On Secure Communication in Sensor Networks under q-Composite Key Predistribution with Unreliable Links

Jun Zhao, *Member, IEEE*

***Abstract*—Many applications of wireless sensor networks (WSNs) require deploying sensors in hostile environments, where an adversary may eavesdrop communications. To secure communications in WSNs, the q-composite key predistribution scheme has been proposed in the literature. In this paper, we investigate secure k-connectivity in WSNs operating under the q-composite scheme, in consideration of the unreliability of wireless links. Secure k-connectivity ensures that any two sensors can find a path in between for secure communication, even when $k-1$ sensors fail. We present conditions on how to set the network parameters such that the network has secure k-connectivity asymptotically almost surely. The result is given in the form of a sharp zero–one law.**

***Index Terms*—Security, sensor networks, key predistribution, wireless communication, link unreliability.**

I. Introduction

Wireless sensor networks (WSNs) enable a broad range of applications including military surveillance, industrial monitoring, and home automation [1]. When WSNs are deployed in hostile environments, cryptographic mechanisms are needed to secure communications between sensors. Because the network topology is often unknown before deployment, the idea of key predistribution has been proposed to protect sensor communications [2].

Since Eschenauer and Gligor [2] introduced the basic key predistribution scheme, key predistribution schemes have been widely studied in the literature [3]–[8]. Among many key predistribution schemes, the q-composite scheme proposed by Chan *et al.* [9] as an extension of the Eschenauer–Gligor scheme [2] has received considerable interest [10]–[16] (the Eschenauer–Gligor scheme is the q-composite scheme in the special case of $q = 1$). The q-composite scheme works as follows. For a WSN with n sensors, prior to deployment, each sensor is independently assigned K_n different keys which are selected uniformly at random from a pool $\mathcal{P}_n$ of P_n distinct keys, where K_n is referred to as the key ring size. After deployment, any two sensors establish a secure link in between if and only if they share at least q key(s) and the physical link constraint between them is satisfied. P_n and K_n are functions of n, with the natural condition $1 \leq q \leq K_n \leq P_n$. Examples of physical link constraints include the reliability of the transmission channel [16]–[19] and the requirement that the distance between two sensors need to be close enough for direct communication [20]–[23]. The q-composite scheme with $q \geq 2$ outperforms the Eschenauer–Gligor scheme with $q = 1$ in terms of the strength against small-scale sensor capture while trading off increased vulnerability in the face of large-scale attacks [9].

In this paper, we investigate secure k-connectivity in WSNs employing the q-composite key predistribution scheme with the physical link constraint represented by the *on*/*off* channel model comprising independent channels which are either *on* or *off*. Secure k-connectivity ensures that any two sensors can find a path in between for secure communication, even when any $k-1$ sensors fail and are deleted from the network topology. The on/off channel model captures the unreliability of wireless links due to physical barriers between sensors or harsh environmental conditions impairing communications [24]–[26]. Our results are given in the form of a *sharp* zero–one law, meaning that the network is securely k-connected asymptotically almost surely (*a.a.s.*) under certain parameter conditions and does not have secure k-connectivity *a.a.s.* if parameters are slightly changed, where an event happens *a.a.s.* if its probability converges to 1 over a sequence of sets (i.e., in this paper, as the number of sensors tends to infinity). In the asymptotic sense, the zero–one law specifies the critical scaling of the model parameters in terms of secure k-connectivity. Despite being asymptotic, such a critical scaling provides useful insights to understand secure WSNs. In a secure WSN, to increase the probability of k-connectivity, it is often required to enlarge the number of keys in each sensor's memory. However, since sensors are expected to have limited memory, it is desirable for key distribution schemes to have low memory requirements [2], [9], [27], [28]. Therefore, it is important to establish a zero–one law in order to carefully dimension the q-composite key predistribution scheme for secure communications between sensors.

We organize the rest of the paper as follows. After Section II describes the system model, Section III presents the results. We survey related work in Section IV. Sections V and VI are

Manuscript received February 15, 2017; revised July 2 and September 21, 2017; accepted November 23, 2017. Date of publication November 29, 2017; date of current version November 29, 2017. This research was supported in part by the Cybersecurity Lab (CyLab) and Department of Electrical & Computer Engineering at Carnegie Mellon University, by Nanyang Technological University, and by Arizona State University. The associate editor coordinating the review of this paper and approving it for publication was V. Aggarwal. (*Corresponding author: Jun Zhao.*)

The author was with Carnegie Mellon University, Pittsburgh, PA 15213, USA, and also with Arizona State University, Tempe, AZ 85281, USA. He is now with Nanyang Technological University, Singapore 639798.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier:

devoted to proving the results. Finally, we conclude the paper in Section VII.

II. System Model

The studied WSN consists of n sensors, employs the q-composite key predistribution scheme, and works under the on/off channel model. We will explain that the graph representing the studied WSN is an intersection of two distinct types of random graphs. The intertwining of random graphs makes the analysis challenging.

We use a node set $\mathcal{V}_n = \{v_1, v_2, \ldots, v_n\}$ to represent the n sensors (the terms sensor and node are interchangeable in this paper). For each node $v_i \in \mathcal{V}_n$, let the set of its K_n different keys be S_i. According to the q-composite key predistribution scheme, S_i is uniformly distributed among all K_n-size subsets of a key pool $\mathcal{P}_n$ of P_n keys.

The q-composite key predistribution scheme is modeled by a uniform q-intersection graph [8] denoted by $G_q(n, K_n, P_n)$. In such a graph defined on the node set $\mathcal{V}_n$, any two distinct nodes v_i and v_j have an edge in between if and only if they share at least q key(s) (an event denoted by Γ_{ij}) . With $|A|$ being the cardinality of a set A, event Γ_{ij} is given by $\big[|S_i \cap S_j| \geq q\big]$.

Under the on/off channel model, each node-to-node channel is independently *on* with probability p_n and *off* with probability $(1-p_n)$, where p_n is a function of n with $0 < p_n \leq 1$. Letting L_{ij} be the event that the channel between distinct nodes v_i and v_j is *on*, we have $\mathbb{P}\left[L_{ij}\right] = p_n$, where $\mathbb{P}[\mathcal{E}]$ denotes the probability that an event $\mathcal{E}$ happens, throughout the paper. The network topology under the on/off channel model is given by an Erdős–Rényi graph $G(n, p_n)$ [29] with the node set being $\mathcal{V}_n$ and the edge set specified by L_{ij}.

Finally, we use $\mathbb{G}_q(n, K_n, P_n, p_n)$ to model the n-node WSN operating under the q-composite scheme and the on/off channel model. In graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ defined on the node set $\mathcal{V}_n$, there exists an edge between nodes v_i and v_j (an event denoted by E_{ij}) if and only if events Γ_{ij} and L_{ij} both happen. We have $E_{ij} = \Gamma_{ij} \cap L_{ij}$. Clearly, the edge set of $\mathbb{G}_q(n, K_n, P_n, p_n)$ is the intersection of the edge sets of $G_q(n, K_n, P_n)$ and $G(n, p_n)$, and these graphs are all defined on the vertex set $\mathcal{V}_n$. Then $\mathbb{G}_q(n, K_n, P_n, p_n)$ can be seen as the intersection of $G_q(n, K_n, P_n)$ and $G(n, p_n)$; i.e.,

$$\mathbb{G}_q(n, K_n, P_n, p_n) = G_q(n, K_n, P_n) \cap G(n, p_n).$$

In Erdős–Rényi graph $G(n, p_n)$, all edges are independent of each other. However, in graph $G_q(n, K_n, P_n)$, the edges are not independent since the events that different pairs of three nodes share q key(s) are not independent. A recent work [8] demonstrates different behavior of $G_q(n, K_n, P_n)$ and $G(n, p_n)$ in terms of clustering coefficient.

Throughout the paper, q and k are arbitrary positive integers and do not scale with n. We define $s(K_n, P_n, q)$ as the probability that two different nodes share at least q key(s) and $t(K_n, P_n, q, p_n)$ as the probability that two distinct nodes have a secure link in $\mathbb{G}_q(n, K_n, P_n, p_n)$. We often write $s(K_n, P_n, q)$ and $t(K_n, P_n, q, p_n)$ as s_n and t_n respectively for simplicity. Clearly, s_n and t_n are the edge probabilities in graphs $G_q(n, K_n, P_n)$ and $\mathbb{G}_q(n, K_n, P_n, p_n)$, respectively. From $E_{ij} = L_{ij} \cap \Gamma_{ij}$ and the independence of L_{ij} and Γ_{ij}, we obtain

$$t_n = \mathbb{P}[E_{ij}] = \mathbb{P}[L_{ij}] \cdot \mathbb{P}[\Gamma_{ij}] = p_n \cdot s_n. \tag{1}$$

By definition, s_n is determined through

$$s_n = \mathbb{P}[\Gamma_{ij}] = \sum_{u=q}^{K_n} \mathbb{P}[|S_i \cap S_j| = u], \tag{2}$$

where it holds for $P_n \geq 2K_n$ that

$$\mathbb{P}[|S_i \cap S_j| = u] = \frac{\binom{K_n}{u}\binom{P_n - K_n}{K_n - u}}{\binom{P_n}{K_n}}, \quad \text{for } u = 1, 2, \ldots, K_n, \tag{3}$$

which along with (1) and (2) induce that under $P_n \geq 2K_n$,

$$t_n = p_n \cdot \sum_{u=q}^{K_n} \frac{\binom{K_n}{u}\binom{P_n - K_n}{K_n - u}}{\binom{P_n}{K_n}}. \tag{4}$$

III. The Results

We now present the results. The natural logarithm function is given by $\ln$. We use the standard asymptotic notation $o(\cdot), \omega(\cdot), O(\cdot), \Omega(\cdot), \Theta(\cdot), \sim$ in [28, Footnote 1]. These symbols and all other limits are understood with $n \to \infty$.

