ISIT'2013 1569719519

On Connectivity Thresholds in Superposition of Random Key Graphs on Random Geometric Graphs

B. Santhana Krishnan
Electrical Engg. Department
IIT Bombay, India
Email: skrishna@ee.iitb.ac.in

Ayalvadi Ganesh
Department of Mathematics,
University of Bristol, United Kingdom
Email: aganesh@bristol.ac.uk

D. Manjunath
Electrical Engg. Department
IIT Bombay, India
Email: dmanju@ee.iitb.ac.in

***Abstract*—In a random key graph (RKG) of n nodes each node is randomly assigned a key ring of K_n cryptographic keys from a pool of P_n keys. Two nodes can communicate directly if they have at least one common key in their key rings. We assume that the n nodes are distributed uniformly in $[0,1]^2$. In addition to the common key requirement, we require two nodes to also be within r_n of each other to be able to have a direct edge. Thus we have a random graph in which the RKG is superposed on the familiar random geometric graph (RGG). For such a random graph, we obtain tight bounds on the relation between K_n, P_n and r_n for the graph to be asymptotically almost surely connected.**

I. Introduction

Several constructions for random graphs have been proposed with different, suitably parametrised, rules to determine the existence of an edge between two nodes. The most well known of these are the Erdős-Rényi (ER) random graphs that have independent edges; [1] is an excellent introduction to the study of such graphs. Most other random graphs have edges that are not independent. An important example of the latter kind is the random geometric graph (RGG), motivated by, among other systems, wireless networks. Here the nodes are randomly distributed in a Euclidean space and there is an edge between two nodes if the Euclidean distance between them is below a specified threshold; [2] provides a comprehensive treatment of such graphs. A more recent example of a random graph with non independent edges is the random key graph (RKG) [3]. Here there is a key pool of size P and each node randomly chooses K of these for its key ring uniformly i.i.d. Two nodes have an edge if they have at least one common key in their key rings. Such networks have also been investigated as uniform random intersection graphs; see e.g., [4]. That the edges are not independent in RGGs and RKGs is evident.

Recently, there is interest in random graphs in which an edge is determined by more than one random property, i.e., *intersection* of different random graphs. The intersection of ER random graphs and RGGs has been of interest for quite some time now. A general form of such graphs is as follows. n nodes are distributed uniformly in an area and the probability that two nodes are connected is a function of their distance and is independent of other edges. This has also been called the random connection model. Recent work on such random graphs are in [5] where connectivity properties are analyzed. In [6], the superposition of an ER random graph on an RKG is considered. The construction of such a graph is as follows: an RKG is first formed based on the key-distribution and each edge in this graph is deleted with a specified probability.

This material is based upon work supported by the Bharti Centre for Communication, EE Department, IIT Bombay.

In this paper, our interest is in the intersection of RKGs and RGGs. n nodes are distributed in a finite Euclidean space and an RGG is formed with edges between nodes that are within r_n of each other. The network has a pool of P_n keys and each node independently chooses for itself a key ring of size K_n. Each edge of this RGG is retained if the two nodes have at least one common key in their key rings. A more formal definition of this graph will be provided in the next section.

An important distinction between the random graph that we consider in this paper and the ones in [5], [6] is that both the RKG and the RGG have non independent edges. This complicates the analysis significantly. The rest of the paper is organized as follows. In the next section we formally describe the model and then provide an overview of the literature. In Section III we state the main result and a sketch of the proof. The formal proof is in Section IV. We conclude in Section V.

II. Preliminaries

The n nodes are uniformly distributed in $\mathscr{A} := [0,1]^2$. Let $x_i \in \mathscr{A}$ be the location of node i. A key pool with P_n cryptographic keys is designated for the network of n nodes. Node i chooses a random subset S_i of keys from the key pool with $|S_i| = K_n$. Our interest is in the random graph $G(P_n, K_n, r_n)$ with n nodes and edges formed as follows. An edge (i,j), between $x_i, x_j \in \mathscr{A}$, is present in $G(P_n, K_n, r_n)$ if both of the following two conditions are satisfied.

