Secure k-Connectivity in Wireless Sensor Networks under an On/Off Channel Model

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

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

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

***Abstract*—Random key predistribution scheme of Eschenauer and Gligor (EG) is a typical solution for ensuring secure communications in a wireless sensor network (WSN). Connectivity of the WSNs under this scheme has received much interest over the last decade, and most of the existing work is based on the assumption of unconstrained sensor-to-sensor communications. In this paper, we study the k-connectivity of WSNs under the EG scheme with physical link constraints; k-connectivity is defined as the property that the network remains connected despite the failure of any $(k-1)$ sensors. We use a simple communication model, where unreliable wireless links are modeled as independent on/off channels, and derive zero-one laws for the properties that $i)$ the WSN is k-connected, and $ii)$ each sensor is connected to at least k other sensors. These zero-one laws improve the previous results by Rybarczyk on the k-connectivity under a fully connected communication model. Moreover, under the on/off channel model, we provide a stronger form of the zero-one law for the 1-connectivity as compared to that given by Yağan.**

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

I. Introduction

Many designs of secure wireless sensor networks (WSNs) (e.g., [1], [5], [7]) rely on a basic *random* key predistribution scheme proposed by Eschenauer and Gligor [10]. For keying a network comprising n sensor nodes[1], this scheme uses an offline *key pool* $\mathcal{P}$ containing P_n keys, where P_n is a function of n. Before deployment, each node is independently equipped with K_n *distinct* keys selected uniformly at *random* from $\mathcal{P}$; here, K_n is also a function of n. The K_n keys in each node comprise the node's *key ring*. After deployment, two communicating nodes can establish a *secure link* if they share a key. More specifically, a secure link exists between two nodes if and only if their key rings have at least one key in common, as message secrecy and authenticity are obtained by using symmetric-key encryption modes [13], [15], [17].

In this paper, we consider the k-connectivity of secure WSNs operating under the key predistribution scheme of Eschenauer-Gligor. A network (or graph) is said to be k-connected[2] if it remains connected despite the deletion any $(k-1)$ nodes. A network is said to be simply connected if it is 1-connected. The k-connectivity also implies that for each pair of nodes in the graph there exist at least k mutually disjoint paths connecting them.

k-connectivity – a fundamental property of networks (graphs) – is particularly important in secure sensor networks where nodes operate autonomously and are physically unprotected. For instance, k-connectivity provides communication security against an adversary that is able to *compromise* up to $(k-1)$ links by launching a sensor capture attack [4]; i.e., two sensors can communicate securely as long as at least one of the k disjoint paths connecting them consists of links that are not compromised by the adversary. Also, k-connectivity improves resiliency against network disconnection due to battery depletion, in both normal mode of operation and under battery-depletion attacks [20], [28]. Furthermore, it enables flexible communication-load balancing across multiple paths so that network energy consumption is distributed without penalizing any access path [11], [21]. In addition, k-connectivity is useful in terms of achieving consensus despite adversarial nodes in the network. Specifically, it is known that for a network to achieve consensus in the presence of adversarial nodes, a necessary and sufficient condition is that the number of adversary-controlled nodes should be less than a half of the network connectivity *and* less than one-third of the number of network nodes [6], [27]. In other words, if $k > 2f$, where f is the number of adversary-controlled nodes, k-connectivity guarantees that consensus can be reached in a network with $n > 3f$ nodes.

With this motivation in mind, our goal is to study the k-connectivity of secure WSNs and we will do so by analyzing the induced *random graph* models. To begin with, the basic key predistribution scheme is often modeled by a *random key graph*, $G(n, K_n, P_n)$, also known as a *uniform random intersection graph*, whose properties have been extensively analyzed [2], [5], [18], [22], [26]. Random key graphs have also recently been used for various applications, e.g., cryptanalysis of hash functions [3], trust networks [14], recommender systems using collaborative filtering [16], and modeling "small world" networks [25]. The zero-one laws for k-connectivity [19] and 1-connectivity [2], [18], [26] of random key graphs have already been established. However,

[1]We consider the terms sensor, node and vertex interchangeable.

