Topological Properties of Wireless Sensor Networks Under the Q-Composite Key Predistribution Scheme With Unreliable Links

Jun Zhao, Osman Yagan and Virgil Gligor

January 24, 2014

CMU-CyLab-14-002

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Topological properties of wireless sensor networks under the q-composite key predistribution scheme with unreliable links

Jun Zhao, Osman Yağan and Virgil Gligor

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

***Abstract*—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 [12] (IEEE IT 2012) and we [15] (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 [12], [15]. Specifically, we show that the number of nodes with an arbitrary 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 [7] (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 comprising 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 an arbitrary 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 [12] and we [14], [15] 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 [12].

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. In Section IV, we detail the steps of establishing Theorem 1 through Lemma 1. Section V provides the proof of Lemma 1 by the help of Propositions 1 and 2, which are proved in Sections VI and VII, respectively. Subsequently, we present numerical experiments in Section VIII to confirm our analytical results, whereas we discuss the results for the case of $q = 1$ in particular in Section IX. Section X is devoted to relevant results in the literature. Next, we conclude the paper and identify future research directions in Section XI, followed by Appendices A and B.

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. With $S_{ij} := S_i \cap S_j$, event Γ_{ij} equals $\big[|S_{ij}| \geq q\big]$, 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 $G(n, p_n)$ [5] 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 $E_{ij} := \Gamma_{ij} \cap C_{ij}$ and also write E_{ij} as $E_{v_i v_j}$ when necessary. 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, where the subscripts "s" and "e" are short for "secure" and "edge", respectively. $p_{s,q}$ 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 events 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 $o(\cdot), \omega(\cdot), O(\cdot), \sim$.[1]

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 $\frac{K_n^2}{P_n} = o(1)$. 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 an arbitrary 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 $n \to \infty$,*

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

[1] Specifically, given two positive functions $f(n)$ and $g(n)$,
1) $f(n) = o\left(g(n)\right)$ signifies $\lim_{n\to\infty}[f(n)/g(n)] = 0$.
2) $f(n) = \omega\left(g(n)\right)$ means $\lim_{n\to\infty}[f(n)/g(n)] = \infty$; i.e., $g(n) = o\left(f(n)\right)$.
3) $f(n) = O\left(g(n)\right)$ signifies that there exists a positive constant c such that $f(n) \leq cg(n)$ for all n sufficiently large.
4) $f(n) \sim g(n)$ means $\lim_{n\to\infty}[f(n)/g(n)] = 1$; namely, $f(n)$ and $g(n)$ are asymptotically equivalent.

Remark 1. *Theorem 1 for graph $\mathbb{G}_q$ establishes that the number of nodes with an arbitrary 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*

$$-\frac{1}{2}\ln\ln n \le \beta_n < \frac{1}{2}\ln\ln n \tag{7}$$

such that

$$p_{e,q} = \frac{\ln n + (\ell-1)\ln\ln n + \beta_n}{n}. \tag{8}$$

In fact, it is clear that (8) follows from (6); and with (5), it holds that

$$\frac{np_{e,q} - \ln n + (\ln\ln n)/2}{\ln\ln n} < \ell \le \frac{np_{e,q} - \ln n + (\ln\ln n)/2}{\ln\ln n} + 1,$$

which along with (6) further leads to (7) in view of

$$\begin{aligned}\beta_n &= np_{e,q} - \ln n - (\ell-1)\ln\ln n,\\ &< np_{e,q} - \ln n - [np_{e,q} - \ln n + (\ln\ln n)/2] + \ln\ln n\\ &= (\ln\ln n)/2,\end{aligned}$$

and

$$\begin{aligned}\beta_n &= np_{e,q} - \ln n - (\ell-1)\ln\ln n,\\ &\ge np_{e,q} - \ln n - [np_{e,q} - \ln n + (\ln\ln n)/2]\\ &= -(\ln\ln n)/2.\end{aligned}$$

The proof of Theorem 1 is given in the next four sections. 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*

$$p_{e,q} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}, \tag{9}$$

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

$$\mathbb{P}[\delta \ge k] \to e^{-\frac{e^{-\alpha^*}}{(k-1)!}} = \begin{cases}1, & \text{if } \alpha^* = \infty,\\ 0, & \text{if } \alpha^* = -\infty.\end{cases} \tag{10}$$

Remark 3. *Corollary 1 for graph $\mathbb{G}_q$ presents the asymptotically exact probability and a zero-one law [13] 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: $P_n \ge 3K_n$ for all n sufficiently large. We present the details in Section IX.*

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

B. Establishing Corollary 1 Given Theorem 1

Given (9) (a condition in Corollary 1), we determine ℓ and β_n through (5) and (6) in Theorem 1. Then

$$\begin{aligned}\ell &= \left\lfloor \frac{(k-1)\ln\ln n + \alpha_n + (\ln\ln n)/2}{\ln\ln n} \right\rfloor + 1\\ &= k + \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor,\end{aligned} \tag{11}$$

and

$$\begin{aligned}\beta_n &= (k-1)\ln\ln n + \alpha_n - \left(k + \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor - 1\right)\ln\ln n,\\ &= \alpha_n - \left\lfloor \frac{\alpha_n}{\ln\ln n} + \frac{1}{2} \right\rfloor \ln\ln n.\end{aligned} \tag{12}$$

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

Case ①: $-\frac{1}{2}\ln\ln n \le \alpha_n < \frac{1}{2}\ln\ln n$. Then from (11) and (12), 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,

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

Then with $e^{\infty} = \infty$ and $e^{-\infty} = 0$, (10) follows in case ①.

Case ②: $\alpha_n \ge \frac{1}{2}\ln\ln n$. Then from (11) and (12), it holds that $\ell \ge k + 1$. Hence, $\mathbb{P}[\delta \ge k] \to 1$ by Theorem 1, leading to (10) in case ②.

Case ③: $\alpha_n < -\frac{1}{2}\ln\ln n$. Then from (11) and (12), it holds that $\ell \le k - 1$. Consequently, $\mathbb{P}[\delta \ge k] \to 0$ by Theorem 1, resulting in (10) in case ③.

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 $\mathbb{G}_q$ 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 2 in Appendix A, 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 2 applies owing to $\frac{{K_n}^2}{P_n} = o(1)$ which holds in both Theorem 1 and Corollary 1). Thus, with (4) (resp., (9)) 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 below that the properties (a) and (b) in Theorem 1 (resp., (10) in Corollary

1) still hold. To do this, first, if $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n \pm O(\ln\ln n)}{n}$, then from Lemma 2, we obtain

$$p_{e,q} = p_n \cdot p_{s,q} = p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q \cdot [1 \pm o(1)]$$
$$= \frac{\ln n \pm O(\ln\ln n)}{n} \cdot [1 \pm o(1)] = \frac{\ln n \pm O(\ln\ln n)}{n};$$

second, with $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$ replacing (9) in Corollary 1, in proving (10), we introduce an extra condition $|\alpha_n| \le \ln\ln n$ by a coupling argument, the explanation of which is deferred to the next paragraph. Hence, from $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, $|\alpha_n| \le \ln\ln n$ and Lemma 2, it holds that $p_{e,q} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n \pm O(1)}{n}$.

We now present the coupling argument which confines α_n as $|\alpha_n| \le \ln\ln n$ to establish Corollary 1 with (9) replaced by $p_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$. First, if $\lim_{n\to\infty}\alpha_n = \alpha^* \in (-\infty, \infty)$ (i.e., $-\infty < \alpha^* < \infty$), it is clear that α_n is bounded; namely, $|\alpha_n| = O(1)$, so $|\alpha_n| \le \ln\ln n$ follows in this case. Therefore, in deriving (10), we only need to consider $\lim_{n\to\infty}\alpha_n = \alpha^* = \infty$ and $\lim_{n\to\infty}\alpha_n = \alpha^* = -\infty$. Setting $\widehat{\alpha}_n$ as $\min\{\alpha_n, \ln\ln n\}$ and $\widetilde{\alpha}_n$ as $\max\{\alpha_n, -\ln\ln n\}$, we define $\widehat{p}_n$ and $\widetilde{p}_n$ through

$$\widehat{p}_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \widehat{\alpha}_n}{n},$$

and

$$\widetilde{p}_n \cdot \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q = \frac{\ln n + (k-1)\ln\ln n + \widetilde{\alpha}_n}{n}.$$

With $\widehat{p}_n \le p_n \le \widetilde{p}_n$, similar to the argument in Section V-B in our work [14] (we omit the details here due to the space limitation), there exist graph couplings such that $\mathbb{G}_q(n, K_n, P_n, \widehat{p}_n)$ is a spanning subgraph of $\mathbb{G}_q(n, K_n, P_n, p_n)$, which is further a spanning subgraph of $\mathbb{G}_q(n, K_n, P_n, \widetilde{p}_n)$. Clearly, if $\lim_{n\to\infty}\alpha_n = \infty$, then $\lim_{n\to\infty}\widehat{\alpha}_n = \infty$ and $|\widehat{\alpha}_n| \le \ln\ln n$ for all n sufficiently large; and if $\lim_{n\to\infty}\alpha_n = -\infty$, then $\lim_{n\to\infty}\widetilde{\alpha}_n = -\infty$ and $|\widetilde{\alpha}_n| \le \ln\ln n$ for all n sufficiently large. Then by the fact that the probability that a graph has a minimum node degree at least k is no less than the probability that an arbitrary spanning subgraph has a minimum node degree at least k, we can introduce the condition $|\alpha_n| \le \ln\ln n$ in establishing (10).

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: $K_n = \omega(1)$, $\frac{{K_n}^2}{P_n} = o(1)$, (4) and (9). Clearly, condition $\frac{{K_n}^2}{P_n} = o(1)$ implies $P_n \ge 3K_n$ 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], [7]. Finally, (4) and (9) present the range of $p_{e,q}$ that is of interest.

IV. Establishing Theorem 1

A. Proving property (a)

For $h = 0, 1, \ldots$, with ϕ_h counting the number of nodes with degree h in $\mathbb{G}_q$, we will show that ϕ_h asymptotically follows a Poisson distribution with mean λ_h. This is done by using the method of moments; specifically, in view of [4, Theorem 2.13], we will obtain the desired result upon establishing

$$\mathbb{P}[\text{Nodes } v_1, v_2, \ldots, v_m \text{ have degree } h] \sim {\lambda_h}^m / n^m. \quad (13)$$

Therefore, if Lemma 1 below holds, then the proof of property (a) in Theorem 1 is completed; in particular, we will have that for any integers $h \ge 0$ and $\ell \ge 0$,

$$\mathbb{P}[\phi_h = \ell] \sim (\ell!)^{-1}{\lambda_h}^\ell e^{-\lambda_h}. \quad (14)$$

Lemma 1. *Given (4) (i.e., $p_{e,q} = \frac{\ln n \pm O(\ln\ln n)}{n}$), $K_n = \omega(1)$ and $\frac{{K_n}^2}{P_n} = o(1)$, then for any integers $m \ge 1$ and $h \ge 0$, we have*

$$\mathbb{P}[\textit{Nodes } v_1, v_2, \ldots, v_m \textit{ have degree } h] \sim (h!)^{-m}(np_{e,q})^{hm}e^{-mnp_{e,q}};$$

i.e., (13) follows with λ_h set by

$$\lambda_h = n(h!)^{-1}(np_{e,q})^h e^{-np_{e,q}}. \quad (15)$$

Section V details the proof of Lemma 1. Given (4), we obtain the following two results, which are frequently used in the rest of the paper:

$$p_{e,q} \sim \frac{\ln n}{n}, \quad (16)$$

and

$$p_{e,q} \le \frac{2\ln n}{n} \text{ for all } n \text{ sufficiently large.} \quad (17)$$

B. Proving property (b)

For any $\gamma \ge 0$, properties ① and ② below follow.

① The event $(\delta \ge \gamma)$ (i.e., the event that the minimum node degree of graph $\mathbb{G}$ is at least γ) is equivalent to the event $\bigcap_{h=0}^{\gamma-1}(\phi_h = 0)$ (i.e., no node has degree falling in $\{0, 1, \ldots, \gamma-1\}$).

