Connectivity in Secure Wireless Sensor Networks under Transmission Constraints

Jun Zhao, Osman Yagan, and Virgil Gligor

March 3, 2014

CMU-CyLab-14-003

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Connectivity in Secure Wireless Sensor Networks under Transmission Constraints

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

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

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

***Abstract*—In wireless sensor networks (WSNs), the Eschenauer–Gligor (EG) key pre-distribution scheme is a widely recognized way to secure communications. Although the connectivity properties of secure WSNs with the EG scheme have been extensively investigated, few results address physical transmission constraints. These constraints reflect real–world implementations of WSNs in which two sensors have to be within a certain distance from each other to communicate. In this paper, we present *zero–one laws* for connectivity in WSNs employing the EG scheme under transmission constraints. These laws improve recent results [9], [10] significantly and help specify the *critical transmission ranges* for connectivity. Our analytical findings, which are also confirmed via numerical experiments, provide precise guidelines for the design of secure WSNs in practice. In addition to secure WSNs, our theoretical results are also applied to frequency hopping of wireless networks, as discussed in detail.**

***Keywords*—Connectivity, key predistribution, random graphs, security, transmission constraints, wireless sensor networks.**

I. Introduction

The Eschenauer–Gligor key pre-distribution scheme [6] is regarded as a typical approach to secure communications in wireless sensor networks (WSNs). In this scheme (referred to as the EG scheme hereafter), before sensors are deployed, each sensor is independently assigned the same number of distinct cryptographic keys selected uniformly at random from a common key pool. After deployment, any two sensors can securely communicate over an existing wireless link if and only if they share at least one key.

Connectivity in secure WSNs employing the EG scheme has been extensively studied in the literature [2], [9], [10], [16], [17], [24]. However, most existing research [2], [16], [17], [24] unrealistically assumes unconstrained sensor-to-sensor communications; i.e., any two sensors can communicate regardless of the distance between them. Recently, few results [9], [10] take transmission constraints into consideration, but do not provide zero–one laws for connectivity.

In this paper, we establish *zero–one laws* for connectivity in WSNs operating under the EG scheme with practical transmission constraints. We present significantly improved conditions for asymptotic connectivity over those of Krishnan *et al.* [9] and Krzywdziński and Rybarczyk [10], and also demonstrate that as the parameters move further away from these conditions, the network rapidly becomes asymptotically disconnected. Our results provide useful guidelines for dimensioning the EG scheme and adjusting sensor transmission power to ensure network connectivity. Moreover, our zero–one laws enable us to determine the *critical transmission ranges* for connectivity. Intuitively, as the transmission range surpasses (resp., falls below) the critical value and grows (resp., declines) further, the network immediately enters an asymptotically connected (resp., disconnected) state.

To model transmission constraints, we use the popular *disk model* [7], [11], [13], [19], in which each sensor's transmission area is a disk with the same radius; i.e., two sensors have to be within the radius distance to communicate directly. The network area in our analysis is either a torus or a square. The square accounts for the real–world *boundary effect* whereby some transmission region of a sensor close to the network boundary may fall outside of the network field. In contrast, the torus eliminates the boundary effect.

The rest of the paper is organized as follows. In Section II, we describe the system model. Section III presents the main results, leading to the discussion of critical transmission ranges in Section IV. Afterwards, we explain the basic ideas of the proofs in Section V. We provide numerical experiments in Section VI. In Section VII, we discuss the application of our results to frequency hopping. Section VIII reviews related work, and Section IX concludes the paper. The Appendix contains a few details of the proofs, while we explain the rest of them in the full version [1] of this paper.

II. System Model

In a WSN with size n and sensor set $\mathcal{V}=\{v_1,v_2,\ldots,v_n\}$, the EG scheme independently assigns a set of K_n distinct cryptographic keys, which are selected uniformly at random from a pool of P_n keys, to each sensor node. The set of keys of each sensor is called the key ring and is denoted by S_x for sensor v_x. The EG scheme is modeled by a *random key graph* [9], [16], [24], denoted by $G_{RKG}(n, K_n, P_n)$ in which an edge exists between two nodes[1] v_x and v_y if and only if they possess at least one common key; i.e., the event $[S_x \cap S_y \neq \emptyset]$, denoted by K_{xy}, holds. As for the sensor distribution, the same as much previous work [7], [9], [10], [19], we consider that the n nodes are independently and uniformly deployed in a network area $\mathcal{A}$.

[1] The terms sensor and node are interchangeable.

The disk model induces a *random geometric graph* [7], [9], [10], [13], [19], denoted by $G_{RGG}(n, r_n, \mathcal{A})$, in which an edge exists between two sensors if and only if their distance is no greater than r_n. In a secure WSN using the EG scheme under the disk model, two sensors v_x and v_y establish a link in between if and only if they share at least one key and are within distance r_n. We denote by E_{xy} the event that this link exists. If we let graph $G(n, \theta_n, \mathcal{A})$ model such a WSN, it is straightforward to see $G(n, \theta_n, \mathcal{A})$ is the intersection[2] of random key graph $G_{RKG}(n, K_n, P_n)$ and random geometric graph $G_{RGG}(n, r_n, \mathcal{A})$; namely,

$$G(n, \theta_n, \mathcal{A}) = G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A}),$$

where parameters K_n, P_n and r_n are together represented by θ_n. Also, if we let region $\mathcal{A}$ be either a torus $\mathcal{T}$ or a square $\mathcal{S}$, each with a unit area, we obtain the two graphs

$$G(n, \theta_n, \mathcal{T}) = G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{T}),$$

and

$$G(n, \theta_n, \mathcal{S}) = G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{S}).$$

We let p_s be the probability of key sharing between two sensors and note that p_s is also the edge probability in random key graph $G_{RKG}(n, K_n, P_n)$. It holds that $p_s = \mathbb{P}[K_{xy}] = \mathbb{P}[S_x \cap S_y \neq \emptyset]$. Clearly, if $P_n < 2K_n$, then $p_s = 1$. If $P_n \geq 2K_n$, as shown in previous work [2], [16], [24], we have $p_s = 1 - \binom{P_n - K_n}{K_n} / \binom{P_n}{K_n}$. By [27, Lemma 8], if[3] ${K_n}^2/P_n = o(1)$, then

$$p_s = {K_n}^2/P_n \cdot \left[1 \pm O\big({K_n}^2/P_n\big)\right] \sim {K_n}^2/P_n. \quad (1)$$

We will frequently use (1) throughout the paper.

Let p_e be the probability that a link exists between two sensors in the WSN modeled by graph $G(n, \theta_n, \mathcal{A})$; i.e., p_e is the edge probability in $G(n, \theta_n, \mathcal{A})$. It holds that $p_e = \mathbb{P}[E_{xy}]$. When $\mathcal{A}$ is the torus $\mathcal{T}$, clearly p_e equals $\pi {r_n}^2 \cdot p_s$; and if ${K_n}^2/P_n = o(1)$, then $p_e \sim \pi {r_n}^2 \cdot {K_n}^2/P_n$ by (1). When $\mathcal{A}$ is the square $\mathcal{S}$, it is a simple matter to show $p_e \geq (1 - 2r_n)^2 \cdot \pi {r_n}^2 \cdot p_s$ (with $r_n \leq \frac{1}{2}$) and $p_e \leq \pi {r_n}^2 \cdot p_s$. The reason is that for the position of v_x satisfying the condition that v_x's distance to all four edges of $\mathcal{S}$ are at least $2r_n$ with $r_n \leq \frac{1}{2}$, given the position of v_x, the probability that v_y falls in v_x's transmission area is $\pi {r_n}^2$; and for the position of v_x not satisfying the above condition, the probability that v_y falls in v_x's transmission area is upper bounded by $\pi {r_n}^2$. Then on $\mathcal{S}$, it holds that $p_e \sim \pi {r_n}^2 \cdot p_s$ if $r_n = o(1)$ (note that $r_n = o(1)$ implies $r_n \leq \frac{1}{2}$ for all n sufficiently large). Therefore, on $\mathcal{S}$, if $r_n = o(1)$ and ${K_n}^2/P_n = o(1)$, we further obtain $p_e \sim \pi {r_n}^2 \cdot {K_n}^2/P_n$ in view of (1).

