Percolation in the Secrecy Graph

Amites Sarkar∗ Martin Haenggi†

July 8, 2011

Abstract
Secrecy graphs model the connectivity of wireless networks under secrecy constraints. Directed edges in the graph are present whenever a node can talk to another node securely in the presence of eavesdroppers. In the case of infinite networks, a critical parameter is the maximum density of eavesdroppers that can be accommodated while still guaranteeing an infinite component in the network, i.e., the percolation threshold. We focus on the case where the location of the nodes and the eavesdroppers are given by Poisson point processes. We present bounds for different types of percolation, including in-, out- and undirected percolation.

1 Introduction
To assess the impact of secrecy constraints in wireless networks, we have recently introduced a random geometric graph, the so-called secrecy graph, that represents the network or communication graph including only links over which secure communication is possible [8].

We assume that a transmitter can choose the rate such that it can communicate to any receiver that is closer than any of the eavesdroppers. This way, the secrecy constraint translates into a simple geometric constraint for secrecy. Natural topics for investigation include the degree distributions and the threshold at which infinite components cease to exist. Since the resulting graph is directed, there are different types of components, including in-, out-, and undirected components. In each case, the percolation threshold (in terms of the density of eavesdroppers) is different.

In this paper, we give an overview of the progress made in the last three years on the percolation thresholds for secrecy graphs, introduce new methods, and present improved bounds for the case where nodes and eavesdroppers form independent Poisson point processes.

∗Department of Mathematics, Western Washington University, Bellingham, WA 98225, USA. Email: amites.sarkar@wwu.edu
†Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA. Email: mhaenggi@nd.edu
2 Model

Our model is as follows. Let \( \mathcal{P} \) and \( \mathcal{P}' \) be independent Poisson processes, of intensities 1 and \( \lambda \) respectively, in \( \mathbb{R}^d \). The case \( d = 2 \) provides a good example. We will call the points of \( \mathcal{P} \) black points and the points of \( \mathcal{P}' \) red points. Now define a directed graph, the directed secrecy graph \( \vec{G}_{\text{sec}} \), on vertex set \( \mathcal{P} \), by sending a directed edge from \( x \in \mathcal{P} \) to \( y \in \mathcal{P} \) if there is no point of \( \mathcal{P}' \) in the open ball \( D(x, \| x - y \|) \) centered at \( x \) with radius \( \| x - y \| \). Note that it makes no difference whether we consider open or closed balls since, with probability 1, there are no two points of \( \mathcal{P} \cup \mathcal{P}' \) at the same distance from any point of \( \mathcal{P} \).

The motivation for this construction is that \( x \in \mathcal{P} \) can send a message to \( y \in \mathcal{P} \) without being overheard by an eavesdropper from \( \mathcal{P}' \). For more details, see [8], where the model was originally defined.

Our main aim in this paper is to study the critical value(s) of \( \lambda \) for various types of percolation in \( \vec{G}_{\text{sec}} \) in the plane (precise definitions will be given later). We will also make some comments about the situation in higher dimensions.

Let us remark that the indegree and outdegree distributions in \( \vec{G}_{\text{sec}} \) have been obtained in [16] and [8] respectively. We summarize the results below.

**Theorem 1.** The outdegree distribution in \( \vec{G}_{\text{sec}} \) is geometric with mean \( 1/\lambda \), and the indegree \( I \) has moment generating function

\[
\mathbb{E}(e^{tI}) = \mathbb{E}(e^{V_d(e^{t-1})/\lambda}),
\]

where \( V_d \) is the random variable representing the volume of a randomly chosen cell in a Voronoi tessellation associated with a unit intensity Poisson process in \( \mathbb{R}^d \). Equivalently, if \( f_d(t) \) is the probability density function of \( V_d \), then

\[
\mathbb{P}(I = k) = \frac{1}{k!} \int_0^\infty f_d(t)e^{-t/\lambda} (t/\lambda)^k dt.
\]

**Proof.** Fix a vertex \( x \in \mathcal{P} \). Label the points of \( \mathcal{P} \cup \mathcal{P}' \setminus \{x\} = \{y_1, y_2, \ldots \} \) in order of increasing distance from \( x \). Now \( x \) has outdegree \( k \) if and only if the \( k \) nearest points \( y_1, \ldots, y_k \) to \( x \) belong to \( \mathcal{P} \) and \( y_{k+1} \in \mathcal{P}' \). The probability of this is \( \left( \frac{1}{1+\lambda} \right)^k \frac{\lambda}{1+\lambda} \). Consequently, the outdegree distribution is geometric with mean \( 1/\lambda \).

