Connectivity results for sensor networks under a random pairwise key predistribution scheme

Osman Yağan
CyLab
Carnegie Mellon University, Pittsburgh, PA 15213.
Email: oyagan@andrew.cmu.edu

Armand M. Makowski
Department of Electrical and Computer
Engineering, and Institute for Systems Research
University of Maryland, College Park, MD 20742.
Email: armand@isr.umd.edu

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

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

I. Introduction

Random key predistribution is one of the approaches proposed in the literature for addressing security challenges in resource-constrained wireless sensor networks (WSNs). The idea of randomly assigning secure keys to the sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor [5]. Following their original work, a large number of key predistribution schemes have been proposed; see the survey articles [2], [15], [16], [17].

Here we consider the random pairwise key predistribution scheme proposed by Chan et al. in [3]: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from 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. A secure link can then be established between two communicating nodes 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. The random pairwise predistribution scheme has a number of advantages over the scheme of Eschenauer and Gligor: (i) Even if some nodes are captured, the secrecy of the remaining nodes is *perfectly* preserved; (ii) Unlike earlier schemes, the pairwise scheme enables both node-to-node authentication and quorum-based node revocation.

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 are within wireless communication with each other). We seek conditions on n and K under which $\mathbb{H}(n;K)$ is a connected graph with very high probability as n grows large. As in the case of the Eschenauer-Gligor scheme, such conditions may provide guidelines for dimensioning purposes (although they are possibly too optimistic given the full visibility assumption used).

We report on the following zero-one law for connectivity in $\mathbb{H}(n;K)$: With $K \geq 2$ (resp. $K = 1$), the probability that $\mathbb{H}(n;K)$ is a connected graph approaches 1 (resp. 0) as n grows large. This is done by establishing a computable lower bound on the probability of connectivity for each $K \geq 2$. Applying this lower bound with $K = 2$ we see that for $n = 20$, the graph is connected with probability larger than 0.98, whereas with only 50 sensors, this probability of connectivity becomes larger than 0.999. Thus, connectivity is already achievable with high probability under very small values of K and n. These values are much smaller than the ones implied by a heuristic transfer of classical connectivity results from Erdős-Rényi graphs (as was done in the original paper of Chan et al. [3] and in [8]). The results obtained here correct misleading predictions made in these earlier papers, and form the basis for a reappraisal of the scalability of the random pairwise predistribution scheme; see [19], [22] for details.

The random graph $\mathbb{H}(n;K)$ is known in the literature on random graphs as the random K-out graph [1], [6], [13]. Fenner and Frieze [6, Thm. 2.1, p. 348] have established the zero-one law given here by a completely different approach which focuses on the vertex and edge connectivity parameters. While their analysis also leads to a lower bound on the probability of connectivity, the lower bound obtained here is sharper than theirs for $K \geq 3$.

The paper is organized as follows: In Section II, we give a formal model for the random pairwise predistribution scheme of Chan et al., and introduce the induced random K-out graph.

The main results of the paper concerning the connectivity of random K-out graphs are presented in Section III; there we also compare them against the earlier results of Fenner and Frieze. Various comments are given in Section IV. Proofs are omitted due to space limitations but can be found in [23].

II. Model

All statements involving limits, including asymptotic equivalences, are understood with n going to infinity. The cardinality of any discrete set S is denoted by $|S|$.

A. The random pairwise key predistribution scheme

The random pairwise key predistribution scheme of Chan et al. is parametrized by two positive integers n and K such that $K < n$. There are n nodes which are 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 $\mathcal{N}_{-i}$ – Each of the nodes in $\Gamma_{n,i}(K)$ is said to be paired to node i. Specifically, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

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

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

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

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

Once this offline random pairing has been created, we construct the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$, one for each node, as follows: Assumed available is a collection of nK distinct cryptographic keys $\{\omega_{i|\ell},\ i = 1, \ldots, n;\ \ell = 1, \ldots, K\}$. These keys are drawn from a very large pool of keys; in practice the pool size is assumed to be much larger than nK, and can be safely taken to be infinite for the purpose of our discussion.

