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

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

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

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

Abstract—The $q$-composite key predistribution scheme is used prevalently for secure communications in large-scale wireless sensor networks (WSNs). Prior work explores topological properties of WSNs employing the $q$-composite scheme for $q = 1$ with unreliable communication links modeled as independent on/off channels. In this paper, we investigate topological properties related to the node degree in WSNs operating under the $q$-composite scheme and the on/off channel model. Our results apply to general $q$ and are stronger than those reported for the node degree in prior work even for the case of $q$ being 1. Specifically, we show that the number of nodes with certain degree is asymptotically equivalent in distribution to a Poisson random variable, present the asymptotic probability distribution for the minimum degree of the network, and establish the asymptotically exact probability for the property that the minimum degree is at least an arbitrary value. Numerical experiments confirm the validity of our analytical findings.

Index Terms—Random intersection graph, random key graph, $s$-intersection graph, connectivity, node degree, key predistribution, wireless sensor network.

I. INTRODUCTION

The basic key predistribution scheme of Eschenauer and Gligor has been recognized as a typical solution to secure communication in wireless sensor networks (WSNs) and studied extensively in the literature over the last decade [1]–[11]. The idea is that cryptographic keys are assigned before deployment to ensure secure sensor-to-sensor communications.

The $q$-composite key predistribution scheme proposed by Chan et al. [1] as an extension of the basic Eschenauer–Gligor scheme (the $q$-composite scheme in the case of $q = 1$) has received much interest since its introduction.

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. Then two sensors establish a secure link in between after deployment 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 both functions of $n$ for generality, with the natural condition $1 \leq K_n \leq P_n$. Examples of physical link constraints include the reliability of the transmission channel and the distance between two sensors close enough for communication. The $q$-composite scheme with $q \geq 2$ outperforms the basic Eschenauer–Gligor scheme with $q = 1$ in terms of the strength against small-scale network capture attacks while trading off increased vulnerability in the face of large-scale attacks [1].

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 comprising independent channels which are either on or off. The degree of a node $v$ is the number of nodes having secure 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 certain degree is asymptotically equivalent in distribution to a Poisson random variable, 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 and we consider the WSNs with $q = 1$ and show results for several topological properties, yet results about node degree in these prior work are weaker than our analytical findings even 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 the $q$-composite scheme and the on/off channel model is an intersection of two distinct types of random graphs. It is the intertwining of these two graphs that makes our analysis challenging.

We organize the rest of the paper as follows. Section II describes the system model in detail. Afterwards, we present and discuss the results in Section III. Subsequently, we provide 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 and identify future research directions in Section VI.

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 use a node set $V = \{v_1, v_2, \ldots, v_n\}$ to represent the $n$ sensors. For each node $v_i \in V$, 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.

1A sensor is also referred to as a node.
The $q$-composite key predistribution scheme is modeled by a uniform $q$-intersection graph denoted by $G_q(n, K_n, P_n)$, which is defined on the node set $V$ such that any two distinct nodes $v_i$ and $v_j$ sharing at least $q$ key(s) (an event denoted by $\Gamma_{ij}$) have an edge in between. Clearly, $\Gamma_{ij}$ equals event $|S_i \cap S_j| \geq q$, where $|A|$ with $A$ as a set means the cardinality of $A$.

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 $0 < p_n \leq 1$. Denoting by $C_{ij}$ the event that the channel between distinct nodes $v_i$ and $v_j$ is on, we have $\mathbb{P}[C_{ij}] = p_n$, where $\mathbb{P}[E]$ denotes the probability that event $E$ happens, throughout the paper. The on/off channel model is represented by an Erdős-Rényi graph $G(n, p_n)$ [52] defined on the node set $V$ such that $v_i$ and $v_j$ have an edge in between if event $C_{ij}$ occurs.