III. The Main Results

We detail the main results below. The notation "ln" stands for the natural logarithm function.

A. Connectivity in a Secure WSN on a Unit Torus

Theorem 1 presents a zero–one law for connectivity in $G(n, \theta_n, \mathcal{T})$, which models a secure WSN working under the EG scheme and the disk model on the unit torus $\mathcal{T}$.

Theorem 1. *For graph $G(n, \theta_n, \mathcal{T})$ as the intersection of random key graph $G_{RKG}(n, K_n, P_n)$ and random geometric graph $G_{RGG}(n, r_n, \mathcal{T})$ on a unit torus $\mathcal{T}$, if $K_n = \omega(\ln n)$, $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$, $\frac{K_n}{P_n} = o\big(\frac{1}{n}\big)$ and*

$$\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n} \sim a \cdot \frac{\ln n}{n} \quad (2)$$

for some positive constant a, then

$$\lim_{n \to \infty} \mathbb{P}\left[\, G(n, \theta_n, \mathcal{T}) \textit{ is connected.} \,\right] = \begin{cases} 0, & \textit{if } a < 1, \\ 1, & \textit{if } a > 1. \end{cases}$$

Remark 1. *In Theorem 1, we have $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big) = o(1)$, under which we know from Section II that $\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n}$ in (2) asymptotically equals the edge probability in graph $G(n, \theta_n, \mathcal{T})$.*

B. Connectivity in a Secure WSN on a Unit Square

Theorem 2 gives a zero–one law for connectivity in $G(n, \theta_n, \mathcal{S})$, which models a secure WSN working under the EG scheme and the disk model on the unit square $\mathcal{S}$.

Theorem 2. *For graph $G(n, \theta_n, \mathcal{S})$ as the intersection of random key graph $G_{RKG}(n, K_n, P_n)$ and random geometric graph $G_{RGG}(n, r_n, \mathcal{S})$ on a unit square $\mathcal{S}$, if $K_n = \omega(\ln n)$, $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$, $\frac{K_n}{P_n} = o\big(\frac{1}{n}\big)$ and*

$$\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n} = \begin{cases} b \cdot \dfrac{\ln \frac{n P_n}{{K_n}^2}}{n}, & \textit{for } \dfrac{{K_n}^2}{P_n} = \omega\Big(\dfrac{1}{n^{1/3} \ln n}\Big), \\ b \cdot \dfrac{4 \ln \frac{P_n}{{K_n}^2}}{n}, & \textit{for } \dfrac{{K_n}^2}{P_n} = O\Big(\dfrac{1}{n^{1/3} \ln n}\Big), \end{cases} \quad (4)$$

for some positive constant b, where $\frac{{K_n}^2}{P_n} \cdot n^{1/3} \ln n$ is assumed either bounded for all n or converging to ∞ as $n \to \infty$, then

$$\lim_{n \to \infty} \mathbb{P}\left[\, G(n, \theta_n, \mathcal{S}) \textit{ is connected.} \,\right] = \begin{cases} 0, & \textit{if } b < 1, \\ 1, & \textit{if } b > 1. \end{cases}$$

Remark 2. *In Theorem 2, we explain $r_n = o(1)$ as follows. From condition $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, then for all n sufficiently large, $\frac{{K_n}^2}{P_n} < 1$ holds and $\ln \frac{P_n}{{K_n}^2}$ is positive. Under condition $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$, it further holds that $\ln \frac{P_n}{{K_n}^2} = O(\ln n)$, which is used in (4) to yield $\frac{{K_n}^2}{P_n} \cdot \pi {r_n}^2 = \Theta\big(\frac{\ln n}{n}\big)$, leading to $r_n = o(1)$ given $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$. Finally, as given in Section II, $\frac{{K_n}^2}{P_n} = o(1)$ and $r_n = o(1)$ together result in the asymptotic equivalence between $\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n}$ and the edge probability in graph $G(n, \theta_n, \mathcal{S})$.*

We explain that the conditions in Theorems 1 and 2 are

[2] Graphs in this paper are all undirected. With two graphs G_1 and G_2 defined on the same vertex set, two vertices have an edge in between in $G_1 \cap G_2$ if and only if these two vertices have an edge in G_1 and also have an edge in G_2.

[3] We use the standard Landau asymptotic notation $o(\cdot), O(\cdot), \omega(\cdot), \Omega(\cdot), \Theta(\cdot)$ and $\sim$; in particular, for two sequences f_n and g_n, the relation $f_n \sim g_n$ means $\lim_{n \to \infty} f_n/g_n = 1$.

practical for sensor networks. Recall that n is the number of sensors, the key ring size K_n controls the number of keys in each sensor's memory and P_n is the key pool size. As noted in previous work [4], [6], [21], in real-world implementations of sensor networks, K_n is often larger than $\ln n$ as well as being several orders of magnitude smaller than P_n and n due to limited memory and computational capability of sensors, and P_n is larger than n. Therefore, conditions $K_n = \omega(\ln n)$, $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$ and $\frac{K_n}{P_n} = o\big(\frac{1}{n}\big)$ are all practical.

Connectivity results with more fine-grained scalings for graphs $G(n, \theta_n, \mathcal{T})$ and $G(n, \theta_n, \mathcal{S})$ are provided in the full version [1] of this paper. In particular, the results therein cover the case of $a = 1$ in Theorem 1 and the case of $b = 1$ in Theorem 2, respectively.

IV. Critical Transmission Ranges

We follow the standard definition of critical transmission range in wireless network [11], [19], [20]. Specifically, for a network with topology modeled by graph $\mathcal{G}(r_n)$ with r_n as the transmission range, $r_n^\star$ is said to be the critical transmission range if (i) and (ii) below both hold:

(i) $\lim_{n\to\infty} \mathbb{P}\left[\,\mathcal{G}(cr_n^\star) \text{ is connected.}\,\right] = 0$ for any positive constant $c < 1$, and

(ii) $\lim_{n\to\infty} \mathbb{P}\left[\,\mathcal{G}(cr_n^\star) \text{ is connected.}\,\right] = 1$ for any constant $c > 1$.

A. The Critical Transmission Range for Connectivity in a Secure WSN on a Unit Torus

By Theorem 1, we determine the critical transmission range $r_n^\star(\mathcal{T})$ for connectivity in a secure WSN on a unit torus modeled by graph $G(n, \theta_n, \mathcal{T})$ through

$$\pi\left[r_n^\star(\mathcal{T})\right]^2 \cdot \frac{{K_n}^2}{P_n} = \frac{\ln n}{n},$$

inducing the following expression of $r_n^\star(\mathcal{T})$:

$$r_n^\star(\mathcal{T}) = \sqrt{\frac{\ln n}{\pi n} \cdot \frac{P_n}{{K_n}^2}}. \tag{5}$$

By (5), it is clear that with n fixed, $r_n^\star(\mathcal{T})$ decreases as $\frac{{K_n}^2}{P_n}$ increases. This is expected since as mentioned in Remark 1 after Theorem 1, $\frac{{K_n}^2}{P_n}$ asymptotically equals the probability that two sensors share at least one key; and $\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n}$ asymptotically equals the edge probability in $G(n, \theta_n, \mathcal{T})$. As the probability of key sharing increases, sensors can reduce their transmission ranges to maintain network connectivity.

