k-Connectivity in Random Graphs induced by Pairwise Key Predistribution Schemes

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

***Abstract*—Random key predistribution schemes serve as a viable solution for facilitating secure communication in Wireless Sensor Networks (WSNs). We analyze *reliable* connectivity of a *heterogeneous* WSN under the random pairwise key predistribution scheme of Chan et al. According to this scheme, each of the n sensor nodes 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 is *paired* with 1 (respectively, K_n) other node selected uniformly at random; each *pair* is then assigned a unique pairwise key so that they can securely communicate with each other. A main question in the design of secure and heterogeneous WSNs is how should the parameters n, μ, and K_n be selected such that resulting network exhibits certain desirable properties with high probability. Of particular interest is the *strength* of connectivity often studied in terms of k-connectivity; i.e., with $k=1,2,\ldots$, the property that the network remains connected despite the removal of any $k-1$ nodes or links.In this paper, we answer this question by analyzing the *inhomogeneous random K-out graph* model naturally induced under the heterogeneous pairwise scheme. It was recently established that this graph is 1-connected asymptotically almost surely (a.a.s.) if and only if $K_n=\omega(1)$. Here, we show that for $k=2,3,\ldots$, we need to set $K_n=\frac{1}{1-\mu}(\log n+(k-2)\log\log n+\omega(1))$ for the network to be k-connected a.a.s. The result is given in the form of a zero-one law indicating that the network is a.a.s. *not* k-connected when $K_n=\frac{1}{1-\mu}(\log n+(k-2)\log\log n-\omega(1))$. We present simulation results to demonstrate the usefulness of the results in the finite node regime.**

Keywords: Random graphs, connectivity, security, wireless sensor networks.

I. Introduction

Wireless sensor networks (WSNs) form the backbone of several application domains including environmental sensing, battlefield surveillance, and healthcare monitoring [1]. A typical wireless sensor network comprises of a collection of distributed sensor nodes. The limited computation and communication capabilities of WSNs precludes the use of traditional key exchange and distribution protocols to safeguard these networks [2]–[4]. Moreover, WSNs are often deployed for sensitive applications in hostile environments making them susceptible to adversarial attacks.

In their seminal work, Eschenauer and Gligor [2] addressed the issue of facilitating security in WSNs by introducing a scheme based on *random* predistribution of symmetric keys. Subsequently, several variants of the random key predistribution approach emerged; e.g., see [5], [6] and the references therein. Among them is a widely adopted approach called the random *pairwise* key predistribution scheme by Chan et al. [7]. The random pairwise scheme is implemented in two phases. In the first phase, each sensor node is paired *offline* with K distinct nodes chosen uniformly at random among all other sensor nodes. Next, a *unique* pairwise key is inserted in the memory modules of each of the paired sensors. After deployment, two sensor nodes can communicate securely only if they have at least one key in common. In Section II, we provide more details about the implementation of this scheme and its heterogeneous variant introduced in [8]. The major advantages of the pairwise scheme include resilience against node capture and replication attacks, and quorum-based key revocation.

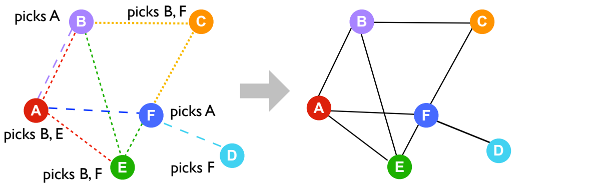

Fig. 1. A WSN with 6 nodes secured by the heterogeneous random pairwise key predistribution scheme. Each type-1 (resp. type-2) node randomly selects 1 (resp. $K_n=2$) node and a unique pairwise key is given to node pairs per selection; in this example, nodes A, C and E are type-2 and the rest (B, D, F) are type-1. Two nodes can communicate securely if they have at least one key in common. This induces a graph with edges corresponding to node pairs that share a key.

