Towards k-connectivity in Heterogeneous Sensor Networks under Pairwise Key Predistribution

Mansi Sood and Osman Yağan
Department of Electrical and Computer Engineering and CyLab,
Carnegie Mellon University, Pittsburgh, PA, 15213 USA
msood@cmu.edu, oyagan@ece.cmu.edu

***Abstract*—We study the secure and reliable connectivity of wireless sensor networks under the *heterogeneous* pairwise key predistribution scheme. This scheme was recently introduced as an extension of the random pairwise key predistribution scheme of Chan et al. to accommodate networks where the constituent sensors have different capabilities or requirements for security and connectivity. For simplicity, we consider a heterogeneous network where each of the n sensors is classified as type-1 (respectively, type-2) with probability μ (respectively, $1-\mu$) where $0 < \mu < 1$. Each type-1 (respectively, type-2) node selects 1 (respectively, K_n) other nodes uniformly at random to be *paired* with; according to the pairwise scheme each pair is then assigned a unique pairwise key so that they can securely communicate with each other. We establish critical conditions on n, μ, and K_n such that the resulting network has minimum node degree of at least k with high probability in the limit of large network size. Our result constitutes a zero-one law for the minimum node degree of the recently introduced inhomogeneous random K-out graph model. This constitutes a crucial step towards establishing a similar zero-one law for the k-connectivity of the graph; i.e., for the property that the network remains connected despite the failure of any $k-1$ nodes or links. We present numerical results that indicate the usefulness of our results in selecting the parameters of the scheme in practical settings with finite number of sensors.**

***Index Terms*—Wireless Sensor Networks, Random Graphs, Connectivity, Security**

I. Introduction

A. Background and Motivation

Wireless sensor networks (WSNs) are of vital importance in numerous application domains including environmental sensing, health monitoring, surveillance and tracking [1]. The affordability, scalability, low-power consumption and ease of installation has made WSNs the backbone of several emerging technologies [2]. WSNs are often deployed in hostile environments making them susceptible to adversarial attacks and operational failures. The limited energy, computation, and communication capabilities of WSNs precludes the use of standard cryptosystems to safeguard these networks [3]. Eschenauer and Gligor addressed this issue of security in WSNs by introducing the notion of random key predistribution in their pioneering work [4]. Following this work, several variants of random key predistribution emerged; e.g., see [5], [6] and the references therein.

This work was supported in part by the National Science Foundation through grant CCF #1617934.

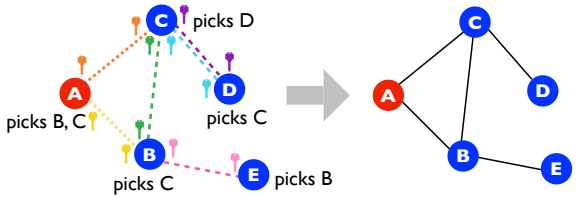

Fig. 1: *A WSN comprising 5 nodes secured by the heterogeneous random pairwise key predistribution scheme. Each type-1 (resp. type-2) node randomly picks 1 (resp. $K = 2$) nodes and a unique pairwise key is given to node pairs per selection; in this example, node A is type-2 and others are type-1. Two nodes can communicate if they have at least one pairwise key in common. This induces a graph with edges corresponding to node pairs which share at least one key in common.*

One of the widely acclaimed schemes is the random *pairwise* key predistribution scheme proposed by Chan et al. in [7]. The random pairwise key predistribution scheme comprises of two phases. First, each sensor node is paired offline with K nodes chosen uniformly at random among all sensor nodes. Next, a unique pairwise key is distributed to all node pairs in which at least one of the nodes is paired to the other during the offline node-pairing step. After deployment, two sensor nodes can communicate securely if they have at least one pairwise key in common. In Section II, we give the precise implementation details of this scheme and its heterogeneous variant proposed in [8]. The pairwise key predistribution scheme preserves the secrecy of rest of the network in case of node capture attacks, and also enables node-to-node authentication and quorum-based revocation [7].

