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 connectivity properties of secure WSNs with the EG scheme widely recognized way to secure communications. Although the Eschenauer–Gligor (EG) key pre-distribution scheme is a helpful specification for connectivity. 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 Krzywydiński 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 [2], [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 $\mathcal{S}_v$ for sensor $v$. 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 $v_x$ and $v_y$ if and only if they possess at least one common key; i.e., the event $\mathcal{S}_x \cap \mathcal{S}_y \neq \emptyset$, denoted by $K_{xy}$, holds. As for the sensor distribution, the same as much previous work [2], [9], [10], [19], we consider that the $n$ nodes are independently and uniformly deployed in a network area $A$.

1The terms sensor and node are interchangeable.
The disk model induces a random geometric graph \([7, 9, 10, 13, 19]\), denoted by \(G_{RGC}(n, r_n, A)\), 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 \(G(n, \theta_n, A)\) model such a WSN, it is straightforward to see \(\Pr(G(n, \theta_n, A)\) is the intersection\(^3\) of random key graph \(G_{RKG}(n, K, P)\) and random geometric graph \(G_{RGG}(n, r_n, A)\); namely,

\[
G(n, \theta_n, A) = G_{RKG}(n, K, P_n) \cap G_{RGG}(n, r_n, A),
\]

where parameters \(K_n, P_n\) and \(r_n\) are together represented by \(\theta_n\). Also, if we let region \(A\) be either a square \(S\), or a square with each area, we obtain the two graphs

\[
G(n, \theta_n, T) = G_{RKG}(n, K, P_n) \cap G_{RGG}(n, r_n, T),
\]

and

\[
G(n, \theta_n, S) = G_{RKG}(n, K, P_n) \cap G_{RGG}(n, r_n, S).
\]

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

\[
p_x = K_n^2/P_n \cdot \left[1 \pm O(K_n^2/P_n)\right] \sim K_n^2/P_n.
\]

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 \(G(n, \theta_n, A)\); i.e., \(p_e\) is the edge probability in \(G(n, \theta_n, A)\). It holds that \(p_e = \Pr[K_{xy}]\). When \(A\) is the torus \(T\), clearly \(p_e\) equals \(\pi r_n^2 \cdot p_x\); 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 \(A\) is the square \(S\), it is a simple matter to show \(p_e \leq (1 - 2r_n^2) \cdot \pi r_n^2 \cdot p_x\) (with \(r_n \leq \frac{1}{2}\)) and \(p_e \leq \pi r_n^2 \cdot p_x\). The reason is that for the position of \(v_x\) satisfying the condition that \(v_x\)'s distance to all four edges of \(S\) 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 \(S\), it holds that \(p_e \sim \pi r_n^2 \cdot p_x\) 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 \(S\), 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.

\(^2\)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 \(o()\), \(O()\), \(\omega()\), \(\Omega()\), \(\Theta()\), and \(\sim\); in particular, for two sequences \(f_n\) and \(g_n\), the relation \(f_n \sim g_n\) means \(\lim_{n \to \infty} f_n/g_n = 1\).

A. Connectivity in a Secure WSN on a Unit Torus

Theorem \(\[\]\) 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 \(K_n = o(\ln n)\), \(K_n^2/P_n = O\left(\frac{1}{\ln n}\right)\). \(K_n^2/P_n = \omega\left(\frac{1}{\ln n}\right)\), \(K_n^2/P_n = o\left(\frac{1}{\ln n}\right)\) and

\[
\pi r_n^2 \cdot K_n^2/P_n \sim a \cdot \frac{\ln n}{n}
\]

for some positive constant \(a\), then

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

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

B. Connectivity in a Secure WSN on a Unit Square

Theorem \(\[\]\) gives a zero-one law for connectivity in \(G(n, \theta_n, S)\), which models a secure WSN working under the EG scheme and the disk model on the unit square \(S\).