When all sensors can communicate with each other meaning that one-hop secure communication between a pair of sensors hinges solely on them having a common key, pairwise scheme induces a class of random graphs known as *random K-out graphs* [9]–[12] constructed as follows. Each of the n nodes draws K arcs towards K distinct nodes chosen uniformly at random among all others. The orientation of the arcs is then ignored, yielding an *undirected* graph.

Let $\mathbb{H}(n;K)$ denote the resulting random K-out graph whose edges represent the secure communication links of the corresponding WSN. A key question in the design of secure WSNs under a *random* key predistribution scheme is how to set the scheme parameters so that the resulting network has certain desirable properties with high probability; e.g., connectivity [2], [11], [13]–[15], reliability against node/edge failures [12], [16]–[18], resilience against node capture attacks [19], [20], containing a connected sub-network with a *large* number of nodes [19], [21], etc. Some of these questions have been answered for the standard (i.e., homogeneous) pairwise scheme through analyzing random K-out graphs. In particular, it was shown [10], [11] that if $K \geq 2$, then the resulting graph is 1-connected with high probability. More precisely, the following zero-one law holds:

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

Recently deployed networks are increasingly relying on integrating information from sensor nodes with widely varying resources and requirements [22]–[24]. The increasing adoption of heterogeneous designs has also been in response to the poor performance and scalability of homogeneous ad-hoc networks; see [25] and the references therein. A growing body of literature is now analyzing heterogeneous variants of classical key predistribution schemes [8], [25]–[28]. In order to design a secure network comprising of nodes with differing 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, $1 - \mu$), where $0 < \mu < 1$. 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 $\mathbb{H}(n; \mu, K_n)$. So far, very little is known, concerning aforementioned design questions, about the heterogeneous pairwise scheme and the induced random graph $\mathbb{H}(n; \mu, K_n)$. The analysis of its 1-connectivity given in [8] yielded the surprising result that

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

This paper aims to study 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].In the context of WSNs, the property of k-connectivity is highly desirable since it provides a degree of fault tolerance when aggregating information from multiple sensors [31]. Reliability against the failure of sensors or links is particularly critical in applications where the risk of adversarial capture is high, e.g., in battlefield surveillance and applications in which the sensors maybe left unattended for long time [32], [33]. Reliability is also important in life-critical applications such as health monitoring. Finally, a k-connected WSN can at any given time support up to $k-1$ mobile nodes without disrupting connectivity [33].

In [34, Conjecture 2], we conjectured that, taking evidence from several other random graph models [29], [33], [35], there would exist a zero-one law for k-connectivity analogous to the zero-one law for the minimum node degree being at least k. In this work, we prove that this conjecture indeed holds. We derive scaling conditions on μ, K_n such that the inhomogeneous random K-out graph is k-connected asymptotically almost surely as n gets large, where $k = 2, 3, \ldots$. We present our result in terms of a sharp zero-one law. For any $k \geq 2$, we show that if $K_n = \frac{1}{1-\mu}(\log n + (k-2)\log\log n + \omega(1))$, then $\mathbb{H}(n; \mu, K_n)$ is k-connected asymptotically almost surely (a.a.s.). In contrast, if $K_n = \frac{1}{1-\mu}(\log n + (k-2)\log\log n - \omega(1))$, then $\mathbb{H}(n; \mu, K_n)$ is a.a.s. *not* k-connected.

This result shows that if there is a positive fraction of type-1 nodes, then type-2 nodes must make $K_n = \Omega(\log n)$ selections for the network to achieve k-connectivity for any $k = 2, 3, \ldots$. This is rather unexpected given that the network is a.a.s. 1-connected under any $K_n = \omega(1)$. The result is also in contrast with most other random graph models where the zero-one law for k-connectivity appears in a form that reduces to a zero-one law for 1-connectivity by simply setting $k = 1$. Through simulations we study the impact of the parameters (μ, K_n) on the probability of k-connectivity when the number of nodes is finite and observe an agreement with our asymptotic results.