The random pairwise key predistribution scheme induces a class of random graphs known as *random K-out graphs* [9]–[12]: each of the n vertices is assigned K arcs towards K distinct vertices that are selected uniformly at random, and then the orientation of the arcs is ignored. Let $\mathbb{H}(n; K)$ denote the resulting random K-out graph. In [10], [11], it was shown that if $K \geq 2$, then the resulting graph is 1-connected with high probability. More precisely, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; K) \text{ is connected}\right] = \begin{cases} 1 & \text{if} \quad K \geq 2, \\ 0 & \text{if} \quad K = 1. \end{cases}$$

Emerging real-world networks are characterized by heterogeneous nodes differing in their roles, resources, hardware limitations and connectivity requirements [13]–[15]. This made

it necessary to develop and analyze heterogeneous variants of classical key predistribution schemes. From a theoretical stand point, this corresponds to advancing the literature pertaining to connectivity in inhomogeneous variants of classical random graph models. In order to model differing node capabilities, [8] introduced a heterogeneous pairwise key predistribution scheme in which each node is classified as type-1 (respectively, type-2) with probability μ (respectively, $1-\mu$), $0 < \mu < 1$. Then, each type-1 (respectively, type-2) node selects one node (respectively, K_n nodes) uniformly at random from all other nodes; see Figure 1. The heterogeneous pairwise key predistribution scheme induces an inhomogeneous random K-out graph, denoted $\mathbb{H}(n;\mu,K_n)$. The analysis of 1-connectivity in [8] of $\mathbb{H}(n;\mu,K_n)$ yielded the rather surprising result that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n;\mu,K_n) \text{ is connected}\right] = \begin{cases} 1 & \text{if } K_n = \omega(1), \\ < 1 & \text{otherwise.} \end{cases}$$

This paper is motivated by the fact that in many applications it is desirable to have a *stronger* notion of connectivity; e.g., the network remaining connected despite edge or node failures and removals. To this end, this work initiates a study on the k-connectivity of WSNs under the heterogeneous pairwise scheme. A network is said to be k-connected if it remains connected despite the removal of any $k-1$ of its nodes or edges[1]. Moreover, in a k-connected graph, there are at least k mutually disjoint paths between any pair of nodes. In the context of WSNs, the property of k-connectivity is highly desirable since it makes the network resilient to the failure of up to $k-1$ sensor nodes or $k-1$ links. Such failures could arise in practice due to operational failures, adversarial capture of nodes, or battery depletion. In addition to providing reliability against failures, k-connectivity facilitates the incorporation of mobile nodes with intermittent connectivity. A k-connected WSN can at any given time support up to $k-1$ mobile nodes without disrupting connectivity. This motivates us to study reliable connectivity, namely k-connectivity in networks secured by the heterogeneous pairwise key distribution scheme.

We envision that the simplicity of graph construction and unique connectivity properties position the K-out graph as a promising model for many real-world networks in addition to WSNs. Recently, a structure similar to the random K-out graph was proposed in [17, Algorithm 1] for generating anonymity graphs to facilitate diffusion of transaction information, thereby making the crypto-currency network robust to *de-anonymization* attacks. Given their sparse yet connected structure, random K-out graphs can potentially be useful also for payment channels used for scaling cryptocurrency networks such as the Lightning Network [18]. We further motivate our work by noting that in these additional potential applications as well, it would be of interest to study the the k-connectivity property and to understand the impact of heterogeneity. For example, having at least k *mutually disjoint* paths between every pair of nodes would be useful in payment channels since some links could fail due to depletion of funds.

[1]The notion of k-connectivity used in this paper refers to k-vertex connectivity, which is defined as the property that the graph remains connected after deletion of any $k-1$ vertices. It is known [16] that a k-vertex connected graph is always k-edge connected, meaning that it will remain connected despite the removal of any $k-1$ edges. Thus, we say that a graph is k-connected (without explicitly referring to vertex-connectivity) to refer to the fact that it will remain connected despite the deletion of any $k-1$ vertices or edges.

B. Main Contributions

In this paper, we initiate the analysis of k-connectivity in WSNs secured by the heterogeneous pairwise key predistribution scheme which induces an inhomogeneous random K-out graph $\mathbb{H}(n;\mu,K_n)$. We establish a zero-one law for the property that the minimum node degree is at least k. In particular, we present conditions on μ and K_n such that the resulting graph has minimum degree at least k with probability approaching one (respectively, zero) constituting the one-law (respectively, zero-law), as the number of nodes gets large. Numerical results are presented to demonstrate the usefulness of these results in selecting the parameters of the pairwise scheme when the number of nodes is finite. An interesting finding is that for inhomogeneous random K-out graphs, the number of *additional* edges needed to go from 1-connectivity to k-connectivity with $k \geq 2$ is *unexpectedly* larger as compared to many other random graph models studied before; see Table I for details.