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

\[
\pi r_n^2 \cdot K_n^2/P_n = \begin{cases} b \cdot \frac{\ln P_n}{K_n^2}, & \text{for } K_n^2/P_n = o\left(\frac{1}{\ln n}\right), \\ b \cdot \frac{4 \ln P_n}{K_n^2}, & \text{for } K_n^2/P_n = o\left(\frac{1}{\ln n}\right). \end{cases}
\]

for some positive constant \(b\), where \(K_n^2/P_n \cdot \ln n/\ln n\) is assumed either bounded for all \(n\) or converging to \(\infty\) as \(n \to \infty\), then

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

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

We explain that the conditions in Theorems \(\[\]\) and \(\[\]\) are
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 $K_n = \omega(\ln n)$, $K_n^2/P_n = O(1/\ln n)$, $K_n^2/n = \omega(1/\ln n)$ and $K_n^2/P_n = \omega(1/\ln n)$ are all practical.

Connectivity results with more fine-grained scalings for graphs $G(n, \theta_n, T)$ and $G(n, \theta_n, S)$ are provided in the full version [11] 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 [3] 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 $G(r_n)$ with $r_n$ as the transmission range, $r_n^*$ is said to be the critical transmission range if (i) and (ii) below both hold:

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

(ii) $\lim_{n\to\infty} P[G(cr_n^*) \text{ is connected.}] = 1$ 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 $r_n^*(T)$ for connectivity in a secure WSN on a unit torus modeled by graph $G(n, \theta_n, T)$ through

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

inducing the following expression of $r_n^*(T)$:

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

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

Along with (5), condition $K_n^2/P_n = \omega(\ln n/n)$ in Theorem [1] leads to $r_n^*(T) = o(1)$. This is anticipated as the node density $n$ grows to infinity.

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

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

$$\pi [r_n^*(S)]^2 \cdot \frac{K_n^2}{P_n} = \left\{ \begin{array}{ll}
\frac{\ln n + P_n}{n}, & \text{for } K_n^2/P_n = \omega\left(\frac{1}{n^{1/3} \ln n}\right), \\
4 \ln \frac{P_n}{K_n^2}, & \text{for } K_n^2/P_n = O\left(\frac{1}{n^{1/3} \ln n}\right),
\end{array} \right. \quad (6)$$

so $r_n^*(S)$ is specified by

$$r_n^*(S) = \left\{ \begin{array}{ll}
\sqrt{\frac{\ln n + P_n}{n \pi n K_n^2}}, & \text{for } K_n^2/P_n = \omega\left(\frac{1}{n^{1/3} \ln n}\right), \\
2 \sqrt{4 \ln \frac{P_n}{K_n^2}}, & \text{for } K_n^2/P_n = O\left(\frac{1}{n^{1/3} \ln n}\right).
\end{array} \right. \quad (7)$$

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

Second, similar to Remark [2], $K_n^2/P_n = \omega(\ln n/n)$ and (7) imply $r_n^*(S) = o(1)$.

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

Fourth, we compute $\lim_{n \to \infty} \left\{ \pi [r_n^*(S)]^2 \cdot K_n^2/P_n / \left(\frac{\ln n}{n}\right) \right\}$ 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 $\lim_{n \to \infty} \left\{ \pi [r_n^*(S)]^2 \cdot K_n^2/P_n / \left(\frac{\ln n}{n}\right) \right\}$ are 8 and $2\pi$, respectively [9], [10]. By (7), it is clear that

$$\lim_{n \to \infty} \left\{ \pi [r_n^*(S)]^2 \cdot K_n^2/P_n / \left(\frac{\ln n}{n}\right) \right\} = \left\{ \begin{array}{ll}
1 + \lim_{n \to \infty} \left(\frac{\ln \frac{P_n}{K_n^2}}{\ln n}\right), & \text{for } K_n^2/P_n = \omega\left(\frac{1}{n^{1/3} \ln n}\right), \\
4 \lim_{n \to \infty} \left(\frac{\ln \frac{P_n}{K_n^2}}{\ln n}\right), & \text{for } K_n^2/P_n = O\left(\frac{1}{n^{1/3} \ln n}\right).
\end{array} \right. \quad (8)$$