Now, fix $i = 1, \ldots, n$ and let $\ell_{n,i} : \Gamma_{n,i}(K) \to \{1, \ldots, K\}$ denote a labeling of $\Gamma_{n,i}(K)$. For each node j in $\Gamma_{n,i}(K)$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}(K)$ is realized as $\{j_1, \ldots, j_K\}$ with $1 \le j_1 < \ldots < j_K \le n$, 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. Inherent to this construction is the fact that the key $\omega^{\star}_{n,ij}$ is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise predistribution scheme. The key ring $\Sigma_{n,i}(K)$ of node i is the set

$$\begin{aligned} &\Sigma_{n,i}(K) \qquad (1)\\ &\quad = \quad \{\omega^{\star}_{n,ij},\ j \in \Gamma_{n,i}(K)\} \cup \{\omega^{\star}_{n,ji},\ i \in \Gamma_{n,j}(K)\}. \end{aligned}$$

As mentioned earlier, under full visibility, two nodes, say i and j, can establish a secure link if at least one of the events $i \in \Gamma_{n,j}(K)$ or $j \in \Gamma_{n,j}(K)$ takes 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 $\omega^{\star}_{n,ji}$. By construction this scheme supports node-to-node authentication.

B. The induced random graphs

Under full visibility the pairwise predistribution scheme naturally gives rise to the following class of random graphs: With $n = 2, 3, \ldots$ and positive integer $K < n$, the distinct nodes i and j are said to be adjacent, written $i \sim j$, if and only if they have at least one key in common in their key rings. Thus, with the notation (1), we have

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

or, equivalently,

$$i \sim j \quad \text{iff} \quad i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K). \qquad (2)$$

Let $\mathbb{H}(n; K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (2). In the literature on random graphs, the random graph $\mathbb{H}(n; K)$ is usually referred to as a random K-out graph [1], [6], [13].

We close with some notation. Throughout we write

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

Furthermore, let $\lambda(n; K)$ denote the probability of edge assignment (between any two nodes) in $\mathbb{H}(n; K)$. Under the enforced independence assumptions, it is plain from (2) that

$$\begin{aligned} \lambda(n; K) &= 1 - \left(1 - \frac{K}{n-1}\right)^2 \\ &= \frac{2K}{n-1} - \left(\frac{K}{n-1}\right)^2. \end{aligned} \qquad (3)$$

III. The results

Throughout it will be convenient to use the notation

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

and

$$a(K) = e^{-\frac{1}{2}(K+1)(K-2)} \qquad (4)$$

with n and K arbitrary positive integers.

A. A tight bound and its consequences

Our main technical result is given next; its proof, given in [23], adapts classical arguments used for proving the one-law for connectivity in Erdős-Rényi graphs [4, Section 3.4.2, p. 42].

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

$$P(n;K) \geq 1 - a(K)Q(n;K) \tag{5}$$

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

The bound (5) gives some indication as to how fast the convergence $\lim_{n\to\infty} P(n;K) = 1$ occurs when $K \geq 2$, with the convergence becoming faster with larger K as would be expected; see also (7) below. Although the right handside of (5) may be negative for small values of n (in which case the bound is trivial), it is already positive when $n = 2(K+1)$ (hence also past $n(K)$).

For $K = 2$, since $n(2) = 16$, the bound (5) becomes

$$P(n;2) \geq 1 - \frac{155}{n^3}, \quad n \geq 16. \tag{6}$$

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

$$P(n;2) \leq P(n,K), \quad K = 2, \ldots, n-1. \tag{7}$$

Making use of (6) we then conclude

$$P(n;K) \geq 1 - \frac{155}{n^3}, \qquad \begin{array}{c} n \geq 16, \\ K = 2, \ldots, n-1. \end{array} \tag{8}$$

A zero-one law for connectivity is presented next.

