Geometric Graphs with Randomly Deleted Edges - Connectivity and Routing Protocols

K. Krzywdziński[1] and K. Rybarczyk[1]

Adam Mickiewicz University, Poznań, Poland

Abstract. In the article we study important properties of random geometric graphs with randomly deleted edges which are natural models of wireless ad hoc networks with communication constraints. We concentrate on two problems which are most important in the context of theoretical studies on wireless ad hoc networks. The first is how to set parameters of the network (graph) to have it connected. The second is the problem of an effective message transmition i.e. the problem of construction of routing protocols in wireless networks. We provide a thorough mathematical analysis of connectivity property and a greedy routing protocol. The models we use are: an intersection of a random geometric graph with an Erdős–Rényi random graph and an intersection of a random geometric graph with a uniform random intersection graph. The obtained results are asymptotically tight up to a constant factor.

1 Introduction

1.1 Background

A random geometric graph is a widely used model of wireless ad hoc networks. A wireless ad hoc network is a collection of devices randomly deployed over a given area and equipped with radio transmitters. This type of networks have proved to have many applications in environment and industrial monitoring, security, cell phone networks etc. It is generally assumed that in wireless ad hoc networks direct communication between two nodes is possible if they are mutually in their transmission range, thus the usage of random geometric graphs seems natural. In random geometric graphs vertices are located in the Euclidean plane according to a given probability distribution and two vertices v and w are connected by an edge if their Euclidean distance is not greater than some constant r (for a monograph on random geometric graphs see [21]). The vertices of the model represent devices and edges arise if appropriate devices are in mutual transmission range. A random geometric graph, though concise enough to promote strong theoretical results, frequently does not apply directly to networks in realistic settings. In fact, wireless links in real networks may be extremely unreliable. Moreover, the connections are sometimes constrained by security requirements. In reality the message transmission between devices may be obstructed and the direct communication is possible only if additional conditions are also fulfilled. Therefore it is justified to introduce new graph models which are considerably closer to reality than a random geometric graph. In the context of theoretical studies on wireless networks two questions concerning new models seem to be of main importance: how to set parameters of the network to have it connected and whether routing protocols are effective in the network. Both of them are related to the message transmission problem in wireless ad hoc networks, which is the main subject of this article.

1.2 Related work

The most important results on connectivity of random geometric graphs were obtained by Gupta and Kumar in [14] and Penrose (see [21] and references therein). In [14] Gupta and Kumar considered a random graph in which n vertices are uniformly distributed in a disk of a unit area and two vertices are connected by an edge if they are at distance at most $r(n)$. It was shown that if $\pi r^2(n) = (\ln n + c(n))/n$ and $c(n) \to \infty$ then the probability that an instance of the considered random graph model is connected tends to 1 as n tends to infinity. In concluding remarks Gupta and Kumar proposed a generalised random geometric graph, which models wireless ad hoc network with independent link constraints. In the model two vertices at distance at most $r(n)$ are connected with probability $p(n)$. Gupta and Kumar conjectured that if

$$\pi p(n) r^2(n) = \frac{\ln n + c(n)}{n} \tag{1}$$

and $c(n) \to \infty$ then a random geometric graph with independently deleted edges is connected with probability tending to one as $n \to \infty$. Properties of the model were later studied for example in [9] and [26]. In [26] Yi et al. showed a Poisson approximation of the number of isolated nodes in a random geometric graph with independently deleted edges for r and p as in (1) and $c(n) \to c$. The result implies that as $c(n) \to -\infty$ a random geometric graph with independently deleted edges is disconnected with probability tending to one as $n \to \infty$. To the best of our knowledge no sufficient conditions for connectivity are known. The model proposed by Gupta and Kumar is also related to the so–called "bluetooth model" (see [22] and references therein). However the results proved in this article are much stronger than those which would follow from the results concerning "bluetooth model" and the models comparison.

Sometimes link constraints in a wireless network are not independent and another model should be used. This is the case of wireless sensor networks with random key predistribution. The widely recognised solution to the problem of security of the message transmission in those networks is so–called random key predistribution introduced in [12]. So far, the studies on wireless sensor networks with random key predistribution reveal either experimental results (see for example [6, 12, 15]) or concentrate only on the security aspects, neglecting a limited transmission range (i.e. properties of uniform random intersection graphs are studied, see for example [1, 2, 8, 23]). As it is pointed out in [8] the model with both security and transmission limitations is an intersection of a random geometric graph and a uniform random intersection graph. Its variant has only recently been analysed in rigorous mathematical manner in [17]. However in [17] an additional assumption on deployment knowledge is made and the techniques used cannot be applied to the model studied in this article.