From (8), we observe a phase transition of $r_n^*(S)$ when $K_n^2/P_n$ 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 $r_n^*(T)$ of a torus $T$. The intuition is that, in integrating all possible points in the network region $A$ to compute the expected number of isolated nodes, for $A$ being the square $S$ with the boundary
effect, different areas on contribute the dominant part of the integral as \( \frac{K_{\omega}^2}{P_n} n^{1/3} \ln n \) vary from unbounded to bounded, while \( \mathcal{A} \) being the torus \( T \), 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 \( G(n, \theta_n, A) \) follows once we establish the same result for its Poissonized version, graph \( G_{\text{Poisson}}(n, \theta_n, A) \), where the only difference between \( G_{\text{Poisson}}(n, \theta_n, A) \) and \( G(n, \theta_n, A) \) is that the node distribution of the former is a homogeneous Poisson point process with intensity \( n \) on \( A \) 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 \( G_{\text{Poisson}}(n, \theta_n, A) \), to prove the zero-law of connectivity, it suffices to show the corresponding zero-law for the absence of isolated nodes.

3) Method of the moments: For graph \( G_{\text{Poisson}}(n, \theta_n, A) \), to demonstrate the zero–law for 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

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

and

\[
\mathbb{P}[I_x \cap I_y] \leq \left\{ \mathbb{P}[I_x] \right\}^2 \cdot [1 + o(1)].
\]

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 \( T \), 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 \( S \), as well as the proof of Lemma 1 are provided in the full paper [1].

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

\[
\mathbb{P}[I_x] = \int_{\mathcal{A}} e^{-n p_x |D_{r_n}(v_x)|} dv_x,
\]

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

\[
\mathbb{P}[I_x \cap I_y \mid (|S_{xy}| = u)] = \int_{\mathcal{A} \cap D_{r_n}(v_x)} e^{-n (p_x |D_{r_n}(v_x)| + p_y |D_{r_n}(v_y)| - \phi_u |D_{r_n}(v_x) \cap D_{r_n}(v_y)|)} dv_x dv_y,
\]

and

\[
\mathbb{P}[I_x \cap I_y \mid (|S_{xy}| = 0)] = \int_{\mathcal{A}} \int_{\mathcal{A}} e^{-n (p_x |D_{r_n}(v_x)| + p_y |D_{r_n}(v_y)| - \phi_0 |D_{r_n}(v_x) \cap D_{r_n}(v_y)|)} dv_x dv_y,
\]

with \( \phi_0 \) meaning \( \phi_u \) when \( u = 0 \).

B. One-Laws by the Analogy between Random Graphs

To prove the one–laws, we relate graph \( G(n, \theta_n, A) \) (i.e., \( G_{\text{RKG}}(n, K_n, P_n) \cap G_{\text{RGG}}(n, r_n, A) \)) to the intersection of an Erdős–Rényi graph [3] and the random geometric graph \( G_{\text{RGG}}(n, r_n, A) \), where an Erdős–Rényi graph \( G_{\text{ER}}(n, P_n) \) 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 \( G_{\text{RKG}}(n, K_n, P_n) \) and Erdős–Rényi graph \( G_{\text{ER}}(n, P_n) \) 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 \( G_{\text{RKG}}(n, K_n, P_n) \) and \( G_{\text{ER}}(n, P_n) \) (and the analogy between their respective intersections with \( G_{\text{RGG}}(n, r_n, A) \)) needs rigorous arguments. Our Lemma 2 below involves rigorous reasoning and is detailed in Appendix C.