Theorem 1 below presents a sharp zero–one law for k-connectivity in a graph $\mathbb{G}_q(n, K_n, P_n, p_n)$. In the secure sensor network modeled by $\mathbb{G}_q(n, K_n, P_n, p_n)$, k-connectivity enables any two sensors to have secure communication either directly or through the help of relaying nodes, even when any $k-1$ sensors are removed from the network.

Theorem 1 *For a graph $\mathbb{G}_q(n, K_n, P_n, p_n)$, with a sequence α_n defined through*

$$t_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \tag{5}$$

where t_n denoting the edge probability of $\mathbb{G}_q(n, K_n, P_n, p_n)$ is given by (4), then it holds under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$ that

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{G}_q(n, K_n, P_n, p_n) \\ \textit{is } k\textit{-connected.}\end{array}\right]$$

$$= \begin{cases} 0, & \textit{if } \lim_{n\to\infty} \alpha_n = -\infty, \quad (6a)\\ 1, & \textit{if } \lim_{n\to\infty} \alpha_n = \infty. \quad (6b)\end{cases}$$

Theorem 1 presents a strong zero–one law for k-connectivity in graph $\mathbb{G}_q(n, K_n, P_n, p_n)$, where a critical scaling of t_n can be set as $\frac{\ln n + (k-1)\ln\ln n + c}{n}$ with any constant c. In addition, the conditions $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$ in Theorem 1 are reasonable, since it is expected [2], [4], [9], [15] that for security purposes, the key pool size P_n is at least on the order of the node number n, and is much larger than the number K_n of keys on each sensor. For example, for n between 1000 and 10000, Di Pietro *et al.* [14] find that a suitable choice is to set P_n as $\frac{n \ln n}{32}$ and set K_n as $\ln n$.

IV. Related Work

We now compare Theorem 1 in this paper with related results [11], [16], [17], [28] in the literature. After the detailed comparison, we discuss more related work.

Comparison with [11]. Recently, [11, Theorem 1] presents the result on the probability of minimum degree being at least k in $\mathbb{G}_q(n, K_n, P_n, p_n)$. An extension to k-connectivity is also given in [11]. Below, we first explain that the results for k-connectivity in this paper are stronger than the k-connectivity results in [11], and then show that the proof techniques in this paper are more advanced than those in [11].

To ensure k-connectivity (i.e., the one-law part), we need $t_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ with $\lim_{n\to\infty} \alpha_n = \infty$. Then the requirement on the key ring size K_n (i.e., the number of keys on each sensor) in this paper for k-connectivity is $K_n = \Omega\Big(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\Big)$ according to Lemma 1-Property (ii) below, while the requirement on the key ring size K_n in [11] for k-connectivity satisfies $K_n = \omega\left(n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}}\right)$ according to Lemma 1-Property (iii) below, although the k-connectivity result in [11] mentions $K_n = \Omega(n^{\epsilon})$ for a positive constant ϵ (note that $\omega\left(n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}}\right)$ for $q \geq 2$ satisfies $\Omega(n^{\epsilon})$ for $\epsilon \leq 1-\frac{1}{q}$). Then we see that the order $n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}}$ of the minimal K_n in [11] is more than the square of the order $n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}$ of the minimal K_n in this paper, given $n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}} \Big/ \Big(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\Big)^2 = \ln n$.

Lemma 1 below presents the requirement on the key ring size K_n in this paper and [11] for k-connectivity.

Lemma 1 *Under $P_n = \omega(1)$, if the sequence α_n defined by (5) satisfies either $\lim_{n\to\infty} \alpha_n = \infty$ or $|\alpha_n| = o(\ln n)$, then*

(i) we have $K_n = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{P_n}\Big)$;

(ii) if $P_n = \Omega(n)$ (a condition of Theorem 1 in this paper), we have $K_n = \Omega\Big(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\Big)$;

(iii) if $\frac{K_n}{P_n} = o\left(\frac{1}{n\ln n}\right)$ (a condition in the discussion of [11]), we have $K_n = \omega\left(n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}}\right)$.

Proof of Lemma 1:

Proving property (i):

Given (5) (i.e., $t_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$), we know from either $\lim_{n\to\infty} \alpha_n = \infty$ or $|\alpha_n| = o(\ln n)$ that $t_n = \Omega\big(\frac{\ln n}{n}\big)$. Note that when $|\alpha_n| = o(\ln n)$, we have the stronger result $t_n = \Theta\big(\frac{\ln n}{n}\big)$, but we can still write $t_n = \Omega\big(\frac{\ln n}{n}\big)$. Then $t_n = \Omega\big(\frac{\ln n}{n}\big)$ and $t_n = p_n s_n$ of (1) imply

$$s_n = \Omega\bigg(\frac{\ln n}{n p_n}\bigg). \tag{7}$$

Note that the q-composite scheme enforces the natural condition $1 \leq q \leq K_n \leq P_n$. Recently, in [8, Lemma 6], Bloznelis shows $s_n \leq \frac{\left[\binom{K_n}{q}\right]^2}{\binom{P_n}{q}}$, which further means

$$s_n \leq \frac{({K_n}^q/q!)^2}{(P_n-q)^q/q!} = \frac{1}{q!}\bigg(\frac{{K_n}^2}{P_n-q}\bigg)^q \sim \frac{1}{q!}\bigg(\frac{{K_n}^2}{P_n}\bigg)^q, \tag{8}$$

where the last step uses $P_n = \omega(1)$.

We use (7) and (8) to derive $\frac{{K_n}^2}{P_n} = \Omega\Big(\big(\frac{\ln n}{np_n}\big)^{\frac{1}{q}}\Big)$, which implies

$$K_n = \sqrt{\Omega\Big(\big(\tfrac{\ln n}{np_n}\big)^{\frac{1}{q}}\Big) \cdot P_n} = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{P_n}\Big).$$

Proving property (ii):

We use the condition $P_n = \Omega(n)$ of property (ii) and the result $K_n = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{P_n}\Big)$ of property (i) to obtain $K_n = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{n}\Big) = \Omega\Big(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\Big)$.

Proving property (iii):

We use the condition $\frac{K_n}{P_n} = o\left(\frac{1}{n\ln n}\right)$ of property (iii) and the result $K_n = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{P_n}\Big)$ of property (i) to derive $K_n = \Omega\Big(n^{-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}} \cdot \sqrt{\omega(K_n n \ln n)}\Big) = \sqrt{K_n} \cdot \omega\left(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2}+\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\right)$, which further implies $K_n = \omega\left(n^{1-\frac{1}{q}}(\ln n)^{1+\frac{1}{q}}{p_n}^{-\frac{1}{q}}\right)$. ■

We have explained above that the k-connectivity results in this paper are stronger than the k-connectivity results in [11]. We now discuss the underlying reason: the proof techniques in this paper are better than those in [11]. Specifically, the challenges for k-connectivity analysis in graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ result from the dependencies between the edges as well as the intertwining between different random graphs $G_q(n, K_n, P_n)$ and $G(n, p_n)$ in the graph intersection $\mathbb{G}_q(n, K_n, P_n, p_n) = G_q(n, K_n, P_n) \cap G(n, p_n)$. The edge dependencies in $\mathbb{G}_q(n, K_n, P_n, p_n)$ exist since the events that different pairs of three nodes share q key(s) are not independent. To address the above challenges for k-connectivity analysis, we carefully analyze the graph structure of $\mathbb{G}_q(n, K_n, P_n, p_n)$ and present a direct proof. In contrast, [11] provides an indirect proof by building the relationship between $\mathbb{G}_q(n, K_n, P_n, p_n)$ and another simpler random graph where the above dependencies between the edges are canceled out. As already discussed above, the k-connectivity results derived from our direct proof are much stronger than those derived from the indirect proof in [11].

Comparison with [16], [17]. As detailed in Section II, the graph model $\mathbb{G}_q(n, K_n, P_n, p_n) = G_q(n, K_n, P_n) \cap G(n, p_n)$ studied in this paper represents the topology of a secure sensor network employing the q-composite key predistribution scheme [2] under the on/off channel model. When $q = 1$, graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ reduces to $\mathbb{G}_1(n, K_n, P_n, p_n)$, which models the topology of a secure sensor network employing the Eschenauer–Gligor key predistribution scheme under the on/off channel model. For graph $\mathbb{G}_1(n, K_n, P_n, p_n)$, Yağan [16] presents a zero–one law for connectivity, while Zhao *et al.* [17] extend the result to k-connectivity. Below we compare [16], [17] and this paper. First, our result is for general q, while the results of [16], [17] are only for the case of q being 1. Second, our result eliminates Yağan's condition on the existence of $\lim_{n\to\infty}(p_n \ln n)$, and eliminates [17]'s condition that either there exists $\epsilon > 0$ such that $s(K_n, P_n, 1)p_n n > \epsilon$ holds for all n sufficiently large or $\lim_{n\to\infty}[s(K_n, P_n, 1)p_n n] = 0$.