Along with (5), condition $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$ in Theorem 1 leads to $r_n^\star(\mathcal{T}) = o(1)$. This is anticipated as the node density n grows to ∞.

B. The Critical Transmission Range for Connectivity in a Secure WSN on a Unit Square

By Theorem 2, we determine the critical transmission range $r_n^\star(\mathcal{S})$ for connectivity in a secure WSN on a unit square modeled by graph $G(n, \theta_n, \mathcal{S})$ through

$$\pi\left[r_n^\star(\mathcal{S})\right]^2 \cdot \frac{{K_n}^2}{P_n} = \begin{cases} \dfrac{\ln \frac{nP_n}{{K_n}^2}}{n}, & \text{for } \frac{{K_n}^2}{P_n} = \omega\Big(\frac{1}{n^{1/3}\ln n}\Big), \\[2ex] \dfrac{4\ln \frac{P_n}{{K_n}^2}}{n}, & \text{for } \frac{{K_n}^2}{P_n} = O\Big(\frac{1}{n^{1/3}\ln n}\Big), \end{cases} \tag{6}$$

so $r_n^\star(\mathcal{S})$ is specified by

$$r_n^\star(\mathcal{S}) = \begin{cases} \sqrt{\dfrac{\ln \frac{nP_n}{{K_n}^2}}{\frac{\pi n {K_n}^2}{P_n}}}, & \text{for } \frac{{K_n}^2}{P_n} = \omega\Big(\frac{1}{n^{1/3}\ln n}\Big), \\[3ex] 2\sqrt{\dfrac{\ln \frac{P_n}{{K_n}^2}}{\frac{\pi n {K_n}^2}{P_n}}}, & \text{for } \frac{{K_n}^2}{P_n} = O\Big(\frac{1}{n^{1/3}\ln n}\Big). \end{cases} \tag{7}$$

First, by (7), the critical transmission range $r_n^\star(\mathcal{S})$ decreases as $\frac{{K_n}^2}{P_n}$ increases. Similar to the discussion on $r_n^\star(\mathcal{T})$, this is also expected in that as the probability $\frac{{K_n}^2}{P_n}$ of key sharing increases, sensors can reduce their transmission ranges to maintain network connectivity.

Second, similar to Remark 2, $\frac{{K_n}^2}{P_n} = \omega\big(\frac{\ln n}{n}\big)$ and (7) imply $r_n^\star(\mathcal{S}) = o(1)$.

Third, we relate the critical transmission ranges of the unit square $\mathcal{S}$ and torus $\mathcal{T}$, namely $r_n^\star(\mathcal{S}) \geq r_n^\star(\mathcal{T})$ for all n sufficiently large. Intuitively, this relationships is caused by the boundary effects of $\mathcal{S}$. Specifically, two sensors close to opposite edges of the square may be unable to establish a link on the square $\mathcal{S}$ but may have a link in between on the torus $\mathcal{T}$ because of possible wrap-around connections on the torus. In view of (5) and (7), for $\frac{{K_n}^2}{P_n} = \omega\left(\frac{1}{n^{1/3}\ln n}\right)$, it is clear that for all n sufficiently large, $r_n^\star(\mathcal{S}) \geq r_n^\star(\mathcal{T})$ due to $\frac{\ln \frac{P_n}{{K_n}^2}}{n} \geq 0$, which follows from condition $\frac{{K_n}^2}{P_n} = o(1)$ in Theorem 2. For $\frac{{K_n}^2}{P_n} = O\left(\frac{1}{n^{1/3}\ln n}\right)$, it follows that $4\frac{\ln \frac{P_n}{{K_n}^2}}{n} \geq 4\ln(n^{1/3}\ln n) \geq \ln n$ for all n sufficiently large, so that $r_n^\star(\mathcal{S}) \geq r_n^\star(\mathcal{T})$ for all n sufficiently large.

Fourth, we compute $\lim\limits_{n\to\infty}\left\{\pi\left[r_n^\star(\mathcal{S})\right]^2 \cdot \frac{{K_n}^2}{P_n} \big/ \big(\frac{\ln n}{n}\big)\right\}$ based on (7). This will enable us to compare our results with the best known to date (viz., Section VIII), where the upper bounds on $\lim\limits_{n\to\infty}\left\{\pi\left[r_n^\star(\mathcal{S})\right]^2 \cdot \frac{{K_n}^2}{P_n} \big/ \big(\frac{\ln n}{n}\big)\right\}$ are 8 and 2π, respectively [9], [10]. By (7), it is clear that

$$\begin{aligned} &\lim_{n\to\infty}\left\{\left[\pi\left[r_n^\star(\mathcal{S})\right]^2 \cdot \frac{{K_n}^2}{P_n}\right] \Big/ \left(\frac{\ln n}{n}\right)\right\} \\ &= \begin{cases} 1 + \lim\limits_{n\to\infty}\Big(\ln \frac{P_n}{{K_n}^2} \Big/ \ln n\Big), & \text{for } \frac{{K_n}^2}{P_n} = \omega\Big(\frac{1}{n^{1/3}\ln n}\Big), \\ 4\lim\limits_{n\to\infty}\Big(\ln \frac{P_n}{{K_n}^2} \Big/ \ln n\Big), & \text{for } \frac{{K_n}^2}{P_n} = O\Big(\frac{1}{n^{1/3}\ln n}\Big). \end{cases} \end{aligned} \tag{8}$$

From (8), we observe a phase transition of $r_n^\star(\mathcal{S})$ when $\frac{{K_n}^2}{P_n}$ is of the order of $\frac{1}{n^{1/3}\ln n}$. Note that by (5), there is no such phase transition for the critical range $r_n^\star(\mathcal{T})$ of a torus $\mathcal{T}$. The intuition is that, in integrating all possible points in the network region $\mathcal{A}$ to compute the expected number of isolated nodes, for $\mathcal{A}$ being the square $\mathcal{S}$ with the boundary effect, different areas on contribute the dominant part of the integral as $\frac{{K_n}^2}{P_n} \cdot n^{1/3} \ln n$ vary from unbounded to bounded, while $\mathcal{A}$ being the torus $\mathcal{T}$, there is no such phenomenon in the absence of boundary effect.

V. Basic Ideas for the Proofs

A. Zero-Laws by Evaluating Minimum Node Degree

1) Poissonization and de-Poissonization: We demonstrate the zero–laws using the standard Poissonization technique [13]. The idea is that the zero–law for graph $G(n, \theta_n, \mathcal{A})$ follows once we establish the same result for its Poissonized version, graph $G_{\text{Poisson}}(n, \theta_n, \mathcal{A})$, where the only difference between $G_{\text{Poisson}}(n, \theta_n, \mathcal{A})$ and $G(n, \theta_n, \mathcal{A})$ is that the node distribution of the former is a homogeneous Poisson point process with intensity n on $\mathcal{A}$ while that of the latter is a uniform n-point process. The details are proved in the full version [1].

