin{cases} 0 & \text{if } \ c < \tau(p^\star) \\ 1 & \text{if } \ c > \tau(p^\star) \end{cases} \end{aligned} \tag{5}$$

with the threshold $\tau(p^\star)$ specified in (3).

A case of particular interest arises when $p^\star > 0$ since requiring (4) now amounts to

$$\left(2K_n - \frac{K_n^2}{n-1}\right) \sim \ \frac{c}{p^\star} \log n \tag{6}$$

for some $c > 0$. Any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ which behaves like (6) must necessarily satisfy $K_n = o(n)$, and it is easy to see that requiring (4) is equivalent to

$$K_n \sim \ t \log n \tag{7}$$

for some $t > 0$ with c and t related by $t = \frac{c}{2p^\star}$. With this reparametrization, Theorem 4.1 takes a simpler form:

Theorem 4.2: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to (0,1)$ such that $\lim_{n\to\infty} p_n = p^\star > 0$. Under the condition (7) for some $t > 0$, we have

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ contains no isolated nodes}\right] \\ &= \lim_{n\to\infty} \mathbb{P}\left[\mathbb{H} \cap \mathbb{G}(n;\theta_n) \text{ is connected}\right] \\ &= \begin{cases} 0 & \text{if } \ t < \widehat{\tau}(p^\star) \\ 1 & \text{if } \ t > \widehat{\tau}(p^\star) \end{cases} \end{aligned} \tag{8}$$

where we have set

$$\widehat{\tau}(p) := \frac{\tau(p)}{2p} = \frac{1}{p - \log(1-p)}, \quad 0 < p \leq 1. \tag{9}$$

This alternate formulation is particularly relevant for the case $p_n = p^\star \in (0,1)$ for all $n = 1,2,\ldots$, which captures situations when channel conditions are not affected by the number of users. Such simplifications do not occur in the more realistic case $p^\star = 0$ which corresponds to the situation where channel conditions are indeed influenced by the number of users in the system – The more users in the network, the more likely they will experience interferences from other users.

We now present numerical results that verify (8). In all the simulations, we fix the number of nodes at $n = 200$. We consider the channel parameters $p = 0.2$, $p = 0.4$, $p = 0.6$, $p = 0.8$, and $p = 1$ (the full visibility case), while varying the pairwise scheme parameter K from 1 to 25. For each parameter pair (K,p), we generate 500 independent samples of the graph $\mathbb{H} \cap \mathbb{G}(n;K,p)$ and count the number of times (out of a possible 500) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 500, we obtain the (empirical) probabilities for the events of interest. The results for connectivity are depicted in Figure 1, where

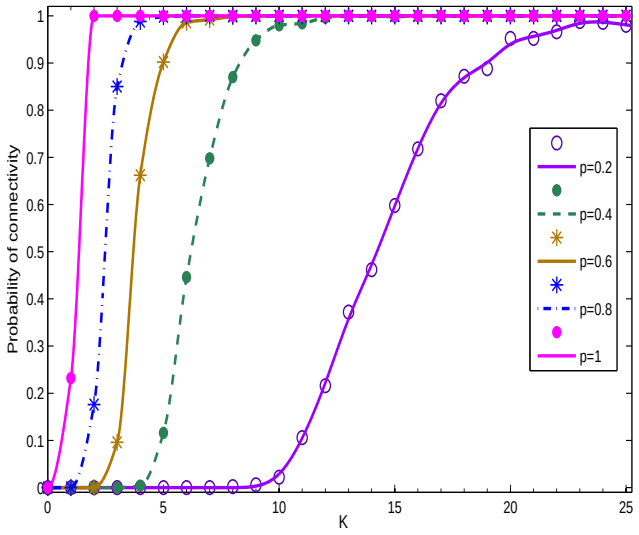

Fig. 1. Probability that $\mathbb{H} \cap \mathbb{G}(n; K, p)$ is connected with respect to K for various p values with $n = 200$. The figure clearly verifies Theorem 4.2.

the curve fitting tool of MATLAB is used. It is easy to check that for each value of $p \neq 1$, the threshold of connectivity matches what is prescribed by (8), namely $K = \widehat{\tau}(p) \log n$. It is also seen that, if the channel is poor, i.e., if p is close to zero, then the required K value to ensure connectivity can be much larger than that of the full visibility case $p = 1$. Due to space limitations, we do not depict the results regarding the property of node isolation; see [17]. However, the results indicate that the difference between the estimated probabilities of graph connectivity and absence of isolated nodes is quite small, in agreement with (8).

V. Discussion and Comments

A. Comparing with the full-visibility case

At this point the reader may wonder as to what form would Theorem 4.1 take in the context of full visibility– In the setting developed here this corresponds to $p = 1$ (see the curve for $p = 1$ in Figure 1) so that $\mathbb{H} \cap \mathbb{G}(n; \theta)$ coincides with $\mathbb{H}(n; K)$. Relevant results were obtained recently by the authors in [15].

Theorem 5.1: For any K a positive integer, it holds that

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

The case where the parameter K is scaled with n is now an easy corollary of Theorem 5.1.