Comparison with [28]. Recently, [28] studies connectivity of secure sensor networks under the q-composite key predistribution scheme, when two sensors sharing q key(s) also need to satisfy constraints of the well-known disk model [15], [20], [22], [23] for direct communication; i.e., two sensors have to be within certain distance to establish a link. In addition to the disk model, [28] also considers the combination of the disk model and the on/off channel model. Although the networks in [28] represent more complex graphs, the results of [28] are just for connectivity (not for k-connectivity), and just about one-laws (not about zero–one laws). In fact, even if zero-laws are added, [28] presents weaker granularity of zero–one laws compared with this paper, as explained below. We now present the zero–one law under the disk model in detail. In secure sensor networks employing the q-composite scheme under the disk model where n sensors are independently and uniformly deployed in a network field $\mathcal{A}$ of unit area, two sensors have a secure link in between if and only if (i) they share at least q keys, and (ii) they have a distance no greater than r_n. The former constraint results in a uniform q-intersection graph $G_q(n, K_n, P_n)$ discussed before, whereas the latter constraint induces a random geometric graph $G_{RGG}(n, r_n, \mathcal{A})$, so the network is modeled by the intersection $G_q(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A})$. If the network field $\mathcal{A}$ is a unit torus so that the boundary effect [30], [31] is ignored, the one-law in [28] and its zero-law extension [31] present the following results: under $K_n = \omega(\ln n)$, $K_n = o\Big(\min\big\{\sqrt{P_n}, \frac{P_n}{n}\big\}\Big)$, $r_n = o(1)$ and

$$s(K_n, P_n, q) \cdot \pi {r_n}^2 \sim \frac{c \ln n}{n} \tag{9}$$

for a positive constant c, graph $G_q(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A})$ is disconnected *a.a.s.* if $c < 1$ and connected *a.a.s.* if $c > 1$. Note that although the results in [28] actually use $\frac{1}{q!}\big(\frac{{K_n}^2}{P_n}\big)^q \cdot \pi {r_n}^2$ in (9), we replace it by $s(K_n, P_n, q) \cdot \pi {r_n}^2$ for better comparison given $s_n \sim \frac{1}{q!}\big(\frac{{K_n}^2}{P_n}\big)^q$. If the boundary effect of network fields is considered; for example, if the network field $\mathcal{A}$ is a unit square with the boundary effect, then the results need to replace $\frac{c \ln n}{n}$ in (9) by $c \times \max\big\{\frac{\ln n + \ln[1/s(K_n, P_n, q)]}{n}, \ \frac{4 \ln[1/s(K_n, P_n, q)]}{n}\big\}$. Hence, the results considering the boundary effect under the disk model are complex and different from those under the on/off channel model. Below we discuss only the case of ignoring the boundary effect of network fields, in order to compare the disk model with the on/off channel model.

From Theorem 1, under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$, with α_n defined through

$$s(K_n, P_n, q) \cdot p_n = \frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}, \tag{10}$$

graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ (i.e., $G_q(n, K_n, P_n) \cap G(n, p_n)$) is not k-connected *a.a.s.* if $\lim_{n \to \infty} \alpha_n = -\infty$ and k-connected *a.a.s.* if $\lim_{n \to \infty} \alpha_n = \infty$.

As discussed above, the connectivity results under the disk model ignoring the boundary effect use the scaling $\frac{c \ln n}{n}$ for $c < 1$ or $c > 1$, whereas the scaling in this paper is $\frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}$ for $\lim_{n \to \infty} \alpha_n = -\infty$ or $\lim_{n \to \infty} \alpha_n = \infty$ (for $k = 1$, the scaling in this paper becomes $\frac{\ln n + \alpha_n}{n}$). The scaling $\frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}$ in this paper ($\frac{\ln n + \alpha_n}{n}$ for $k = 1$) is more fine-grained than the scaling $\frac{c \ln n}{n}$ in [28] because a deviation of $\alpha_n = \pm \Omega(\ln n)$ is required to get the zero–one law in the form of $\frac{c \ln n}{n}$ for $c < 1$ or $c > 1$, whereas in $\frac{\ln n + \alpha_n}{n}$, it suffices to have an unbounded deviation, e.g., even $\alpha_n = \pm \ln \ln \cdots \ln n$ will do. Put differently, when $k = 1$, the scaling $\frac{\ln n + \alpha_n}{n}$ in this paper covers the case of $c = 1$ in $\frac{c \ln n}{n}$, and shows that in this case, the graph could be connected or disconnected *a.a.s.*, depending on the limit of α_n. Although this paper and [28] use different scalings, we note that graph $G_q(n, K_n, P_n) \cap G(n, p_n)$ and $G_q(n, K_n, P_n) \cap G_{RGG}(n, r_n, \mathcal{A})$ have similar connectivity properties when they are *matched* through edge probabilities so that $s(K_n, P_n, q) \cdot p_n$ in (10) is equivalent with $s(K_n, P_n, q) \cdot \pi {r_n}^2$ in (9) (i.e. when p_n and $\pi {r_n}^2$ are the same).

We now explain that the results for k-connectivity under the on/off channel model in this paper are stronger than those under the disk model in [28]. Specifically, this paper considers $K_n = \Omega\Big(n^{\frac{1}{2} - \frac{1}{2q}} (\ln n)^{\frac{1}{2q}} {p_n}^{-\frac{1}{2q}}\Big)$ from Lemma 1-Property (ii), while [28] requires $K_n = \omega\Big(n^{1 - \frac{1}{q}} (\ln n)^{\frac{1}{q}} (\pi {r_n}^2)^{-\frac{1}{q}}\Big)$ according to Footnote 1 below[1]. In other words, when p_n and $\pi {r_n}^2$ are the same, the order for minimal K_n in [28] is roughly the square of the order for minimal K_n in this paper.

In addition to the above differences, similar to [11], the reference [28] also uses an indirect proof by building the relationship between the studied graph and another simpler random graph where the dependencies between the edges are canceled out. In contrast, this paper's proof is based on an direct analysis of the graph structure.

Connectivity of graph $G_q(n, K_n, P_n)$. Graph $G_q(n, K_n, P_n)$ models the topology of a secure sensor network with the q-composite key predistribution under full visibility, which means that any node pair have active channels in between so the only requirement for a secure link is the sharing of at least q keys. For $G_q(n, K_n, P_n)$, Bloznelis and Łuczak [32] have derived a zero–one law for connectivity, while an extension to k-connectivity has been given by Bloznelis and Rybarczyk [8], [33]. Other properties of $G_q(n, K_n, P_n)$ are also considered in the literature [13]. When $q = 1$, $G_1(n, K_n, P_n)$ models the topology of a secure sensor network with the Eschenauer–Gligor key predistribution scheme under full visibility. For $G_1(n, K_n, P_n)$, its connectivity has been investigated extensively [14], [15], [27], [34], [35].

Connectivity of Erdős–Rényi graph $G(n, p_n)$. Erdős and Rényi [29] introduce the random graph model $G(n, p_n)$ defined on a node set with size n such that an edge between any

[1] Although the results in [28] mention $K_n = \omega(\ln n)$, we show that the required condition satisfies $K_n = \omega\Big(n^{1 - \frac{1}{q}} (\ln n)^{\frac{1}{q}} (\pi {r_n}^2)^{-\frac{1}{q}}\Big)$. From (9), to ensure connectivity, [28] needs $s(K_n, P_n, q) \cdot \pi {r_n}^2 \sim \frac{c \ln n}{n}$ with $c > 1$, which with the condition $r_n = o(1)$ implies $s(K_n, P_n, q) = \Omega\big(\frac{\ln n}{n \cdot \pi {r_n}^2}\big)$. Then similar to the proof of Lemma 1-Property (i) (we just replace p_n therein by $\pi {r_n}^2$), we derive $K_n = \Omega\Big(n^{-\frac{1}{2q}} (\ln n)^{\frac{1}{2q}} {p_n}^{-\frac{1}{2q}} \cdot \sqrt{P_n}\Big)$, which along with $K_n = o\big(\frac{P_n}{n}\big)$ (a condition in [28]) implies $K_n = \omega\Big(n^{1 - \frac{1}{q}} (\ln n)^{\frac{1}{q}} (\pi {r_n}^2)^{-\frac{1}{q}}\Big)$.

two nodes exists with probability p_n independently of all other edges. Graph $G(n, p_n)$ models the topology induced by a sensor network under the on/off channel model (when geometric constraints for transmissions are not considered). From [29]'s result and our Theorem 1, Erdős–Rényi graph $G(n, p'_n)$ and graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ have similar connectivity properties when they are *matched* through edge probabilities (i.e. when p'_n equals t_n in the left hand side of (5)).