For the indegree distribution, we again fix \( x \in \mathcal{P} \), and temporarily rescale the model so that \( \mathcal{P} \) and \( \mathcal{P}' \) have intensities \( 1/\lambda \) and 1 respectively. This does not affect either degree distribution. The vertex \( x \) has indegree \( k \) if and only if there are exactly \( k \) points of \( \mathcal{P} \) in the Voronoi cell \( C \) defined by \( \mathcal{P}' \cup \{x\} \) containing \( x \). If \( C \) has volume \( V \), then

\[
\mathbb{P}(C \cap \mathcal{P} = k) = \frac{1}{k!} e^{-V/\lambda} (V/\lambda)^k.
\]

The result follows.

Unfortunately, \( f_d(t) \) is only known when \( d = 1 \), when \( f_1(t) = 4te^{-2t} \). Consequently, the indegree distribution in \( \vec{G}_{\text{sec}} \) remains unknown for \( d \geq 2 \). However, its mean is of course \( 1/\lambda \) in all dimensions.
3 Percolation

For a model of an infinite undirected random graph, percolation is said to occur if an infinite component occurs with positive probability. (In fact, this probability is almost always 1 by Kolmogorov’s 0-1 law – see Theorem 2.) Since $\vec{G}_{\text{sec}}$ is a directed graph, there are several things we could mean by “component”, which lead to several definitions of percolation. Following [2], we distinguish five distinct events. First, write $G_{\text{sec}}$ for the undirected graph obtained from $\vec{G}_{\text{sec}}$ by removing the orientations of the edges and replacing any resulting double edges by single edges, and $G'_{\text{sec}}$ for the undirected graph obtained from $\vec{G}_{\text{sec}}$ by including only those edges $xy$ for which both $\vec{xy} \in \vec{G}_{\text{sec}}$ and $\vec{yx} \in \vec{G}_{\text{sec}}$. We write $U$ for the event that $G_{\text{sec}}$ has an infinite component, $O$ for the event that $\vec{G}_{\text{sec}}$ has an infinite out-component, $I$ for the event that $\vec{G}_{\text{sec}}$ has an infinite in-component, $S$ for the event that $G_{\text{sec}}$ has an infinite strongly connected subgraph, and $B$ for the event that $G'_{\text{sec}}$ has an infinite component. Here, an out (resp. in)-component is a subgraph with a spanning subtree whose edges are all directed away from (resp. towards) a root vertex, and a strongly connected subgraph is one where there are directed paths from $x$ to $y$ for all $x$ and $y$ in the subgraph. As noted in [2], we have the following implications:

$$B \Rightarrow S \Rightarrow (I \text{ and } O), \quad (I \text{ or } O) \Rightarrow U. \quad (1)$$

Let $X$ denote any of $U, O, I, S$ or $B$, and let $p_X(\lambda, d) = P(X)$.

**Theorem 2.** For all values of $\lambda$ and $d$, and all choices of $X$, $p_X(\lambda, d)$ is either 0 or 1.

**Proof.** Let $E$ be the event that $\vec{G}_{\text{sec}}$ has an infinite $X$-component. By Kolmogorov’s 0-1 law, it is enough to show that $E$ is a tail event, meaning that, for all $K > 0$, $E$ depends only on vertices at distance greater than $K$ from the origin $O$. Fix $K > 0$. Then, for any $\varepsilon > 0$, there is a $K_\varepsilon > K$ such that the probability that there exists a vertex at distance at least $K_\varepsilon$ from $O$ that is not prohibited by $P'$ from sending a directed edge to some vertex within $K$ of the origin is less than $\varepsilon$. This is because one can calculate the expected number of black vertices $v$ at distance at least $L$ from $O$ whose nearest red point is at distance more than $\|v\| - K$ as

$$\int_L^\infty e^{-\lambda \alpha_d(r-K)^d} S_d r^{d-1} dr$$

where $S_d = 2\pi^{d/2}/\Gamma(d/2)$ and $\alpha_d = \pi^{d/2}/\Gamma(1+d/2)$ are the surface area and volume respectively of a unit $d$ dimensional ball. The integrand above is a polynomial times a (super-) exponentially decreasing function, so the integral converges. Hence the integral can be made less than $\varepsilon$ by suitable choice of $L$. Note that this probability is taken over the restriction of $P \cup P'$ to $\mathbb{R}^d \setminus D(O, K)$.

