Exact Analysis of \( k \)-Connectivity in Secure Sensor Networks with Unreliable Links

Jun Zhao  
CyLab and Dept. of ECE  
Carnegie Mellon University  
Email: junzhao@cmu.edu

Osman Yağan  
CyLab and Dept. of ECE  
Carnegie Mellon University  
Email: oyagan@ece.cmu.edu

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

Abstract—The Eschenauer–Gligor (EG) random key predistribution scheme has been widely recognized as a typical approach to secure communications in wireless sensor networks (WSNs). However, there is a lack of precise probability analysis on the reliable connectivity of WSNs under the EG scheme. To address this, we rigorously derive the asymptotically exact probability of \( k \)-connectivity in WSNs employing the EG scheme with unreliable links represented by independent on/off channels, where \( k \)-connectivity ensures that the network remains connected despite the failure of any \((k−1)\) sensors or links. Our analytical results are confirmed via numerical experiments, and they provide precise guidelines for the design of secure WSNs that exhibit a desired level of reliability against node and link failures.

Index Terms—Connectivity, key predistribution, minimum degree, random graphs, security, wireless sensor networks.

I. INTRODUCTION

The Eschenauer–Gligor (EG) random key predistribution scheme [4] has been widely regarded as a typical solution to secure communications in wireless sensor networks (WSNs) [5], [6], [7], [8], [9], [10], [12], [15]. The scheme operates as follows. In a WSN with \( n \) sensors, before deployment, each sensor is independently assigned \( K_n \) distinct keys which are selected uniformly at random from a pool of \( P_n \) keys, where \( K_n \) and \( P_n \) are both functions of \( n \). After deployment, any two sensors can securely communicate over an existing wireless link if and only if they share at least one key.

Wireless links between nodes may become unavailable due to the presence of physical barriers between nodes or because of harsh environmental conditions severely impairing transmission. We model unreliable links as independent channels, each being on with probability \( p_n \) or being off with probability \((1−p_n)\), where \( p_n \) is a function of \( n \) for generality. Such on/off channel model has been used in the context of secure WSNs [9], [15], [12], and is shown to well approximate the disk model [5], [6], [9], [15], [12], where any two nodes need to be within a certain distance to establish a wireless link in between.

Given the randomness involved in the EG key predistribution scheme, and the unreliability of wireless links, there arises a basic question as to how one can adjust the EG scheme parameters \( K_n \) and \( P_n \), and the link parameter \( p_n \), so that the resulting network is securely and reliably connected. Reliability against the failure of sensors or links is particularly important in WSN applications where sensors are deployed in hostile environments (e.g., battlefield surveillance), or, are unattended for long periods of time (e.g., environmental monitoring), or, are used in life-critical applications (e.g., patient monitoring). To answer the question above, this paper presents the asymptotically exact probability of \( k \)-connectivity in secure WSNs under the EG scheme with unreliable links. A network (or a graph) is said to be \( k \)-connected if it remains connected despite the deletion of any \((k−1)\) nodes or links. An equivalent definition is that each node can find at least \( k \) internally node-disjoint paths to any other node. With \( k = 1 \), \( k \)-connectivity simply means connectivity.

Our result on the asymptotically exact probability of \( k \)-connectivity complements a zero-one law established in our prior work [15], [12], and is significant to obtain a precise understanding of the connectivity behavior of secure WSNs. First, with the zero-one law, one is only provided with design choices which lead to networks that are \( k \)-connected with high probability or to that are not \( k \)-connected with high probability, where an event happens “with high probability” if its probability asymptotically converges to 1. Given the trade-offs involved between connectivity, security and memory load [4], [9], it would be more useful to have a complete picture by obtaining the asymptotically exact probability of \( k \)-connectivity. In addition, there may be situations where the network designer is interested in having a guaranteed level of \( k \)-connectivity (one-laws would provide conditions for that) but may also be interested in having some level of \( k \)-connectivity without such guarantees (one-laws would fail short in providing this). Our result fills this gap. Finally, it is not possible to determine the width of the phase transition from zero-one laws; the width of the phase transition is often calculated by the difference in parameters that it takes to increase the probability of \( k \)-connectivity from \( \epsilon \) to \((1−\epsilon)\), for some \( \epsilon < 0.5 \). In other words, it is not clear from zero-one laws how sensitive the probability of \( k \)-connectivity is to the variations in the EG scheme parameters \( K_n \) and \( P_n \), and the link parameter \( p_n \). By providing the asymptotically exact probability of \( k \)-connectivity, our findings provide a clear picture of these intricate relationships.

The rest of the paper is organized as follows. We describe the system model in Section II. Section III presents the main results as Theorem 1, which is established in Section IV. In Section VI, we present numerical experiments that confirm our analytical findings. Afterwards, Section VII surveys related work, and Section VIII concludes the paper. The Appendix presents a few useful lemmas and their proofs.

II. SYSTEM MODEL

We now explain the system model. Consider a WSN with \( n \) sensors operating under the EG scheme and with wireless
links modeled by independent on/off channels. Let a node set $V = \{v_1, v_2, \ldots, v_n\}$ represent the $n$ sensors. According to the EG scheme, each node $v_i \in V$ is independently assigned a set (denoted by $S_i$) of $K_n$ distinct cryptographic keys, which are selected uniformly at random from a key pool of $P_n$ keys. Any pair of nodes can then secure an existing communication link as long as they have at least one key in common.

The EG scheme results in a random key graph [1], [7], [10], also known as a uniform random intersection graph. This graph denoted by $G(n, K_n, P_n)$ is defined on the node set $V$ such that any two distinct nodes $v_i$ and $v_j$ have an edge in between, an event denoted by $\Gamma_{ij}$, if and only if they share at least one key. Thus, the event $\Gamma_{ij}$ means $(S_i \cap S_j \neq \emptyset)$.

Under the on/off channel model for unreliable links, each wireless link is independently being on with probability $p_n$ or being off with probability $\left(1 - p_n\right)$. Defining $C_{ij}$ as the event that the channel between $v_i$ and $v_j$ is on, we have $\mathbb{P}[C_{ij}] = p_n$, with $\mathbb{P}[A]$ throughout the paper meaning the probability that event $A$ happens. The on/off channel model induces an Erdős-Rényi graph $G(n, p_n)$ [2] defined on the node set $V$ such that $v_i$ and $v_j$ have an edge in between if $C_{ij}$ takes place.

