On Topological Properties of Wireless Sensor Networks under the q-Composite Key Predistribution Scheme with On/Off Channels

Jun Zhao, Osman Yağan and Virgil Gligor

CyLab and Dept. of ECE
Carnegie Mellon University
{junzhao, oyagan, virgil}@andrew.cmu.edu

***Abstract*—To be considered for an IEEE Jack Keil Wolf ISIT Student Paper Award. The seminal q-composite key predistribution scheme [3] (IEEE S&P 2003) is used prevalently for secure communications in large-scale wireless sensor networks (WSNs). Yağan [10] (IEEE IT 2012) and we [13] (IEEE ISIT 2013) explore topological properties of WSNs employing the q-composite scheme in the case of $q = 1$ with unreliable communication links modeled as independent on/off channels. However, it is challenging to derive results for general q under such on/off channel model. In this paper, we resolve such challenge and investigate topological properties related to node degree in WSNs operating under the q-composite scheme and the on/off channel model. Our results apply to general q, yet there has not been any work in the literature reporting the corresponding results even for $q = 1$, which are stronger than those about node degree in [10], [13]. Specifically, we show that the number of nodes with any degree asymptotically converges to a Poisson distribution, present the asymptotic probability distribution for the minimum node degree of the network, and establish the asymptotically exact probability for the property that the minimum node degree is at least an arbitrary value. Numerical experiments confirm the validity our analytical findings.**

***Index Terms*—key predistribution, minimum degree, random graphs, security, topological properties, wireless sensor networks.**

I. Introduction

Key predistribution scheme has been recognized as a typical solution to secure communication in wireless sensor networks and studied extensively in the literature over the last decade [2], [3], [6], [9]–[14]. The idea is to randomly assign cryptographic keys to sensors before network deployment.

The q-composite key predistribution scheme proposed by Chan *et al.* [3] as an extension of the Eschenauer-Gligor scheme [6] (the q-composite scheme in the case of $q = 1$) has received much interest [2], [9]–[14] since its introduction. The q-composite scheme when $q \geq 2$ outperforms the Eschenauer-Gligor scheme in terms of the strength against small-scale network capture attacks while trading off increased vulnerability in the face of large-scale attacks.

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 of P_n keys, where K_n and P_n are both functions of n, with $K_n \leq P_n$. Then two sensors establish a link in between after deployment if and only if they share at least q keys *and* the physical link constraint between them is satisfied. Examples of physical link constraints include the reliability of the transmission channel and the distance between two sensors close enough for communication.

In this paper, we investigate topological properties related to node degree in WSNs employing the q-composite key predistribution scheme with general q under the *on*/*off* channel model as the physical link constraint compromising independent channels which are either *on* or *off*. The degree of a node v is the number of nodes having links with v; and the minimum (node) degree of a network is the least among the degrees of all nodes. Specifically, we demonstrate that the number of nodes with any degree asymptotically converges to a Poisson distribution, establish the asymptotic probability distribution for the minimum degree of the network, and derive the asymptotically exact probability for the property that the minimum degree is no less than an arbitrary value. Yağan [10] and we [12], [13] consider the WSNs with $q = 1$ and show results for several topological properties, yet results about node degree in both work are even weaker than our analytical findings when the general q is set as 1.

Our approach to the analysis is to explore the induced random graph models of the WSNs. As will be clear in Section II, the graph modeling a WSN under q-composite scheme and the on/off channel model is an intersection of two graphs belonging to different kinds, which renders the analysis challenging due to the intertwining of the two distinct types of random graphs [10].

We organize the rest of the paper as follows. Section II describes the system model in detail. Afterwards, we elaborate and discuss the results in Section III. Subsequently, we present numerical experiments in Section IV to confirm our analytical results, whereas Section V is devoted to relevant results in the literature. Next, we conclude the paper in Section VI and identify future research directions. At the end, the Appendix offers the proof of a lemma.

II. System Model

We elaborate the graph modeling of a WSN with n sensors, which employs the q-composite key predistribution scheme and works under the on/off channel model. We consider a node set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ to represent the n sensors (a sensor is also referred to as a node). For each node $v_i \in \mathcal{V}$, the set of its K_n different keys is denoted by S_i, which is uniformly distributed among all K_n-size subsets of a key pool of P_n keys, and is referred to as the key ring of node v_i.

