Designing secure networks with q-composite key predistribution under different link constraints

Jun Zhao
junzhao@alumni.cmu.edu

***Abstract*—In many applications of wireless sensor networks (WSNs), sensors are deployed in hostile environments where an adversary can eavesdrop communications. To secure communications in WSNs, the q-composite key predistribution scheme has been widely recognized as a suitable approach. In this paper, we investigate connectivity in secure WSNs operating under the q-composite scheme, in consideration of different link constraints: the unreliability of wireless links and the requirement that two sensors have to be within certain distance to have a link. We formally derive conditions on how to scale the model parameters so that the network is securely connected with high probability when the number of sensors becomes large. The results are given in the form of zero–one laws and provide useful guidelines for designing securely and reliably connected sensor networks.**

***Index Terms*—Security, key predistribution, wireless networks, link constraints, random graphs.**

I. Introduction

In wireless sensor networks, random key predistribution schemes have been extensively used to secure communications [1]–[5], [14]. Introduced in the seminal work of Eschenauer and Gligor [3], the idea of random key predistribution has the following two steps: (i) before deployment, sensors are loaded with cryptographic keys selected in some random manner, and (ii) after deployment, for sensors that are close enough for communication and also happen to share some keys, they use the shared keys to generate link keys for secure communication.

Based on the seminal work [3], Chan *et al.* [2] propose the q-composite key predistribution scheme which has widely been recognized as an appropriate solution to secure communications in sensor networks. The q-composite scheme works as follows. For a sensor network with n nodes, in the key predistribution phase, a large *key pool* consisting of P_n cryptographic keys is used to select *uniformly at random* K_n distinct keys for each sensor node. These K_n keys constitute the *key ring* of a sensor, and are installed in the sensor's memory. After deployment, two sensors establish secure communication over an existing link if and only if their key rings have at least q keys in common. Both P_n and K_n are functions of n for generality, with the natural condition $1 \leq q \leq K_n \leq P_n$.

The q-composite scheme is an extension of the Eschenauer–Gligor scheme [3]; in the Eschenauer–Gligor scheme, a secure link between two sensors require the sharing of just one key, instead of q keys. In other words, the q-composite scheme with $q = 1$ reduces to the Eschenauer–Gligor scheme. Chan *et al.* [2] show that the q-composite scheme with $q \geq 2$ outperforms the Eschenauer–Gligor scheme in terms of resilience to small-scale sensor capture attacks while trading off increased vulnerability in the presence of large-scale attacks. In both schemes, after sensors are deployed, common keys are found in the neighbor discovery phase whereby a random constant is enciphered in all keys of a node and broadcast along with the resulting ciphertext block in a given area limited by the transmission power/range; i.e., in a local neighborhood.

Over the last decade, the q-composite scheme has received much interest in the literature [1], [5], [6], [8], [14]. However, there is a lack of rigorous analysis on connectivity in secure sensor networks operating under the q-composite scheme with practical link constraints. This paper closes the above gap. Specifically, we investigate connectivity in secure WSNs operating under the q-composite scheme, in consideration of different link constraints: the unreliability of wireless links (represented by an on/off channel model), and the requirement that two sensors have to be within certain distance to have a link (represented by a disk model). The on/off channel model comprises independent channels which are either on or off, and captures the unreliability of wireless links due to the presence of physical barriers between sensors or because of harsh environmental conditions severely impairing communications [9], [11]. In the disk model [13], [15]–[17], [19], [20], each node's transmission area is a disk with a transmission radius r_n, with r_n being a function of n for generality, where n is the number of nodes. Two nodes have to be within r_n (their distance is at most r_n) for direct communication. As for the node distribution, the same as much previous work [13], [15]–[17], [20], [22], we consider that the n nodes are independently and uniformly deployed in a torus of unit area.