Finally, we denote by $\mathcal{G}(n, K_n, P_n, p_n)$ the underlying graph of the $n$-node WSN under the EG scheme with unreliable links. We often write $\mathcal{G}$ rather than $\mathcal{G}(n, K_n, P_n, p_n)$ for brevity. Graph $\mathcal{G}$ is defined on the node set $V$ such that there exists an edge between nodes $v_i$ and $v_j$ if events $\Gamma_{ij}$ 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 $\mathcal{G}$ is the intersection of $G(n, K_n, P_n)$ and $G(n, p_n)$: $\mathcal{G} = G(n, K_n, P_n) \cap G(n, p_n)$. (1)

We define $s_n$ as the probability that two distinct nodes share at least one key and $q_n$ as the probability that two distinct nodes have an edge in between in graph $\mathcal{G}$. Clearly, $s_n$ and $q_n$ both depend on $K_n$ and $P_n$, while $q_n$ depends also on $p_n$. As shown in previous work [1], [7], [10], $s_n$ is determined through

$$s_n = \mathbb{P}[\Gamma_{ij}] = \begin{cases} 1 - \left(\frac{p_n - K_n}{P_n}\right)/\left(\frac{P_n}{K_n}\right), & \text{if } P_n > 2K_n, \\ 1, & \text{if } P_n \leq 2K_n. \end{cases}$$

Then by the independence of $C_{ij}$ and $\Gamma_{ij}$, we have

$$q_n = \mathbb{P}[E_{ij}] = \mathbb{P}[C_{ij}] \cdot \mathbb{P}[\Gamma_{ij}] = p_n \cdot s_n.$$ (2)

$$= \begin{cases} p_n \cdot \left(1 - \left(\frac{p_n - K_n}{P_n}\right)/\left(\frac{P_n}{K_n}\right)\right), & \text{if } P_n > 2K_n, \\ p_n, & \text{if } P_n \leq 2K_n. \end{cases}$$ (3)

III. THE MAIN RESULTS

We present the main results below. Throughout the paper, $k$ is a positive integer and does not scale with $n$, and $e$ is the base of the natural logarithm function, $\ln$. We use the standard asymptotic notation $o(\cdot)$, $O(\cdot)$, $\omega(\cdot)$, $\Omega(\cdot)$, $\Theta(\cdot)$ and $\sim$; in particular, for two positive sequences $a_n$ and $b_n$, the relation $a_n \sim b_n$ means $\lim_{n \to \infty} a_n/b_n = 1$.

Theorem 1. For graph $\mathcal{G}(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$ and $K_n^2/P_n = o(1)$, with $q_n$ denoting the edge probability and a sequence $\alpha_n$ defined through

$$q_n = \frac{\ln n + (k - 1) \ln \ln n + n \alpha_n}{n},$$ (4)

if $\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, \infty)$, then as $n \to \infty$, $\mathbb{P}[\text{Graph } \mathcal{G}(n, K_n, P_n, p_n) \text{ is } k\text{-connected.}] \to e^{-\frac{e^{-\alpha^*}}{k!}}$.

Theorem 1 provides the asymptotically exact probability of $k$-connectivity in graph $\mathcal{G}$. Its proof is given in the next section. From (3), for all $n$ sufficiently large, under $P_n > 2K_n$ which is clearly implied by the condition $K_n^2/P_n = o(1)$, the edge probability $q_n$ in graph $\mathcal{G}$ is given by the expression $\left[1 - \left(\frac{P_n - K_n}{P_n}\right)/\left(\frac{P_n}{K_n}\right)\right]$. With a much simpler approximation $p_n \cdot K_n^2/P_n$ for $q_n$, we present below a corollary of Theorem 1.

Corollary 1. For graph $\mathcal{G}(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$ and $K_n^2/P_n = o\left(\frac{1}{\ln n}\right)$, with a sequence $\beta_n$ defined through

$$p_n \cdot \frac{K_n^2}{P_n} = \ln n + (k - 1) \ln \ln n + \beta_n,$$

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

$$\mathbb{P}[\text{Graph } \mathcal{G}(n, K_n, P_n, p_n) \text{ is } k\text{-connected.}] \to e^{-\frac{e^{-\beta^*}}{k!}}.$$ (5)

Setting $p_n = 1$ in Theorem 1 and Corollary 1, we obtain the corresponding results for random key graph $G(n, K_n, P_n)$ in view of (1). Furthermore, we can use monotonicity arguments [15] to derive the zero-one laws for $k$-connectivity in graph $\mathcal{G}$. Specifically, under the conditions of Theorem 1 (resp., Corollary 1), graph $\mathcal{G}$ is $k$-connected with high probability if $\lim_{n \to \infty} \alpha_n = \infty$ (resp., $\lim_{n \to \infty} \beta_n = \infty$), and is not $k$-connected with high probability if $\lim_{n \to \infty} \alpha_n = -\infty$ (resp., $\lim_{n \to \infty} \beta_n = -\infty$). The arguments are straightforward from our work [15] and are omitted here due to space limitation.

Before establishing Corollary 1 using Theorem 1, we explain the practicality of the conditions in Theorem 1 and Corollary 1: $P_n = \Omega(n), K_n^2/P_n = o(1)$ and $K_n^2/P_n = o\left(\frac{1}{\ln n}\right)$, the first condition indicates that the key pool size $P_n$ should grow at least linearly with $n$, which holds in practice [4], [10], [9].

The second condition $K_n^2/P_n = o(1)$ and $K_n^2/P_n = o\left(\frac{1}{\ln n}\right)$ (note that the latter implies the former) are also practical in secure sensor network applications since $P_n$ is expected to be several orders of magnitude larger than $K_n$ [4], [10], [9].

We now prove Corollary 1 using Theorem 1. We have the conditions of Corollary 1: $P_n = \Omega(n), K_n^2/P_n = o(1)$, and $\lim_{n \to \infty} \beta_n = \beta^* \in (-\infty, \infty)$. First, it is clear that $\beta_n = \beta^* + o(1)$. Under $K_n^2/P_n = o\left(\frac{1}{\ln n}\right)$, it holds that $s_n = \frac{K_n^2}{P_n} \cdot \left[1 + O\left(\frac{K_n^2}{P_n}\right)\right]$. In view of (1), we see from (2) and (5) that $q_n = p_n \cdot s_n = p_n \cdot \frac{K_n^2}{P_n} \cdot \left[1 + O\left(\frac{K_n^2}{P_n}\right)\right] = \ln n + (k - 1) \ln \ln n + \beta_n$, from [15, Lemma 8], it follows that

$$\mathbb{P}[\text{Graph } \mathcal{G}(n, K_n, P_n, p_n) \text{ is } k\text{-connected.}] \to e^{-\frac{e^{-\beta^*}}{k!}}.$$ (6)

With $\alpha_n$ defined by (4), we use (6) to derive $\alpha_n = \beta^* + o(1)$, which yields that $\alpha^*$ denoting $\lim_{n \to \infty} \alpha_n$ equals $\beta^*$. Then in view of $\alpha^* = \beta^*$ and that the conditions of Theorem 1 all hold given the conditions of Corollary 1 (note that $K_n^2/P_n = o\left(\frac{1}{\ln n}\right)$ implies $K_n^2/P_n = o(1)$), Corollary 1 follows from Theorem 1.

