Topological Properties of Secure Wireless Sensor Networks Under the \( q \)-Composite Key Predistribution Scheme With Unreliable Links

Jun Zhao, Member, IEEE

Abstract—Security is an important issue in wireless sensor networks (WSNs), which are often deployed in hostile environments. The \( q \)-composite key predistribution scheme has been recognized as a suitable approach to secure WSNs. Although the \( q \)-composite scheme has received much attention in the literature, there is still a lack of rigorous analysis for secure WSNs operating under the \( q \)-composite scheme in consideration of the unreliability of links. One main difficulty lies in analyzing the network topology, whose links are not independent. Wireless links can be unreliable in practice due to the presence of physical barriers between sensors or because of harsh environmental conditions severely impairing communications. In this paper, we resolve the difficult challenge and investigate topological properties related to node degree in WSNs operating under the \( q \)-composite scheme with unreliable communication links modeled as independent ON/OFF channels. Specifically, we derive the asymptotically exact probability for the property of minimum degree being at least \( k \), present the asymptotic probability distribution for the minimum degree, and demonstrate that the number of nodes with a fixed degree is in distribution asymptotically equivalent to a Poisson random variable. We further use the theoretical results to provide useful design guidelines for secure WSNs. Experimental results also confirm the validity of our analytical findings.

Index Terms—Security, key predistribution, wireless sensor networks, random graphs, topological properties.

I. INTRODUCTION

WIRELESS sensor networks (WSNs) enable a broad range of applications including military surveillance, home automation, and patient monitoring [1]. In many scenarios, since WSNs are deployed in adversarial environments, security becomes an important issue. To this end, key predistribution has been recognized as a typical solution to secure WSNs [2]. The idea is to randomly assign cryptographic keys to sensors before network deployment.

Various key predistribution schemes have been studied in the literature [1]–[13].

The \( q \)-composite key predistribution scheme proposed by Chan et al. [1] as an extension of the Eschenauer-Gligor scheme [2] (the \( q \)-composite scheme in the case of \( q = 1 \)) has received much interest [10]–[17] 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 [1] 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 [3], [5] and the requirement that the distance between two sensors should be close enough for communication [16].

Communication links between sensor nodes may not be available due to the presence of physical barriers between nodes or because of harsh environmental conditions severely impairing transmission. To represent unreliable links, we use the ON/OFF channel model where each link is either on (i.e., active) with probability \( p_n \) or off (i.e., inactive) with probability \( 1 - p_n \), where \( p_n \) is a function of \( n \) for generality.

In addition to link failure, sensor nodes are also prone to failure in WSNs deployed in hostile environments. To ensure reliability against the failure of sensors, we study the property of minimum degree being at least \( k \) so that each sensor is directly connected to at least \( k \) other sensors. This means that a sensor may still be connected to a sufficient number of sensors even if some neighbors fail. Note that 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. Another related graph property is \( k \)-connectivity, which is stronger than the property of minimum degree being at least \( k \). A network (or a graph) is said to be \( k \)-connected if it remains connected despite the deletion of any \((k - 1)\) nodes [18], [19]; a network is simply deemed connected if it is 1-connected. Hence, \( k \)-connectivity provides a guarantee of...
network reliability against the failure of \((k - 1)\) sensors due to adversarial attacks, battery depletion, harsh environmental conditions, etc.

In view of the above, we investigate topological properties related to node degree in WSNs employing the \(q\)-composite key predistribution scheme under the on/off channel model as the physical link constraint comprising independent channels which are either on or off. Specifically, we derive the asymptotically exact probabilities for the property of minimum degree being at least \(k\), establish the asymptotic probability distribution for the minimum degree, and show that the number of nodes with a fixed degree is in distribution asymptotically equivalent to a Poisson random variable. Our results are useful for designing secure WSNs under link and node failure.

We summarize our contributions in the following two subsections. We first present our results on node degree for a secure WSN employing the \(q\)-composite key predistribution scheme under the on/off channel model. Then we use the results to provide useful design guidelines for secure WSNs.

A. Results

For \(G_q\) denoting a secure sensor network with the \(q\)-composite key predistribution scheme under the on/off channel model, we present several results related to node degree, by considering the conditions on \(p_{e,q}\), which denotes the probability of a secure link between two sensors. The secure link probability \(p_{e,q}\) is given by

\[
p_{e,q} = p_n \left( 1 - \sum_{u=0}^{q-1} \frac{\binom{Kn}{u} \binom{Kn-h}{Kn-u}}{\binom{Kn}{Kn}} \right),
\]

as shown in Equation (8) on Page 1791 later.

For the network \(G_q\), we now present the results, which are further elaborated in Section III-A.

- First, we derive the asymptotically exact probabilities for the property of minimum degree being at least \(k\). Specifically, if \(p_{e,q} = \frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}\) for a constant integer \(k \geq 1\) and a sequence \(\alpha_n\) satisfying \(\lim_{n \to \infty} \alpha_n = [\alpha]\), then the probability that \(G_q\) has a minimum degree at least \(k\) converges to \(e^{-\frac{\ln \ln n + \alpha_n}{n}}\), which equals (i) \(e^{-\frac{\ln \ln n + \alpha_n}{n}}\) if \(\lim_{n \to \infty} \alpha_n = \alpha\) \(\in (-\infty, \infty)\), (ii) \(1\) if \(\lim_{n \to \infty} \alpha_n = \infty\), and (iii) \(0\) if \(\lim_{n \to \infty} \alpha_n = -\infty\).

- We extend the above result to provide the asymptotic probability distribution for the minimum degree. Specifically, when \(\alpha_n\) above can be written as \(\alpha_n = b \ln \ln n + \beta_n\) for a constant integer \(b\) and a sequence \(\beta_n\) satisfying \(-1 < \lim inf_{n \to \infty} \beta_n \leq \lim sup_{n \to \infty} \beta_n < 1\) (i.e., \(c_1 \ln \ln n \leq \beta_n \leq c_2 \ln \ln n\) for constants \(-1 < c_1 \leq c_2 < 1\)), we have the following:
  - if \(k + b \geq 1\) and \(\lim_{n \to \infty} \beta_n \in [\alpha, \infty)\), then the minimum degree of \(G_q\) in the asymptotic sense equals (i) \(k + b\) with probability \(e^{-\frac{\ln \ln n + \beta_n}{n}}\); (ii) \(k + b - 1\) with probability \(1 - e^{-\frac{\ln \ln n + \beta_n}{n}}\); and (iii) other values with probability \(0\);
  - if \(k + b \leq 0\), then the minimum degree of \(G_q\) in the asymptotic sense equals \(0\) with probability \(1\).

- Our results on minimum degree are obtained by analyzing the number of nodes with a fixed degree. Specifically, we show that for a non-negative constant integer \(h\), the number of nodes in \(G_q\) with degree \(h\) is in distribution asymptotically equivalent to a Poisson random variable with mean \(n(\lambda h)^{-1} (np_{e,q})^h e^{-np_{e,q}}\).

B. Design Guidelines for Secure Sensor Networks

Based on the above results, for \(G_q\) denoting a secure sensor network employing the \(q\)-composite key predistribution scheme under the on/off channel model, we obtain several guidelines below for choosing parameters to ensure that the network \(G_q\) has certain minimum node degree. The guidelines are given by enforcing conditions on \(p_{e,q}\), the probability of a secure link between two sensors. Note that \(p_{e,q} = p_n \left( 1 - \sum_{u=0}^{q-1} \frac{\binom{Kn}{u} \binom{Kn-h}{Kn-u}}{\binom{Kn}{Kn}} \right)\); see Equation (8) later.

For the network \(G_q\), we now present the design guidelines, which are further explained in Section III-B.

- First, to ensure that the network \(G_q\) has a minimum degree no less than \(k\) (i.e., to ensure that each sensor is directly connected to at least \(k\) other sensors), we can choose network parameters to have

\[
p_{e,q} \geq \frac{\ln n + (k+c_1-1) \ln \ln n}{n}
\]

for a constant \(c_1 > 0\), where the positive constant \(c_1\) can be arbitrarily small.

- Second, to guarantee that the network \(G_q\) has a minimum degree at least \(k\) with probability no less than \(\rho\), we choose parameters to have

\[
p_{e,q} \geq \frac{\ln n + (k-1) \ln \ln n - \ln[(k-1)! \frac{1}{e}]}{n}
\]

(2)

- Third, to ensure that the network \(G_q\) has a minimum degree being \(k\) exactly, we can choose network parameters to have

\[
p_{e,q} = \frac{\ln n + (k+c_2-1) \ln \ln n}{n}
\]

for a constant \(0 < c_2 < 1\), where the positive constant \(c_2\) can be arbitrarily small.

C. Roadmap

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 prove Theorems 1 and 2 using Theorem 3. In Section V, we detail the steps of establishing Theorem 3 through Lemma 1. Section VI provides the proof of Lemma 1 by the help of Propositions 1 and 2, which are proved in Sections VII and VIII, respectively. Subsequently, we present experiments in Section IX to confirm our analytical results. Section X is devoted to relevant results in the literature. Finally, we conclude the paper in Section XI.
II. System Model

Our approach to the analysis is to explore the induced random graph models of the WSNs. As will be clear soon, 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 [5], [20].

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 $V = \{v_1, v_2, \ldots, v_n\}$ to represent the $n$ sensors (a sensor is also referred to as a node). For each node $v_i \in V$, 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 with size $P_n$. Then by the independence of events $C_{ij}$ and $\Gamma_{ij}$, we obtain

$$p_{c,q} = \Pr[\mathcal{E}_{ij}] = \Pr[C_{ij}] \cdot \Pr[\mathcal{I}_{ij}] = p_n \cdot p_{s,q}.$$  

(7)

Summarizing (5) (6) (7), we derive that under $P_n \geq 2K_n$, the link probability $p_{c,q}$ is given by

$$p_{c,q} = p_n \cdot \left[1 - \sum_{u=0}^{q-1} \left(\frac{P_n}{K_n}ight)^u \left(\frac{K_n - u}{K_n - q}ight)^u\right].$$  

(8)

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". As already mentioned, all asymptotic statements are understood with $n \rightarrow \infty$, and we use the standard asymptotic notation $o(\cdot), O(\cdot), \omega(\cdot), \Omega(\cdot), \Theta(\cdot), \sim$; see [3, Page 2-Footnote 1]. In particular, for two positive sequences $f_n$ and $g_n$, $f_n \sim g_n$ signifies $\lim_{n \rightarrow \infty} \frac{f_n}{g_n} = 1$; namely, $f_n$ and $g_n$ are asymptotically equivalent.