The heterogeneity of node types makes $\mathbb{H}(n; \mu, K_n)$ a complicated model and the proofs involve techniques that are different from those used for the homogeneous K-out random graph [10], [11]. Moreover, the proof for this case varies significantly from results on 1-connectivity for inhomogeneous random K-out graphs [8] and uses new tools including *conditional* negative association (of certain random variables of interest) introduced recently in [36].

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 $a_n = \mathrm{o}(b_n)$, $a_n = \omega(b_n)$, $a_n = \mathrm{O}(b_n)$, $a_n = \Theta(b_n)$, 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 say that an event occurs with high probability (whp) or asymptotically almost surely (a.a.s.) if it holds with *probability tending to one* as $n \to \infty$. The cardinality of a discrete set A is denoted by $|A|$ and the set of all positive integers by $\mathbb{N}_0$.

II. Inhomogeneous Random K-out Graphs

In order to facilitate heterogeneous network designs, [8] extended the pairwise scheme of Chan et al. [7] for enabling incorporation of sensor nodes differing in their resources and requirements. The heterogeneous random pairwise key predistribution scheme is implemented as follows. Consider a network comprising of n nodes indexed by labels $i = 1, 2, \ldots n$ with unique IDs: $\mathrm{Id}_1, \ldots, \mathrm{Id}_n$. Each node is assigned 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 node (respectively, type-2 node) selects K_1 (respectively, K_2) distinct nodes uniformly at random from among all other nodes. At the end

[1] The notion of k-connectivity used in this paper coincides with k-vertex connectivity, which is defined as the property that the graph remains connected after deletion of any $k-1$ vertices. It is known 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 [29], [30, p. 11]. 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.

of this process, nodes v_i and v_j are deemed to be *paired* if at least one of them selected the other; i.e., either v_i selects v_j, or v_j selects v_i, or both.

Once the offline pairing process is complete, the set of keys to be inserted to nodes are determined as follows. For any v_i, v_j that are *paired* with each other as described above, a unique pairwise key ω_{ij} is generated and inserted in the memory modules of both nodes v_i and v_j along with the corresponding node IDs. It is important to note that ω_{ij} is assigned *exclusively* to nodes v_i and v_j to be used solely in securing the communication between them. 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].

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 $K_1, K_2, \ldots$ need to be studied separately. 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. Let $\mathcal{N} := \{1, 2, \ldots, n\}$ denote the set of node labels and $\mathcal{N}_{-i} := \{1, 2, \ldots, n\} \setminus i$. For each $i \in \mathcal{N}$, let $\Gamma_{n,i} \subseteq \mathcal{N}_{-i}$ denote the labels corresponding to the selections made by node v_i from $\mathcal{N}_{-i}$ uniformly at random. Under the assumptions enforced, $\Gamma_{n,1}, \ldots, \Gamma_{n,n}$ are mutually independent given the types of nodes.

Under the *full-visibility* assumption, i.e., when one-hop secure communication between a pair of sensors hinges solely on them having a common key, 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. We say that two distinct nodes v_i and v_j are adjacent, denoted by $v_i \sim v_j$ if they have at least one common key in their respective key rings. More formally, we have

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

The adjacency condition (1) gives rise to the inhomogeneous random K-out graph on the vertex set on the vertex set $\{v_1, \ldots, v_n\}$. We denote this graph as $\mathbb{H}(n; \mu, K_n)$, which explicitly reflects the dependence of the induced random graph on the scheme parameters μ and K_n. Lastly, noting that with probability μ (resp., $1 - \mu$), a node is labeled as type-1 (resp., type-2) and selects 1 (resp., K_n) neighbors, the average number of selections per node denoted by $\langle K_n \rangle$ is given by

$$\langle K_n \rangle = \mu + (1 - \mu) K_n. \tag{2}$$

In view of their distinctive connectivity properties, (inhomogeneous) random K-out graphs are of interest in their own right with applications going beyond key predistribution in WSNs. For example, a recent work proposed a structure similar to the random K-out graph to enable diffusion by proxy thereby making the cryptocurrency network robust to de-anonymization attacks [37, Algorithm 1].