Our results are given in the form of sharp zero–one laws, meaning that the network is connected with high probability under certain parameter conditions and does not have connectivity with high probability if parameters are slightly changed, where an event happens "with high probability" if its probability converges to 1 asymptotically (i.e., as the number of sensors tends to infinity). The zero–one laws specify the critical scaling of the model parameters in terms of connectivity; in other words, the zero–one laws determine the exact threshold of connectivity and provide a precise guideline for ensuring connectivity. Obtaining such a precise guideline is particularly crucial in a secure WSN setting as explained below. To increase the chance of connectivity, it is often required to increase the number of keys kept in each sensor's memory. However, since sensors are expected to have limited memory, it is desirable for practical key distribution schemes to have low memory requirements [2], [3], [24], [26]. Thus, it is important to establish zero–one laws in order to carefully dimension the q-composite scheme for

Jun Zhao obtained his PhD from Carnegie Mellon University, Pittsburgh, PA, USA. He is now a postdoc jointly with Arizona State University, Tempe, AZ, USA, and Princeton University, Princeton, NJ, USA.

This research was supported in part by Arizona State University, by the U.S. National Science Foundation under Grant CNS-1422277, and by the U.S. Defense Threat Reduction Agency under Grant HDTRA1-13-1-0029. This research was also supported in part by CyLab and Department of Electrical & Computer Engineering at Carnegie Mellon University.

network connectivity.

We organize the rest of the paper as follows. Section II describes the system model. Afterwards, we present the analytical results in Section III and the proofs in Section IV. Section V surveys related work. Finally, we conclude the paper in Section VI.

II. System Model

Our approach to the analysis is to explore the induced random graph model of our studied WSN. As will be clear, the graph model is an intersection of three distinct types of random graphs. The intertwining of random graphs makes our analysis challenging.

A *uniform random q-intersection graph* induced by the q-composite scheme. We use $G_q(n, K_n, P_n)$ to denote the graph topology induced by the q-composite scheme. This graph is known as a *uniform random q-intersection graph* [1], [4] in the literature, and is constructed on a node set with size n as follows. Each node is independently assigned a set of K_n different keys, selected uniformly at random from a pool of P_n keys. An edge exists between two nodes if and only if they have at least q keys in common.

An *Erdős–Rényi graph* induced by unreliable links. With each link being active with probability p_n and inactive with probability $(1 - p_n)$, the link unreliability yields an *Erdős–Rényi graph* $G_{ER}(n, p_n)$ [27].

A *random geometric graph* induced by the disk model with the uniform node distribution. The disk model with the uniform node distribution induces a so-called *random geometric graph* $G_{RGG}(n, r_n)$ [20], which is defined as follows. Let n nodes be uniformly and independently deployed in a torus of unit area. An edge exists between two nodes if and only if their distance is no greater than r_n.

Graph intersection. We denote by $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$ the underlying graph of the n-node WSN operating under the q-composite scheme, the on/off channel model and transmission constraints. Clearly, the edge set of $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$ is the intersection of the edge sets of $G_q(n, K_n, P_n)$, $G_{ER}(n, p_n)$, and $G_{RGG}(n, r_n)$, and these graphs are all defined on the vertex set. Then $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$ can be seen as the intersection of $G_q(n, K_n, P_n)$, $G_{ER}(n, p_n)$, and $G_{RGG}(n, r_n)$; i.e.,

$$\begin{aligned}&\mathbb{G}_q(n, K_n, P_n, p_n, r_n)\\ &= G_q(n, K_n, P_n) \cap G_{ER}(n, p_n) \cap G_{RGG}(n, r_n). \quad (1)\end{aligned}$$

III. The Results

Before presenting the results, we introduce some notation as follows. The natural logarithm function is given by $\ln$. All limits are understood with $n \to \infty$. We use the standard asymptotic notation $o(\cdot), \omega(\cdot), O(\cdot), \Omega(\cdot), \Theta(\cdot), \sim$ (see [29, Footnote 1]). In particular, "$\sim$" represents asymptotic equivalence and is defined as follows: for two positive sequences f_n and g_n, the relation $f_n \sim g_n$ means $\lim_{n\to\infty}(f_n/g_n) = 1$. We let $\mathbb{P}[\mathcal{E}]$ denote the probability that an event $\mathcal{E}$ happens.

Theorem 1 below presents a sharp zero–one law for connectivity in a graph $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$. Connectivity means that any two nodes of the graph can find a path in between [9], [30]. In the secure sensor network modeled by $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$, connectivity enables any two sensors to have secure communication either directly or through the help of relaying nodes.