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

We now present the results of graph $\mathbb{G}_q$ below. Theorem 1 provides the probability of minimum degree being at least $k$ in $\mathbb{G}_q$.

Theorem 1 (Minimum Degree in Graph $\mathbb{G}_q$): For graph $\mathbb{G}_q$ with $K_n = \omega(1)$ and $\frac{\ln n}{n^\alpha} = o(1)$, if there exist a constant integer $k \geq 1$ and a sequence $\alpha_n$ satisfying $\lim_{n \rightarrow \infty} \alpha_n \in (-\infty, \infty)$ such that

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

(9)

then with $\delta$ denoting the minimum degree of $\mathbb{G}_q$, we have

$$\lim_{n \rightarrow \infty} \Pr[\delta \geq k] = \begin{cases} 0, & \text{if } \lim_{n \rightarrow \infty} \alpha_n = \alpha^* \in (-\infty, \infty), \\ e^{-\frac{n^{\alpha^*}}{K_n}}, & \text{if } \lim_{n \rightarrow \infty} \alpha_n = \alpha^* \in (-\infty, \infty), \\ 1, & \text{if } \lim_{n \rightarrow \infty} \alpha_n = \alpha^* \in (-\infty, \infty), \\ 0, & \text{if } \lim_{n \rightarrow \infty} \alpha_n = -\infty. \end{cases}$$  

(10a) (10b) (10c)

Remark 1: The results (10a) (10b) (10c) can be compactly summarized as $\lim_{n \rightarrow \infty} \Pr[\delta \geq k] = e^{-\min_{n \rightarrow \infty} \alpha_n}.$

Interpreting Theorem 1: Theorem 1 for graph $\mathbb{G}_q$ presents the asymptotically exact probability and a zero–one law for the event that $\mathbb{G}_q$ has a minimum degree no less than $k$, \ldots
where a zero–one law means that the probability of a graph having a certain property asymptotically converges to 0 under some conditions and to 1 under some other conditions. To establish Theorem 1, we explain the basic ideas in Section III-C, and more technical details in Section IV.

While Theorem 1 above is for the property of minimum degree being at least some value, we now present Theorem 2 below, which gives a more fine-grained result to provide the asymptotic probability distribution for the minimum degree.

**Theorem 2 (Minimum Degree in Graph \( G_q \): More Fine-Grained Results Compared With Theorem 1):** Under the conditions of Theorem 1, if \( \alpha_n \), in Equation (9) can be written as

\[
\alpha_n = b \ln \ln n + \beta_n
\]

for a constant integer \( b \) and a sequence \( \beta_n \) satisfying

\[
-1 < \liminf_{n \to \infty} \frac{\beta_n}{\ln \ln n} \leq \limsup_{n \to \infty} \frac{\beta_n}{\ln \ln n} < 1,
\]

then with \( \delta \) denoting the minimum degree of \( G_q \), the properties ①–⑤ below follow:

① for \( k + b \leq 0 \) (which implies \( b \leq -k \leq -1 \) given \( k \geq 1 \), we have

\[
\begin{align*}
\lim_{n \to \infty} \mathbb{P}[\delta = 0] &= 1, \\
\lim_{n \to \infty} \mathbb{P}[\delta > 0] &= 0;
\end{align*}
\]

and for \( k + b \geq 1 \) (i.e., \( b \geq 1 - k \)), we obtain properties ②–⑤:

② \( \lim_{n \to \infty} \mathbb{P}[(\delta = k + b) \text{ or } (\delta = k + b - 1)] = 1; \)

③ if \( \lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty) \), then

\[
\begin{align*}
\lim_{n \to \infty} \mathbb{P}[\delta = k + b] &= e^{-\frac{\beta^*}{(k+1)(k+2)}}, \\
\lim_{n \to \infty} \mathbb{P}[\delta = k + b - 1] &= 1 - e^{-\frac{\beta^*}{(k+1)(k+2)}};
\end{align*}
\]

④ if \( \lim_{n \to \infty} \beta_n = \infty \), then

\[
\begin{align*}
\lim_{n \to \infty} \mathbb{P}[\delta = k + b] &= 1, \\
\lim_{n \to \infty} \mathbb{P}[\delta \neq k + b] &= 0;
\end{align*}
\]

⑤ if \( \lim_{n \to \infty} \beta_n = -\infty \), then

\[
\begin{align*}
\lim_{n \to \infty} \mathbb{P}[\delta = k + b - 1] &= 1, \\
\lim_{n \to \infty} \mathbb{P}[\delta \neq k + b - 1] &= 0.
\end{align*}
\]

Remark 2: The above results ③–⑤ for \( k + b \geq 1 \) and \( \lim_{n \to \infty} \beta_n \in [-\infty, \infty] \) can be compactly summarized as that the minimum degree of \( G_q \) in the asymptotic sense equals (i) \( k + b \) with probability \( e^{-\frac{\beta_n}{(k+1)(k+2)}} \), (ii) \( k + b - 1 \) with probability \( 1 - e^{-\frac{\beta_n}{(k+1)(k+2)}} \), and (iii) other values with probability 0, while results ① says that if \( k + b \leq 0 \), then the minimum degree of \( G_q \) in the asymptotic sense equals 0 with probability 1.

Interpreting Theorem 2: Theorem 2 presents the asymptotic probability distribution for the minimum degree. We explain that Theorem 2 is more fine-grained than Theorem 1. We discuss first Theorem 2’s result ① and then its results ②–⑤.

(i) In result ① above, \( b \leq -k \leq -1 \) follows from \( k + b \leq 0 \) and \( k \geq 1 \). Using \( b \leq -1 \) and (12) in (11), we have \( \lim_{n \to \infty} \alpha_n = -\infty \), so we use (10c) of Theorem 1 to obtain \( \delta < k \) almost surely (an event happens almost surely if its probability converges 1 as \( n \to \infty \)), where \( \delta \) denotes the minimum degree of \( G_q \). For comparison, (13a) of Theorem 2 presents the stronger result that \( \delta = 0 \) almost surely.

(ii) In the above results ②–⑤ where \( k + b \geq 1 \) holds (i.e., \( b \geq 1 - k \)), we derive from (11) and (12) that

\[
\begin{align*}
\lim_{n \to \infty} \alpha_n &= \begin{cases} \\
\infty, & \text{if } b \geq 1, \\
\beta^*, & \text{if } b = 0 \text{ and } \lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty), \\
\infty, & \text{if } b = 0 \text{ and } \lim_{n \to \infty} \beta_n = \infty, \\
-\infty, & \text{if } b \neq 0 \text{ and } \lim_{n \to \infty} \beta_n = -\infty, \\
-\infty, & \text{if } b \leq -1.
\end{cases}
\]

Below we discuss (17a)–(17e), respectively.

- For (17a) above, (10b) of Theorem 1 says \( \delta \geq k \) almost surely, while ② of Theorem 2 presents the stronger result that \( \delta \) equals \( k + b \) or \( k + b - 1 \) almost surely (note \( b \geq 1 \) in (17a)).

- For (17b) above, (10a) of Theorem 1 says \( \delta \geq k \) with probability \( e^{-\frac{\beta^*}{(k+1)(k+2)}} \) asymptotically, while ③ of Theorem 2 presents the stronger result that \( \delta \) equals \( k \) (note \( b = 0 \) in (17b) here) with probability \( e^{-\frac{\beta^*}{(k+1)(k+2)}} \) asymptotically, and equals \( k - 1 \) with probability \( 1 - e^{-\frac{\beta^*}{(k+1)(k+2)}} \) asymptotically (note \( b = 0 \) in (17b) here).

- For (17c) above, (10b) of Theorem 1 says \( \delta \geq k \) almost surely, while ④ of Theorem 2 presents the stronger result that \( \delta = k \) almost surely (note \( b = 0 \) in (17c) here).

- For (17d) above, (10c) of Theorem 1 says \( \delta < k \) almost surely, while ⑤ of Theorem 2 presents the stronger result that \( \delta = k - 1 \) almost surely (note \( b = 0 \) in (17d) here).

- For (17e) above, (10c) of Theorem 1 says \( \delta < k \) almost surely, while ⑥ of Theorem 2 presents the stronger result that \( \delta \) equals \( k + b \) or \( k + b - 1 \) almost surely (note \( b \leq -1 \) in (17e)).

Summarizing the above, compared with Theorem 1, Theorem 2 presents a more fine-grained result for minimum degree in \( G_q \).

To prove Theorem 2, we provide the basic ideas in Section III-C, and more technical details in Section IV.

Theorems 1 and 2 above are for the property of minimum degree being at least \( k \). We now consider a stronger graph/network property, namely \( k \)-connectivity.

**Extension to \( k \)-Connectivity:** We can extend Theorem 1 to obtain the probability of \( k \)-connectivity in \( G_q \).
Specifically, we can replace \( \lim_{n \to \infty} P[G_q \text{ is } k\text{-connected}] \) by \( \lim_{n \to \infty} P[K_n = \omega(1) \text{ and } \frac{K_n^2}{n} = o(1) \text{ by a stronger condition set} \) at the cost of replacing \( K_n = \omega(1) \) and \( \frac{K_n^2}{n} = o(1) \) by \( \frac{K_n^2}{n} = o\left(\frac{1}{\ln n}\right) \), \( P_n = o\left(\frac{1}{\ln n}\right) \) and \( K_n = \Omega(n') \) for a positive constant \( \epsilon \). Due to space limitation, we present the proof in the full version [22].

**B. Design Guidelines for Secure Sensor Networks**

Based on the above results, now we provide several design guidelines of minimum strength of degree.

