Connectivity of Wireless Sensor Networks Secured by The Heterogeneous Random Pairwise Key Predistribution Scheme

Rashad Eletreby and Osman Yağan

***Abstract*— We investigate the connectivity of wireless sensor networks secured by the heterogeneous random pairwise key predistribution scheme. In contrast to the homogeneous scheme proposed by Chan et al., where each node is paired (offline) with K other nodes chosen uniformly at random; herein, each node is classified as class-1 with probability μ or class-2 with probability $1-\mu$, for $0<\mu<1$, independently. Then, each class-1 (respectively, class-2) node is paired (offline) with K_1 (respectively, K_2) other nodes selected uniformly at random. We consider the particular case when $K_1=1$ and $K_2=K$. The heterogeneous random pairwise scheme induces an inhomogeneous random K-out graph $\mathbb{H}(n;\mu,K_n)$, where n denotes the number of nodes and K_n denotes a scaling of K with respect to the network size n. Hence, establishing the connectivity of wireless sensor networks secured by the heterogeneous random pairwise scheme maps to deriving conditions on how to scale K_n with respect to the network size n such that the graph is connected with high probability as n tends to infinity. With $K_1=1$, we show that i) when $K_n=K$ for all $n=2,3,\ldots$ for a positive, finite integer K with $K\geq 2$, the resulting graph is *not* connected with a positive probability. In this case, we derive a tight upper bound on the probability of connectivity and verify the results via simulations. Moreover, ii) we prove that when K_n is chosen such that $\lim_{n\to\infty} K_n=\infty$, the graph is connected with high probability as n tends to infinity.**

Keywords: Random graphs, Connectivity, Security.

I. Introduction

Wireless sensor networks (WSNs) provide numerous applications in diverse areas such as battlefield surveillance, environmental sensing, health care monitoring, among others [1]. Such a broad portfolio of applications is possible thanks to the unique characteristics of WSNs, namely their low cost, low power consumption, ease of deployment, mobility, and scalability [2]. Although these characteristics have led to the widespread adoption of WSNs in multiple contexts, they do, however, pose a serious concern regarding the *security* aspect of the network [3].

WSNs are usually deployed in hostile environments and left unattended, thus they should be equipped with security mechanisms to defend against attacks such as node capture attacks and eavesdropping. The unique characteristics of WSNs, however, prevent the use of standard cryptosystems that were developed for more capable networks [3]. For instance, public-key cryptosystems are deemed too complex for WSNs as they require excessive energy consumption and computational overhead [4]. On the other hand, symmetric cryptosystems were shown to require much less energy, but their key distribution mechanisms were inadequate for WSNs. For instance, using a single-mission key would render the network extremely vulnerable to node-capture attacks, while using pairwise keys for each pair of nodes would require huge memory requirements.

Random key *pre*-distribution schemes were introduced in the seminal work of Eschenauer and Gligor [4] with the aim of establishing lightweight key distribution mechanisms that are suitable for WSNs, hence allowing symmetric cryptosystems to be utilized in commodity WSNs. Since then, researchers have pushed the frontiers of WSN security research and come up with a multitude of practical mechanisms for random key distribution in WSNs. One of these prominent schemes is the random pairwise key predistribution scheme proposed by Chan et al. in [5]. The random pairwise predistribution scheme has a number of advantages over the original scheme of Eschenauer and Gligor: (i) It is *perfectly resilient* against node capture attacks [5]; (ii) Unlike earlier schemes, this pairwise scheme enables both distributed node-to-node authentication and quorum-based node revocation.

The random pairwise scheme is described as follows: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from among all other nodes. If nodes i and j were paired during the node-pairing stage (i.e., which happens if either node i gets paired with node j, node j gets paired with node i, or both), a unique (pairwise) key is generated and stored in the memory modules of each of the paired sensors together with both their IDs. After deployment, a secure link can be established between two communicating nodes if they have at least one pairwise key in common. The random pairwise scheme gives rise to a class of random graphs denoted by *random K-out graphs* [6], [7]. In particular, Let $\mathbb{H}(n;K)$ denote the random graph on the vertex set $\{1,\ldots,n\}$ where distinct nodes i and j are adjacent if they have at least one pairwise key in common. This random graph models the random pairwise key predistribution scheme under full visibility (whereby all nodes are within wireless communication range of each other).

Consider a WSN secured by the random pairwise scheme. A natural question to ask is: *How should the value of K be selected so that the resulting network is securely connected?*, i.e., there exists a secure communication path between every pair of nodes. After all, the randomness involved in the node-pairing process could give rise to isolated components of nodes that are paired with each others but not to other nodes, rendering the network *disconnected*. The connectivity of the random pairwise scheme was investigated in [8], where it

R. Eletreby and O. Yağan are with Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Pittsburgh, PA, 15213 USA. Email: {reletreby@cmu.edu, oyagan@ece.cmu.edu}

was shown that

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

In other words, it is sufficient to set $K = 2$ to obtain a network that is connected with high probability as the network size tends to infinity (a tight bound for the case of finite n was also given in [8]).

We present a heterogeneous variant of the random pairwise scheme where nodes are classified into two classes according to their characteristics as well as their connectivity and security requirements. In particular, we consider the case where each node is classified as class-1 with probability μ or class-2 with probability $1-\mu$ for $0 < \mu < 1$, independently. Each of class-1 (respectively, class-2) nodes is paired with K_1 (respectively, K_2) other nodes, independently. As with the original scheme, if nodes i and j were paired in the (offline) node-pairing process (i.e., which happens when either node i gets paired with node j, node j gets paired with node i, or both), a unique (pairwise) key is generated and stored in the memory modules of nodes i and j together with both their IDs. After deployment, a secure link can be established between nodes i and j if they have at least one pairwise key in common. With $\boldsymbol{\mu} = (\mu, 1-\mu)$ and $\boldsymbol{K} = (K_1, K_2)$, the *heterogeneous* random pairwise scheme gives rise to the *inhomogeneous* random K-out graph $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}\right)$ where distinct nodes i and j are adjacent if they have at least one pairwise key in common. Specific details are given in Section II.