Theorem 1 *For a graph $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$, if there exists a positive constant c such that*

$$\frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q \cdot p_n \cdot \pi {r_n}^2 \sim c \cdot \frac{\ln n}{n}, \quad (2)$$

then it holds under $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$ that

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{G}_q(n, K_n, P_n, p_n, r_n)\\ \textit{is connected.}\end{array}\right] = \begin{cases} 0, & \textit{if } c < 1, \quad (3a)\\ 1, & \textit{if } c > 1. \quad (3b)\end{cases}$$

We explain that the left hand side of (2) is an asymptotic expression for the edge probability of $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$. To see this, for two sensors selecting K_n keys independently from the same pool of P_n keys, the probability that they share at least q keys equals $\sum_{u=q}^{K_n} \frac{\binom{K_n}{u}\binom{P_n - K_n}{K_n - u}}{\binom{P_n}{K_n}}$, which asymptotically becomes $\frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q$ [4], [14]. In addition, p_n is the probability of a link being active, $\pi {r_n}^2$ is the probability that two sensors are within the transmission range r_n on a torus of unit area.

We discuss the practicality of the conditions $P_n = \Omega(n)$ and $\frac{{K_n}^2}{P_n} = o(1)$ in Theorem 1. Both conditions are enforced here merely for technical reasons, but they hold trivially in realistic wireless sensor network applications because it is expected [2], [3], [26] that for security purposes, the key pool size P_n will be much larger than both the number n of participating sensors and the number K_n of keys on each sensor; for example, in a practical sensor network, P_n is tens of thousands, n is thousands or hundreds, and K_n is few dozens or small hundreds [31], [38], [47].

IV. Proof of Theorem 1

To establish Theorem 1, we need to prove the zero-law (3a) and the one-law (3b), respectively.

Clearly, if a graph G is connected, then G contains no isolated node [20]. To prove the zero-law (3a), we obtain the corresponding zero-law for the absence of isolated node. This is further done by the method of moments [33, Page 55] applied to the total number of isolated nodes. We provide more details in the full version [48].

To prove the one-law (3b), since connectivity is a monotone increasing graph property, we associate $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$ with a subgraph via graph coupling and show that the subgraph is connected with high probability. Given (1), we first present Lemma 1 below to have a graph coupling between $G_q(n, K_n, P_n)$ and an Erdős–Rényi graph. Following Rybarczyk's notation [34], we write

$$G_1 \preceq G_2 \quad (\text{resp.}, G_1 \preceq_{1-o(1)} G_2) \quad (4)$$

if there exists a graph coupling under which G_1 is a spanning subgraph of G_2 with probability 1 (resp., $1 - o(1)$).

Lemma 1 *If $K_n = \omega\big(\max\{\ln n, \frac{\sqrt{P_n}}{n}\}\big)$ and $K_n = o\big(\min\{\sqrt{P_n}, \frac{P_n}{n}\}\big)$, then*

$$G_{ER}(n, \tfrac{1}{q!} \cdot \tfrac{{K_n}^{2q}}{{P_n}^q} \cdot [1 - o(1)]) \preceq_{1-o(1)} G_q(n, K_n, P_n). \quad (5)$$

From Lemma 1, we further know that $\mathbb{G}_q(n, K_n, P_n, p_n, r_n)$ has a subgraph $G_{ER}(n, p_n \cdot \frac{1}{q!} \cdot \frac{{K_n}^{2q}}{{P_n}^q} \cdot [1 - o(1)]) \cap G_{RGG}(n, r_n)$, whose connectivity results have been recently derived by Penrose [49]. Based on the above, the proof of Theorem 1 is

straightforward.

We now detail the proof of Lemma 1. We introduce an auxiliary graph called a *binomial random q-intersection graph* $H_q(n, s_n, P_n)$ [1], [6], [37] defined later. We couple graph $G_q(n, K_n, P_n)$ with a binomial random q-intersection graph in Lemma 2 below, while we couple a binomial random q-intersection graph with an Erdős–Rényi graph in Lemma 3 below. Lemma 1 is proved using Lemmas 2 and 3.