2) Relationship between connectivity and the absence of isolated nodes: Clearly, for a graph, its connectivity implies the absence of isolated nodes. Hence, for graph $G_{\text{Poisson}}(n, \theta_n, \mathcal{A})$, to prove the zero-law of connectivity, it suffices to show the corresponding zero-law for the the absence of isolated nodes.

3) Method of the moments: For graph $G_{\text{Poisson}}(n, \theta_n, \mathcal{A})$, to demonstrate the zero-law for the the absence of isolated nodes, we use the method of the moments. By [27, Fact 1 and Lemma 1], with I_x denoting the event that node v_x is isolated, the proof is completed once we establish

$$\lim_{n\to\infty} n\mathbb{P}[I_x] = \infty, \tag{9}$$

and

$$\mathbb{P}[I_x \cap I_y] \leq \big\{\mathbb{P}[I_x]\big\}^2 \cdot [1 + o(1)]. \tag{10}$$

To prove (9) and (10), we present Lemma 1 which evaluates $\mathbb{P}[I_x]$ and $\mathbb{P}[I_x \cap I_y]$. For $\mathcal{A}$ being the unit torus $\mathcal{T}$, the details of establishing (9) and (10) are given in the Appendix. The proofs of (9) and (10) in the case of $\mathcal{A}$ being the unit square $\mathcal{S}$, as well as the proof of Lemma 1, are provided in the full paper [1].

Lemma 1. *In graph $G_{\textit{Poisson}}(n, \theta_n, \mathcal{A})$, let I_x be the event that node v_x is isolated, and $D_{r_n}(\hat{v_x})$ be the intersection of $\mathcal{A}$ and the disk centered at position $\hat{v_x} \in \mathcal{A}$ with radius r_n. We have*

$$\mathbb{P}[I_x] = \int_{\mathcal{A}} e^{-np_s|D_{r_n}(\hat{v_x})|}\, d\hat{v_x}; \tag{11}$$

and with ϕ_u denoting $\mathbb{P}\big[K_{xj} \cap K_{yj} \mid (|S_{xy}| = u)\big]$, where $u = 0, 1, \ldots, K_n$, then for $u = 1, 2, \ldots, K_n$,

$$\mathbb{P}\big[I_x \cap I_y \mid (|S_{xy}| = u)\big] = \int_{\mathcal{A}} \int_{\mathcal{A}\setminus D_{r_n}(\hat{v_x})} e^{-n\{p_s|D_{r_n}(\hat{v_x})| + p_s|D_{r_n}(\hat{v_y})| - \phi_u|D_{r_n}(\hat{v_x}) \cap D_{r_n}(\hat{v_y})|\}}\, d\hat{v_x} d\hat{v_y}, \tag{12}$$

and

$$\mathbb{P}\big[I_x \cap I_y \mid (|S_{xy}| = 0)\big] = \int_{\mathcal{A}} \int_{\mathcal{A}} e^{-n\{p_s|D_{r_n}(\hat{v_x})| + p_s|D_{r_n}(\hat{v_y})| - \phi_0|D_{r_n}(\hat{v_x}) \cap D_{r_n}(\hat{v_y})|\}}\, d\hat{v_x} d\hat{v_y}, \tag{13}$$

with ϕ_0 meaning ϕ_u when $u = 0$.

B. One-Laws by the Analogy between Random Graphs

To prove the one–laws, we relate graph $G(n, \theta_n, \mathcal{A})$ (i.e., $G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A})$) to the intersection of an Erdős-Rényi graph [5] and the random geometric graph $G_{RGG}(n, r_n, \mathcal{A})$, where an Erdős–Rényi graph $G_{ER}(n, p_n)$ is defined on a set of n nodes such that any two nodes establish an edge in between independently with probability p_n. As already observed in the literature [2], [16], [17], [24], random key graph $G_{RKG}(n, K_n, P_n)$ and Erdős-Rényi graph $G_{ER}(n, p_n)$ have similar connectivity properties when they are *matched* through edge probabilities asymptotically. However, these two graphs have vastly different behaviors for clustering coefficient and number of triangles [22], [23]. Hence, the approach of exploiting the analogy between $G_{RKG}(n, K_n, P_n)$ and $G_{ER}(n, p_n)$ (and the analogy between their respective intersections with $G_{RGG}(n, r_n, \mathcal{A})$) needs rigorous arguments. Our Lemma 2 below involves rigorous reasoning and is detailed in Appendix C.

Lemma 2. *If $K_n = \omega\left(\ln n\right)$, $\frac{K_n}{P_n} = o\big(\frac{1}{n}\big)$ and $\frac{{K_n}^2}{P_n} = o(1)$, then there exists p_n with*

$$p_n = \frac{{K_n}^2}{P_n} \cdot [1 - o(1)] \tag{14}$$

such that for any topology $\mathcal{A}$ and any monotone increasing graph property[4] $\mathscr{P}$,

$$\begin{aligned}&\mathbb{P}[\, G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A}) \textit{ has } \mathscr{P}.\,] \\ &\quad \geq \mathbb{P}[\, G_{ER}(n, p_n) \cap G_{RGG}(n, r_n, \mathcal{A}) \textit{ has } \mathscr{P}.\,] - o(1).\end{aligned}$$

Lemmas 3 and 4 below present zero–one laws for connectivity in graphs $G_{ER}(n, p_n) \cap G_{RGG}(n, r_n, \mathcal{T})$ and $G_{ER}(n, p_n) \cap G_{RGG}(n, r_n, \mathcal{S})$, respectively, which are based on results recently established by Penrose [14]. Their proofs are straightforward from [14, Theorem 2.3] and [14, Theorem 2.5 and Proposition 8.5], respectively; see the full version [1] of this paper for the explanations. Since connectivity in a monotone property, it is clear to derive the one-laws in Theorems by Lemmas 2, 3 and 4.

Lemma 3 (An implication of [14, Theorem 2.3])**.** *Consider the intersection of Erdős–Rényi graph $G_{ER}(n, p_n)$ and random geometric graph $G_{RGG}(n, r_n, \mathcal{T})$. If*

$$\pi {r_n}^2 p_n \sim c \cdot \frac{\ln n}{n} \tag{15}$$

[4] A graph property is called monotone increasing if it holds under the addition of edges in a graph.

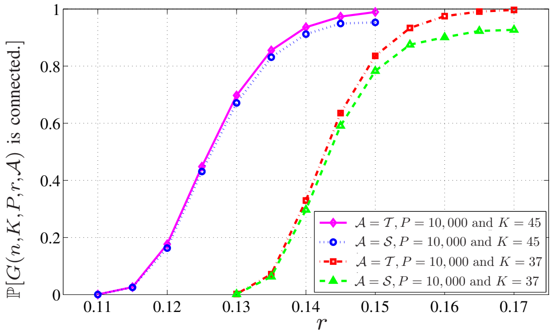

Fig. 1. A plot of the empirical probability that graph $G(n, K, P, r, \mathcal{A})$ (i.e., $G(n, \theta, \mathcal{A})$) is connected as a function of r with $n = 2,000$, where $\mathcal{A}$ is either the unit torus $\mathcal{T}$ or the unit square $\mathcal{S}$.

for some positive constant c, then

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l} G_{ER}(n,p_n) \\ \cap\, G_{RGG}(n,r_n,\mathcal{T}) \\ \textit{is connected.}\end{array}\right] = \begin{cases} 0, & \textit{if } c < 1, \\ 1, & \textit{if } c > 1. \end{cases} \tag{16}$$