The connectivity of a wireless network implies possibility of the message transmition from any device to any other device. However it yields another question: how this message should be send? This is a folklore result that the simplest method of the message transmission in wireless ad hoc network is forwarding a routed message to the neighbour closest (in the sense of Euclidian distance, angle or other) to the destination. Such greedy forwarding, basing on the topology of the network graph, is called geographic routing. In geographic routing two main assumptions are made. The first one, that each network device possesses information about its own and about its neighbours positions. The second, that the source of a message is provided with the position of the destination. As any device knows only about its immediate neighbours, there is often insufficient information for it to make a good decision on the forwarding direction and a packet may get trapped. Already numerous attempts to enhance the greedy algorithm in general setting have been proposed (see for example [5, 19, 20]). Routing in the network with unreliable links has been also studied (see for example [27]). The mathematical analysis of the greedy routing protocol in random geometric graph was the subject of [25]. However, to the best of our knowledge none of the results considered analytical analysis of the greedy routing protocol in wireless networks with unreliable links.

1.3 Our contribution

In the article we analyse in detail theoretical models of wireless networks with independent link constraints and wireless sensor networks with random key predistribution. We maintain the assumption that in the graph model a link between vertices is possible if they are at distance at most r, at the same time making an additional one, that the link may be obstructed with a certain probability. We analyse in detail asymptotic properties of two models. First of the considered models is a random geometric graph with independently disappearing edges, proposed in [14]. In the second model the edge deletion depends on the structure of a uniform random intersection graph. More precisely, we analyse the models which are an intersection of a random geometric graph with an Erdős–Rényi random graph (see [14]) and an intersection of a random geometric graph with a uniform random intersection graph (see [8]).

For the first time we present a thorough mathematical analysis of a greedy routing protocol in wireless networks with link constraints. Moreover we provide a solution to the conjecture posed in [14] concerning connectivity of the random geometric graph model with independently deleted edges (an intersection of a random geometric graph with Erdős–Rényi random graph). In Theorem 4 an answer is given and the obtained result is tight up to a constant factor. In addition in Theorem 3 we state sufficient conditions for connectivity of the model of wireless sensor network with random key predistribution (an intersection of a random geometric graph with a uniform random intersection graph). This is the first analytical result which takes into account both security and transmission range constraints in this type of networks. Moreover we show how to set parameters of the network with communication constraints in such way that the greedy routing protocol effectively delivers the message to the destination. We also set an upper bound on the length of transmission path in the presented greedy routing protocol.

1.4 The article organisation

The article is organised as follows. In Section 2 we introduce the models and provide a version of the greedy protocol which is considered in the article. Section 3 discusses the routing protocol in networks modelled by a graph with independent communication constraints, whereas Section 4 shows a sketch of analogous results for the model of wireless sensor network with random key predistribution.

2 Preliminaries

2.1 Definitions of the models

In further considerations we make an assumption that $\mathbb{D}$ is a disk of a unit area. However it should be pointed out that the results apply also to a wider class of areas after rescaling and repeating the proofs. We assume that $V = V_n$ is a set of n points independently, uniformly distributed on $\mathbb{D}$, $0 < r = r(n) < 1/\sqrt{\pi}$, $p = p(n) \in [0; 1]$ are real numbers and $d = d(n)$ is a positive integer. The assumption $r(n) \leq 1/\sqrt{\pi}$ is a natural one, since otherwise radius of $\mathbb{D}$ would be smaller than transmission range in the modelled network. Moreover, for any two points $v, v' \in \mathbb{D}$, by $\|v, v'\|$ we denote their Euclidian distance.

Let $G_r(n)$ be a random geometric graph, i.e. a graph with the vertex set $V = V_n$ and the edge set $E(G_r(n)) = \{vv' : v, v' \in V \text{ and } \|v, v'\| \leq r\}$.

We denote by $G_r(n, p)$ an instance of the graph model suggested by Gupta and Kumar in [14]. A random graph $G_r(n, p)$ is obtained form $G_r(n)$ by independently deleting each edge with probability $1 - p$ (i.e. each edge stays in a graph independently with probability p). Notice that in $G_r(n, p)$ the edge set is an intersection of the edge sets of $G_r(n)$ and an Erdős–Rényi random graph $G(n, p)$, in which each edge appears independently with probability p (see [3, 16]).