IV. ESTABLISHING THEOREM 1

For any graph, $k$-connectivity implies that its minimum degree is at least $k$, while the other way does not hold since a graph may have isolated components, each of which is $k$-connected within itself. However, for random graph $\mathcal{G}(n, K_n, P_n, p_n)$, as given by Lemma 1 below, we have shown it is unlikely under certain conditions that $\mathcal{G}(n, K_n, P_n, p_n)$ is not $k$-connected but has a minimum degree at least $k$. 
Lemma 2. ([15, Section IX]). For graph $G(n, K_n, P_n, p_n)$ under $P_n = \Omega(n)$, $K_n = o(1)$ and $q_n = o(1)$, it holds that

$$\mathbb{P}\left[\text{Graph } G \text{ is not } k\text{-connected, but has a minimum degree at least } k.\right] = o(1).$$

We show that the conditions in Lemma 1 all hold given the conditions of Theorem 1: $P_n = \Omega(n)$, $K_n = o(1)$ and $q_n = \frac{\ln(n + 1)}{n}\frac{1}{1 - \frac{1}{n}} + o(1)$ with $\lim_{n \to \infty} q_n = \alpha^* \in (-\infty, \infty)$. To see this, we only need to prove that $q_n = o(1)$ needed in Lemma 1 follows from the conditions of Theorem 1. Clearly, it holds that $|\alpha_n| = O(1)$ from $\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, \infty)$. Then in view of $|\alpha_n| = O(1)$ and the fact that $k$ does not scale with $n$, we obtain from (4) that

$$q_n \sim \frac{\ln n}{n},$$

which clearly implies $q_n = o(1)$.

From Lemma 1 and

$$\mathbb{P}\left[\text{Graph } G \text{ is } k\text{-connected.}\right] = \mathbb{P}\left[\text{Graph } G \text{ has a minimum degree at least } k.\right] - \mathbb{P}\left[\text{Graph } G \text{ is not } k\text{-connected, but has a minimum degree at least } k.\right],$$

Theorem 1 on $k$-connectivity of $G$ will be proved once we demonstrate Lemma 2 below on the minimum degree of $G$.

Lemma 2. Under the conditions of Theorem 1, it holds that

$$\lim_{n \to \infty} \mathbb{P}[\text{G has a minimum degree at least } k.] = e^{-\frac{\alpha_n}{1 - \alpha_n}}.$$  

To prove Lemma 2, we first show that the number of nodes in $G$ with a certain degree converges in distribution to a Poisson random variable. With $\phi_h$ denoting the number of nodes with degree $h$ in $G$, $h = 0, 1, \ldots$, we use the method of moments to prove that $\phi_h$ asymptotically follows a Poisson distribution with mean $\lambda_h$. Specifically, from [11, Theorem 7], it follows for any integers $h \geq 0$ and $\ell \geq 0$ that

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

since $\mathbb{P}[\text{Nodes } v_1, v_2, \ldots, v_m \text{ all have degree } h] \sim \lambda_h^m/n^m$, which is shown by Lemma 3 below with

$$\lambda_h = n(h!)^{-1}(nq_n)^{h/e(\alpha_n)}.$$  

Lemma 3. For graph $G$ under the conditions of Theorem 1, $\mathbb{P}[v_1, v_2, \ldots, v_m \text{ all have degree } h] \sim (h!)^{-m}(nq_n)^{hm/e(\alpha_n)}$ holds for any integers $m \geq 1$ and $h \geq 0$.

As explained above, Lemma 3 shows (8) with $\lambda_h$ given by (9). Then the proof of Lemma 2 will be completed once we establish Lemma 3 and the result that (8) implies Lemma 2. Below we will demonstrate that (8) implies Lemma 2, and then detail the proof of Lemma 3.

A. Proving that (8) implies Lemma 2

Recall that $\phi_h$ denotes the number of nodes with degree $h$ in graph $G$. With $\delta$ defined as the minimum degree of graph $G$, then the event $(\delta \geq k)$ is the same as $\bigcap_{h=0}^{k-1}(\phi_h = 0)$ (i.e., the event that no node has a degree falling in $\{0, 1, \ldots, k - 1\}$). Hence, we obtain

$$\mathbb{P}[\delta \geq k] = \mathbb{P}\left[\bigcap_{h=0}^{k-1}(\phi_h = 0)\right] \leq \mathbb{P}[\phi_{k-1} = 0],$$

and by the union bound, it holds that

$$\mathbb{P}[\delta \geq k] \geq \mathbb{P}[\phi_{k-1} = 0] - \sum_{h=0}^{k-2} \mathbb{P}[\phi_h \neq 0].$$  

To use (10) and (11), we compute $\mathbb{P}[\phi_h \neq 0]$ given (8) and thus evaluate $\lambda_h$ specified in (9). Applying (4) and (7) to (9), and considering $\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, \infty)$, we establish

$$\lambda_h = n(h!)^{-1}(nq_n)^{h/e(\alpha_n)}$$

$$= n(h!)^{-1}(1/n)^h e^{-\ln n - (k-1)\ln n - \alpha_n}$$

$$= (h!)^{-1}(1/n)^h e^{-\alpha_n}$$

$$\begin{cases} 0, & \text{for } h = 0, 1, \ldots, k - 2, \\ \frac{(e^{-\alpha_n})}{(k-1)!}, & \text{for } h = k - 1, \\ \infty, & \text{for } h = k, k + 1, \ldots. \\ \end{cases}$$

By (8) and (12), we derive that as $n \to \infty$,

$$\mathbb{P}[\phi_h = 0] \to \begin{cases} 1, & \text{for } h = 0, 1, \ldots, k - 2, \\ e^{-\alpha_n}, & \text{for } h = k - 1, \\ 0, & \text{for } h = k, k + 1, \ldots. \\ \end{cases}$$

Using (13) in (10) and (11), we obtain $\mathbb{P}[\delta \geq k] \to e^{-\alpha_n}$; i.e., Lemma 2 is proved.