Corollary 5.2: For any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n \geq 2$ for all n sufficiently large, we have the one-law

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; K_n) \text{ is connected}\right] = 1.$$

Each node in $\mathbb{H}(n; K)$ has degree at least K, so that no node is ever isolated in $\mathbb{H}(n; K)$. This is in sharp contrast with the model studied here, as reflected by the full zero-one law for node isolation in Theorem 4.1.

Theorem 5.1 and its Corollary 5.2 together show that very small values of K suffice to ensure asymptotically almost sure (a.a.s.) connectivity of the random graph $\mathbb{H}(n; K)$. However, we stress that these two results cannot be recovered from Theorem 4.1 whose zero-one laws are derived under the assumption $p_n < 1$ for all $n = 1, 2, \ldots$. To further confuse matters, even if the scaling $p : \mathbb{N}_0 \to (0, 1)$ were to satisfy $\lim_{n\to\infty} p_n = 1$, only the one-laws in Theorem 4.1 remain since $\tau(p^\star) = 0$ (and $\widehat{\tau}(p^\star) = 0$) at $p^\star = 1$. Although this might be expected given the absence of isolated nodes in $\mathbb{H}(n; K)$, the one-laws for both the absence of isolated nodes and graph connectivity in $\mathbb{H} \cap \mathbb{G}(n; \theta)$ still require conditions on the behavior of the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$, namely (7).

B. Comparing $\mathbb{H} \cap \mathbb{G}(n; \theta)$ with ER graphs

In the original paper of Chan et al. [6] (as in the reference [10]), the connectivity analysis of the pairwise scheme was based on ER graphs [4] – It was assumed that the random graph induced by the pairwise scheme under a communication model (taken mostly as the disk model [9]) behaves *like* an ER graph. This was done without any analytical justification. Later, it was shown [15] that the full visibility model $\mathbb{H}(n; K)$ has major differences with an ER graph. For instance, the edge assignments are (negatively) correlated in $\mathbb{H}(n; K)$ while independent in ER graphs; see [15] for a detailed discussion on the differences of $\mathbb{H}(n; K)$ and $\mathbb{G}(n; p)$. In a similar manner, it is easy to check that the edge assignments in $\mathbb{H} \cap \mathbb{G}(n; \theta)$ are also negatively correlated. Therefore, the model $\mathbb{H} \cap \mathbb{G}(n; \theta)$ can not be equated to an ER graph and the results obtained in this paper are not consequences of classical results for ER graphs.

However, there exist certain similarities between $\mathbb{H} \cap \mathbb{G}(n; \theta)$ and ER graphs. For instance, recall the well-known zero-one law for ER graphs: For any scaling $p : \mathbb{N}_0 \to [0, 1]$ satisfying $p_n \sim c \, \frac{\log n}{n}$ for some $c > 0$, it holds that

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

Also, observe that the condition (4) can be rephrased more compactly as

$$p_n \lambda_n(K_n) \sim c \, \frac{\log n}{n}, \qquad c > 0$$

while keeping the results (5) unchanged. Thus, here as well the zero-one laws are expressed by having the probability of link assignment be compared against the critical scaling $\frac{\log n}{n}$.

Despite this similarity, the condition $c > \tau(p^\star)$ that ensures a.a.s. connectivity in $\mathbb{H} \cap \mathbb{G}(n; \theta)$ is not the same as the condition $c > 1$ that ensures a.a.s. connectivity in ER graphs; see (3). Thus, the connectivity behavior of the model $\mathbb{H} \cap \mathbb{G}(n; \theta)$ is in general different from an ER graph, and a "transfer" of the connectivity results from ER graphs can not be taken as granted. Yet, the connectivity behaviors of the two models match in the practically relevant case (for WSNs) $\lim_{n\to\infty} p_n = p^\star = 0$ since $\tau(0) = 1$. Therefore, one might expect ER graphs to be useful *proxies* in dimensioning the pairwise scheme in the context of WSNs.

C. Future work

One possible extension of the work presented here would be to consider a more realistic communication model; e.g., the popular disk model [9] which takes into account the geographical positions of the sensor nodes. Assume that the nodes are distributed over a region $\mathcal{R}$ of the plane. According to the *disk model*, nodes i and j located at $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$ in $\mathcal{R}$ are able to communicate if

$$\| \boldsymbol{x_i} - \boldsymbol{x_j} \| < \rho \tag{10}$$

where ρ is called the transmission range. Once the nodes are randomly distributed over the region $\mathcal{R}$, the graph induced under the condition (10) is known as a random geometric graph [11], denoted $\mathbb{G}(n;\rho)$.