Our result provides a crucial step towards establishing a zero-one law for k-connectivity in inhomogeneous random K-out graphs. In particular, since minimum node degree being at least k constitutes a necessary condition for k-connectivity, the zero-law established here also provides a zero-law for k-connectivity. In fact, taking evidence from several other random graph models [16], [19], [20], we conjecture that the one-law for k-connectivity will also be identical to the one-law established here for minimum node degree being at least k. This conjecture is supported further through numerical results.

C. Notation

All limits are understood with the number of nodes n going to infinity. While comparing asymptotic behavior of a pair of sequences $\{a_n\},\{b_n\}$, we use $a_n = \mathrm{o}(b_n)$, $a_n = \mathrm{O}(b_n)$, $a_n = \Theta(b_n)$, and $a_n = \omega(b_n)$ with their meaning in the standard Landau notation. All random variables are defined on the same probability triple $(\Omega,\mathcal{F},\mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. We let $\mathbb{1}\{A\}$ denote the indicator random variable which takes the value 1 if event A occurs and 0 otherwise. We say that an event holds with high probability (whp) if it holds with probability one as $n \to \infty$. We denote the cardinality of any discrete set A by $|A|$ and the set of all positive integers by $\mathbb{N}_0$.

II. System Model

A. Heterogeneous random pairwise key predistribution

The widely studied pairwise key predistribution scheme proposed by Chan et al. [7] was extended in [8] to *heterogeneous* settings to accommodate networks where sensors differ in their capabilities and mission requirements. The steps undertaken

to establish secure connectivity in the heterogeneous random pairwise key predistribution scheme are as follows. Consider a network comprising of n nodes which are labeled as $i = 1, 2, \dots n$ and assigned unique IDs: $\mathrm{Id}_1, \dots, \mathrm{Id}_n$. Each node is labeled as type-1 (respectively, type-2) with probability μ (respectively, $1-\mu$) independently from other nodes where $0 < \mu < 1$. In the (offline) *initialization* phase, each type-1 (respectively, type-2) node selects K_1 (respectively, K_2) other nodes chosen uniformly at random. The homogeneous pairwise scheme [7] corresponds to the case where $\mu = 0$ and all nodes choose exactly K nodes to be paired with.

Define $\mathcal{N} := \{1, 2, \dots, n\}$ and $\mathcal{N}_{-i} := \{1, 2, \dots, n\} \setminus i$. For each $i \in \mathcal{N}$, let $\Gamma_{n,i} \subseteq \mathcal{N}_{-i}$ denote the subset of nodes selected by node i from $\mathcal{N}_{-i}$ uniformly at random. With $t_i \in \{1, 2\}$ denoting the type of node i, we have for any $A \subseteq \mathcal{N}_{-i}$

$$\mathbb{P}[\Gamma_{n,i} = A \mid t_i = \ell] = \begin{cases} \binom{n-1}{K_\ell}^{-1} & \text{if } |A| = K_\ell, \\ 0 & \text{otherwise.} \end{cases}$$

We further assume that $\Gamma_{n,1}, \dots, \Gamma_{n,n}$ are mutually independent given the types of nodes.

Once the offline pairing process has been completed, we insert key rings $\Sigma_{n,1}, \dots, \Sigma_{n,n}$ in the memory modules as follows. If $i \in \Gamma_{n,j} \vee j \in \Gamma_{n,i}$, i.e., either node i selects node j or node j selects node i or both, we generate a pairwise key ω_{ij} and store this key and the corresponding node IDs in the memory modules of both nodes i and j. It is important to note that the key ω_{ij} is assigned *exclusively* to nodes i and j to be used in securing the communication between them. This strategy of assigning unique keys to nodes which were paired during the offline node-pairing process is the reason why this approach is called the *pairwise* key predistribution scheme. Having unique, pairwise keys brings several advantages including distributed node-to-node authentication and resilience to node capture attacks [7].

In the post-deployment *key-setup* phase, nodes first broadcast their IDs to their neighbors following which each node searches for the corresponding IDs in their key rings. Finally, node pairs wishing to communicate verify each others' identities through a cryptographic handshake [7]. Thus, by construction, the pairwise key predistribution facilitates node-to-node authentication.