[2]The definition of k-connectivity given here is referred to as the *k-vertex*-connectivity in the literature; *k-edge*-connectivity is defined similarly for graphs that remain connected despite the deletion of any $k-1$ edges. It is worth noting that k-vertex-connectivity implies k-edge-connectivity [9].

in the context of *wireless* sensor networks, the application of random key graph requires the assumption of a fully connected wireless communication model; i.e., *any* pair of nodes have a direct communication link in between.

In this paper, we drop the assumption of a fully connected communication model and study the k-connectivity of secure WSNs under *physical link constraints*. To this end, we say that a secure link exists between two nodes if and only if their key rings have at least one key in common *and* the physical link constraint between them is satisfied. Specifically, in this paper, we consider a simple communication model that consists of independent channels that are either *on* (with probability p_n) or *off* (with probability $(1-p_n)$). Under this on/off channel model, a secure link exists between two sensors as long as their key rings have at least one key in common *and* the channel between them is *on*. We denote the graph representing the underlying network as $\mathbb{G}_{on}$; see Section III for precise definitions of the system model.

We derive zero-one laws in the random graph $\mathbb{G}_{on}$ for k-connectivity and the property that the *minimum node degree* is at least k; see Theorem 1. To the best of our knowledge, these results constitute the first complete analysis of the k-connectivity of WSNs under physical link constraints and may provide useful design guidelines in dimensioning the EG scheme; i.e., in selecting its parameters to ensure the desired k-connectivity property. The main result of the paper also implies a zero-one law for k-connectivity in random key graph $G(n, K_n, P_n)$ (see Corollary 2); and the established result is shown to improve that given previously by Rybarczyk [18] (see Section IV-D for details). Moreover, for the 1-connectivity of $\mathbb{G}_{on}$, we provide a stronger form of the zero-one law as compared to that given by Yağan [24]; see Section IV-D.

We organize the rest of the paper as follows: In Section II, we survey the relevant results from the literature, while in Section III we give a detailed description of the system model $\mathbb{G}_{on}$. The main results of the paper, namely the zero-one laws for k-connectivity and minimum node degree in $\mathbb{G}_{on}$, are presented in Section IV along with a discussion and comparison with the relevant results from literature. The proofs of the main results are omitted here due to space limitations, but all details can be found in [29].

II. Related Work

Early work by Erdős and Rényi [8] and Gilbert [12] introduces the random graph $G(n, p)$, which is defined on n nodes and there exists an edge between any two nodes with probability p *independently* of all other edges. The probability p can be a function of n, in which case we refer to it as p_n. Throughout the paper, we refer to the random graph $G(n, p_n)$ as an Erdős-Rényi (ER) graph following the convention in the literature.

Erdős and Rényi [8] prove that when p_n is $\frac{\ln n+\alpha_n}{n}$, graph $G(n, p_n)$ is *asymptotically almost surely*[3] (a.a.s.) connected (resp., not connected) if $\lim_{n\to\infty}\alpha_n = \infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$). In later work [9], they further explore k-connectivity in $G(n, p_n)$ and show that if $p_n = \frac{\ln n+(k-1)\ln\ln n+\alpha_n}{n}$, $G(n, p_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty}\alpha_n = \infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$).

[3] We say that an event takes place *asymptotically almost surely* if its probability approaches to 1 as $n \to \infty$.