A binomial random q-intersection graph $H_q(n, s_n, P_n)$ is constructed on n nodes by the following process. There exists a key pool of size P_n. Each key in the pool is added to each node *independently* with probability s_n. Clearly, the difference between a binomial random q-intersection graph $H_q(n, s_n, P_n)$ and a uniform random q-intersection graph $G_q(n, K_n, P_n)$ is that in $H_q(n, s_n, P_n)$, the number of keys assigned to each node obeys a binomial distribution with P_n as the number of trials, and with s_n as the success probability in each trial, while in $G_q(n, K_n, P_n)$, such number equals K_n with probability 1.

Lemma 2 *If $K_n = \omega(\ln n)$ and $K_n = o\big(\sqrt{P_n}\big)$, with s_n set by*

$$s_n = \tfrac{K_n}{P_n}\Big(1 - \sqrt{\tfrac{3 \ln n}{K_n}}\Big), \tag{6}$$

then it holds that

$$H_q(n, s_n, P_n) \preceq_{1-o(1)} G_q(n, K_n, P_n). \tag{7}$$

Lemma 3 *If $s_n P_n = \omega(\ln n)$, $n s_n = o(1)$, $P_n {s_n}^2 = o(1)$ and $n^2 {s_n}^2 P_n = \omega(1)$, then there exits some p_n satisfying*

$$p_n = \tfrac{(P_n {s_n}^2)^q}{q!} \cdot [1 - o(1)] \tag{8}$$

such that Erdős–Rényi graph $G_{ER}(n, p_n)$ obeys

$$G_{ER}(n, p_n) \preceq_{1-o(1)} H_q(n, s_n, P_n). \tag{9}$$

Lemma 2 is based on [1, Lemma 4] and further explained in the full version [48]. We present the proof of Lemma 3 below.

Proof of Lemma 3:

In binomial random q-intersection graph $H_q(n, P_n, s_n)$, let $\mathcal{V}_i$ be the set of sensors assigned with key κ_i from the key pool ($i = 1, 2, \ldots, P_n$). V_i denoting the cardinality of $\mathcal{V}_i$ (i.e., $V_i := |\mathcal{V}_i|$) obeys a binomial distribution $\text{Bin}(n, s_n)$, with n as the number of trials, and s_n as the success probability in each trial. Clearly, we can generate the random set $\mathcal{V}_i$ in the following equivalent manner: First draw the cardinality V_i from the distribution $\text{Bin}(n, s_n)$, and then choose V_i distinct nodes uniformly at random from the set $\mathcal{V}$ of all nodes.

Given $\mathcal{V}_i$ introduced above, we define below random graph $H(V_i)$ on node set $\mathcal{V}$: $H(V_i)$ is constructed by establishing edges between any and only pair of nodes in $\mathcal{V}_i$; i.e., $H(V_i)$ has a clique on $\mathcal{V}_i$ and no edges between nodes outside of this clique. If a realization of the random variable V_i satisfies $V_i < 2$, then the corresponding $H(V_i)$ will be an empty graph.

We now explain the connection between $H(V_i)$ and the binomial random q-intersection graph $H_q(n, P_n, s_n)$. We let an operator $\mathcal{O}_q$ take a multigraph [40] with possibly multiple edges between two nodes as its argument. The operator returns a simple graph with an undirected edge between two nodes i and j, if and only if the input multigraph has at least q edges between these nodes. Recall that two nodes in $H_q(n, P_n, s_n)$ need to share at least q keys to have an edge in between. Then, with $H(V_1), \ldots, H(V_{P_n})$ generated independently, it is straightforward to see

$$\mathcal{O}_q\left(\bigcup_{i=1}^{P_n} H(V_i)\right) =_{\text{st}} H_q(n, P_n, s_n), \tag{10}$$

with $=_{\text{st}}$ denoting statistical equivalence.

We now introduce auxiliary random graphs $L(n, X)$ and $L_q(n, X)$, both defined on the n-size node set $\mathcal{V}$, where X is a non-negative random integer variable. Note that X can also be a fixed value with probability 1. We sample X node pairs *with repetition* from all pairs of $\mathcal{V}$ (a pair is unordered). In graph $L(n, X)$ (resp., $L_q(n, X)$), two nodes have an edge in between if and only if the node pair is sampled at least once (resp., q times).