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

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

such that for any topology \( \mathcal{A} \) and any monotone increasing graph property \( \mathcal{P} \),

\[
\mathbb{P}[G_{\text{RKG}}(n, K_n, P_n) \cap G_{\text{RGG}}(n, r_n, A) \mathcal{P}] \geq \mathbb{P}[G_{\text{ER}}(n, P_n) \cap G_{\text{RGG}}(n, r_n, A) \mathcal{P}] - o(1).
\]

Lemmata 3 and 4 below present zero–one laws for connectivity in graphs \( G_{\text{ER}}(n, P_n) \cap G_{\text{RGG}}(n, r_n, T) \) and \( G_{\text{ER}}(n, P_n) \cap G_{\text{RGG}}(n, r_n, S) \), 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 \( G_{\text{ER}}(n, P_n) \) and random geometric graph \( G_{\text{RGG}}(n, r_n, T) \). If

\[
\pi r_n^2 \cdot P_n \sim c \cdot \frac{\ln n}{n}
\]
Lemma 4. For some positive constant $d$, then
\[
\lim_{n \to \infty} \mathbb{P} \left[ \frac{G_{ER}(n,p_n)}{G_{RG}(n,r_n,T)} \right] = \begin{cases} 
0, & \text{if } c < 1, \\
1, & \text{if } c > 1. 
\end{cases}
\]

(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 $G_{RG}(n,r_n,S)$. If
\[
\pi r_n^2 p_n = \begin{cases} 
\frac{\ln n}{n}, & \text{for } p_n = \omega \left( \frac{1}{n^{\gamma} \ln n} \right), \\
\frac{4 \ln n}{n}, & \text{for } p_n = O \left( \frac{1}{n^{\gamma} \ln n} \right),
\end{cases}
\]
for some positive constant $d$, then
\[
\lim_{n \to \infty} \mathbb{P} \left[ \frac{G_{ER}(n,p_n)}{G_{RG}(n,r_n,S)} \right] = \begin{cases} 
0, & \text{if } d < 1, \\
1, & \text{if } d > 1.
\end{cases}
\]

VI. NUMERICAL EXPERIMENTS

We present numerical simulation in the non-asymptotic regime to support our asymptotic results. We write graph $G(n, K, P, r, A)$ as $G(n, K, P, r, A)$. In Figure 1 we depict the probability that graph $G(n, K, P, r, A)$ (i.e., $G(n, \theta, A)$) is connected, where $A$ is either the unit torus $\mathcal{T}$ or the unit square $S$; and the subscript $n$ is removed since we fix the number of nodes at $n = 2,000$ in all experiments. For each pair $(A, K, P, r)$, we generate 500 independent samples of $G(n, K, P, r, A)$ 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 $G(n, K, P, r, A)$ 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]. Alternatively, 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 $A$, which is either a unit torus $\mathcal{T}$ or a unit square $S$, and all nodes have the same transmission range $r$, then $G_f$ is exactly $G(\theta, n, T)$ when $A = \mathcal{T}$ and $G(n, \theta, S)$ when $A = S$. Our zero–one laws on connectivity of $G(n, \theta, T)$ and $G(n, \theta, S)$ 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 et al. consider graph $G(n, \theta, A)$, where the network region $A$ is either a disk $\mathcal{D}$ or a square $S$, each of unit area. They show that for graph $G(n, \theta, \mathcal{D})$ or $G(n, \theta, S)$, if $\pi r^2 n \cdot \frac{K_n}{P_n} = \omega(\frac{1}{\ln n})$ and $\frac{K_n^2}{P_n} = \omega(\frac{1}{\ln n})$, the number of isolated nodes asymptotically follows a Poisson distribution with mean $e^{-\alpha}$. Pishro-Nik et al. also obtain such result on asymptotic Poisson distribution with condition $\frac{K_n^2}{P_n} = \omega(\frac{1}{\ln n})$ generalized to $\frac{K_n^2}{P_n} = \Omega(\frac{1}{\ln n})$. In practical
WSNs, $K_n$ is expected to be several orders of magnitude smaller than $P_n$ [4], [6], [21], so it often holds that $K_n^2 = o\left(\frac{1}{P_n}\right)$, which is not addressed in the two work above [15] and is addressed in our theorems. Recently, for graph $G(n, \theta, S)$, Krzywdziński and Rybarczyk [10] and Krishnan et al. [9] obtain connectivity results, covering the case of $K_n^2 = o\left(\frac{1}{P_n}\right)$. We elaborate their theoretical findings below and explain that our results significantly improve theirs. Krzywdziński and Rybarczyk [10] present that in $G(n, \theta, S)$ on $S$, if $\pi r_n^2 - K_n^2 \geq \frac{8\ln n}{n}$ with $K_n \geq 2$ and $P_n = \omega(1)$, then $G(n, \theta, S)$ is almost surely connected. Krishnan et al. [9] demonstrate that if $\pi r_n^2 - K_n^2 \geq 2\frac{\ln n}{n}$ with $K_n = \omega(1)$ and $K_n^2 = o\left(\frac{1}{P_n}\right)$, then $G(n, \theta, S)$ is almost surely connected. Both only provide upper bounds on $\lim_{n \to \infty} \left\{ \pi \left(r_n^*(S)\right)^2 \cdot K_n^2 / (\ln n) \right\}$, with one being 8 and the other being $2\pi$, respectively. $r_n^*(S)$ is the critical transmission range for connectivity in $G(n, \theta, S)$. In this paper, we determine the exact value of this limit by deriving $r_n^*(S)$. As illustrated in Figure 2 we plot the term $\lim_{n \to \infty} \left\{ \pi \left(r_n^*(S)\right)^2 \cdot K_n^2 / (\ln n) \right\}$ with respect to $\lim_{n \to \infty} \left( \ln \left(K_n^2 / P_n\right) / (\ln n) \right)$. The curve of the exact values is based on our result in Section IV.