- First, to ensure that \( G_q \) has a minimum degree no less than \( k \), we can choose network parameters to set
  \[
  p_{c,q} \geq \frac{\ln n + (k + c_1 - 1) \ln n}{n} \text{ for a constant } c_1 > 0, \tag{18}
  \]
  where the positive constant \( c_1 \) can be arbitrarily small. To see this, since (18) implies that \( \alpha_n \) defined by (9) (i.e., \( p_{c,q} = \frac{\ln(n+(k-1)\ln n+\alpha_n)}{n} \)) satisfies \( \lim_{n \to \infty} \alpha_n = \infty \), we use Theorem 1 to have \( P[G_q \text{ has a minimum degree at least } k] = 1 \).

- Second, to guarantee that \( G_q \) has a minimum degree at least \( k \) with probability no less than \( \rho \), we choose parameters to ensure
  \[
  p_{c,q} \geq \frac{\ln n + (k - 1) \ln n - \ln[(k - 1)! / \rho]}{n}. \tag{19}
  \]
  To see this, since (19) implies that \( \alpha_n \) defined by (9) (i.e., \( p_{c,q} = \frac{\ln(n+(k-1)\ln n+\alpha_n)}{n} \)) satisfies \( \alpha_n \geq -\ln[(k - 1)! / \rho] \) we use Theorem 1 to obtain \( P[G_q \text{ has a minimum degree at least } k] \geq e^{\ln[(k-1)! / \rho]} = \rho \).

- Third, to ensure that \( G_q \) has a minimum degree being \( k \) exactly, we can choose network parameters to have
  \[
  p_{c,q} = \frac{\ln n + (k + c_2 - 1) \ln n}{n} \text{ for a constant } 0 < c_2 < 1, \tag{20}
  \]
  where the positive constant \( c_2 \) can be arbitrarily small. To see this, (20) implies that \( \alpha_n \) defined by (9) (i.e., \( p_{c,q} = \frac{\ln(n+(k-1)\ln n+\alpha_n)}{n} \)) equals \( c_2 \ln n, n \) so \( b \) in (11) is 0 with \( \beta_n \) satisfying (11) and \( \lim_{n \to \infty} \beta_n = \infty \). Then we use Theorem 1-Result 6 to obtain \( P[\text{Minimum degree of } G_q \text{ equals } k \text{ exactly}] = 1 \).

**C. Basic Ideas to Establish Theorems 1 and 2**

We establish Theorems 1 and 2 for minimum degree in graph \( G_q \) by analyzing the number of nodes with a fixed degree, for which we present Theorem 3 below. The details of using Theorem 3 to prove Theorems 1 and 2 are given in Section IV.

**Theorem 3 (Possion Distribution for Number of Nodes With a Fixed Degree in Graph \( G_q \)):** For graph \( G_q \) with \( K_n = \omega(1) \) and \( K_n^2 = o(1) \), if
\[
p_{c,q} = \frac{\ln n + O(\ln \ln n)}{n}, \quad (21)
\]
(i.e., \( n p_{c,q,\ln n} \text{ is bounded} \)), then for a non-negative constant integer \( h \), the number of nodes in \( G_q \) with degree \( h \) is in distribution asymptotically equivalent to a Poisson random variable with mean \( \lambda_{n,h} \equiv n(h!)^{-1}(n p_{c,q})^h e^{-n p_{c,q}} \); i.e., as \( n \to \infty \),
\[
P[ \text{The number of nodes in } G_q \text{ with degree } h \text{ equals } \ell ] = \left( \frac{1}{\ell!} \right) (1 - \lambda_{n,h})^\ell e^{\lambda_{n,h}} \to 1, \quad \text{for } \ell = 0, 1, \ldots \tag{22}
\]
Interpreting Theorem 3: Theorem 3 for graph \( G_q \) shows that the number of nodes with a fixed degree follows a Poisson distribution asymptotically.

**D. The Practicality of the Theorem Conditions**

We check the practicality of the conditions in Theorem 1: \( K_n = \omega(1) \) and \( K_n^2 = o(1) \). The condition \( K_n = \omega(1) \) means that the key ring size \( K_n \) on a sensor grows with the number \( n \) of sensors and thus it follows trivially in secure wireless sensor networks [10], [23], [24]. For \( k \)-connectivity, the condition on \( K_n \) (i.e., \( K_n = \Omega(n') \)) is more appealing than \( K_n = \Omega(n') \) because \( \epsilon \) can be arbitrarily small.

In addition, \( K_n = o\left(\frac{n}{\ln n}\right) \) holds in practice since the key pool size \( P_n \) is expected to be several orders of magnitude larger than the key ring size \( K_n \) (see [2, Sec. 2.1] and [5, Sec. III-B]).

**IV. PROOFS OF THEOREMS 1 AND 2 USING THEOREM 3**

As explained in Section III-C, we establish Theorems 1 and 2 based on Theorem 3. Theorems 1 and 2 present results of \( \delta \), where \( \delta \) denotes the minimum degree of \( G_q \). With \( \Phi_{n,h} \) denoting the number of nodes with degree \( h \) in \( G_q \), Theorem 3 provides the asymptotic distribution of \( \Phi_{n,h} \). To use Theorem 3 for proving Theorems 1 and 2, we now discuss the relationship between \( \delta \) and \( \Phi_{n,h} \). For non-negative integer \( \mu \), it is straightforward to see properties 1 and 2 below.

1. The event \( (\delta \geq \mu) \) (i.e., the event that the minimum node degree of graph \( G_q \) is at least \( \mu \)) is equivalent to the event \( \bigcup_{h=0}^{\mu-1} (\Phi_{n,h} = 0) \) (i.e., no node has degree falling in \( \{0, 1, \ldots, \mu - 1\} \)).

2. The event \( (\delta \leq \mu) \) (i.e., the event that the minimum node degree of graph \( G_q \) is at most \( \mu \)) and the event \( \bigcup_{h=0}^{\mu} (\Phi_{n,h} \neq 0) \) (i.e., there is at least one node with degree at most \( \mu \)) are equivalent.

Therefore, for any integer \( \xi \), we obtain
\[
P[\delta \geq \xi + 1] = P\left( \bigcap_{h=0}^{\xi} (\Phi_{n,h} = 0) \right) \quad \text{(by property } 1) \]
\[
\leq P[\Phi_{n,\xi} = 0], \quad \text{if } \xi \geq 0, \tag{23}
\]
\[ P[\delta \leq \xi - 2] \leq P\left[ \bigcup_{h=0}^{\xi-2} (\Phi_{n,h} \neq 0) \right] \text{ (by property } \Theta) \]
\[ \leq \sum_{h=0}^{\xi-2} P[\Phi_{n,h} \neq 0] \text{ (by the union bound), if } \xi \geq 2, \quad (24) \]

\[ P[\delta \geq \xi] \leq P\left[ \bigcap_{h=0}^{\xi-1} (\Phi_{n,h} = 0) \right] \text{ (by property } \Theta) \]
\[ = 1 - P\left[ \bigcup_{h=0}^{\xi-1} (\Phi_{n,h} \neq 0) \right] \geq 1 - \sum_{h=0}^{\xi-1} P[\Phi_{n,h} \neq 0] \text{ (by the union bound)} \]
\[ = P[\Phi_{n,k-1} = 0] - 1[k \geq 2] \times \sum_{h=0}^{k-2} P[\Phi_{n,h} \neq 0], \quad (25) \]

where the indicator variable \(1[k \geq 2]\) equals 1 if \(k \geq 2\) and 0 if \(k < 2\).

To use (23)–(26), we will compute \(P[\Phi_{n,h} = 0]\) and \(P[\Phi_{n,h} \neq 0]\) for \(h = 0, 1, \ldots\). To this end, we use Theorem 3, which shows that \(\Phi_{n,h}\) is in distribution asymptotically equivalent to a Poisson random variable with mean \(\lambda_{n,h}\) specified by
\[ \lambda_{n,h} := n(h!)^{-1}(np_{e,q})^h e^{-np_{e,q}}; \quad (27) \]

i.e.,
\[ P[\Phi_{n,h} = \ell] \sim (\ell!)^{-1}\lambda_{n,h}^\ell e^{-\lambda_{n,h}}. \quad (28) \]

To assess \(\lambda_{n,h}\) in (27), we use (9) about \(p_{e,q}\) (i.e., \(p_{e,q} = \frac{\ln n + (k-1)\ln n + \alpha_n}{n}\)). While \(\alpha_n\) in Theorem 2 is given by (11) and satisfies \(|\alpha_n| = O(\ln \ln n) = o(\ln n)\) for a constant integer \(b\) and a sequence \(\beta_n\) under (12), \(\alpha_n\) in Theorem 1 may not satisfy \(|\alpha_n| = o(\ln n)\). However, we can still introduce the additional condition \(|\alpha_n| = o(\ln n)\) in proving Theorem 1, as explained in Appendix E of the full version [22]. The idea is to show that whenever Theorem 1 with \(|\alpha_n| = o(\ln n)\) holds, then Theorem 1 regardless of \(|\alpha_n| = o(\ln n)\). Now under \(|\alpha_n| = o(\ln n)\) in Theorem 1, we obtain
\[ p_{e,q} \sim \frac{\ln n}{n}, \quad (29) \]

where \(f_n \sim g_n\) for two positive sequences \(f_n\) and \(g_n\) means \(\lim_{n \to \infty} f_n/g_n = 1\); i.e., (29) means \(\lim_{n \to \infty} p_{e,q}/(\ln n) = 1\).

Then we substitute (9) and (29) into (27) to derive
\[ \lambda_{n,h} = n(h!)^{-1}(np_{e,q})^h e^{-(np_{e,q})} \sim n(h!)^{-1}(\ln n)^h \times e^{-\ln n - (k-1)\ln n - \alpha_n} \]
\[ = (h!)^{-1}(\ln n)^h+1-k e^{-\alpha_n}. \quad (30) \]

We now use Theorem 3 (i.e., (28)) to prove Theorem 1 under the additional condition \(|\alpha_n| = o(\ln n)\), which we can introduce based on the above discussion. Then we evaluate \(P[\delta \geq k]\). Given \(k \geq 1\), we know from (25) and (28) that
\[ P[\delta \geq k] \leq e^{-\lambda_{n,k-1}} \times [1 + o(1)], \quad (31) \]

and from (26) and (28) that
\[ P[\delta \geq k] \geq e^{-\lambda_{n,k-1}} \times [1 - o(1)] - 1[k \geq 2] \]
\[ \times \sum_{h=0}^{k-2} \{(1 - e^{-\lambda_{n,h}}) \times [1 + o(1)]\}. \quad (32) \]

Based on (31) and (32), we discuss the following cases.