$E_1 : \ \|x_i - x_j\| \leq r_n$
$E_2 : \ S_i \cap S_j \neq \emptyset$

Condition E_1 produces a random geometric graph with cutoff r_n. Imposing condition E_2 on E_1 retains the edges of the random geometric graph for which the two nodes have a common key. Thus $G(P_n, K_n, r_n)$ is a RKG-RGG.

$G(r_n)$ will refer to a random geometric graph in which an edge (i,j) is determined only by E_1. Similarly, $G(P_n, K_n)$ will refer to the RKG where an edge (i,j) is determined only by E_2. The following is known about the connectivity of these types of random graphs.

Theorem 1. [7, Theorems 2.1, 3.2] In $G(r_n)$, let $\pi r_n^2 = \frac{\log n + c_n}{n}$. Then

$$\liminf_{n\to\infty} \Pr\left(G(r_n) \text{ is disconnected}\right) \geq e^{-c}\left(1-e^{-c}\right)$$
$$\text{if } \lim_{n\to\infty} c_n = c \text{ and } 0 < c < \infty,$$
$$\lim_{n\to\infty} \Pr\left(G(r_n) \text{ is connected}\right) = 1$$
$$\text{if and only if } c_n \to +\infty.$$

This theorem is also available from [8, Theorem 2].

Theorem 2. [3, Theorem 4.1] In $G(P_n, K_n)$, let $K_n \geq 2$ and $\frac{K_n^2}{P_n} = \frac{\log n + c_n}{n}$. Then,

$$\lim_{n\to\infty} \Pr\left(G(P_n, K_n) \text{ is connected}\right) = 0$$
$$\text{if } \lim_{n\to\infty} c_n = -\infty,$$
$$\lim_{n\to\infty} \Pr\left(G(P_n, K_n) \text{ is connected}\right) = 1$$
$$\text{for } \sigma > 0, \text{ if } K_n \to \infty,\ P_n \geq \sigma n \ \&\ \lim_{n\to\infty} c_n = \infty.$$

If $r_n = \sqrt{2}$ we see that $G(P_n, K_n, r_n)$ is a RKG $G(P_n, K_n)$ and Theorem 2 applies. In fact it is easy to argue that if $r_n = r > 0$, then Theorem 2 applies. Further note that if the condition for Theorem 1 is satisfied with $c_n \to \infty$ and $c_n \in o(\log n)$ then the minimum degree in $G(r_n)$ will be a constant. This means that if an RKG is now superposed on this, the graph will be disconnected with a constant probability if the probability that two nodes share a key is less than 1. Thus we will need c_n to be such that the minimum degree in $G(r_n)$ is unbounded; we assume $n\pi r_n^2 = d_n$, where $d_n \in \omega(\log n)$, and $d_n \in o(n)$.

III. Main Result

The main result of this paper is the following theorem that characterizes the probability of connectivity of an RKG-RGG intersection random graph.

Theorem 3. Let $K_n \geq 2$, $K_n, P_n \to \infty$, $K_n^2/P_n \to 0$, $P_n \geq 2K_n$ and $P_n \geq \sigma n r_n^2$ where $\sigma > 0$ is a constant. Then

1) If $\pi r_n^2 \frac{K_n^2}{P_n} = \frac{\log n + c_1}{n}$ with $0 < c_1 < \infty$ then
$$\lim_{n\to\infty} \Pr\left(G(P_n, K_n, r_n) \text{ is disconnected}\right) \geq \frac{e^{-c_1}}{4}.$$
2) If $\pi r_n^2 \frac{K_n^2}{P_n} > \frac{2\pi}{1-\delta}\frac{\log n}{n}$ for any δ, $0 < \delta < 1$, then for some $c_3 > 0$ and some c_2, $0 < c_2 < \infty$,
$$\lim_{n\to\infty} \Pr\left(G(P_n, K_n, r_n) \text{ is connected}\right) \geq 1 - \frac{c_2}{n^{c_3}}.$$
Thus $\Pr\left(G(P_n, K_n, r_n) \text{ is connected}\right) \to 1$.