Connectivity of wireless networks under the disk model or its variants. Many connectivity studies [15], [20]–[23] of wireless networks use the disk model, where two nodes have to be within certain distance for direct communication. For the node distribution, two common models are as follows: 1) the uniform node distribution, where nodes are uniformly and independently deployed in a network field, and 2) the Poisson node distribution, where nodes are distributed according to a Poisson point process. Results under these two distributions are often shown to be equivalent since they can be connected via Chebyshev's inequality, which bounds the number of nodes in a Poisson point process; see (de)Poissonization in [36, Proof of Theorem 1.2] and [37, Proof of Proposition 6.1]. A wireless network with n nodes is often modeled by a *random geometric graph* [36], [37] $G_{RGG}(n, r_n, \mathcal{A})$, where n nodes are uniformly and independently distributed in a network field $\mathcal{A}$ and two nodes have an edge in between if and only if their distance is at most the transmission range r_n. (k-)Connectivity in $G_{RGG}(n, r_n, \mathcal{A})$ has been widely investigated in the literature [20], [36]–[40], where $\mathcal{A}$ may exhibit the boundary effect and letting $\mathcal{A}$ be a torus eliminates the boundary effect [30], [31]. Gupta and Kumar [20] show that with $\mathcal{D}$ being a disk of unit area, graph $G_{RGG}(n, r_n, \mathcal{D})$ is *a.a.s.* connected if and only if the sequence α_n defined by $\pi {r_n}^2 = \frac{\ln n + \alpha_n}{n}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Penrose [36] extend the result to k-connectivity for $G_{RGG}(n, r_n, \mathcal{T})$ on a torus $\mathcal{T}$. Penrose [36] also studies k-connectivity in graph $G_{RGG}(n, r_n, \mathcal{S})$ on the square $\mathcal{S}$, while the exact formula of r_n to ensure k-connectivity is obtained later by Li *et al.* [38] as well as by Wan and Yi [39]. To further characterize the k-connectivity behavior, Ta *et al.* [40] derive the phase transition width of k-connectivity in a d-dimensional random geometric graph for $d = 1, 2, 3$.

The disk model has been generalized to represent more generic wireless connections. One generalization called the *general connection model* has received much interest [30], [41]–[43]. In this model, two nodes separated by a distance x are directly connected with probability $f(x)$ for a function $f : [0, \infty) \to [0, 1]$, independent of the event that any other pair of nodes are directly connected. Mao and Anderson [30], [41] obtain a strong connectivity result of wireless networks under this general connection model and under the Poisson node distribution, where the nodes are distributed according to a Poisson point process. Their connectivity result under the general connection model generalizes the result under the (traditional) disk model by Gupta and Kumar [20] for the disk model. An early analysis of connectivity of wireless networks under the general connection model is presented by Ta *et al.* [42], where they prove the probability of connectivity is asymptotically equivalent to the probability of having no isolated node. By analyzing the number of isolated nodes under the general connection model, Mao and Anderson [43] show the differences between the dense network model, the extended network model, and the infinite network model. For a comprehensive discussion of connectivity in wireless networks under the general connection model or other alternatives, we refer interested readers to an excellent book by Mao [44].

Connectivity of wireless networks under the log-normal connection model. Despite being very useful, the above general connection model and its special case, the disk model, have a major limitation: connections are assumed to be independent in some sense; more specifically, as long as two nodes are within certain distance, they have a link in between (or with some probability in the general connection model), no matter how many other communicating nodes are nearby. The above assumption may not hold in reality due to the interference between connections. Taking into account of this, the following log-normal connection model has been considered [45], [46]. In this model, two nodes are directly connected if the received power at one node from the other node, whose attenuation obeys the log-normal model, is at least a given threshold [46]. Hekmat and Van Mieghem [45] investigate connectivity under the log-normal connection model, but their results assume that the node isolation events are independent. Without relying on this assumption, Yang *et al*. [46] provide more rigorous results by showing a necessary condition and a sufficient condition to ensure connectivity, where the bounds in the two parts differ by a constant factor only.

Connectivity of wireless information-theoretic secure networks. In addition to the use of cryptographic techniques, security of wireless networks has also been studied from the information-theoretic perspective, where physical layer techniques are utilized to protect communications [47], [48]. This thread of research is orthogonal to our work.

Connectivity of wireless networks under the disk model with unreliable links. A wireless network under the disk model on a network area $\mathcal{A}$ with unreliable links can be modeled by the intersection of a random geometric graph $G_{RGG}(n, r_n, \mathcal{A})$ and an Erdős–Rényi graph $G(n, p_n)$. Below we discuss studies of this graph intersection in the literature.

For graph $G(n, p_n) \cap G_{RGG}(n, r_n, \mathcal{A})$, Yi *et al.* [18] investigate the distribution for the number of isolated nodes. Yi *et al.* [18], [21] also explore the impact of unreliable nodes to the number of isolated nodes. Gupta and Kumar [20] present connectivity results for random geometric graph $G_{RGG}(n, r_n, \mathcal{A})$. In the same work [20], they also propose the Gupta–Kumar conjecture for connectivity in the intersection of a random geometric graph and an Erdős–Rényi graph. Specifically, the conjecture states that under $\pi {r_n}^2 p_n = \frac{\ln n + \alpha_n}{n}$, graph $G_{RGG}(n, r_n, \mathcal{D}) \cap G(n, p_n)$ on the disk $\mathcal{D}$ of unit area is *a.a.s.* connected if and only if $\lim_{n\to\infty} \alpha_n = \infty$. One significant attempt to answer the Gupta–Kumar conjecture is the work by Pishro-Nik *et al.* [23], where $G_{RGG}(n, r_n, \mathcal{S}) \cap G(n, p_n)$ on a unit square $\mathcal{S}$ is considered. Yet, they assume that $G_{RGG}(n, r_n, \mathcal{S}) \cap G(n, p_n)$ is k-connected whenever its minimum degree is at least k. This assumption is verified by Penrose [37] recently with a lengthy proof. In fact, the results of Penrose [37] also address the Gupta–Kumar conjecture. The difficulty of the conjecture is to analyze the connection structure when two distinct kinds of graphs intersect: even if individual graphs are highly connected, the resulting topology after intersection can still become disconnected. Penrose [37] obtain that the connectivity result of $G_{RGG}(n, r_n, \mathcal{T}) \cap G(n, p_n)$ on a unit torus $\mathcal{T}$ resembles the Gupta–Kumar conjecture, but the connectivity result of $G_{RGG}(n, r_n, \mathcal{S}) \cap G(n, p_n)$ on a unit square $\mathcal{S}$ is more complex. According to Penrose [37], the underlying reason for different connectivity results under the torus and under the square is the impact of the boundary effect on the asymptotics for the number of isolated nodes.

V. Ideas for Proving Theorem 1

In this section, we explain the basic ideas to prove Theorem 1. We first introduce an additional condition $|\alpha_n| = o(\ln n)$, and then use the relationship between connectivity and the absence of isolated nodes.

We first show that the extra condition $|\alpha_n| = o(\ln n)$ can be introduced in proving Theorem 1, where $|\alpha_n|$ is the absolute value of α_n. From (5) in Theorem 1, since α_n measures the deviation of the edge probability t_n from the critical scaling $\frac{\ln n + (k-1)\ln\ln n}{n}$, we call the extra condition $|\alpha_n| = o(\ln n)$ as *the confined deviation*. Then our goal is to show

$$\text{Theorem 1 with the confined deviation} \implies \text{Theorem 1.} \tag{11}$$

We write t_n back as $t(K_n, P_n, q, p_n)$ and remember that given K_n, P_n, q and p_n, one can determine α_n from (4) and (5). To show (11), we first present Lemma 2 on graph coupling [49].

Lemma 2 *For a graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$, with a sequence α_n defined by (5) (i.e., $t_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$), the following results hold:*

(a) If $\lim_{n\to\infty} \alpha_n = -\infty$, there exists a graph $\mathbb{G}_q(n, \widetilde{K_n}, \widetilde{P_n}, \widetilde{p_n})$ under $\widetilde{P_n} = \Omega(n)$, $\frac{\widetilde{K_n}^2}{\widetilde{P_n}} = o(1)$ and $t(\widetilde{K_n}, \widetilde{P_n}, q, \widetilde{p_n}) = \frac{\ln n + (k-1)\ln\ln n + \widetilde{\alpha_n}}{n}$ with $\lim_{n\to\infty} \widetilde{\alpha_n} = -\infty$ and $\widetilde{\alpha_n} = -o(\ln n)$, such that there exists a graph coupling under which $\mathbb{G}_q(n, K_n, P_n, p_n)$ is a spanning subgraph of $\mathbb{G}_q(n, \widetilde{K_n}, \widetilde{P_n}, \widetilde{p_n})$.

(b) If $\lim_{n\to\infty} \alpha_n = \infty$, there exists a graph $\mathbb{G}_q(n, \widehat{K_n}, \widehat{P_n}, \widehat{p_n})$ under $\widehat{P_n} = \Omega(n)$, $\frac{\widehat{K_n}^2}{\widehat{P_n}} = o(1)$ and $t(\widehat{K_n}, \widehat{P_n}, q, \widehat{p_n}) = \frac{\ln n + (k-1)\ln\ln n + \widehat{\alpha_n}}{n}$ with $\lim_{n\to\infty} \widehat{\alpha_n} = \infty$ and $\widehat{\alpha_n} = o(\ln n)$, such that there exists a graph coupling under which $\mathbb{G}_q(n, K_n, P_n, p_n)$ is a spanning supergraph of $\mathbb{G}_q(n, \widehat{K_n}, \widehat{P_n}, \widehat{p_n})$.