The q-composite key predistribution scheme is modeled by a graph denoted by $G_q(n, K_n, P_n)$, which is defined on the vertex set $\mathcal{V}$ such that any two different nodes v_i and v_j sharing

at least q keys (such event is denoted by Γ_{ij}) have an edge in between. Clearly, Γ_{ij} equals event $\big[|S_i \cap S_j| \geq q\big]$, where $|A|$ with A as a set means the cardinality of A.

Under the on/off channel model, each node-to-node channel independently has probability p_n of being *on* and probability $(1-p_n)$ of being *off*, where p_n is a function of n. Denoting by C_{ij} the event that the channel between distinct nodes v_i and v_j is *on*, we have $\mathbb{P}\left[C_{ij}\right] = p_n$, where $\mathbb{P}[\mathcal{E}]$ denotes the probability that event $\mathcal{E}$ happens, throughout the paper. The on/off channel model is represented by an Erdős-Rényi graph $G(n, p_n)$ [4] defined on the node set $\mathcal{V}$ such that v_i and v_j have an edge in between if event C_{ij} happens.

Finally, we denote by $\mathbb{G}_q(n, K_n, P_n, p_n)$ the underlying graph of the n-node WSN operating under the q-composite key predistribution scheme and the on/off channel model. We often write $\mathbb{G}_q$ rather than $\mathbb{G}_q(n, K_n, P_n, p_n)$ for notation brevity. Graph $\mathbb{G}_q$ is defined on the node set $\mathcal{V}$ such that there exists an edge between nodes v_i and v_j if events Γ_{ij} and C_{ij} happen at the same time. We set event $E_{ij} := \Gamma_{ij} \cap C_{ij}$. It is clear that $\mathbb{G}_q$ can be seen as the intersection of $G_q(n, K_n, P_n)$ and $G(n, p_n)$, meaning

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

We define $p_{s,q}$ as the probability that two different nodes share at least q keys and $p_{e,q}$ as the probability that two distinct nodes have a link in between. $p_{s,q}$ and $p_{e,q}$ both rely on K_n, P_n and q, while $p_{e,q}$ also depends on p_n. By definition, $p_{s,q}$ is determined through

$$p_{s,q} = \mathbb{P}[\Gamma_{ij}] = \sum_{u=\max\{q,\, 2K_n - P_n\}}^{K_n} \mathbb{P}[|S_i \cap S_j| = u], \quad (1)$$

where

$$\mathbb{P}[|S_i \cap S_j| = u] = \begin{cases} \frac{\binom{K_n}{u}\binom{P_n - K_n}{K_n - u}}{\binom{P_n}{K_n}}, & \text{for } \max\{0, 2K_n - P_n\} \leq u \leq K_n, \\ 0, & \text{otherwise,} \end{cases} \quad (2)$$

since S_i and S_j are independently and uniformly selected from all K_n-size subsets of a key pool with size P_n. Then by the independence of C_{ij} and Γ_{ij}, we obtain

$$p_{e,q} = \mathbb{P}[E_{ij}] = \mathbb{P}[C_{ij}] \cdot \mathbb{P}[\Gamma_{ij}] = p_n \cdot p_{s,q}. \quad (3)$$

III. The Results and Discussion

We present and discuss the results in this section. Throughout the paper, q is a positive integer and does not scale with n; $\mathbb{N}_0$ stands for the set of all positive integers; $\mathbb{R}$ is the set of all real numbers; e is the base of the natural logarithm function, $\ln$; and the floor function $\lfloor x \rfloor$ is the largest integer not greater than x. We consider $e^{\infty} = \infty$ and $e^{-\infty} = 0$. The term "for all n sufficiently large" means "for any $n \geq N$, where $N \in \mathbb{N}_0$ is selected appropriately". We use the standard asymptotic notation $o(\cdot), \omega(\cdot), O(\cdot), \sim$. In particular, for two positive functions $f(n)$ and $g(n)$, $f(n) \sim g(n)$ signifies $\lim_{n\to\infty}[f(n)/g(n)] = 1$; namely, $f(n)$ and $g(n)$ are asymptotically equivalent.