Previous work [2], [18], [26] investigates the zero-one law for connectivity in random key graph $G(n, K_n, P_n)$, where P_n and K_n are the key pool size and the key ring size, respectively. Blackburn and Gerke [2] prove that if $K_n \geq 2$ and $P_n = \lfloor n^{\xi}\rfloor$, where ξ is a positive constant, $G(n, K_n, P_n)$ is a.a.s. connected (resp., not connected) if $\liminf_{n\to\infty}\frac{K_n^2 n}{P_n \ln n} > 1$ (resp., $\limsup_{n\to\infty}\frac{K_n^2 n}{P_n \ln n} < 1$). Yağan and Makowski [26] demonstrate that if[4] $K_n \geq 2$, $P_n = \Omega(n)$ and $\frac{K_n^2}{P_n} = \frac{\ln n+\alpha_n}{n}$, then $G(n, K_n, P_n)$ is a.a.s. connected (resp., not connected) if $\lim_{n\to\infty}\alpha_n = \infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$). Rybarczyk [18] obtains the same result without requiring $P_n = \Omega(n)$. She also establishes [19, Remark 1, p. 5] a zero-one law for k-connectivity in $G(n, K_n, P_n)$ by exploiting the similarity between $G(n, K_n, P_n)$ and a random intersection graph via a coupling argument. Specifically, she proves that if $K_n \geq 2$, $P_n = \Theta\big(n^{\xi}\big)$ for some $\xi > 1$, and $\frac{K_n^2}{P_n} = \frac{\ln n+(k-1)\ln\ln n+\alpha_n}{n}$, then $G(n, K_n, P_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty}\alpha_n = \infty$ (resp., $\lim_{n\to\infty}\alpha_n = -\infty$).

Recently Yağan [24] gives a zero-one law for connectivity (i.e., 1-connectivity) in graph $G(n, K_n, P_n) \cap G(n, p_n)$, which is the intersection of random key graph $G(n, K_n, P_n)$ and ER graph $G(n, p_n)$, and clearly is equivalent to our system model $\mathbb{G}_{on}$; see Section III. Specifically, he shows that if $K_n \geq 2$, $P_n = \Omega(n)$ and $p_n \cdot \left[1 - \frac{\binom{P_n-K_n}{K_n}}{\binom{P_n}{K_n}}\right] \sim c \cdot \frac{\ln n}{n}$ with c being a positive constant, and $\lim_{n\to\infty}(p_n \ln n)$ exists, then graph $G(n, K_n, P_n) \cap G(n, p_n)$ is a.a.s. connected (resp., not connected) if $c > 1$ (resp., $c < 1$).

A comparison of our results with the related work is given in Section IV-D.

III. The System Model $\mathbb{G}_{on}$

Consider a vertex set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$. For each node $v_i \in \mathcal{V}$, we define S_i as the key ring of node v_i; i.e., the set of K_n distinct keys of node v_i that are selected uniformly at random from a key pool $\mathcal{P}$ of P_n keys. The random key graph, denoted $G(n, K_n, P_n)$, is defined on the vertex set $\mathcal{V}$ through the following notion of adjacency: Between any two distinct nodes v_i and v_j, there exists an undirected edge, the event of which is denoted by K_{ij}, if their key rings have at least one

[4] We use the standard asymptotic notation $o(\cdot), O(\cdot), \Theta(\cdot), \Omega(\cdot), \sim$. That is, given two positive functions $f(n)$ and $g(n)$,

1) $f(n) = o\left(g(n)\right)$ means $\lim_{n\to\infty}\frac{f(n)}{g(n)} = 0$.
2) $f(n) = O\left(g(n)\right)$ means that there exist positive constants c_1 and N_1 such that $f(n) \leq c_1 g(n)$ for all $n \geq N_1$.
3) $f(n) = \Omega\left(g(n)\right)$ means that there exist positive constants c_2 and N_2 such that $f(n) \geq c_2 g(n)$ for all $n \geq N_2$.
4) $f(n) = \Theta\left(g(n)\right)$ means $f(n) = O\left(g(n)\right)$ and $f(n) = \Omega\left(g(n)\right)$.
5) $f(n) \sim g(n)$ means $\lim_{n\to\infty}\frac{f(n)}{g(n)} = 1$.

key in common; i.e.,

$$K_{ij} = [S_i \cap S_j \neq \emptyset], \text{ for } 1 \leq i < j \leq n.$$

As mentioned in Section I, here we assume a communication model that consists of independent channels that are either *on* (with probability p_n) or *off* (with probability $1-p_n$). For distinct nodes v_i and v_j, let C_{ij} denote the event that the communication channel between them is *on*. The events $\{C_{ij},\ 1 \leq i < j \leq n\}$ are mutually independent such that

$$\mathbb{P}[C_{ij}] = p_n, \text{ for } 1 \leq i < j \leq n. \tag{1}$$

This communication model can be modeled by an Erdős-Rényi graph $G(n, p_n)$ on the vertices $\mathcal{V}$ such that there exists an edge between nodes v_i and v_j if the communication channel between them is on; i.e., if the event C_{ij} takes place.