The second considered model represents a wireless sensor network with random key predistribution. As noticed in [8] (see also [17]) it is an intersection of $G_r(n)$ and a uniform random intersection graph $\mathcal{G}(n, m, d)$. In a uniform random intersection graph $\mathcal{G}(n, m, d)$ each vertex $v \in V$ chooses a subset from an auxiliary arbitrarily given feature set $W = W_n$ of cardinality $m = m(n)$. More precisely, given $d = d(n)$, each vertex $v \in V$ is attributed a subset of features $S(v)$ chosen uniformly at random from all $d(n)$–element subsets of W. A uniform random intersection graph is a graph with the vertex set $V = V_n$ and the edge set $E(\mathcal{G}(n,m,d)) = \{vv' : v, v' \in V \text{ and } S(v) \cap S(v') \neq \emptyset\}$. In fact $\mathcal{G}(n,m,d)$ is a variant of a widely studied random intersection graph. The model of a random intersection graph was studied for the first time in [18, 24] and its generalised version was introduced in [13]. By $\mathcal{G}_r(n,m,d)$ we denote a graph with the vertex set V_n and an edge set $E(G_r(n)) \cap E(\mathcal{G}(n,m,d))$, where $G_r(n)$ and $\mathcal{G}(n,m,d)$ are independent (i.e. their edge sets are constructed independently).

2.2 Greedy routing protocol

Notice that in $G_r(n)$ a set of n' vertices that are mutually at distance at most r form a clique. In contrast those vertices in $G_r(n,p)$ and $\mathcal{G}_r(n,m,d)$ behave like $G(n',p)$ and $\mathcal{G}(n',m,d)$, respectively. Therefore, in $G_r(n,p)$ and $\mathcal{G}_r(n,m,d)$, in a close neighbourhood of the destination the network does not have any features of a random geometric graph and the geographic routing would fail. We propose a new routing protocol, which is a combination of a modified geographic compass routing and the standard Breadth First Search procedure (BFS). Recall that in geographic routing we assume that: each network device possesses information about its own and about its neighbours positions and the source of a message is provided with the position of the destination.

The algorithm parameter $0 < \varepsilon < 1/2$ is chosen prior to algorithm start and remains constant throughout the execution. Let G be a graph representing the network and r be a transmission range. Denote by s the source, by t the destination and by $G[t]$ a subgraph of G induced on the vertices at distance at most r from t (in the transmission range of t). The algorithm CompassPlus is as follows:

First s has a token, which contains a message.
1. Denote by v a vertex in possession of the token.
2. (Compass Routing Mode) If $\|v,t\| > r$, then send the token to a neighbour w of v at distance at least εr, such that the measure of the angle $\angle tvw$ is minimised.
3. (BFS Routing Mode) If $\|v,t\| \leq r$, then use BFS on $G[t]$ to route the message (i.e. use a path established by the Breath First Search procedure).

3 Geographic routing in $G_r(n,p)$

In further considerations by the length of a path we mean the number of its edges in the graph. Moreover by $D(v)$ we denote a disk of radius r and centre in a point $v \in \mathbb{D}$. In this section we prove the following theorem.

Theorem 1. *Let $C > 8$, $p = p(n) \in [0;1]$ and $r = r(n) \in (0; 1/\sqrt{\pi}]$. If*

$$\pi r^2 p \geq C \frac{\ln n}{n}, \tag{2}$$

then $G_r(n,p)$ is connected with probability tending to 1 as $n \to \infty$.
Moreover if $0 < \varepsilon < \min\{\sqrt{1 - 8/C}, 1/2\}$, then with probability tending to 1 as

$n \to \infty$ CompassPlus delivers information in $G_r(n,p)$ in at most $2\|s,t\|/(\varepsilon r(n)) + \ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6) + 4$ steps between any two vertices s,t in some set of size $n(1-o(1))$.

It follows by the result from [26] that if $\pi r^2 p \le C\frac{\ln n}{n}$ and $C < 1$ then with probability $1-o(1)$ $G_r(n,p)$ is disconnected. Therefore r and p fulfilling equation

$$\pi r^2 p = C\frac{\ln n}{n}. \tag{3}$$

establish a threshold function for the connectivity and efficient delivery property in $G_r(n,p)$ and the obtained result is tight up to a constant factor. Since augmenting value of p or r may only make a graph more connected in further considerations we concentrate on the case given by (3) for $C > 8$.

The proof of Theorem 1 proceeds as follows. In Lemma 1 we prove that with probability close to one during Compass Routing Mode of CompassPlus a message is delivered from s to some vertex contained in $D(t)$. Moreover we give an upper bound on the length of the path that a message have to pass from s to a vertex in $D(t)$. In Lemma 2 we show that with probability $1-o(1)$ the message may be sent from any vertex from $D(t)$ to t using BFS Routing Mode of CompassPlus and we give an upper bound on the length of the path. In Lemmas 3 and 4 we finish the proof of the first part of Theorem 1. Lemma 5 implies the second part of Theorem 1.