A. The Results of Graph $\mathbb{G}_q$

Denoting by δ the minimum node degree of graph $\mathbb{G}_q$, we detail the results of $\mathbb{G}_q$ below.

Theorem 1. *Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0, P : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to [0,1]$ with $K_n = \omega(1)$ and ${K_n}^2/P_n = o(1)$. If*

$$p_{e,q} = \frac{\ln n \pm O(\ln \ln n)}{n}, \quad (4)$$

(i.e., $\frac{np_{e,q} - \ln n}{\ln \ln n}$ is bounded for all n), the following properties (a) and (b) for graph $\mathbb{G}_q$ hold.

(a) *The number of nodes in $\mathbb{G}_q$ with any degree converges to a Poisson distribution as $n \to \infty$.*

(b) *Defining ℓ and β_n by*

$$\ell := \left\lfloor \frac{np_{e,q} - \ln n + (\ln \ln n)/2}{\ln \ln n} \right\rfloor + 1, \quad (5)$$

and

$$\beta_n := np_{e,q} - \ln n - (\ell - 1) \ln \ln n, \quad (6)$$

and recalling δ as the minimum node degree of $\mathbb{G}_q$, we obtain

- $(\delta \neq \ell) \cap (\delta \neq \ell - 1)$ *with a probability going to 0 as $n \to \infty$;*
- *if $\lim_{n\to\infty} \beta_n = \beta^* \in (-\infty, \infty)$, then as $n \to \infty$,*

$$\begin{cases} \delta = \ell \text{ with a probability converging to } e^{-\frac{e^{-\beta^*}}{(k-1)!}}, \\ \delta = \ell - 1 \text{ with a probability tending to } \left(1 - e^{-\frac{e^{-\beta^*}}{(k-1)!}}\right); \end{cases}$$

- *if $\lim_{n\to\infty} \beta_n = \infty$, then as $n \to \infty$,*

$$\begin{cases} \delta = \ell \text{ with a probability approaching to } 1, \\ \delta \neq \ell \text{ with a probability going to } 0; \end{cases} \quad \text{and}$$

- *if $\lim_{n\to\infty} \beta_n = -\infty$, then as $n \to \infty$,*

$$\begin{cases} \delta = \ell - 1 \text{ with a probability tending to } 1, \\ \delta \neq \ell - 1 \text{ with a probability converging to } 0. \end{cases}$$

Remark 1. *Theorem 1 for graph $\mathbb{G}_q$ establishes that the number of nodes with any degree follows an asymptotic Poisson distribution and presents the asymptotic probability distribution for the minimum degree of the network, where an asymptotic Poisson distribution of a variable ν means that there exists another variable μ such that $\mathbb{P}[\nu = i] \sim \mathbb{P}[\mu = i]$ for any non-negative integer i.*

Remark 2. *Equations (5) and (6) are determined by finding ℓ and β_n with $-\frac{1}{2}\ln\ln n \leq \beta_n < \frac{1}{2}\ln\ln n$ such that $p_{e,q} = \frac{\ln n + (\ell-1)\ln\ln n + \beta_n}{n}$.*

The detailed proof of Theorem 1 is given in our technical report [14] and is omitted here owing to the space limitation. A corollary of Theorem 1 is as follows.

Corollary 1. *Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0, P : \mathbb{N}_0 \to \mathbb{N}_0$ and $p : \mathbb{N}_0 \to [0,1]$ with $K_n = \omega(1)$ and ${K_n}^2/P_n = o(1)$. For a positive integer k, with probability $p_{e,q}$ satisfying*

$$p_{e,q} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \quad (7)$$

with $\lim_{n\to\infty}\alpha_n = \alpha^* \in [-\infty, \infty]$*, then as* $n \to \infty$*,*

$$\mathbb{P}[\delta \geq k] \to e^{-\frac{e^{-\alpha^*}}{(k-1)!}} = \begin{cases} 1, \text{ if } \alpha^* = \infty, \\ 0, \text{ if } \alpha^* = -\infty. \end{cases} \tag{8}$$