B. Proving Lemma 3

We use $V_m$ to denote the node set $\{v_1, v_2, \ldots, v_m\}$. Lemma 3 evaluates the probability that each of $V_m$ has degree $h$. To compute such probability, we look at whether at least two of $V_m$ have an edge in between, and whether at least two of $V_m$ have at least one common neighbor. To this end, we define $P_1$ as the probability of event

$$\{ (\text{each of } V_m \text{ has degree } h) \}$$

$$\cap \{ \text{at least two of } V_m \text{ have an edge in between} \}$$

$$\cup \{ \text{at least two of } V_m \text{ have at least one common neighbor} \},$$

and define $P_2$ as the probability of event

$$\{ (\text{each of } V_m \text{ has degree } h) \}$$

$$\cap \{ \text{no two of } V_m \text{ have any edge in between} \}$$

$$\cup \{ \text{no two of } V_m \text{ have any common neighbor} \}.$$  

Then $\mathbb{P}[\text{each of } V_m \text{ has degree } h] = P_1 + P_2$. Thus, Lemma 3 will hold once we establish the following two propositions.

Proposition 1. Under the conditions of Theorem 1, it holds that

$$P_1 = o((h!)^{-m}(nq_n)^{hm/e(\alpha_n)}),$$

Proposition 2. Under the conditions of Theorem 1, it holds that

$$P_2 \sim (h!)^{-m}(nq_n)^{hm/e(\alpha_n)}.$$
Recalling $S_i$ as the key set on node $v_i$, we define a $m$-tuple $T_m$ through $T_m := (S_1, S_2, ..., S_m)$. Then we define $L_m$ as $L_m := (C_m, T_m)$. With $L_m$, we have the on/off states of all channels between nodes $v_1, v_2, ..., v_m$ and the key sets $S_1, S_2, ..., S_m$ on these $m$ nodes, so all edges between these $m$ nodes in graph $G$ are determined. Let $C_m, T_m$ and $L_m$ be the sets of all possible $C_m, T_m$ and $L_m$, respectively.

Now we further introduce some notation to characterize how nodes $v_1, v_2, ..., v_m$ have edges with nodes of $V_m$, where $V_m$ denotes $\{v_{m+1}, v_{m+2}, ..., v_n\}$. Let $N_i$ be the neighborhood set of node $v_i$, i.e., the set of nodes that have edges with $v_i$. We also define set $\overline{N}_i$ as the set $\{v_{m+1}, v_{m+2}, ..., v_n\} \setminus N_i$. Then we are ready to define sets $M_{j_1,j_2, ..., j_m}$ for all $j_1, j_2, ..., j_m \in \{0, 1\}$ which characterize the relationships between sets $N_i$ for $i = 1, 2, ..., m$. We define

$$M_{j_1,j_2, ..., j_m} := \bigcap_{i=1,2, ..., m; j_i = 1} N_i \cap \bigcap_{i=1,2, ..., m; j_i = 0} \overline{N}_i.$$  

(14)

In other words, for $i = 1, 2, ..., m$, if $N_i$ is not empty, each node in $N_i$ belongs to $M_{j_1,j_2, ..., j_m}$ if $j_i = 1$ and does not belong to $M_{j_1,j_2, ..., j_m}$ if $j_i = 0$. Also, if $j_1 = j_2 = ... = j_m = 0$, then $M_{j_1,j_2, ..., j_m} = \bigcap_{i=1}^m \overline{N}_i$. The sets $M_{j_1,j_2, ..., j_m}$ for $j_1, j_2, ..., j_m \in \{0, 1\}$ are mutually disjoint, and constitute a partition of the set $V_m$ (a partition is allowed to contain empty sets). By the definition of $M_{j_1,j_2, ..., j_m}$ for $j_1, j_2, ..., j_m \in \{0, 1\}$, we have

$$\sum_{j_1,j_2, ..., j_m \in \{0, 1\}} |M_{j_1,j_2, ..., j_m}| = |V_m| = n - m, \tag{15}$$

and

$$\sum_{j_1,j_2, ..., j_m \in \{0, 1\}; \sum_{i=1}^m j_i \geq 1} |M_{j_1,j_2, ..., j_m}| = \left| \bigcup_{i=1}^m N_i \right| \cap \overline{V}_m. \tag{16}$$

We further define $2^m$-tuple $M_m$ through

$$M_m = \{M_{j_1,j_2, ..., j_m} : j_1, j_2, ..., j_m \in \{0, 1\}\} = \{M_{00,0,0,0}, M_{00,0,0,1}, M_{00,0,1,0}, M_{00,0,1,1}, ..., M_{11,1,1,1}\},$$

where $|M_{j_1,j_2, ..., j_m}|$ means the cardinality of $M_{j_1,j_2, ..., j_m}$.

Under event $E_2$, the set $M_m$ is determined and we denote its value by $M_m^{(0)}$, which satisfies

$$|M_{00,0,0,0}| = h, \quad \text{for } i = 1, 2, ..., m;$$

$$|M_{00,0,0,0}| = 0, \quad \text{for } i = 1, 2, ..., m;$$

$$|M_{00,0,0,0}| = n - m - h.$$  

To analyze event $E_2$, we define $L_m^{(0)}$ such that $(L_m \in L_m^{(0)})$ is the event that no two of nodes $v_1, v_2, ..., v_m$ have any common neighbor. In view of events $(L_m \in L_m^{(0)}), (M_m = M_m^{(0)})$ and $E_2$, then $E_2$ is the same as $(L_m \in L_m^{(0)}) \cap (M_m = M_m^{(0)})$; i.e.,

$$E_2 = [\{L_m \in L_m^{(0)}\} \cap (M_m = M_m^{(0)})].$$  

(18)

We define $M_m(L_m)$ for $L_m \in L_m$ as the set of $M_m$ under which each of $V_m$ has degree $h$. Thus, the event that each of $V_m$ has degree $h$ is $(L_m \in L_m) \cap (M_m \in M_m(L_m))$, which together with (18) yields

$$E_1 = \bigcup_{L_m \in L_m} \mathbb{P}\left((L_m = L_m^{(0)}) \cap (M_m = M_m^{(0)})\right).$$  

(19)

Now we prove Propositions 1 and 2 based on (18) and (19). The inequality below following from (7) will be applied often:

$$q_n \leq \frac{21 \ln n}{n} \quad \text{for all } n \text{ sufficiently large.} \tag{20}$$

1) The Proof of Proposition 1

In view of (19) and considering the disjointness of events $(L_m = L_m^{(0)}) \cap (M_m = M_m^{(0)})$ for $L_m \in L_m$ and $M_m \in M_m(L_m)$, we express $\mathbb{P}[E_i]$ as

$$\sum_{L_m \in L_m, M_m \in M_m(L_m)} \mathbb{P}\left((L_m = L_m^{(0)}) \cap (M_m = M_m^{(0)})\right).$$  

(21)

We evaluate (21) by computing

$$\mathbb{P}\left((M_m = M_m^{(0)}) \mid (L_m = L_m^{(0)})\right).$$  

(22)