Finally, we denote by $G_q(n, K_n, P_n)$ 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 $G_q$ rather than $G_q(n, K_n, P_n, p_n)$ for notation brevity. Graph $G_q$ is defined on the node set $V$ such that there exists an edge between nodes $v_i$ and $v_j$ if and only if events $\Gamma_{ij}$ and $C_{ij}$ happen at the same time. We set event $E_{ij} := \Gamma_{ij} \cap C_{ij}$. Then $G_q$ can be seen as the intersection of $G_q(n, K_n, P_n)$ and $G(n, p_n)$, i.e.,

$$G_q = G_q(n, K_n, P_n) \cap G(n, p_n).$$

We define $p_{s,q}$ as the probability that two different nodes share at least $q$ key(s) and $p_{e,q}$ as the probability that two distinct nodes have a secure link in $G_q$. Clearly, $p_{s,q}$ and $p_{e,q}$ are the edge probabilities in graphs $G_q(n, K_n, P_n)$ and $G_q$, respectively. $p_{s,q}$ and $p_{e,q}$ both depend on $K_n, P_n$ and $q$, while $p_{e,q}$ also depends on $p_n$. By definition, $p_{s,q}$ is determined through

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

where it is shown [6], [7] that

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

From $E_{ij} = \Gamma_{ij} \cap C_{ij}$ and the independence of $C_{ij}$ and $\Gamma_{ij}$, we obtain

$$p_{e,q} = \mathbb{P}[E_{ij}] = \mathbb{P}[C_{ij}] \cdot \mathbb{P}[\Gamma_{ij}] = p_n \cdot p_{s,q}.$$
Remark 1. Property (b) of Theorem 7 presents the asymptotic probability distribution for the minimum degree of the network.

We present a corollary of Theorem 1 below. The corollary is established with the help of a graph coupling argument [12] (see the full version [6] for the detailed proof).

Corollary 1. For graph $G_q$ under $K_n = \omega(1)$ and $K_n^2 / P_n = o(1)$, with some sequence $\beta_n$ defined by

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

for some positive integer $k$, and with $\delta$ denoting the minimum degree of $G_q$, it holds that

$$\lim_{n \to \infty} P[\delta \geq k] = \begin{cases} e^{-\frac{-\beta_n^*}{(k-1)\ln n}}, & \text{if } \lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty), \\ 1, & \text{if } \lim_{n \to \infty} \beta_n = \infty, \\ 0, & \text{if } \lim_{n \to \infty} \beta_n = -\infty. \end{cases}$$

Remark 2. Corollary 1 presents the asymptotically exact probability and a zero–one law [12] (a kind of phase transition [40]) for the event that graph $G_q$ has a minimum node degree no less than $k$.

Remark 3. Setting $p_n$ to 1 in Theorem 7 and Corollary 1 we obtain corresponding results [24] for topological properties in uniform $q$-intersection graph $G_q(n, K_n, P_n)$.

Remark 4. In Theorem 7 and Corollary 1 given $K_n = \omega(1)$, we have $q < K_n$ for all $n$ sufficiently large since $q$ does not scale with $n$. From $K_n^2 / P_n = o(1)$, it is clear that $K_n < P_n$ for all $n$ sufficiently large.

B. Practicality of Conditions

We check the practicality of the conditions in Theorem 7 and Corollary 1 $K_n = \omega(1)$, $\frac{K_n^2}{P_n} = o(1)$, and (4)–(6). First, the condition $K_n = \omega(1)$ follows in wireless sensor network applications [2] since $K_n$ is often logarithmic [2] with $n$, the number of sensor nodes in the network. Second, the condition $\frac{K_n^2}{P_n} = o(1)$ also holds in practice since the key pool size $P_n$ is expected to be several orders of magnitude larger than $K_n$ [11, 5]. Finally, (4)–(6) present the range of $p_{e,q}$ that is of interest.

C. Analogos of Theorem 7 and Corollary 7

Analogous results to those of Theorem 1 and Corollary 1 can be given with $p_{e,q}$ at all places substituted by $p_n \cdot \frac{1}{q(\frac{K_n^2}{P_n})^3}$, due to $p_{e,q} = p_n \cdot p_{s,q}$ from (5) and the replacement of $p_{s,q}$ by $\frac{1}{q(\frac{K_n^2}{P_n})^3}$ given Lemma 7 below. However, extra conditions have to be added for some results. The details as well as the proof of Lemma 7 are provided in the full version [6].