For any graph that is not k-connected, its spanning subgraph is not k-connected. Also, for any k-connected graph, its spanning supergraph is k-connected. Given the above, Lemma 2 clearly implies (11). Hence, in proving Theorem 1, we can always assume the confined deviation $|\alpha_n| = o(\ln n)$. In the rest of the paper, we often write $\mathbb{G}_q(n, K_n, P_n, p_n)$ as $\mathbb{G}_q$ for notation brevity.

Given the conditions of Theorem 1 (i.e., $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$), and the extra $|\alpha_n| = o(\ln n)$ introduced in Section V, we utilize Lemma 1 to have $K_n = \Omega\Big(n^{\frac{q-1}{2q}}(\ln n)^{\frac{1}{2q}}\Big) = \omega(1)$. Then given $K_n = \omega(1)$ and $\frac{{K_n}^2}{P_n} = o(1)$, we use [11, Theorem 1] to obtain

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{G}_q \text{ has a minimum} \\ \text{node degree at least } k.\end{array}\right]$$
$$= \begin{cases} 0, & \text{if } \lim_{n\to\infty} \alpha_n = -\infty, \quad \text{(12a)} \\ 1, & \text{if } \lim_{n\to\infty} \alpha_n = \infty. \quad \text{(12b)} \end{cases}$$

Since a necessary condition for a graph to be k-connected is that the minimum node degree is at least k, (12a) clearly implies the zero-law (6a) of k-connectivity. Moreover, given (12b), the one-law (6b) of k-connectivity will be proved once we show Lemma 3 below. Note that we can introduce $|\alpha_n| = o(\ln n)$ from the argument in Section V.

Lemma 3 *For a graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$, if the sequence α_n defined by (5) satisfies $\lim_{n\to\infty} \alpha_n = \infty$ and $|\alpha_n| = o(\ln n)$, then*

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l}\mathbb{G}_q \textit{ has a minimum node degree at least } k, \\ \textit{but is not } k\textit{-connected.}\end{array}\right] = 0. \tag{13}$$

Lemma 3 is established in Section VI. Due to space limitation, we provide many details in the full version [50].

VI. Establishing Lemma 3

For a graph, let its *node connectivity* be the minimum number of nodes that need to be removed to disconnect the remaining nodes from each other. Then a graph is k-connected if and only if its node connectivity is at least k. A graph is not k-connected if and only if its node connectivity is less than k. To prove Lemma 3, we have

$$\mathbb{P}\left[\begin{array}{l}\mathbb{G}_q \text{ has a minimum node degree at least } k, \\ \text{but is not } k\text{-connected.}\end{array}\right]$$
$$\leq \sum_{\ell=0}^{k-1} \mathbb{P}\left[\begin{array}{l}\mathbb{G}_q\text{'s node connectivity equals } \ell, \text{ and} \\ \mathbb{G}_q\text{'s minimum node degree is greater than } \ell\end{array}\right]. \tag{14}$$

We define event $F_{n,\ell}$ as follows:

$$\begin{aligned} F_{n,\ell} :\ & \text{the event that } \mathbb{G}_q\text{'s node connectivity equals } \ell, \\ & \text{and } \mathbb{G}_q\text{'s minimum node degree is greater than } \ell. \end{aligned} \tag{15}$$

Then the summation in (14) becomes $\sum_{\ell=0}^{k-1} \mathbb{P}[F_{n,\ell}]$. The idea [17] in establishing Lemma 3 is to find an upper bound on $\sum_{\ell=0}^{k-1} \mathbb{P}[F_{n,\ell}]$ and show that this bound goes to zero as $n \to \infty$.

We begin by finding the needed upper bound. Let $\mathcal{N}$ denote the collection of all non-empty subsets of the node set $\{v_1, \ldots, v_n\}$ in graph $\mathbb{G}_q$. Recalling that S_i denotes the set of K_n keys on node v_i, we introduce an event $E_n(\boldsymbol{X}_n)$ in the following manner:

$$E_n(\boldsymbol{X}_n) = \bigcup_{T \subseteq \mathcal{N}:\ |T| \geq 1} \left[|\cup_{j\in T} S_j| \ \leq\ X_{n,|T|}\right]$$

where $\boldsymbol{X}_n = [X_{n,1},\ X_{n,2},\ \ldots,\ X_{n,n}]$ is an n-dimensional integer-valued array. We define r_n^* by

$$r_n^* := \min\left(\left\lfloor \frac{P_n}{K_n}\right\rfloor,\ \left\lfloor \frac{n}{2}\right\rfloor\right). \tag{16}$$

We set

$$X_{n,i} = \begin{cases} K_n, & \text{for } i = 1, \\ \max\{\lfloor (1+\varepsilon)K_n\rfloor, \lfloor \lambda K_n i\rfloor\}, & \text{for } i = 2, \ldots, r_n^*, \\ \lfloor \mu P_n\rfloor, & \text{for } i = r_n^*+1, \ldots, n, \end{cases} \tag{17}$$

for an arbitrary constant $0 < \varepsilon < 1$ and constants λ and μ specified below. Recalling the condition $P_n = \Omega(n)$, we let $P_n \geq \sigma n$ for all n sufficiently large, where σ is certain positive constant. We select λ and μ satisfying $0 < \lambda < \frac{1}{2}$, $\max\left(2\lambda\sigma, \lambda\left(\frac{e^2}{\sigma}\right)^{\frac{\lambda}{1-2\lambda}}\right) < 1$, $0 < \mu < \frac{1}{2}$ and $\max\left(2\left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}, \sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right) < 1$, such that the event $E_n(\boldsymbol{X}_n)$ defined above satisfies

$$\lim_{n\to\infty} \mathbb{P}\left[E_n(\boldsymbol{X}_n)\right] = 0. \tag{18}$$

Given $\mathbb{P}[F_{n,\ell}] \leq \mathbb{P}[E_n(\boldsymbol{X}_n)] + \mathbb{P}\left[F_{n,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right]$, and (18), we will obtain the result $\lim_{n\to\infty}\mathbb{P}[F_{n,\ell}] = 0$ once establishing the following proposition. After showing $\lim_{n\to\infty}\mathbb{P}[F_{n,\ell}] = 0$, since k does not scale with n, we further derive $\lim_{n\to\infty}(\sum_{\ell=0}^{k-1}\mathbb{P}[F_{n,\ell}]) = 0$, which along with (14) and (15) completes proving Lemma 3.

Proposition 1 *For a graph $\mathbb{G}_q(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$, if the sequence α_n defined by (5) (i.e., $t_n = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$) satisfies $\lim_{n\to\infty}\alpha_n = \infty$ and $|\alpha_n| = o(\ln n)$, then for $\ell = 0, 1, \ldots, k-1$, we have $\lim_{n\to\infty}\mathbb{P}\left[F_{n,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right] = 0$.*

Proof of Proposition 1:

Recall that the node set of graph $\mathbb{G}_q$ is $\mathcal{V}_n = \{v_1, v_2, \ldots, v_n\}$, and $F_{n,\ell}$ denotes the event that graph $\mathbb{G}_q$'s node connectivity equals ℓ, and $\mathbb{G}_q$'s minimum node degree is greater than ℓ. Below we analyze the graph structure of $\mathbb{G}_q$ when event $F_{n,\ell}$ happens. When graph $\mathbb{G}_q$'s node connectivity equals ℓ, we have by definition that there exists a subset U of the node set $\mathcal{V}_n = \{v_1, v_2, \ldots, v_n\}$ nodes with $|U| = \ell$ such that $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ is disconnected, where $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ denotes the subgraph of $\mathbb{G}_q$ with the node set restricted to $\mathcal{V}_n \setminus U$. We consider $n \geq \ell + 3$ so $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ has at least three nodes. Since $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ is disconnected, $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ has a set of components (say m components where $m \geq 2$) such that the following ⓐ and ⓑ both happen: ⓐ each component is either self-connected or has only one node; ⓑ different components are disconnected from each other. Considering that $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ has m components in total for some $m \geq 2$, given $|\mathcal{V}_n \setminus U| = n - \ell$, we pick one component with at most $\lfloor \frac{n-\ell}{2}\rfloor$ nodes, and call this component S. Below we explain that S cannot have only one node. By contradiction, if S has only one node, supposing that this node is v_*, then v_* does not have neighbors in $\mathcal{V}_n \setminus U$, meaning that v_*'s neighbors in $\mathbb{G}_q$ all belong to the set U. Hence, with $|U| = \ell$, v_*'s degree in $\mathbb{G}_q$ is at most ℓ, contradicting with the condition that $\mathbb{G}_q$'s minimum degree is greater than ℓ. Summarizing the above analysis, whenever $F_{n,\ell}$ happens, there exist disjoint subsets U, S of the node set $\mathcal{V}_n = \{v_1, v_2, \ldots, v_n\}$ with $|U| = \ell$ and $2 \leq |S| \leq \lfloor \frac{n-\ell}{2}\rfloor$ such that

① with $\mathbb{G}_q(S)$ denoting the subgraph of $\mathbb{G}_q$ with the node set restricted to S, $\mathbb{G}_q(S)$ is connected;

② with $\mathbb{G}_q(\mathcal{V}_n \setminus U)$ denoting the subgraph of $\mathbb{G}_q$ with the node set restricted to $\mathcal{V}_n \setminus U$, S is isolated in $\mathbb{G}_q(\mathcal{V}_n \setminus U)$.