In the rest of this paper, we assume $K_1 = 1$ and $K_2 \geq 2$ as in [8] for simplicity. The more general cases with arbitrary number of node types and arbitrary scheme parameters $K_1, K_2, \dots$, should be studied in a separate paper. We assume that $0 < \mu < 1$ is fixed and K_2 scales with n. From here onward, let K_n denote the scaling of K_2 with n. In [8], the 1-connectivity of the network under this setting was studied. In particular, it was shown that the network is connected whp only if K_n grows unboundedly large as $n \to \infty$ (irrespective of μ). This was in stark contrast with the results for the homogeneous case where it is known that the network is connected whp if $K \geq 2$ (with K being the number of choices made by every node). The main goal of this paper is to initiate a study on the k-connectivity of the network under the same setting; e.g., by revealing conditions on K_n and μ required for the network to be k-connected whp.

B. Inhomogeneous Random K-out graph

A WSN comprising of n sensors secured by the heterogeneous pairwise key predistribution scheme can be modeled by an inhomogeneous random K-out graph defined as follows. Two distinct nodes i and j are said to be adjacent, written $i \sim j$, if and only if they have at least one common key in their respective key rings as defined above. Equivalently, nodes i and j are adjacent if either node picks the other or both; i.e.,

$$i \sim j \quad \text{if} \quad j \in \Gamma_{n,i} \vee i \in \Gamma_{n,j}. \tag{1}$$

Thus, given a set of n nodes, the adjacency condition (1) gives a precise edge construction on the vertex set $\{1, 2, \dots, n\}$. We denote the graph constructed using (1) as $\mathbb{H}(n; \mu, K_n)$. Further, let $\langle K_n \rangle$ denote the average number of selections per node given by $\mu + (1-\mu)K_n$. We note that if $\mu = 0$, the inhomogeneous random K-out graph becomes equivalent to the homogeneous random K-out graph [10]–[12].

III. Results and Discussion

In this section, we present our main technical result: a zero-one law for the minimum node degree of the inhomogeneous random K-out graph being at least k. We then provide a discussion on the implications of our main result, and we explain why it is expected to pave the way to establish a similar zero-one law for k-connectivity. Finally, we provide experimental results that demonstrate the usefulness of our result in the finite node regime and support our conjecture that an analog of Theorem 1 holds for k-connectivity.

A. Main results

We refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* if it satisfies the condition

$$2 \leq K_n < n, \quad n = 2, 3, \dots.$$

Our main result is presented next.

Theorem 1: Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ and μ such that $0 < \mu < 1$. With $\langle K_n \rangle = \mu + (1-\mu)K_n$ and a positive integer $k \geq 2$ let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through

$$\langle K_n \rangle = \log n + (k-2) \log \log n + \gamma_n, \tag{2}$$

for all $n = 2, 3, \dots$. Then, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l} \text{Min. node degree of} \\ \mathbb{H}(n; \mu, K_n) \text{ is } \geq k \end{array} \right] = \begin{cases} 1 & \text{if } \lim_{n\to\infty} \gamma_n = +\infty, \\ 0 & \text{if } \lim_{n\to\infty} \gamma_n = -\infty. \end{cases}$$

Theorem 1 establishes scaling conditions on $\langle K_n \rangle$ (i.e., on K_n and μ) such that the minimum node degree of the inhomogeneous random K-out graph $\mathbb{H}(n; \mu, K_n)$ is at least k, *and* less than k, respectively, with high probability as the number of nodes approaches infinity. Put differently, it establishes a *zero-one law* for the property that $\mathbb{H}(n; \mu, K_n)$ has minimum degree of at least k. An immediate consequence

of Theorem 1 is that $\langle K_n \rangle$ must scale as $\Omega(\log n)$ for the minimum node degree to be at least k. The scaling condition (2) in Theorem 1 can be equivalently expressed in terms of the network parameters μ and K_n as follows

$$K_n = \frac{\log n + (k-2)\log\log n}{1-\mu} + \gamma_n. \tag{3}$$

The proof of Theorem 1 is based on applying the method of first and second moments [21] to a random variable counting the number of nodes with degree less than k. The dichotomous results with γ_n approaching $+\infty$ and $-\infty$ can be intuitively viewed as a consequence of the expected number of nodes with degree less than k approaching ∞ (respectively, 0) as γ_n goes to ∞ (respectively, $-\infty$). However, the complex inter-dependencies in the node degrees make this analysis quite challenging. In particular, the second moment analysis requires careful consideration of several cases for the node degree of a pair of nodes and the selections made by them. Due to space constraints, we provide a brief sketch of the proof for Theorem 1 in Section IV; all details can be found in [22].