Theorem 3.2: With any positive integer K, we have

$$\lim_{n\to\infty} P(n;K) = \begin{cases} 0 & \text{if } K = 1 \\ \\ 1 & \text{if } K \geq 2. \end{cases} \tag{9}$$

The one-law in Theorem 3.2 is an easy consequence of the bound (5), while the zero-law of Theorem 3.2 is proved separately in [23]. Theorem 3.2 easily yields the behavior of graph connectivity as the parameter K is scaled with n, but first some terminology: We refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* whenever it satisfies the natural conditions

$$K_n < n, \quad n = 2, 3, \ldots. \tag{10}$$

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

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

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

B. Earlier results of Fenner and Frieze

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

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

$$\lim_{n\to\infty} \mathbb{P}\left[C_v(n;K) = K\right] = 1 \tag{11}$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[C_e(n;K) = K\right] = 1, \tag{12}$$

while

$$\lim_{n\to\infty} P(n;1) = 0. \tag{13}$$

The one-law in Theorem 3.2 is immediate from either (11) or (12) since $\mathbb{H}(n;K)$ is connected if either $C_v(n;K) \geq 1$ or $C_e(n;K) \geq 1$. The zero-law in Theorem 3.2 coincides with (13), and was obtained in [6] with the help of results by Katz [11] concerning random mappings. In [23] we give a completely different proof for (13); it uses classical enumeration results for the set of undirected graphs on n nodes which are connected and have exactly n edges [7, p. 133-134].

Inspection of the proof of Theorem 3.4 given in [6, Thm. 2.1, p. 348] yields the lower bound

$$P(n;K) \geq 1 - b(n;K)Q(n;K) \tag{14}$$

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

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

with

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

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

The lower bound (14) has the same form as the one given in Theorem 3.1, but is weaker (i.e., is a smaller lower bound) than (5) except for $K = 2$. Indeed it is easy to check that

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

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

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

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

with

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

Thus, the lower bound given in Theorem 3.1 for the probability of network connectivity approaches one much faster than the bound (14) inferred from [6]. To illustrate this fact, with $n = 50$ we have plotted the behavior of $a(K)$, $b(K)$ and $b(n;K)$ with respect to K in Figure 1. As expected from the remarks above, $a(K)$ approaches zero much faster (in fact exponentially fast) than $b(n;K)$ as K increases. Although $K = 2$ is already enough to ensure connectivity with high probability, in a realistic WSN setting, we expect K to

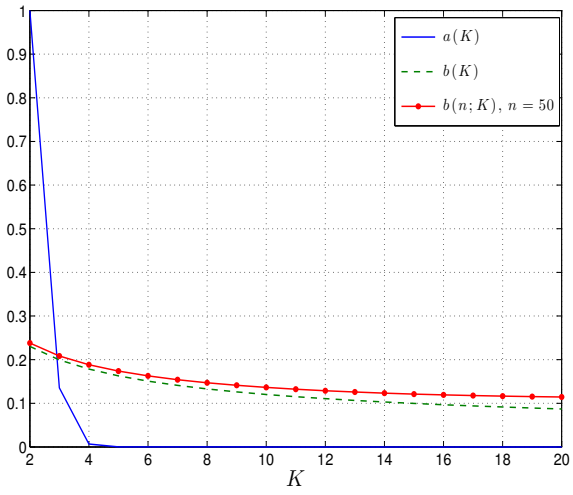

Fig. 1. *For $n = 50$, we compare the coefficients $a(K)$, $b(K)$ and $b(n;K)$. It is clear that $a(K) < b(K) < b(n;K)$ for all $K = 3, 4, \ldots$, so that the lower bound $1 - a(K)Q(n;K)$ obtained here is stronger (i.e., larger) than the lower bound $1 - b(n;K)Q(n;K)$ derived in [6].*

take larger values in order to accommodate other network requirements and to ensure connectivity under severe channel conditions [21].

IV. Comments

We now provide some comments concerning the results.