Finally, the graph $\mathbb{G}_{on}(n, K_n, P_n, p_n)$ is defined on the vertices $\mathcal{V}$ such that two distinct nodes v_i and v_j have an edge in between, denoted E_{ij}, if the events K_{ij} and C_{ij} take place at the same time. In other words, we have

$$E_{ij} = K_{ij} \cap C_{ij}, \text{ for } 1 \leq i < j \leq n, \tag{2}$$

so that

$$\mathbb{G}_{on}(n, K_n, P_n, p_n) = G(n, K_n, P_n) \cap G(n, p_n). \tag{3}$$

Throughout, we simplify the notation by writing $\mathbb{G}_{on}$ instead of $\mathbb{G}_{on}(n, K_n, P_n, p_n)$.

Throughout, we let $p_s(K_n, P_n)$ be the probability that the key rings of two distinct nodes share at least one key and let $p_e(K_n, P_n, p_n)$ be the probability that there exists a link between two distinct nodes in $\mathbb{G}_{on}$. For simplicity, we write $p_s(K_n, P_n)$ as p_s and write $p_e(K_n, P_n, p_n)$ as p_e. Then

$$p_s := \mathbb{P}[K_{ij}], \text{ for } 1 \leq i < j \leq n. \tag{4}$$

It is easy to derive p_s in terms of K_n and P_n as shown in previous work [2], [18], [26]. In fact, we have

$$p_s = \mathbb{P}[S_i \cap S_j \neq \emptyset] = \begin{cases} 1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}, & \text{if } P_n \geq 2K_n; \\ 1, & \text{if } P_n < 2K_n. \end{cases} \tag{5}$$

Given (2), the independence of the events C_{ij} and K_{ij} yields

$$p_e := \mathbb{P}[E_{ij}] = \mathbb{P}[C_{ij}] \cdot \mathbb{P}[K_{ij}] = p_n \cdot p_s \tag{6}$$

from (1) and (4). Substituting (5) into (6), we obtain

$$p_e = p_n \cdot \left[1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}}\right] \quad \text{if } P_n \geq 2K_n. \tag{7}$$

IV. Main Results and Discussion

A. A Zero-One Law for k-Connectivity in Graph $\mathbb{G}_{on}$

Recall that we denote by $\mathbb{G}_{on}$ the random graph induced by the EG scheme under the on/off channel model. The main result of this paper, given below, establishes zero-one laws for k-connectivity and for the property that the minimum node degree is no less than k in graph $\mathbb{G}_{on}$. Note that throughout this paper, k is a positive integer and does not scale with n.

Let $\mathbb{R}$ stand for the set of all real numbers; and let $\mathbb{N}_0$ be the set of all positive integers. We refer to any pair of mappings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* as long as it satisfies the natural conditions $K_n \leq P_n$ for each $n = 1, 2, \ldots$. Similarly, any mapping $p : \mathbb{N}_0 \to (0, 1)$ defines a scaling.

Theorem 1. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$, $p : \mathbb{N}_0 \to (0, 1)$ such that $K_n \geq 2$ for all n sufficiently large. We define a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ such that for any $n \in \mathbb{N}_0$, we have*

$$p_e = \frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}. \tag{8}$$

The properties (a) and (b) below hold.