Lemma 1. *Let $0 < \varepsilon \le 1/2$ and (3) with $C > 8$ be fulfilled. Then with probability at least $1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right)$ for any $s \in V(G_r(n,p))$ and any point $t \in \mathbb{D}$ CompassPlus in Compass Routing Mode constructs in $G_r(n,p)$ a path of length at most $2\|s,t\|/(\varepsilon r(n))$ between s and some vertex contained in $D(t)$.*

Proof. Denote by $\mathcal{A}$ the event: "For all $v,t \in V(G_r(n,p))$ there exists w such that, w is a neighbour of v at distance at least εr from v, $\angle tvw$ is minimised and

$$\|w,t\| < \|v,t\| - (\varepsilon r)/2." \tag{4}$$

Notice that

$$\mathbb{P}(\mathcal{A}) = 1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right) \tag{5}$$

implies the thesis. Namely $\mathcal{A}$ implies that for all $s,t \in V(G_r(n,p))$ all steps of Compas Routing Mode of CompassPlus are possible and in each step a distance between t and a vertex in possession of the message is shortened by $(\varepsilon r)/2$. Let $s = v_0, v_1, \ldots, v_l \in D(t)$ be a path constructed by Compas Routing Mode. If for all $1 \le i \le l$ we have $\|v_i,t\| < \|v_{i-1},t\| - (\varepsilon r)/2$, thus inductively $\|v_l,t\| < \|v_0,t\| - l(\varepsilon r)/2 = \|s,t\| - l(\varepsilon r)/2$. Therefore $l \le 2\|s,t\|/(\varepsilon r(n))$ and the constructed path is of length at most $2\|s,t\|/(\varepsilon r(n))$.

Therefore it remains to prove (5). Notice that $D(v)$ may be divided by 4 lines coming through v (4 diameters of $D(v)$ pairwise creating angles 45^o, 90^o and 135^o) into 8 equal parts. All parts are 1/8 of the disk $D(v)$ and all of them may be enumerated by $1,\ldots,8$. Given the division, if k–th part is contained in

$\mathbb{D}$ we denote by $D_{k,\varepsilon}(v)$ a subset of its points, which are at distance at least εr from v (see Figure 1). We also have to take into consideration border conditions. Therefore if k–th part of the division is not contained entirely in $\mathbb{D}$, we rotate it around v until it is contained in $\mathbb{D}$ and then denote by $D_{k,\varepsilon}(v)$ its subset of points, which are at distance at least εr from v (see $D_{5,\varepsilon}(v')$ on Figure 1). Notice that either $t \in D(v)$ or the segment (v,t) intersects at least one of the sets $D_{k,\varepsilon}(v)$, $k = 1,\ldots,8$. Therefore either $t \in D(v)$ (equivalently $v \in D(t)$) or the next vertex in possession of the token should lie on some sector $D_{k,\varepsilon}(v)$. For example on Figure 1, three vertices in $D(v')$ do not belong to any sector $D_{k,\varepsilon}(v)$, but they cannot be intermediate vertices in Compass Routing Mode. However they may be t. Moreover, if $t \notin D(v)$, (v,t) intersects $D_{k,\varepsilon}(v)$ and $w \in D_{k,\varepsilon}(v)$ then w is at distance at least εr from v and $\angle tvw$ is at most 45^o (see Figure 2).

Now we bound the probability that for all $v \in V$ and all $1 \le k \le 8$ there exists a neighbour of v in $D_{k,\varepsilon}(v)$. Let $N_{k,\varepsilon}(v)$ be the set of neighbours of v in $G_r(n,p)$ contained in $D_{k,\varepsilon}(v)$. Then for any constant $0 \le \varepsilon < 1/2$

$$\begin{aligned}\mathbb{P}\left(\exists_v \exists_k N_{k,\varepsilon}(v) = \emptyset\right) &\le \sum_{v\in V}\sum_{1\le k\le 8} \mathbb{P}\left(N_{k,\varepsilon}(v) = \emptyset\right)\\ &\le 8n\left(1 - \tfrac{(1-\varepsilon^2)\pi r^2 p}{8}\right)^{n-1}\\ &\le (1+o(1))8\exp\left(-n\tfrac{(1-\varepsilon^2)C\ln n}{8n} + \ln n\right)\\ &= O\left(n^{-\frac{C(1-\varepsilon^2)-8}{8}}\right).\end{aligned}$$

Therefore with probability $1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right)$ for all $v \in V$ and all $1 \le k \le 8$ a set $D_{k,\varepsilon}(v)$ contains a neighbour of v, i.e.

$$\mathbb{P}\left(\forall_v \forall_k N_{k,\varepsilon}(v) \ne \emptyset\right) = 1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right).$$