A. Correlated edge assignments

For each p in $[0,1]$ and $n = 2, 3, \ldots$, let $\mathbb{G}(n;p)$ denote the Erdős-Rényi graph on the vertex set $\{1, \ldots, n\}$ with edge probability p. While edge assignments are mutually independent in $\mathbb{G}(n;p)$, they are strongly correlated in $\mathbb{H}(n;K)$ in that they are *negatively associated* in the sense of Joag-Dev and Proschan [10]; see [18], [21] 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 $\lambda(n;K) = p$. As a result, neither Theorem 3.1 nor Corollary 3.3 are consequences of classical results for Erdős-Renyi graphs [1]. See also the discussion in Section IV-C.

B. Connectivity vs. absence of isolated nodes

To drive the point further, note the following: In many known classes of random graphs, the absence of isolated nodes and graph connectivity are asymptotically equivalent properties, e.g., Erdős-Rényi graphs [1], [4], geometric random graphs [12] and random key graphs [14], [18], [20]. This equivalence, when it holds, is exploited by first establishing the zero-one law for the absence of isolated nodes, a step which is usually much simpler to complete with the help of the method of first and second moments [9, p. 55]. However, there are no isolated nodes in $\mathbb{H}(n;K)$ since each node is of degree at least K. Thus, the class of random graphs studied here provides an example where graph connectivity and the absence of isolated nodes are not asymptotically equivalent properties; in fact this is what makes the proof of the zero-law (given in [23]) more intricate.

C. Earlier analysis via transfers

In the original paper of Chan et al. [3] (as in the reference [8]), the connectivity of $\mathbb{H}(n;K)$ was analyzed through the following two-step process: (i) First, the random graph $\mathbb{H}(n;K)$ was equated with an Erdős-Rényi graph so that the edge assignment probabilities are asymptotically equivalent; (ii) Then, classical connectivity results for Erdős-Rényi graphs were formally transferred to $\mathbb{H}(n;K)$ under this constraint.

We revisit this transfer argument in some details: First, there is no loss of generality in writing any scaling $p : \mathbb{N}_0 \to [0,1]$ for the edge assignment probability in Erdős-Rényi graphs in the form

$$p_n = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{15}$$

for some deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$. Also, recall [1] that the property of graph connectivity admits the zero-one law

$$\lim_{n\to\infty} \mathbb{P}[\ \mathbb{G}(n;p_n) \text{ is connected }] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty. \end{cases} \tag{16}$$

It is tempting to use this result as follows: A given scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ is said to be *asymptotically matched* to a scaling $p : \mathbb{N}_0 \to [0,1]$ for Erdős-Rényi graphs provided $\lambda(n;K_n) \sim p_n$. This ensures that the expected degrees (per node) in the random graphs $\mathbb{G}(n;p_n)$ and $\mathbb{H}(n;K_n)$ are asymptotically equivalent. In view of (3) this requirement amounts to

$$p_n \sim \frac{2K_n}{n-1} - \left(\frac{K_n}{n-1}\right)^2. \tag{17}$$

If the scaling $p : \mathbb{N}_0 \to [0,1]$ is put in the form (15) for some deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, then (17) becomes

$$\frac{2K_n}{n-1} - \left(\frac{K_n}{n-1}\right)^2 \sim \frac{\log n + \alpha_n}{n}. \tag{18}$$

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

$$\lim_{n\to\infty} P(n;K_n) = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{19}$$

should then hold by a formal transfer of (16). This approach, though appealing for its simplicity, leads to incorrect conclusions as we now show.

Indeed, consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n = K^\star$ for some positive integer $K^\star$ for all n sufficiently large. On that range, the requirement (18) leads to the corresponding deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ being given by

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

for some sequence $t : \mathbb{N}_0 \to \mathbb{R}_+$ with $\lim_{n\to\infty} t_n = 1$. Thus, we have $\lim_{n\to\infty} \alpha_n = -\infty$ regardless of the value of $K^\star$, and according to (19) we would conclude that $\lim_{n\to\infty} P(n; K^\star) = 0$ for *all* positive integers $K^\star$, in clear contradiction with Theorem 3.2.