B. Discussion

Recall that a k-connected graph remains connected upon deletion of any $k-1$ nodes or edges. Consequently, for a graph to be k-connected, the minimum node degree for the graph must be at least k. Thus, Theorem 1 also provides a necessary condition for k-connectivity in networks secured by the heterogeneous pairwise key predistribution scheme. In particular, under scaling (2), Theorem 1 automatically gives the corresponding zero-law for k-connectivity. Furthermore, in most random graph models including Erdős-Rényi graphs [16], random key graphs [19] and random geometric graphs [20], the conditions required to ensure a minimum node degree of at least k are shown to be sufficient to make the graph k-connected whp. This is done by showing that it is highly unlikely for the corresponding graph to be *not* k-connected if all nodes have at least k neighbors. In light of this (as well as our numerical studies presented in Section III-C), we conjecture the following zero-one law for k-connectivity.

Conjecture 2: Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ and μ such that $0 < \mu < 1$. With a positive integer $k \geq 2$ let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through (2). Then, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l} \mathbb{H}(n;\mu,K_n) \textit{ is} \\ k\textit{-connected} \end{array} \right] = \begin{cases} 1 & \textit{if } \lim_{n\to\infty} \gamma_n = +\infty, \\ 0 & \textit{if } \lim_{n\to\infty} \gamma_n = -\infty. \end{cases}$$

We now discuss the implications of Theorem 1 on connectivity for heterogeneous pairwise predistribution scheme and compare the results with other key predistribution schemes. Table I summarizes the mean node degree requirements for having 1-connectivity and k-connectivity for homogeneous and inhomogeneous versions of random K-out graphs [8], [10] and *random key graphs* induced by the EG scheme [4], [23]–[25]. For the inhomogeneous versions, the table entries correspond to the mean degree of the *least connected* node type. We also added the corresponding results for Erdős-Rényi graphs [16] for comparison. An interesting observation is that for the inhomogeneous random K-out graph, going from 1-connectivity to k-connectivity requires an increase of $\log n + (k-2)\log\log n$ in the mean degree. This is much larger than what is required (i.e., $(k-1)\log\log n$) in the other models seen in Table I. In addition, we see that the homogeneous pairwise key predistribution scheme incurs the least overhead in terms of the edges and keys required to achieve 1-connectivity or k-connectivity. For instance, if all nodes select two neighbors, the resulting network is securely 2-connected. However, the analysis of 1-connectivity in [8] and Theorem 1 together suggest that the perceived benefits of the pairwise scheme reduce in the face of heterogeneity when $K_1 = 1$, i.e., when a positive fraction of nodes picks just one other node to be paired with.

Random graph	**1-connectivity**	**k-connectivity**, $k \geq 2$
Homogeneous K-out	4	$2k$
Inhomogeneous K-out	$\omega(1)$	$\log n + (k-2)\log\log n + \omega(1)$
Homogeneous random key	$\log n + \omega(1)$	$\log n + (k-1)\log\log n + \omega(1)$
Inhomogeneous random key	$\log n + \omega(1)$	$\log n + (k-1)\log\log n + \omega(1)$
Erdős-Rényi	$\log n + \omega(1)$	$\log n + (k-1)\log\log n + \omega(1)$

TABLE I: *Comparing the mean node degree necessary for 1-connectivity and k-connectivity in several random graph models. For inhomogeneous K-out and inhomogeneous random key graphs, the values given in the table correspond to the mean degree for the* least *connected node type.*

C. Simulation results

This section presents empirical studies which probe the applicability of Theorem 1 in the non-asymptotic regime with finite number of sensors. For each experiment, we fix the number of nodes at $n = 500$ and generate 1000 independent realizations of the inhomogeneous random K-out graph $\mathbb{H}(n;\mu,K_n)$. To obtain the empirical probability of minimum node degree being at least k, we divide the number of instances for which the generated graph has minimum node degree of at least k by the total number 1000 of instances generated. Likewise, we compute the empirical probability for k-connectivity by counting the number of times (out of 1000) for which the resulting graph is k-connected.