Now we shall prove that event $\forall_v \forall_k N_{k,\varepsilon}(v) \ne \emptyset$ implies event $\mathcal{A}$. If event $\forall_v \forall_k N_{k,\varepsilon}(v) \ne \emptyset$ occurs then for all $v,t \in V$ such that $\|v,t\| \ge r$ a step in Compas Routing Mode of CompassPlus is always possible. Now it remains to show that under $\forall_v \forall_k N_{k,\varepsilon}(v) \ne \emptyset$, if in a step w receives the message form v then (4) is true. Consider an instance of $G_r(n,p)$ such that for all $v \in V$ and all $1 \le k \le 8$ there exists a neighbour of v in $D_{k,\varepsilon}(v)$ (i.e. for any v and any k a set $N_{k,\varepsilon}(v)$ is nonempty). Let k be such that the segment (v,t) intersects $D_{k,\varepsilon}(v)$. By above assumptions there exists w – a neighbour of v, in $D_{k,\varepsilon}(v)$. Let t' be a point at distance εr from v and such that $\angle tvt' = 45^o$ (see Figure 2). It is easy to see that

$$\text{either } D_{k,\varepsilon}(v) \subseteq D(t) \text{ (i.e. } w \in D(t)) \quad \text{ or } \|w,t\| \le \|t',t\|.$$

Therefore for any v and w, if $\|v,t\| \ge r$ and $0 < \varepsilon < 1/2$, then (see Figure 2)

$$\begin{aligned}\|w,t\|^2 \le \|t',t\|^2 &\le \left(\|v,t\| - \tfrac{\sqrt{2}\varepsilon r}{2}\right)^2 + \tfrac{1}{2}(\varepsilon r)^2\\ &= \left(\|v,t\| - \tfrac{\varepsilon r}{2}\right)^2 - \varepsilon r\left((\sqrt{2}-1)\|v,t\| - \tfrac{3}{4}\varepsilon r\right) < \left(\|v,t\| - \tfrac{\varepsilon r}{2}\right)^2.\end{aligned}$$

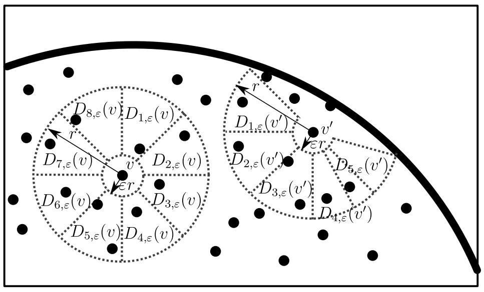

Fig. 1. Division into $D_{k,\varepsilon}(v)$.

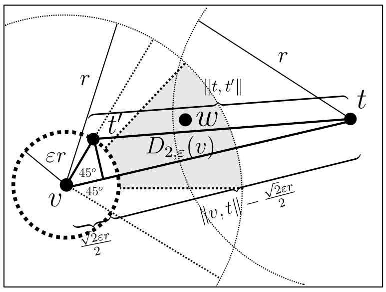

Fig. 2. One step of CompassPlus

Thus if $\|v,t\| \geq r$ and $\varepsilon < 1/2$, then

$$\|w,t\| < \|v,t\| - (\varepsilon r)/2.$$

Thus $\forall_v \forall_k N_{k,\varepsilon}(v) \neq \emptyset$ implies $\mathcal{A}$ and we have

$$\mathbb{P}(\mathcal{A}) \geq \mathbb{P}(\forall_v \forall_k N_{k,\varepsilon}(v) \neq \emptyset) = 1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right).$$

□

A simple corollary of the above lemma is the result stated below. It is only a little less tight than this from [25] but may be shown by much simpler methods. Moreover here the parameter $o(1)$ from [25] is replaced by $O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right)$ (constant may be calculated effectively after careful insight into the proof of Lemma 1) and the length of the path is estimated.

Theorem 2. *Let $0 < \varepsilon \leq 1/2$ and $\pi r^2 = C \ln n/n$, where $C > 8$. Then with probability at least $1 - O\left(n^{-(C(1-\varepsilon^2)-8)/8}\right)$ for any $s, t \in V(G_r(n))$* CompassPlus *constructs in $G_r(n)$ a path of length at most $2\|s,t\|/(\varepsilon r(n)) + 1$ between s and t.*

Proof. Follows immediately by Lemma 1 and fact that $G_r(n)$ is $G_r(n, 1)$. □

Now we concentrate on the BFS Routing Mode. In fact we prove that with probability close to one $G[t]$ is connected and have small diameter (as a graph) for almost all $t \in V(G_r(n,p))$. This proves that in BFS Routing Mode of CompassPlus the message is delivered in short time.

For any graph G and any vertices $v, v' \in V(G)$, by $dist(v, v')$ we denote their distance in G (i.e the length of the shortest path between v and v' in G).