Our paper is motivated by the following question. *Consider the particular case when $K_1 = 1$ and $K_2 = K$. How should the value of K be selected (perhaps as a function of the network size n) such that the resulting network is connected with high probability?* An appealing answer would be to draw on the results given in [8] (see (1)), perhaps by setting K such that $\mathbb{E}\left[\mathcal{K}\right] = \mu + (1-\mu)K \geq 2$, where $\mathcal{K}$ denotes a random variable that takes the value 1 with probability μ and the value K with probability $1-\mu$. In other words, $\mathbb{E}\left[\mathcal{K}\right]$ gives the *mean* number of nodes that an arbitrary node gets paired with. We show that such an approach, although appealing, generates networks that are *not connected* with positive probability. In particular, we show that when $K_1 = 1$, choosing any *finite* integer value of K (with $K \geq 2$) would render the graph not connected with a positive probability that depends on μ and K. Surprisingly, we show that for the resulting graph to be connected with high probability, K has to scale with the network size n such that $\lim_{n\to\infty} K_n = \infty$. Our results on the one-law of connectivity do not enforce a particular dependency between the sequences K_n and n, other than $\lim_{n\to\infty} K_n = \infty$, hence K_n need only be selected such that it eventually tends to infinity as n tends to infinity, e.g., $K_n = \log\log\ldots\log n$.

II. System Model

All statements involving limits, including asymptotic equivalences, are understood with n going to infinity. The cardinality of any discrete set S is denoted by $|S|$. The random variables (rvs) under consideration are all 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 holds with high probability (whp) if it holds with probability 1 as $n \to \infty$.

A. The heterogeneous random pairwise key predistribution scheme

The heterogeneous random pairwise key predistribution scheme builds on the homogeneous scheme of Chan et al. [5]. In particular, we consider a network consisting of n nodes which are labelled $i = 1, \ldots, n$ with unique ids $\mathrm{Id}_1, \ldots, \mathrm{Id}_n$. In contrast to the homogeneous scheme proposed by Chan et al., where each node is paired (offline) with K other nodes chosen uniformly at random; herein, each node is classified as class-1 with probability μ or class-2 with probability $1-\mu$, for $0 < \mu < 1$, independently. Then, each class-1 (respectively, class-2) node is paired (offline) with K_1 (respectively, K_2) other nodes selected uniformly at random. As with the homogeneous scheme, two nodes i and j can communicate securely after deployment if either i was paired with j or j was paired with i or both. Throughout, we focus on the particular case with $K_1 = 1$ and $K_2 = K$, hence we simplify our notations by writing K instead of $\boldsymbol{K} = (1, K)$ and μ instead of $\boldsymbol{\mu} = (\mu, 1-\mu)$. We assume that the probability μ is fixed and does not scale with n, while K is assumed to be scaled with n. Write $\mathcal{N} := \{1, \ldots n\}$, and set $\mathcal{N}_{-i} := \mathcal{N} \backslash \{i\}$ for each $i = 1, \ldots, n$. Formally speaking, with node i we associate a subset $\Gamma_{n,i}(\mu, K)$ (whose size depends on the class of node i) of nodes selected at *random* from $\mathcal{N}_{-i}$. Each of the nodes in $\Gamma_{n,i}(\mu, K)$ is said to be *paired* to node i. Specifically, for any subset $A \subseteq \mathcal{N}_{-i}$, we require

$$\mathbb{P}\left[\Gamma_{n,i}(\mu, K) = A \,\middle|\, t_i = j\right] = \begin{cases} \binom{n-1}{K_j}^{-1} & \text{if } |A| = K_j \\ \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where t_i denotes the class of node i, $K_1 = 1$, and $K_2 = K$. Thus, the selection of $\Gamma_{n,i}(\mu, K)$ is done *uniformly* among all subsets of $\mathcal{N}_{-i}$ whose sizes depend on the class of node i. In particular, if node i is class-1 (respectively, class-2), the selection is done uniformly at random among all subsets of $\mathcal{N}_{-i}$ of size exactly 1 (respectively, K). The random variables $\Gamma_{n,1}(\mu, K), \ldots, \Gamma_{n,n}(\mu, K)$ are assumed to be *mutually independent* so that

$$\begin{aligned} &\mathbb{P}\left[\Gamma_{n,i}(\mu, K) = A_i \,\middle|\, t_i,\ i = 1, \ldots, n\right] \\ &= \prod_{i=1}^{n} \mathbb{P}\left[\Gamma_{n,i}(\mu, K) = A_i \,\middle|\, t_i\right] \end{aligned} \tag{3}$$

for arbitrary $A_1, \ldots, A_n$ subsets of $\mathcal{N}_{-1}, \ldots, \mathcal{N}_{-n}$, respectively.

Once this offline random pairing has been created, we construct the key rings $\Sigma_{n,1}(\mu, K), \ldots, \Sigma_{n,n}(\mu, K)$, in the memory modules of the corresponding nodes as follows: if

$$i \in \Gamma_{n,j}(\mu, K) \vee j \in \Gamma_{n,j}(\mu, K)$$

then, a unique pairwise key ω_{ij} is generated and stored in both $\Sigma_{n,i}(\mu, K)$ and $\Sigma_{n,j}(\mu, K)$ along with the IDs of both nodes. Note that the key ω_{ij} is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise predistribution scheme.

After deployment, each node first broadcasts its ID to its immediate neighbors. Once a neighbor node receives the broadcast, it searches its key ring for the ID of the broadcasting node to tell if they share a common pairwise key for secure communication. Secure communication can then take place between key-sharing nodes by means of a cryptographic handshake [5].

As mentioned earlier, under full visibility, two nodes, say i and j, can establish a secure link if at least one of the events $i \in \Gamma_{n,j}(\mu, K)$ or $j \in \Gamma_{n,j}(\mu, K)$ is taking place. Note that both events can take place, in which case the memory modules of node i and j both contain the distinct keys ω_{ij} and ω_{ji}. By construction this scheme supports node-to-node authentication.