(a) If $\frac{K_n^2}{P_n} = o(1)$ and either *$p_e n = \Omega(1)$* or *$p_e n = o(1)$, then*

$$\lim_{n \to \infty} \mathbb{P}[\mathbb{G}_{on} \textit{ is } k\textit{-connected}] = 0 \quad \textit{if } \lim_{n \to \infty} \alpha_n = -\infty, \tag{9}$$

and

$$\lim_{n \to \infty} \mathbb{P}\left[\begin{array}{c} \textit{Minimum node degree} \\ \textit{of } \mathbb{G}_{on} \textit{ is no less than } k \end{array}\right] = 0 \quad \textit{if } \lim_{n \to \infty} \alpha_n = -\infty. \tag{10}$$

(b) If $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$, then

$$\lim_{n \to \infty} \mathbb{P}[\mathbb{G}_{on} \textit{ is } k\textit{-connected}] = 1 \quad \textit{if } \lim_{n \to \infty} \alpha_n = \infty, \tag{11}$$

and

$$\lim_{n \to \infty} \mathbb{P}\left[\begin{array}{c} \textit{Minimum node degree} \\ \textit{of } \mathbb{G}_{on} \textit{ is no less than } k \end{array}\right] = 1 \quad \textit{if } \lim_{n \to \infty} \alpha_n = \infty. \tag{12}$$

Note that if we combine (9) and (11), we obtain the zero-one law for k-connectivity in $\mathbb{G}_{on}$, whereas combining (10) and (12) leads to the zero-one law for the minimum node degree. Therefore, Theorem 1 presents the zero-one laws of k-connectivity and the minimum node degree in graph $\mathbb{G}_{on}$. We also see from (8) that the critical scaling for both properties is given by $p_e = \frac{\ln n + (k-1) \ln \ln n}{n}$. The sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ defined through (8) therefore measures by how much the probability p_e deviates from the critical scaling.

In case (b) of Theorem 1, the conditions $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$ indicate that the size of the key pool P_n should grow at least linearly with the number of sensor nodes in the network, and should grow unboundedly with the size of each key ring. These conditions are enforced here merely for technical reasons, but they hold trivially in practical wireless sensor network applications [4], [5], [10]. Again, the condition $\frac{K_n^2}{P_n} = o(1)$ enforced for the zero-law in Theorem 1 is not a stringent one since P_n is expected to be several orders of magnitude larger than K_n. Finally, the condition that either $p_e n = \Omega(1)$ or $p_e n = o(1)$ is made to avoid degenerate situations. In fact, in most cases of interest it holds that $p_e n = \Omega(1)$ as otherwise graph $\mathbb{G}_{on}$ becomes *trivially* disconnected. To see this, notice that $p_e n$ is an upper bound on the *expected* degree of a node and that the *expected* number of edges in the graph is less than $p_e n^2$; yet, a connected graph on n nodes must have at least $(n-1)$ edges.

B. *Results with an approximation of probability p_s*

An analog of Theorem 1 can be given with a simpler form of the scaling than (8); i.e., with p_s replaced by the more easily expressed quantity K_n^2/P_n, and hence with p_e replaced by $p_n K_n^2/P_n$. In fact, in the case of random key graph $G(n, K_n, P_n)$, it is a common practice [2], [18], [26] to replace p_s by $\frac{K_n^2}{P_n}$, owing mostly to the fact that [26]

$$p_s \sim \frac{K_n^2}{P_n} \quad \text{if} \quad \frac{K_n^2}{P_n} = o(1). \tag{13}$$

However, when random key graph $G(n, K_n, P_n)$ is intersected with an ER graph $G(n, p_n)$ (i.e., for $\mathbb{G}_{on}$) this simplification does not occur naturally (even under (13)), and as seen below, simpler forms of the zero-one laws are obtained at the expense of extra conditions enforced on the parameters K_n and P_n.

Corollary 1. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$, $p : \mathbb{N}_0 \to (0, 1)$ such that $K_n \geq 2$ for all n sufficiently large. We define a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ such that for any $n \in \mathbb{N}_0$, we have*

$$p_n \cdot \frac{K_n^2}{P_n} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}. \tag{14}$$

The properties (a) and (b) below hold.