Lemma 2. *Let $C > 8$ and (3) be fulfilled, $v \in V(G_r(n,p))$ and $G[v]$ be a subgraph of $G_r(n,p)$ induced on vertices contained in $D(v)$. Then with probability $1 - o(1)$ (where $o(1)$ is uniformly bounded over all $v \in V(G_r(n,p))$) $G[v]$ is connected and for all $v' \in V(G[v])$ we have*

$$dist(v', v) \leq \ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6) + 4.$$

Proof. For any $v \in V(G_r(n,p))$ the figure $\mathbb{D} \cap D(v)$ may be divided into 6 (or less) connected, not necessarily disjoint parts of diameter (in the sense of Euclidian norm) at most r and area $\pi r^2/6$, such that each of them contains v. For example if $D(v) \subseteq \mathbb{D}$, then $D(v)$ may be divided into 6 equal parts by 3 lines containing v pairwise making angle 60^o. Denote by $G_i(v)$, $1 \le i \le 6$, a subgraph of $G_r(n,p)$ induced on the vertices contained in the i-th part of the division.

For any $v \in V(G_r(n,p))$ and $1 \le i \le 6$ denote by $N = N(i,v) = |V(G_i(v)) \setminus \{v\}|$ a random variable counting the vertices of $G_i(v)$ except v. Surely N is binomialy distributed $\mathrm{Bin}(n-1,P)$, where $P = \pi r^2/6$. Therefore

$$\mathbb{E}N = (n-1)P = (1+o(1))nr^2\pi/6 \to \infty, \tag{6}$$

$$\mathrm{Var}N = P(1-P)(n-1) \le \mathbb{E}N. \tag{7}$$

Let $J = \left[\, (\pi r^2(n-1))(1-(nr^2)^{-1/3})/6\,;\,(\pi r^2(n-1))(1+(nr^2)^{-1/3})/6 \,\right]$. By Chebyshev's inequality

$$\mathbb{P}(N \notin J) = \mathbb{P}\left(|N - \mathbb{E}N| > \mathbb{E}N(nr^2)^{-1/3}\right) \le \frac{VarN}{(\mathbb{E}N)^2(nr^2)^{-2/3}} = o(1).$$

For all $\bar{n} \in J$ we have $\bar{n} = (1+o(1))\pi nr^2/6$ and by (3)

$$p = \frac{C}{6}\frac{\ln n}{\frac{\pi r^2 n}{6}} \ge \frac{4}{3}\frac{\ln\frac{\pi r^2 n}{6}}{\frac{\pi r^2 n}{6}} = (1+o(1))\frac{4}{3}\frac{\ln(\bar{n}+1)}{\bar{n}+1}.$$

Denote by $\mathcal{A}_G$ an event that $\mathrm{diam}G \le \ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6) + 4$ and G is connected. Notice that all the vertices in $G_i(v)$ are pairwise in transmission range. Therefore, since $4/3 > 1$, by classical results on the connectivity and the diameter of an Erdős–Rényi random graph (see [3, 4, 7, 10, 11]) for $G_i = G_i(v)$ we have $\mathbb{P}\left(\mathcal{A}_{G_i} \;\middle|\; N = \bar{n}\right) = 1 - o(1)$, where $o(1)$ is uniformly bounded over all values $\bar{n} \in J$. Denote by $\mathcal{A}^C_{G_i}$ a complement of the event $\mathcal{A}_{G_i}$, then

$$\mathbb{P}\left(\mathcal{A}^C_{G_i}\right) \le \sum_{\bar{n}\in J}\mathbb{P}\left(\mathcal{A}^C_{G_i} \;\middle|\; N = \bar{n}\right)\mathbb{P}(N = \bar{n}) + \mathbb{P}(N \notin J) = o(1),$$

thus $\mathbb{P}\left(\exists_{1\le i\le 6}\mathcal{A}^C_{G_i(v)}\right) \le \sum_{i=1}^{6}\mathbb{P}\left(\mathcal{A}^C_{G_i(v)}\right) = o(1)$. Therefore with probability $1 - o(1)$ all graphs $G_i(v)$, $1 \le i \le 6$, are connected. Each vertex from $D(v)$ is contained in at least one of the graphs $G_i(v)$, therefore the lemma follows. □

Lemma 3. *Let $C > 8$, (3) be fulfilled, $t \in \mathbb{D}$ be any point and $G[t]$ be a subgraph of $G_r(n,p)$ induced on the vertices contained in $D(t)$. Then $G[t]$ is connected with probability $1 - o(1)$.*