B. Inhomogeneous random K-out graph

Under full visibility the heterogeneous pairwise key predistribution scheme naturally gives rise to the inhomogeneous random K-out graph, defined as follows: With $n = 2, 3, \ldots$, $0 < \mu < 1$ and positive integer $K < n$, we say that the distinct nodes i and j are adjacent, written $i \sim j$, if and only if they have at least one key in common in their key rings, namely

$$i \sim j \quad \text{iff} \quad \Sigma_{n,i}(\mu, K) \cap \Sigma_{n,j}(\mu, K) \neq \emptyset,$$

or, equivalently

$$i \sim j \quad \text{iff} \quad i \in \Gamma_{n,j}(\mu, K) \vee j \in \Gamma_{n,j}(\mu, K). \tag{4}$$

Let $\mathbb{H}(n; \mu, K)$ denote the undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacency notion (4). The homogeneous case, when all nodes belong to the same class and are paired with K other nodes at random reduces to the homogeneous random K-out graph $\mathbb{H}(n; K)$ [6], [7].

III. Main results

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

$$K_n < n, \quad n = 2, 3, \ldots.$$

Our main technical results, given next, characterize the connectivity of the inhomogeneous random K-out graph induced by the heterogeneous random pairwise key predistribution scheme. Throughout, it will be convenient to use the notation

$$P(n; \mu, K_n) := \mathbb{P}\left[\mathbb{H}(n; \mu, K_n) \text{ is connected}\right]$$

and

$$C(\mu, K) = \frac{1}{1 + \frac{2e^2}{\mu^2} e^{2(1-\mu)(K-1)}} \tag{5}$$

with $0 < \mu < 1$ and a positive, finite-integer K.

The following result establishes an upper bound on the probability of connectivity of inhomogeneous random K-out graphs when $K_n = K$ for all $n = 2, 3, \ldots$, where K is a positive, finite integer with $K \geq 2$.

Theorem 3.1: Consider a probability distribution $\boldsymbol{\mu} = (\mu, 1-\mu)$ with $\mu > 0$ such that a vertex is labeled as class-1 with probability μ or class-2 with probability $1-\mu$. Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n = K$ for all $n = 2, 3, \ldots$, where K is a positive, finite integer with $K \geq 2$. It holds that

$$\limsup_{n \to \infty} P(n; \mu, K_n) \leq 1 - C(\mu, K)$$

The following result establishes a one-law for connectivity of inhomogeneous random K-out graphs when $\lim_{n\to\infty} K_n = \infty$.

Theorem 3.2: Consider a probability distribution $\boldsymbol{\mu} = (\mu, 1-\mu)$ with $\mu > 0$ such that a vertex is labeled as class-1 with probability μ or class-2 with probability $1-\mu$. Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $\lim_{n\to\infty} K_n = \infty$. It holds that

$$\lim_{n \to \infty} P(n; \mu, K_n) = 1$$

Theorems 3.1 and 3.2 state that $\mathbb{H}(n; \mu, K_n)$ is connected with high probability if K_n is chosen such that $\lim_{n\to\infty} K_n = \infty$. On the other hand, if K_n is chosen such that $K_n = K$ for all $n = 2, 3, \ldots$, where K is a positive, finite integer with $K \geq 2$, the probability of connectivity of $\mathbb{H}(n; \mu, K_n)$ is bounded from above by $1 - C(\mu, K)$ with $C(\mu, K) > 0$. In other words, any *finite* choice for K_n gives rise to a positive probability of $\mathbb{H}(n; \mu, K_n)$ being asymptotically not connected.

Our results reveal the striking differences between the homogeneous and the inhomogeneous random K-out graphs. In particular, setting $K_n = 2$ for all $n = 2, \ldots$ is sufficient to ensure that the homogeneous random K-out graph $\mathbb{H}(n; K_n)$ is connected with high probability (see [8, Theorem 3.2]). However, when a positive fraction of the nodes get paired, each, with *only* one node, the network will be *not* connected with a positive probability if each of the remaining nodes is paired with K_n other nodes, when $K_n = K$ for all $n = 2, 3, \ldots$, where K is a positive, finite integer with $K \geq 2$.

Although we show that the connectivity of $\mathbb{H}(n; \mu, K_n)$ requires $\lim_{n\to\infty} K_n = \infty$, our results do not *enforce* any particular relationship between the behavior of K_n and n, other than $\lim_{n\to\infty} K_n = \infty$. For example, setting $K_n = \log\log\ldots\log n$ would be sufficient to ensure that $\lim_{n\to\infty} K_n = \infty$, hence guarantees the connectivity of the resulting network. Remarkably, the graph can be connected with order of magnitude fewer links, in total, compared to most other random graph models such as Erdős-Rényi graphs [9], random key graphs [10], and inhomogeneous random key graphs [11], where the mean degree (respectively, the *minimum* mean degree in the inhomogeneous random key graphs) has to be on the order of $\log n$ to ensure connectivity. In contrast, the mean degree of $\mathbb{H}(n; \mu, K_n)$ is of order $2K_n$, where the only requirement on K_n is to have $\lim_{n\to\infty} K_n = \infty$, e.g., $K_n = \log\log\ldots\log n$.

In comparing with other models, we find it relevant to draw parallels between the *practical* requirements of the heterogeneous random pairwise key predistribution scheme, presented here, and other random key predistribution schemes. We focus on the classical random key predistribution scheme proposed by Eschenauer and Gligor [4] as well as the heterogeneous random key predistribution scheme proposed recently by Yağan [11]. As for Eschenauer and Gligor scheme, Di Pietro et al. [12] showed that for practical consideration, the universal key ring size has to be on the order of $\log n$ (with the key pool size being of order $n \log n$) such that the resulting network is both connected and *resilient* to node capture attacks[1]. As for the heterogeneous random key predistribution scheme, the requirements on the key ring sizes may increase by orders of magnitude depending on the *smallest* key ring size, see [11] for details. Conversely, the heterogeneous random pairwise key predistribution scheme requires much less average key ring size to ensure both connectivity and resiliency[2], i.e., order of $2K_n$ with K_n being any sequence that satisfies $\lim_{n\to\infty} K_n = \infty$. One example of such a sequence is $K_n = \log\log\ldots\log n$. Hence, from a practical standpoint, the heterogeneous random pairwise key distribution requires orders of magnitude less memory requirements to establish both connectivity and resiliency.