The first statement of the theorem is proved in the usual way by considering the probability of finding at least one isolated node in the network for a specified (P_n, K_n, r_n). The second part takes a slightly different approach. We divide $\mathscr{A}$ into smaller square cells whose lengths are proportional to r_n. We then consider a set of overlapping tessellations where a cell in one tessellation overlaps with four cells in the other tessellation. Connectivity of $G(P_n, K_n, r_n)$ is ensured as follows: (1) all cells are dense, i.e., all cells have $\Theta(n\ r_n^2)$ nodes inside them, and (2) the nodes in each cell form a connected subgraph. The tessellations are illustrated in Fig. 2. The proof will identify the (P_n, K_n, r_n) that achieves both of these properties.

IV. Proof of Theorem 3

We will repeatedly use the following inequality. For any $0 < x < 1$, and any positive integer n,

$$\exp\left(-\frac{nx}{1-x}\right) < (1-x)^n < \exp(-nx). \quad (1)$$

See [9, Appendix A] for details.

Also, we will be using the following lemma from [3].

Lemma 1. If $\lim_{n\to\infty} \frac{K_n^2}{P_n} = 0$, then

$$\beta_n := 1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}} \sim \frac{K_n^2}{P_n}.$$

β_n is the probability that two nodes share a key.

A. Proof of Statement 1 of Theorem 3

Let Z_i denote the event that node $i, 1 \leq i \leq n$, is isolated, and define $a_n := \pi r_n^2$, $\beta_n := 1 - \left(\binom{P_n - K_n}{K_n}/\binom{P_n}{K_n}\right)$. Observe that β_n is the probability that two nodes have at least one common key. From Bonferroni inequalities and symmetry,

$$\Pr\left(\bigcup_{i=1}^{n} Z_i\right) \geq \sum_{i=1}^{n} \Pr(Z_i) - \sum_{1\leq i<j\leq n} \Pr(Z_i \cap Z_j).$$
$$= n\Pr(Z_1) - \binom{n}{2}\Pr(Z_1 \cap Z_2) \quad (2)$$

Clearly,
$$\Pr(Z_1) = (1 - a_n\beta_n)^{n-1}.$$

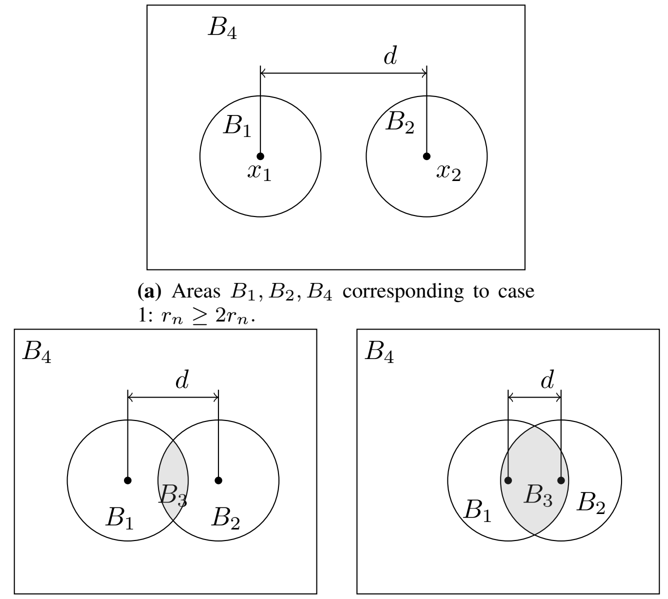
Let $a_n\beta_n = (\log n + c_1)/n$, with $0 < c_1 < \infty$. Using (1), we can show that

$$n\Pr(Z_1) \geq \exp(-c_1)\ \exp\left(-\frac{(\log n + c_1)^2}{n - (\log n + c_1)}\right). \quad (3)$$

The details are in [9, Appendix B].