Through simulations, we study the impact of the probability of assignment to type-1 (μ) and the number of selections made by type-2 nodes (K_n) on the probability that minimum node degree is at least k, for various k values. A smaller value of μ corresponds to a network dominated by type-2 nodes and thus the resulting random graph $\mathbb{H}(n;\mu,K_n)$ has a larger probability of having a minimum node degree of at least k. Figure 2 illustrates this phenomenon by comparing the cases with $\mu = 0.1$ and $\mu = 0.9$. Moreover, for $k_1 \geq k_2 \geq 2$, the event that a graph has a minimum node degree of at least k_1 is a subset of the event that a graph has a minimum node degree

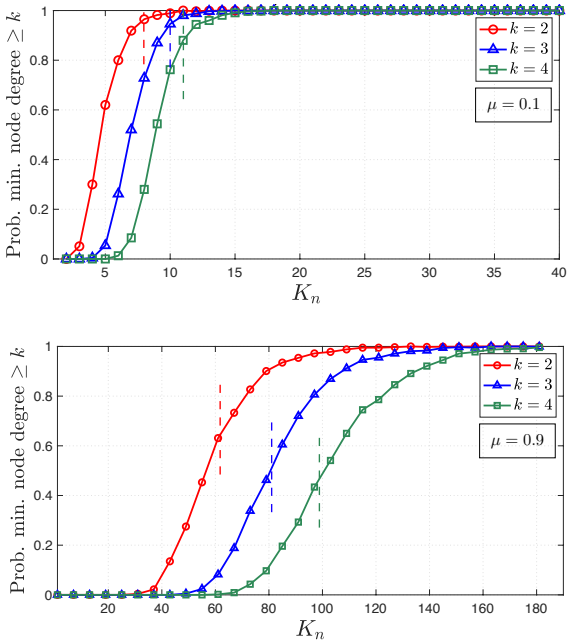

Fig. 2: *Empirical probability (computed by averaging* 1000 *independent experiments for each data point) for the minimum node degree being no less than* k *as a function of* K_n *for* $n = 500$ *and* $\mu = 0.1, 0.9$.

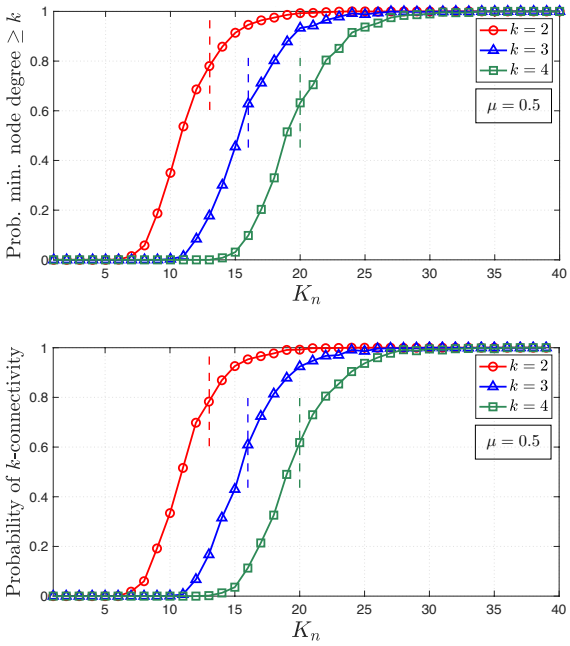

Fig. 3: *Empirical probability (computed by averaging* 1000 *independent experiments for each data point) of* k*-connectivity and minimum node degree being no less than* k *as a function of* K_n *for* $n = 500$, $\mu = 0.5$ *and* $k = 2, 3, 4$.

greater than or equal to k_2. Thus, we see an upwards shift in the curves when going from $k = 4$ to $k = 2$.

In each figure, we also plot a vertical-dashed line corresponding to the critical threshold of having minimum node degree at least k asserted by Theorem 1 through scaling condition (3). Namely, vertical dashed lines represent the K_n value satisfying

$$K_n = \left\lceil \frac{\log n + (k-2)\log\log n}{1-\mu} \right\rceil. \tag{4}$$

The desired probability of minimum node degree being no less than k is 0 for small values of K_n and increases sharply to 1 in a neighborhood of the threshold described by (4). Thus, we find a good agreement between our numerical results and Theorem 1 even when the number of nodes is finite.

Finally, we test the validity of Conjecture 2 for k-connectivity. Figure 3 presents the empirical probability of k-connectivity and minimum node degree being no less than k as k varies from 2 to 4 and $\mu = 0.5$. We observe a striking similarity between the plots for minimum node degree and k-connectivity. Although not shown here for brevity, the same phenomenon is observed in all experiments with different parameter settings for μ and k. This provides strong evidence in favour of minimum node degree being at least k and k-connectivity being *asymptotically* equivalent properties in inhomogeneous random K-out graphs.