Lemma 4 (An implication of [14, Theorem 2.5 and Proposition 8.5])**.** *Consider the intersection of Erdős–Rényi graph $G_{ER}(n, p_n)$ and random geometric graph $G_{RGG}(n, r_n, \mathcal{S})$. If*

$$\pi {r_n}^2 p_n = \begin{cases} d \cdot \frac{\ln \frac{n}{p_n}}{n}, & \textit{for } p_n = \omega\left(\frac{1}{n^{1/3}\ln n}\right), \\ d \cdot \frac{4\ln \frac{1}{p_n}}{n}, & \textit{for } p_n = O\left(\frac{1}{n^{1/3}\ln n}\right), \end{cases} \tag{17}$$

for some positive constant d, then

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l} G_{ER}(n,p_n) \\ \cap\, G_{RGG}(n,r_n,\mathcal{S}) \\ \textit{is connected.}\end{array}\right] = \begin{cases} 0, & \textit{if } d < 1, \\ 1, & \textit{if } d > 1. \end{cases}$$

VI. Numerical Experiments

We present numerical simulation in the non-asymptotic regime to support our asymptotic results. We write graph $G(n, \theta_n, \mathcal{A})$ as $G(n, K_n, P_n, r_n, \mathcal{A})$. In Figure 1, we depict the probability that graph $G(n, K, P, r, \mathcal{A})$ (i.e., $G(n, \theta, \mathcal{A})$) is connected, where $\mathcal{A}$ is either the unit torus $\mathcal{T}$ or the unit square $\mathcal{S}$; and the subscript n is removed since we fix the number of nodes at $n = 2,000$ in all experiments. For each pair $(\mathcal{A}, K, P, r)$, we generate 500 independent samples of $G(n, K, P, r, \mathcal{A})$ and count the number of times that the obtained graphs are connected. Then the count divided by 500 becomes the empirical probability for connectivity. As illustrated, we observe the evident threshold behavior in the probability that $G(n, K, P, r, \mathcal{A})$ is connected as such probability transitions from zero to one as r varies slightly from a certain value.

VII. Application in Frequency Hopping

Frequency hopping is a classic approach for transmitting wireless signals by switching a carrier among different frequency channels. Frequency hopping offers improved communication resistance to narrowband interference, jamming attacks, and signal interception by eavesdroppers. It also enables more efficient bandwidth utilization than fixed-frequency transmission [8]. For these reasons, military radio systems, such as `HAVE QUICK` and `SINCGARS` [12], use frequency hopping extensively. A typical method of implementing frequency hopping is for the sender and receiver to first agree on a *secret seed* and a *pseudorandom number generator* (PRNG). Then the seed is input to the PRNG by both the sender and the receiver to produce a sequence of pseudo-random frequencies, each of which is used for communication in a time interval [8].

We consider a wireless network of n nodes where nodes establish shared secret seeds for frequency hopping as follows. Each node uniformly and independently selects K_n secret seeds out of a *secret pool* consisting of P_n secret seeds. Two nodes can communicate with each other via frequency hopping if and only if they share at least one secret seed *and* are within each other's transmission range. Two nodes can derive a *unique* seed from the shared seeds in several ways. For example, the unique seed could be the cryptographic hash of the concatenated seeds shared between two nodes [4]. Alternately, if two nodes u and v share a seed k_{uv} (which might also be shared by other pairs of nodes), they can establish a probabilistically unique secret seed $H(u, v, k_{uv})$, where the two node identities are ordered and H is an entropy-preserving cryptographic hash function.

The above way of bootstrapping seeds has the following advantages. First, without knowledge of a PRNG seed, an adversary cannot predict in advance the frequency that two nodes will use. In addition, each communicating pair of nodes can generate a secret seed that differs from the seed that another nearby node pair uses. Then it is also likely that distinct communicating node pairs located in the same vicinity utilize different frequencies. Thus, without any additional coordination protocol to avoid using the same frequency, distinct communicating node pairs nearby could work simultaneously without causing co-channel interference.

Now we construct a graph G_f based on the above scenario. Each of the n wireless nodes represents a node in G_f. There exists an edge between two nodes in G_f if and only if they can communicate with each other via frequency hopping; i.e., they share a secret seed and are in communication range with each other. Therefore, if all n nodes are uniformly and independently deployed in a network area $\mathcal{A}$, which is either a unit torus $\mathcal{T}$ or a unit square $\mathcal{S}$, and all nodes have the same transmission range r_n, then G_f is exactly $G(n, \theta_n, \mathcal{T})$ when $\mathcal{A} = \mathcal{T}$ and $G(n, \theta_n, \mathcal{S})$ when $\mathcal{A} = \mathcal{S}$. Our zero–one laws on connectivity of $G(n, \theta_n, \mathcal{T})$ and $G(n, \theta_n, \mathcal{S})$, allow us to find the network parameters under which G_f is connected. This provides useful guideline for the design of large-scale wireless networks with frequency hopping.

VIII. Related Work

Yi [25] *et al.* consider graph $G(n, \theta_n, \mathcal{A})$, where the network region $\mathcal{A}$ is either a disk $\mathcal{D}$ or a square $\mathcal{S}$, each of unit area. They show that for graph $G(n, \theta_n, \mathcal{D})$ or $G(n, \theta_n, \mathcal{S})$, if $\pi {r_n}^2 \cdot \frac{{K_n}^2}{P_n} = \frac{\ln n + \alpha}{n}$ and $\frac{{K_n}^2}{P_n} = \omega\left(\frac{1}{\ln n}\right)$, the number of isolated nodes asymptotically follows a Poisson distribution with mean $e^{-\alpha}$. Pishro-Nik *et al.* [15] also obtain such result on asymptotic Poisson distribution with condition $\frac{{K_n}^2}{P_n} = \omega\left(\frac{1}{\ln n}\right)$ generalized to $\frac{{K_n}^2}{P_n} = \Omega\left(\frac{1}{\ln n}\right)$. In practical

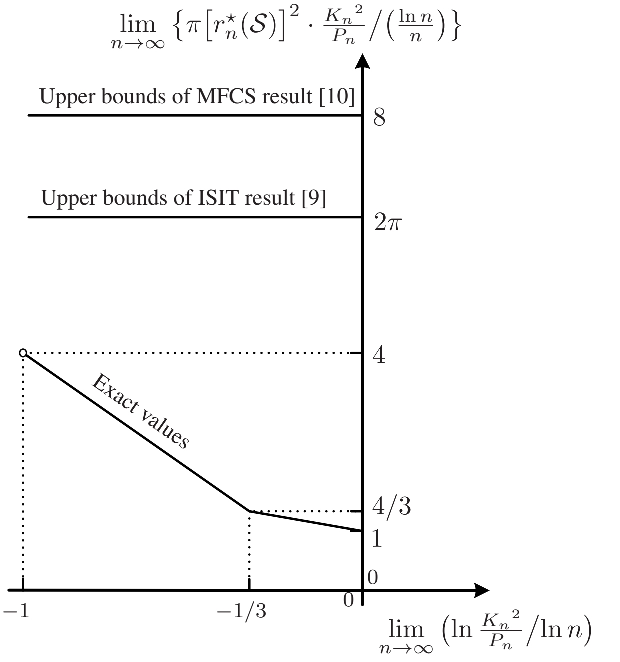

Fig. 2. A comparison of the connectivity results for graph $G(n,\theta_n,\mathcal{S})$, the intersection of random key graph $G_{RKG}(n,K_n,P_n)$ and random geometric graph $G_{RGG}(n,r_n,\mathcal{A})$, where $r_n^\star(\mathcal{S})$ is the critical transmission range for connectivity in $G(n,\theta_n,\mathcal{S})$.