For random key graph $G_{RKG}(n, K_n, P_n)$, Blackburn and Gerke [3], 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 $K_n^2 = o\left(\frac{\ln n}{P_n}\right)$, 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 $G_{RGG}(n, r, A)$ has been widely studied due to its application to wireless networks. Gupta and Kumar [7] show that when $A$ is a unit-area disk $\mathcal{T}$ and $\pi r_n^2 = \frac{\ln n + c_\alpha}{\alpha_n}$, $G_{RGG}(n, r, D)$ is almost surely connected if and only if $\lim_{n \to \infty} \alpha_n = \infty$. Penrose [13] explores $k$-connectivity in $G_{RGG}(n, r, A)$, where $A$ is a $d$-dimensional unit cube with $d \geq 2$. For $A$ being the unit torus $\mathcal{T}$, he obtains that with $r_n$ denoting the minimum $r_n$ to ensure $k$-connectivity in $G_{RGG}(n, r, \mathcal{T})$, where $k \geq 1$, then the probability that $\pi r_n^2$ is at most $\ln n + (k - 1)\ln n - \ln((k - 1)! + 1)$ asymptotically converges to $e^{-e^{-\alpha}}$. Li et al. [11] prove that with $k \geq 2$, to have graph $G_{RGG}(n, r, S)$ asymptotically $k$-connected with probability at least $e^{-e^{-\alpha}}$ for some $\alpha$, a sufficient condition is that the term $\pi r_n^2$ is at least $\ln n + (2k - 3)\ln n - 2\ln((k - 1)! + 1)$, and a necessary condition is that $\pi r_n^2$ is no less than $\ln n + (k - 1)\ln n - \ln((k - 1)! + 1) + \alpha$. For $k \geq 2$, Wan et al. [19] determine the exact formula of $\alpha_n$ such that graph $G_{RGG}(n, r, S)$ or $G_{RGG}(n, r, D)$ is asymptotically $k$-connected with probability $e^{-e^{-\alpha}}$, where as noted above, $D$ 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 been investigated in several work by the authors [21], [27]–[29].