III. Results and Discussion

In this section, we present our main technical result: a zero-one law for k-connectivity of inhomogeneous random K-out graphs induced by the pairwise key predistribution scheme.

A. Main results

We refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying the conditions $2 \leq K_n < n$ for all $n = 2, 3, \ldots$ as a *scaling*. We say that a graph is k-connected if it remains connected despite the deletion of any $k-1$ vertices or edges. Next, we present our first main result that characterizes the critical scaling of the scheme parameters (μ, K_n) under which the inhomogeneous random K-out graph $\mathbb{H}(n; \mu, K_n)$ is k-connected asymptotically almost surely.

Theorem 3.1: 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 an integer* $k \geq 2$ *let the sequence* $\gamma : \mathbb{N}_0 \to \mathbb{R}$ *be defined through*

$$\langle K_n \rangle = \log n + (k - 2) \log \log n + \gamma_n, \tag{3}$$

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

$$\lim_{n \to \infty} \mathbb{P} \left[\begin{array}{l} \mathbb{H}(n; \mu, K_n) \textit{ is} \\ k\textit{-connected} \end{array} \right] = \begin{cases} 1 & \textit{if } \lim_{n \to \infty} \gamma_n = +\infty, \\ 0 & \textit{if } \lim_{n \to \infty} \gamma_n = -\infty. \end{cases} \tag{4}$$

Due to space limit, we provide a brief proof sketch in the Appendix. The full proof of Theorem 3.1 is given in [38].

We note that (3) presents solely a definition of the sequence γ_n without any loss of generality; it does not an impose any assumption on the parameters (μ, K_n). The scaling condition (3) could also be expressed more explicitly in terms of K_n as

$$K_n = \frac{\log n + (k - 2) \log \log n}{1 - \mu} + \gamma_n \tag{5}$$

with the corresponding zero-one law (4) unchanged.

Theorem 3.1 provides a sharp zero-one law for the k-connectivity of the random graph $\mathbb{H}(n; \mu, K_n)$ as the size of the network grows large. Put differently, it establishes *critical* scaling conditions on the parameters of the pairwise scheme (μ, K_n) under which the resulting WSN will be securely and reliably connected whp. We see from [34, Theorem 1] that the critical scaling conditions for k-connectivity coincide with those for the minimum node degree to be at least k. This is similar to the case with most random graph models including Erdős-Rényi (ER) graphs [29], random key graphs [33] and random geometric graphs [35].

It follows from Theorem 3.1 that if there is a positive fraction μ of type-1 nodes, then type-2 nodes must make $K_n = \Omega(\log n)$ selections for the network to achieve k-connectivity for any $k = 2, 3, \ldots$. As discussed below, this result is rather unexpected given that the network is a.a.s. 1-connected under any $K_n = \omega(1)$ as shown in [27]. This gap between 1-connectivity and k-connectivity for $k \geq 2$ is in contrast with most other random graph models where the zero-one law for k-connectivity appears in a form that reduces to a zero-one law for 1-connectivity by simply setting $k = 1$; see more in Section III-B.

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

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.

B. Discussion

We discuss some of the implications of Theorems 3.1 on the reliable connectivity of WSNs under the heterogeneous pairwise key predistribution scheme. In particular, our results will be compared against those obtained for other key predistribution schemes including the homogeneous pairwise scheme.