WSNs, K_n is expected to be several orders of magnitude smaller than P_n [4], [6], [21], so it often holds that $\frac{K_n{}^2}{P_n}=o\big(\frac{1}{\ln n}\big)$, which is not addressed in the two work above [15], [25] and is addressed in our theorems. Recently, for graph $G(n,\theta_n,\mathcal{S})$, Krzywdziński and Rybarczyk [10] and Krishnan *et al.* [9] obtain connectivity results, covering the case of $\frac{K_n{}^2}{P_n}=o\big(\frac{1}{\ln n}\big)$. We elaborate their theoretical findings below and explain that our results significantly improve theirs. Krzywdziński and Rybarczyk [10] present that in $G(n,\theta_n,\mathcal{S})$ on $\mathcal{S}$, if $\pi r_n{}^2\cdot\frac{K_n{}^2}{P_n}\geq\frac{8\ln n}{n}$ with $K_n\geq 2$ and $P_n=\omega(1)$, then $G(n,\theta_n,\mathcal{S})$ is almost surely[5] connected. Krishnan *et al.* [9] demonstrate that if $\pi r_n{}^2\cdot\frac{K_n{}^2}{P_n}\geq\frac{2\pi\ln n}{n}$ with $K_n=\omega(1)$ and $\frac{K_n{}^2}{P_n}=o(1)$, then $G(n,\theta_n,\mathcal{S})$ is almost surely connected. Both only provide upper bounds on $\lim_{n\to\infty}\left\{\pi\big[r_n^\star(\mathcal{S})\big]^2\cdot\frac{K_n{}^2}{P_n}\big/\big(\frac{\ln n}{n}\big)\right\}$, with one being 8 and the other being 2π, where $r_n^\star(\mathcal{S})$ is the critical transmission range for connectivity in $G(n,\theta_n,\mathcal{S})$. In this paper, we determine the exact value of this limit by deriving $r_n^\star(\mathcal{S})$. As illustrated in Figure 2, we plot the term $\lim_{n\to\infty}\left\{\pi\big[r_n^\star(\mathcal{S})\big]^2\cdot\frac{K_n{}^2}{P_n}\big/\big(\frac{\ln n}{n}\big)\right\}$ with respect to $\lim_{n\to\infty}\big(\ln\frac{K_n{}^2}{P_n}/\ln n\big)$. The curve of the exact values is based on our result (8) in Section IV.

For random key graph $G_{RKG}(n,K_n,P_n)$, Blackburn and Gerke [2], Rybarczyk [16], and Yağan and Makowski [24] establish zero–one laws for its connectivity. In particular, Rybarczyk's result is that with $K_n\geq 2$ for all n sufficiently large and $\frac{K_n{}^2}{P_n}=\frac{\ln n+\alpha_n}{n}$, graph $G_{RKG}(n,K_n,P_n)$ is almost surely connected (resp., disconnected) if $\lim_{n\to\infty}\alpha_n=\infty$ (resp., $\lim_{n\to\infty}\alpha_n=-\infty$). Rybarczyk [17] also shows zero–one laws for k-connectivity, where k-connectivity means that the graph remains connected despite the removal of any $(k-1)$ nodes.

Random geometric graph $G_{RGG}(n,r_n,\mathcal{A})$ has been widely studied due to its application to wireless networks. Gupta and Kumar [7] show that when $\mathcal{A}$ is a unit-area disk $\mathcal{D}$ and $\pi r_n{}^2=\frac{\ln n+\alpha_n}{n}$, $G_{RGG}(n,r_n,\mathcal{D})$ is almost surely connected if and only if $\lim_{n\to\infty}\alpha_n=\infty$. Penrose [13] explores k-connectivity in $G_{RGG}(n,r,\mathcal{A})$, where $\mathcal{A}$ is a d-dimensional unit cube with $d\geq 2$. For $\mathcal{A}$ being the unit torus $\mathcal{T}$, he obtains that with ρ_n denoting the minimum r_n to ensure k-connectivity in $G_{RGG}(n,r_n,\mathcal{T})$, where $k\geq 1$, then the probability that $\pi\rho_n{}^2$ is at most $\ln n+(k-1)\ln\ln n-\ln[(k-1)!]+\alpha$ asymptotically converges to $e^{-e^{-\alpha}}$. Li *et al.* [11] prove that with $k\geq 2$, to have graph $G_{RGG}(n,r,\mathcal{S})$ asymptotically k-connected with probability at least $e^{-e^{-\alpha}}$ for some α, a sufficient condition is that the term $\pi r_n{}^2$ is at least $\ln n+(2k-3)\ln\ln n-2\ln[(k-1)!]+2\alpha$; and a necessary condition is that $\pi r_n{}^2$ is no less than $\ln n+(k-1)\ln\ln n-\ln[(k-1)!]+\alpha$. For $k\geq 2$, Wan *et al.* [19] determine the exact formula of r_n such that graph $G_{RGG}(n,r,\mathcal{S})$ or $G_{RGG}(n,r_n,\mathcal{D})$ is asymptotically k-connected with probability $e^{-e^{-\alpha}}$, where as noted above, $\mathcal{D}$ is a disk of unit area.

In addition to the intersection of random key graphs and random geometric graphs in this work and papers [9], [10], [15], [25], and the intersection of Erdős–Rényi graphs and random geometric graphs [9], [10], [14], [15], [26], other kinds of random graph intersections have recently investigated in several work by the authors [21], [27]–[29].

IX. Conclusion

We establish zero–one laws for connectivity in secure wireless sensor networks employing the widely-used Eschenauer–Gligor key pre-distribution scheme under transmission constraints. Such zero–one laws significantly improve recent results [9], [10] in the literature. Our theoretical findings are confirmed via numerical experiments, and are applied to frequency hopping of wireless networks.

References

[1] J. Zhao, O. Yağan, and V. Gligor. Connectivity in secure wireless sensor networks under transmission constraints. 2014. Available online at `http://www.andrew.cmu.edu/user/junzhao/EG.pdf`

[2] S. R. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16), August 2009.

[3] M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Netw.*, 53:19–26, January 2009.

[4] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. IEEE Symposium on Security and Privacy*, May 2003.

[5] P. Erdős and A. Rényi. On random graphs, I. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.

[6] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *Proc. ACM CCS*, 2002.

[7] P. Gupta and P. R. Kumar. Critical power for asymptotic connectivity in wireless networks. In *Proc. IEEE CDC*, pages 547–566, 1998.

[8] D. Herrick, P. Lee, and L. Ledlow. Correlated frequency hopping-an improved approach to HF spread spectrum communications. In *Proc. Tactical Communications Conference*, 1996.

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

[10] K. Krzywdziński and K. Rybarczyk. Geometric graphs with randomly deleted edges — connectivity and routing protocols. *Mathematical Foundations of Computer Science*, 6907:544–555, 2011.

[11] X. Li, P. Wan, Y. Wang, and C. Yi. Fault tolerant deployment and topology control in wireless networks. In *Proc. ACM MobiHoc*, 2003.

[5] An event occurs *almost surely* if its probability approaches to 1 as $n\to\infty$.

[12] M. Maiuzzo, T. Harwood, and W. Duff. Radio frequency distribution system (RFDS) for cosite electromagnetic compatibility. In *IEEE International Symposium on Electromagnetic Compatibility*, 2005.

[13] M. Penrose. On k-connectivity for a geometric random graph. *Random Struct. Algorithms*, 15:145–164, 1999.