Consider two circles of radius r_n centered at x_1 and x_2. Let B_3 be the intersection of the two circles, B_1 (resp. B_2) be the part of the circle at x_1 (resp. x_2) excluding B_3 and $B_4 := \mathscr{A} \setminus (B_1 \cup B_2)$. Let $d := \|x_1 - x_2\|$. The areas of the regions B_i depend on d and we will use B_i to also to refer to the areas. Further, let n_i be the number of nodes in B_i for $1 \leq i \leq 4$. Ignoring the edge effects, when $(n-2)$ nodes are distributed uniformly in $\mathscr{A}$ the n_i form a multinomial distribution with probabilities equal to B_i. We consider the following three cases as shown in Fig. 1a, 1b and 1c.

1) $d > 2r_n$: This case happens with probability $1 - 4a_n$. Here $B_3 = 0$ and hence $n_3 = 0$. $Z_1 \cap Z_2$ is true if each of the n_1 nodes in B_1 do not share a key with Node 1,



(a) Areas B_1, B_2, B_4 corresponding to case 1: $r_n \geq 2r_n$.

(b) Areas B_1, B_2, B_3, B_4 corresponding to case 2: $d < r_n \leq 2r_n$.

(c) Areas B_1, B_2, B_3, B_4 corresponding to case 3: $d \leq r_n$

Fig. 1: Areas to be considered for Nodes-1 and 2 to be jointly isolated.

and each of the n_2 nodes in B_2 do not share a key with Node 2. Hence

$$\mathsf{Pr}\left(Z_1 \cap Z_2 | d > 2r_n\right) = \left(1 - 2\ a_n\beta_n\right)^{n-2} \quad (4)$$

2) $r_n \leq d \leq 2r_n$: This case happens with probability $3a_n$. In this case, for $Z_1 \cap Z_2$ to be true the n_1 nodes in B_1 and n_2 nodes in B_2 should be as in the previous case. In addition we will need that the n_3 nodes in B_3 not share a key with either Node 1 or Node 2.

$$\mathsf{Pr}\left(Z_1 \cap Z_2 | r_n \leq d \leq 2r_n\right) \leq \exp\left(-(n-2)\left(2 - \left\|\frac{\tilde{\beta}_n}{\beta_n} - 2\right\|\right) a_n\beta_n\right) \quad (5)$$

where $\tilde{\beta}_n := 1 - \left(\binom{P_n - 2K_n}{K_n} / \binom{P_n}{K_n}\right)$. See [9, Appendix C] for details.

3) $d < r_n$: This case happens with probability a_n. For $Z_1 \cap Z_2$ to be true, the conditions of the previous case should be satisfied. In addition Nodes 1 and 2 should also not share a key. Identical to the second term in (5), we have

$$\mathsf{Pr}\left(Z_1 \cap Z_2 | 0 \leq d \leq r_n\right) \leq \exp\left(-(n-2)\left(2 - \left\|\frac{\tilde{\beta}_n}{\beta_n} - 2\right\|\right) a_n\beta_n\right) \quad (6)$$

See [9, Appendix D] for details.

From (4), (5) and (6) the unconditional joint probability of two nodes being isolated is bounded as:

$$\mathsf{Pr}\left(Z_1 \cap Z_2\right) \leq \left(1 - 4a_n\right)\left(1 - 2\ a_n\beta_n\right)^{n-2} + 4a_n \frac{\exp\left(\log n \left[\gamma - \frac{c_1(2-\gamma)}{\log n} + \frac{(4-2\gamma)a_n\beta_n}{\log n}\right]\right)}{n^2}.$$

where $\gamma := \left\|\frac{\tilde{\beta}_n}{\beta_n} - 2\right\|$.