With E_{ij} denoting the event that there exists an edge in $\mathbb{H}(n;\mu,K_n)$ between nodes v_i and v_j, we have

$$\begin{aligned}\mathbb{P}[E_{ij}] &= 1-(1-\mathbb{P}[i\in\Gamma_{n,j}])(1-\mathbb{P}[j\in\Gamma_{n,i}]),\\ &= 1-\left(1-\frac{\langle K_n\rangle}{n-1}\right)^2 = \frac{2\langle K_n\rangle}{n-1}-\left(\frac{\langle K_n\rangle}{n-1}\right)^2. \quad (6)\end{aligned}$$

Thus, if $\langle K_n\rangle = \mathrm{o}(n)$, then the mean degree in $\mathbb{H}(n;\mu,K_n)$ is $2\langle K_n\rangle(1+o(1))$, while the mean degree of type-1 nodes is $1+\langle K_n\rangle$. Table I presents a comparison of the mean node degree needed for having 1-connectivity and k-connectivity a.a.s. for homogeneous and inhomogeneous random K-out graphs [8], [10], and *random key graphs* induced by the Eschenauer-Gligor scheme [2], [26], [28], [39]. For inhomogeneous models, the table entries correspond to the mean degree of the *least connected* node type. We also included the corresponding results for ER graphs [29] for comparison.

An interesting observation is that for the inhomogeneous K-out graph, increasing the strength of connectivity from 1 to $k \geq 2$ 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 fact, for most random graph models, the zero-one law for 1 connectivity can be obtained from the corresponding result for k-connectivity by setting $k=1$; this can be confirmed from the entries in Table I for homogeneous/inhomogeneous random key graphs and ER graphs. To the best of our knowledge, inhomogeneous K-out graphs is the only model where the critical scalings for 1-connectivity and 2-connectivity differ significantly.

From the perspective of key predistribution schemes, 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 and k-connectivity. Theorem 3.1 and the results in [27] show that the efficiency of the pairwise scheme in achieving reliable connectivity *reduces* when sensors involved are heterogeneous and the application requires setting $K_1 = 1$; i.e., when a positive fraction of nodes picks just one other node to be paired with. Nevertheless, it is still the case that the heterogeneous pairwise scheme requires slightly smaller mean degree and number of keys per node than the heterogeneous Eschenuer-Gligor scheme [28]; compare the entries for inhomogeneous K-out graph with inhomogeneous random key graph in Table I.

C. Simulations

We present simulation results to show the impact of the number of choices made by type-2 nodes (K_n) and the probability of a node being assigned type-1 (μ) on the probability that the resulting WSN is k-connected. We consider a network of $n = 1000$ nodes secured by the heterogeneous pairwise scheme with parameters $\mu = 0.2, 0.5, 0.8$ and varying K_n. For each parameter tuple (n,μ,K_n,k), 1000 independent realizations for $\mathbb{H}(n;\mu,K_n)$ are generated and empirical probability of k-connectivity is plotted in Figure 2.

A smaller value of μ corresponds to a network dominated by type-2 nodes. Consequently, for a low μ regime, the resulting graph is more dense and we expect to see stronger connectivity. Conversely, when μ is large, it takes a higher value for the parameter K_n to achieve the same strength of connectivity. This trend is reflected in Figure 2 wherein the minimum K_n required to make the network k-connected whp increases as μ increases. We point out that the scale of the plots for different μ has been chosen differently for compactly reporting roughly the same number of values of K_n on either side of the phase transition. Whenever a network is k-connected, it automatically implies that the network is ℓ-connected for all $\ell < k$. This manifests as the upward shift in the probability of connectivity as k decreases in Figure 2.

The vertical dashed lines seen in Figure 2 correspond to the *critical* thresholds of K_n indicated by Theorem 3.1; i.e., to

$$K_n = \left\lceil \frac{\log n + (k-2)\log\log n}{1-\mu} \right\rceil. \quad (7)$$

It is evident that the probability of k-connectivity increases sharply from 0 to 1 within a small neighborhood of K_n defined in (7). The last plot in Figure 2 shows the largest value of k for which the network is k-connected in at least 990 out of 1000 realizations for a given μ and K_n. From this plot, we see that to achieve a desired level of reliable connectivity with a probability of at least 99%, a network designer can trade-off a smaller K_n for a larger value of $1-\mu$ and vice versa. For instance, if the goal is to design a secure network of 1000 nodes which is 3-connected with probability 0.99, this can be achieved by setting the parameters (K_n,μ) as $(15, 0.1)$, or $(20, 0.3)$ or $(30, 0.5)$.