With $C_m$ and $T_m$ defined such that $(C_m = C_m^{(0)}, T_m^{(0)})$, event $(L_m = L_m^{(0)})$ is the union of events $(C_m = C_m^{(0)})$ and $(T_m = T_m^{(0)})$. Since $(C_m = C_m^{(0)})$ and $(M_m = M_m^{(0)})$ are independent, we get

$$\mathbb{P}\left((M_m = M_m^{(0)}) \mid (T_m = T_m^{(0)})\right) = \prod_{j_1 \in \{0, 1\}} \mathbb{P}[w \in M_{0, j_1, j_2, ..., j_m}] \times \mathbb{P}[w \in M_{1, j_1, j_2, ..., j_m}]$$  

(23)

where $f(n - m, M_m^{(0)})$ is the number of ways assigning the $(n - m)$ nodes from $\sum_{i=1}^m V_m$ to $M_{j_1,j_2, ..., j_m}$ such that $|M_{j_1,j_2, ..., j_m}|$ equals $|M_{j_1,j_2, ..., j_m}|$, for $j_1, j_2, ..., j_m \in \{0, 1\}$. Then

$$f(n - m, M_m^{(0)}) = \prod_{j_1,j_2, ..., j_m \in \{0, 1\}: \sum_{i=1}^m j_i \geq 1} (|M_{j_1,j_2, ..., j_m}|)!$$

(24)

which along with (15) yields

$$f(n - m, M_m^{(0)}) \leq \left[(n - m)! \mid M_m^{(0)}\right].$$

$$\sum_{j_1,j_2, ..., j_m \in \{0, 1\}: \sum_{i=1}^m j_i \geq 1} |M_{j_1,j_2, ..., j_m}| \leq n \sum_{i=1}^m j_i \geq 1.$$  

(25)

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

$$\mathbb{P}[w \in M_{j_1,j_2, ..., j_m}] \mid T_m = T_m^{(0)} \leq \mathbb{P}[E_{w_v}] \mid T_m = T_m^{(0)} = \mathbb{P}[E_{w_v}] = q_n,$$

(26)

where $E_{w_v}$ is the event that an edge exists between nodes $w$ and $v_1$. Substituting (25) and (26) into (23), and denoting $\sum_{j_1,j_2, ..., j_m \in \{0, 1\}: \sum_{i=1}^m j_i \geq 1} |M_{j_1,j_2, ..., j_m}|$ by $\Lambda$, we obtain

$$\prod_{j_1,j_2, ..., j_m \in \{0, 1\}: \sum_{i=1}^m j_i \geq 1} \Lambda \leq (n q_n)^\Lambda \times \mathbb{P}[w \in M_{0,0}] \mid T_m = T_m^{(0)}. $$

(27)

To further evaluate (22) based on (27), we will prove below that if $(L_m \notin L_m^{(0)})$ or $(M_m \neq M_m^{(0)})$, then

$$\text{for a non-negative integer } x, \text{ the term } 0^x \text{ is short for } \begin{array}{c} \overbrace{0000} \vdots \overbrace{0000} \end{array}. \text{ Also, }$$

(28)
On the one hand, if \( L^*_m \not\subset L_m^{(0)} \), 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. Hence, \( \{v_{i_1}, v_{i_2}\} \not\subset \{(u_{i_1}^{(1)}, N_i^{(1)} \cap V_m \} \) holds. Then from (16), we have \( \Lambda = \bigcup_{i=1}^{m} N_i \) - \( \{v_{i_1}, v_{i_2}\} \cap V_m \leq h \cdot m - 2 \). On the other hand, if \( M_m^* \not= M_m^{(0)} \), then there exist \( i_3 \) and \( i_4 \) with \( 1 \leq i_3 < i_4 \leq m \) such that \( N_{i_3} \cap N_{i_4} \not= \emptyset \). Then from (16), \( \Lambda \leq \bigcup_{i=1}^{m} N_i \leq \left( \sum_{i=1}^{m} |N_i| \right) - |N_{i_3} \cap N_{i_4}| \leq h \cdot m - 1 \) follows. Thus, we have proved (28), which along with (15) leads to

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

(29)

From (7), it is true that \( q_n \sim \ln n \), implying \( q_n > 1 \) for all \( n \) sufficiently large. Then substituting (28) and (29) into (27), we obtain that if \( \left( L^*_m \not\subset \bigcup_{i=1}^{n} S_i \right) \) or \( (M_m^* \not= M_m^{(0)}) \), then for all \( n \) sufficiently large, it holds that

\[
(22) \quad (q_n)^{h \cdot m - 1} \times \mathbb{P}[w \in M_0 \mid T_m = T_m^{*}] < \mathbb{P}[|T_m - T_m^*| = \text{R.H.S.}(30)].
\]

(30)

To bound \( \mathbb{P}[T_m = T_m^*] \), note that \( M_m \) is a 2-\( m \)-tuple. Among the \( 2^m \) elements of the tuple, each of \( |M_{1,2,3, \ldots, m}| \) \( 1, 2, 3, \ldots, m \) is at least 0 and at most \( h \); and the remaining element \( |M_0| \) can be determined by (15). Then it's straightforward that \( \mathbb{P}[M_m^{(0)}(L_m^{*})] \leq (h + 1)^{2^m - 1} \). Using this result in (31), and considering \( (L_m \equiv L_m^{*}) \) 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

\[
(21) \quad (h + 1)^{2^m - 1} \cdot \mathbb{P}[T_m - T_m^*] < \mathbb{P}[|T_m - T_m^*| = \text{R.H.S.}(30)].
\]

(31)

From (32) and \( q_n \sim \ln n \) as \( n \to \infty \) by (7), the proof of Proposition 1 is completed once we show

\[
\sum_{T_m^* \in T_m^*} \mathbb{P}[T_m - T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] < e^{-\ln n} \cdot \left( 1 + o(1) \right).
\]

(32)

C. Establishing (33)

From (61) and (62) (Lemma 4 in the Appendix), we get

\[
\mathbb{P}[w \in M_0 \mid T_m = T_m^*] \leq \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \mathbb{P}[|T_m - T_m^*| = \text{R.H.S.}(30)]
\]

(33)

For all \( n \) sufficiently large, where \( S_i^* := S_i \cap S_{i-j}^* \), and with \( T_i \) (i.e.), \( q_n \sim \ln n \) \( m^2 \cdot n^2 \), \( m^2 \cdot n \), which are substituted into (34) to (33) once we prove

\[
\sum_{T_m^* \in T_m^*} \mathbb{P}[T_m - T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \leq 1 + o(1).
\]

(34)

L.H.S. of (35) 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 \( 0 < \delta < 1 \).