② The event $(\delta \le \gamma)$ (i.e., the event that the minimum node degree of graph $\mathbb{G}$ is at most γ) and the event $\bigcup_{h=0}^{\gamma}(\phi_h \ne 0)$ (i.e., there is at least one node with degree at most γ) are equivalent.

Therefore,

$$\mathbb{P}[\delta \geq \ell+1] = \mathbb{P}\left[\bigcap_{h=0}^{\ell}(\phi_h = 0)\right] \text{ (by property ①)}$$
$$\leq \mathbb{P}[\phi_\ell = 0], \tag{18}$$
$$\mathbb{P}[\delta \leq \ell-2] \leq \mathbb{P}\left[\bigcup_{h=0}^{\ell-2}(\phi_h \neq 0)\right] \text{ (by property ②)}$$
$$\leq \sum_{h=0}^{\ell-2}\mathbb{P}[\phi_h \neq 0] \quad \text{(by the union bound)}, \tag{19}$$
$$\mathbb{P}[\delta \geq \ell] = \mathbb{P}\left[\bigcap_{h=0}^{\ell-1}(\phi_h = 0)\right] \text{ (by property ①)}$$
$$\leq \mathbb{P}[\phi_{\ell-1} = 0], \tag{20}$$

and

$$\mathbb{P}[\delta \geq \ell] = \mathbb{P}\left[\bigcap_{h=0}^{\ell-1}(\phi_h = 0)\right] \text{ (by property ①)}$$
$$= 1 - \mathbb{P}\left[\bigcup_{h=0}^{\ell-1}(\phi_h \neq 0)\right]$$
$$\geq 1 - \sum_{h=0}^{\ell-1}\mathbb{P}[\phi_h \neq 0] \text{ (by the union bound)}$$
$$= \mathbb{P}[\phi_{\ell-1} = 0] - \sum_{h=0}^{\ell-2}\mathbb{P}[\phi_h \neq 0]. \tag{21}$$

To use (18-21), we compute $\mathbb{P}[\phi_h \neq 0]$ for $h = 0, 1, \ldots$ given (14) and thus evaluate λ_h defined in (15). To calculate λ_h, we begin with looking at $p_{e,q}$ based on (5) and (6).

As noted after Remark 2, we have (7) and (8). Substituting (8) and (16) into (15) to compute λ_h, we have

$$\lambda_h = n(h!)^{-1}(np_{e,q})^h e^{-np_{e,q}}$$
$$\sim n(h!)^{-1}(\ln n)^h \times e^{-\ln n-(\ell-1)\ln\ln n-\beta_n}$$
$$= (h!)^{-1}(\ln n)^{h+1-\ell}e^{-\beta_n}.$$

By (7), it further follows that

$$\lambda_h \begin{cases} \to 0, \text{ for } h = 0, 1, \ldots, \ell-2; \\ \sim \frac{e^{-\beta_n}}{(\ell-1)!}, \text{ for } h = \ell-1; \\ \to \infty, \text{ for } h = \ell, \ell+1, \ldots. \end{cases} \tag{22}$$

Applying (22) to (14),

$$\mathbb{P}[\phi_h = 0] \sim e^{-\lambda_h} \begin{cases} \to 1, \text{ for } h = 0, 1, \ldots, \ell-2; \\ \sim e^{-\frac{e^{-\beta_n}}{(\ell-1)!}}, \text{ for } h = \ell-1; \\ \to 0, \text{ for } h = \ell, \ell+1, \ldots. \end{cases} \tag{23}$$

Using (23) in (18-21), it holds that

$$\mathbb{P}[\delta \geq \ell+1] = o(1), \tag{24}$$
$$\mathbb{P}[\delta \leq \ell-2] = o(1), \tag{25}$$

and

$$\mathbb{P}[\delta \geq \ell] \sim e^{-\frac{e^{-\beta_n}}{(\ell-1)!}}. \tag{26}$$

Then from (24) and (25),

$$\mathbb{P}[(\delta \neq \ell) \cap (\delta \neq \ell-1)] = \mathbb{P}[\delta \geq \ell+1] + \mathbb{P}[\delta \leq \ell-2]$$
$$= o(1); \tag{27}$$

from (24) and (26),

$$\mathbb{P}[\delta = \ell] = \mathbb{P}[\delta \geq \ell] - \mathbb{P}[\delta \geq \ell+1]$$
$$\sim e^{-\frac{e^{-\beta_n}}{(\ell-1)!}}$$
$$\to \begin{cases} e^{-\frac{e^{-\beta^*}}{(k-1)!}}, & \text{if } \lim_{n\to\infty}\beta_n = \beta^* \in (-\infty, \infty), \\ 1, & \text{if } \lim_{n\to\infty}\beta_n = \infty, \\ 0, & \text{if } \lim_{n\to\infty}\beta_n = -\infty; \end{cases} \tag{28}$$

and from (27) and (28),

$$\mathbb{P}[\delta = \ell-1]$$
$$= 1 - \mathbb{P}[(\delta \neq \ell) \cap (\delta \neq \ell-1)] - \mathbb{P}[\delta = \ell]$$
$$\to \begin{cases} 1 - e^{-\frac{e^{-\beta^*}}{(k-1)!}}, & \text{if } \lim_{n\to\infty}\beta_n = \beta^* \in (-\infty, \infty), \\ 0, & \text{if } \lim_{n\to\infty}\beta_n = \infty, \\ 1, & \text{if } \lim_{n\to\infty}\beta_n = -\infty. \end{cases} \tag{29}$$

Property (b) of Theorem 1 is established with (27-29). □

V. The Proof of Lemma 1

To start with, we consider several notation that will be used throughout. We recall that C_{ij} is the event that the communication channel between distinct nodes v_i and v_j is *on*. Then we set $\mathbf{1}[C_{ij}]$ as the indicator variable of event C_{ij} by

$$\mathbf{1}[C_{ij}] := \begin{cases} 1, \text{ if the channel between } v_i \text{ and } v_j \text{ is } \textit{on}; \\ 0, \text{ if the channel between } v_i \text{ and } v_j \text{ is } \textit{off}. \end{cases}$$

We denote by $\mathcal{C}_m$ a $\binom{m}{2}$-tuple consisting of all possible $\mathbf{1}[C_{ij}]$ with $1 \leq i < j \leq m$ as follows:

$$\mathcal{C}_m := (\mathbf{1}[C_{12}], , \ldots, \mathbf{1}[C_{1m}], \quad \mathbf{1}[C_{23}], , \ldots, \mathbf{1}[C_{2m}],$$
$$\mathbf{1}[C_{34}], \ldots, \mathbf{1}[C_{3m}], \quad \ldots, \quad \mathbf{1}[C_{(m-1),m}]).$$

Recalling S_i as the key set on node v_i, we define a m-tuple $\mathcal{T}_m$ through

$$\mathcal{T}_m := (S_1, S_2, \ldots, S_m).$$

Then we define $\mathcal{L}_m$ as

$$\mathcal{L}_m := (\mathcal{C}_m, \mathcal{T}_m).$$

With $\mathcal{L}_m$, we have the *on*/*off* states of all channels between nodes $v_1, v_2, \ldots, v_m$ and the key sets $S_1, S_2, \ldots, S_m$ on these m nodes, so all edges between these nodes in graph $\mathbb{G}_q$ are determined.

Let $\mathbb{C}_m, \mathbb{T}_m$ and $\mathbb{L}_m$ be the sets of all possible $\mathcal{C}_m, \mathcal{T}_m$ and $\mathcal{L}_m$, respectively. We define $\mathbb{L}_m^{(0)}$ such that $\big(\mathcal{L}_m \in \mathbb{L}_m^{(0)}\big)$ is the event that there is no edge between any two of nodes $v_1, v_2, \ldots, v_m$; i.e.,

$$\mathbb{L}_m^{(0)} := \{\mathcal{L}_m \mid (|S_i \cap S_j| < q) \text{ or } (\mathbf{1}[C_{ij}] = 0), \quad \forall i, j \text{ with } 1 \le i < j \le m.\}. \tag{30}$$

We define N_i as the neighborhood set of node v_i for $i = 1, 2, \ldots, m$, and define the node set $M_{j_1 j_2 \ldots j_m}$ for all $j_1, j_2, \ldots, j_m \in \{0, 1\}$ by

$$M_{j_1 j_2 \ldots j_m} := \left\{ w \;\middle|\; \begin{array}{l} w \in \mathcal{V} \setminus \{v_1, v_2, \ldots, v_m\}; \text{ and} \\ \text{for } i = 1, 2, \ldots, m, \begin{cases} w \in N_i \text{ if } j_i = 1; \\ w \notin N_i \text{ if } j_i = 0. \end{cases} \end{array} \right\}.$$

Clearly, the sets $M_{j_1 j_2 \ldots j_m}$ for $j_1, j_2, \ldots, j_m \in \{0, 1\}$ are mutually disjoint. Setting $\mathcal{V}_m := \{v_1, v_2, \ldots, v_m\}$ and $\overline{\mathcal{V}_m} := \mathcal{V} \setminus \mathcal{V}_m$, we obtain

$$\bigcup_{j_1, j_2, \ldots, j_m \in \{0,1\}} |M_{j_1 j_2 \ldots j_m}| = \overline{\mathcal{V}_m}, \tag{31}$$

and

$$\bigcup_{\substack{j_1, j_2, \ldots, j_m \in \{0,1\}: \\ \sum_{i=1}^m j_i \ge 1.}} |M_{j_1 j_2 \ldots j_m}| = \Big(\bigcup_{i=1}^m N_i \Big) \cap \overline{\mathcal{V}_m}. \tag{32}$$

We define 2^m-tuple $\mathcal{M}_m$ through[2]

$$\begin{aligned} \mathcal{M}_m &:= \big(|M_{j_1 j_2 \ldots j_m}| \mid j_1, j_2, \ldots, j_m \in \{0, 1\}\big) \\ &= \big(|M_{0^m}|, |M_{0^{m-1}1}|, |M_{0^{m-2}1,0}|, |M_{0^{m-2}1,1}|, \ldots\big). \end{aligned}$$

Let $\mathcal{E}$ be the event that each of $v_1, v_2, \ldots, v_m$ has a degree of h. Given $\mathcal{L}_m \in \mathbb{L}_m$, we define $\mathbb{M}_m(\mathcal{L}_m)$ as the set of $\mathcal{M}_m$ under the condition that $\mathcal{E}$ occurs. Then it's straightforward to compute $\mathbb{P}[\mathcal{E}]$ via

$$\mathbb{P}[\mathcal{E}] = \sum_{\substack{\mathcal{L}_m^* \in \mathbb{L}_m, \\ \mathcal{M}_m^* \in \mathbb{M}_m(\mathcal{L}_m^*).}} \mathbb{P}\big[\big(\mathcal{L}_m = \mathcal{L}_m^*\big) \cap \big(\mathcal{M}_m = \mathcal{M}_m^*\big)\big]. \tag{33}$$

Given that event $\mathcal{E}$ happens, if any two of nodes $v_1, v_2, \ldots, v_m$ do not have any common neighbor in $\overline{\mathcal{V}_m} = \mathcal{V} \setminus \{v_1, v_2, \ldots, v_m\}$, then $\mathcal{M}_m$ is determined and denoted by $\mathcal{M}_m^{(0)}$ which satisfies

$$\begin{cases} |M_{0^{i-1},1,0^{m-i}}| = h, & \text{for } i = 1, 2, \ldots, m; \\ |M_{j_1 j_2 \ldots j_m}| = 0, & \text{for } \sum_{i=1}^m j_i > 1; \\ |M_{0^m}| = n - m - hm. \end{cases}$$

By (33), we further write $\mathbb{P}[\mathcal{E}]$ as the sum of

$$\sum_{\substack{\mathcal{L}_m^* \in \mathbb{L}_m, \\ \mathcal{M}_m^* \in \mathbb{M}_m(\mathcal{L}_m^*): \\ \big(\mathcal{L}_m^* \notin \mathbb{L}_m^{(0)}\big) \\ \text{or } \big(\mathcal{M}_m^* \ne \mathcal{M}_m^{(0)}\big)}} \mathbb{P}\big[\big(\mathcal{L}_m = \mathcal{L}_m^*\big) \cap \big(\mathcal{M}_m = \mathcal{M}_m^*\big)\big] \tag{34}$$

and

$$\mathbb{P}\big[\big(\mathcal{L}_m \in \mathbb{L}_m^{(0)}\big) \cap \big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big)\big]. \tag{35}$$

Consequently, Lemma 1 holds after we prove the following Propositions 1 and 2. In the rest of the paper, we will often use $1 + x \le e^x$ for any $x \in \mathbb{R}$ and $1 - xy \le (1 - x)^y \le 1 - xy + \frac{1}{2}x^2y^2$ for $0 \le x < 1$ and $y = 0, 1, 2, \ldots$ (Fact 2 in [14]).