Remark 3. *Corollary 1 for graph* $\mathbb{G}_q$ *presents the asymptotically exact probability and a zero-one law [11] for the event that* $\mathbb{G}_q$ *has a minimum node degree no less than* k*.*

Remark 4. *Setting* p_n *as* 1 *in Theorem 1 and Corollary 1, we obtain corresponding results for topological properties in graph* $G_q(n, K_n, P_n)$*.*

Remark 5. *In the case of* $q = 1$*, we have proved the results of Theorem 1 and Corollary 1 without the condition* ${K_n}^2/P_n = o(1)$*, yet under a weaker condition:* $P_n \geq 3K_n$ *for all* n *sufficiently large. The details can be found in our technical report [14] and is again omitted due to the space limitation.*

We now explain the steps of proving Corollary 1 through Theorem 1.

B. Establishing Corollary 1 Given Theorem 1

Given (7) (a condition in Corollary 1), we determine ℓ and β_n through (5) and (6) in Theorem 1. Then

$$\begin{aligned} \ell &= \left\lfloor \frac{(k-1)\ln\ln n + \alpha_n + (\ln\ln n)/2}{\ln\ln n} \right\rfloor + 1 \\ &= k + \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor, \end{aligned} \tag{9}$$

and

$$\begin{aligned} \beta_n &= (k-1)\ln\ln n + \alpha_n - \left(k + \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor - 1\right)\ln\ln n, \\ &= \alpha_n - \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor \ln\ln n. \end{aligned} \tag{10}$$

Given condition $\lim_{n\to\infty}\alpha_n = \alpha^* \in [-\infty, \infty]$ in Corollary 1, we consider the following three cases: ① $-\frac{1}{2}\ln\ln n \leq \alpha_n < \frac{1}{2}\ln\ln n$, ② $\alpha_n \geq \frac{1}{2}\ln\ln n$ and ③ $\alpha_n < -\frac{1}{2}\ln\ln n$.

Case ①: $-\frac{1}{2}\ln\ln n \leq \alpha_n < \frac{1}{2}\ln\ln n$. Then from (9) and (10), we obtain $\ell = k$ and $\beta_n = \alpha_n$. It further holds that $\lim_{n\to\infty}\beta_n = \lim_{n\to\infty}\alpha_n = \alpha^* \in [-\infty, \infty]$. Therefore, by Theorem 1,

$$\mathbb{P}[\delta \geq k] \to \begin{cases} 1, \text{ if } \alpha^* = \infty, \\ 0, \text{ if } \alpha^* = -\infty, \\ e^{-\frac{e^{-\alpha^*}}{(k-1)!}}, \text{ if } \alpha^* \in (-\infty, \infty). \end{cases}$$

Then with $e^{\infty} = \infty$ and $e^{-\infty} = 0$, (8) follows in case ①.

Case ②: $\alpha_n \geq \frac{1}{2}\ln\ln n$. Then from (9) and (10), it holds that $\ell \geq k+1$. Hence, $\mathbb{P}[\delta \geq k] \to 1$ by Theorem 1, leading to (8) in case ②.

Case ③: $\alpha_n < -\frac{1}{2}\ln\ln n$. Then from (9) and (10), it holds that $\ell \leq k-1$. Consequently, $\mathbb{P}[\delta \geq k] \to 0$ by Theorem 1, resulting in (8) in case ②.

Summarizing cases ① ② and ③ above, Corollary 1 holds by Theorem 1.

C. Analogs of Theorem 1 and Corollary 1 with an Approximation of $p_{e,q}$

Analogous results of Theorem 1 and Corollary 1 can be given with $p_{e,q}$ in $\mathbb{G}$ substituted by a quantity expressed by K_n, P_n and q; i.e., with $p_{s,q}$ replaced by $\frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q$ given Lemma 1 below, and hence with $p_{e,q}$ replaced by $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q$ due to $p_{e,q} = p_n \cdot p_{s,q}$ from (3) (Lemma 1 applies owing to $\frac{{K_n}^2}{P_n} = o(1)$ which holds in both Theorem 1 and Corollary 1). Thus, with (4) (resp., (7)) replaced by $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n \pm O(\ln\ln n)}{n}$ (resp., $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$), and keeping all the conditions in Theorem 1 (resp., Corollary 1, we demonstrate that the properties (a) and (b) in Theorem 1 (resp., (8) in Corollary 1) still hold. The details of the proof can be found in our technical report [14].