- If \(\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, \infty)\), (30) implies for \(k \geq 1\) that
\[ \lambda_{n,h} \to 0 \quad \text{for } h = 0, 1, \ldots, k-2, \quad \text{if } k \geq 2, \]
\[ \to \begin{cases} 
0, & \text{for } h = 0, 1, \ldots, k-2, \quad \text{if } k \geq 2, \\
\frac{e^{-\alpha^*}}{(k-1)!}, & \text{for } h = k-1. 
\end{cases} \quad (33a) \]

Applying (33b) to (31), and applying (33a) (33b) to (32), we have \(e^\frac{-\alpha^*}{(k-1)!} \times [1 - o(1)] \leq P[\delta \geq k] \leq e^\frac{-\alpha^*}{(k-1)!} \times [1 + o(1)]\) so that \(\lim_{n \to \infty} P[\delta \geq k] = e^\frac{-\alpha^*}{(k-1)!}\); i.e., (10a) is proved.

- If \(\lim_{n \to \infty} \alpha_n = \infty\), then (30) implies for \(k \geq 1\) that
\[ \lambda_{n,h} \to 0 \quad \text{for } h = 0, 1, \ldots, k-1. \quad (34) \]

Substituting (34) into (31), and substituting (34) into (32), we obtain \([1 - o(1)] \leq P[\delta \geq k] \leq [1 + o(1)]\) so that \(\lim_{n \to \infty} P[\delta \geq k] = 1\); i.e., (10b) is proved.

- If \(\lim_{n \to \infty} \alpha_n = -\infty\), then (30) implies for \(k \geq 1\) that
\[ \lambda_{n,k-1} \to \infty. \quad (35) \]

Using (35) in (31), we have \(P[\delta \geq k] \leq o(1)\) so that \(\lim_{n \to \infty} P[\delta \geq k] = 0\); i.e., (10c) is proved.

We now use Theorem 3 (i.e., (28)) to prove Theorem 2. The condition (12) on \(\beta_n\) implies that there are constants \(c_1\) and \(c_2\) with \(-1 < c_1 < c_2 < 1\) such that
\[ c_1 \ln \ln n \leq \beta_n \leq c_2 \ln \ln n, \quad \text{for all } n \text{ sufficiently large}, \quad (36) \]

which implies
\[ (\ln n)^{-c_2} \leq e^{-\beta_n} \leq (\ln n)^{-c_1}, \quad \text{for all } n \text{ sufficiently large}. \quad (37) \]

Using (11) in (9), we have \(p_{e,q} = \frac{\ln n + (k+b-1)\ln n + \beta_n}{n}\), which along with (36) implies \(p_{e,q} \sim \frac{\ln n}{n}\). Then similar to (30), we derive \(\lambda_{n,h} \sim (h!)^{-1}(\ln n)^{h+1-(k+b)} e^{-\beta_n}. \)
Applying (37) to this result and noting $-1 < c_1 \leq c_2 < 1$, we find

$$
\lambda_{n,h} \sim \begin{cases} 
0, & \text{for } h = 0, 1, \ldots, k + b - 2, \\
\frac{e^{-\beta_n}}{(k + b - 1)!}, & \text{for } h = k + b - 1, \text{ if } k + b \geq 1; \\
\infty, & \text{for } h = \max\{k + b, 0\}, \\
\max\{k + b, 0\} + 1, & \text{if } k + b = 1.
\end{cases}
$$

(38)

Using (38) in (28), we get

$$
\mathbb{P}[\Phi_{n,h} = 0 \sim e^{-\lambda_{n,h}}]
\begin{array}{ll}
\rightarrow 1, & \text{for } h = 0, 1, \ldots, k + b - 2, \\
\rightarrow 0, & \text{if } k + b = 2, \\
\rightarrow e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}, & \text{for } h = k + b - 1, \text{ if } k + b \geq 1; \\
\rightarrow 0, & \text{for } h = \max\{k + b, 0\}, \\
\end{array}
$$

(39a)

$$
\rightarrow e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}, & \text{for } h = k + b - 1, \text{ if } k + b \geq 1; \\
\rightarrow 0, & \text{for } h = \max\{k + b, 0\}, \\
$$

(39b)

$$
\rightarrow 0, & \text{if } k + b = 1.
$$

(39c)

If $k + b \leq 0$, then (39c) gives $\mathbb{P}[\Phi_{n,0} = 0 \rightarrow 0$, which along with (25) and (26) yields $\mathbb{P}[\delta \geq 1] = \mathbb{P}[\Phi_{n,0} = 0 \rightarrow 0$ so that we further obtain $\lim \mathbb{P}[\delta = 0] = 1$ and $\lim \mathbb{P}[\delta > 0] = 0$. Hence, property \( \Box \) of Theorem 2 is proven.

Below we consider the case of $k + b \geq 1$ to prove properties \( \Box \)–\( \Box \) of Theorem 2.

Given $k + b \geq 1$, we derive from (24) and (39a) that

$$
\mathbb{P}[\delta \leq k + b - 2] \leq \sum_{h = 0}^{k+b-2} \mathbb{P}[\Phi_{n,h} \neq 0] \rightarrow 0, \text{ if } k + b \geq 2, \\
= 0, \text{ if } k + b = 1,
$$

which implies

$$
\mathbb{P}[\delta \leq k + b - 2] = o(1).
$$

(40)

Given $k + b \geq 1$, we obtain from (23) and (39c) that

$$
\mathbb{P}[\delta \geq k + b + 1] \leq \mathbb{P}[\Phi_{n,k+b} = 0] = o(1).
$$

(41)

Given $k + b \geq 1$, we show from (25) and (39b) that

$$
\mathbb{P}[\delta \geq k + b] \leq \mathbb{P}[\Phi_{n,k+b-1} = 0] \sim e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}},
$$

(42)

and show from (26) and (39a) that

$$
\mathbb{P}[\delta \geq k + b] \geq \mathbb{P}[\Phi_{n,k+b-1} = 0] - 1[k + b \geq 2] \cdot \sum_{h = 0}^{k+b-2} \mathbb{P}[\Phi_{n,h} \neq 0] \sim e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}.
$$

(43)

Then (42) and (43) together induce

$$
\mathbb{P}[\delta \geq k + b] \sim e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}.
$$

(44)

From (40) and (41), we have

$$
\mathbb{P}[\delta \neq k + b] \cap (\delta \neq k + b - 1] = \mathbb{P}[\delta \geq k + b + 1] + \mathbb{P}[\delta \leq k + b - 2] = o(1); \text{ (45)}
$$

\[\text{from (41) and (44), we obtain} \]

$$
\mathbb{P}[\delta = k + b] = \mathbb{P}[\delta \geq k + b] - \mathbb{P}[\delta \geq k + b + 1] \sim e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}, \text{ if } \lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty),
$$

$$
\to 1, \text{ if } \lim_{n \to \infty} \beta_n = \infty,
$$

$$
\to 0, \text{ if } \lim_{n \to \infty} \beta_n = -\infty;
$$

(46)

and from (45) and (46), we conclude

$$
\mathbb{P}[\delta = k + b - 1] = 1 - \mathbb{P}[\delta \neq k + b] \cap (\delta \neq k + b - 1] - \mathbb{P}[\delta = k + b] \\
\sim 1 - e^{-\frac{e^{-\beta_n}}{(k + b - 1)!}}, \text{ if } \lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty),
$$

$$
\to 0, \text{ if } \lim_{n \to \infty} \beta_n = \infty,
$$

$$
\to 1, \text{ if } \lim_{n \to \infty} \beta_n = -\infty.
$$

(47)

Properties \( \Box \)–\( \Box \) of Theorem 3 follow from (45)–(47).

To summarize, We have used Theorem 3 (proved in Section V later) to establish Theorem 1 under the additional condition $|\alpha_n| = o(ln n)$, and to establish Theorem 2. In Appendix E of the full version [22], we explain that whenever Theorem 1 with $|\alpha_n| = o(ln n)$ holds, then Theorem 1 regardless of $|\alpha_n| = o(ln n)$.

\( \blacksquare \)

V. Establishing Theorem 3

A. Method of Moments

For $h = 0, 1, \ldots$, with $\Phi_{n,h}$ counting the number of nodes with degree $h$ in $\mathbb{G}_q$, we will show that $\Phi_{n,h}$ asymptotically follows a Poisson distribution with mean $\lambda_{n,h}$. This is done by using the method of moments; specifically, in view of [25, Th. 2.13], we will obtain the desired result upon establishing

$$
\mathbb{P}[\text{Nodes } v_1, v_2, \ldots, v_m \text{ have degree } h] \sim \lambda_{n,h}^m / m!.
$$

(48)

Therefore, if Lemma 1 below holds, then the proof of property (a) in Theorem 3 is completed; in particular, we will have that for any integers $h \geq 0$ and $\ell \geq 0$,

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

(49)

Lemma 1: Given (21) (i.e., $p_{e,q} = \frac{\ln n + O(ln n)}{n}$), $K_n = \omega(1)$ and $\frac{K_n^2}{\alpha_n} = o(1)$, then for any integers $m \geq 1$ and $h \geq 0$, we have

$$
\mathbb{P}[\text{Nodes } v_1, v_2, \ldots, v_m \text{ have degree } h] \sim (h!)^{-m} (n p_{e,q})^h m! e^{-n p_{e,q}};
$$

i.e., (48) follows with $\lambda_{n,h}$ set by

$$
\lambda_{n,h} = n (h!)^{-1} (n p_{e,q})^h e^{-n p_{e,q}};
$$

(50)

Section VI details the proof of Lemma 1. Given (21), we obtain the following two results, which are frequently used in the rest of the paper:

$$
p_{e,q} \sim \frac{\ln n}{n}.
$$

(51)
and
\[ p_{v,q} \leq \frac{2 \ln n}{n} \text{ for all } n \text{ sufficiently large.} \] (52)

VI. 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 \( 1[C_{ij}] \) as the indicator variable of event \( C_{ij} \) by
\[
1[C_{ij}] = \begin{cases} 
1, & \text{if the channel between } v_i \text{ and } v_j \text{ is on;} \\
0, & \text{if the channel between } v_i \text{ and } v_j \text{ is off.}
\end{cases}
\]

We denote by \( \mathcal{C}_m \) a \((m)\)-tuple consisting of all possible \( 1[C_{ij}] \) with \( 1 \leq i < j \leq m \) as follows:
\[
\mathcal{C}_m := (1[C_{12}], \ldots, 1[C_{1m}], 1[C_{23}], \ldots, 1[C_{2m}],
1[C_{34}], \ldots, 1[C_{3m}], \ldots, 1[C_{(m-1),m}]).
\]

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 \( G_m \) are determined.