Proof. The proof is analogous to the proof of the above lemma. We only have to replace v by t and omit the assumption that v is a vertex of $G_i(v)$. Moreover we have to add $G_7(t)$ – a graph induced on the vertices contained in the circle with centre in t and area equal $\pi r^2/6$. Then we can prove that with probability $1 - o(1)$ all graphs $G_i(v)$, $1 \le i \le 7$, are connected. This implies that $G[t]$ is connected (it is a union of $G_i(v)$). □

Lemma 4. *Let $C > 8$ and* (3) *be fulfilled. Then $G_r(n,p)$ is connected with probability tending to* 1 *as $n \to \infty$.*

Proof. Let t be the centre of $\mathbb{D}$. By Lemma 3 $G[t]$ is connected with probability $1 - o(1)$. If we set $0 < \varepsilon < \min(\sqrt{1 - 8/C}, 1/2)$, then by Lemma 1 with probability $1 - o(1)$ every vertex from $V(G_r(n,p))$ is connected by a path with at least one vertex from $V(G[t])$. Therefore any two vertices from $V(G_r(n,p))$ are connected by a path with probability tending to 1 as $n \to \infty$. $\square$

Lemma 5. *Let $C > 8$, $0 < \varepsilon < \min(\sqrt{1 - 8/C}, 1/2)$ and* (3) *be fulfilled. Then with probability tending to* 1 *as $n \to \infty$* CompassPlus *delivers information in $G_r(n,p)$ in at most $2\|s,t\|/(\varepsilon r(n)) + \ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6) + 4$ steps between any two vertices s, t in some set of size $n(1 + o(1))$.*

Proof. Let $t \in V(G_r(n,p))$. Denote $G[t]$ as in Lemma 2 and by $\mathcal{A}_t$ event that for all $v' \in V(G[t])$ we have $dist(v', t) \leq \ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6) + 4$ and $G[t]$ is connected. Let $\delta(n) = \max_{t \in V(G_r(n,p))} \mathbb{P}(\mathcal{A}_t^c)$, where $\mathcal{A}_t^c$ is a complement of $\mathcal{A}_t$ By Lemma 2

$$\delta(n) = o(1) \tag{8}$$

Let $X = \sum_{t \in V(G_r(n,p))} X_t$, where X_t is an indicator random variable of the event $\mathcal{A}_t^c$. Then $\mathbb{E}X = \sum_t \mathbb{E}X_t \leq \delta(n)n$ and by Markov's inequality

$$\mathbb{P}\left(X \geq \sqrt{\delta(n)}n\right) \leq \frac{\mathbb{E}X}{\sqrt{\delta(n)}n} = \sqrt{\delta(n)} = o(1) \tag{9}$$

Therefore the number of destination vertices such that the routing may fail at the BFS Routing Mode with probability $1 - o(1)$ is at most $\sqrt{\delta(n)}n = o(n)$. This combined with Lemma 1 finishes the proof. $\square$

4 Geographic routing in $\mathcal{G}_r(n, m, d)$

Analogous results to those presented in the previous section may be obtained for $\mathcal{G}_r(n, m, d)$.

Theorem 3. *Let $d \geq 2$ and $m = m(n) \to \infty$ be such that*

$$\frac{\pi r^2 d^2}{m} \geq C \frac{\ln n}{n} \text{ and } C > 8. \tag{10}$$

Then with probability tending to 1 *as $n \to \infty$ a graph $\mathcal{G}_r(n,m,d)$ is connected. Moreover if $0 < \varepsilon < \min(\sqrt{1 - 8/C}, 1/2)$ with probability $1 - o(1)$* CompassPlus *delivers information in at most $2\|s,t\|/(\varepsilon r(n)) + (1 + o(1))\ln(\pi r^2 n/6)/\ln\ln(\pi r^2 n/6)$ steps between any two vertices $s, t \in V(\mathcal{G}_r(n,m,d))$ in some set of size $n(1 - o(1))$.*

Proof (Sketch of the proof). In order to obtain the above result we have to repeat the reasoning from the previous section with two minor modifications.

In the proof of Lemma 1 we have only to make changes in calculation from the first equation. We should notice that, for values of d as in (10), a vertex v' lying in $D(v)$ is not connected by an edge with v with probability $\binom{m-d}{d}/\binom{m}{d} = 1-(1+o(1))d^2/m$ independently of all other vertices. Therefore $\mathbb{P}\left(N_{k,\varepsilon}(v) = \emptyset\right) \leq \exp\left(-(1+o(1))(1-\varepsilon^2)\pi r^2 d^2/m\right)$.