Lemma 1. *If* $\frac{{K_n}^2}{P_n} = o(1)$*, then* $p_{s,q} \sim \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q$ *.*

See Appendix for the proof of Lemma 1.

D. The Practicality of the Conditions in Theorem 1 and Corollary 1

We check the practicality of the conditions in Theorem 1 and Corollary 1: $K_n = \omega(1)$, ${K_n}^2/P_n = o(1)$, (4) and (7). Clearly, condition $\frac{{K_n}^2}{P_n} = o(1)$ implies $P_n \geq 3K_n$ for all n sufficiently large. The condition $K_n = \omega(1)$ follows trivially in wireless sensor network applications since K_n is often at least logarithmic with n, the number of sensor nodes in the network. In addition, the condition $\frac{{K_n}^2}{P_n} = o(1)$ satisfies in practice since the key pool size P_n is expected to be several orders of magnitude larger than the key ring size K_n [3], [6]. Finally, (4) and (7) present the range of $p_{e,q}$ that is of interest.

IV. Numerical Experiments

To confirm the results in Theorem 1, we now provide numerical experiments in the non-asymptotic regime; i.e., when parameter values are set according to real-world wireless sensor network scenarios. As we will see from the simulation, the experimental observations are in agreement with our theoretical findings.

In all experiments, we fix the number of nodes at $n = 2,000$ and the key pool size at $P = 10,000$. In Figure 1, we plot the probability distribution for the number of nodes with degree h in graph $\mathbb{G}_q(n, K, P, p)$ for $h = 2, 3$ from both the simulation and the analysis, with $q = 2$, $K = 36$ and $p = 0.7$. On the one hand, for the simulation, we generate $2,000$ independent samples of $\mathbb{G}_q(n, K, P, p)$ and record the count (out of a possible $2,000$) that the number of nodes with degree h for each h equals a particular non-negative number M. Then the empirical probabilities are obtained by dividing the counts by $2,000$. On the other hand, we approximate the analytical curves by the asymptotic results as explained below. Property (a) of Theorem 1 notes that with the parameter conditions therein, the number of nodes in $\mathbb{G}_q(n, K_n, P_n, p_n)$ with any degree approaches to a Poisson distribution as $n \to \infty$; and in our technical report [14], for

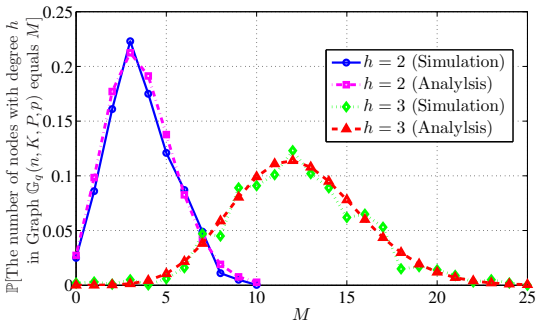

Fig. 1. A plot of the probability distribution for the number of nodes with degree h for $h = 2, 3$ in graph $\mathbb{G}_q(n, K, P, p)$ with $n = 2,000$, $q = 2$, $P = 10,000$, $K = 36$ and $p = 0.7$.