An upper bound on $\binom{n}{2}\mathsf{Pr}\left(Z_1 \cap Z_2\right)$ is obtained for some $\epsilon > 0$ by using $a_n = d_n/n$ and $a_n\beta_n = \frac{\log n + c_1}{n}$ in the preceding inequality.

$$\binom{n}{2}\mathsf{Pr}\left(Z_1 \cap Z_2\right) \leq \exp\left(-c_1\right) \frac{\exp\left(-c_1 + \frac{4(\log n + c_1)}{n}\right)}{2} + \frac{2}{n^{\epsilon}}. \quad (7)$$

See [9, Appendix F and Appendix E] for details. Using (3) and (7) in (2), the lower bound on $\mathsf{Pr}\left(\cup_{i=1}^{n} Z_i\right)$ is

$$\begin{aligned} \mathsf{Pr}\left(\cup_{i=1}^{n} Z_i\right) \geq\ & \exp\left(-c_1\right)\left(\exp\left(-\frac{(\log n + c_1)^2}{n - (\log n + c_1)}\right)\right. \\ & \left. - \frac{\exp\left(-c_1 + \frac{4(\log n + c_1)}{n}\right)}{2} - \frac{\exp\left(2c_1\right)}{n^{\epsilon}}\right) \\ \geq\ & \frac{\exp\left(-c_1\right)}{4}. \end{aligned} \quad (8)$$

Combining (8) with Lemma 1, we have the necessary condition of Theorem 3. □

Remark 1. If $a_n\beta_n = \left(\log n + c_n\right)/n$ for any $c_n \to \infty$, then using the union bound, we see that asymptotically almost surely, there are no isolated nodes in the graph $G\left(P_n, K_n, r_n\right)$.

B. *Proof of Statement 2 of Theorem 3*

We consider two overlapping tessellations on $\mathscr{A}$ as shown in Fig. 2, call them tessellations 1 and 2. In both tessellations, $\mathscr{A}$ is divided into square cells of size $s_n \times s_n$ where $1/s_n$ is an integer and $r_n = \sqrt{2}s_n$. This means that two nodes in the same cell are within communicating range of each other. Note the overlapping structure in the cells of the two tessellations.

For the proof we show the following.

1) In each of the tessellations, every cell is dense. Specifically, every cell has $\Theta(ns_n^2)$ nodes w.h.p (with high probability).
2) W.h.p the subgraph of $G(P_n, K_n, r_n)$ induced by the nodes in a cell forms a single connected component. Further w.h.p, the subgraphs of every cell in a tessellation have this property.
3) Use the preceding results and the overlapping structure of the two tessellations to argue that the graph is connected w.h.p.

First, we analyse deneseness of each cell. Recall that $na_n = d_n$, where $d_n \in \omega(\log n)$ and $d_n \in o(n)$. Let N_i denote the number of nodes in cell i, $1 \leq i \leq 1/s_n^2$. Clearly N_i is a binomial random variable with parameters (n, s_n^2). Let W_i indicate the event that cell i is not dense, i.e. for any fixed $0 < \delta < 1$, $|N_i - ns_n^2| \geq \delta ns_n^2$. Using Chernoff bounds on N_i, we have $\mathsf{Pr}\left(W_i = 1\right) \leq 2\ \exp\left(-ns_n^2\delta^2/4\right)$. The union bound is used to show that that every cell is dense w.h.p, see [9, Appendix G] for details.

$$\mathsf{Pr}\left(\bigcup_{i=1}^{1/s_n^2} W_i\right) \leq \frac{1}{s_n^2}\mathsf{Pr}\left(W_i\right) \leq \exp\left(-\frac{\theta\delta^2 d_n}{8\pi}\right) \to 0. \quad (9)$$