Moreover in the proofs of Lemmas 2 and 3 instead of results on connectivity and the diameter stated in [3, 4, 7, 10, 11] we should use results from [23]. In order to prove only the connectivity result for the case $m = n^\alpha$ (α – a constant) we may also use the result from [1]. $\square$

5 Concluding remarks

We have shown how to set the parameters of a wireless ad hoc network with independent communication constraints and wireless sensor network with random key predistribution in such a way that they are connected and messages' transmission in greedy manner functions well with probability close to 1. For that purpose we have used the models which are random geometric graphs with randomly deleted edges and gave asymptotic results on their properties. We have also mentioned the necessary condition for disconnectivity of the network, which shows that the obtained result is tight up to a constant factor. Moreover we have set an upper bound on the length of transmission paths in the presented greedy routing protocol.

Acknowledgements. We thank an anonymous referee for the remark on the "bluetooth model". This work is partially supported by the Ministry of Science and Higher Education grant NN206 017 32/2452 and partially supported by the Ministry of Science and Higher Education grant NN206565740.

References

1. S. R. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16):5130–5140, 2009.
2. M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Networks*, 53(1):19–26, 2009.
3. B. Bollobás. *Random Graphs.* Academic Press, 1985.
4. B. Bollobás. The diameter of random graphs. *IEEE Trans. Inform. Theory*, 36:285–288, 1990.
5. P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia. Routing with guaranteed delivery in ad hoc wireless network. *Wireless Networks*, 7(6):609–616, 2001.
6. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 197–213, Washington, DC, USA, 2003. IEEE Computer Society.
7. F. Chung and L. Lu. The diameter of sparse random graphs. *Adv. in Appl. Math.*, 26(4):257–279, 2001.
8. R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Sensor networks that are provably resilient. In *Proc 2nd IEEE Int Conf Security Privacy Emerging Areas Commun Networks (SecureComm 2006), Baltimore, MD, 2006*, 2006.

9. J. Diaz, J.Petit, and M. Serna. Faulty random geometric networks. *Parallel Processing Letters*, 10(4):343–357, 2000.
10. P. Erdős and A. Rényi. On random graphs I. *Publ. Math. Debrecen*, 6:290–297, 1959.
11. P. Erdős and A. Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hungar. Acad. Sci.*, 5:17–61, 1960.
12. L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, New York, NY, USA, 2002. ACM Press.
13. E. Godehardt and J. Jaworski. Two models of random intersection graphs for classifcation. In *Studies in Classifcation, Data Analysis and Knowledge Organization*, pages 67–81. Springer, 2003.
14. P. Gupta and P. R. Kumar. *Critical Power for Asymptotic Connectivity in Wireless Networks*, chapter Critical Power for Asymptotic Connectivity in Wireless Networks, pages 547–566. Birkhauser, 1998.
15. J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 43–52. ACM, 2004.
16. S. Janson, T. Łuczak, and A. Ruciński. *Random Graphs*. Wiley, 2001.
17. J. Jaworski, M. Ren, and K. Rybarczyk. Random key predistribution for wireless sensor networks using deployment knowledge. *Computing*, 85(1–2):57–76, 2009.
18. M. Karoński, E. R. Scheinerman, and K.B. Singer-Cohen. On random intersection graphs: The subgraph problem. *Combinatorics, Probability and Computing*, 8:131–159, 1999.
19. B. Karp and H. T. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, 2000.
20. F. Kuhn, R. Wattenhofer, and A. Zollinger. Worst-case optimal and average-case efficient geometric ad-hoc routing. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 267 – 278, 2003.
21. M. Penrose. *Random Geometric Graphs*. Oxford University Press, 2003.
22. A. Pettarin, A. Pietracaprina, and G. Pucci. On the expansion and diameter of bluetooth-like topologies. In A Fiat and P. Sanders, editors, *Algorithms - ESA 2009, 17th Annual European Symposium, Copenhagen, Denmark, September 7-9, 2009. Proceedings. LNCS 5757*, pages 528–539. Springer, 2009.
23. K. Rybarczyk. Diameter, connectivity, and phase transition of the uniform random intersection graph. *Discrete Mathematics.* (2011),doi:10.1016/j.disc.2011.05.029.
24. K. B. Singer-Cohen. Random intersection graphs. PhD Thesis, Department of Mathematical Sciences, The Johns Hopkins University, 1995.
25. P-J Wan, C-W Yi, F. Yao, and X. Jia. Asymptotic critical transmission radius for greedy forward routing in wireless ad hoc networks. In *MobiHoc*, pages 25–36, 2006.
26. C-W Yi, P-J Wan, K-W Lin, and C-H Huang. Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with unreliable nodes and links. *Discrete Mathematics, Algorithms, and Applications*, 2(1):107–124, 2010.
27. M. Z. Zamalloa, K. Seada, B. Krishnamachari, and A. Helmy. Efficient geographic routing over lossy links in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3):1–33, 2008.