IX. Conclusion

We establish zero–one laws for connectivity in secure wireless sensor networks 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

K. Rybarczyk. Diameter, connectivity and phase transition of the

K. Rybarczyk. Sharp threshold functions for the random intersection

http://arxiv.org/abs/1311.3897v1

H. Psilard, N. Kapur, M. Penrose. Connectivity properties of


http://arxiv.org/abs/1311.3897v1

P.-J. Wan and C.-W. Yi. Asymptotic critical transmission radius and critical neighbor number for k-connectivity in wireless ad hoc

Q. Wang, X. Wang, and X. Lin. Mobility increases the connectivity


O. Yagan and A. M. Makowski. On the existence of triangles in

O. Yagan 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.

O. Yagan and A. M. Makowski. Zero–one laws for connectivity


J. Zhao, O. Yagan, and V. Gligor. Topological properties of wireless
sensor networks under the q-composite key predistribution scheme

A. Establishing (10) on the unit torus $T$

On the unit torus $T$, it holds that $D_{r_n}(v_x) = \pi r_n^2$ for
any $v_x \in T$. Since $T$ has an area of 1, by Lemma 10 (10) it holds that

$$\mathbb{P}[I_x] = \int_T e^{-n p |D_{r_n}(v_x)|} dv_x = e^{-\pi r_n^2 p_n n}.$$  

(18)

As given in (10), $p_n \sim \frac{K_n}{r_n^2}$, which with condition (2) induces $\pi r_n^2 p_n \sim a \ln n$. With $a < 1$, we have $\pi r_n^2 p_n \leq a \frac{1}{4} \ln n$, which is used in (18) to derive

$$n \mathbb{P}[I_x] = n e^{-\pi r_n^2 p_n n} \geq n e^{-a \frac{1}{4} \ln n} = n^{a - \frac{1}{4}} \ln n \rightarrow \infty \text{ as } n \rightarrow \infty.$$  

B. Establishing (11) on the unit torus $T$

By the law of total probability, it is clear that

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

(19)

Note that here we consider $A$ as the torus $T$. Applying Lemma 11 to (19), we derive

$$\mathbb{P}[I_x \cap I_y \mid (|S_{xy}| = u)] \leq \int_T \int_T e^{-n p |D_{r_n}(v_x)| + p |D_{r_n}(v_y)| - \phi_n |D_{r_n}(v_x) \cap D_{r_n}(v_y)|} dv_x dv_y.$$  

(20)

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

$$\mathbb{P}[I_x \cap I_y \mid (|S_{xy}| = u)] \leq \left(1 - 4 \pi r_n^2 e^{-2 \pi r_n^2 p_n n}ight)e^{-2 \pi r_n^2 p_n n}.\quad (21)$$

Substituting (21) into (19), we obtain

$$\mathbb{P}[I_x \cap I_y] \leq \left(1 - 4 \pi r_n^2 e^{-2 \pi r_n^2 p_n n}ight) + 4 \pi r_n^2 e^{-2 \pi r_n^2 p_n n} \sum_{u=0}^{K_n} \mathbb{P}[|S_{xy}| = u] e^{-\pi r_n^2 \phi_n u}.$$  

(22)

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

$$\sum_{u=0}^{K_n} \mathbb{P}[|S_{xy}| = u] e^{-\pi r_n^2 \phi_n u} = o(1).\quad (23)$$

By our (27) Lemma 10, $\mathbb{P}[|S_{xy}| = u] \leq \frac{1}{u} \left(\frac{K_n^2}{r_n^2 - K_n^2}ight)^u$ holds, which along with our (11) Lemma 5 gives rise to

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

(24)