Proposition 1. *Given (4) (i.e., $p_{e,q} = \frac{\ln n \pm O(\ln \ln n)}{n}$), $K_n = \omega(1)$ and $\frac{{K_n}^2}{P_n} = o(1)$, we have*

$$(34) = o\left((h!)^{-m} (np_{e,q})^{hm} e^{-mnp_{e,q}}\right).$$

Proposition 2. *Given (4) (i.e., $p_{e,q} = \frac{\ln n \pm O(\ln \ln n)}{n}$), $K_n = \omega(1)$ and $\frac{{K_n}^2}{P_n} = o(1)$, we have*

$$(35) \sim (h!)^{-m} (np_{e,q})^{hm} e^{-mnp_{e,q}}.$$

VI. The Proof of Proposition 1

We embark on the evaluation of (34) by computing

$$\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^*\big) \mid \mathcal{L}_m = \mathcal{L}_m^*\big]. \tag{36}$$

With $\mathcal{C}_m^*$ and $\mathcal{T}_m^*$ defined such that $\mathcal{L}_m^* = (\mathcal{C}_m^*, \mathcal{T}_m^*)$, event $\big(\mathcal{L}_m = \mathcal{L}_m^*\big)$ is the union of events $\big(\mathcal{C}_m = \mathcal{C}_m^*\big)$ and $\big(\mathcal{T}_m = \mathcal{T}_m^*\big)$. Since $(\mathcal{C}_m = \mathcal{C}_m^*)$ and $(\mathcal{M}_m = \mathcal{M}_m^*)$ are independent, we obtain

$$(36) = \mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^*\big) \mid \big(\mathcal{T}_m = \mathcal{T}_m^*\big)\big].$$

For any $j_1, j_2, \ldots, j_m \in \{0, 1\}$, for any distinct nodes $w_1 \in \overline{\mathcal{V}_m}$ and $w_2 \in \overline{\mathcal{V}_m}$, events $(w_1 \in M_{j_1 j_2 \ldots j_m})$ and $(w_2 \in M_{j_1 j_2 \ldots j_m})$ are not independent [11], but are conditionally independent given $(\mathcal{T}_m = \mathcal{T}_m^*)$ (with the key sets $S_1, S_2, \ldots, S_m$ specified as $S_1^*, S_2^*, \ldots, S_m^*$, respectively). Therefore,

$$\begin{aligned} (36) = f(n - m, \mathcal{M}_m^*) &\mathbb{P}[w \in M_{0^m}^* \,|\, \mathcal{T}_m = \mathcal{T}_m^*]^{|M_{0^m}^*|} \times \\ &\prod_{\substack{j_1, j_2, \ldots, j_m \in \{0,1\}: \\ \sum_{i=1}^m j_i \ge 1.}} \mathbb{P}[w \in M_{j_1 j_2 \ldots j_m}^* \,|\, \mathcal{T}_m = \mathcal{T}_m^*]^{|M_{j_1 j_2 \ldots j_m}^*|}, \end{aligned} \tag{37}$$

where $f\big(\sum_{i=1}^\ell x_i, (x_1, x_2, \ldots, x_\ell)\big)$ for integers $\ell \ge 1$ and $x_i \ge 0$ with $i = 1, 2, \ldots, \ell$ is determined by

$$\begin{aligned} f\bigg(\sum_{i=1}^\ell x_i, (x_1, x_2, \ldots, x_\ell)\bigg) &:= \binom{\sum_{i=1}^\ell x_i}{x_1} \binom{\sum_{i=2}^\ell x_i}{x_2} \cdots \binom{\sum_{i=\ell-1}^\ell x_i}{x_{\ell-1}} \binom{x_\ell}{x_\ell} \\ &= \frac{\big(\sum_{i=1}^\ell x_i\big)!}{x_1! x_2! \ldots x_\ell!}. \end{aligned} \tag{38}$$

From (38) and

$$\sum_{j_1, j_2, \ldots, j_m \in \{0,1\}} |M_{j_1 j_2 \ldots j_m}^*| = n - m \tag{39}$$

[2]For a non-negative integer x, the term 0^x is short for $\underbrace{00\ldots0}_{\text{“}x\text{” number of “0”}}$.

which holds by (31), we have

$$\begin{aligned} & f(n-m, \mathcal{M}_m^*) \\ =& \frac{(\sum_{j_1,j_2,\ldots,j_m\in\{0,1\}} |M^*_{j_1j_2\ldots j_m}|)!}{\prod_{j_1,j_2,\ldots,j_m\in\{0,1\}}(|M^*_{j_1j_2\ldots j_m}|!)} \\ =& \frac{(n-m)!\Big/\Big(n-m-\sum_{\substack{j_1,j_2,\ldots,j_m\in\{0,1\}:\\ \sum_{i=1}^m j_i\geq 1.}} |M^*_{j_1j_2\ldots j_m}|\Big)!}{\prod_{\substack{j_1,j_2,\ldots,j_m\in\{0,1\}:\\ \sum_{i=1}^m j_i\geq 1.}}(|M^*_{j_1j_2\ldots j_m}|!)} \qquad (40) \\ \leq & n^{\sum_{\substack{j_1,j_2,\ldots,j_m\in\{0,1\}:\\ \sum_{i=1}^m j_i\geq 1.}} |M^*_{j_1j_2\ldots j_m}|}. \qquad (41) \end{aligned}$$

Denoting $\sum_{\substack{j_1,j_2,\ldots,j_m\in\{0,1\}:\\ \sum_{i=1}^m j_i\geq 1.}} |M^*_{j_1j_2\ldots j_m}|$ by Λ, we prove $\Lambda \leq hm-1$ below if $\big(\mathcal{L}_m^* \notin \mathbb{L}_m^{(0)}\big)$ or $\big(\mathcal{M}_m^* \neq \mathcal{M}_m^{(0)}\big)$.

On the one hand, assuming $\mathcal{L}_m^* \notin \mathbb{L}_m^{(0)}$, there exist i_1 and i_2 with $1 \leq i_1 < i_2 \leq m$ such that nodes v_{i_1} and v_{i_2} are neighbors with each other. Hence, $\{v_{i_1}, v_{i_2}\} \subseteq [(\bigcup_{i=1}^m N_i) \bigcap \mathcal{V}_m]$. Then from (32),

$$\Lambda = \left|\bigcup_{i=1}^m N_i\right| - \left|\left(\bigcup_{i=1}^m N_i\right) \cap \mathcal{V}_m\right| \leq hm-2.$$

On the other hand, assuming $\mathcal{M}_m^* \neq \mathcal{M}_m^{(0)}$, there exist i_3 and i_4 with $1 \leq i_3 < i_4 \leq m$ such that $N_{i_3} \cap N_{i_4} \neq \emptyset$. Then from (32),

$$\Lambda \leq \left|\bigcup_{i=1}^m N_i\right| \leq \left(\sum_{i=1}^m |N_i|\right) - |N_{i_3} \cap N_{i_4}| \leq hm-1.$$

To summarize, if $\big(\mathcal{L}_m^* \notin \mathbb{L}_m^{(0)}\big)$ or $\big(\mathcal{M}_m^* \neq \mathcal{M}_m^{(0)}\big)$, we have

$$\Lambda \leq hm-1, \qquad (42)$$

along with (39) leading to

$$|M^*_{0^m}| = n-m-\Lambda > n-m-hm. \qquad (43)$$

For any $j_1, j_2, \ldots, j_m \in \{0,1\}$ with $\sum_{i=1}^m j_i \geq 1$, there exists $t \in \{0,1,\ldots,m\}$ such that $j_t = 1$, so

$$\begin{aligned} & \mathbb{P}\big[w \in M_{j_1j_2\ldots j_m} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \\ & \leq \mathbb{P}[E_{wv_t} \mid \mathcal{T}_m = \mathcal{T}_m^*] = \mathbb{P}[E_{wv_t}] = p_{e,q}, \qquad (44) \end{aligned}$$

where E_{wv_t} is the event that there exists an edge between nodes w and v_t in graph $\mathbb{G}_q$.

Substituting (41-44) into (37), we obtain that if $\big(\mathcal{L}_m^* \notin \mathbb{L}_m^{(0)}\big)$ or $\big(\mathcal{M}_m^* \neq \mathcal{M}_m^{(0)}\big)$, then

$$(36) < (np_{e,q})^{hm-1} \times \mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm}. \qquad (45)$$

Applying (36) and (45) to (34),we get

$$\begin{aligned} (34) < & \sum_{\mathcal{L}_m^*\in\mathbb{L}_m} \Big\{|\mathbb{M}_m(\mathcal{L}_m^*)| \\ & \times \text{R.H.S. of (45)} \times \mathbb{P}\big[\mathcal{L}_m = \mathcal{L}_m^*\big]\Big\}. \qquad (46) \end{aligned}$$

To bound $|\mathbb{M}_m(\mathcal{L}_m^*)|$, note that $\mathcal{M}_m$ is a 2^m-tuple. Among the 2^m elements of the tuple, each of $|M_{j_1j_2\ldots j_m}|\big|_{\substack{j_1,j_2,\ldots,j_m\in\{0,1\}:\\ \sum_{i=1}^m j_i\geq 1.}}$ is at least 0 and at most h; and the remaining element $|M_{0^m}|$ can be determined by (39). Then it's straightforward that

$$|\mathbb{M}_m(\mathcal{L}_m^*)| \leq (h+1)^{2^m-1}. \qquad (47)$$

Using (47) in (46), and considering $\big(\mathcal{L}_m = \mathcal{L}_m^*\big)$ is the union of independent events $\big(\mathcal{T}_m = \mathcal{T}_m^*\big)$ and $\big(\mathcal{C}_m = \mathcal{C}_m^*\big)$, and $\sum_{\mathcal{C}_m^*\in\mathbb{C}_m} \mathbb{P}\big[\mathcal{C}_m = \mathcal{C}_m^*\big] = 1$, we derive

$$\begin{aligned} (34) < & (h+1)^{2^m-1}(np_{e,q})^{hm-1} \times \sum_{\mathcal{T}_m^*\in\mathbb{T}_m} \Big\{\mathbb{P}\big[\mathcal{T}_m = \mathcal{T}_m^*\big] \\ & \times \mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm}\Big\}. \qquad (48) \end{aligned}$$

From (48) and $\lim_{n\to\infty} np_{e,q} = \infty$ by (16), the proof of Proposition 1 is completed once we show

$$\begin{aligned} & \sum_{\mathcal{T}_m^*\in\mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*]\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm} \\ & \leq e^{-mnp_{e,q}} \cdot [1+o(1)]. \qquad (49) \end{aligned}$$

A. Establishing (49)

From (80) and (82) (viz., Lemma 3 in Appendix A), it holds that

$$\begin{aligned} & \mathbb{P}[w \in M^*_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm} \\ & = \mathbb{P}[w \in M^*_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n}\mathbb{P}[w \in M^*_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{-m-hm} \\ & \leq e^{-mnp_{e,q}+(q+2)!\binom{m}{2}n(p_{e,q})^{\frac{q+1}{q}}+\frac{np_{e,q}p_n}{K_n}\sum_{1\leq i<j\leq m}|S^*_{ij}|} \\ & \quad \times (1-mp_{e,q})^{-m-hm}, \qquad (50) \end{aligned}$$

where $S^*_{ij} = S^*_i \cap S^*_j$. With (16) (i.e., $p_{e,q} \sim \frac{\ln n}{n}$), we have $m^2np_{e,q}{}^2 = o(1)$ and $mp_{e,q} = o(1)$, which are substituted into (50) to induce (49) once we prove

$$\sum_{\mathcal{T}_m^*\in\mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*]e^{\frac{np_{e,q}p_n}{K_n}\sum_{1\leq i<j\leq m}|S^*_{ij}|} \leq 1+o(1). \qquad (51)$$