Numerical Study

We explore the validity of Theorem 3.1 via computer simulations. We look at the probability that $\mathbb{H}(n;\mu,K_n)$ is connected when $\mu = 0.9$ and as the parameter K_n varies from $K_n = 2$ to $K_n = 20$. We set $n = 3000$ and generate 3000 independent samples of the graph $\mathbb{H}(n;\mu,K_n)$ and count the number of times (out of a possible 3000) that the obtained graph is connected. Dividing this count by 3000, we obtain the (empirical) probability that $\mathbb{H}(n;\mu,K_n)$ is connected. The results, depicted in Figure 1, readily confirm Theorem 3.1 and the bound (5).

In Figure 2, we recall (5) and explore the interplay between μ and K as governed by $C(\mu,K)$. Our objective is to show the effect of increasing μ on the minimum value of K required to achieve a target bound on the probability of connectivity. More precisely, we set $C(\mu,K) = 0.001$ (implying that the probability of connectivity is upper bounded by 0.999), and vary μ from 0.05 to 0.95. For each value of μ, we compute the corresponding value of K, theoretically from (5) and empirically via simulations, that would achieve the target bound, i.e., $C(\mu,K) = 0.001$. Observe that as μ increases, more nodes get classified as class-1, hence a higher value of K is needed to increase the probability of connectivity. We set $n = 3000$ and perform 3000 independent simulations for each data point.

[1]A network is said to be resilient to node capture attacks if the adversary needs to capture a large number of nodes to compromise the confidentiality of the network [12].

[2]Recall that nodes which were paired to one another have a *unique* key in the heterogeneous random pairwise scheme, hence capturing a node only compromises the links corresponding to this node, leading to perfect resiliency.

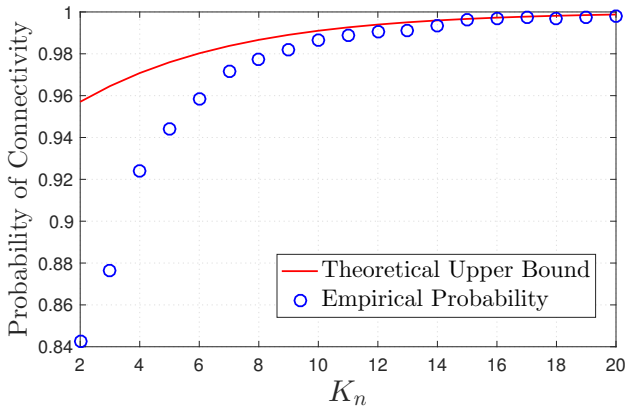

Fig. 1. *The empirical probability $P(n;\mu,K_n)$ vs. K_n for $n = 3000$ and $\mu = 0.9$, along with the theoretical upper bound given by Theorem 3.1. Empirical probabilities approach the upper bound as K_n increases.*

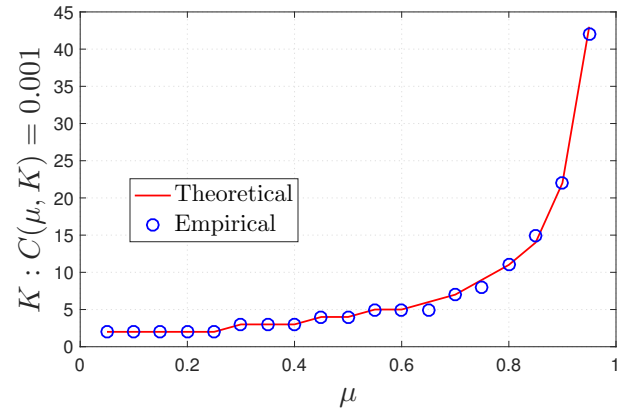

Fig. 2. *The theoretical as well as empirical values of K corresponding to $C(\mu,K) = 0.001$ as μ varies from 0.05 to 0.95. The network size n is set to 3000.*

IV. Preliminaries

Throughout, we will make use of the following results.

Fact 4.1: For $r = 1,\ldots,\lfloor \frac{n}{2} \rfloor$ and $n = 1,2,\ldots$, we have

$$\binom{n}{r} \le \left(\frac{n}{r}\right)^r \left(\frac{n}{n-r}\right)^{n-r} \tag{6}$$

Due to space limitations, we give the proof of Fact 4.1 in [15, Fact 4.1].

For $0 \le K \le x \le y$, we have

$$\frac{\binom{x}{K}}{\binom{y}{K}} = \prod_{\ell=0}^{K-1} \left(\frac{x-\ell}{y-\ell}\right) \le \left(\frac{x}{y}\right)^K \tag{7}$$

since $\frac{x-\ell}{y-\ell}$ decreases as ℓ increases from $\ell = 0$ to $\ell = K-1$.

Moreover, we have

$$1 \pm x \le e^{\pm x}, \quad 0 \le x \le 1 \tag{8}$$

and

$$1 - e^{-x} \ge \frac{x}{2}, \quad 0 \le x \le 1 \tag{9}$$

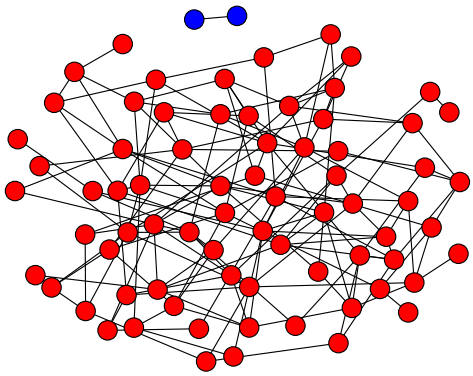

Fig. 3. *A realization of the inhomogeneous random K-out graph $\mathbb{H}(n;\mu,K_n)$ with $K_1=1$ and $K_2=3$. The graph is clearly disconnected as it contains an isolated component of two class-1 nodes, highlighted in blue. We set $n=75$ and $\mu=0.5$.*

Throughout, we set

$$\binom{x}{y}=0, \quad \text{whenever } x<y. \tag{10}$$

V. A PROOF OF THEOREM 3.1

In what follows, we establish that

$$\limsup_{n\to\infty} P(n;\mu,K_n) \le 1-C(\mu,K) \tag{11}$$

whenever $K_n=K$ for all $n=2,3,\ldots$, where K is a positive, finite integer satisfying $K\ge 2$. In particular, with class-1 nodes, each, being paired with only one node, we will show that whenever class-2 nodes, each, gets paired with K_n other nodes for $K_n=K$ for all $n=2,3,\ldots$ and with $K\ge 2$, there will be a positive probability that the graph is *not* connected.