Let \( \mathcal{L}_m, \mathcal{T}_m \) and \( \mathcal{L}_m \) be the sets of all possible \( \mathcal{C}_m, \mathcal{T}_m \) and \( \mathcal{L}_m \), respectively. We define \( \mathcal{L}_m^{(0)} \) such that \( \mathcal{L}_m \in \mathcal{L}_m^{(0)} \) is the event that there is no edge between any two of nodes \( v_1, v_2, \ldots, v_m \), i.e.,
\[
\mathcal{L}_m^{(0)} := \{ \mathcal{L}_m \mid (|S_i \cap S_j| < q) \text{ or } (1[C_{ij}] = 0), \forall i, j \text{ with } 1 \leq i < j \leq m. \}.
\]

We define \( N_j \) 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
\[
M_{j_1,j_2,\ldots,j_m} := \{ w \in V \setminus \{v_1, v_2, \ldots, v_m\} : \text{and for } i = 1, 2, \ldots, m, \begin{cases} w \in N_i & \text{if } j_i = 1; \\
\neg w \in N_i & \text{if } j_i = 0. \end{cases} \}
\]

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 \( V_m := \{v_1, v_2, \ldots, v_m\} \) and \( V_m := V \setminus V_m \), we obtain
\[
\bigcup_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1,j_2,\ldots,j_m}| = \overline{V}_m,
\]
and
\[
\bigcup_{j_1, j_2, \ldots, j_m \in \{0, 1\}, \sum_{i=1}^m j_i \geq 1} |M_{j_1,j_2,\ldots,j_m}| = \left( \bigcup_{i=1}^m N_i \right) \cap \overline{V}_m.
\]

We define \( 2^m \)-tuple \( \mathcal{M}_m \) through
\[
\mathcal{M}_m := \{ [M_{j_1,j_2,\ldots,j_m}] \mid j_1, j_2, \ldots, j_m \in \{0, 1\} \} = \{ |M_{00}^m|, |M_{01}^m|, |M_{10}^m|, |M_{11}^m|, \ldots \}.
\]

Let \( \mathcal{E} \) be the event that each of \( v_1, v_2, \ldots, v_m \) has a degree of \( h \). Given \( \mathcal{L}_m \in \mathcal{L}_m \), we define \( \mathcal{M}_m(\mathcal{L}_m) \) 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
\[
\mathbb{P}[\mathcal{E}] = \sum_{\mathcal{L}_m \in \mathcal{L}_m} \mathbb{P}[\{ \mathcal{L}_m = \mathcal{L}_m^* \} \cap \{ \mathcal{M}_m = \mathcal{M}_m^* \}] = \mathbb{P}[\mathcal{E}].
\]

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 \( \overline{V}_m \), \( \mathcal{M}_m \) is determined and denoted by \( \mathcal{M}_m(0) \) which satisfies
\[
\begin{cases}
|M_{01}^{m-1,0^{m-1}}| = h, & \text{for } i = 1, 2, \ldots, m; \\
|M_{11}^{j_1,j_2,\ldots,j_m}| = 0, & \text{for } \sum_{i=1}^m j_i > 1; \\
|M_{00}^m| = n - m - hm.
\end{cases}
\]

By (56), we further write \( \mathbb{P}[\mathcal{E}] \) as the sum of
\[
\sum_{\mathcal{L}_m \in \mathcal{L}_m} \mathbb{P}[\{ \mathcal{L}_m = \mathcal{L}_m^* \} \cap \{ \mathcal{M}_m = \mathcal{M}_m^* \}] = \mathbb{P}[\mathcal{E}]
\]
and
\[
\mathbb{P}[\{ \mathcal{L}_m \in \mathcal{L}_m(0) \} \cap \{ \mathcal{M}_m = \mathcal{M}_m(0) \}] = \mathbb{P}[\mathcal{E}].
\]

Consequently, Lemma 1 holds after we prove the following Propositions 1 and 2. In the rest of the paper, we will often use \( 1 + x \leq e^x \) for any \( x \in \mathbb{R} \) and \( 1 - xy \leq (1 - x)^y \leq 1 - xy + \frac{1}{2}x^2y^2 \) for \( 0 \leq x < 1 \) and \( y = 0, 1, 2, \ldots \). (Fact 2 in [3]).

**Proposition 1**: Given (21) (i.e., \( p_{e,q} = \frac{\ln n + O(\ln \ln n)}{n} \)),
\[
K_n = \omega(1) \text{ and } \delta \frac{1}{\ln n} = o(1), \text{ we have }
\]
\[
\mathbb{P}[\{ \mathcal{M}_m = \mathcal{M}_m^* \} \mid \mathcal{L}_m = \mathcal{L}_m^*] = o(h)^{-m}(np_{e,q})^h e^{-mn_{p_{e,q}}}.
\]

**Proposition 2**: Given (21) (i.e., \( p_{e,q} = \frac{\ln n + O(\ln \ln n)}{n} \)),
\[
K_n = \omega(1) \text{ and } \delta \frac{1}{\ln n} = o(1), \text{ we have }
\]
\[
\mathbb{P}[\{ \mathcal{M}_m = \mathcal{M}_m^* \} \mid \mathcal{L}_m = \mathcal{L}_m^*] = o(h)^{-m}(np_{e,q})^h e^{-mn_{p_{e,q}}}.
\]

VII. THE PROOF OF PROPOSITION 1

We embark on the evaluation of (57) by computing
\[
\mathbb{P}[\{ \mathcal{M}_m = \mathcal{M}_m^* \} \mid \mathcal{L}_m = \mathcal{L}_m^*].
\]

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

1 For a non-negative integer \( x \), the term \( 0^x \) is short for \( 0 \ldots 0 \).
For any \( j_1, j_2, \ldots, j_m \in \{0, 1\} \), for any distinct nodes \( w_1 \in V_m \) and \( w_2 \in V_m \), events \( \{w_1 \in M_{j_1j_2\ldots j_m}\} \) and \( \{w_2 \in M_{j_1j_2\ldots j_m}\} \) are not independent [8], but are conditionally independent given \( T_m = T_m^* \) (with the key sets \( S_1, S_2, \ldots, S_m \) specified as \( S_1', S_2', \ldots, S_m' \), respectively). Therefore,

\[
(59) = f(n - m, M_m^*) \mathbb{P}[w \in M_m^* \mid T_m = T_m^*] \left| M_m^\ast \right|
\times \prod_{j_1, j_2, \ldots, j_m \in \{0, 1\}} \mathbb{P}[w \in M_{j_1j_2\ldots j_m}^*] \left| M_m^\ast \right|
\times |T_m = T_m^*| \left| M_{j_1j_2\ldots j_m}^\ast \right|
\]

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

\[
f(\sum_{i=1}^\ell x_i, (x_1, x_2, \ldots, x_\ell)) = \frac{\left(\sum_{i=1}^\ell x_i\right) \left(\sum_{i=2}^\ell x_i\right) \ldots \left(\sum_{i=\ell}^\ell x_i\right)}{x_\ell! x_{\ell-1}! \ldots x_1!}.
\]

From (61) and

\[
\sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1j_2\ldots j_m}^*| = n - m
\]

which holds by (54), we have

\[
f(n - m, M_m^*) = \frac{(m \sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1j_2\ldots j_m}^*|)!}{\prod_{j_1, j_2, \ldots, j_m \in \{0, 1\}} (|M_{j_1j_2\ldots j_m}^*|)!} \frac{(n - m)!}{(n - m - \sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1j_2\ldots j_m}^*|)!}
\]

\[
\leq n - \sum_{i=1}^m N_i \left| M_{i1i2\ldots i_m}^\ast \right|
\]

Denoting \( \sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1j_2\ldots j_m}^*| \) by \( \Lambda \), we prove \( \Lambda \leq hm - 1 \) below if \( (L_m^* \notin L_m^*(0)) \) or \( (M_m^* \neq L_m^*(0)) \).

On the one hand, assuming \( L_m^* \notin L_m^*(0) \), 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, \( \{v_{i_1}, v_{i_2}\} \subseteq (U_{i=1}^m N_i) \cap V_m \). Then from (55),

\[
\Lambda = \left| \bigcup_{i=1}^m N_i \right| - \left( \bigcup_{i=1}^m N_i \right) \cap V_m \leq hm - 2.
\]

On the other hand, assuming \( M_m^* \neq L_m^*(0) \), 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 (55),

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

To summarize, if \( (L_m^* \notin L_m^*(0)) \) or \( (M_m^* \neq L_m^*(0)) \), we have

\[
\Lambda \leq hm - 1,
\]

along with (62) leading to

\[
|M_m^*| = n - m - \Lambda > n - m - hm.
\]

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

\[
P[w \in M_{j_1j_2\ldots j_m} \mid T_m = T_m^*] = \mathbb{P}[|E_{wv_t} \setminus T_m^*| = \mathbb{P}[E_{wv_t} = P_{c.e}].
\]

where \( E_{wv_t} \) is the event that there exists an edge between nodes \( w \) and \( v_t \) in graph \( G_q \).