(a) If $\frac{K_n^2}{P_n} = O\big(\frac{1}{\ln n}\big)$ and $\lim_{n\to\infty}[\ln n + (k-1)\ln\ln n + \alpha_n] = \infty$, then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \textit{ is } k\textit{-connected}\right] = 0 \quad \textit{if} \ \lim_{n\to\infty} \alpha_n = -\infty, \tag{15}$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\textit{Minimum node degree}\\ \textit{of } \mathbb{G}_{on} \textit{ is no less than } k\end{array}\right] = 0 \ \ \textit{if} \ \lim_{n\to\infty} \alpha_n = -\infty. \tag{16}$$

(b) If $P_n = \Omega(n)$ and $\frac{K_n^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}_{on} \textit{ is } k\textit{-connected}\right] = 1 \quad \textit{if} \ \lim_{n\to\infty} \alpha_n = \infty, \tag{17}$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\textit{Minimum node degree}\\ \textit{of } \mathbb{G}_{on} \textit{ is no less than } k\end{array}\right] = 1 \quad \textit{if} \ \lim_{n\to\infty} \alpha_n = \infty. \tag{18}$$

Note that the condition $\frac{K_n^2}{P_n} = O\big(\frac{1}{\ln n}\big)$ enforced in Corollary 1 implies both $\frac{K_n}{P_n} = o(1)$ and $\frac{K_n^2}{P_n} = o(1)$, and thus it is a stronger condition than those enforced in Theorem 1.

C. *A Zero-One Law for k-Connectivity in Random Key Graphs*

We now provide a useful corollary of Theorem 1 that gives a zero-one law for k-connectivity in the random key graph $G(n, K_n, P_n)$. As discussed in Section IV-D below, this result improves the one given *implicitly* by Rybarczyk [19].

Corollary 2. *Consider a positive integer k, and scalings $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n \geq 2$ for all n sufficiently large. With $\alpha : \mathbb{N}_0 \to \mathbb{R}$ given by*

$$\frac{K_n^2}{P_n} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \quad n = 1, 2, \ldots, \tag{19}$$

the following two properties hold.

(a) If either $\frac{K_n^2}{P_n} = \Omega\big(\frac{1}{n}\big)$ or $\frac{K_n^2}{P_n} = o\big(\frac{1}{n}\big)$, *then*

$$\lim_{n\to\infty} \mathbb{P}\left[G(n, K_n, P_n) \textit{ is } k\textit{-connected}\right] = 0 \ \textit{if} \ \lim_{n\to\infty} \alpha_n = -\infty.$$

(b) If $P_n = \Omega(n)$, then

$$\lim_{n\to\infty} \mathbb{P}\left[G(n, K_n, P_n) \textit{ is } k\textit{-connected}\right] = 1 \ \textit{if} \ \lim_{n\to\infty} \alpha_n = \infty.$$

D. *Discussion and Comparison with Related Results*

As already noted in the literature [2], [8], [9], [18], [19], [26], Erdős-Rényi graph $G(n, p_n)$ and random key graph $G(n, K_n, P_n)$ have similar k-connectivity properties when they are *matched* through their link probabilities; i.e. when $p_n = p_s$ with p_s defined in (5). In particular, Erdős and Rényi [9] has shown that if $p_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, then $G(n, p_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty} \alpha_n = \infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$). Similarly, Rybarczyk [19] has proven that under some extra conditions (i.e., $P_n = \Theta\big(n^{\xi}\big)$ with $\xi > 1$) that if $p_s = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, then $G(n, K_n, P_n)$ is a.a.s. k-connected (resp., not k-connected) if $\lim_{n\to\infty} \alpha_n = \infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$).

The analogy between these two results could be exploited to conjecture similar k-connectivity results for our system model $\mathbb{G}_{on}$. To see this, recall from (3) that

$$\mathbb{G}_{on} = G(n, K_n, P_n) \cap G(n, p_n). \tag{20}$$

Since $G(n, K_n, P_n)$ and $G(n, p_s)$ have similar k-connectivity properties, it would seem intuitive to replace $G(n, K_n, P_n)$ with $G(n, p_s)$ in the above equation (20). Then, using

$$\mathbb{G}_{on} \simeq G(n, p_s) \cap G(n, p_n) = G(n, p_n p_s) = G(n, p_e),$$

we would automatically obtain Theorem 1 via the aforementioned result of Erdős and Rényi [9]. Unfortunately, such heuristic approaches can not be taken for granted as $G(n, K_n, P_n) \neq G(n, p_s)$ in general. For instance, the two graphs are shown [23], [25] to exhibit quite different characteristics in terms of properties including *clustering coefficient, number of triangles*, etc. To this end, Theorem 1 formally validates the above intuition for the k-connectivity property. It is also worth mentioning that we established Theorem 1 (see [29]) with a direct proof that does not rely on coupling arguments between random key graph and ER graph.