Observe that when a positive fraction of the nodes, each, gets paired with only one node, the graph may contain isolated components consisting of two class-1 nodes, say i and j, that were paired with each other, i.e., $\Gamma_{n,i}(\mu,K_n)=\{j\}$, $\Gamma_{n,j}(\mu,K_n)=\{i\}$, and $\Gamma_{n,\ell}(\mu,K_n)\subseteq\mathcal{N}\setminus\{i,j,\ell\}$ for all $\ell\in\mathcal{N}\setminus\{i,j\}$. Indeed, these isolated components render the graph disconnected. A graphical illustration is given in Figure 3. Our approach in establishing Theorem 3.1 relies on the method of second moment applied to a variable that counts the number of isolated components that contain two vertices of class-1.

Recall that t_i denotes the class of node i. Let $U_{ij}(n;\mu,K_n)$ denote the event that nodes i and j are both class-1 *and* are forming an isolated component, i.e.,

$$\begin{aligned} &U_{ij}(n;\mu,K_n) \\ &=\left(\bigcap_{\ell\in\mathcal{N}\setminus\{i,j\}}[\Gamma_{n,\ell}(\mu,K_n)\subseteq\mathcal{N}\setminus\{i,j,\ell\}]\right) \\ &\quad\cap[\Gamma_{n,i}(\mu,K_n)=\{j\}]\cap[\Gamma_{n,j}(\mu,K_n)=\{i\}] \\ &\quad\cap[t_1=1]\cap[t_2=1] \end{aligned} \tag{12}$$

Next, let

$$\chi_{ij}(n;\mu,K_n)=\mathbf{1}\left[U_{ij}(n;\mu,K_n)\right]$$

and

$$Y(n;\mu,K_n)=\sum_{1\le i<j\le n}\chi_{ij}(n;\mu,K_n)$$

Clearly, $Y(n;\mu,K_n)$ gives the number of isolated components in $\mathbb{H}(n;\mu,K_n)$ that contain two vertices of class-1. We will show that with $K_n=K$ for $n=2,3,\ldots$, for a positive, finite integer K with $K\ge 2$, we have

$$\limsup_{n\to\infty}\mathbb{P}\left[Y(n;\mu,K_n)=0\right]\le 1-C(\mu,K)$$

Recall that if $\mathbb{H}(n;\mu,K_n)$ is connected, then it does not contain any isolated component. However, $\mathbb{H}(n;\mu,K_n)$ may or may not be connected if it does not contain an isolated component consisting of two nodes of class-1. It follows that

$$P(n;\mu,K_n)\le\mathbb{P}\left[Y(n;\mu,K_n)=0\right]$$

Hence, establishing (11) is equivalent to establishing

$$\limsup_{n\to\infty}\mathbb{P}\left[Y(n;\mu,K_n)=0\right]\le 1-C(\mu,K) \tag{13}$$

where $C(\mu,K_n)$ is given by (5).

By applying the method of second moments [14, Remark 3.1, p. 55] on $Y(n;\mu,K_n)$, we get

$$\mathbb{P}[Y(n;\mu,K_n)=0]\le 1-\frac{\left(\mathbb{E}[Y(n;\mu,K_n)]\right)^2}{\mathbb{E}[Y^2(n;\mu,K_n)]} \tag{14}$$

where

$$\begin{aligned}\mathbb{E}[Y(n;\mu,K_n)]&=\sum_{1\le i<j\le n}\mathbb{E}\left[\chi_{ij}(n;\mu,K_n)\right]\\&=\binom{n}{2}\mathbb{E}[\chi_{12}(n;\mu,K_n)]\end{aligned} \tag{15}$$

and

$$\begin{aligned}&\mathbb{E}[Y^2(n;\mu,K_n)]\\&=\mathbb{E}\left[\sum_{1\le i<j\le n}\sum_{1\le\ell<m\le n}\chi_{ij}(n;\mu,K_n)\chi_{\ell m}(n;\mu,K_n)\right]\\&=\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\right]\\&\quad+\binom{n}{2}\binom{2}{1}\binom{n-2}{1}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\chi_{13}(n;\mu,K_n)\right]\\&\quad+\binom{n}{2}\binom{2}{2}\binom{n-2}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\chi_{34}(n;\mu,K_n)\right]\end{aligned}$$

by exchangeability and the binary nature of the random variables $\{\chi_{ij}(n;\mu,K_n)\}_{1\le i<j\le n}$. Observe that

$$\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\chi_{13}(n;\mu,K_n)\right]=0,$$

since $[U_{12}(n;\mu,K_n)\cap U_{13}(n;\mu,K_n)]=\emptyset$ by definition. Hence,

$$\begin{aligned}&\mathbb{E}[Y^2(n;\mu,K_n)]\\&=\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\right]\end{aligned} \tag{16}$$

$$+\binom{n}{2}\binom{n-2}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\chi_{34}(n;\mu,K_n)\right]$$

Using (15) and (16), we get

$$\frac{\mathbb{E}[Y^2(n;\mu,K_n)]}{\left(\mathbb{E}[Y(n;\mu,K_n)]\right)^2}=\frac{1}{\binom{n}{2}\mathbb{E}[\chi_{1,2}(n;\mu,K_n)]} + \frac{\binom{n}{2}\binom{n-2}{2}\mathbb{E}[\chi_{1,2}(n;\mu,K_n)\chi_{3,4}(n;\mu,K_n)]}{\left(\binom{n}{2}\mathbb{E}[\chi_{1,2}(n;\mu,K_n)]\right)^2} \tag{17}$$

The next two results will help establish (13).