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

From \( p_n < n^{-\delta}(\ln n)^{-1} \), \( |S_i^*| \leq K_n \) for \( 1 \leq i < j \leq m \) and (20), then for all \( n \) sufficiently large, it holds that

\[
\mathbb{P}[w \in M_0 \mid T_m = T_m^*] \geq \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \mathbb{P}[|T_m - T_m^*| = \text{R.H.S.}(30)]
\]

(35)

\[
\sum_{T_m^* \in T_m^*} \mathbb{P}[T_m - T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \leq e^{-\ln n} \cdot \left( 1 + o(1) \right).
\]

(36)

By [15, Fact 5] and \( 1 - x \leq e^{-x} \) for any real \( x \), it holds that

\[
\sum_{T_m^* \in T_m^*} \mathbb{P}[T_m - T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \leq e^{-\ln n} \cdot \left( 1 + o(1) \right)
\]

(37)

For \( n \) sufficiently large, from \( p_n \geq n^{-\delta}(\ln n)^{-1} \) and (20) (i.e., \( q_n = \ln n \), \( m^2 \cdot n^2 \)), we have

\[
\sum_{T_m^* \in T_m^*} \mathbb{P}[T_m - T_m^*] \mathbb{P}[w \in M_0 \mid T_m = T_m^*] \geq e^{-\ln n} \cdot \left( 1 + o(1) \right)
\]

(38)

Hence, for \( n \) sufficiently large, we apply (41) and (42) and \( P_n > 2K_n \) (which holds from the condition \( \frac{P_n}{K_n} = o(1) \)) to produce

\[
\frac{K_n \cdot (1 - x) \cdot \ln n}{2 \cdot x \cdot n^2} \leq 2K_n \cdot (1 - x) \cdot \ln n \leq 2K_n \cdot (1 - x) \cdot \ln n
\]

(40)

By [15, Lemma 7] that \( \frac{K_n \cdot \ln (1 - y)}{\ln n} = \omega(1) \). Then for an arbitrary constant \( c > 2 \), it holds that \( \frac{K_n}{P_n} \geq K_n \geq \frac{c^2 m}{(c - 2)(1 - s)} \), which holds for all \( n \) sufficiently large. Hence,

\[
e^{-\ln n} \cdot \left( 1 + o(1) \right)
\]

(41)

The use of (40) (43) and (44) in (37) yields

\[
\mathbb{P}[\text{R.H.S. of (37)}] \leq e^{2\ln m \cdot \ln n} \cdot \ln n \leq e^{2\ln m \cdot \ln n}
\]

(42)
To derive $H_{n,m}$ iteratively based on (45), we compute $H_{n,2}$ below. Setting $m = 2$ in L.H.S. of (35) and considering the independence between $(S_1 = S_1^*)$ and $(S_2 = S_2^*)$, we gain

$$H_{n,2} = \sum_{S_1^* \in S_2^*} \mathbb{P}[S_1 = S_1^*] \sum_{S_2^* \in S_2^*} \mathbb{P}[S_2 = S_2^*] e^{\frac{m-m_k}{2}|S_1^* \cap S_2^*|}. \quad (46)$$

Clearly, $\sum_{S_2^* \in S_2^*} \mathbb{P}[S_2 = S_2^*] e^{\frac{m-m_k}{2}|S_1^* \cap S_2^*|}$ equals R.H.S. of (37) with $m = 2$. Then from (45) and (46),

$$H_{n,2} \leq \sum_{S_1^* \in S_2^*} \mathbb{P}[S_1 = S_1^*] e^{\frac{m-m_k}{2} n_1} \leq e^{\frac{m-m_k}{2} n_1} n. \quad (47)$$

Therefore, it holds via (45) and (47) that

$$H_{n,m} \leq (e^{\frac{m-m_k}{2} n_1})^{m-(m-k)/2} e^{\frac{m-m_k}{2} n_1} n \leq e^{\frac{m-m_k}{2} n_1} n. \quad (48)$$

Finally, from cases a) and b), for $n$ sufficiently large, $H_{n,m}$ is at most $\max\{e^{m+m_k}, e^{\frac{m-m_k}{2} n_1} n\}$. Then (35) follows.

V. THE PROOF OF PROPOSITION 2

We define $c_m(0)$ and $t_m(0)$ by $c_m(0) = (0, 0, \ldots, 0)$ and $t_m(0) = \{T_m \mid S_1 \cap S_1 = \emptyset, 1 \leq i < j \leq m\}$. Clearly, $(c_m = c_m(0))$ or $(T_m \in t_m(0))$ each implies $(\mathbb{L}_m \in L_m(0))$. Also, $(c_m = c_m(0))$ and $(M_m = M_m(0))$ are independent of each other.

Thus, with $P_2 = \mathbb{P}\{c_m \in L_m(0) \cap (M_m = M_m(0))\}$, we derive

$$P_2 \geq \mathbb{P}[c_m = c_m(0)] \mathbb{P}[M_m = M_m(0)]. \quad (49)$$

Given that event $c_m = c_m(0)$ is $\bigcap_{1 \leq i < j \leq m} C_{ij}$ and event $T_m \in t_m(0)$ is $\bigcup_{1 \leq i < j \leq m} T_{ij}$, using the union bound, we get

$$\mathbb{P}[c_m = c_m(0)] \geq 1 - \sum_{1 \leq i < j \leq m} \mathbb{P}[C_{ij}] \geq 1 - m^2 \frac{p_n}{2}, \quad (50)$$

and

$$\mathbb{P}[T_m \in t_m(0)] \geq 1 - \sum_{1 \leq i < j \leq m} \mathbb{P}[T_{ij}] \geq 1 - m^2 s_n/2. \quad (51)$$

Denoting ${(h_l)^m}} m_m e^{-m_m q_n}$ by $\Lambda$, we will prove

$$\mathbb{P}[M_m = M_m(0)] \sim \Lambda, \quad (52)$$

and

$$\mathbb{P}[\{M_m = M_m(0) \mid (T_m \in t_m(0))\}] \geq \Lambda [1 - o(1)]. \quad (53)$$

Substituting (50) and (52) into (48), and applying (51) and (53) to (49), we get (i) $P_2/\Lambda \geq (1 - \min\{s_n, p_n\} / m^2/2)[1 - o(1)]$.

From (52), we get (ii) $P_2 \leq \mathbb{P}[M_m = M_m(0)] \leq \Lambda [1 + o(1)]$.

Combining (i) and (ii) above and using min$\{s_n, p_n\} \leq \sqrt{s_n} p_n = \sqrt{q_n} = o(1)$ which holds from $q_n \leq s_n p_n$ and (7), Proposition 2 follows. Below we establish (52) and (53).