We now compare our results with those of Rybarczyk [19] for the k-connectivity of random key graph $G(n, K_n, P_n)$. As already noted, Rybarczyk [19, Remark 1, p. 5] has established an analog of Corollary 2, but under assumptions much *stronger* than ours. In particular, her result requires $P_n = \Theta\big(n^{\xi}\big)$ where $\xi > 1$. In comparison, Corollary 2 established here enforces only $P_n = \Omega(n)$, which is clearly a much weaker condition than $P_n = \Theta\big(n^{\xi}\big)$ with $\xi > 1$. More importantly, our condition

$P_n = \Omega(n)$ requires (from (19)) only $K_n = \Omega\big(\sqrt{\ln n}\big)$ for the one-law to hold; i.e., for $\mathbb{G}_{on}$ to be k-connected. However, the condition $P_n = \Theta\big(n^{\xi}\big)$ with $\xi > 1$ enforced in [19] requires the key ring sizes to satisfy $K_n = \Omega\big(\sqrt{n^{\xi-1}\ln n}\big)$ with $\xi-1 > 0$. This condition $K_n = \Omega\big(\sqrt{n^{\xi-1}\ln n}\big)$ not only constitutes a much stronger requirement than $K_n = \Omega\big(\sqrt{\ln n}\big)$, but it also renders the k-connectivity result given in [19] *not applicable* in the context of WSNs. This is because K_n controls the number of keys kept in each sensor's memory, and should be very small [10] due to limited memory and computational capability of sensor nodes; in general $K_n = O(\ln n)$ is accepted [5] as a reasonable bound on the key ring sizes.

Finally, we compare Theorem 1 with the zero-one law given by Yağan [24] for the 1-connectivity of $\mathbb{G}_{on}$. As mentioned in Section II above, he shows that if

$$p_e \sim c \cdot \frac{\ln n}{n} = \frac{\ln n + (c-1)\ln n}{n}, \tag{21}$$

then $\mathbb{G}_{on}$ is a.a.s. connected (resp., not connected) if $c > 1$ (resp., $c < 1$). This is done under the additional conditions that $P_n = \Omega(n)$ (required only for the one-law) and that $\lim_{n\to\infty} p_n \ln n$ exists (required only for the zero-law). On the other hand, Theorem 1 given here establishes (by setting $k = 1$) that, if

$$p_e = \frac{\ln n + \alpha_n}{n}, \tag{22}$$

then $\mathbb{G}_{on}$ is a.a.s. connected (resp., not connected) if $\lim_{n\to\infty} \alpha_n = \infty$ (resp., $\lim_{n\to\infty} \alpha_n = -\infty$). This result relies on the extra conditions $P_n = \Omega(n)$ and $\frac{K_n}{P_n} = o(1)$ for the one-law and on $\frac{K_n^2}{P_n} = o(1)$ for the zero-law.

Comparing (21) and (22), we see that our 1-connectivity result for $\mathbb{G}_{on}$ is somewhat more fine-grained than Yağan's [24]. This is because, a deviation of $\alpha_n = \pm\Omega(\ln n)$ is required to get the zero-one law in the form (21), whereas in our formulation (22), it suffices to have an unbounded deviation; e.g., even $\alpha_n = \pm \ln\ln\cdots\ln n$ will do. Put differently, we cover the case of $c = 1$ in (21) (i.e., the case when $p_e \sim \frac{\ln n}{n}$) and show that $\mathbb{G}_{on}$ could be a.a.s. connected or not connected, depending on the limit of α_n; in fact, if (21) holds with $c > 1$, we see from Theorem 1 that $\mathbb{G}_{on}$ is not only 1-connected but also k-connected for any $k = 1, 2, \ldots$. However, it is worth noting that the additional conditions assumed in [24] are *weaker* than those we enforce in Theorem 1 for $k = 1$.