IV. Conclusion

In this work, we analyze reliable connectivity of sensor networks secured by the heterogeneous pairwise key predistribution scheme. In particular, for the inhomogeneous random

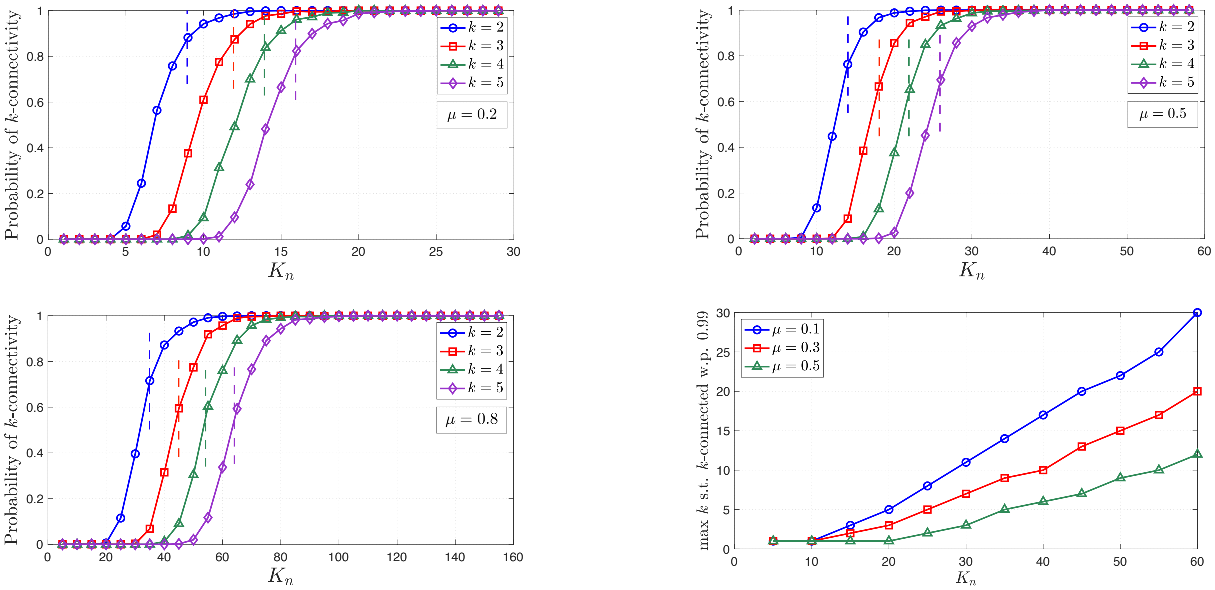

Fig. 2. Empirical probability of k-connectivity of $\mathbb{H}(n;\mu,K_n)$ averaged over $1,000$ experiments when $n = 1000$, varying K_n and three different μ values; K_n is the number of choices made by type-2 nodes and μ is the fraction of type-1 nodes. The vertical dashed lines in indicate the threshold $K_n = \left\lceil \frac{\log n + (k-2)\log\log n}{1-\mu} \right\rceil$ corresponding to the scaling condition (5) in Theorem 3.1. The last plot shows the maximum value of k such that $\mathbb{H}(n;\mu,K_n)$ is k-connected with probability (w.p.) at least 0.99.