Substituting (64-67) into (60), we obtain that if \( (L_m^* \notin L_m^*(0)) \) or \( (M_m^* \neq L_m^*(0)) \), then

\[
(59) < (n p_{c.e})^{-h m - 1} \times \mathbb{P}[w \in M_m^* \mid T_m = T_m^*] \leq n^{-m-hm - 1}.
\]

Applying (59) and (68) to (57), we get

\[
(57) < \sum_{L_m^* \in L_m} \mathbb{P} \left[ M_m^* \in L_m \right] \times R.H.S. \text{ of } (68) \times \mathbb{P} \left[ L_m = L_m^* \right].
\]

To bound \( \mathbb{P} \left[ M_m^* \in L_m^* \right] \), note that \( M_m^* \) is a \( 2^m \)-tuple. Among the \( 2^m \) elements of the tuple, each of \( |M_{j_1j_2\ldots j_m}| \mid j_1, j_2, \ldots, j_m \in \{0, 1\} \mid \) is at least 0 and at most \( h \); and the remaining element \( |M_{j_1j_2\ldots j_m}| \) can be determined by (62).

Then it’s straightforward that

\[
\mathbb{P} \left[ M_m^* \in L_m^* \right] \leq (h + 1)^{2^m - 1}.
\]

Using (70) in (69), and considering \( (L_m^* = L_m^*) \) is the union of independent events \( (T_m = T_m^*) \) and \( (C_m = C_m^*) \), and \( \sum_{c_m \in C_m^*} \mathbb{P}[C_m = C_m^*] = 1 \), we derive

\[
(57) < (h + 1)^{2^m - 1} \times \mathbb{P}[T_m = T_m^*] \times \mathbb{P} \left[ w \in M_m^* \mid T_m = T_m^* \right] \leq n^{-m-hm - 1}.
\]

From (71) and \( \lim_{m \to \infty} n p_{c.e} = \infty \) by (51), the proof of Proposition 1 is completed once we show

\[
\sum_{T_m \in T_m^*} \mathbb{P}[T_m = T_m^*] \mathbb{P} \left[ w \in M_m^* \mid T_m = T_m^* \right] \leq e^{-m n p_{c.e}} \cdot [1 + o(1)].
\]

A. Establishing (72)

From Lemma 3 of [22], it holds that

\[
\mathbb{P} \left[ w \in M_m^* \mid T_m = T_m^* \right] \times \mathbb{P} \left[ \mathbb{P}[w \in M_m^* \mid T_m = T_m^*] \right] \times \mathbb{P}[T_m = T_m^*] = e^{-m n p_{c.e}} \cdot \sum_{1 \leq i \leq j \leq m} |S_{ij}| + \frac{n p_{c.e}}{k_m} \sum_{1 \leq i < j \leq m} |S_{ij}|.
\]

where \( S_{ij} = S_i^* \setminus S_j^* \). With (51) (i.e., \( p_{c.e} \sim \frac{\ln n}{m} \)), we have \( m^2 n p_{c.e} \propto 0(1) \) and \( m p_{c.e} = o(1) \), which are substituted into (73) to induce (72) once we prove

\[
\sum_{T_m \in T_m^*} \mathbb{P}[T_m = T_m^*] e^{-m n p_{c.e}} \sum_{1 \leq i < j \leq m} |S_{ij}| \leq 1 + o(1).
\]
L.H.S. of (74) 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 $\delta$ is an arbitrary constant with $0 < \delta < 1$.

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

From $p_n < n^{-\delta}(\ln n)^{-1}$, (52) (namely, $p_{c,q} \leq \frac{2\ln n}{n}$) and $|S^*_i| \leq K_n$ for $1 \leq i < j \leq m$, it holds that

$$e^{-\frac{np_c p_{\mathrm{np}}}{K_n} \sum_{i=1}^{m-1} |S_{im}|} < e^{\frac{2\ln n}{n} - \delta (\ln n)^{-1}} < e^{m^2 \delta^2},$$

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

$$H_{n,m} < e^{m^2 \delta^2} \sum_{T_m \in T_m} P[T_m = T_m] = e^{m^2 \delta^2},$$

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

We relate $H_{n,m}$, $H_{n,m-1}$ and assess $H_{n,m}$ iteratively. First, with $T_m = (S_1^*, S_2^*, \ldots, S_m^*)$, event $(T_m = T_m)$ is the intersection of independent events: $(T_{m-1} = T_{m-1})$ and $(S_m = S_m^*)$. Then we have

$$H_{n,m} = \sum_{T_m \in T_m} \left( P[T_m = T_{m-1}] \cap (S_m = S_m^*) \right) \times e^{-\frac{np_c p_{\mathrm{np}}}{K_n} \sum_{i=1}^{m-1} |S_{im}|}$$

$$= H_{n,m-1} \cdot \sum_{S_m \in S_m^*} P[S_m = S_m^*] e^{-\frac{np_c p_{\mathrm{np}}}{K_n} \sum_{i=1}^{m-1} |S_{im}|},$$

By $\sum_{i=1}^{m-1} |S_{im}| = \sum_{i=1}^{m-1} |S_i^* \cap S_m^*| \leq m |S_m^* \cap (\bigcup_{i=1}^{m-1} S_i^*)|$ and (52) (i.e., $p_{c,q} \leq \frac{2\ln n}{n}$), we get

$$e^{-\frac{np_c p_{\mathrm{np}}}{K_n} \sum_{i=1}^{m-1} |S_{im}|} \leq e^{2np_p p_{\mathrm{np}} \ln n} e^{-\frac{np_c p_{\mathrm{np}}}{K_n} |S_m^* \cap (\bigcup_{i=1}^{m-1} S_i^*)|},$$

further leading to

$$H_{n,m} \leq \sum_{u=0}^{K_n} P \left[ |S_m^* \cap \left( \bigcup_{i=1}^{m-1} S_i^* \right)| = u \right] e^{2np_p p_{\mathrm{np}} \ln n}.$$ (76)

Denoting $|\bigcup_{i=1}^{m-1} S_i^*|$ by $v$, then we obtain that for $u \in [\max\{0, K_n + v - P_n\}, K_n]$, $P \left[ |S_m^* \cap \left( \bigcup_{i=1}^{m-1} S_i^* \right)| = u \right] = \binom{m}{u} \left( \frac{P_n - v}{P_n} \right)^u \left( \frac{K_n}{K_n - u} \right)^{K_n - u}.$ (77)

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

L.H.S. of (77)

$$\leq \binom{mK_n}{u} \left( \frac{P_n - K_n}{K_n - u} \right)^{K_n - u} \frac{K_n!}{u!} \left( \frac{P_n - K_n}{P_n} \right)^{P_n - K_n}$$

$$\leq \frac{1}{u!} \left( \frac{mK_n}{P_n - K_n} \right)^u.$$

(78)

For $u \notin [\max\{0, K_n + v - P_n\}, K_n]$, L.H.S. of (77) equals 0. Then from (76) and (78),

R.H.S. of (76) $\leq \sum_{u=0}^{K_n} \frac{1}{u!} \left( \frac{mK_n}{P_n - K_n} \right)^u e^{2np_p p_{\mathrm{np}} \ln n}$

$$\leq e^{mK_n^2/p_n - K_n} e^{2np_p p_{\mathrm{np}} \ln n}.$$ (79)

By $\frac{K_n^2}{p_n} = o(1)$ and Lemma 2 of [22],

$$\frac{K_n^2}{P_n - K_n} \leq \frac{K_n^2}{\frac{1}{n} \left[ 1 + o(1) \right]} = \left( \frac{n}{q} p_{s,q} \right)^{\frac{1}{2}} \cdot \left[ 1 + o(1) \right].$$ (80)

For $n$ sufficiently large, from $p_n \geq n^{-\delta}(\ln n)^{-1}$ and (52) (i.e., $p_{c,q} = p_{n} p_{s,q} \leq \frac{2\ln n}{n}$), we have

$$p_{s,q} = p_{n}^{-1} p_{c,q} \leq p_{n}^{-1} 2n^{-1} \ln n \leq 2n^{-\delta - 1}(\ln n)^{2}. (81)$$

From (80) and (81),

$$\frac{K_n^2}{P_n - K_n} \leq \left[ \frac{n}{q} 2n^{-\delta - 1}(\ln n)^{2} \right]^\frac{1}{2} \cdot \left[ 1 + o(1) \right] \leq 3q \cdot n^{-\frac{1}{2}}.$$ (82)

Given $K_n = \omega(1)$, for arbitrary constant $c > q$ and for all $n$ sufficiently large, $\frac{K_n^2}{P_n - K_n} \geq \frac{2c q m}{(e - q)(1 - q)}$ holds. Then

$$e^{2np_p p_{\mathrm{np}} \ln n} \leq e^{\left( \frac{c q m}{(e - q)(1 - q)} \right) \ln n}.$$ (83)

The use of (79) (82) and (83) in (76) yields

$$H_{n,m}/H_{n,m-1} \leq \text{R.H.S. of (76)} \leq e^{3q m \cdot \frac{1}{2} \ln (\ln n)^{2}} \leq \left( \frac{3q}{n} \right)^{\frac{1}{2}}.$$ (84)

To derive $H_{n,m}$ iteratively based on (84), we compute $H_{n,2}$ below. By definition, setting $m = 2$ in L.H.S. of (74) and considering the independence between events $(S_1 = S_1^*)$ and $(S_2 = S_2^*)$, we gain

$$H_{n,2} \leq \sum_{S_1 \in S_1^*} \sum_{S_2 \in S_2^*} P[S_1 = S_1^*] e^{np_p p_{\mathrm{np}} |S_1^* \cap S_2^*|}.$$ (85)

Clearly, $\sum_{S_2 \in S_2^*} P[S_2 = S_2^*] e^{np_p p_{\mathrm{np}} |S_1^* \cap S_2^*|}$ equals R.H.S. of (76) with $m = 2$. Then from (84) and (85),

$$H_{n,2} \leq \sum_{S_1 \in S_1^*} P[S_1 = S_1^*] e^{2np_p p_{\mathrm{np}} \ln (\ln n)^{2}} = e^{6q m \cdot \frac{1}{2} \ln (\ln n)^{2}}.$$ (86)

Therefore, it holds via (84) and (86) that

$$H_{n,m} \leq \left( \frac{3q}{n} \right)^{\frac{1}{2}} + \left( \frac{6q}{m^2 + m - 2n} \right)^{\frac{1}{2}} (\ln n)^{\frac{1}{2}}.$$ (87)

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

$$H_{n,m} \leq \max \left\{ e^{m^{2} \delta^{2}}, e^{2q m \cdot m + m - 2n} \right\}$$

With $n \to \infty$, $H_{n,m} \leq 1 + o(1)$ (i.e., (74)) follows.