We further analyze the graph structure of $\mathbb{G}_q$ when event $F_{n,\ell}$ happens. We let $v_\#$ be an arbitrary node in set U (recall $|U| = \ell$). Since graph $\mathbb{G}_q$'s node connectivity equals ℓ under $F_{n,\ell}$, deleting the $\ell - 1$ nodes of $U \setminus \{v_\#\}$ in $\mathbb{G}_q$ will still preserve connectivity of the remaining graph $\mathbb{G}_q((\mathcal{V}_n \setminus U) \cup \{v_\#\})$. Since we know from ② above that there is no edge between any node in S and any node in $(\mathcal{V}_n \setminus U) \setminus S$, to ensure connectivity of $\mathbb{G}_q((\mathcal{V}_n \setminus U) \cup \{v_\#\})$, we have

③ for any node $v_\#$ in set U, $v_\#$ has at least one neighbor in S and at least one neighbor in $(\mathcal{V}_n \setminus U) \setminus S$.

Now we define $C_n(S)$ and $D_n(S, U)$ to represent ① and ② above. In addition, we define $B_n(S, U)$ as the event that any node in set U has at least one neighbor in S; i.e., $B_n(S, U)$ relaxes the requirement in ③ above. Summarizing the above, we know that $F_{n,\ell}$ is a subevent of $\bigcup_{\substack{|U|=\ell,\\ 2\leq|S|\leq\lfloor\frac{n-\ell}{2}\rfloor}} [B_n(S, U) \cap C_n(S) \cap D_n(S, U)]$. We let $\mathcal{N}_{n,\ell}$ be the collection of the subsets of $\mathcal{V}_n$ with exactly ℓ elements, and let $\mathcal{N}_r(\mathcal{V}_n \setminus U)$ be the collection of the subsets of $\mathcal{V}_n \setminus U$ with exactly r elements. Then from the union bound, we obtain

$$\begin{aligned} &\mathbb{P}\left[F_{n,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right] \\ &\leq \sum_{U\in\mathcal{N}_{n,\ell}} \sum_{r=2}^{\lfloor\frac{n-\ell}{2}\rfloor} \sum_{S\in\mathcal{N}_r(\mathcal{V}_n\setminus U)} \\ &\qquad \mathbb{P}\left[B_n(S, U) \cap C_n(S) \cap D_n(S, U) \cap \overline{E_n(\boldsymbol{X}_n)}\right]. \end{aligned} \tag{19}$$

For each $r = 2, 3, \ldots, \lfloor \frac{n-\ell}{2}\rfloor$, when S is $\{v_1, \ldots, v_r\}$, and U is $\{v_{r+1}, \ldots, v_{r+\ell}\}$, we let $B_n(S, U), C_n(S), D_n(S, U)$ be $B_{n,r,\ell}, C_{n,r}, D_{n,r,\ell}$. We further define $A_{n,r,\ell} := B_{n,r,\ell} \cap C_{n,r} \cap D_{n,r,\ell}$. Then by exchangeability, we obtain from (19) that

$$\begin{aligned} &\mathbb{P}\left[F_{n,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right] \\ &\leq \sum_{r=2}^{\lfloor\frac{n-\ell}{2}\rfloor} \binom{n}{\ell}\binom{n-\ell}{r}\, \mathbb{P}\left[A_{n,r,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right], \end{aligned} \tag{20}$$

where we use $|\mathcal{N}_{n,\ell}| = \binom{n}{\ell}$ and $|\mathcal{N}_r(\mathcal{V}_n \setminus U)| = \binom{n-\ell}{r}$. Then the proof of Proposition 1 will be completed once we show

$$\lim_{n\to\infty} \sum_{r=2}^{\lfloor\frac{n-\ell}{2}\rfloor} \binom{n}{\ell}\binom{n-\ell}{r}\, \mathbb{P}\left[A_{n,r,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right] = 0,$$
$$\text{for } \ell = 0, 1, \ldots, k-1. \tag{21}$$

We now analyze $A_{n,r,\ell} := B_{n,r,\ell} \cap C_{n,r} \cap D_{n,r,\ell}$. For each $j = r+1, \ldots, n$, we define $u_{r,j}$ as the set of nodes, each of which belongs to $\{v_1,\ldots,v_r\}$ and also has an "on" channel with node v_j. For $j=r+1,\ldots r+\ell$, we define

$$\mathcal{B}^{(j)}_{n,r,\ell} := \cup_{i\in u_{r,j}}\Gamma_{ij}, \tag{22}$$

and for $j=r+\ell+1,\ldots,n$, we define

$$\mathcal{D}^{(j)}_{n,r,\ell} := \cap_{i\in u_{r,j}}\overline{\Gamma_{ij}}. \tag{23}$$

Then we have

$$B_{n,r,\ell} = \bigcap_{j=r+1}^{r+\ell}\mathcal{B}^{(j)}_{n,r,\ell}, \text{ and } D_{n,r,\ell} \ = \bigcap_{j=r+\ell+1}^{n}\mathcal{D}^{(j)}_{n,r,\ell}. \tag{24}$$

Conditioning on the random variables $\{S_i,\ i=1,\ldots,r\}$ and $\{\mathbf{1}[L_{ij}],\ i,j=1,\ldots,r\}$ (these two sets determine the event $C_{n,r}$), the events $\{\mathcal{B}^{(j)}_{n,r,\ell},\ j=r+1,\ldots,r+\ell\}$ and $\{\mathcal{D}^{(j)}_{n,r,\ell},\ j=r+\ell+1,\ldots,n\}$ are all conditionally independent. Then we conclude via $A_{n,r,\ell} := B_{n,r,\ell}\cap C_{n,r}\cap D_{n,r,\ell}$ and (24) that

$$\begin{aligned}
&\mathbb{P}\left[A_{n,r,\ell}\cap\overline{E_n(\boldsymbol{X}_n)}\right]\\
&=\mathbb{E}\left[\mathbf{1}\left[C_{n,r}\cap\overline{E_n(\boldsymbol{X}_n)}\right]\right.\\
&\quad\times\prod_{j=r+1}^{r+\ell}\mathbb{P}\left[\mathcal{B}^{(j)}_{n,r,\ell}\ \middle|\ \begin{array}{ll} S_i, & i=1,\ldots,r,\\ \mathbf{1}[L_{ij}], & i=1,\ldots,r,\\ & j=r+1,\ldots r+\ell.\end{array}\right]\\
&\quad\left.\times\prod_{j=r+\ell+1}^{n}\mathbb{P}\left[\mathcal{D}^{(j)}_{n,r,\ell}\ \middle|\ \begin{array}{ll} S_i, & i=1,\ldots,r,\\ \mathbf{1}[L_{ij}], & i=1,\ldots,r,\\ & j=r+\ell+1,\ldots n.\end{array}\right]\right],
\end{aligned} \tag{25}$$

where the expectation is taken over random variables $\{S_i,\ i=1,\ldots,r\}$ and $\left\{\mathbf{1}[L_{ij}],\ \begin{array}{l} i=1,\ldots,r,\\ j=r+1,\ldots n.\end{array}\right\}$.

For $j=r+1,\ldots,r+\ell$, from (22), it holds by the union bound that

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{B}^{(j)}_{n,r,\ell}\ \middle|\ \begin{array}{ll} S_i, & i=1,\ldots,r,\\ \mathbf{1}[L_{ij}], & i=1,\ldots,r,\\ & j=r+1,\ldots r+\ell.\end{array}\right]\\
&\leq\sum_{i\in u_{r,j}}\mathbb{P}\big[\Gamma_{ij}\mid S_i\big]=\sum_{i\in u_{r,j}}s_n=s_n|u_{r,j}|.
\end{aligned} \tag{26}$$

With $u_{r,j}=\sum_{i=1}^{r}\mathbf{1}[L_{ij}]$, $|u_{r,j}|$ follows a binomial distribution with r trials and the success probability p_n in each trial. Hence, from $t_n=s_np_n$, it holds that

$$\mathbb{E}\left[s_n|u_{r,j}|\right]=s_n\cdot rp_n=rt_n. \tag{27}$$

Given $\{S_i,\ i=1,\ldots,r\}$ and $\{\mathbf{1}[L_{ij}],\ i,j=1,\ldots,r\}$, the probability of $\left[|(\bigcup_{i\in u_{r,j}}S_i)\cap S_j|\ \geq\ q\right]$ is given by $\frac{\binom{|\cup_{i\in u_{r,j}}S_i|}{q}\binom{K_n}{q}}{\binom{P_n}{q}}$. Then on the event $\overline{E_n(\boldsymbol{X}_n)}$ in (16) which ensures $|\cup_{i\in u_{r,j}}S_i|>X_{n,|u_{r,j}|}$, it follows that

$$\mathbb{P}\left[\mathcal{D}^{(j)}_{n,r,\ell}\ \middle|\ \begin{array}{ll} S_i, & i=1,\ldots,r,\\ \mathbf{1}[L_{ij}], & i=1,\ldots,r,\\ & j=r+\ell+1,\ldots n.\end{array}\right]\leq 1-\frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}. \tag{28}$$