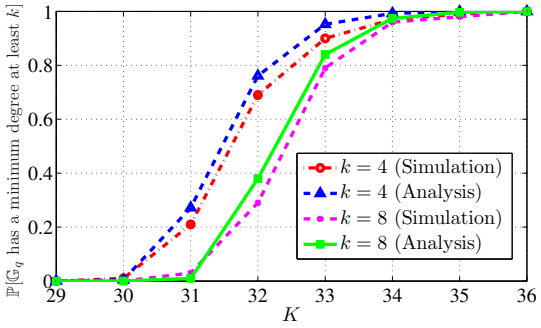

Fig. 2. A plot of the probability that graph $\mathbb{G}_q(n, K, P, p)$ has a minimum node degree at least k as a function of K for $k = 4$ and $k = 8$ with $q = 2$, $n = 2,000$, $P = 10,000$, and $p = 0.8$.

the asymptotic Poisson distribution of the number of nodes with degree h for any non-negative integer h, we specify the mean as $n(h!)^{-1}(np_{e,q})^h e^{-np_{e,q}}$ (denoted by λ_h). We derive λ_h by computing the corresponding probability of $p_{e,q}$ in $\mathbb{G}_q(n, K, P, p)$ through $p_{e,q} = p \cdot \sum_{u=q}^{K} \left[\binom{K}{u}\binom{P-K}{K-u}/\binom{P}{K}\right]$ given (1-3) and $P > 2K$. Then for each h, we plot a Poisson distribution with mean λ_h as the curve corresponding to the analysis. We observe that the curves generated from the simulation and those obtained by the analysis are close to each other, confirming the result on asymptotic Poisson distribution in property (a) of Theorem 1.

In Figure 2, we depict the probability that graph $\mathbb{G}_q(n, K, P, p)$ has a minimum node degree at least k from both the simulation and the analysis, for $q = 2$ and $p = 0.8$ and K varying from 29 to 36 (we still set $n = 2,000$ and $P = 10,000$). Similar to the experiments for Figure 1 above, we also generate $2,000$ independent samples of graph $\mathbb{G}_q(n, K, P, p)$ and record the count that the minimum degree of graph $\mathbb{G}_q(n, K, P, p)$ is no less than k; and the empirical probability of $\mathbb{G}_q(n, K, P, p)$ having a minimum degree at least k is derived by averaging over the $2,000$ experiments. The analytical curves in Figure 2 are also approximated by the asymptotical results as follows. First, we compute the corresponding probability of $p_{e,q}$ in $\mathbb{G}_q(n, K, P, p)$ through the aforementioned form $p_{e,q} = p \cdot \sum_{u=q}^{K} \left[\binom{K}{u}\binom{P-K}{K-u}/\binom{P}{K}\right]$. Then we determine α_n by (7). We write α_n as α here as n is fixed. Then with an approximation to the asymptotical results in Corollary 1, we plot the analytical curves by considering that the minimum degree of $\mathbb{G}_q(n, K, P, p)$ is at least k with probability $e^{-\frac{e^{-\alpha}}{(k-1)!}}$. The observation that the curves generated from the simulation and the analytical curves are close to each other is in accordance with Corollary 1.

V. Related Work

Erdős and Rényi [4] and Gilbert [7] propose the random graph model $G(n, p_n)$ defined on a node set with size n such that an edge between any two nodes exists with probability p_n *independently* of all other edges. For graph $G(n, p_n)$, Erdős and Rényi [4] derive the asymptotically exact probabilities for connectivity the property that the minimum degree is at least 1, by proving first that the number of isolated nodes converges to a Poisson distribution as $n \to \infty$. Later, they extend the results to general k in [5], obtaining the asymptotic Poisson distribution for the number of nodes with any degree and the asymptotically exact probabilities for k-connectivity and the event that the minimum degree is at least k, where k-connectivity is defined as the property that the network remains connected in spite of the removal of any $(k-1)$ nodes.

For graph $\mathbb{G}_q(n, K_n, P_n)$, Bloznelis *et al.* [2] demonstrate that a connected component with at at least a constant fraction of n emerges asymptotically when probability $p_{e,q}$ exceeds $1/n$. Recently, still for $G_q(n, K_n, P_n)$, Bloznelis [1] establishes the asymptotic Poisson distribution for the number of nodes with any degree. Our results in Theorem 1 by setting p_n as 1 imply his result; in particular, the result that he obtains is a special case of property (a) in our Theorem 1.