IV. Sketch of the Proof of Theorem 1

In this section, we provide a brief outline for the proof of Theorem 1; all details can be found in [22]. Our proof employs the method of first and second moments [21] applied to count variables representing the number of nodes in $\mathbb{H}(n;\mu,K_n)$ with degree less than k. With any $d = 0, 1, \ldots$, let $Z_{n,d}$ denote the number of nodes in $\mathbb{H}(n;\mu,K_n)$ with degree d. In other words, we let $Z_{n,d} = \sum_{i=1}^{n} \mathbb{1}\{\deg(v_i) = d\}$, where $\deg(v_i)$ is the degree of node v_i. To provide an intuitive explanation for the dichotomy arising in Theorem 1 (depending on the limiting value of the sequence γ_n), we present the next result on the mean value of $Z_{n,d}$ under an additional technical condition on γ_n; as can be seen in the detailed proof of Theorem 1 given in [22], this condition is not needed for our result to hold.

Lemma 1: With γ_n *defined through (2), let* $|\gamma_n| = \mathrm{o}(\log n)$. *Then, the expected number of nodes with degree* d *satisfies*

$$\mathbb{E}\left[Z_{n,d}\right] = \Theta(1)\exp\left\{-(k-1-d)\log\log n - \gamma_n\right\}.$$

In order to see how the zero-one law arises in Theorem 1, substitute $d = k-1$ in Lemma 1. We see that $\mathbb{E}[Z_{n,k-1}] = \Theta(e^{-\gamma_n})$ so that it approaches 0 (respectively, ∞) as γ_n tends to ∞ (respectively, $-\infty$). This dichotomy forms the basis of defining γ_n in the *critical* scaling condition (2), and the accompanying zero-one law given in Theorem 1.

To establish the one-law, we use the Markov inequality applied to the integer-valued random variable $Z_{n,d}$ leading to $\mathbb{P}[Z_{n,d} \leq 1] \leq \mathbb{E}[Z_{n,d}]$. This gives

$$\mathbb{P}[Z_{n,d} = 0] = 1 - \mathbb{P}[Z_{n,d} \leq 1] \geq 1 - \mathbb{E}[Z_{n,d}]. \tag{5}$$

From Lemma 1, when $\gamma_n \to \infty$, we see that $\mathbb{E}[Z_{n,d}] \to 0$ for all $d = 1, 2, \ldots, k-1$. Using this in (5), we get

$$\lim_{n\to\infty} \mathbb{P}[Z_{n,d} = 0] = 1, \quad d = 0, 1, \ldots k-1$$

which is equivalent to the one-law

$$\lim_{n\to\infty} \mathbb{P}\left[\text{Min. node degree of } \mathbb{H}(n;\mu,K_n) \text{ is } \geq k\right] = 1.$$

In order to obtain a zero-law, we invoke the method of second moments. Using the Cauchy-Schwarz inequality it can be shown [21] that

$$\mathbb{P}[Z_{n,d} \neq 0] \geq \frac{(\mathbb{E}[Z_{n,d}])^2}{\mathbb{E}[Z_{n,d}^2]}. \tag{6}$$

From exchangeability of the indicator random variables $\mathbb{1}\{\deg(v_i) = d\}$, $i = 1, 2, \ldots, n$, we have

$$\frac{\mathbb{E}[Z_{n,d}^2]}{(\mathbb{E}[Z_{n,d}])^2} = \frac{1}{\mathbb{E}[Z_{n,d}]} + \frac{n-1}{n} \frac{\mathbb{P}[\deg(v_1) = \deg(v_2) = d]}{(\mathbb{P}[\deg(v_1) = d])^2}. \tag{7}$$

In view of (6)-(7), we get $\mathbb{P}[Z_{n,d} \neq 0] \to 1$ if the following two results are established.

1) $\lim_{n\to\infty} \mathbb{E}[Z_{n,d}] = \infty$,
2) $\limsup_{n\to\infty} \frac{\mathbb{P}[\deg(v_1) = \deg(v_2) = d]}{(\mathbb{P}[\deg(v_1) = d])^2} \leq 1$.