(b4) if $\lim_{n \to \infty} \alpha_n = -\infty$, then as $n \to \infty$, 

$$\delta = \ell - 1 \text{ with a probability tending to } 1,$$

$$\delta \neq \ell - 1 \text{ with a probability converging to } 0.$$
We derive $\lambda_{n,h}$ by computing the corresponding probability of $p_{e,q}$ in $G_q(n, K, P, p)$ through

$$p_{e,q} = p \cdot \sum_{u=0}^{K} \left[ \frac{K-u}{K} \right] \left( \frac{P-K}{K} \right)^{u} \left( \frac{P}{K} \right)^{P-K}$$

(7)
given (1) and $P > 2K$. Then for each $h$, we plot a Poisson distribution with mean $\lambda_{n,h}$ 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 $G_q(n, K, P, p)$ has a minimum node degree at least $k$ from both the simulation and the analysis, for $k = 4$ and $k = 8$ with $q = 2$ 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 $G_q(n, K, P, p)$ and record the count that the minimum degree of graph $G_q(n, K, P, p)$ is no less than $k$; and the empirical probability of $G_q(n, K, P, p)$ 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 asymptotic results as follows. First, we compute the corresponding probability of $p_{e,q}$ in $G_q(n, K, P, p)$ through (7). Then based on (6), we determine $\beta$ through $p_{e,q} = \frac{\ln n + (k-1) \ln \ln n + \beta}{\ln \ln n}$. Then with an approximation to the asymptotic results in Corollary 1, we plot the analytical curves by considering that the minimum degree of $G_q(n, K, P, p)$ is at least $k$ with probability $e^{\frac{\beta}{(k-1)^{\frac{1}{n}}}}$. 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 [52] 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 [52] 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 [53], obtaining the asymptotic Poisson distribution for the number of nodes with certain 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. Since its introduction, graph $G(n, p_n)$ has been widely investigated [25]–[55].

For graph $G_q(n, K_n, P_n)$, Bloznelis et al. [7] demonstrate that a connected component with at least a constant fraction of $n$ emerges asymptotically when the edge probability $p_{e,q}$ exceeds $1/n$. Bloznelis and Łuczak [51] have recently considered $k$-connectivity throughout this paper means $k$-vertex-connectivity [51].

connectivity and perfect matching. Still in $G_q(n, K_n, P_n)$, Bloznelis et al. [20] investigate assortativity and clustering, while for asymptotic node degree distribution, Bloznelis [19] analyzes clustering coefficient and the degree distribution of a typical node. We [21] compute the probability distribution for the minimum node degree. Recently, Bloznelis and Rybarczyk [22] and we [23] have derived the asymptotically exact probability of $k$-connectivity. Several variants or generalizations of graph $G_q(n, K_n, P_n)$ are also considered in the literature [7], [18]–[20].

When $q = 1$, for graph $G_1(n, K_n, P_n)$ (also referred to as a random key graph [8], [10], [11] or a uniform random intersection graph [9], [13]) and some of its variants, a number of properties have been extensively studied in the literature including component evolution [43], connectivity [9], [10], [13], $k$-connectivity [12], [37], node degree distribution [14]–[17] and independent sets [31], [32].

In graph $G_1$, Ya˘gan [2] presents zero–one laws for connectivity and for the property that the minimum degree is at least 1. We extend Ya˘gan’s results to general $k$ for $G_1$ in [4].

Krishnan et al. [8] and Krzywydziński and Rybarczyk [38] 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 basic Eschenauer–Gligor key predistribution scheme), not under the on/off channel model but under the well-known disk model [45]–[50], 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 [3] 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 a wireless sensor network operating under the $q$-composite key predistribution scheme with on/off channels. The network is modeled by the superposition of an Erdős-Rényi graph on a uniform $q$-intersection graph. Numerical simulation is shown to be in agreement with our theoretical findings.

Two future research directions are as follows. To begin with, we can consider physical link constraints different with the on/off channel model, where one candidate is the aforementioned disk model. Another extension is to derive the asymptotically exact probability and thus a zero–one law for $k$-connectivity in graph $G_q$. Note that a zero–law for $k$-connectivity follows immediately from Corollary 1 since $k$-connectivity implies the property of minimum node degree being at least $k$. The one–law and the asymptotically exact probability result will follow if we show that under certain conditions, the probability that $C_q$ has a minimum node degree no less than $k$ but is not $k$-connected converges to 0 as $n \to \infty$. Best Student Paper Finalist in 2014 IEEE International Symposium on Information Theory (ISIT)