Acknowledgements

This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the US Army Research Office and by the MURI grant W 911 NF 0710287 also from the US Army Research Office.

References

[1] F. Anjum. Location dependent key management using random key-predistribution in sensor networks. In *Proc. of ACM WiSe*, 2006.
[2] S. R. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16), 2009.
[3] S. R. Blackburn, D. R. Stinson, and J. Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Cryptology ePrint Archive, Report 2010/030, 2010. http://eprint.iacr.org/.
[4] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. of IEEE Symposium on Security and Privacy*, 2003.
[5] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Redoubtable sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(3):13:1–13:22, 2008.
[6] D. Dolev. The byzantine generals strike again. 1981.
[7] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *Proc. of INFOCOM*, 2004.
[8] P. Erdős and A. Rényi. On random graphs, I. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.
[9] P. Erdős and A. Rényi. On the strength of connectedness of random graphs. *Acta Math. Acad. Sci. Hungar*, pages 261–267, 1961.
[10] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of ACM CCS*, 2002.
[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5:11–25, October 2001.
[12] E. N. Gilbert. Random graphs. *The Annals of Mathematical Statistics*, 30:1141–1144, 1959.
[13] V. Gligor and P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In *Fast Software Encryption*, pages 92–108, 2001.
[14] V. Gligor, A. Perrig, and J. Zhao. Brief encounters with a random key graph. In *Proc. of the 17th Security Protocols Workshop (SPW 17)*, Cambridge, U.K, April 2009. Lecture Notes in Computer Science (LNCS), volume 7028. Springer Verlag.
[15] C. S. Jutla. Encryption modes with almost free message integrity. In *Proc. of Eurocrypt*, pages 529–544, 2001.
[16] P. Marbach. A lower-bound on the number of rankings required in recommender systems using collaborativ filtering. In *Proc. IEEE CISS*, 2008.
[17] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In *Proc. of ACM CCS*, pages 196–205, 2001.
[18] K. Rybarczyk. Diameter, connectivity and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311, 2011.
[19] K. Rybarczyk. Sharp threshold functions for the random intersection graph via a coupling method. *Electr. Journal of Combinatorics*, 18:36–47, 2011.
[20] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proc. of the 7th International Workshop on Security Protocols*, pages 172–194, 2000.
[21] X. Wang, X. Wang, and J. Zhao. Impact of mobility and heterogeneity on coverage and energy consumption in wireless sensor networks. In *Proc. of IEEE ICDCS*, pages 477–487, June 2011.
[22] O. Yağan. *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*. PhD thesis, Dept. of ECE, College Park (MD), June 2011. Available online at http://hdl.handle.net/1903/11910.
[23] O. Yağan and A. M. Makowski. On the existence of triangles in random key graphs. In *Proc. of 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2009)*, pages 1567 –1574, October 2009.
[24] O. Yağan. Performance of the Eschenauer-Gligor key distribution scheme under an on/off channel. *IEEE Transactions on Information Theory*, 58(6):3821–3835, June 2012.
[25] O. Yağan and A. M. Makowski. Random key graphs – can they be small worlds? In *Proc. of International Conference on Networks and Communications (NETCOM)*, pages 313 –318, December 2009.
[26] O. Yağan and A. M. Makowski. Zero-one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, May 2012.
[27] H. Zhang and S. Sundaram. Robustness of complex networks: Reaching consensus despite adversaries. *Arxiv*, February 2013. Available online at `arXiv:1203.6119 [cs.SI]`.
[28] J. Zhao and X. Wang. General connectivity in mobile wireless ad hoc network with infrastructure support. *Arxiv*, May 2013. Available online at `arXiv: 1305.2623 [cs.IT]`.
[29] J. Zhao, O. Yağan, and V. Gligor. 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]`.