L.H.S. of (51) is denoted by $H_{n,m}$ and evaluated below. For each fixed and sufficiently large n, we consider: a) $p_n < n^{-\delta}(\ln n)^{-1}$ and b) $p_n \geq n^{-\delta}(\ln n)^{-1}$, where δ is an arbitrary constant with $0 < \delta < 1$.

a) $p_n < n^{-\delta}(\ln n)^{-1}$

From $p_n < n^{-\delta}(\ln n)^{-1}$, (17) (namely, $p_{e,q} \leq \frac{2\ln n}{n}$) and $|S^*_{ij}| \leq K_n$ for $1 \leq i < j \leq m$, it holds that

$$e^{\frac{np_{e,q}p_n}{K_n}\sum_{i=1}^{m-1}|S^*_{im}|} < e^{2\ln n\cdot n^{-\delta}(\ln n)^{-1}\cdot\binom{m}{2}} < e^{m^2n^{-\delta}},$$

which is substituted into $H_{n,m}$ to bring about

$$H_{n,m} < e^{m^2n^{-\delta}} \sum_{\mathcal{T}_m^*\in\mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*] = e^{m^2n^{-\delta}},$$

b) $p_n \geq n^{-\delta}(\ln n)^{-1}$

We relate $H_{n,m}$ to $H_{n,m-1}$ and assess $H_{n,m}$ iteratively. First, with $\mathcal{T}_m^* = (S_1^*, S_2^*, \ldots, S_m^*)$, event $(\mathcal{T}_m = \mathcal{T}_m^*)$ is

the intersection of independent events: $(\mathcal{T}_{m-1}=\mathcal{T}^*_{m-1})$ and $(S_m=S^*_m)$. Then we have

$$\begin{aligned}&H_{n,m}\\&=\sum_{\substack{\mathcal{T}^*_{m-1}\in\mathbb{T}_{m-1},\\ S^*_m\in\mathbb{S}_m}}\Big(\mathbb{P}[(\mathcal{T}_{m-1}=\mathcal{T}^*_{m-1})\cap(S_m=S^*_m)]\times\\&\qquad e^{\frac{np_{e,q}p_n}{K_n}\sum_{1\le i<j\le m-1}|S^*_{ij}|}e^{\frac{np_{e,q}p_n}{K_n}\sum_{i=1}^{m-1}|S^*_{im}|}\Big)\\&=H_{n,m-1}\cdot\sum_{S^*_m\in\mathbb{S}_m}\mathbb{P}[S_m=S^*_m]e^{\frac{np_{e,q}p_n}{K_n}\sum_{i=1}^{m-1}|S^*_{im}|}.\end{aligned}\tag{52}$$

By $\sum_{i=1}^{m-1}|S^*_{im}|=\sum_{i=1}^{m-1}|S^*_i\cap S^*_m|\le m\big|S^*_m\cap\big(\bigcup_{i=1}^{m-1}S^*_i\big)\big|$ and (17) (i.e., $p_{e,q}\le\frac{2\ln n}{n}$), we get

$$e^{\frac{np_{e,q}p_n}{K_n}\sum_{i=1}^{m-1}|S^*_{im}|}\le e^{\frac{2mp_n\ln n}{K_n}|S^*_m\cap(\bigcup_{i=1}^{m-1}S^*_i)|},$$

further leading to

$$\begin{aligned}&H_{n,m}/H_{n,m-1}\\&\le\sum_{u=0}^{K_n}\mathbb{P}\bigg[\bigg|S^*_m\bigcap\Big(\bigcup_{i=1}^{m-1}S^*_i\Big)\bigg|=u\bigg]e^{\frac{2ump_n\ln n}{K_n}}.\end{aligned}\tag{53}$$

Denoting $\big|\bigcup_{i=1}^{m-1}S^*_i\big|$ by v, then we obtain that for $u\in[\max\{0,K_n+v-P_n\},K_n]$,

$$\mathbb{P}\bigg[\bigg|S^*_m\bigcap\Big(\bigcup_{i=1}^{m-1}S^*_i\Big)\bigg|=u\bigg]=\frac{\binom{v}{u}\binom{P_n-v}{K_n-u}}{\binom{P_n}{K_n}},\tag{54}$$

which together with $K_n\le v\le mK_n$ yields

$$\begin{aligned}&\text{L.H.S. of (54)}\\&\le\frac{(mK_n)^u}{u!}\cdot\frac{(P_n-K_n)^{K_n-u}}{(K_n-u)!}\cdot\frac{K_n!}{(P_n-K_n)^{K_n}}\\&\le\frac{1}{u!}\bigg(\frac{mK_n{}^2}{P_n-K_n}\bigg)^u.\end{aligned}\tag{55}$$

For $u\notin[\max\{0,K_n+v-P_n\},K_n]$, L.H.S. of (54) equals 0. Then from (53) and (55),

$$\begin{aligned}\text{R.H.S. of (53)}&\le\sum_{u=0}^{K_n}\frac{1}{u!}\bigg(\frac{mK_n{}^2}{P_n-K_n}\cdot e^{\frac{2mp_n\ln n}{K_n}}\bigg)^u\\&\le e^{\frac{mK_n{}^2}{P_n-K_n}\cdot e^{\frac{2mp_n\ln n}{K_n}}}.\end{aligned}\tag{56}$$

By $\frac{K_n{}^2}{P_n}=o(1)$ and Lemma 2,

$$\frac{K_n{}^2}{P_n-K_n}\le\frac{K_n{}^2}{P_n}\cdot[1+o(1)]\le\big(q!p_{s,q}\big)^{\frac{1}{q}}\cdot[1+o(1)].\tag{57}$$

For n sufficiently large, from $p_n\ge n^{-\delta}(\ln n)^{-1}$ and (17) (i.e., $p_{e,q}=p_np_{s,q}\le\frac{2\ln n}{n}$), we have

$$p_{s,q}=p_n{}^{-1}p_{e,q}\le p_n{}^{-1}\cdot 2n^{-1}\ln n\le 2n^{\delta-1}(\ln n)^2.\tag{58}$$

From (57) and (58),

$$\begin{aligned}\frac{K_n{}^2}{P_n-K_n}&\le[q!\cdot 2n^{\delta-1}(\ln n)^2]^{\frac{1}{q}}\cdot[1+o(1)]\\&\le 3q\cdot n^{\frac{\delta-1}{q}}(\ln n)^{\frac{2}{q}}.\end{aligned}\tag{59}$$

Given $K_n=\omega(1)$, for arbitrary constant $c>q$ and for all n sufficiently large, $\frac{K_n}{p_n}\ge\frac{2cq\cdot m}{(c-q)(1-\delta)}$ holds. Then

$$e^{\frac{2mp_n\ln n}{K_n}}\le e^{\frac{(c-q)(1-\delta)}{cq}\ln n}=n^{\frac{(c-q)(1-\delta)}{cq}}.\tag{60}$$

The use of (56) (59) and (60) in (53) yields

$$\begin{aligned}&H_{n,m}/H_{n,m-1}\le\text{R.H.S. of (53)}\\&\le e^{3qm\cdot n^{\frac{\delta-1}{q}}(\ln n)^{\frac{2}{q}}\cdot n^{\frac{(c-q)(1-\delta)}{cq}}}\le\Big(e^{3q\cdot n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}\Big)^m.\end{aligned}\tag{61}$$

To derive $H_{n,m}$ iteratively based on (61), we compute $H_{n,2}$ below. By definition, setting $m=2$ in L.H.S. of (51) and considering the independence between events $(S_1=S^*_1)$ and $(S_2=S^*_2)$, we gain

$$H_{n,2}=\sum_{S^*_1\in\mathbb{S}_m}\mathbb{P}[S_1=S^*_1]\sum_{S^*_2\in\mathbb{S}_m}\mathbb{P}[S_2=S^*_2]e^{\frac{np_{e,q}p_n}{K_n}|S^*_1\cap S^*_2|}.\tag{62}$$

Clearly, $\sum_{S^*_2\in\mathbb{S}_m}\mathbb{P}[S_2=S^*_2]e^{\frac{np_{e,q}p_n}{K_n}|S^*_1\cap S^*_2|}$ equals R.H.S. of (53) with $m=2$. Then from (61) and (62),

$$H_{n,2}\le\sum_{S^*_1\in\mathbb{S}_m}\mathbb{P}[S_1=S^*_1]e^{6q\cdot n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}=e^{6q\cdot n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}.\tag{63}$$

Therefore, it holds via (61) and (63) that

$$\begin{aligned}H_{n,m}&\le\Big(e^{3q\cdot n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}\Big)^{m+(m-1)+\ldots+3}\cdot e^{6q\cdot n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}\\&=e^{\frac{3}{2}q(m^2+m-2)n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}.\end{aligned}$$

Finally, summarizing cases a) and b), we report

$$H_{n,m}\le\max\Big\{e^{m^2n^{-\delta}},e^{\frac{3}{2}q(m^2+m-2)n^{\frac{\delta-1}{c}}(\ln n)^{\frac{2}{q}}}\Big\}.$$

With $n\to\infty$, $H_{n,m}\le 1+o(1)$ (i.e., (51)) follows.

VII. The Proof of Proposition 2

We define $\mathcal{C}^{(0)}_m$ and $\mathbb{T}^{(0)}_m$ by

$$\mathcal{C}^{(0)}_m=(\underbrace{0,0,\ldots,0}_{\binom{m}{2}\text{ number of ``0''}}),$$

and

$$\mathbb{T}^{(0)}_m=\{\mathcal{T}_m\mid|S_i\cap S_j|<q,\ \forall i,j\text{ with }1\le i<j\le m.\}.$$

Clearly, $\big(\mathcal{C}_m=\mathcal{C}^{(0)}_m\big)$ or $\big(\mathcal{T}_m\in\mathbb{T}^{(0)}_m\big)$ each implies $\big(\mathcal{L}_m\in\mathbb{L}^{(0)}_m\big)$. Also, $\big(\mathcal{C}_m=\mathcal{C}^{(0)}_m\big)$ and $\big(\mathcal{M}_m=\mathcal{M}^{(0)}_m\big)$ are independent with each other. Therefore, with (35) $=\mathbb{P}\big[\big(\mathcal{L}_m\in\mathbb{L}^{(0)}_m\big)\cap\big(\mathcal{M}_m=\mathcal{M}^{(0)}_m\big)\big]$, we get

$$(35)\ge\mathbb{P}\big[\mathcal{C}_m=\mathcal{C}^{(0)}_m\big]\mathbb{P}\big[\mathcal{M}_m=\mathcal{M}^{(0)}_m\big],\tag{64}$$

and

$$(35)\ge\mathbb{P}\big[\mathcal{T}_m\in\mathbb{T}^{(0)}_m\big]\mathbb{P}\big[\big(\mathcal{M}_m=\mathcal{M}^{(0)}_m\big)\,\big|\,\big(\mathcal{T}_m\in\mathbb{T}^{(0)}_m\big)\big].\tag{65}$$

Given $\big(\mathcal{C}_m = \mathcal{C}_m^{(0)}\big) = \overline{\bigcup_{1\le i<j\le m} C_{ij}}$ and $\big(\mathcal{T}_m \in \mathbb{T}_m^{(0)}\big) = \overline{\bigcup_{1\le i<j\le m} \Gamma_{ij}}$, applying the union bound, we obtain

$$\mathbb{P}\big[\mathcal{C}_m = \mathcal{C}_m^{(0)}\big] \ge 1 - \sum_{1\le i<j\le m} \mathbb{P}[C_{ij}] \ge 1 - m^2 p_n/2, \quad (66)$$

and

$$\mathbb{P}\big[\mathcal{T}_m \in \mathbb{T}_m^{(0)}\big] \ge 1 - \sum_{1\le i<j\le m} \mathbb{P}[\Gamma_{ij}] \ge 1 - m^2 p_{s,q}/2. \quad (67)$$

In the following two subsections, we will prove

$$\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big] \sim (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}}, \quad (68)$$

and

$$\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \mid \big(\mathcal{T}_m \in \mathbb{T}_m^{(0)}\big)\big] \ge (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}} \cdot [1 - o(1)]. \quad (69)$$

Substituting (66) and (68) into (64), and applying (67) and (69) to (65), we have

$$\frac{(35)}{(h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}}} \ge (1 - \min\{p_{s,q}, p_n\} \cdot m^2/2) \cdot [1 - o(1)]. \quad (70)$$

From (68), we get

$$(35) \le \mathbb{P}\big[\mathcal{M}_m \in \mathbb{M}_m^{(0)}\big] \le (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}} \cdot [1 + o(1)]. \quad (71)$$

Combining (70) and (71), and using $\min\{p_{s,q}, p_n\} \le \sqrt{p_{s,q}p_n} = \sqrt{p_{e,q}} \le \sqrt{\frac{2\ln n}{n}} = o(1)$ which holds from $p_{e,q} = p_{s,q}p_n$ and (17), Proposition 2 follows. Below we detail the proofs of (68) and (69).