K-out graphs induced under this scheme, we derive conditions on the scheme parameters such that the resulting network is k-connected with probability approaching one (respectively, zero) as the number of nodes gets large for $k = 2, 3, \ldots$. Our result augments the existing literature on providing formal guarantees on 1-connectivity of the class of random graphs secured by the heterogeneous pairwise scheme. In the future, it would be of interest to analyze k-connectivity of inhomogeneous random K-out graphs with $r > 2$ node types and arbitrary parameters $K_1, \ldots, K_r$ associated with each type.

V. Proof Outline

In this section, we outline the high-level steps of the proof of Theorem 3.1. Due to space constraints, the full proof is presented in [38].

A. Zero-law: From minimum node degree to k-connectivity

Let δ denote the *minimum* node degree in $\mathbb{H}(n;\mu,K_n)$, i.e., $\delta := \min_{i=1,\ldots,n}\{\deg(v_i)\}$, with $\deg(v_i)$ denoting the number of edges incident on vertex v_i.

Let κ_v denote the *minimum* number of vertices that need to be removed from $\mathbb{H}(n;\mu,K_n)$ to make it *not* connected. As before, we say that $\mathbb{H}(n;\mu,K_n)$ is k-connected if $\kappa_v \geq k$. We always have $\kappa_v \leq \delta$ since removing all neighbors of a node with degree δ would render the node *isolated*, making the graph disconnected. Thus, for all $k = 1, 2, \ldots$, it holds that $[\kappa_v \geq k] \subseteq [\delta \geq k]$, which gives

$$\mathbb{P}[\kappa_v \geq k] \leq \mathbb{P}[\delta \geq k]. \tag{8}$$

In view of (8), the zero-law given in [34, Theorem 1] leads to

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n;\mu,K_n) \text{ is } k\text{-connected}\right] = 0 \quad \text{if} \quad \lim_{n\to\infty} \gamma_n = -\infty \tag{9}$$

establishing the zero-law of Theorem 3.1.

B. A sufficient condition for the one-law for k-connectivity

We now discuss the one-law of Theorem 3.1, namely showing that $\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n;\mu,K_n) \text{ is } k\text{-connected}\right] = 1$ if $\lim_{n\to\infty} \gamma_n = +\infty$. From [34, Theorem 1] we see that $\mathbb{P}[\delta \geq k] \to 1$ when $\gamma_n \to +\infty$. Recalling that $[\kappa_v \geq k] \subseteq [\delta \geq k]$, we write

$$\begin{aligned}
\mathbb{P}[\kappa_v \geq k] &= \mathbb{P}[\kappa_v \geq k,\ \delta \geq k] \\
&= \mathbb{P}[\delta \geq k] - \mathbb{P}[\delta \geq k, \kappa_v < k], \qquad (10)\\
&= \mathbb{P}[\delta \geq k] - \mathbb{P}\left[\cup_{\ell=0}^{k-1}\{\delta \geq k, \kappa_v = \ell\}\right] \\
&\geq \mathbb{P}[\delta \geq k] - \mathbb{P}\left[\cup_{\ell=0}^{k-1}\{\delta > \ell, \kappa_v = \ell\}\right] \\
&= \mathbb{P}[\delta \geq k] - \sum_{\ell=0}^{k-1} \mathbb{P}\left[\delta > \ell, \kappa_v = \ell\right]. \qquad (11)
\end{aligned}$$

Using the one-law of [34, Theorem 1] in (11), we see that the one-law for k-connectivity will follow if we establish that

$$\lim_{n\to\infty} \mathbb{P}[\delta > \ell, \kappa_v = \ell] = 0 \quad \text{if} \quad \lim_{n\to\infty} \gamma_n = +\infty \tag{12}$$

for each $\ell = 0, 1, \ldots, k-1$.

Conditions in (12) encode the *improbability* for $\mathbb{H}(n;\mu,K_n)$ to have minimum node degree of at least $\ell + 1$ and yet be disconnected by deletion of a set of ℓ nodes. The proof presented in [38] establishes (12) by deriving a tight upper bound on $\mathbb{P}[\delta > \ell, \kappa_v = \ell]$ which goes to zero as n gets large for each $\ell = 0, 1, \ldots, k-1$.