Proposition 5.1: Consider a probability distribution $\boldsymbol{\mu}=(\mu,1-\mu)$ with $\mu>0$ such that a vertex is labeled as class-1 with probability μ or class-2 with probability $1-\mu$. Let $K_n=K$ for all $n=2,3,\ldots$, where K is a positive, finite integer with $K\geq 2$, it holds that

$$\lim_{n\to\infty}\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\right]= \frac{\mu^2}{2}\exp\Big(-2-2(1-\mu)(K-1)\Big) \tag{18}$$

Due to space limitations, we give the proof of Proposition 5.1 in [15, Proposition 5.1].

Proposition 5.2: Consider a probability distribution $\boldsymbol{\mu}=(\mu,1-\mu)$ with $\mu>0$ such that a vertex is labeled as class-1 with probability μ or class-2 with probability $1-\mu$. Let $K_n=K$ for all $n=2,3,\ldots$, where K is a positive, finite integer with $K\geq 2$, it holds that

$$\lim_{n\to\infty}\left(\frac{\binom{n}{2}\binom{n-2}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\chi_{34}(n;\mu,K_n)\right]}{\left(\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\mu,K_n)\right]\right)^2}\right)=1 \tag{19}$$

Due to space limitations, we give the proof of Proposition 5.2 in [15, Proposition 5.2].

The main result (11) now follows by virtue of (13) and (14) as we combine (17), (18), and (19).

VI. A PROOF OF THEOREM 3.2

In what follows, we establish that

$$\lim_{n\to\infty}P(n;\mu,K_n)=1 \tag{20}$$

whenever $\lim_{n\to\infty}K_n=\infty$.

Observe that when $\lim_{n\to\infty}K_n=\infty$, the upper bound given in (5) becomes zero, hence Theorem 3.1 gives

$$\lim_{n\to\infty}P(n;\mu,K_n)\leq 1$$

which sheds some light on the possibility that Theorem 3.2 could be established when $\lim_{n\to\infty}K_n=\infty$. However, the given bound is trivial, hence a rigorous proof is needed to show that when $\lim_{n\to\infty}K_n=\infty$, we *precisely* have

$$\lim_{n\to\infty}P(n;\mu,K_n)=1$$

In what follows, we give our proof for Theorem 3.2. Observe that for any non-empty subset S of nodes, i.e., $S\subseteq\mathcal{N}$, we say that S is *isolated* in $\mathbb{H}(n;\mu,K_n)$ if there are no edges in $\mathbb{H}(n;\mu,K_n)$ between the nodes in S and the nodes in the complement $S^c=\mathcal{N}-S$. This is characterized by the event $B_n(\mu,K_n;S)$ given by

$$B_n(\mu,K_n;S)=\bigcap_{i\in S}\bigcap_{j\in S^c}\left([i\notin\Gamma_{n,j}(\mu,K_n)]\cap[j\notin\Gamma_{n,i}(\mu,K_n)]\right).$$

Note that if $\mathbb{H}(n;\mu,K_n)$ is *not* connected, then there must exist a non-empty subset S of nodes which is isolated. Recall that each node in $\mathbb{H}(n;\mu,K_n)$ is either class-1 (hence, gets paired with 1 other node) with probability μ or class-2 (hence, gets paired with K_n other node) with probability $1-\mu$. Thus, we may observe isolated sets in $\mathbb{H}(n;\mu,K_n)$ of cardinality $r=2,3,\ldots,\lfloor\frac{n}{2}\rfloor$[3]. Thus, with $D_n(\mu,K_n)$ denoting the event that $\mathbb{H}(n;\mu,K_n)$ is connected, we have the inclusion

$$D_n(\mu,K_n)^c\subseteq\cup_{S\in\mathcal{P}_n:\ 2\leq|S|\leq\lfloor\frac{n}{2}\rfloor}B_n(\mu,K_n;S) \tag{21}$$

where $\mathcal{P}_n$ stands for the collection of all non-empty subsets of $\mathcal{N}$. A standard union bound argument immediately gives

$$\begin{aligned}\mathbb{P}\left[D_n(\mu,K)^c\right]&\leq\sum_{S\in\mathcal{P}_n:2\leq|S|\leq\lfloor\frac{n}{2}\rfloor}\mathbb{P}\left[B_n(\mu,K_n;S)\right]\\&=\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\left(\sum_{S\in\mathcal{P}_{n,r}}\mathbb{P}\left[B_n(\mu,K_n;S)\right]\right)\end{aligned} \tag{22}$$

where $\mathcal{P}_{n,r}$ denotes the collection of all subsets of $\mathcal{N}$ with exactly r elements.

For each $r=1,\ldots,n$, we simplify the notation by writing $B_{n,r}(\mu,K_n)=B_n(\mu,K_n;\{1,\ldots,r\})$. Under the enforced assumptions, exchangeability implies

$$\mathbb{P}\left[B_n(\mu,K_n;S)\right]=\mathbb{P}\left[B_{n,r}(\mu,K_n)\right],\quad S\in\mathcal{P}_{n,r}$$

and the expression

$$\sum_{S\in\mathcal{P}_{n,r}}\mathbb{P}\left[B_n(\mu,K_n;S)\right]=\binom{n}{r}\mathbb{P}\left[B_{n,r}(\mu,K_n)\right] \tag{23}$$

follows since $|\mathcal{P}_{n,r}|=\binom{n}{r}$. Substituting into (22) we obtain the bounds

$$\mathbb{P}\left[D_n(\mu,K_n)^c\right]\leq\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[B_{n,r}(\mu,K_n)\right]. \tag{24}$$

For each $r=2,\ldots,\lfloor\frac{n}{2}\rfloor$, it is easy to check that

$$\begin{aligned}&\mathbb{P}\left[B_{n,r}(\mu,K_n)\right]\\&=\left(\mu\frac{\binom{r-1}{1}}{\binom{n-1}{1}}+(1-\mu)\frac{\binom{r-1}{K_n}}{\binom{n-1}{K_n}}\right)^r\cdot\\&\quad\cdot\left(\mu\frac{\binom{n-r-1}{1}}{\binom{n-1}{1}}+(1-\mu)\frac{\binom{n-r-1}{K_n}}{\binom{n-1}{K_n}}\right)^{n-r}\end{aligned} \tag{25}$$