A. Establishing (68)

We have

$$\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big] \sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \Big\{\mathbb{P}\big[\mathcal{T}_m = \mathcal{T}_m^*\big]\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \mid \big(\mathcal{T}_m = \mathcal{T}_m^*\big)\big]\Big\},$$

where

$$\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \mid \big(\mathcal{T}_m = \mathcal{T}_m^*\big)\big] = f\big(n-m, \mathcal{M}_m^{(0)}\big)\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm} \times \prod_{i=1}^{m} \mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*]^h, \quad (72)$$

with function f specified in (38). From (40),

$$f\big(n-m, \mathcal{M}_m^{(0)}\big) = \frac{(n-m)!}{(n-m-hm)!(h!)^m} \sim (h!)^{-m} n^{hm}. \quad (73)$$

We will establish

$$\sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \Big\{\mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*] \prod_{i=1}^{m} \big\{\mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}}^{(0)} \,\big|\, \mathcal{T}_m = \mathcal{T}_m^*\big]^h\big\}\Big\} \ge {p_{e,q}}^{hm} \cdot [1 - o(1)]. \quad (74)$$

We use (73) and (74) as well as (80) (viz., Lemma 3 in Appendix A) in evaluating $\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big]$ above. Then

$$\begin{aligned}&\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big] \\ &\ge (h!)^{-m} n^{hm} \cdot [1 - o(1)] \cdot (1 - mp_{e,q})^n \times \\ &\sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*] \prod_{i=1}^{m} \big\{\mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} \,|\, \mathcal{T}_m = \mathcal{T}_m^*]^h\big\} \\ &\ge (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}} \cdot [1 - o(1)]. \end{aligned} \quad (75)$$

Substituting (49) (73) above and (81) in Lemma 3 into the computation of $\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big]$ yields

$$\begin{aligned}&\mathbb{P}\big[\mathcal{M}_m = \mathcal{M}_m^{(0)}\big] \\ &\le (h!)^{-m} n^{hm} {p_{e,q}}^{hm} \times [1 + o(1)] \times \\ &\sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*]\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm} \\ &\sim (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}}. \end{aligned} \quad (76)$$

Then (68) follows from (75) and (76). Namely, (68) holds upon the establishment of (74), which is proved below. First, from (83) in Lemma 3, with $\mathcal{T}_m^* = (S_1^*, S_2^*, \ldots, S_m^*)$ and $S_{ij}^* = S_i^* \cap S_j^*$, we get

$$\begin{aligned}&\prod_{i=1}^{m} \mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}}^{(0)} \mid \mathcal{T}_m = \mathcal{T}_m^*\big]^h \\ &\ge {p_{e,q}}^{hm} \prod_{i=1}^{m} \left[1 - \left((q+2)!m(p_{e,q})^{\frac{1}{q}} + \frac{p_n}{K_n} \sum_{j\in\{1,2,\ldots,m\}\setminus\{i\}} |S_{ij}^*|\right)\right]^h \\ &\ge {p_{e,q}}^{hm} \left(1 - (q+2)!hm^2(p_{e,q})^{\frac{1}{q}} - \frac{2hp_n}{K_n} \sum_{1\le i<j\le m} |S_{ij}^*|\right). \end{aligned}$$

With $p_{e,q} = o(1)$ by (16), we obtain (74) once proving

$$\frac{p_n}{K_n} \sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \left(\mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*] \sum_{1\le i<j\le m} |S_{ij}^*|\right) = o(1). \quad (77)$$

Clearly, $|S_{ij}^*| \le K_n$. If $\mathcal{T}_m^* \in \mathbb{T}_m^{(0)}$, it further holds that $|S_{ij}^*| < q$. Consequently, from (67), $K_n = \omega(1)$ and $p_n p_{s,q} = p_{e,q} \le \frac{2\ln n}{n}$, the proof of (77) becomes evident by

$$\begin{aligned}&\text{L.H.S. of (77)} \\ &\le \binom{m}{2} p_n \cdot \mathbb{P}[\mathcal{T}_m^* \in \mathbb{T}_m \setminus \mathbb{T}_m^{(0)}] + \frac{q}{K_n} \cdot p_n \cdot \mathbb{P}[\mathcal{T}_m^* \in \mathbb{T}_m^{(0)}] \\ &\le m^2/2 \cdot p_n \cdot m^2 p_{s,q}/2 + \frac{q}{K_n} \\ &\le m^4 n^{-1} \ln n/2 + o(1) \\ &\to 0, \text{ as } n \to \infty. \end{aligned}$$

B. Establishing (69)

We have

$$\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \cap \big(\mathcal{T}_m \in \mathbb{T}_m^{(0)}\big)\big] = \sum_{\mathcal{T}_m^* \in \mathbb{T}_m^{(0)}} \Big\{\mathbb{P}\big[\mathcal{T}_m = \mathcal{T}_m^*\big]\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \mid \big(\mathcal{T}_m = \mathcal{T}_m^*\big)\big]\Big\},$$

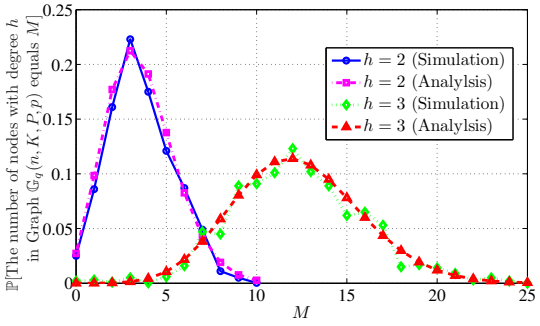

Fig. 1. A plot of the probability distribution for the number of nodes with degree h for $h = 2, 3$ in graph $\mathbb{G}_q(n, K, P, p)$ with $n = 2,000$, $q = 2$, $P = 10,000$, $K = 36$ and $p = 0.7$.

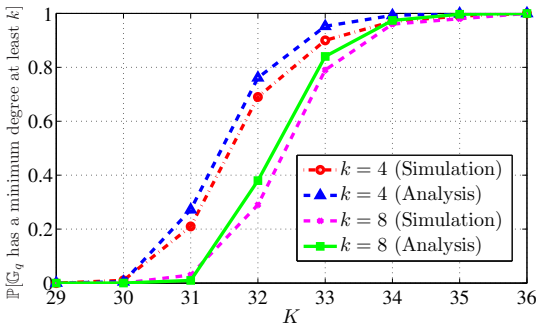

Fig. 2. A plot of the probability that graph $\mathbb{G}_q(n, K, P, p)$ has a minimum node degree at least k as a function of K for $k = 4$ and $k = 8$ with $q = 2$, $n = 2,000$, $P = 10,000$, and $p = 0.8$.

where $\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \mid \big(\mathcal{T}_m = \mathcal{T}_m^*\big)\big]$ as given by (72) equals

$$f\big(n-m, \mathcal{M}_m^{(0)}\big)\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*]^{n-m-hm} \times \prod_{i=1}^{m} \big\{\mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*]^h\big\}, \tag{78}$$

with $f\big(n-m, \mathcal{M}_m^{(0)}\big)$ computed in (73). For $\mathcal{T}_m^* \in \mathbb{T}_m^{(0)}$, from $|S_{ij}^*| < q$ and (83) in Lemma 3, we derive

$$\mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \geq p_{e,q}\left[1 - (q+2)!m(p_{e,q})^{\frac{1}{q}} - \frac{qp_n}{K_n}\right]. \tag{79}$$

Substituting (73) (79) above and (80) in Lemma 3 into (78), and using $p_{e,q} = o(1)$ and $K_n = \omega(1)$, we conclude that

$$\begin{aligned}\mathbb{P}\big[\big(\mathcal{M}_m = \mathcal{M}_m^{(0)}\big) \cap \big(\mathcal{T}_m \in \mathbb{T}_m^{(0)}\big)\big] &\geq \mathbb{P}[\mathcal{T}_m \in \mathbb{T}_m^{(0)}] \cdot (h!)^{-m} n^{hm} \cdot [1 - o(1)] \\ &\quad \times (1 - mp_{e,q})^{n-m-hm} {p_{e,q}}^{hm} \\ &\quad \times \left[1 - (q+2)!m(p_{e,q})^{\frac{1}{q}} - \frac{qp_n}{K_n}\right]^{hm} \\ &\sim (h!)^{-m}(np_{e,q})^{hm} e^{-mnp_{e,q}}.\end{aligned}$$

VIII. 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. In proving property (a) of Theorem 1, we establish that the number of nodes in $\mathbb{G}_q(n, K_n, P_n, p_n)$ with degree h approaches to a Poisson distribution with mean $\lambda_h = n(h!)^{-1}(np_{e,q})^h e^{-np_{e,q}}$ as $n \to \infty$. We derive λ_h by computing the corresponding probability of $p_{e,q}$ in $\mathbb{G}_q(n, K, P, p)$ through $p_{e,q} = p \cdot \sum_{u=q}^{K} \left[\binom{K}{u}\binom{P-K}{K-u}\Big/\binom{P}{K}\right]$ 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 $p_{e,q} = p \cdot \sum_{u=q}^{K} \left[\binom{K}{u}\binom{P-K}{K-u}\Big/\binom{P}{K}\right]$. Then we determine α_n by (9). 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.

IX. Results for Graph $\mathbb{G}_1$

For graph $\mathbb{G}_1$ (i.e., $\mathbb{G}_q$ in the special case of $q = 1$), we have derived asymptotically exact probabilities for k-connectivity

and the property that the minimum node degree is at least k with arbitrary k. Compared with Theorem 1 and Corollary 1 for $\mathbb{G}_q$, our results for $\mathbb{G}_1$ as presented in the following Theorem 2 does not need the condition $\frac{{K_n}^2}{P_n} = o(1)$, and only requires a weaker condition: $P_n \geq 3K_n$ for all n sufficiently large.

Theorem 2. *Consider a positive integer k and 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 $P_n \geq 3K_n$ for all n sufficiently large. Let the sequence α: $\mathbb{N}_0 \to \mathbb{R}$ be defined through*

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

For $\lim_{n\to\infty} \alpha_n = \alpha^* \in [-\infty, \infty]$, the properties (a) and (b) below hold.

(a) If $K_n = \omega(1)$, then as $n \to \infty$,

$$\mathbb{P}\left[\begin{array}{c}\textit{The minimum node degree}\\ \textit{of graph } \mathbb{G} \textit{ is at least } k.\end{array}\right] \to e^{-\frac{e^{-\alpha^*}}{(k-1)!}}.$$

(b) If $P_n = \Omega(n)$, then as $n \to \infty$,

$$\mathbb{P}\left[\textit{Graph } \mathbb{G} \textit{ is } k\textit{-connected.}\right] \to e^{-\frac{e^{-\alpha^*}}{(k-1)!}}.$$

We provide the proof of Theorem 2 in Appendix B.