Below we we will prove that on the event $\overline{E_n(\boldsymbol{X}_n)}$, it holds for all n sufficiently large that

$$\mathbb{E}\left[1-\frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}\right]\leq g_{r,n}, \tag{29}$$

for function $g_{r,n}$ defined by

$$g_{r,n}:=\begin{cases}\min\left\{e^{-(1+\frac{\varepsilon_2}{2})t_n},e^{-\lambda_2t_nr}\right\}, & \text{for } r=2,\ldots,r_n^*,\\ e^{-\lambda_2t_nr}+e^{-\mu_2K_n}, & \text{for } r=r_n^*+1,\ldots,n.\end{cases} \tag{30}$$

In view of (25)–(29), considering the mutual independence among $\left\{|u_{r,j}|\right\}\big|_{j=r+1,\ldots,n}$ and $\mathbf{1}\left[C_{n,r}\cap\overline{E_n(\boldsymbol{X}_n)}\right]$, and using $\mathbb{E}\big[\mathbf{1}[C_{n,r}\cap\overline{E_n(\boldsymbol{X}_n)}]\big]\leq\mathbb{P}[C_{n,r}]$, we obtain

$$\begin{aligned}
&\mathbb{P}\left[A_{n,r}\cap\overline{E_n(\boldsymbol{X}_n)}\right]\\
&\leq\mathbb{P}[C_{n,r}]\times\min\{(rt_n)^\ell,\ 1\}\times {g_{r,n}}^{n-r-\ell}.
\end{aligned} \tag{31}$$

To establish (29), below we we first prove that on the event $\overline{E_n(\boldsymbol{X}_n)}$, it holds for all n sufficiently large that

$$1-\frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}\leq f(|u_{r,j}|) \tag{32}$$

for $f(|u_{r,j}|)$ defined by

$$\begin{aligned}
&f(|u_{r,j}|):=\\
&\begin{cases}1-s_n, & \text{for } |u_{r,j}|=1,\\ (1-s_n)^{\max\{(1+\varepsilon_2),\ \lambda_2|u_{r,j}|\}}, & \text{for } |u_{r,j}|=2,\ldots,r_n^*,\\ e^{-\mu_2K_n} & \text{for } |u_{r,j}|=r_n^*+1,\ldots,n.\end{cases}
\end{aligned} \tag{33}$$

We now establish (32) and use (32) to show (29). We will use the following result given by [8, Lemma 6]:

$$s_n\leq\frac{\left[\binom{K_n}{q}\right]^2}{\binom{P_n}{q}}. \tag{34}$$

For $|u_{r,j}|=1$, it holds that

$$1-\frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}=1-\frac{\left[\binom{K_n}{q}\right]^2}{\binom{P_n}{q}}\leq 1-s_n. \tag{35}$$

For $|u_{r,j}|=2,\ldots,r_n^*$, it holds that

$$\begin{aligned}
&\frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}\geq s_n\cdot\frac{\binom{X_{|u_{r,j}|,n}}{q}}{\binom{K_n}{q}}\\
&\qquad=s_n\cdot\max\left\{\frac{\binom{\lfloor(1+\varepsilon)K_n\rfloor}{q}}{\binom{K_n}{q}},\frac{\binom{\lfloor\lambda K_n|u_{r,j}|\rfloor}{q}}{\binom{K_n}{q}}\right\}.
\end{aligned} \tag{36}$$

From Lemma 1-Property (ii), we obtain $K_n = \Omega\Big(n^{\frac{1}{2}-\frac{1}{2q}}(\ln n)^{\frac{1}{2q}}{p_n}^{-\frac{1}{2q}}\Big) = \omega(1)$. As proved in the full version [50], given $K_n=\omega(1)$, for any constants ε_2 and λ_2

satisfying $0 < \varepsilon_2 < (1+\varepsilon)^q - 1$ and $0 < \lambda_2 < \lambda^q < \left(\frac{1}{2}\right)^q < 1$, we have for all n sufficiently large that

$$\max\left\{ \frac{\binom{\lfloor(1+\varepsilon)K_n\rfloor}{q}}{\binom{K_n}{q}},\ \frac{\binom{\lfloor\lambda K_n|u_{r,j}|\rfloor}{q}}{\binom{K_n}{q}} \right\} \geq \max\{(1+\varepsilon_2),\ \lambda_2|u_{r,j}|\}. \tag{37}$$

From $0 \leq s_n \leq 1$ and $\max\{(1+\varepsilon_2), \lambda_2|u_{r,j}|\} > 1$, we obtain

$$1 - s_n \cdot \max\{(1+\varepsilon_2), \lambda_2|u_{r,j}|\} \leq (1-s_n)^{\max\{(1+\varepsilon_2),\lambda_2|u_{r,j}|\}}. \tag{38}$$

Using (37) (38) in (36), we have for $|u_{r,j}| = 2, \ldots, r_n^*$ that

$$1 - \frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}} \leq (1-s_n)^{\max\{(1+\varepsilon_2),\lambda_2|u_{r,j}|\}}. \tag{39}$$

For $|u_{r,j}| = r_n^*+1, \ldots, n$, it holds that

$$1 - \frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}} = 1 - \frac{\binom{\lfloor\mu P_n\rfloor}{q}\binom{K_n}{q}}{\binom{P_n}{q}} \leq e^{-\frac{\binom{\mu P_n}{q}\binom{K_n}{q}}{\binom{P_n}{q}}}. \tag{40}$$

As proved by in the full version [50], for any constant μ_2 satisfying $0 < \mu_2 < (q!)^{-1}\mu^q$, we obtain for all n sufficiently large that

$$\frac{\binom{\lfloor\mu P_n\rfloor}{q}\binom{K_n}{q}}{\binom{P_n}{q}} \geq \mu_2 K_n, \tag{41}$$

which with (40) further implies

$$1 - \frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}} \leq e^{-\mu_2 K_n} \text{ for } |u_{r,j}| = r_n^*+1, \ldots, n. \tag{42}$$

Summarizing (35) (39) and (42), on the event $\overline{E_n(\boldsymbol{X}_n)}$, we obtain (32) for all n sufficiently large. Now we use (32) to show (29). From (32) and the binomial distribution of $|u_{r,j}|$, for $r = 2, \ldots, r_n^*$, it holds that

$$\mathbb{E}\left[1 - \frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}\right] \tag{43}$$

$$\leq (1-p_n)^r + rp_n(1-p_n)^{r-1}(1-s_n) + [1-(1-p_n)^r - rp_n(1-p_n)^{r-1}](1-s_n)^{1+\varepsilon_2}. \tag{44}$$

For $r = 2, \ldots, r_n^*$, based on (44) and $t_n = p_n s_n$, we can further show

$$(43) \leq e^{-(1+\frac{\varepsilon_2}{2})t_n}. \tag{45}$$

Given (32) and $0 < \lambda_2 < 1$, we obtain that $1 - \frac{\binom{X_{|u_{r,j}|,n}}{q}\binom{K_n}{q}}{\binom{P_n}{q}}$ is upper bounded by $(1-s_n)^{\lambda_2|u_{r,j}|}$ for $|u_{r,j}| = 0, \ldots, r_n^*$. Then it holds for $r = 2, \ldots, r_n^*$ that

$$(43) \leq \mathbb{E}\left[(1-s_n)^{\lambda_2|u_{r,j}|}\right] = \left\{1 - p_n[1-(1-s_n)^{\lambda_2}]\right\}^r.$$

Then we obtain for $r = 2, \ldots, r_n^*$ that

$$(43) \leq e^{-\lambda_2 t_n r}, \tag{46}$$

by deriving $\left\{1 - p_n[1-(1-s_n)^{\lambda_2}]\right\}^r \leq (1 - p_n \cdot \lambda_2 s_n)^r \leq e^{-\lambda_2 p_n s_n r} = e^{-\lambda_2 t_n r}$, where we use $(1-s_n)^{\lambda_2} \leq 1 - \lambda_2 s_n$ due to $0 \leq s_n \leq 1$ and $0 < \lambda_2 < \lambda^q < \left(\frac{1}{2}\right)^q < 1$, the fact that $1 + x \leq e^x$ for any real x, and also $p_n s_n = t_n$.

On the range $r = r_n^*+1, \ldots, n$, we establish

$$\begin{aligned}(43) &\leq \mathbb{E}\big[(1-s_n)^{\lambda_2|u_{r,j}|} \cdot \mathbf{1}\left[|u_{r,j}| \leq r_n^*\right]\big] \\ &\quad + \mathbb{E}\big[e^{-\mu_2 K_n} \cdot \mathbf{1}\left[|u_{r,j}| > r_n^*\right]\big] \\ &\leq \mathbb{E}\big[(1-s_n)^{\lambda_2|u_{r,j}|}\big] + e^{-\mu_2 K_n} \\ &\leq e^{-\lambda_2 t_n r} + e^{-\mu_2 K_n},\end{aligned} \tag{47}$$

where the last step uses the result proved in (46).

The result (29) is now proved given (45) (46) and (47). Then as explained, we obtain (31), where the term $\mathbb{P}[C_{n,r}]$ in (31) is bounded below.