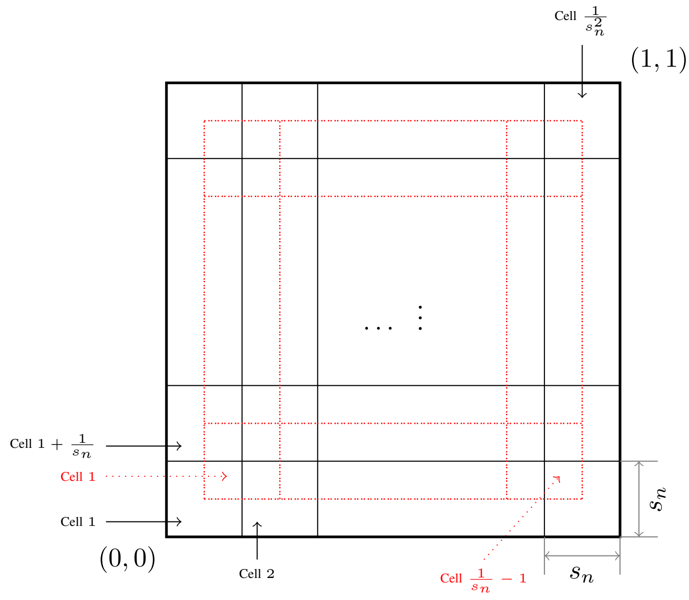


Fig. 2: Tessellation of $[0,1]^2$ (with cell numbers given inside the cells). Tessellation 1(2) is shown using continuous(dotted) line divisions.

Now consider the sub-graph formed by nodes in Cell i; denote this subgraph by G_i. We show that $\Pr\left(\{\cap_{i=1}^{1/s_n^2}\{G_i \text{ is connected}\}\right) \to 1$. This in turn is achieved by showing that for every i there are no components of size $1, 2, \ldots, N_i/2$ in G_i. To simplify the notation, in the following we will drop the reference to the parameters r_n, K_n, and P_n.

For Cell i, define the following events.

$$
\begin{aligned}
S &\subseteq \{1,2,\ldots,N_i\} \text{ is a subset of nodes in Cell } i \\
&\quad \text{with } |S| \geq 1. \\
C_i(S) &:= \text{Event that subgraph induced by nodes in } S \\
&\quad \text{forms a connected component.} \\
B_i(S) &:= S \text{ and } S^c \text{ have no edges between} \\
&\quad \text{them, where } S \cup S^c = \{1,2,\ldots,N_i\} \\
A_i(S) &:= B_i(S) \cap C_i(S). \\
D_i &= \bigcup_{l=1}^{\lceil N_i/2 \rceil} \bigcup_{S:|S|=l} A_i(S).
\end{aligned}
$$

Further, let $C_{i,l}$ and $A_{i,l}$ denote, respectively, $C_i(S)$ and $A_i(S)$ with $|S| = l$. Then the sufficient condition for G_i to be connected w.h.p is to have $\Pr(D_i) \to 0$. Conditioning on W_i, we have

$$
\begin{aligned}
\Pr(D_i) &= \sum_{j\in\{0,1\}} \Pr(D_i|W_i = j) \Pr(W_i = j) \\
&\leq \Pr(D_i|W_i = 0) + \Pr(W_i = 1).
\end{aligned}
$$

The preceding inequality is obtained by using $\Pr(W_i = 0) \leq 1$ and $\Pr(D_i|W_i = 1) \leq 1$.

Let $U_{i,l}$ be the random variable that denotes the number of distinct keys in the component of size l in G_i. Adapting [3, (56) from Lemma 10.2] for each cell, for any $x \in \{K_n, K_n+1, \ldots \min(lK_n, P_n)\}$, we have (10).

$$
\begin{aligned}
\Pr(A_{i,l}) \leq\ & \Pr(U_{i,l} \leq x) \exp\left(-(\lfloor N_i \rfloor - l)\frac{K_n^2}{P_n}\right) \\
&+ \Pr(C_l) \exp\left(-(\lfloor N_i \rfloor - l)\frac{K_n(x+1)}{P_n}\right). \quad (10)
\end{aligned}
$$

From [3, Lemma 10.1 and (69)], we know that

$$
\begin{aligned}
\Pr(U_{i,l} \leq x) &\leq \binom{P_n}{x}\left(\frac{x}{P_n}\right)^{lK_n} \\
\Pr(C_{i,l}) &\leq l^{l-2}\beta_n^{l-1}.
\end{aligned}
$$

Now consider all the cells in a tessellation.

$$
\Pr\left(\cup_{i=1}^{\left(\frac{1}{s_n}-1\right)^2} D_i\right) \leq \frac{\Pr(D_i|W_i = 0)}{s_n^2} + \frac{\Pr(W_i = 1)}{s_n^2}.
$$

From (9), $(1/s_n^2)\ \Pr(W_i = 1) \to 0$. Thus we focus on showing that $(1/s_n^2)\Pr(D_i|W_i = 0) \to 0$. This implies that all $G_i(P_n, K_n, r_n)$ are connected w.h.p.