To see why this last relation holds, recall that for nodes $\{1,\ldots,r\}$ to be isolated in $\mathbb{H}(n;\mu,K_n)$, we need that (i) none of the sets $\Gamma_{n,1}(\mu,K_n),\ldots,\Gamma_{n,r}(\mu,K_n)$ contains an

[3]Note that if vertices S form an isolated set then so do vertices $\mathcal{N}-S$, hence the sum need to be taken only until $\lfloor\frac{n}{2}\rfloor$.

element from the set $\{r+1,\ldots,n\}$; and (ii) none of the sets $\Gamma_{n,r+1}(\mu,K_n),\ldots,\Gamma_{n,n}(\mu,K_n)$ contains an element from $\{1,\ldots,r\}$. More precisely, we must have

$$\Gamma_{n,i}(\mu,K_n)\subseteq\{1,\ldots,r\}\setminus\{i\},\quad i=1,\ldots,r$$

and

$$\Gamma_{n,j}(\mu,K_n)\subseteq\{r+1,\ldots,n\}\setminus\{j\},\quad j=r+1,\ldots,n.$$

Hence, the validity of (25) is now immediate from (2) and the mutual independence of the rvs $\Gamma_{n,1}(\mu,K_n),\ldots,\Gamma_{n,n}(\mu,K_n)$. Observe that on the range $r=2,\ldots,K_n$, the set $\{1,\ldots,r\}$ can not contain any class-2 nodes, but (25) still holds (as an upper bound) by virtue of (10).

We now show that under the enforced assumptions of Theorem 3.2, we have

$$\lim_{n\to\infty}\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\,\mathbb{P}\left[B_{n,r}(\mu,K_n)\right]=0$$

which in turn establishes Theorem 3.2 by virtue of (24).

We use (7), (8), and (25) to get

$$\begin{aligned}
&\mathbb{P}\left[B_{n,r}(\mu,K_n)\right]\\
&\le\left(\mu\frac{\binom{r-1}{1}}{\binom{n-1}{1}}+(1-\mu)\frac{\binom{r-1}{K_n}}{\binom{n-1}{K_n}}\right)^r\cdot\\
&\quad\cdot\left(\mu\frac{\binom{n-r-1}{1}}{\binom{n-1}{1}}+(1-\mu)\frac{\binom{n-r-1}{K_n}}{\binom{n-1}{K_n}}\right)^{n-r}\\
&\le\left(\mu\left(\frac{r-1}{n-1}\right)+(1-\mu)\left(\frac{r-1}{n-1}\right)^{K_n}\right)^r\cdot\\
&\quad\cdot\left(\mu\left(\frac{n-r-1}{n-1}\right)+(1-\mu)\left(\frac{n-r-1}{n-1}\right)^{K_n}\right)^{n-r}\\
&\le\left(\mu\left(\frac{r}{n}\right)+(1-\mu)\left(\frac{r}{n}\right)^{K_n}\right)^r\cdot\\
&\quad\cdot\left(\mu\left(1-\frac{r}{n}\right)+(1-\mu)\left(1-\frac{r}{n}\right)^{K_n}\right)^{n-r}\\
&=\mu^r\left(\frac{r}{n}\right)^r\left(1+\frac{1-\mu}{\mu}\left(\frac{r}{n}\right)^{K_n-1}\right)^r\left(1-\frac{r}{n}\right)^{n-r}\cdot\\
&\quad\cdot\left(1-(1-\mu)\left(1-\left(1-\frac{r}{n}\right)^{K_n-1}\right)\right)^{n-r}\\
&\le\mu^r\left(\frac{r}{n}\right)^r\left(1-\frac{r}{n}\right)^{n-r}\left(1+\frac{1-\mu}{\mu}\left(\frac{r}{n}\right)^{K_n-1}\right)^r\cdot\\
&\quad\cdot\left(1-(1-\mu)\left(1-e^{-r\left(\frac{K_n-1}{n}\right)}\right)\right)^{n-r}\\
&\le\mu^r\left(\frac{r}{n}\right)^r\left(1-\frac{r}{n}\right)^{n-r}\exp\Bigg(\frac{1-\mu}{\mu}r\left(\frac{r}{n}\right)^{K_n-1}\qquad(26)\\
&\quad-(1-\mu)(n-r)\left(1-e^{-r\left(\frac{K_n-1}{n}\right)}\right)\Bigg)
\end{aligned}$$

Combining (6) with (26), we conclude that

$$\begin{aligned}
\mathbb{P}\left[D_n(\mu,K_n)^c\right]&\le\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[B_{n,r}(\mu,K_n)\right]\\
&\le\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\mu^r A_{n,r}\qquad(27)
\end{aligned}$$

where we define

$$\begin{aligned}
A_{n,r}:=\exp\Bigg(&\frac{1-\mu}{\mu}r\left(\frac{r}{n}\right)^{K_n-1}\qquad(28)\\
&-(1-\mu)(n-r)\left(1-e^{-r\left(\frac{K_n-1}{n}\right)}\right)\Bigg)
\end{aligned}$$

with $2\le r\le n/2$.