**VIII. THE PROOF OF PROPOSITION 2**

We define $C_m$ and $\tau_m$ by

$$C_m^{(0)} \left( \begin{array}{c} 0, 0, \ldots, 0 \end{array} \right),$$

and

$$\tau_m^{(0)} = \{ T_m \mid |S_i \cap S_j| < q, \forall i, j \text{ with } 1 \leq i < j \leq m \}. $$
Clearly, \( C_m = C_m^{(0)} \) or \( T_m \in T_m^{(0)} \) each implies \( (C_m \in L_m^{(0)}) \). Also, \( (C_m = C_m^{(0)}) \) and \( (M_m = M_m^{(0)}) \) are independent with each other. Therefore, with (58) = \( P \left[ \{ C_m \in C_m^{(0)} \} \cap \{ M_m = M_m^{(0)} \} \right] \), we get
\[
(58) \geq \mathbb{P}[C_m = C_m^{(0)}] \mathbb{P}[M_m = M_m^{(0)}],
\]
with function \( f \) specified in (61). From (63),
\[
f(n-m, M_m^{(0)}) = \frac{(n-m)!}{(n-m-hm)!} \sim (h!)^{-m} n^{-hm}.
\]

We will establish
\[
\sum_{T_m \in T_m^{(0)}} \left\{ \mathbb{P}[T_m = T_m^*] \prod_{i=1}^{m} \mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} | T_m = T_m^*] \right\} 
\geq p_{e,q}^{-hm} \cdot [1 - o(1)].
\]

We use (96) and (97) as well as Lemma 3 of [22] in evaluating \( \mathbb{P}[M_m = M_m^{(0)}] \) above. Then
\[
\mathbb{P}[M_m = M_m^{(0)}] 
\geq (h!)^{-m} n^{-hm} \cdot [1 - o(1)] \cdot (1 - m p_{e,q})^n 
\times \sum_{T_m \in T_m^{(0)}} \mathbb{P}[T_m = T_m^*] \prod_{i=1}^{m} \mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} | T_m = T_m^*] 
\geq (h!)^{-m} (n p_{e,q})^h n^{-hm} \cdot [1 - o(1)].
\]

Substituting (72) (96) above and Lemma 3 of [22] into the computation of \( \mathbb{P}[M_m = M_m^{(0)}] \) yields
\[
\mathbb{P}[M_m = M_m^{(0)}] 
\leq [1 - o(1)] \cdot (1 - m p_{e,q})^n 
\times \sum_{T_m \in T_m^{(0)}} \mathbb{P}[T_m = T_m^*] \prod_{i=1}^{m} \mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} | T_m = T_m^*] 
\leq (h!)^{-m} n^{-hm} p_{e,q}^{-hm} \cdot [1 + o(1)].
\]

Substituting (91) and (92) into (87), and applying (90) and (92) to (88), we have
\[
(58) \geq (1 - m p_{s,q} \cdot m^2/2) \cdot [1 - o(1)].
\]

From (91), we get
\[
(58) \leq \mathbb{P}[M_m \in M_m^{(0)}] 
\leq (h!)^{-m} (n p_{e,q})^h n^{-hm} \cdot [1 + o(1)].
\]

Combining (93) and (94), and using \( \min\{p_{s,q} \cdot p_n \} \leq \sqrt{p_{s,q} \cdot p_n} \leq \sqrt{2 \ln n \over m} \leq o(1) \) which holds from \( p_{s,q} = p_s \cdot p_n \) and (52), Proposition 2 follows. Below we detail the proofs of (91) and (92).

\textbf{A. Establishing (91)}

We have
\[
\mathbb{P}[M_m = M_m^{(0)}] = \sum_{T_m \in T_m^{(0)}} \left\{ \mathbb{P}[T_m = T_m^*] \mathbb{P}\left[ (M_m = M_m^{(0)}) \mid (T_m = T_m^*) \right] \right\},
\]
where
\[
\mathbb{P}\left[ (M_m = M_m^{(0)}) \mid (T_m = T_m^*) \right] = f(n-m, M_m^{(0)}) \mathbb{P}[w \in M_{0^{m-1},1,0^{m-i}} | T_m = T_m^*] \cdot n^{-hm} 
\times \prod_{i=1}^{m} \mathbb{P}[w \in M_{0^{i-1},1,0^{m-i}} | T_m = T_m^*]^h,
\]

\[
\mathbb{P}[M_m = M_m^{(0)}] \leq \left( \frac{m}{2} \right) p_n \cdot \mathbb{P}[T_m \in T_m] \sum_{1 \leq i \leq m} |S_{ij}^*| \cdot \sum_{i=1}^{m} |S_{ij}^*| = o(1).
\]

Clearly, \( |S_{ij}^*| \leq K_n \). If \( T_m \in T_m^{(0)} \), it further holds that \( |S_{ij}^*| < q \). Consequently, from (90), \( p_n \cdot \mathbb{P}[T_m \in T_m^{(0)}] \leq \frac{2 \ln n}{m} \), the proof of (100) becomes evident by

\textbf{L.H.S. of (100)}
\[
\leq \left( \frac{m}{2} \right) p_n \cdot \mathbb{P}[T_m \in T_m \setminus T_m^{(0)}] + q \cdot \frac{p_n}{K_n} \cdot \mathbb{P}[T_m \in T_m^{(0)}] 
\leq m^2/2 \cdot p_n \cdot m^2 p_{s,q}/2 + \frac{q}{K_n}.
\]
\[ \leq m^4 n^{-1} \ln n/2 + o(1) \]
\[ \rightarrow 0, \text{ as } n \rightarrow \infty. \]

**B. Establishing (92)**

We have

\[
P\left( \left\{ \mathcal{M}_m = \mathcal{M}_m^0 \right\} \cap \{ T_m \in \mathcal{T}_m^0 \} \right) = \sum_{T_m \in \mathcal{T}_m^0} \left\{ \mathbb{P}[T_m = T_m^\ast] \mathbb{P}\left[ \left( \mathcal{M}_m = \mathcal{M}_m^0 \right) \mid (T_m = T_m^\ast) \right] \right\},
\]

where \( \mathbb{P}\left[ \left( \mathcal{M}_m = \mathcal{M}_m^0 \right) \mid (T_m = T_m^\ast) \right] \) as given by (95) equals

\[
f(n - m, \mathcal{M}_m^0) \mathbb{P}[w \in M_0m \mid T_m = T_m^\ast]^{n - m - h_m} \times \prod_{i=1}^{m} \left\{ \mathbb{P}[w \in M_0^{i-1}, 1, 0, m - i \mid T_m = T_m^\ast]^{h_m} \right\},
\]

with \( f(n - m, \mathcal{M}_m^0) \) computed in (96). For \( T_m^\ast \in \mathcal{T}_m^0 \), from \( |S_{ij}^\dagger| < q \) and Lemma 3 of [22], we derive

\[
\mathbb{P}[w \in M_0^{i-1}, 1, 0, m - i \mid T_m = T_m^\ast] \geq p_{e,q} \left[ 1 - (q + 2)!m(p_{e,q})^{\frac{1}{m}} - \frac{q m}{K_n} \right].
\]

Substituting (96) (102) above and Lemma 3 of [22] into (101), we conclude that

\[
\mathbb{P}\left( \left\{ \mathcal{M}_m = \mathcal{M}_m^0 \right\} \cap \{ T_m \in \mathcal{T}_m^0 \} \right) \geq \mathbb{P}[T_m \in \mathcal{T}_m^0] \cdot (h!)^{-m n^m} \cdot \left[ 1 - o(1) \right] \\
\times (1 - m p_{e,q})^{n - m - h_m} p_{e,q}^{h_m} \\
\times \left[ 1 - (q + 2)!m(p_{e,q})^{\frac{1}{m}} - \frac{q m}{K_n} \right]^{h_m} \\
\sim (h!)^{-m (n p_{e,q})^{h_m} e^{-m n p_{e,q}}}. \]

**IX. Experimental Results**

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

In Figure 1, we depict the probability that graph \( G_q(n, K, P, p) \) has a minimum node degree at least \( k \) as a function of \( K \) for \( n = 2, 000, q = 2, P = 10, 000, \) and \( p = 0.8 \).

In Figure 2, we depict the probability that graph \( G_q(n, K, P, p) \)’s minimum node degree equals \( k \) exactly as a function of \( K \) for \( k = 0, 1, 2, 3, 4, 5 \) with \( n = 3000, q = 2, P = 100000, \) and \( p = 0.5 \).

\[ \alpha_n \text{ as } \alpha \text{ here as } \alpha \text{ is fixed}; \text{i.e., } p_{e,q} = \frac{\ln n + (k - 1) \ln \ln n + \alpha}{n}. \]

Then given Remark 1 after Theorem 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 \( e^{-\frac{a_n}{(k - 1)}} \). The observation that the simulation and the analytical curves in Figure 1 are close is in accordance with Theorem 1.

In Figures 1 and 3, the curves with legends labelled “(E)” are experimental curves produced from experiments, while the curves with legends labelled “(A)” are analytical curves generated from theoretical analysis. In Figure 2, we depict the probability that graph \( G_q(n, K, P, p) \)’s minimum node degree equals \( k \) exactly as a function of \( K \) for \( k = 0, 1, 2, 3, 4, 5 \) with \( n = 3000, q = 2, P = 100000, \) and \( p = 0.5 \).