To bound $\mathbb{P}[C_{n,r}]$, we let $\mathbb{G}_q(r)$ be the subgraph of $\mathbb{G}_q$ restricted to the vertex set $\{v_1, \ldots, v_r\}$, and note that $C_{n,r}$ means the event of $\mathbb{G}_q(r)$ being connected. Let $\mathcal{T}_r$ denote the collection of all spanning trees on the vertex set $\{v_1, \ldots, v_r\}$. We can show for any $T \in \mathcal{T}_r$ that the probability of T being a subgraph of $\mathbb{G}_q(r)$ is ${t_n}^{r-1}$, where we recall t_n as the edge probability in $\mathbb{G}_q$. By Cayley's formula [51], there are r^{r-2} spanning trees on r vertices. This and the above result $\mathbb{P}[T \subseteq \mathbb{G}_q(r)] = {t_n}^{r-1}$ for any $T \in \mathcal{T}_r$, along with the union bound and $\mathbb{P}[C_{n,r}] \leq 1$, together induce

$$\mathbb{P}[C_{n,r}] \leq \min\{r^{r-2}{t_n}^{r-1},\ 1\}. \tag{48}$$

Applying (48) to (31), we obtain

$$\mathbb{P}\left[A_{n,r,\ell} \cap \overline{E_n(\boldsymbol{X}_n)}\right] \leq \min\{r^{r-2}{t_n}^{r-1},\ 1\} \times \min\{(rt_n)^\ell,\ 1\} \times {g_{r,n}}^{n-r-\ell}. \tag{49}$$

The rest of the proof is using (49) to prove (21). Due to space limitation, we provide the details in the full version [50]. ■

VII. Conclusion

In this paper, we present a sharp zero–one law for secure k-connectivity in a wireless sensor network under the q-composite key predistribution scheme with unreliable links. Secure k-connectivity ensures that any two sensors can find a path in between for secure communication even when at most $k-1$ sensors fail. The network is modeled by composing a uniform q-intersection graph with an Erdős–Rényi graph, where the former characterizes the q-composite key predistribution scheme and the latter captures link unreliability.

References

[1] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[2] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *ACM Conference on Computer and Communications Security (CCS)*, 2002, pp. 41–47.

[3] K. Lu, Y. Qian, M. Guizani, and H.-H. Chen, "A framework for a distributed key management scheme in heterogeneous wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, pp. 639–647, 2008.

[4] D. H. Yum and P. J. Lee, "Exact formulae for resilience in random key predistribution schemes," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1638–1642, 2012.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *ACM Conference on Computer and Communications Security (CCS)*, 2003, pp. 62–72.

[6] T. Kwon, J. Lee, and J. Song, "Location-based pairwise key predistribution for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 11, pp. 5436–5442, 2009.

[7] O. Yağan, "Zero–one laws for connectivity in inhomogeneous random key graphs," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4559–4574, 2016.

[8] M. Bloznelis, "Degree and clustering coefficient in sparse random intersection graphs," *The Annals of Applied Probability*, vol. 23, no. 3, pp. 1254–1289, 2013.

[9] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE Symposium on Security and Privacy*, May 2003, pp. 197–213.

[10] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, 2009.

[11] J. Zhao, "Topological properties of wireless sensor networks under the q-composite key predistribution scheme with unreliable links," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1789–1802, June 2017.

[12] J. Zhao, O. Yağan, and V. Gligor, "On topological properties of wireless sensor networks under the q-composite key predistribution scheme with on/off channels," in *IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 1131–1135.

[13] M. Bloznelis, J. Jaworski, and K. Rybarczyk, "Component evolution in a secure wireless sensor network," *Networks*, vol. 53, pp. 19–26, January 2009.

[14] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 3, pp. 13:1–13:22, 2008.

[15] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Connectivity properties of secure wireless sensor networks," in *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2004, pp. 53–58.

[16] O. Yağan, "Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3821–3835, June 2012.

[17] J. Zhao, O. Yağan, and V. Gligor, "k-Connectivity in random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3810–3836, July 2015.

[18] C.-W. Yi, P.-J. Wan, K.-W. Lin, and C.-H. Huang, "Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with unreliable nodes and links," in *IEEE Global Communications Conference (GLOBECOM)*, Nov 2006.

[19] R. Eletreby and O. Yağan, "Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős–Rényi graphs," in *IEEE International Symposium on Information Theory (ISIT)*, 2017, pp. 2920–2924.

[20] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *IEEE Conference on Decision and Control (CDC)*, 1998, pp. 547–566.

[21] C.-W. Yi, P.-J. Wan, X.-Y. Li, and O. Frieder, "Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with Bernoulli nodes," *IEEE Transactions on Communications*, vol. 54, no. 3, pp. 510–517, 2006.

[22] Y. W. Law, L.-H. Yen, R. Di Pietro, and M. Palaniswami, "Secure k-connectivity properties of wireless sensor networks," in *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS)*, Oct 2007, pp. 1–6.

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

[24] W. Wang, M. Chatterjee, and K. Kwiat, "Cooperation in wireless networks with unreliable channels," *IEEE Transactions on Communications*, vol. 59, no. 10, pp. 2808–2817, 2011.

[25] F. Yavuz, J. Zhao, O. Yağan, and V. Gligor, "k-Connectivity in random k-out graphs intersecting Erdős–Rényi graphs," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1677–1692, 2017.

[26] S. Zhao, L. Fu, X. Wang, and Q. Zhang, "Fundamental relationship between nodedensity and delay in wireless ad hoc networks with unreliable links," in *ACM Conference on Mobile Computing and Networking (MobiCom)*, 2011, pp. 337–348.

[27] O. Yağan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2983–2999, May 2012.

[28] J. Zhao, "Probabilistic key predistribution in mobile networks resilient to node-capture attacks," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6714–6734, October 2017.

[29] P. Erdős and A. Rényi, "On random graphs, I," *Publicationes Mathematicae (Debrecen)*, vol. 6, no. 1, pp. 290–297, 1959.

[30] G. Mao and B. D. O. Anderson, "Connectivity of large wireless networks under a general connection model," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1761–1772, 2013.

[31] J. Zhao, "On resilience and connectivity of secure wireless sensor networks under node capture attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 557–571, March 2017.

[32] M. Bloznelis and T. Łuczak, "Perfect matchings in random intersection graphs," *Acta Mathematica Hungarica*, vol. 138, no. 1-2, pp. 15–33, 2013.

[33] M. Bloznelis and K. Rybarczyk, "k-Connectivity of uniform s-intersection graphs," *Discrete Mathematics*, vol. 333, no. 1, pp. 94–100, 2014.

[34] K. Rybarczyk, "Diameter, connectivity and phase transition of the uniform random intersection graph," *Discrete Mathematics*, vol. 311, no. 17, pp. 1998–2019, 2011.

[35] S. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics*, vol. 309, no. 16, pp. 5130–5140, August 2009.

[36] M. D. Penrose, "On k-connectivity for a geometric random graph," *Random Structures & Algorithms*, vol. 15, no. 2, pp. 145–164, 1999.

[37] M. D. Penrose, "Connectivity of soft random geometric graphs," *The Annals of Applied Probability*, vol. 26, no. 2, pp. 986–1028, 2016.

[38] X. Li, P. Wan, Y. Wang, and C. Yi, "Fault tolerant deployment and topology control in wireless networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2003, pp. 117–128.

[39] P.-J. Wan and C.-W. Yi, "Asymptotic critical transmission radius and critical neighbor number for k-connectivity in wireless ad hoc networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2004, pp. 1–8.

[40] X. Ta, G. Mao, and B. D. O. Anderson, "On the phase transition width of k-connectivity in wireless multihop networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 7, pp. 936–949, 2009.

[41] G. Mao and B. D. O. Anderson, "On the asymptotic connectivity of random networks under the random connection model," in *IEEE Conference on Computer Communications (INFOCOM)*, 2011, pp. 631–639.

[42] X. Ta, G. Mao, and B. D. O. Anderson, "On the connectivity of wireless multi-hop networks with arbitrary wireless channel models," *IEEE Communications Letters*, vol. 13, no. 3, pp. 181–183, 2009.

[43] G. Mao and B. D. O. Anderson, "Towards a better understanding of large-scale network models," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 408–421, 2012.

[44] G. Mao, *Connectivity of Communication Networks*. Springer, 2017, ISBN: 978-3-319-52989-9.

[45] R. Hekmat and P. Van Mieghem, "Connectivity in wireless ad-hoc networks with a log-normal radio model," *Mobile Networks and Applications*, vol. 11, no. 3, pp. 351–360, 2006.

[46] T. Yang, G. Mao, and W. Zhang, "Connectivity of large-scale CSMA networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 6, pp. 2266–2275, 2012.

[47] M. Haenggi, "The secrecy graph and some of its properties," in *IEEE International Symposium on Information Theory (ISIT)*, 2008, pp. 539–543.

[48] T. Yang, G. Mao, and W. Zhang, "Connectivity of wireless information-theoretic secure networks," in *IEEE Global Communications Conference (GLOBECOM)*, 2014, pp. 317–323.

[49] K. Rybarczyk, "The coupling method for inhomogeneous random intersection graphs." *The Electronic Journal of Combinatorics*, vol. 24, no. 2, pp. P2–10, 2017.

[50] J. Zhao, "On secure communication in sensor networks under q-composite key predistribution with unreliable links," 2017. [Online]. Available: http://sites.google.com/site/workofzhao/tcomfull.pdf

[51] G. E. Martin, *Counting: The Art of Enumerative Combinatorics*. Springer Science & Business Media, 2013.