By using symmetry and union bound, we have

$$
\begin{aligned}
\frac{\Pr(D_i|W_i = 0)}{s_n^2} &= \left(\frac{1}{s_n^2}\right) \Pr\left(\bigcup_{l=1}^{\lceil N_i/2 \rceil} \bigcup_{S:|S|=l} A_{N_i,l}\right) \\
&\leq \left(\frac{1}{s_n^2}\right) \sum_{l=1}^{\lceil N_i/2 \rceil} \binom{N_i}{l} \Pr(A_{N_i,l}). \quad (11)
\end{aligned}
$$

For the remainder of this section, assume that $n\pi r_n^2\beta_n =: \alpha \log n$. The probability of having isolated nodes in any of the cells is upper bounded as shown below (details are in [9, Appendix H]).

$$
\begin{aligned}
&\Pr(\exists \geq 1 \text{ isolated node in any of the cells}) \\
&\leq \exp\left(-\log n\left(\frac{\left(\frac{\alpha(1-\delta)}{2\pi} - 1\right)}{2}\right)\right) \to 0. \quad (12)
\end{aligned}
$$

Further, the following conditions on the constants are necessary. $0 < \delta < 1$ and $0 < \mu < 0.44$. λ, R are chosen such that $\lambda R > \alpha(1-\delta)/(2\pi)$. We also need $K_n > 2\log 2/\mu$. Further $\sigma, \lambda, \delta, K_n$ must satisfy

$$
\begin{aligned}
\sigma &\geq \frac{(1+\delta)\log 2}{\log\left(\frac{e^{\mu}}{\mu^{1+\mu}}\right)} \\
1 &> \max\left\{\frac{e^{2+\frac{K_n^2}{P_n}}(1+\delta)}{2^{K_n-2}\sigma}, e^{K_n/P_n}\left(\frac{e^2(1+\delta)}{\sigma}\right)^{\lambda}\lambda^{(1-2\lambda)}\right\}.
\end{aligned}
$$

Using (10) in (11), we next prove that all cells in tessellation 1 do not have components of size $2, 3, \ldots N_i/2$. Together with (12), we have $\Pr\left(\{\cap_{i=1}^{1/s_n^2}\{\ G_i \text{ is connected}\}\right) \to 1$.

Following [3, (61)] or [1], the sum term in (11) is evaluated in three parts based on the size of the isolated component l.

1) $2 \leq l \leq R$: In this case, the number of keys shared by the set of nodes which form the isolated component is

small and can be upper bounded by $(1+\epsilon)K_n$, where $0<\epsilon<1$. R is a small integer, See [9, Appendix I] for details.

$$\left(\frac{1}{s_n^2}\right)\sum_{i=2}^{R}\binom{N_i}{l}\mathsf{Pr}\left(A_{N_i,l}\right)\leq\frac{(R-1)c_4}{n^{0.5\left(\frac{(1-\delta)\alpha}{\pi}-1\right)}} \tag{13}$$

where c_4 is an appropriately chosen positive constant.

2) $R+1 \leq l \leq L_1(n)$: Here $L_1(n) = \min\left(\lfloor N_i/2\rfloor, \lfloor P_n/K_n\rfloor - 1\right)$. In this case, the number of keys shared by the set of nodes which form the isolated component is linear in the number of nodes l and is upper bounded by $\lambda l K_n$, where $0<\lambda<1/2$. See [9, Appendix J] for details.

$$\left(\frac{1}{s_n^2}\right)\sum_{i=R+1}^{L_1(n)}\binom{N_i}{l}\mathsf{Pr}\left(A_{N_i,l}\right)\leq \frac{c_5}{n^{0.5(\alpha(1-\delta)/2\pi)}}+\frac{c_6}{n^{c_7}}. \tag{14}$$