Under the disk model, studying the pairwise scheme of Chan et al. amounts to analyzing the intersection of $\mathbb{H}(n;K)$ and $\mathbb{G}(n;\rho)$, say $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$. A direct analysis of this model seems to be very challenging; see below for more on this. However, the simulations suggest that an analog of the zero-one laws obtained here for $\mathbb{H} \cap \mathbb{G}(n;K,p)$ apply also to the model $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$. To verify this, we consider 200 nodes distributed uniformly and independently over a 2-dimensional (1×1) region with toroidal (continuous) boundary conditions. Under the enforced assumptions, there are no border effects and it is easy to check that

$$\mathbb{P}[\, \| \boldsymbol{x_i} - \boldsymbol{x_j} \| < \rho \,] = \pi\rho^2, \quad i \neq j, \;\; i,j = 1,2,\ldots,n.$$

whenever $\rho < 0.5$. We match the two communication models $\mathbb{G}(n;p)$ and $\mathbb{G}(n;\rho)$ by requiring $\pi\rho^2 = p$, and by the same procedure that produced Figure 1, we obtain the empirical probability that $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ is connected for various values of (K,p). The results are depicted in Figure 2 whose resemblance with Figure 1 suggests that the connectivity behaviors of the models $\mathbb{H} \cap \mathbb{G}(n;K,p)$ and $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ are similar. Hence, the results obtained here for the on/off channel model can also be useful in dimensioning the pairwise scheme under the more realistic disk model.

We believe that a complete analysis of $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ is likely to be challenging given the difficulties encountered while dealing with similar problems. For example, the authors in [1], [18] considered the intersection of random geometric graphs with ER graphs. Although zero-one laws for graph connectivity were available for each of these random graphs, the results [1],[18] for the intersection model were limited only to the property of absence of isolated nodes; the connectivity problem is still open for that model. Yi et al. [18] have also considered the intersection of random key graphs with random geometric graphs but the results were again limited to the property of node isolation. To the best our knowledge Theorem 4.1 established here constitutes the only zero-one law for graph connectivity obtained for a model formed by the intersection of multiple random graphs! (Except of course the trivial case where an ER graph intersects another ER graph.)

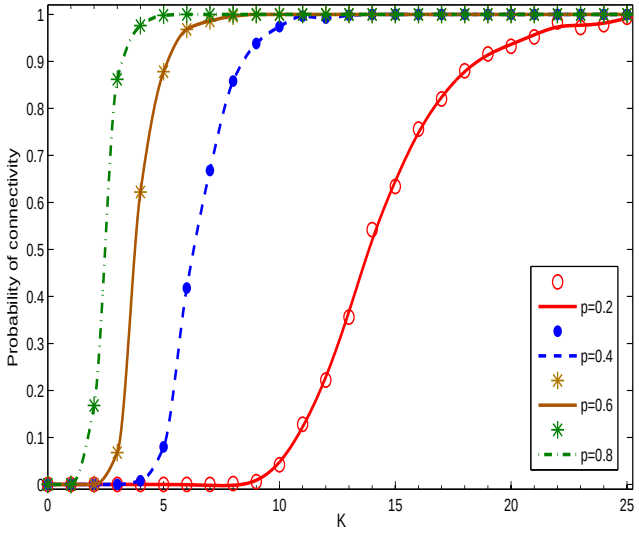

Fig. 2. Probability that $\mathbb{H} \cap \mathbb{G}(n;K,\rho)$ is connected with respect to K. The number of nodes is set to $n = 200$ and ρ is given by $\pi\rho^2 = p$. A comparison with Figure 1 clearly suggests that the results obtained in this paper can also be useful in dimensioning the pairwise scheme under disk model.

REFERENCES

[1] N. P. Anthapadmanabhan and A. M. Makowski, "On the Absence of Isolated Nodes in Wireless Ad-Hoc Networks with Unreliable Links - a Curious Gap," Proceedings of Infocom 2010, San Diego (CA), 2010.

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

[3] M. Bloznelis, J. Jaworski, K. Rybarczyk, "Component evolution in a secure wireless sensor network," *Networks* **53:1** (2009), pp. 19-26.

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

[5] S. A. Çamtepe, B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey," Technical Report TR-05-07, Rensselaer Polytechnic Institute, Computer Science Department, March 2005.

[6] H. Chan, A. Perrig, D. Song, "Random key predistribution schemes for sensor networks," Proceedings of SP 2003, Oakland (CA), May 2003.

[7] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *TISSEC* **11** (2008), pp. 1-22.

[8] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," Proceedings of CCS 2002, pp. 41-47.

[9] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," Proceedings of the 37th IEEE CDC, 1998.

[10] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," Proceedings of SASN 2004.

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

[12] K. Rybarczyk "Diameter, connectivity and phase transition of the uniform random intersection graph," Submitted to *Discrete Mathematics*, July 2009.

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

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

[15] O. Yağan and A. M. Makowski, "On random graphs associated with a pairwise key distribution scheme for wireless sensor networks," submitted to Infocom 2011, June 2010. Available online at http://hdl.handle.net/1903/10601.

[16] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key distribution schemes," submitted to Infocom 2011, June 2010. Available online at http://hdl.handle.net/1903/10604.

[17] O. Yağan and A. M. Makowski, "Modeling the pairwise key distribution scheme in the presence of unreliable links (Extended version)." Available online at http://www.lib.umd.edu/drum/.

[18] C.W. Yi, P.J. Wan, K.W. Lin and C.H. Huang, "Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with unreliable nodes and links," Proceedings of IEEE Globecom 2006.