Note that $p_{e,1}$ is $p_{e,q}$ with $q = 1$, and is the probability that two nodes have a link in between in graph $\mathbb{G}_1$. In establishing Theorem 2, as given within its proof in Appendix B, we have shown that the number of nodes with an arbitrary degree in graph $\mathbb{G}_1$ asymptotically converges to a Poisson distribution. Using the idea similar to that of proving property (b) of Theorem 1 in this paper, we also establish the asymptotic probability distribution for the minimum node degree and for the connectivity of graph $\mathbb{G}_1$. Therefore, we present the following theorem on graph $\mathbb{G}_1$, which is an analog of Theorem 1:

Theorem 3. *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 $P_n \geq 3K_n$ for all n sufficiently large. For*

$$p_{e,1} = \frac{\ln n \pm O(\ln\ln n)}{n},$$

(i.e., $\frac{np_{e,1} - \ln n}{\ln\ln n}$ is bounded for all n), the following properties (a) and (b) for graph $\mathbb{G}_1$ hold.

(a) *If $K_n = \omega(1)$, the number of nodes in $\mathbb{G}_1$ with an arbitrary degree converges to a Poisson distribution as $n \to \infty$.*

(b) *Defining ℓ and β_n by*

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

and

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

we obtain that if $K_n = \omega(1)$, with μ denoting the minimum node degree of graph $\mathbb{G}_1$,

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

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

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

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

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

$$\begin{cases}\mu = \ell - 1 \textit{ with a probability tending to } 1,\\ \mu \neq \ell - 1 \textit{ with a probability converging to } 0;\end{cases}$$

and that if $P_n = \Omega(n)$, with ν denoting the connectivity of graph $\mathbb{G}_1$,

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

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

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

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

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

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

X. Related Work

Erdős and Rényi [5] and Gilbert [8] 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 [5] 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 [6], 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) [12] 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 [14], [15]. As detailed in Section IX, we also derive asymptotically exact probabilities for k-connectivity and the event that the minimum degree no less than k for $\mathbb{G}_1$.

Krishnan *et al.* [9] and Krzywdziński and Rybarczyk [10] 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 [9], [10], [12], 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 [14] 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.

XI. 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 reaches at least k. This will extend our result on the asymptotically exact probability for k-connectivity in graph $\mathbb{G}_1$ (viz., Section IX) 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 [9], [10], [12].

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] A. DasGupta. *Asymptotic Theory of Statistics and Probability*, volume XVII. Springer Texts in Statistics, 2008.

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

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

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

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

[9] 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.

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

[11] K. Rybarczyk. Diameter, connectivity and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311, 2011.

[12] 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.

[13] 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.

[14] 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 .

[15] 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.

Appendix A

A. Additional Lemmas

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

Lemma 3. *In graph* $\mathbb{G}_q$*, for any* $\mathcal{T}_m^* = (S_1^*, S_2^*, \ldots, S_m^*) \in \mathbb{T}_m$ *and any node* $w \in \overline{\mathcal{V}_m}$*, we obtain*

$$\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*] \geq 1 - mp_{e,q}, \tag{80}$$

and for any $i = 1, 2, \ldots, m$*,*

$$\mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \leq p_{e,q}; \tag{81}$$

and if $\frac{{K_n}^2}{P_n} = o(1)$*, the following (82) and (83) hold:*

$$\begin{aligned}&\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\quad \leq e^{-mp_{e,q}+(q+2)!\binom{m}{2}(p_{e,q})^{\frac{q+1}{q}}+\frac{p_{e,q}p_n}{K_n}\sum_{1\leq i<j\leq m}|S_{ij}^*|},\end{aligned} \tag{82}$$

and for any $i = 1, 2, \ldots, m$*,*

$$\begin{aligned}&\mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \\ &\quad \geq p_{e,q}\left[1 - (q+2)!m(p_{e,q})^{\frac{1}{q}} - \frac{p_n}{K_n}\sum_{j\in\{1,2,\ldots,m\}\setminus\{i\}}|S_{ij}^*|\right],\end{aligned} \tag{83}$$

where $S_{ij}^* = S_i^* \cap S_j^*$*.*

Lemma 4. *In graph* $\mathbb{G}_q$*, if* $\frac{{K_n}^2}{P_n} = o(1)$*, then for any three distinct nodes* v_i, v_j *and* v_t *in graph* $\mathbb{G}$ *and for any* $u = 0, 1, \ldots, K_n$*, we obtain that with sufficiently large* n*,*

$$\begin{aligned}&\mathbb{P}[(\Gamma_{it} \cap \Gamma_{jt} \mid (|S_{ij}| = u)] \\ &\quad \leq \frac{p_{s,q}u}{K_n} + (q+2)! \cdot (p_{s,q})^{\frac{q+1}{q}}.\end{aligned}$$

B. The Proof of Lemma 2

We elaborate the proof Lemma 2 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 2 holds once we establish the following (84) and (85):

$$\mathbb{P}[|S_{ij}| = q] \sim (q!)^{-1}\big({K_n}^2/P_n\big)^q, \tag{84}$$

and

$$\mathbb{P}[|S_{ij}| = q] \sim \sum_{u=q}^{K_n} \mathbb{P}[|S_i \cap S_j| = u]. \tag{85}$$

We will first establish (84) 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 $u = 0, 1, \ldots, K_n$,

$$\mathbb{P}[|S_{ij}| = u] = \binom{K_n}{u}\binom{P_n - K_n}{K_n - u}\Big/\binom{P_n}{K_n}. \tag{86}$$

Setting u as q in (86), it is clear that

$$\mathbb{P}[|S_{ij}|=q] = \frac{1}{q!}\left[\frac{K_n!}{(K_n-q)!}\right]^2 \cdot \frac{(P_n-K_n)!}{(P_n-2K_n+q)!} \cdot \frac{(P_n-K_n)!}{P_n!}. \tag{87}$$

For the upper bound on $\mathbb{P}[|S_{ij}| = q]$, using (87) 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

$$\begin{aligned}
&\mathbb{P}[|S_{ij}| = q] \\
&\quad \leq (q!)^{-1} {K_n}^{2q} {P_n}^{K_n - q} (P_n - K_n)^{-K_n} \\
&\quad = (q!)^{-1}\big({K_n}^2/P_n\big)^q \big[1 + K_n/(P_n - K_n)\big]^{K_n} \\
&\quad \leq (q!)^{-1}\big({K_n}^2/P_n\big)^q e^{\frac{{K_n}^2}{P_n - K_n}} \\
&\quad \leq (q!)^{-1}\big({K_n}^2/P_n\big)^q \cdot [1 + o(1)].
\end{aligned} \tag{88}$$

For the part of finding the lower bound, we employ (87), $\frac{{K_n}^2}{P_n} = o(1)$ 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 [14]. 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,

$$\begin{aligned}
&\mathbb{P}[|S_{ij}| = q] \\
&\quad \geq (q!)^{-1}(K_n - q)^{2q}(P_n - 2K_n)^{K_n - q} {P_n}^{-K_n} \\
&\quad = (q!)^{-1}\big[(K_n - q)^2/(P_n - 2K_n)\big]^q \cdot \big(1 - 2K_n/P_n\big)^{K_n} \\
&\quad \sim (q!)^{-1}\big({K_n}^2/P_n\big)^q;
\end{aligned} \tag{89}$$

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 (84) follows from (88) and (89).

Below we focus on proving (85). From (86), 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 (85) 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 2 is completed with (84) and (85).

C. The Proof of Lemma 3

Event $(w \in M_{0^m})$ equals $\overline{\bigcup_{i=1}^m E_{wv_i}}$, where E_{wv_i} is the event that there exists an edge between nodes w and v_i in $\mathbb{G}$. Thus, by a union bound, L.H.S. of (80) is no less than $1 - \sum_{i=1}^m \mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] = 1 - mp_{e,q}$; and given Lemma 4, we establish (82) by

$$\begin{aligned}
&\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\
&\leq 1 - \sum_{i=1}^m \mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\
&\quad + \sum_{1 \leq i < j \leq m} \mathbb{P}[E_{wv_i} \cap E_{wv_j} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\
&\leq 1 - mp_{e,q} + {p_n}^2 \sum_{1 \leq i < j \leq m}\left[\frac{p_{s,q}}{K_n}|S_{ij}^*| + (q+2)!(p_{s,q})^{\frac{q+1}{q}}\right] \\
&\leq 1 - mp_{e,q} + (q+2)!\binom{m}{2}(p_{e,q})^{\frac{q+1}{q}} + \frac{p_{e,q}p_n}{K_n}\sum_{1 \leq i < j \leq m}|S_{ij}^*| \\
&\leq e^{-mp_{e,q} + (q+2)!\binom{m}{2}(p_{e,q})^{\frac{q+1}{q}} + \frac{p_{e,q}p_n}{K_n}\sum_{1 \leq i < j \leq m}|S_{ij}^*|},
\end{aligned} \tag{90}$$

Since event $w \in M^{(0)}_{0^{i-1},1,0^{m-i}}$ equals the intersection of E_{wv_i} and $\overline{\bigcup_{j \in \{1,2,\ldots,m\}\setminus\{i\}} E_{wv_j}}$, L.H.S. of (81) is at most $\mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] = \mathbb{P}[E_{wv_i}] = p_{e,q}$; and given Lemma 4, we obtain (83) by

$$\begin{aligned}
&\mathbb{P}\big[w \in M^{(0)}_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \\
&\geq \mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\
&\qquad - \sum_{j \in \{1,2,\ldots,m\}\setminus\{i\}} \mathbb{P}[E_{wv_i} \cap E_{wv_j} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\
&= p_{e,q} - \sum_{j \in \{1,2,\ldots,m\}\setminus\{i\}} {p_n}^2\left[\frac{p_{s,q}}{K_n}|S_{ij}^*| + (q+2)!(p_{s,q})^{\frac{q+1}{q}}\right] \\
&\geq p_{e,q}\left[1 - (q+2)!m(p_{e,q})^{\frac{1}{q}} - \frac{p_n}{K_n}\sum_{j \in \{1,2,\ldots,m\}\setminus\{i\}}|S_{ij}^*|\right].
\end{aligned}$$

D. The Proof of Lemma 4

To compute the probability of the event $\Gamma_{it} \cap \Gamma_{jt}$ which is equivalent to the event

$$(|S_t \cap S_i| \geq q) \bigcap (|S_t \cap S_j| \geq q),$$

we specify all the possible cardinalities of sets $S_t \cap (S_i \setminus S_j)$, $S_t \cap (S_j \setminus S_i)$, and $S_t \cap (S_i \cap S_j)$. We define event $F(a, b, d)$ as

Given event $(|S_i \cap S_j| = u)$, we define Λ as the set of all possible (a, b, d) with

$$\big[|S_t \cap (S_i \setminus S_j)| = a\big] \cap \big[|S_t \cap (S_j \setminus S_i)| = b\big] \cap [|S_t \cap (S_i \cap S_j)| = d]$$

such that $\Gamma_{it} \cap \Gamma_{jt}$ happens. Then,

$$\mathbb{P}\big[\Gamma_{it} \cap \Gamma_{jt} \mid \big(|S_i \cap S_j| = u\big)\big] = \sum_{(a,b,d)\in\Lambda} g(a, b, d). \quad (91)$$

where

$$\begin{aligned} &g(a, b, d) \\ &:= \mathbb{P}\Big[[|S_t \cap (S_i \setminus S_j)| = a] \cap [|S_t \cap (S_j \setminus S_i)| = b] \\ &\qquad \cap [|S_t \cap (S_i \cap S_j)| = d] \quad | \quad (|S_i \cap S_j| = u)\Big] \\ &= \frac{\binom{u}{d}\binom{K_n-u}{a}\binom{K_n-u}{b}\binom{P_n-2K_n+u}{K_n-a-b-d}}{\binom{P_n}{K_n}}. \end{aligned} \quad (92)$$