Yağan (a co-author of this paper) [10] presents zero-one laws in graph $\mathbb{G}_1$ (our graph $\mathbb{G}_q$ in the case of $q = 1$) for connectivity and for the property that the minimum degree is at least 1. We extend Yağan's results to general k for $\mathbb{G}_1$ in [12], [13]. We also derive asymptotically exact probabilities for k-connectivity and the event that the minimum degree no less than k for $\mathbb{G}_1$ in our technical report [14]. (As noted in Remark 5, we establish in [14] the results of Theorem 1 and Corollary 1 under weaker conditions for the case of $q = 1$; and in this paper, we do not present the corresponding details given in [14] due to the space limitation.)

Krishnan *et al.* [8] and Krzywdziński and Rybarczyk [9] describe results for the probability of connectivity asymptotically converging to 1 in WSNs employing the q-composite key predistribution scheme with $q = 1$ (i.e., the Eschenauer-Gligor key predistribution scheme), not under the on/off channel model but under the well-known disk model [8], [9], [10], where nodes are distributed over a bounded region of a Euclidean plane, and two nodes have to be within a certain distance for communication. Simulation results in our work [12] indicate that for WSNs under the key predistribution scheme with $q = 1$, when the on-off channel model is replaced by the disk model, the performances for k-connectivity and for the property that the minimum degree is at least k do not change significantly.

VI. Conclusion and Future Directions

In this paper, we analyze several topological properties related to node degree in WSNs operating under the q-composite key predistribution scheme with on/off channels. Numerical simulation is shown to be in agreement with our theoretical findings.

Two future research directions are as follows. To begin with, we can derive the asymptotically exact probability and thus a zero-one law for k-connectivity in graph $\mathbb{G}_q$ once we show $\mathbb{G}_q$ becomes k-connected whenever its minimum node degree becomes at least k. This will extend our results for $\mathbb{G}_1$ in our technical report [14] to $\mathbb{G}_q$.

Another extension of our work is to consider physical link constraints different with the on/off channel model, where one candidate is the aforementioned disk model.

References

[1] M. Bloznelis. Degree and clustering coefficient in sparse random intersection graphs. *The Annals of Applied Probability*, 23(3):1254–1289, 2013.

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

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

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

[5] P. Erdős and A. Rényi. On the strength of connectedness of random graphs. *Acta Math. Acad. Sci. Hungar*, pages 261–267, 1961.

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

[7] E. N. Gilbert. Random graphs. *The Annals of Mathematical Statistics*, 30:1141–1144, 1959.

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

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

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

[11] O. Yağan and A. M. Makowski. Zero-one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, May 2012.

[12] J. Zhao, O. Yağan, and V. Gligor. k-Connectivity in secure wireless sensor networks with physical link constraints – the on/off channel model. *Technical Report*, 2012. Available online at http://www.andrew.cmu.edu/user/junzhao/papers/RkgRggTech12.pdf .

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

[14] 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 (extended version). *Technical Report*, 2014. Available online at http://www.andrew.cmu.edu/user/junzhao/papers/QcompTech14.pdf .

Appendix: Establishing Lemma 1

We elaborate the proof Lemma 1 below. We simplify $S_i \cap S_j$ by writing it as S_{ij}. Clearly, $P_n \geq 2K_n$ for all n sufficiently large, due to $\frac{{K_n}^2}{P_n} = o(1)$. Then from (1), $p_{s,q} = \sum_{u=q}^{K_n} \mathbb{P}[|S_{ij}| = u]$ follows. Therefore, Lemma 1 holds once we establish the following (11) and (12):

$$\mathbb{P}[|S_{ij}| = q] \sim (q!)^{-1}\big({K_n}^2/P_n\big)^q, \tag{11}$$

and

$$\mathbb{P}[|S_{ij}| = q] \sim \sum_{u=q}^{K_n} \mathbb{P}[|S_i \cap S_j| = u]. \tag{12}$$

We will first establish (11) by providing an upper bound and a lower bound for $\mathbb{P}[|S_{ij}| = q]$, respectively.