[14] M. Penrose. Connectivity of soft random geometric graphs. *ArXiv e-prints*, November 2013. Available online at `http://arxiv.org/abs/1311.3897v1`

[15] H. Pishro-Nik, K. Chan, and F. Fekri. Connectivity properties of large-scale sensor networks. *Wireless Networks*, 15:945–964, 2009.

[16] K. Rybarczyk. Diameter, connectivity and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311, 2011.

[17] K. Rybarczyk. Sharp threshold functions for the random intersection graph via a coupling method. *Electr. Journal of Combinatorics*, 18:36–47, 2011.

[18] K. Rybarczyk. The coupling method for inhomogeneous random intersection graphs. *ArXiv e-prints*, Jan. 2013. Available online at `http://arxiv.org/abs/1301.0466`

[19] P.-J. Wan and C.-W. Yi. Asymptotic critical transmission radius and critical neighbor number for k-connectivity in wireless ad hoc networks. In *Proc. ACM MobiHoc*, 2004.

[20] Q. Wang, X. Wang, and X. Lin. Mobility increases the connectivity of k-hop clustered wireless networks. In *Proc. ACM MobiCom*, 2009.

[21] O. Yağan. Performance of the Eschenauer-Gligor key distribution scheme under an on/off channel. *IEEE Trans. on Information Theory*, 58(6):3821–3835, 2012.

[22] O. Yağan and A. M. Makowski. On the existence of triangles in random key graphs. In *Proc. Allerton Conference on Communication, Control, and Computing*, pages 1567 –1574, October 2009.

[23] O. Yağan and A. M. Makowski. Random key graphs – can they be small worlds? In *Proc. International Conference on Networks and Communications (NETCOM)*, pages 313 –318, December 2009.

[24] 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.

[25] 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. In *Proc. IEEE GLOBECOM*, Nov 2006.

[26] J. Zhao. k-Connectivity and minimum node degree in wireless networks with unreliable links. In *Proc. of IEEE ISIT*, 2014.

[27] J. Zhao, O. Yağan, and V. Gligor. k-Connectivity in secure wireless sensor networks with physical link constraints — the on/off channel model. *ArXiv e-prints*, 2012. Available online at `http://arxiv.org/abs/1206.1531`

[28] J. Zhao, O. Yağan, and V. Gligor. Secure k-connectivity in wireless sensor networks under an on/off channel model. In *Proc. IEEE ISIT*, pages 2790–2794, 2013.

[29] J. Zhao, O. Yağan, and V. Gligor. Topological properties of wireless sensor networks under the q-composite key predistribution scheme with on/off channels. In *Proc. of IEEE ISIT*, 2014.

Appendix

A. Establishing (9) on the unit torus $\mathcal{T}$

On the unit torus $\mathcal{T}$, it holds that $D_{r_n}(\hat{v_x}) = \pi {r_n}^2$ for any $\hat{v_x} \in \mathcal{T}$. Since $\mathcal{T}$ has an area of 1, by Lemma 1, it holds that

$$\mathbb{P}[I_x] = \int_{\mathcal{T}} e^{-np_s|D_{r_n}(\hat{v_x})|}\,\mathrm{d}\hat{v_x} = e^{-\pi {r_n}^2 p_s n}. \tag{18}$$

As given in (1), $p_s \sim \frac{{K_n}^2}{P_n}$, which with condition (2) induces $\pi {r_n}^2 p_s n \sim a \ln n$. With $a < 1$, we have $a < \frac{a+1}{2}$, and thus for all n sufficiently large, $\pi {r_n}^2 p_s n \leq \frac{a+1}{2} \cdot \ln n$, which is used in (18) to derive

$$\begin{aligned} n\mathbb{P}[I_x] &= ne^{-\pi {r_n}^2 p_s n} \\ &\geq ne^{-\frac{a+1}{2}\cdot \ln n} = n^{\frac{1-a}{2}} \to \infty \text{ as } n \to \infty. \end{aligned}$$

□

B. Establishing (10) on the unit torus $\mathcal{T}$

By the law of total probability, it is clear that

$$\mathbb{P}[I_x \cap I_y] = \sum_{u=0}^{K_n} \mathbb{P}\big[I_x \cap I_y \mid (|S_{xy}| = u) \big] \mathbb{P}[|S_{xy}| = u]. \tag{19}$$

Note that here we consider $\mathcal{A}$ as the torus $\mathcal{T}$. Applying Lemma 1 to (19), we derive

$$\begin{aligned} &\mathbb{P}\big[I_x \cap I_y \mid (|S_{xy}| = u) \big] \\ &\leq \int_{\mathcal{T}} \int_{\mathcal{T}} \\ &\quad e^{-n\{p_s|D_{r_n}(\hat{v_x})| + p_s|D_{r_n}(\hat{v_y})| - \phi_u |D_{r_n}(\hat{v_x}) \cap D_{r_n}(\hat{v_y})|\}} \mathrm{d}\hat{v_x}\mathrm{d}\hat{v_y}. \end{aligned} \tag{20}$$

For any $\hat{v_x} \in \mathcal{T}$ and any $\hat{v_y} \in \mathcal{T}$, we have $D_{r_n}(\hat{v_x}) = \pi {r_n}^2$ and $D_{r_n}(\hat{v_y}) = \pi {r_n}^2$. If $\hat{v_y} \in \mathcal{T} \setminus D_{2r_n}(\hat{v_x})$ (i.e., $\hat{v_x}$ and $\hat{v_y}$ have a distance greater than $2r_n$), where $D_{2r_n}(\hat{v_x})$ is the intersection of $\mathcal{T}$ and the disk centered at $\hat{v_x}$ with radius $2r_n$, then $|D_{r_n}(\hat{v_x}) \cap D_{r_n}(\hat{v_y})| = 0$; and if $\hat{v_y} \in D_{2r_n}(\hat{v_x})$, then $|D_{r_n}(\hat{v_x}) \cap D_{r_n}(\hat{v_y})| \leq \pi {r_n}^2$. Therefore, from (20),

$$\begin{aligned} &\mathbb{P}\big[I_x \cap I_y \mid (|S_{xy}| = u) \big] \\ &\quad \leq \Big(1 - 4\pi {r_n}^2 + 4\pi {r_n}^2 e^{\pi {r_n}^2 \phi_u n}\Big) e^{-2\pi {r_n}^2 p_s n}. \end{aligned} \tag{21}$$

Substituting (21) into (19), we obtain

$$\begin{aligned} &\mathbb{P}[I_x \cap I_y] \\ &\leq (1 - 4\pi {r_n}^2) e^{-2\pi {r_n}^2 p_s n} \\ &\quad + 4\pi {r_n}^2 e^{-2\pi {r_n}^2 p_s n} \sum_{u=0}^{K_n} \Big\{ \mathbb{P}[|S_{xy}| = u] e^{\pi {r_n}^2 \phi_u n} \Big\}. \end{aligned} \tag{22}$$

As shown in Remark 1 after Theorem 1, it follows that $r_n = o(1)$, which with (22) will yield (10) once we establish

$$\sum_{u=0}^{K_n} \Big\{ \mathbb{P}[|S_{xy}| = u] e^{\pi {r_n}^2 \phi_u n} \Big\} = O(1). \tag{23}$$