The zero-law in Theorem 1 follows upon establishing that both conditions hold with $d = k - 1$ when $\gamma_n \to -\infty$. The first condition follows from Lemma 1 when $\gamma_n \to -\infty$ and $d = k - 1$. The proof of the second condition is involved due to the degrees of v_1, v_2 being correlated in several ways. First, if v_1 picks v_2 or vice versa, the degrees of both nodes are affected. Second, if one of the remaining $n-2$ nodes is known to pick v_1, the chances of v_2 being picked by the same node decreases; the exact correlations will also depend on the *type* of that third node. These complex correlations among node degrees makes it necessary to consider several realizations of the graph which result in a particular degree for v_1, v_2. We direct readers to [22] for a complete proof of this result and other details of Theorem 1.

V. Conclusion

In this work we initiate the analysis of k-connectivity in WSNs secured by the heterogeneous pairwise key predistribution scheme; k-connectivity makes the network resilient to failure of up to $k-1$ nodes or links. Our main result provides *critical* conditions on the network and scheme parameters such that with high probability every sensor has at least k other sensors that it can securely communicate with (when the number of nodes gets large). Through numerical simulations, this result is shown to be useful in selecting scheme parameters in the finite node regime. An interesting finding is that for inhomogeneous random K-out graphs, which are induced under the heterogeneous pairwise scheme, the number of *additional* edges needed to go from 1-connectivity to k-connectivity with $k \geq 2$ is much larger than that seen in most other random graph models studied before; see Table I for details.

This paper completes a necessary crucial step towards establishing the k-connectivity under the heterogeneous pairwise scheme. In fact, our numerical results suggest that an analog of our main result with the same critical scaling applies also for k-connectivity of the network. An immediate direction for future work is to prove this conjecture on k-connectivity. It would also be interesting to extend our analysis to a more generalized heterogeneous pairwise key predistribution scheme with $r > 2$ node types and arbitrary scheme parameters $K_1, K_2, \ldots, K_r$ associated with each node type.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of ACM CCS 2002*, pp. 41–47.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 8, no. 2, pp. 2–23, Second 2006.

[6] Y. Xiao and V. K. Rayi and B. Sun and X. Du and F. Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, pp. 2314 – 2341, 2007.

[7] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of IEEE S&P 2003*.

[8] R. Eletreby and O. Yağan, "Connectivity of wireless sensor networks secured by the heterogeneous random pairwise key predistribution scheme," in *Proc. of IEEE CDC 2018*, Dec 2018.

[9] B. Bollobás, *Random graphs*. Cambridge university press, 2001, vol. 73.

[10] T. I. Fenner and A. M. Frieze, "On the connectivity of randomm-orientable graphs and digraphs," *Combinatorica*, vol. 2, no. 4, pp. 347–359, Dec 1982.

[11] O. Yağan and A. M. Makowski, "On the connectivity of sensor networks under random pairwise key predistribution," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5754–5762, Sept 2013.

[12] F. Yavuz, J. Zhao, O. Yağan, and V. Gligor, "Toward k-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6251–6271, 2015.

[13] K. Lu, Y. Qian, M. Guizani, and H. Chen, "A framework for a distributed key management scheme in heterogeneous wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, pp. 639–647, February 2008.

[14] C.-H. Wu and Y.-C. Chung, "Heterogeneous wireless sensor network deployment and topology control based on irregular sensor model," in *Advances in Grid and Pervasive Computing*, 2007, pp. 78–88.

[15] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proc. of IEEE INFOCOM 2005*.

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

[17] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller, and P. Viswanath, "Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 2, no. 2, pp. 29:1–29:35, Jun. 2018.

[18] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[19] J. Zhao, O. Yaan, and V. Gligor, "k-connectivity in random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3810–3836, July 2015.

[20] M. D. Penrose, *Random Geometric Graphs*. Oxford University Press, Jul. 2003.

[21] S. Janson, T. Łuczak, and A. Ruciński, "Random graphs. 2000," *Wiley–Intersci. Ser. Discrete Math. Optim*, 2000.

[22] M. Sood and O. Yağan, "Towards k-connectivity in heterogeneous sensor networks under pairwise key predistribution," http://www.andrew.cmu.edu/user/oyagan/Conferences/gc19.pdf.

[23] O. Yağan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2983–2999, 2012.

[24] O. Yağan, "Zero-one laws for connectivity in inhomogeneous random key graphs," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4559–4574, Aug 2016.

[25] R. Eletreby and O. Yağan, "k-connectivity of inhomogeneous random key graphs with unreliable links," *IEEE Transactions on Information Theory*, pp. 1–1, 2019.