3) $L_1(n)+1 \leq l \leq N_i/2$: In this case, the isolated component is large, and comparable to the size of the subgraph G_i in cell i. Thus the number of keys shared by the nodes which form the isolated component is upper bounded by μP_n, where $0<\mu<0.44$. See [9, Appendix K] for details of the following result.

$$\left(\frac{1}{s_n^2}\right)\sum_{i=L_1(n)+1}^{N_i/2}\binom{N_i}{l}\mathsf{Pr}\left(A_{N_i,l}\right) \leq \exp\left(-c_8\ d_n\right)+\exp\left(-c_9\ d_n\right). \tag{15}$$

Where $c_8>0$, $c_9>((1-\delta)/4\pi)\left(\frac{\mu K_n}{2}-\log 2\right)$.

Remark 2. If tighter upper bounds on $\binom{P_n}{\mu P_n}$ than $(e/\mu)^{\mu P_n}$ are used, then the bound in (15) can be improved in terms of larger range of of μ; i.e. for instance if $\binom{P_n}{\mu P_n}\leq 0.85\left(e/\mu\right)^{\mu P_n}$, then $0<\mu\leq 0.5$ is valid.

Combining (13), (14) and (15), we have

$$\left(\frac{1}{s_n^2}\right)\sum_{i=2}^{N_i/2}\binom{N_i}{l}\mathsf{Pr}\left(A_{N_i,l}\right) \leq \frac{c_4(R+1)}{n^{0.5\left(\frac{(1-\delta)\alpha}{\pi}-1\right)}} +\frac{c_5}{n^{0.5\left(\frac{\alpha(1-\delta)}{2\pi}-1\right)}}+\frac{c_6}{n^{c_7}}+\exp\left(-c_8\ d_n\right)+\exp\left(-c_9\ d_n\right).$$

Further using appropriate positive constants c_2, c_3 and Lemma 1, we have the sufficient condition. Thus from (12), (13), (14) and (15), we have shown that $\mathsf{Pr}\left(T_1\right)\to 1$, where $T_i, i=1$ or 2, represents the event that all cells in tessellation i are connected.

$\mathsf{Pr}\left(T_1\cap T_2\right)\to 1$ implies that the entire graph is connected. We know that $\mathsf{Pr}\left(T_1\right)\to 1$, and $\mathsf{Pr}\left(T_2\right)\to 1$. Thus

$$\mathsf{Pr}\left(T_1\cap T_2\right)=\mathsf{Pr}\left(T_1\right)+\mathsf{Pr}\left(T_2\right)-\mathsf{Pr}\left(T_1\cup T_2\right),$$

$\mathsf{Pr}\left(T_1\cup T_2\right)\leq 1$, and $\mathsf{Pr}\left(T_1\cap T_2\right)\to 1$ which completes the proof. □

V. Discussion and Conclusion

Imposing the random key graph constraint on random geometric graphs was discussed in [6] where it was conjectured that the connectivity threshold will be of the form $n\pi r_n^2\beta_n=\log n+c_n$ for any $c_n\to\infty$. We have obtained this up to a multiplicative constant, as opposed to the additive constant conjectured in [6]. Further, it may also be possible to be less restrictive about $n\pi r_n^2$ and β_n. As we mentioned earlier, the minimum degree should be increasing in n, but we believe that can also be made tighter.

References

[1] B. Bollobas, *Random Graphs*. Cambridge University Press, 2001.

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

[3] O. Yagan 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, May 2012.

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

[5] G. Mao and B. D. O. Anderson, "Towards a better understanding of large scale network models," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 408–421, 2012.

[6] O. Yagan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON-OFF channel," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 3821–3835, Jun. 2012.

[7] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*. Birkhauser, Boston, 1998, pp. 547–566.

[8] M. D. Penrose, "The longest edge of the random minimal spanning tree," *The Annals of Applied Probability*, vol. 7, no. 2, pp. 340–361, 1997.

[9] B. Santhana Krishnan, A. Ganesh, and D. Manjunath, "On connectivity thresholds in the intersection of random key graphs on random geometric graphs," *http://arxiv.org/abs/1301.6422v1*, 2013.