Acknowledgment

This work has been supported in part by National Science Foundation through grant CCF #1617934.

References

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

[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47. [Online]. Available: http://doi.acm.org/10.1145/586110.586117

[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] D. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica*, vol. 32, no. 6, p. 900, 2006.

[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, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, pp. 2314 – 2341, 2007, special issue on security on wireless ad hoc and sensor networks. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366407001752

[7] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of IEEE S&P 2003*, 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 random m-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] O. Yağan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3821–3835, June 2012.

[14] O. Yağan and A. M. Makowski, "Modeling the pairwise key predistribution scheme in the presence of unreliable links," *Information Theory, IEEE Transactions on*, vol. 59, no. 3, pp. 1740–1760, March 2013.

[15] K. Rybarczyk, "Diameter, connectivity, and phase transition of the uniform random intersection graph," *Discrete Mathematics*, vol. 311, no. 17, pp. 1998–2019, 2011.

[16] J. Zhao, O. Yağan, and V. Gligor, "On connectivity and robustness in random intersection graphs," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2121–2136, May 2017.

[17] H. Zhang and S. Sundaram, "Robustness of complex networks with implications for consensus and contagion," in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*. IEEE, 2012, pp. 3426–3432.

[18] F. Yavuz, J. Zhao, O. Yağan, and V. Gligor, "k-connectivity in random k-out graphs intersecting erdős-rényi graphs," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1677–1692, 2017.

[19] A. Mei, A. Panconesi, and J. Radhakrishnan, "Unassailable sensor networks," in *Proc. of the 4th International Conference on Security and Privacy in Communication Netowrks*, ser. SecureComm '08. New York, NY, USA: ACM, 2008.

[20] O. Yağan and A. M. Makowski, "Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?" *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, pp. 1–14, 2016.

[21] M. Bloznelis, J. Jaworski, and K. Rybarczyk, "Component evolution in a secure wireless sensor network," *Netw.*, vol. 53, pp. 19–26, 2009.

[22] K. Lu, Y. Qian, M. Guizani, and H.-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.

[23] 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.

[24] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2, March 2005, pp. 878–890 vol. 2.

[25] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.

[26] R. Eletreby and O. Yağan, "k-connectivity of inhomogeneous random key graphs with unreliable links," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3922–3949, June 2019.

[27] ——, "Connectivity of wireless sensor networks secured by heterogeneous key predistribution under an on/off channel model," *IEEE Transactions on Control of Network Systems*, 2018.

[28] 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.

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

[30] R. Diestel, *Graph Theory*, ser. Electronic library of mathematics. Springer, 2006. [Online]. Available: https://books.google.com/books?id=aR2TMYQr2CMC

[31] X. Liu, "Coverage with connectivity in wireless sensor networks," in *2006 3rd International Conference on Broadband Communications, Networks and Systems*. IEEE, 2006, pp. 1–8.

[32] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key predistribution scheme: Gradual deployment and key ring sizes," *Performance Evaluation*, vol. 70, no. 7-8, pp. 493–512, 2013.

[33] J. Zhao, O. Yağan, 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.

[34] M. Sood and O. Yağan, "Towards k-connectivity in Heterogeneous Sensor Networks under Pairwise Key Predistribution," *arXiv e-prints*, p. arXiv:1907.08049, Jul 2019.

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

[36] D.-M. Yuan, J. An, and X.-S. Wu, "Conditional limit theorems for conditionally negatively associated random variables," *Monatshefte für Mathematik*, vol. 161, no. 4, pp. 449–473, 2010.

[37] 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.

[38] M. Sood and O. Yağan, "A zero-one law for k-connectivity in imhomogeneous random k-out graphs," full version available online at https://www.andrew.cmu.edu/user/oyagan/Conferences/ISIT2020kcon.pdf.

[39] 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.