A. Establishing (53)

We write $\mathbb{P}[M_m = M_m(0)]$ as

$$\sum_{T_m \in T_m(0)} \mathbb{P}[T_m \in T_m(0)] \mathbb{P}\{M_m = M_m(0) \mid (T_m = T_m(0))\},$$

where $\mathbb{P}\{M_m = M_m(0) \mid (T_m = T_m(0))\}$ equals

$$f(n - m, M_m(0)) \mathbb{P}[w \in M_m(0) \mid T_m = T_m(0)] \mathbb{P}[w \in M_m(0) \mid T_m = T_m(0)] \mathbb{P}[w \in M_m(0) \mid T_m = T_m(0)],$$

where $f(n - m, M_m(0))$ is the number of ways assigning the $(n - m)$ nodes from $V_m$ to $M_{j_1, j_2, \ldots, j_m}$ such that $|M_{j_1, j_2, \ldots, j_m}|$ is given by $M_m(0)$ (see (17)). Hence, it holds from (24) that

$$f(n - m, M_m(0)) = \frac{(n - m)!}{(n - m - hm)!} \sim (h_l)^m n_m h_m. \quad (54)$$

We will establish

$$\sum_{T_m \in T_m(0)} \mathbb{P}[T_m = T_m(0)] \prod_{i=1}^m \mathbb{P}[w \in M_{i, i+1, 0, i+1} \mid T_m = T_m(0)] \geq q_n h_m. \quad [1 - o(1)]. \quad (55)$$

We use (54) and (55) as well as (61) (v.i., Lemma 4 in the Appendix) in evaluating $\mathbb{P}[M_m = M_m(0)]$ above. Then

$$\mathbb{P}[M_m = M_m(0)] \geq (h_l)^{-m_n h_m} [1 - o(1)] \times \sum_{T_m \in T_m(0)} \mathbb{P}[T_m = T_m(0)] \prod_{i=1}^m \mathbb{P}[w \in M_{i, i+1, 0, i+1} \mid T_m = T_m(0)] \sim (h_l)^{-m_n h_m} q_n h_m [1 - o(1)]. \quad (56)$$

Substituting (33) (54) above and (63) in Lemma 4 into the computation of $\mathbb{P}[M_m = M_m(0)]$ yields

$$\mathbb{P}[M_m = M_m(0)] \leq (h_l)^{-m_n h_m} q_n h_m [1 + o(1)] \times \sum_{T_m \in T_m(0)} \mathbb{P}[T_m = T_m(0)] \mathbb{P}[w \in M_{i, i+1, 0, i+1} \mid T_m = T_m(0)] \sim (h_l)^{-m_n h_m} q_n h_m [1 + o(1)]. \quad (57)$$

Then (52) follows from (56) and (57). Namely, (52) holds upon the establishment of (55). From (64) in Lemma 4 and $q_n = o(1)$ by (7), we obtain (55) once proving

$$\frac{p_n}{K_n} \sum_{T_m \in T_m(0)} \mathbb{P}[T_m = T_m(0)] \sum_{1 \leq i < j \leq m} |S_{ij}| = o(1). \quad (58)$$

If $T_m \in T_m(0)$, then $|S_{ij}| = 0$. Then from (51), we get (58) by L.H.S. of (58) $p_n \cdot m \cdot (m - 1)/2 = \mathbb{P}[T_m \in T_m \setminus T_m(0)]$.

$$p_n \cdot m^2 / 2 \cdot m^2 s_n / 2 \leq m^4 n^{-1} \ln n / 2 = o(1). \quad (59)$$

B. Establishing (53)

Let $\Delta$ denote $\mathbb{P}\{M_m = M_m(0) \mid (T_m \in t_m(0))\}$. Clearly, $\Delta$ is equivalent to $\mathbb{P}\{M_m = M_m(0) \mid (T_m = T_m(0))\}$ for any $T_m \in t_m(0)$, so it follows that

$$\Delta = f(n - m, M_m(0)) \mathbb{P}[w \in M_{0, m} \mid T_m = T_m(0)] \prod_{i=1}^m \mathbb{P}[w \in M_{0, i, 0, i+1} \mid T_m = T_m(0)] \sim q_n h_m (1 - 2 h_m^2 q_n). \quad (60)$$

Substituting (54) (60) above and (61) in Lemma 4 into (59), we conclude that $\Delta$ is at least

$$\Delta \geq q_n h_m \cdot [1 - o(1)] \times q_n h_m (1 - 2 h_m^2 q_n) \cdot (1 - m q_n) n_m h_m = \Lambda [1 - o(1)]. \quad (61)$$

VI. NUMERICAL EXPERIMENTS

To confirm our analytical results, we now provide numerical experiments in the non-asymptotic regime.
In Figure 1, we depict the probability that graph $G(n, K, P, p)$ is 2-connected from both the simulation and the analysis, as elaborated below. In all set of experiments, we fix the number of nodes at $n = 2,000$ and the key pool size at $P = 10,000$. For the probability $p$ of a communication channel being on, we consider $p = 0.2, 0.5, 0.8$, while varying the parameter $K$ from 3 to 21. For each pair $(K, p)$, we generate 1,000 independent samples of $G(n, K, P, p)$ and count the number of times that the obtained graphs are 2-connected. Then the counts divided by 1,000 become the empirical probabilities.

The curves in Figure 1 corresponding to the analysis are in agreement with our analysis. For a random key graph $G(n, K, p)$, we consider $K = 10$.

Section II, and then use $\frac{\ln n}{\ln \ln n}$ as the analytical reference of $\Pr[G(n, K, P, p)]$ is 2-connected for a comparison with the empirical probabilities. Figure 1 indicates that the experimental results are in agreement with our analysis.

VII. RELATED WORK

Random key graphs. For a random key graph $G(n, K, P, p)$ (viz., Section II) which models the topology induced by the EG scheme, Rybarczyk [7] derives the asymptotically exact probability of connectivity, covering a weaker form of the result in Section II, and then use $\frac{\ln n}{\ln \ln n}$ as the analytical reference of $\Pr[G(n, K, P, p)]$ is 2-connected for a comparison with the empirical probabilities. Figure 1 indicates that the experimental results are in agreement with our analysis.

Random key graphs $\cap$ Erdős–Rényi graphs. As given in Section II, our studied graph $G$ is the intersection of a random key graph $G(n, K, P, p)$ and an Erdős–Rényi graph $G(n, p_n)$. For graph $G$, Yağan [9] establishes a zero-one law for connectivity, and we [15, 12] extend Yağan’s result to $k$-connectivity and show that with $P_n = \Omega(n)$, $K_n = o(1)$ and $q_n$ set as $\ln n^{\frac{1}{n^2}} \ln n + \alpha_n$, graph $G$ is (resp., is not) $k$-connected with high probability if $\lim_{n \to \infty} \alpha_n = \infty$ (resp., $\lim_{n \to \infty} \alpha_n = -\infty$). Compared with this result in [15, 12], our result on the asymptotically exact probability of $k$-connectivity is stronger and more challenging to derive.