By our [27, Lemma 10], $\mathbb{P}[|S_{xy}| = u] \leq \frac{1}{u!}\big(\frac{{K_n}^2}{P_n - K_n}\big)^u$ holds, which along with our [1, Lemma 5] gives rise to

$$\text{L. H. S. of (23)} \leq e^{2\pi {r_n}^2 n \cdot \frac{{K_n}^4}{{P_n}^2} + \frac{{K_n}^2}{P_n - K_n} \cdot e^{\pi {r_n}^2 n \frac{K_n}{P_n}}}. \tag{24}$$

Given $\pi {r_n}^2 n \cdot \frac{{K_n}^2}{P_n} \sim a \ln n$ for constant $a < 1$, then for all n sufficiently large, it holds that

$$\pi {r_n}^2 n \cdot \frac{{K_n}^2}{P_n} \leq \ln n. \tag{25}$$

(25) and $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$ lead to

$$\pi {r_n}^2 n \cdot \frac{{K_n}^4}{{P_n}^2} = O(1). \tag{26}$$

(25) and $K_n = \omega(\ln n)$ result in

$$e^{\pi {r_n}^2 n \frac{K_n}{P_n}} \leq e^{{K_n}^{-1} \ln n} \leq e^{\ln \ln n} = e^{o(1)} \to 1, \text{ as } n \to \infty. \tag{27}$$

Given $\frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, we have $K_n = o(P_n)$ and further

$\frac{{K_n}^2}{P_n-K_n} \sim \frac{{K_n}^2}{P_n} = O\big(\frac{1}{\ln n}\big)$, which with (27) establishes

$$\frac{{K_n}^2}{P_n-K_n}\cdot e^{\pi {r_n}^2 n \frac{K_n}{P_n}} = O\bigg(\frac{1}{\ln n}\bigg). \tag{28}$$

The use of (26) and (28) in (24) yields (23). As explained before, the proof of (10) is now completed. □

C. The Proof of Lemma 2

As used by Rybarczyk [17], a coupling of two random graphs G_1 and G_2 means a probability space on which random graphs G'_1 and G'_2 are defined such that G'_1 and G'_2 have the same distributions as G_1 and G_2, respectively. We denote the coupling by (G_1, G_2, G'_1, G'_2).

Following Rybarczyk's notation [17], we write

$$G_1 \preceq_{1-o(1)} G_2 \tag{29}$$

if there exists a coupling (G_1, G_2, G'_1, G'_2) under which G'_1 is a subgraph of G'_2 with probability $1-o(1)$.

We then describe a graph model called random intersection graph, which has been extensively studied. A random intersection graph $G_{RIG}(n, P_n, t_n)$ is defined on n nodes as follows. There exist a key pool of size P_n; and each key in the pool is added to each sensor with probability t_n.

In view of [3, Lemma 4], if

$$t_n P_n = \omega\left(\ln n\right) \tag{30}$$

and for all n sufficiently large,

$$K_n \geq t_n P_n + \sqrt{3(t_n P_n + \ln n)\ln n}, \tag{31}$$

then

$$G_{RIG}(n, t_n, P_n) \preceq_{1-o(1)} G_{RKG}(n, K_n, P_n). \tag{32}$$

By [17, Lemma 3], if

$$t_n = o\left(1/n\right), \tag{33}$$

and for all n sufficiently large,

$${t_n}^2 P_n < 1, \tag{34}$$

with s_n defined through

$$s_n := {t_n}^2 P_n \cdot \left(1 - n t_n + 2t_n - \frac{{t_n}^2 P_n}{2}\right), \tag{35}$$

then

$$G_{ER}(n, s_n) \preceq_{1-o(1)} G_{RIG}(n, t_n, P_n). \tag{36}$$

By [18], the relation of "$\preceq_{1-o(1)}$" is transitive. In other words, for any three graphs G_a, G_b and G_c, if $G_a \preceq_{1-o(1)} G_b$ and $G_b \preceq_{1-o(1)} G_c$, then $G_a \preceq_{1-o(1)} G_c$. Then given (32) and (36), we obtain that under (30) (31) (33) (34) and (35), it follows that

$$G_{ER}(n, s_n) \preceq_{1-o(1)} G_{RKG}(n, K_n, P_n). \tag{37}$$

By [18], from (37), it further holds that

$$\begin{aligned} &G_{ER}(n, s_n) \cap G_{RGG}(n, r_n, \mathcal{A}) \\ &\preceq_{1-o(1)} \big[G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A})\big]. \end{aligned} \tag{38}$$

By [18], from (38), it is easy to see that for any monotone increasing graph property $\mathscr{P}$,

$$\begin{aligned} &\mathbb{P}[\, G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A}) \text{ has } \mathscr{P}\,] \\ &\geq \mathbb{P}[\, G_{ER}(n, q_n) \cap G_{RGG}(n, r_n, \mathcal{A}) \text{ has } \mathscr{P}\,] - o(1). \end{aligned} \tag{39}$$

From (39), the proof of Lemma 2 is completed with q_n set as s_n if we show that given some appropriately selected t_n and the conditions in Lemma 2, then (30) (31) (33) (34) and

$$s_n = \frac{{K_n}^2}{P_n} \cdot \left[1 - o\left(1\right)\right] \tag{40}$$

with s_n defined in (35) all follow.

We will do so by setting t_n via

$$t_n = \frac{K_n}{P_n}\Bigg(1 - \sqrt{\frac{3\ln n}{K_n}}\Bigg). \tag{41}$$

First, (41) and $K_n = \omega(\ln n)$ yield

$$t_n = \frac{K_n}{P_n} \cdot [1 - o(1)], \tag{42}$$

which along with $K_n = \omega(\ln n)$ further leads to

$$t_n P_n = K_n \cdot [1 - o(1)] = \omega\left(\ln n\right).$$

Given (41) and condition $K_n = \omega(\ln n)$, we obtain (31) in that for all n sufficiently large,

$$\begin{aligned} &K_n - \Big[t_n P_n + \sqrt{3(t_n P_n + \ln n)\ln n}\Big] \\ &= K_n\sqrt{\frac{3\ln n}{K_n}} - \sqrt{3\left[K_n\left(1 - \sqrt{\frac{3\ln n}{K_n}}\right) + \ln n\right]\ln n} \\ &= \sqrt{3K_n \ln n} - \sqrt{3\left[K_n + \sqrt{\ln n}\left(\sqrt{\ln n} - \sqrt{3K_n}\right)\right]\ln n} \\ &\geq \sqrt{3K_n \ln n} - \sqrt{3K_n \ln n} \\ &= 0. \end{aligned}$$

From (42) and condition $\frac{K_n}{P_n} = o\left(\frac{1}{n}\right)$, (33) holds due to

$$t_n = \frac{K_n}{P_n} \cdot [1 - o(1)] = O\left(\frac{1}{n}\right). \tag{43}$$

From (42) and condition $\frac{{K_n}^2}{P_n} = O\left(\frac{1}{\ln n}\right)$, then (34) is true

$${t_n}^2 P_n = \frac{{K_n}^2}{P_n} \cdot \big\{[1 - o(1)]\big\}^2 = O\left(\frac{1}{\ln n}\right). \tag{44}$$

Below we will show (40), where s_n is specified in (35). Owing to (43) and (44), and also using ${t_n}^2 P_n \sim \frac{{K_n}^2}{P_n}$ given in (44), we obtain from (35) that

$$s_n = \frac{{K_n}^2}{P_n} \cdot \left[1 - o\left(1\right)\right];$$

i.e., (40) is proved.

We have shown that (30) (31) (33) (34) and (40) all hold with t_n and s_n set in (41) and (35), respectively, given the conditions in Lemma 2. Then as noted before, with p_n set as s_n, we have established Lemma 2 in view of (39). □