We could also have used a weaker version of the zero-one law (16) which considers scalings $p : \mathbb{N}_0 \to [0, 1]$ of the form

$$p_n \sim c \; \frac{\log n}{n} \tag{20}$$

for some $c > 0$. It is then easy to check from (16) that

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}[\ \mathbb{G}(n; p_n) \text{ is connected }] \\ &= \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c. \end{cases} \end{aligned} \tag{21}$$

This time, (17) requires

$$2K_n \sim c \; \log n \tag{22}$$

under (20), and a formal transfer of (21) suggests the validity of the zero-one law

$$\lim_{n\to\infty} P(n; K_n) = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c. \end{cases} \tag{23}$$

In particular, we read off from (23) that K_n should behave like $\gamma \log n$ with $\gamma > \frac{1}{2}$ (resp. $\gamma < \frac{1}{2}$) in order for $\mathbb{H}(n; K_n)$ to be connected (resp. disconnected) with a probability approaching 1 for n large. Not only does this conclusion fall short of the result given in Corollary 3.3, but it also leads to incorrect design decisions: For instance, the maximum supportable network size evaluated in [3], [8] leads to the conclusion that the random pairwise key predistribution scheme is *not* scalable in the context of WSNs. The results given here form the basis for a reevaluation of these conclusions; see [19], [22] for details.

ACKNOWLEDGMENT

This work was supported by NSF Grant CCF-0729093. We thank the following individuals: Dr. H. Chan of CyLab at Carnegie Mellon University for pointing out reference [3] and for some insightful comments concerning this work; Prof. A. Barg from the Department of Electrical and Computer Engineering at the University of Maryland at College Park for reference [7]; and Prof. A. Srinivasan from the Department of Computer Science at the University of Maryland at College Park for making us aware of the work by Fenner and Frieze [6].

REFERENCES

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

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

[3] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Research in Security and Privacy (SP 2003), Oakland (CA), May 2003, pp. 197-213.

[4] M. Draief and L. Massoulié, *Epidemics and Rumours in Complex Networks*, London Mathematical Society Lecture Notes Series **369**, Cambridge University Press, Cambridge (UK), 2010.

[5] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the ACM Conference on Computer and Communications Security (CSS 2002), Washington (DC), November 2002, pp. 41-47.

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

[7] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge (UK), January 2009.

[8] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in Proceedings of the 2nd ACM Workshop on Security of Ad Hoc And Sensor Networks (SASN 2004), Washington (DC), October 2004.

[9] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

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

[11] L. Katz, "Probability of indecomposability of a random mapping function," *Annals of Mathematical Statistics* **25** (1955), pp. 512-517.

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

[13] T. K. Philips, D. F. Towsley and J. K. Wolf, "On the diameter of a class of random graphs," *IEEE Transactions on Information Theory* **IT-36** (1990), pp. 285–288.

[14] K. Rybarczyk, "Diameter of the uniform random intersection graph with a note on the connectivity and the phase transition," *Discrete Mathematics* **311** (2011), pp. 1998-2019.

[15] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica* **12** (2006), pp. 900-906.

[16] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials* **8** (2006), pp. 2-23.

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

[18] O. Yağan, *Random Graph Modeling of Random Key Distribution Schemes in Wireless Sensor Networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011.

[19] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key predistribution schemes," in Proceeding of the 9th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2011), Princeton (NJ), May 2011.

[20] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs." *IEEE Transactions on Information Theory* **IT-58** (2012), pp. 2983-2999.

[21] O. Yağan and A.M. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *IEEE Transactions on Information Theory*. Accepted for publication (2012).

[22] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key predistribution scheme: Gradual deployment and key ring sizes." Submitted to *Performance Evaluation* (2011).

[23] O. Yağan and A. M. Makowski, "On the connectivity of sensor networks under random pairwise key predisribution." Submitted to *IEEE Transcation on Information Theory* (February 2012). Available online at http://www.andrew.cmu.edu/~oyagan/Journals/Pairwise_IT.pdf.