Next, our goal is to derive an upper bound on $A_{n,r}$ that is valid for all n sufficiently large and $r=2,\ldots,\lfloor\frac{n}{2}\rfloor$, and show that this bound tends to zero as n gets large. Fix $n=2,3,$ sufficiently large. For each $r=2,\ldots,\lfloor\frac{n}{2}\rfloor$, either one of the following should hold

$$\frac{r(K_n-1)}{n}\le 1\quad\text{and}\quad\frac{r(K_n-1)}{n}>1.$$

If it holds that $\frac{r(K_n-1)}{n}\le 1$, then we use (9) to get $1-e^{-r\left(\frac{K_n-1}{n}\right)}\ge\frac{r(K_n-1)}{2n}$. Using this in (28) yields

$$\begin{aligned}
&A_{n,r}\\
&\le\exp\left(\frac{1-\mu}{\mu}r\left(\frac{r}{n}\right)^{K_n-1}-(1-\mu)(n-r)\frac{r(K_n-1)}{2n}\right)\\
&\le\exp\left(\frac{1-\mu}{\mu}r\left(\frac{1}{2}\right)^{K_n-1}-(1-\mu)\frac{r(K_n-1)}{4}\right)\qquad(29)\\
&=\exp\left(-(1-\mu)r\left(\frac{(K_n-1)}{4}-\frac{(0.5)^{K_n-1}}{\mu}\right)\right)\\
&\le\exp\left(-2(1-\mu)\left(\frac{(K_n-1)}{4}-\frac{(0.5)^{K_n-1}}{\mu}\right)\right)\qquad(30)
\end{aligned}$$

where (29) follows from the facts that $n-r\ge n/2$ and $r/n\le 0.5$ on the specified range for r, and (30) follows for all K_n sufficiently large such that $K_n>\left\lceil 4\left(\frac{(0.5)^{K_n-1}}{\mu}\right)+1\right\rceil$ upon noting that $r\ge 2$.

If, on the other hand, it holds that $\frac{r(K_n-1)}{n}>1$, we see that $1-e^{-r\left(\frac{K_n-1}{n}\right)}\ge 1-e^{-1}$. Reporting this into (28) and using $r\le n/2$, we get

$$\begin{aligned}
&A_{n,r}\\
&\le\exp\left(\frac{1-\mu}{\mu}r\left(\frac{r}{n}\right)^{K_n-1}-(1-\mu)(n-r)\left(1-e^{-1}\right)\right)\\
&\le\exp\left(\frac{1-\mu}{\mu}\frac{n}{2}(0.5)^{K_n-1}-(1-\mu)\frac{n}{2}\left(1-e^{-1}\right)\right)\\
&=\exp\left(-(1-\mu)\frac{n}{2}\left(1-e^{-1}-\frac{(0.5)^{K_n-1}}{\mu}\right)\right).\qquad(31)
\end{aligned}$$

Combining (30) and (31) we see that

$$\begin{aligned}
A_{n,r}\le\max\Bigg\{&\exp\left(-2(1-\mu)\left(\frac{K_n-1}{4}-\frac{(0.5)^{K_n-1}}{\mu}\right)\right),\\
&\exp\left(-(1-\mu)\frac{n}{2}\left(1-e^{-1}-\frac{(0.5)^{K_n-1}}{\mu}\right)\right)\Bigg\}.\qquad(32)
\end{aligned}$$

holds for all n sufficiently large and all $r = 2, \ldots, \lfloor \frac{n}{2} \rfloor$. Letting n go to infinity, it is now easy to see that

$$\lim_{n\to\infty} A_{n,r} = 0, \quad 2 \le r \le n/2$$

under the enforced assumption that $\lim_{n\to\infty} K_n = \infty$. Observing that the bound derived on $A_{n,r}$ is independent on r, we get from (27)

$$\sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[B_{n,r}(\mu, K_n)\right] \le o(1) \sum_{r=2}^{\infty} \mu^r = o(1) \frac{\mu^2}{1-\mu}$$

and the conclusion

$$\lim_{n\to\infty} \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[B_{n,r}(\mu, K_n)\right] = 0$$

immediately follows since $0 < \mu < 1$.

VII. Conclusion

We consider a wireless sensor networks secured by the heterogeneous random pairwise key predistribution scheme, where each node is classified as class-1 with probability μ or class-2 with probability $1-\mu$, for $0 < \mu < 1$, independently. We consider the particular case when class-1 (respectively, class-2) node is paired (offline) with 1 (respectively, K) other nodes selected uniformly at random. Our objective is to characterize the connectivity of the resulting network as a function of K. The scheme induces an inhomogeneous random K-out graph $\mathbb{H}(n; \mu, K_n)$, where n denotes the number of nodes and K_n denotes a scaling of K with respect to the network size n. With $K_1 = 1$, we show that i) when $K_n = K$ for all $n = 2, 3, \ldots$ for a positive, finite integer K with $K \ge 2$, the resulting graph is not connected with a positive probability. In this case, we derive a tight upper bound on the probability of connectivity and verify the results via simulations. Moreover, ii) we prove that when K_n is chosen such that $\lim_{n\to\infty} K_n = \infty$, the graph is connected with high probability as n tends to infinity.

As for future work, we plan to investigate the k-connectivity [16], [17] and k-robustness [18], [19], [20] of the network, owing to their significant importance in designing reliable wireless sensor networks. In particular, our results on the 1-connectivity of the network do not provide any guarantees on whether or not the network will remain connected upon the failure (or perhaps, capture) of some sensor nodes. Establishing k-connectivity result would provide reliability guarantees as to what extent the network could remain connected despite the failure of some nodes. In addition, the property of k-robustness plays a key role in various dynamical processes over networks; such as quantifying how resilient message dissemination is against node misbehavior when only local information is used [18].

Acknowledgment

This work has been supported in part by National Science Foundation through grant CCF #1617934. R. Eletreby was funded (in part) by the Dowd Fellowship from the College of Engineering at Carnegie Mellon University. The authors would like to thank Philip and Marsha Dowd for their financial support and encouragement.

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

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

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 3, Mar 2008.

[13] H. Robbins, "A remark on stirling's formula," *The American mathematical monthly*, vol. 62, no. 1, pp. 26–29, 1955.

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

[15] R. Eletreby and O. Yağan, "Connectivity of wireless sensor networks secured by the heterogeneous random pairwise key predistribution scheme," full version available online at https://www.andrew.cmu.edu/user/reletreb/papers/cdc2018full.pdf.

[16] 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.

[17] 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.

[18] H. Zhang and S. Sundaram, "Robustness of complex networks with implications for consensus and contagion," in *Proc. of IEEE CDC 2012*, 2012, pp. 3426–3432.

[19] J. Zhao, O. Yağan, and V. Gligor, "On the strengths of connectivity and robustness in general random intersection graphs," in *Proc. of IEEE CDC 2014*, pp. 3661–3668.

[20] ——, "On connectivity and robustness in random intersection graphs," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2121–2136, May 2017.