For the experimental curves, we generate 2000 independent samples of graph \( G_q(n, K, P, p) \) and record the count (out of a possible 2,000) that the minimum degree of graph \( G_q(n, K, P, p) \) is no less than \( k \). Then the empirical probabilities are obtained by dividing the counts by 2,000. On the other hand, we approximate the analytical curves of Figure 1 by the asymptotic results as explained below. First, we compute the corresponding probability of \( p_{e,q} \) in \( G_q(n, K, P, p) \) through \( p_{e,q} = p \cdot \sum_{u=0}^{K} [K_u] (P-K_u)/[K] \) given (8) and \( P > 2K \). Then we determine \( \alpha \) by (9) (we write
ZHAO: TOPOLOGICAL PROPERTIES OF SECURE WSNs UNDER THE $q$-COMPOSITE KEY PREDISTRIBUTION SCHEME

Fig. 3. A plot of the probability distribution for the number of nodes with degree $h$ for $h = 0, 1, 2$ in graph $G_q(n, K, P, p)$ with $n = 3000$, $q = 2$, $P = 10000$, $K = 35$ and $p = 0.5$.

$\ell^* = \arg \min_{\ell \in \text{integer}} \ell \left\{ \text{peq} \cdot \frac{\ln n + (\ell - 1) \ln \ln n}{\ln n} \right\}$ and further define $\gamma^*$ such that $peq = e^{-n \gamma^* \ln \ln n}$ for $k = \ell^*$, equals $1 - e^{-n \gamma^*}$ for $k = \ell^* - 1$, and equals 0 for $k \neq \ell^* - 1$, and ii) if $\ell^* \leq 0$, then $P[\delta = k]$ equals 1 for $k = 0$, and equals 0 for $k \neq 0$. The observation that the curves generated from the experimental and the analytical curves are close to each other confirms the result on the distribution of the minimum degree in Theorem 2.

In Figure 3, we plot the probability distribution for the number of nodes with degree $h$ in graph $G_q(n, K, P, p)$ for $h = 0, 1, 2$ from both the experiments and the analysis. We set $n = 3000$, $q = 2$, $K = 35$, $P = 10000$, and $p = 0.5$. On the one hand, for the experiments, we generate 2000 independent samples of $G_q(n, K, P, p)$ and record the count (out of a possible 2000) 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 2000. On the other hand, we approximate the analytical curves by the asymptotic results as explained below.

In Theorem 3, we establish that the number of nodes in $G_q(n, K, P, p)$ with degree $h$ approaches a Poisson distribution with mean $\lambda_{n, h} = n(h!)^{-1} (np_{eq})^h e^{-np_{eq}}$ as $n \to \infty$. We derive $\lambda_{n, h}$ by computing the corresponding probability of $peq$ in $G_q(n, K, P, p)$ through $peq = p \cdot \{1 - \sum_{h=1}^{\ell} \binom{K}{h} \frac{(P-K)^h}{(P)^h}\}$ as explained above. Then for each $h$, we plot a Poisson distribution with mean $\lambda_{n, h}$ as the curve corresponding to the analysis. In Figure 3, we observe that the curves generated from the experiments and those obtained by the analysis are close to each other, confirming the result on asymptotic Poisson distribution in Theorem 3.

X. RELATED WORK

Erdős and Rényi [21] 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 [21] derive the asymptotically exact probabilities for connectivity and 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 [26], 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.

Recall that graph $G_q(n, K, P, p)$ models the topology of the $q$-composite key predistribution scheme [27]–[29]. For graph $G_q(n, K, P, p)$, Bloznelis et al. [4] demonstrate that a connected component with at least a constant fraction of $n$ emerges asymptotically when probability $peq$ exceeds $1/n$. Recently, still for $G_q(n, K, P, p)$, Bloznelis [14] establishes the asymptotic Poisson distribution for the number of nodes with any degree. Our results in Theorem 3 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 3.

Yağan [5] presents zero-one laws in graph $G_1$ (our graph $G_q$ in the case of $q = 1$) for connectivity and for the property that the minimum degree is at least 1. Zhao et al. extend Yağan’s results to general $k$ for $G_1$ in [3], [20]. Our results in this paper apply to general $q$, yet the corresponding results for $q = 1$ are already stronger than those in [3], [5], and [20].

Krzywdziński and Rybarczyk [7] and Krishnan et al. [16] 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 [7], [16], [30], [31], 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.

XI. CONCLUSION

In this paper, we analyze topological properties in secure wireless sensor networks (WSNs) operating under the $q$-composite key predistribution scheme with unreliable links modeled as on/off channels. Our analytical results provide useful guidelines for designing secure WSNs. Experiments are shown to be in agreement with our theoretical findings. A future research direction is to consider communication models different from the on/off channel model.

REFERENCES

[1] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. IEEE Symp. Secur. Privacy, May 2003, pp. 197–213.
[2] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 41–47.

[3] J. Zhao, O. Yağan, and V. Gligor, “k-Connectivity in random key graphs with unreliable links,” IEEE Trans. Inf. Theory, vol. 61, no. 7, pp. 3810–3836, Jul. 2015.

[4] M. Bloznelis, J. Jaworski, and K. Rybarczyk, “Component evolution in a secure wireless sensor network.” Network, vol. 53, pp. 19–26, Jan. 2009.

[5] O. Yağan, “Performance of the Eschenauer–Gligor key distribution scheme under an ON/OFF channel,” IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 3821–3835, Jun. 2012.

[6] J. Zhao, “On resilience and connectivity of secure wireless sensor networks under node capture attacks,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 557–571, Mar. 2017.

[7] K. Krzywdziński and K. Rybarczyk, “Geometric graphs with randomly deleted edges — connectivity and routing protocols,” in Proc. Math. Found. Comput. Sci., Aug. 2011, pp. 544–555.

[8] K. Rybarczyk, “Diameter, connectivity, and phase transition of the uniform random intersection graph,” Discrete Math., vol. 311, no. 17, pp. 1998–2019, 2011.

[9] F. Gandino, R. Ferrari, and M. Rebaudengo, “A key distribution scheme for mobile wireless sensor networks: q-s-composite,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 34–47, Jan. 2017.

[10] O. Yağan and A. M. Makowski, “Zero–one laws for connectivity in random key graphs,” IEEE Trans. Inf. Theory, vol. 58, no. 5, pp. 2983–2999, May 2012.

[11] J. Zhao, “On the resilience to node capture attacks of secure wireless sensor networks,” in Proc. 53rd Ann. Allerton Conf. Commun., Control, Comput. (Allerton), Sep. 2015, pp. 887–893.

[12] S. E. Nikoletseas and C. L. Raptopoulos, “On some combinatorial properties of random intersection graphs,” in Algorithms, Probability, Networks, and Games, Cham, Switzerland: Springer, 2015, pp. 370–383.

[13] J. Zhao, “Modeling interest-based social networks: Superimposing Erdos–Renyi graphs over random intersection graphs,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Mar. 2017.

[14] M. Bloznelis, “Degree and clustering coefficient in sparse random intersection graphs,” Ann. Appl. Probab., vol. 23, no. 3, pp. 1254–1289, 2013.

[15] J. Ding, A. Bouabdallah, and V. Tarokh, “Key pre-distributions from graph-based block designs,” IEEE Sensors J., vol. 16, no. 6, pp. 1842–1850, Mar. 2016.

[16] B. S. Krishnan, A. Ganesh, and D. Manjunath, “On connectivity thresholds in superposition of random key graphs on random geometric graphs,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2013, pp. 2389–2393.

[17] J. Zhao, “Designing secure networks with q-composite key predistribution under different link constraints,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Mar. 2017.

[18] E. M. Shahriar, M. Pirani, and S. Sundaram, “Robustness and algebraic connectivity of random interdependent networks,” IFAC-PapersOnLine, vol. 48, no. 22, pp. 252–257, 2015.

[19] S. M. Dibaji and I. Hishii, “Consensus of second-order multi-agent systems in the presence of locally bounded faults,” Syst. Control Lett., vol. 79, pp. 23–29, May 2015.

[20] J. Zhao, O. Yağan, and V. Gligor, “Secure k-connectivity in wireless sensor networks under an on/off channel model,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2013, pp. 2790–2794.

[21] P. Erdős and A. Rényi, “On random graphs. I,” Publicationes Math. (Debrecen), vol. 6, no. 1, pp. 290–297, 1959.

[22] J. Zhao. (2016). Topological Properties of Secure Wireless Sensor Networks Under The q-Composite Key Predistribution Scheme With Unreliable Links. [Online]. Available: https://sites.google.com/site/workofzhao/qcomposite.pdf

[23] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, “Redoubletable sensor networks,” ACM Trans. Inf. Syst. Security, vol. 11, no. 3, pp. 13:1–13:22, 2008.

[24] J. Zhao, “Topology control in secure wireless sensor networks,” in Cyber Security for Industrial Control Systems: From The Viewpoint of Close-Loop, P. Cheng, H. Zhang, and J. Chen, Eds. Boca Raton, FL, USA: CRC Press, 2016, ch. 8, pp. 183–224.

[25] A. DasGupta, “Asymptotic theory of statistics and probability,” in Springer Texts in Statistics, vol. 17. New York, NY, USA: Springer, 2008.

[26] P. Erdős and A. Rényi, “On the strength of connectedness of a random graph,” Acta Math. Acad. Sci. Hungarice, vol. 12, nos. 1–2, pp. 261–267, 1961.

[27] J. Zhao, O. Yağan, and V. Gligor, “On k-connectivity and minimum vertex degree in random s-intersection graphs,” in Proc. ACM-SIAM Meeting Anal. Algorithmics Combinat. (ANALCO), Jan. 2015, pp. 1–15.

[28] M. Farrel et al., “Hyperbolicity, degeneracy, and expansion of random intersection graphs,” in Proc. Int. Workshop Algorithms Models Web-Graph, 2015, pp. 29–41.

[29] D. H. Yum and P. J. Lee, “Exact formulae for resilience in random key predistribution schemes,” IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1638–1642, May 2012.

[30] J. Zhao, O. Yağan, and V. Gligor, “Connectivity in secure wireless sensor networks under transmission constraints,” in Proc. 52nd Annu. Allerton Conf. Commun., Control, Comput., Sep. 2014, pp. 1294–1301.

[31] J. Pandey and B. Gupta, “Distribution of k-connectivity in the secure wireless sensor network,” in Proc. Int. Conf. Recent Adv. Innov. Eng. (ICRAIE), May 2014, pp. 1–6.