With $H(V_i)$ and $L(n, X)$ given above, we show a coupling below under which random graph $L(n, \lfloor V_i/2 \rfloor)$ is a subgraph of random graph $H(V_i)$; i.e.,

$$L(n, \lfloor V_i/2 \rfloor) \preceq H(V_i). \tag{11}$$

By definition, graph $L(n, \lfloor V_i/2 \rfloor)$ has at most $\lfloor V_i/2 \rfloor$ edges and thus contains non-isolated nodes with a number (denoted by ℓ) at most $2 \cdot \lfloor V_i/2 \rfloor \le V_i$. Given an instance $\mathcal{L}$ of random graph $L(n, \lfloor V_i/2 \rfloor)$, we construct set $\mathcal{V}_i$ as the union of the ℓ number non-isolated nodes in $\mathcal{L}$ and the rest $(V_i - \ell)$ nodes selected uniformly at random from the rest $(n - \ell)$ isolated nodes in $\mathcal{L}$. Since graph $H(V_i)$ contains a clique of $\mathcal{V}_i$, it is clear that the induced instance of $H(V_i)$ is a supergraph of the instance $\mathcal{L}$ of graph $L(n, \lfloor V_i/2 \rfloor)$. Then (11) is proved.

Now based on $L(n, \lfloor V_i/2 \rfloor)$, we construct a graph defined on node set $\mathcal{V}$. We add an edge between two nodes in this graph if and only if there exist at least q different number of i such that the two nodes have an edge in each of these $L(n, \lfloor V_i/2 \rfloor)$. By the independence of V_i ($i = 1, 2, \ldots, P_n$) and the definition of $L_q(n, X)$ above, it is clear that such induced graph is statistically equivalent to $L_q\big(n, \sum_{i=1}^{P_n} \lfloor V_i/2 \rfloor\big)$. Namely, we have

$$\mathcal{O}_q\left(\bigcup_{i=1}^{P_n} L(n, \lfloor V_i/2 \rfloor)\right) =_{\text{st}} L_q\big(n, \sum_{i=1}^{P_n} \lfloor V_i/2 \rfloor\big) \tag{12}$$

In view of (10), (11), and (12), we see

$$L_q(n, Y) \preceq H_q(n, P_n, s_n), \tag{13}$$

where Y is defined via

$$Y := \sum_{i=1}^{P_n} W_i, \tag{14}$$

with

$$W_i := \lfloor V_i/2 \rfloor = \tfrac{1}{2}(V_i - \mathrm{I}_{[V_i \text{ is odd}]}). \tag{15}$$

We will provide a lower bound on Y with high probability. By Chebyshev's inequality, it follows that for any $\phi > 0$,

$$\mathbb{P}\big[|Y - \mathbb{E}[Y]| \ge \phi \sqrt{\text{Var}[Y]}\big] \le \phi^{-2}.$$

We compute $\mathbb{E}[Y]$ and $\text{Var}[Y]$ and have the following results (16) and (17) (see the full version [48]). We have

$$\text{Var}[Y] \le 2\mathbb{E}[Y], \tag{16}$$

and

$$\mathbb{E}[Y] = \tfrac{1}{2} n(n-1) P_n {s_n}^2 \cdot [1 \pm o(1)] = \omega(1). \tag{17}$$

where the last step in (17) uses the condition $n^2 {s_n}^2 P_n = \omega(1)$.

Now based on (16) and (17), we select

$$\phi = \frac{\{\mathbb{E}[Y]\}^{\frac{5}{6}}}{2\sqrt{\text{Var}[Y]}}, \tag{18}$$

which with (16) and (17) results in $\phi = \omega(1)$ and hence

$$\mathbb{P}\big[Y < \mathbb{E}[Y] - \phi\sqrt{\text{Var}[Y]}\big] = o(1). \tag{19}$$

Let Z be a Poisson random variable with mean

$$\lambda := \mathbb{E}[Y] - \{\mathbb{E}[Y]\}^{\frac{5}{6}}. \tag{20}$$

With ψ defined by

$$\psi := \tfrac{1}{2}\{\mathbb{E}[Y]\}^{\frac{1}{3}}, \tag{21}$$

from (17) (20) and (21), we conclude that $\psi = \omega(1)$ and $\psi = o(\sqrt{\lambda})$. By [40, Lemma 1.2], it holds that

$$\mathbb{P}\big[Z \geq \lambda + \psi\sqrt{\lambda}\big] \leq e^{\psi\sqrt{\lambda} - (\lambda+\psi\sqrt{\lambda})\ln(1+\frac{\psi}{\sqrt{\lambda}})}. \tag{22}$$