Random key graphs $\cap$ random geometric graphs. Connectivity properties have also been studied in secure sensor networks employing the EG scheme under the disk model, where any two nodes need to be within a certain distance $r_n$ to have a link in between. When nodes are assumed to be uniformly and independently deployed in some region $\mathcal{A}$, the topology of such a network is represented by the intersection of a random key graph $G(n, K_n, P_n)$ and a random geometric graph, where a random geometric graph denoted by $G(n, r_n, \mathcal{A})$ is defined on $n$ nodes independently and uniformly distributed in $\mathcal{A}$ such that an edge exists between two nodes if and only if their distance is at most $r_n$.

Krzywdziński and Rybarczyk [6], Krishnan et al. [5], and we [13] present connectivity results in graph $G(n, K_n, P_n) \cap G(n, r_n, \mathcal{A})$.

With the network region $\mathcal{A}$ being a square of unit area, Krzywdziński and Rybarczyk [6] show that $G(n, K_n, P_n) \cap G(n, r_n, \mathcal{A})$ is connected with high probability if $\pi r_n^2 \cdot K_n^2 \approx \ln n$ for any constant $c > 8$. Krishnan et al. [5] improves the condition on $c$ to $c > 2\pi$. Later we [13] derive the critical value $C^*$ of $c$ as $\max\{1 + \lim_{n \to \infty} \ln \frac{P_n}{K_n^2} / \ln n, 4 \lim_{n \to \infty} \ln \frac{P_n}{K_n} / \ln n\}$; namely, graph $G(n, K_n, P_n) \cap G(n, r_n, \mathcal{A})$ is (resp., is not) connected with high probability for any constant $c > C^*$ (resp., $c < C^*$). There has not been any analogous result for $k$-connectivity reported in the literature.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we consider secure WSNs under the Eschenauer–Gligor (EG) key predistribution scheme with unreliable links and obtain the asymptotically exact probability of $k$-connectivity. A future direction is to consider $k$-connectivity in WSNs employing the EG scheme under the disk model [9, 5] in which two nodes have to be within a certain distance for communication in addition to sharing at least one key.

REFERENCES

For any node \( w \in \bigcup_{m} \), event \( w \in M_{0}^{0,1,0,0} \) means that node \( w \) has an edge with node \( v_{i} \), but has no edge with any node in \( V_{m} \ \backslash \{ v_{i} \} = \{ v_{j} \mid j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \} \} \). Then (63) follows since \( \mathbb{P}[w \in M_{0}^{0,1,0,0} \mid T_{m} = T_{m}^{*}^{*}] = \mathbb{P}[E_{wv_{i}} \cap (\bigcup_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}}) E_{wv_{j}} | T_{m} = T_{m}^{*}] \), where the last step uses the independence between event \( E_{wv} \) and event \( (T_{m} = T_{m}^{*}) \).

We now demonstrate (64). From the above, we have
\[
\mathbb{P}[w \in M_{0}^{0,1,0,0} \mid T_{m} = T_{m}^{*}] = \mathbb{P}[E_{wv} \cap (\bigcup_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}}) E_{wv_{j}} | T_{m} = T_{m}^{*}]
\]

(65) where the last step uses \( \mathbb{P}[E_{wv} \cap T_{m} = T_{m}^{*}] = \mathbb{P}[E_{wv}] \) since event \( E_{wv} \) is independent of event \( (T_{m} = T_{m}^{*}) \).

From (65) and \( \mathbb{P}[E_{wv_{j}}] = q_{n} \), we obtain
\[
q_{n}^{-1} \mathbb{P}[w \in M_{0}^{0,1,0,0} \mid T_{m} = T_{m}^{*}]
\]

so that
\[
q_{n}^{-1} \mathbb{P}[w \in M_{0}^{0,1,0,0} \mid T_{m} = T_{m}^{*}]
\]

(66)
\[
\geq 1 - h \sum_{i=1}^{m} q_{n}^{-1} \mathbb{P}[E_{wv} \cap (\bigcup_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}}) E_{wv_{j}} | T_{m} = T_{m}^{*}].
\]

To analyze (66), we use the union bound and Lemma 5 to get
\[
\mathbb{P}[E_{wv} \cap (\bigcup_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}}) E_{wv_{j}} | T_{m} = T_{m}^{*}]
\]

\[
\leq \sum_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}} \mathbb{P}[E_{wv} \cap E_{wv_{j}} | T_{m} = T_{m}^{*}],
\]

\[
\leq \sum_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}} p_{n}^{2} (K_{n}^{-1} s_{n} | S_{ij}^{*} | + 2 s_{n}^{2}),
\]

which is substituted into (66) to establish (64) by
\[
q_{n}^{-1} \mathbb{P}[w \in M_{0}^{0,1,0,0} \mid T_{m} = T_{m}^{*}]
\]

(67)
\[
\geq 1 - h \sum_{i=1}^{m} 2 m q_{n} + K_{n}^{-1} p_{n} \sum_{j \in \{ 1,2, \ldots, m \} \ \backslash \{ i \}} | S_{ij}^{*} |.
\]

C. The Proof of Lemma 5
We use the inclusion–exclusion principle to obtain
\[
\mathbb{P}[\Gamma_{it} \cap \Gamma_{jt} | (| S_{ij}^{*} | = u)]
\]

(68)
\[
= \mathbb{P}[\Gamma_{it} | (| S_{ij}^{*} | = u)] + \mathbb{P}[\Gamma_{jt} | (| S_{ij}^{*} | = u)] - \mathbb{P}[\Gamma_{it} \cup \Gamma_{jt} | (| S_{ij}^{*} | = u)] = 2 s_{n} - 1 + \left( \frac{p_{n} - (2K_{n} s_{n})}{K_{n}} \right)^{2},
\]

in view that event \( (| S_{ij}^{*} | = u) \) is independent of each of \( \Gamma_{it} \) and \( \Gamma_{jt} \), and event \( \Gamma_{it} \cup \Gamma_{jt} \) means \( S_{i} \cap (S_{i} \cup S_{j}) \neq \emptyset \).

By [9, Lemma 5.1] and [15, Fact 2], we derive
\[
(1 - s_{n}) \frac{2K_{n} s_{n} - u}{K_{n}} \leq 1 - s_{n} \left( \frac{2K_{n} s_{n} - u}{K_{n}} \right)^{2} \leq 1 - 2 s_{n} + \frac{K_{n}^{-1} s_{n}}{K_{n}} + s_{n}^{2},
\]

which is substituted into (68) to complete the proof.