For all n sufficiently large, given $P_n \geq 2K_n$ and (2), we derive that for $u = 0, 1, \ldots, K_n$,

$$\mathbb{P}[|S_{ij}| = u] = \binom{K_n}{u}\binom{P_n - K_n}{K_n - u}\Big/\binom{P_n}{K_n}. \tag{13}$$

Setting u as q in (13), it is clear that

$$\mathbb{P}[|S_{ij}|=q] = \frac{1}{q!}\left[\frac{K_n!}{(K_n-q)!}\right]^2 \cdot \frac{(P_n-K_n)!}{(P_n-2K_n+q)!} \cdot \frac{(P_n-K_n)!}{P_n!}. \tag{14}$$

For the upper bound on $\mathbb{P}[|S_{ij}| = q]$, using (14) and $\frac{{K_n}^2}{P_n - K_n} = o(1)$ which holds from $\frac{{K_n}^2}{P_n} = o(1)$, and applying the fact that $1 + x \leq e^x$ for any real x, we have

$$\begin{aligned}
&\mathbb{P}[|S_{ij}| = q] \\
&\quad \leq (q!)^{-1} {K_n}^{2q} {P_n}^{K_n - q} (P_n - K_n)^{-K_n} \\
&\quad = (q!)^{-1}\big({K_n}^2/P_n\big)^q \big[1 + K_n/(P_n - K_n)\big]^{K_n} \\
&\quad \leq (q!)^{-1}\big({K_n}^2/P_n\big)^q e^{\frac{{K_n}^2}{P_n - K_n}} \\
&\quad \leq (q!)^{-1}\big({K_n}^2/P_n\big)^q \cdot [1 + o(1)].
\end{aligned} \tag{15}$$

For the part of finding the lower bound, we employ (14), $\frac{{K_n}^2}{P_n} = o(1)$ and $\big(1 - \frac{2K_n}{P_n}\big)^{K_n} \to 1$ as $n \to \infty$ which follows by $\frac{{K_n}^2}{P_n} = o(1)$ and Fact 3 in our paper [12]. We also use $\frac{(K_n - q)^2}{P_n - 2K_n} \sim \frac{{K_n}^2}{P_n}$ due to $K_n = \omega(q)$ by $K_n = \omega(1)$, and $P_n = \omega(K_n)$ by $\frac{{K_n}^2}{P_n} = o(1)$. Therefore,

$$\begin{aligned}
&\mathbb{P}[|S_{ij}| = q] \\
&\quad \geq (q!)^{-1}(K_n - q)^{2q}(P_n - 2K_n)^{K_n - q} {P_n}^{-K_n} \\
&\quad = (q!)^{-1}\big[(K_n - q)^2/(P_n - 2K_n)\big]^q \cdot \big(1 - 2K_n/P_n\big)^{K_n} \\
&\quad \sim (q!)^{-1}\big({K_n}^2/P_n\big)^q;
\end{aligned} \tag{16}$$

i.e., $(q!)^{-1}\big({K_n}^2/P_n\big)^q \cdot [1 - o(1)]$ is a lower bound for $\mathbb{P}[|S_{ij}| = q]$. Then (11) follows from (15) and (16).

Below we focus on proving (12). From (13), for $u \geq q$,

$$\begin{aligned}
&\mathbb{P}[|S_{ij}| = u]/\mathbb{P}[|S_{ij}| = q] \\
&= q!(u!)^{-1}\left[\prod_{r=0}^{u-q-1}(K_n - q - r)\right]\Big/\left[\prod_{r=0}^{u-q-1}(P_n - 2K_n + u - r)\right] \\
&\leq [(u-q)!]^{-1}\big({K_n}^2/P_n\big)^{u-q}.
\end{aligned}$$

Setting $t := u - q$ and using $\frac{{K_n}^2}{P_n} = o(1)$, we obtain (12) by

$$\begin{aligned}
&\left\{\sum_{u=q}^{K_n}\mathbb{P}[|S_{ij}| = q]\right\}\Big/\mathbb{P}[|S_{ij}| = q] \\
&\quad \leq \sum_{t=0}^{\infty}\big[t!^{-1}\big({K_n}^2/P_n\big)^t\big] = e^{{K_n}^2/P_n} \to 1, \text{ as } n \to \infty.
\end{aligned}$$

The proof of Lemma 1 is completed with (11) and (12). □