From $\psi = o(\sqrt{\lambda})$, then for all n sufficiently large, we have $\ln\big(1+\frac{\psi}{\sqrt{\lambda}}\big) \geq \frac{\psi}{\sqrt{\lambda}} - \frac{\psi^2}{2\lambda}$ (derived from a Taylor expansion), which is used in (22) to yield

$$\begin{aligned}\mathbb{P}\big[Z \geq \lambda + \psi\sqrt{\lambda}\big] &\leq e^{\psi\sqrt{\lambda} - (\lambda+\psi\sqrt{\lambda})\left(\frac{\psi}{\sqrt{\lambda}} - \frac{\psi^2}{2\lambda}\right)} \\ &= e^{\frac{\psi^2}{2}\left(\frac{\psi}{\sqrt{\lambda}} - 1\right)}.\end{aligned} \tag{23}$$

Applying $\psi = \omega(1)$ and $\psi = o(\sqrt{\lambda})$ to (23), we obtain

$$\mathbb{P}\big[Z \geq \lambda + \psi\sqrt{\lambda}\big] = o(1). \tag{24}$$

From (18) (20) and (21), we establish

$$\begin{aligned}\lambda + \psi\sqrt{\lambda} &\leq \mathbb{E}[Y] - \{\mathbb{E}[Y]\}^{\frac{5}{6}} + \tfrac{1}{2}\{\mathbb{E}[Y]\}^{\frac{1}{3}} \cdot \sqrt{\mathbb{E}[Y]} \\ &= \mathbb{E}[Y] - \phi\sqrt{\text{Var}[Y]}.\end{aligned} \tag{25}$$

Given (19) (24) and (25), we use the union bound to obtain

$$\begin{aligned}&\mathbb{P}[Y \geq Z] \\ &\geq \mathbb{P}\Big[\big(Y \geq \mathbb{E}[Y] - \phi\sqrt{\text{Var}[Y]}\big) \cap (\lambda + \psi\sqrt{\lambda} \geq Z)\Big] \\ &\geq 1 - \mathbb{P}\big[Y < \mathbb{E}[Y] - \phi\sqrt{\text{Var}[Y]}\big] - \mathbb{P}\big[\lambda + \psi\sqrt{\lambda} < Z\big] \\ &\to 1, \text{ as } n \to \infty.\end{aligned} \tag{26}$$

Given (26), by the definition of graph $L_q(n, X)$, it is easy to construct a coupling such that $L_q(n, Z)$ is a subgraph of $L_q(n, Y)$ with probability $1 - o(1)$; namely,

$$L_q(n, Z) \preceq_{1-o(1)} L_q(n, Y). \tag{27}$$

From [41, Proof of Claim 1], for a Poisson random variable Z with mean λ, in sampling Z node pairs *with repetition* from all pairs of an n-size node set, the number of draws of different pairs are independent Poisson random variables with mean

$$\mu := \lambda \Big/ \binom{n}{2}. \tag{28}$$

Thus, $L_q(n, Z)$ with Z following a Poisson distribution with mean λ is an Erdős–Rényi graph [27] in which each edge independently appears with a probability that a Poisson random variable with mean μ is at least q, i.e., a probability of

$$\varrho_n := \sum_{x=q}^{\infty} \frac{\mu^x e^{-\mu}}{x!}. \tag{29}$$

In view that $L_q(n, Z)$ is equivalent to $G_{ER}(n, \varrho_n)$, then from (13) and (27), it follows that

$$G_{ER}(n, \varrho_n) \preceq_{1-o(1)} H_q(n, P_n, s_n), \tag{30}$$

which is exactly (9) in the statement of Lemma 3. Therefore, the proof of Lemma 3 is completed once we show that ϱ_n defined in (29) satisfies (8) (i.e., $\varrho_n = p_b \cdot [1 \pm o(1)]$).