For integers x and y with $x \geq y \geq 0$, given $\binom{x}{y} = \frac{x!}{y!(x-y)!}$, it is easy to check by direct inspection that $\frac{(x-y)^y}{y!} \leq \binom{x}{y} \leq \frac{x^y}{y!}$. Then with $\frac{{K_n}^2}{P_n - K_n}$ denoted by γ for the brevity of notation, we get

$$\begin{aligned} &g(a, b, d) \\ &\leq \frac{u^d}{d!} \cdot \frac{(K_n - u)^a}{a!} \cdot \frac{(K_n - u)^b}{b!} \\ &\quad \times \frac{(P_n - 2K_n + u)^{K_n-a-b-d}}{(K_n - a - b - d)!} \cdot \frac{K_n!}{(P_n - K_n)^{K_n}} \\ &\leq \frac{1}{a!b!d!} u^d {K_n}^{2(a+b)+d} (P_n - K_n)^{-(a+b+d)} \\ &= \frac{1}{a!b!d!} \left(\frac{u}{K_n}\right)^d \gamma^{a+b+d}. \end{aligned} \quad (93)$$

We determine the set Λ as follows. First, it's clear that any (a, b, d) in Λ satisfies

$$\begin{aligned} &0 \leq a \leq |S_i \setminus S_j| = K_n - u, \\ &0 \leq b \leq |S_j \setminus S_i| = K_n - u, \\ &0 \leq d \leq u, \\ &a + b + d \leq |S_t| = K_n, \\ &a + d = |S_t \cap S_i| \geq q, \text{ and} \\ &b + d = |S_t \cap S_j| \geq q. \end{aligned}$$

Therefore, Λ is the set of all possible (a, b, d) with

$$\begin{aligned} &0 \leq d \leq u, \\ &\max\{0, q - d\} \leq a \leq K_n - u, \text{ and} \\ &\max\{0, q - d\} \leq b \leq \min\{K_n - u, K_n - a - d\}. \end{aligned}$$

Then it is straightforward to check

- if $q \leq u$, then $(0, 0, q) \in \Lambda$; and
- if $q > u$, then $(0, 0, q) \notin \Lambda$.

Hence, from (91),

$$\begin{aligned} &\mathbb{P}\big[\Gamma_{it} \cap \Gamma_{jt} \mid \big(|S_i \cap S_j| = u\big)\big] - \mathbf{1}[q \leq u] \cdot g(0, 0, q) \\ &= \sum_{(a,b,d)\in\Lambda\setminus\{(0,0,d)\}} g(a, b, d). \end{aligned} \quad (94)$$

We define Λ_1 as the set of all possible (a, b, d) satisfying

$$\begin{aligned} &d \geq 0, \\ &a \geq \max\{0, q - d\}, \text{ and} \\ &b \geq \max\{0, q - d\}, \end{aligned}$$

and define $\Lambda_2 := \Lambda_1 \setminus \{(0, 0, q)\}$. Clearly, $\Lambda \subseteq \Lambda_1$; and $\Lambda \setminus \{(0, 0, q)\} \subseteq \Lambda_2$. All (a, b, d) in Λ_2 can be divided into the following cases:

- $d = q, a \geq 1, b \geq 0$;
- $d > q, a \geq 0, b \geq 0$; and
- $d < q, a \geq q - d, b \geq q - d$.

From (93) (94) and $\Lambda \setminus \{(0, 0, d)\} \subseteq \Lambda_2$,

$$\begin{aligned} &\mathbb{P}\big[\Gamma_{it} \cap \Gamma_{jt} \mid \big(|S_i \cap S_j| = u\big)\big] - \mathbf{1}[q \leq u] \cdot g(0, 0, q) \\ &\leq \sum_{a,b,d:\ (a,b,d)\in\Lambda_2} \frac{1}{a!b!d!} \left(\frac{u}{K_n}\right)^d \gamma^{a+b+d} \\ &\leq \frac{1}{q!} \left(\frac{u\gamma}{K_n}\right)^q \sum_{a=1}^{\infty} \frac{\gamma^a}{a!} \sum_{b=0}^{\infty} \frac{\gamma^b}{b!} \\ &\quad + \sum_{d=q+1}^{\infty} \frac{1}{d!} \left(\frac{u\gamma}{K_n}\right)^d \sum_{a=0}^{\infty} \frac{\gamma^a}{a!} \sum_{b=0}^{\infty} \frac{\gamma^b}{b!} \\ &\quad + \sum_{d=0}^{q-1} \frac{1}{d!} \left(\frac{u\gamma}{K_n}\right)^d \sum_{a=q-d}^{\infty} \frac{\gamma^a}{a!} \sum_{b=q-d}^{\infty} \frac{\gamma^b}{b!}. \end{aligned} \quad (95)$$

From $\frac{{K_n}^2}{P_n} = o(1)$, we have $P_n = \omega(K_n)$ and further obtain

$$\gamma = \frac{{K_n}^2}{P_n - K_n} \sim \frac{{K_n}^2}{P_n} = o(1). \quad (96)$$

For any non-negative integer ϕ, by $\gamma = o(1)$ in (96),

$$\begin{aligned} \sum_{t=\phi}^{\infty} \frac{\gamma^t}{t!} &= \gamma^\phi \sum_{\tau=0}^{\infty} \frac{\gamma^\tau}{(\tau + \phi)!} \quad \text{(by setting } \tau = t - \phi) \\ &\leq \gamma^\phi \sum_{\tau=0}^{\infty} \frac{1}{\tau!\phi!} \gamma^\tau = \frac{\gamma^\phi}{\phi!} \cdot e^\gamma \leq \frac{\gamma^\phi}{\phi!} \cdot [1 + o(1)]. \end{aligned} \quad (97)$$

Applying (97) to (95),

$$\begin{aligned} &\mathbb{P}\big[\Gamma_{it} \cap \Gamma_{jt} \mid \big(|S_i \cap S_j| = u\big)\big] - \mathbf{1}[q \leq u] \cdot g(0, 0, q) \\ &\leq \frac{1}{q!} \left(\frac{u\gamma}{K_n}\right)^q \gamma \cdot [1 + o(1)] + \frac{\gamma^{q+1}}{(q+1)!} \cdot [1 + o(1)] \\ &\quad + \sum_{d=0}^{q-1} \frac{1}{d!} \left(\frac{u\gamma}{K_n}\right)^d \frac{\gamma^{2(q-d)}}{[(q-d)!]^2} \cdot [1 + o(1)]. \end{aligned} \quad (98)$$

To bound the last term in (98), we have

$$\sum_{d=0}^{q-1} \frac{1}{d!}\left(\frac{u\gamma}{K_n}\right)^d \frac{\gamma^{2(q-d)}}{[(q-d)!]^2} \le \sum_{d=0}^{q-1} \gamma^{2(q-d)} \le \sum_{d=0}^{q-1} \gamma^{q+1} = q\gamma^{q+1} \tag{99}$$

Then using (99) in (98),

$$\begin{aligned}
&\mathbb{P}\big[\Gamma_{it} \cap \Gamma_{jt} \mid \big(|S_i \cap S_j| = u\big)\big] - \mathbf{1}[q \le u] \cdot g(0,0,q) \\
&\le \frac{\gamma^{q+1}}{q!} \cdot [1 + o(1)] + \frac{\gamma^{q+1}}{(q+1)!} \cdot [1 + o(1)] \\
&\quad + q\gamma^{q+1} \cdot [1 + o(1)] \\
&\le \left[q + \frac{1}{q!} + \frac{1}{(q+1)!}\right]\gamma^{q+1} \cdot [1 + o(1)] \\
&\le (q+2)\gamma^{q+1}.
\end{aligned} \tag{100}$$

From Lemma 2 and $\gamma \sim \frac{{K_n}^2}{P_n}$ established in (96),

$$p_{s,q} \sim \frac{1}{q!}\left(\frac{{K_n}^2}{P_n}\right)^q \sim \frac{\gamma^q}{q!}.$$

Hence, for any constant $c > 1$, for sufficiently large n,

$$\frac{\gamma^q}{q!} \le c p_{s,q}$$

Then by setting $1 < c \le \big(\frac{q+1}{q}\big)^{\frac{q}{q+1}}$, for sufficiently large n, we obtain

$$\begin{aligned}
(q+2)\gamma^{q+1} &\le (q+2)\big(cp_{s,q} \cdot q!\big)^{\frac{q+1}{q}} \\
&= (q+2)c^{\frac{q+1}{q}}(q!)^{\frac{q+1}{q}}\big(p_{s,q}\big)^{\frac{q+1}{q}} \\
&\le (q+2) \cdot (q+1)/q \cdot (q!) \cdot q \cdot \big(p_{s,q}\big)^{\frac{q+1}{q}} \\
&= (q+2)! \cdot \big(p_{s,q}\big)^{\frac{q+1}{q}}
\end{aligned} \tag{101}$$

Now we evaluate $g(0,0,q)$. From (92), it holds that

$$g(0,0,q) = \frac{\binom{u}{q}\binom{P_n - 2K_n + u}{K_n - q}}{\binom{P_n}{K_n}}.$$

Then with

$$\mathbb{P}[|S_i \cap S_j| = q] = \frac{\binom{K_n}{q}\binom{P_n - K_n}{K_n - q}}{\binom{P_n}{K_n}},$$

we further obtain

$$\begin{aligned}
&\frac{g(0,0,q)}{\mathbb{P}[|S_i \cap S_j| = q]} \\
&= \frac{\binom{u}{q}\binom{P_n - 2K_n + u}{K_n - q}}{\binom{K_n}{q}\binom{P_n - K_n}{K_n - q}} \\
&= \frac{\frac{\prod_{i=0}^{q-1}(u-i)}{q!} \cdot \frac{\prod_{i=0}^{K_n-q-1}(P_n - 2K_n + u - i)}{(K_n - q)!}}{\frac{\prod_{i=0}^{q-1}(K_n - i)}{q!} \cdot \frac{\prod_{i=0}^{K_n-q-1}(P_n - K_n - i)}{(K_n - q)!}} \\
&= \left(\prod_{i=0}^{q-1} \frac{u-i}{K_n - i}\right)\left(\prod_{i=0}^{q-1} \frac{P_n - 2K_n + u - i}{P_n - K_n - i}\right) \\
&= \left[\prod_{i=0}^{q-1}\left(\frac{u}{K_n} - \frac{i(K_n - u)}{K_n(K_n - i)}\right)\right]\left[\prod_{i=0}^{q-1}\left(1 - \frac{K_n - u}{P_n - K_n - i}\right)\right] \\
&\le \left(\frac{u}{K_n}\right)^q.
\end{aligned} \tag{102}$$

From (102) and $p_{s,q} = \sum_{u=q}^{K_n} \mathbb{P}[|S_i \cap S_j| = u]$ by definition of $p_{s,q}$, we have

$$g(0,0,q) \le \left(\frac{u}{K_n}\right)^q \cdot p_{s,q} \le \frac{u}{K_n} \cdot p_{s,q}. \tag{103}$$

The proof of Lemma 4 is completed by the substitution of (101) and (103) into (100).

APPENDIX B
ESTABLISHING THEOREM 2 FOR GRAPH $\mathbb{G}_1$

A. Proving Property (a) of Theorem 2

In view of Corollary 1 and Theorem 2, property (a) of Theorem 2 will be proved if we show condition $\frac{{K_n}^2}{P_n} = o(1)$ for graph $\mathbb{G}_q$ in Corollary 1 can be substituted by a weaker condition: $P_n \ge 3K_n$ for all n sufficiently large, when q is set as 1 (i.e., graph $\mathbb{G}_q$ becomes $\mathbb{G}_1$). Recall that Corollary 1 is proved by Theorem 1. We check the proofs of Corollary 1 and Theorem 1, and identify the following places where $\frac{{K_n}^2}{P_n} = o(1)$ is used:

(i) (57)–(63) with $p_n \ge n^{-\delta}(\ln n)^{-1}$ and $0 < \delta < 1$ to demonstrate $H_{n,m} \le 1 + o(1)$, where condition $p_n \ge n^{-\delta}(\ln n)^{-1}$ is an assumption to discuss case b) in establishing (49) as case a) therein deals with $p_n < n^{-\delta}(\ln n)^{-1}$; and $H_{n,m}$ means L.H.S. of (51) and is also given in (106) below for clarity.