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

$$\pi r_n^2 n \cdot \frac{K_n^2}{r_n^2} \leq \ln n.\quad (25)$$

(25) and $\frac{K_n^2}{r_n^2} = O\left(\frac{1}{\ln n}\right)$ lead to

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

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

$$e^{-\pi r_n^2 n \frac{K_n^4}{r_n^2 - K_n^2}} \leq e^{-\pi r_n^2 \ln n} = e^{o(1)} \rightarrow 1, \text{ as } n \rightarrow \infty.$$  

(27)

Given $\frac{K_n^2}{r_n^2} = O\left(\frac{1}{\ln n}\right)$, we have $K_n = o(P_n)$ and further
\[
\frac{K_n^2 - K_n}{P_n - K_n} \sim \frac{K_n^2}{P_n} - O\left(\frac{1}{\ln n}\right),
\]
which with (27) establishes
\[
\frac{K_n^2}{P_n - K_n} \cdot e^{n^{2/3} K_n^2 P_n} = O\left(\frac{1}{\ln n}\right). \tag{28}
\]
The use of (26) and (28) in (24) yields (23). As explained before, the proof of (10) is now completed. \hfill \square

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 \(RIG(n, P_n, t_n)\) 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
\[
t_n P_n = \omega(\ln n) \tag{30}
\]
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
\[
t_n = o(1/n), \tag{33}
\]
and for all \(n\) sufficiently large,
\[
t_n^2 P_n < 1, \tag{34}
\]
with \(s_n\) defined through
\[
s_n := t_n^2 P_n \cdot \left(1 - n t_n + 2 t_n - \frac{t_n^2 P_n}{2}\right) \tag{35}
\]
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 \(G_a \preceq_{1-o(1)} G_c\). 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
\[
G_{ER}(n, s_n) \cap G_{RGG}(n, r_n, A) \preceq_{1-o(1)} \left[ G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, A) \right]. \tag{38}
\]
By [18], from (38), it is easy to see that for any monotone increasing graph property \(\mathcal{P}\),
\[
P\left[ G_{RKG}(n, K_n, P_n) \cap G_{RGG}(n, r_n, A) \text{ has } \mathcal{P} \right]
\geq P\left[ G_{ER}(n, s_n) \cap G_{RGG}(n, r_n, A) \text{ has } \mathcal{P} \right] - o(1). \tag{39}
\]
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
\[
s_n = \frac{K_n^2}{P_n} \cdot [1 - o(1)] \tag{40}
\]
with \(s_n\) defined in (35) all follow.

We will do so by setting \(t_n\) via
\[
t_n = \frac{K_n}{P_n} \left(1 - \sqrt{\frac{3 \ln n}{K_n}}\right). \tag{41}
\]
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
\[
t_n P_n = K_n \cdot [1 - o(1)] = \omega(\ln n). \tag{43}
\]
Given (41) and condition \(K_n = \omega(\ln n)\), we obtain (31) in that for all \(n\) sufficiently large,
\[
K_n - \left[t_n P_n + \sqrt{3(t_n P_n + \ln n) \ln n}\right]
= K_n \left[\frac{3 \ln n}{K_n} - \sqrt{\frac{3 \ln n}{K_n} + [1 - \frac{3 \ln n}{K_n} + \ln n] \ln n}\right]
\geq -\sqrt{3 K_n \ln n - \sqrt{3 K_n \ln n}} = 0.
\]
From (42) and condition \(K_n^2/P_n = o\left(\frac{1}{\ln n}\right)\), (35) 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 \(K_n^2/P_n = O\left(\frac{1}{\ln n}\right)\), then (34) is true
\[
t_n^2 P_n = K_n^2 \cdot \left(1 - o(1)\right)^2 = O\left(\frac{1}{\ln n}\right). \tag{44}
\]
Below we will show (40), where \(s_n\) is specified in (35).
Owing to (43) and (44), and also using \(t_n^2 P_n = K_n^2/P_n\) given in (44), we obtain from (35) that
\[
s_n = \frac{K_n^2}{P_n} \cdot [1 - o(1)]; \tag{45}
\]
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). \hfill \square