From [43, Proposition 1], ϱ_n in (29) can be bounded by

$$\frac{\mu^q e^{-\mu}}{q!} < \varrho_n < \frac{\mu^q e^{-\mu}}{q!} \cdot \left(1 - \frac{\mu}{q+1}\right)^{-1}. \tag{31}$$

From (17) (20) (28), and conditions $n^2 {s_n}^2 P_n = \omega(1)$ and $P_n {s_n}^2 = o(1)$, it follows that

$$\begin{aligned}\mu := \lambda \Big/ \binom{n}{2} &= P_n {s_n}^2 \Big[1 - O\Big(\big(n^2 {s_n}^2 P_n\big)^{-\frac{1}{6}}\Big)\Big] \\ &= P_n {s_n}^2 \cdot [1 - o(1)] = o(1).\end{aligned} \tag{32}$$

Using (32) in (31), we obtain

$$\varrho_n \sim \frac{\mu^q e^{-\mu}}{q!} \sim \frac{(P_n {s_n}^2)^q}{q!}. \tag{33}$$

From [34, Fact 3], for Erdős–Rényi graphs $G_{ER}(n, p_n')$ and $G_{ER}(n, p_n'')$, if $p_n' \leq p_n''$, then $G_{ER}(n, p_n') \preceq G_{ER}(n, p_n'')$. Therefore, by (30) (33) and [44, Fact 3] on the transitivity of graph coupling, we can set $p_n = \frac{(P_n {s_n}^2)^q}{q!} \cdot [1 - o(1)]$ to have $G_{ER}(n, p_n) \preceq_{1-o(1)} H_q(n, P_n, s_n)$. ■

V. Related Work

Recall that the q-composite key predistribution scheme with $q = 1$ reduces to the Eschenauer–Gligor scheme [3]. (k)-Connectivity and other related properties of sensor networks with the Eschenauer–Gligor scheme under different communication models are analyzed in the literature [7], [12], [15], [18], [21], [23], [39], [45], [46].

The uniform random q-intersection graph has been extensively studied in prior work in terms of various properties, including (k)-connectivity [4], [8], [10], [25], [28], (k)-robustness [36], clustering [37], giant component [1], and perfect matching [8], and resilience [32], [42].

Chan and Fekri [35] approximate a uniform random q-intersection graph by an Erdős–Rényi graph and thus approximate the sensor network with the q-composite scheme under the disk model as the intersection of an Erdős–Rényi graph and a random geometric graph, in order to obtain connectivity results of the network. However, there is a lack of rigorous argument for this approximation. A formal argument is needed because an Erdős–Rényi graph and a uniform random q-intersection graph used to represent the q-composite scheme are quite different; e.g., edges are all independent in the former but are not in the latter [1], [14], [37]. By graph coupling, we rigorously bridge these two graphs.

VI. Conclusion

In this paper, we present a sharp zero–one law for connectivity in a secure wireless sensor network operating with the q-composite key predistribution scheme under unreliable wireless links and the well-known disk model that two sensors have to be within certain distance to have a link. The network is modeled by composing a uniform q-intersection graph with an Erdős-Rényi graph and then with a random geometric graph, where the uniform q-intersection graph characterizes the q-composite key predistribution scheme, the Erdős-Rényi graph captures the on/off channel model, and the random geometric graph represents the disk model. The zero–one law provides useful guidelines for designing securely and reliably connected sensor networks.

REFERENCES

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

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

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

[4] 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.

[5] O. Yağan, *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*. PhD thesis, Dept. of ECE, College Park (MD), June 2011. Available online at http://hdl.handle.net/1903/11910

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

[7] J. Zhao, O. Yağan, and V. Gligor, "On connectivity and robustness in random intersection graphs," *IEEE Transactions on Automatic Control*, 2017.

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

[9] Y. Liu, Y. Cui, and X. Wang, "Connectivity and transmission delay in large-scale cognitive radio ad hoc networks with unreliable secondary links," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 7016–7029, 2015.

[10] J. Zhao, O. Yağan, and V. Gligor, "On k-connectivity and minimum vertex degree in random s-intersection graphs," in *ACM-SIAM Meeting on Analytic Algorithmics and Combinatorics (ANALCO)*, 2015.

[11] I.-H. Hou, "Packet scheduling for real-time surveillance in multihop wireless sensor networks with lossy channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1071–1079, 2015.