(ii) (82) and (83) in Lemma 3 proved by the help of Lemma 4, which is further shown based on Lemma 2.

First, for (i), we will prove $H_{n,m} \le 1 + o(1)$ is still true for $\mathbb{G}_1$ with $P_n \ge 3K_n$ for all n sufficiently large, instead of $\frac{{K_n}^2}{P_n} = o(1)$. The proof process starts with (53) and (56) which still hold for $\mathbb{G}_1$; i.e., we have

$$H_{n,m}/H_{n,m-1} \le \sum_{u=0}^{K_n} \mathbb{P}\left[\left|S_m^* \bigcap \left(\bigcup_{i=1}^{m-1} S_i^*\right)\right| = u\right] e^{\frac{2ump_n \ln n}{K_n}} \tag{104}$$

$$\le e^{\frac{m{K_n}^2}{P_n - K_n}} \cdot e^{\frac{2mp_n \ln n}{K_n}}, \tag{105}$$

where

$$H_{n,m} = \sum_{\mathcal{T}_m^* \in \mathbb{T}_m} \mathbb{P}[\mathcal{T}_m = \mathcal{T}_m^*] e^{\frac{np_{e,1}p_n}{K_n} \sum_{1 \le i < j \le m} |S_{ij}^*|}. \quad (106)$$

By Fact 5 in [14],

$$p_{s,1} \ge 1 - \left(1 - K_n/P_n\right)^{K_n} \ge 1 - e^{-{K_n}^2/P_n}. \quad (107)$$

For n sufficiently large, from $p_n \ge n^{-\delta}(\ln n)^{-1}$ (this holds as discussed above) and $p_{e,1} = p_n p_{s,1} \le \frac{2 \ln n}{n}$, we have

$$p_{s,1} = {p_n}^{-1} p_{e,1} \le {p_n}^{-1} \cdot 2n^{-1} \ln n \le 2n^{\delta - 1} (\ln n)^2. \quad (108)$$

Hence, for n sufficiently large, we apply (107) (108) and $P_n \ge 3K_n > 2K_n$ to produce

$$\begin{aligned} &{K_n}^2/(P_n - K_n) < 2{K_n}^2/P_n \le -2\ln(1 - p_{s,1}) \\ &\le -2\ln(1 - 2n^{\delta-1}(\ln n)^2) \le 2\sqrt{2} n^{\frac{\delta-1}{2}} \ln n. \end{aligned} \quad (109)$$

Given $K_n = \omega(1)$, for arbitrary constant $c > 2$ and for all n sufficiently large, $\frac{K_n}{p_n} \ge \frac{4c \cdot m}{(c-2)(1-\delta)}$ holds. Then

$$e^{\frac{2mp_n \ln n}{K_n}} \le e^{\frac{(c-2)(1-\delta)}{2c} \ln n} = n^{\frac{(c-2)(1-\delta)}{2c}}. \quad (110)$$

The use of (105) (109) and (110) in (105) yields

$$\begin{aligned} &H_{n,m}/H_{n,m-1} \\ &\le e^{2\sqrt{2} m n^{\frac{\delta-1}{2}} \cdot n^{\frac{(c-2)(1-\delta)}{2c}} \cdot \ln n} \le \left(e^{3n^{\frac{\delta-1}{c}} \ln n}\right)^m. \end{aligned} \quad (111)$$

To derive $H_{n,m}$ iteratively based on (111), we compute $H_{n,2}$ below. By definition, setting $m = 2$ in L.H.S. of (106) and considering the independence between events $(S_1 = S_1^*)$ and $(S_2 = S_2^*)$, we gain

$$H_{n,2} = \sum_{S_1^* \in \mathbb{S}_m} \mathbb{P}[S_1 = S_1^*] \sum_{S_2^* \in \mathbb{S}_m} \mathbb{P}[S_2 = S_2^*] e^{\frac{np_{e,1}p_n}{K_n} |S_1^* \cap S_2^*|}. \quad (112)$$

Clearly, $\sum_{S_2^* \in \mathbb{S}_m} \mathbb{P}[S_2 = S_2^*] e^{\frac{np_{e,1}p_n}{K_n} |S_1^* \cap S_2^*|}$ equals R.H.S. of (104) with $m = 2$. Then from (111) and (112),

$$H_{n,2} \le \sum_{S_1^* \in \mathbb{S}_m} \mathbb{P}[S_1 = S_1^*] e^{6n^{\frac{\delta-1}{c}} \ln n} = e^{6n^{\frac{\delta-1}{c}} \ln n}. \quad (113)$$

Therefore, it holds via (111) and (113) that

$$\begin{aligned} H_{n,m} &\le \left(e^{3n^{\frac{\delta-1}{c}} \ln n}\right)^{m+(m-1)+\ldots+3} \cdot e^{6n^{\frac{\delta-1}{c}} \ln n} \\ &= e^{\frac{3}{2}(m^2+m-2) n^{\frac{\delta-1}{c}} \ln n}. \end{aligned}$$

Finally, summarizing cases a) and b), we report

$$H_{n,m} \le \max\left\{e^{m^2 n^{-\delta}}, e^{\frac{3}{2}(m^2+m-2) n^{\frac{\delta-1}{c}} \ln n}\right\}.$$

With $n \to \infty$, $H_{n,m} \le 1 + o(1)$ (i.e., (106)) follows.

Second, for (ii), we will prove that (82) and (83) in Lemma 3 still hold for $\mathbb{G}_1$ with $P_n \ge 3K_n$ for all n sufficiently large, instead of $\frac{{K_n}^2}{P_n} = o(1)$ (the other two inequalities (80) and (81) in Lemma 3 are clearly still true for $\mathbb{G}_1$ without any changes to the proofs as they do not require $\frac{{K_n}^2}{P_n} = o(1)$).

We will prove the following lemma in which the two inequalities (114) and (115) imply (82) with $q = 1$, and (83) with $q = 1$, respectively.

Lemma 5. *Given $P_n \ge 3K_n$ and any $\mathcal{T}_m^* = (S_1^*, S_2^*, \ldots, S_m^*) \in \mathbb{T}_m$, for any node $w \in \mathcal{V}_m$, we obtain*

$$\begin{aligned} &\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\quad \le e^{-mp_{e,1} + m^2 {p_{e,1}}^2 + {K_n}^{-1} p_{e,1} p_n \sum_{1 \le i < j \le m} |S_{ij}^*|}; \end{aligned} \quad (114)$$

and for any $i = 1, 2, \ldots, m$,

$$\begin{aligned} &\mathbb{P}\big[w \in M_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \\ &\ge p_{e,1}\left(1 - 2mp_{e,1} - {K_n}^{-1} p_n \sum_{j \in \{1,2,\ldots,m\} \setminus \{i\}} |S_{ij}^*|\right), \end{aligned} \quad (115)$$

where $S_{ij}^* = S_i^* \cap S_j^*$.

To demonstrate Lemma 5, we will prove the following Lemma 6, which is an analog of Lemma 4.

Lemma 6. *If $P_n \ge 3K_n$, then for any three distinct nodes v_i, v_j and v_t in graph $\mathbb{G}_1$ and for any $u = 0, 1, \ldots, K_n$, we have*

$$\mathbb{P}[(\Gamma_{it} \cap \Gamma_{jt} \mid (|S_{ij}| = u)] \le {K_n}^{-1} p_{s,1} u + 2{p_{s,1}}^2.$$

The Proof of Lemma 5:

Event $(w \in M_{0^m})$ equals $\overline{\bigcup_{i=1}^m E_{wv_i}}$, where E_{wv_i} is the event that there exists an edge between nodes w and v_i in graph $\mathbb{G}_1$. Thus, given Lemma 3, we establish (114) by

$$\begin{aligned} &\mathbb{P}[w \in M_{0^m} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\le 1 - \sum_{i=1}^m \mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\quad + \sum_{1 \le i < j \le m} \mathbb{P}[E_{wv_i} \cap E_{wv_j} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\le 1 - mp_{e,1} + {p_n}^2 \sum_{1 \le i < j \le m} \left({K_n}^{-1} p_{s,1} |S_{ij}^*| + 2{p_{s,1}}^2\right) \\ &\le e^{-mp_{e,1} + m^2 {p_{e,1}}^2 + {K_n}^{-1} p_{e,1} p_n \sum_{1 \le i < j \le m} |S_{ij}^*|}. \end{aligned}$$

Since event $w \in M^{(0)}_{0^{i-1},1,0^{m-i}}$ equals the intersection of E_{wv_i} and $\overline{\bigcup_{j \in \{1,2,\ldots,m\} \setminus \{i\}} E_{wv_j}}$, given Lemma 6, we obtain (115) by

$$\begin{aligned} &\mathbb{P}\big[w \in M^{(0)}_{0^{i-1},1,0^{m-i}} \mid \mathcal{T}_m = \mathcal{T}_m^*\big] \\ &\ge \mathbb{P}[E_{wv_i} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &\qquad - \sum_{j \in \{1,2,\ldots,m\} \setminus \{i\}} \mathbb{P}[E_{wv_i} \cap E_{wv_j} \mid \mathcal{T}_m = \mathcal{T}_m^*] \\ &= p_{e,1} - \sum_{j \in \{1,2,\ldots,m\} \setminus \{i\}} {p_n}^2 \big({K_n}^{-1} p_{s,1} |S_{ij}^*| + 2{p_{s,1}}^2\big) \\ &\ge p_{e,1}\left(1 - 2mp_{e,1} - {K_n}^{-1} p_n \sum_{j \in \{1,2,\ldots,m\} \setminus \{i\}} |S_{ij}^*|\right). \end{aligned}$$

The Proof of Lemma 6:

$$
\begin{aligned}
&\mathbb{P}[\Gamma_{it} \cap \Gamma_{jt} \mid (|S_{ij}| = u)] \\
&= \mathbb{P}[\Gamma_{it} \mid (|S_{ij}| = u)] + \mathbb{P}[\Gamma_{jt} \mid (|S_{ij}| = u)] \\
&\quad - (1 - \mathbb{P}[\overline{\Gamma_{it}} \cap \overline{\Gamma_{jt}} \mid (|S_{ij}| = u)]) \\
&= 2p_{s,1} - 1 + \binom{P_n - (2K_n - u)}{K_n} \Big/ \binom{P_n}{K_n} \\
&\leq 2p_{s,1} - 1 + (1 - p_{s,1})^{\frac{2K_n - u}{K_n}} \text{ (by Lemma 5.1 in [12])} \\
&\leq 2p_{s,1} - p_{s,1}(2K_n - u)/K_n + {p_{s,1}}^2 \big[(2K_n - u)/K_n\big]^2/2 \\
&\leq {K_n}^{-1} p_{s,1} u + 2{p_{s,1}}^2.
\end{aligned}
$$

B. Proving Property (b) of Theorem 2

With η and ζ being the connectivity and the minimum node degree of graph $\mathbb{G}_1$, the connectivity η is at most the minimum node degree ζ since each node in a η-connected graph has a degree at least η. Then

$$\mathbb{P}[\eta \geq k] = \mathbb{P}[\zeta \geq k] - \mathbb{P}[(\eta < k) \cap (\zeta \geq k)].$$

Therefore, in view that property (a) of Theorem 2 has been established, the proof of property (b) of Theorem 2 is completed given $\mathbb{P}[(\eta < k) \cap (\zeta \geq k)] = o(1)$, which follows via

$$\mathbb{P}[(\eta < k) \cap (\zeta \geq k)] \leq \sum_{h=0}^{k-1} \mathbb{P}[(\eta = h) \cap (\zeta > h)],$$

if under $P_n \geq 3K_n$ for all n sufficiently large, $P_n = \Omega(n)$ and $p_{e,1} = \frac{\ln n + (k-1)\ln\ln n + \alpha_n}{n}$, for $h = 0, 1, \ldots, k-1$, we show

$$\mathbb{P}[(\eta = h) \cap (\zeta > h)] = o(1). \tag{116}$$

(116) has a proof almost the same as that of Equation (128) in [14]. We visit the relevant steps of establishing the latter therein and remove unnecessary conditions to establish the former. The details are omitted here since the proofs are very similar.