[12] J. Zhao, "Sharp transitions in random key graphs," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1182–1188, 2015.

[13] B. Krishnan, A. Ganesh, and D. Manjunath, "On connectivity thresholds in superposition of random key graphs on random geometric graphs," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2389–2393, 2013.

[14] J. Zhao, "Topological properties of wireless sensor networks under the q-composite key predistribution scheme with unreliable links," *IEEE/ACM Transactions on Networking*, 2017.

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

[16] J. Zhao, "The absence of isolated node in geometric random graphs," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 881–886, 2015.

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

[18] J. Zhao, "Analyzing connectivity of heterogeneous secure sensor networks," *IEEE Transactions on Control of Network Systems*, 2016.

[19] X. Liu, K. Zheng, J. Zhao, X.-Y. Liu, X. Wang, and X. Di, "Information-centric networks with correlated mobility," *IEEE Transactions on Vehicular Technology*, 2016.

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

[21] J. Zhao, "A comprehensive guideline for choosing parameters in the eschenauer–gligor key predistribution," in *Allerton Conference on Communication, Control, and Computing (Allerton)*, 2016.

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

[23] J. Zhao, O. Yağan, and V. Gligor, "Connectivity in secure wireless sensor networks under transmission constraints," in *Allerton Conference on Communication, Control, and Computing*, 2014.

[24] O. Yağan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, pp. 2983–2999, May 2012.

[25] J. Zhao, "Parameter control in predistribution schemes of cryptographic keys," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 863–867, 2015.

[26] 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*, pp. 53–58, 2004.

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

[28] J. Zhao, "Modeling interest-based social networks: Superimposing Erdos–Renyi graphs over random intersection graphs," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017.

[29] X. Liu, K. Zheng, J. Zhao, X. Y. Liu, X. Wang, and X. Di, "Information-centric networks with correlated mobility," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2016.

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

[31] 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.

[32] J. Zhao, "On the resilience to node capture attacks of secure wireless sensor networks," in *Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 887–893, 2015.

[33] S. Janson, T. Łuczak, and A. Ruciński, *Random graphs*. Wiley-Interscience Series on Discrete Mathematics and Optimization, 2000.

[34] K. Rybarczyk, "Sharp threshold functions for the random intersection graph via a coupling method," *The Electronic Journal of Combinatorics*, vol. 18, pp. 36–47, 2011.

[35] K. Chan and F. Fekri, "A resiliency-connectivity metric in wireless sensor networks with key predistribution schemes and node compromise attacks," *Physical Communication*, vol. 1, no. 2, pp. 134–145, 2008.

[36] J. Zhao, "Robustness of complex networks with applications to random graphs," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 1062–1065, 2015.

[37] M. Bloznelis, J. Jaworski, and V. Kurauskas, "Assortativity and clustering of sparse random intersection graphs," *The Electronic Journal of Probability*, vol. 18, no. 38, pp. 1–24, 2013.

[38] J. Zhao, O. Yağan, and V. Gligor, "k-Connectivity in random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, pp. 3810–3836, July 2015.

[39] J. Zhao, "Critical behavior in heterogeneous random key graphs," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 868–872, 2015.

[40] M. Penrose, *Random Geometric Graphs*. Oxford University Press, July 2003.

[41] J. A. Fill, E. R. Scheinerman, and K. B. Singer-Cohen, "Random intersection graphs when $m = \omega(n)$: An equivalence theorem relating the evolution of the $G(n, m, p)$ and $G(n, p)$ models," *Random Structures & Algorithms*, vol. 16, pp. 156–176, Mar. 2000.

[42] J. Zhao, "On resilience and connectivity of secure wireless sensor networks under node capture attacks," *IEEE Transactions on Information Forensics and Security*, 2016.

[43] B. Klar, "Bounds on tail probabilities of discrete distributions," *Probability in the Engineering and Informational Sciences*, vol. 14, pp. 161–171, 4 2000.

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

[45] 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*, pp. 53–58, 2004.

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

[47] 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.

[48] J. Zhao, "Designing secure networks with q-composite key predistribution under different link constraints," 2017. Full version of this paper, available online at https://sites.google.com/site/workofzhao/ICASSP17-design.pdf

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