Now, for each choice of $X$, $X$-percolation is unaffected by the removal of a finite number of vertices. Also, with probability 1, there are only finitely many
vertices within distance $K_ε$ of the origin. Consequently, up to probability zero events, $E$ is also the event that there is an infinite component in $G_1$, the directed graph obtained from $G_{sec}$ by removing all vertices of $P$ inside $B(O, K_ε)$ and all edges incident with them. But, with probability $1 - ε$, taken over the restriction of $P \cup P'$ to $ℝ^d \setminus B(O, K)$, this does not depend on points within distance $K$ of the origin. Since this holds for all $ε > 0$, $E$ is, up to a set of probability zero, equal to an event that does not depend on points within distance $K$ of the origin. Consequently, $E$ is a tail event.

An alternative proof of Theorem 2 proceeds by noting that the Poisson process is ergodic and that percolation is translation invariant, so automatically has probability either 0 or 1. We have given a complete proof from first principles, since the proof of Theorem 23 makes use of a similar technique (among other ingredients).

Since, for a fixed instance of $P$, adding points to $P'$ can only remove edges from $G_{sec}$, the probability $p_X(λ, d)$ is non-increasing in $λ$. Define the critical intensity $λ_{X,d}$ by the formula

$$λ_{X,d} = \inf\{λ : p_X(λ, d) = 0\} = \sup\{λ : p_X(λ, d) = 1\}$$

and write (just for this paper) $λ_X = λ_{X,2}$. We reiterate that increasing $λ$ decreases the probability of percolation, in our formulation of the model. From (1), we have

$$λ_B ≤ λ_S ≤ \min\{λ_I, λ_O\}, \quad \max\{λ_I, λ_O\} ≤ λ_U. \quad (2)$$

Our first aim is to provide bounds on $λ_X$. While doing this, we survey various methods that have been used for other continuum percolation models. All of these are from [7], [11] and [15], on percolation in the Gilbert disc model, and from [2] and [10], on percolation in the $k$-nearest neighbour model.

### 3.1 Branching processes ([7], [10], [11], [15])

For both the Gilbert disc model and the $k$-nearest neighbour model (the “traditional models”), the basic method is as follows. We start with a vertex $x$ of $P$, grow the cluster containing $x$ in “generations”, and compare the growing cluster to a branching process. For the most natural way of doing this (details below), the branching process has more points than the cluster, so, in all dimensions, if the branching process dies out, so will the cluster. We can now use classical results which tell us when certain branching processes die out. Consequently, in all dimensions, branching processes give lower bounds for thresholds in the traditional models, i.e., they show that for certain parameters, percolation does not occur.

In the following, we will describe the method for the Gilbert disc model, although it is almost the same as for the $k$-nearest neighbour model. Assume that the origin $O$ is a point of $P$. First pick the points of $P$ within distance $r$ of $O$ – these are the first generation. The second generation are the points
of $\mathcal{P}$ which are each within distance $r$ of some first generation point, but are not in the first generation themselves (i.e., they are not within distance $r$ of $O$). The third generation are the points of $\mathcal{P}$ not belonging to the first two generations, but which are each within distance $r$ of some second generation point, and so on. The associated branching process is obtained by setting each offspring size distribution to be $\text{Po}(\pi r^2)$, so that we are essentially growing the same cluster containing $O$, but ignoring the fact that the various discs we have scanned for points actually overlap. In [7], Gilbert argues that if $\pi r^2 \leq 1$, the branching process dies out with probability 1, so that the critical area for percolation is at least 1. When $\pi r^2 > 1$, it is possible to calculate (numerically) the probability that the branching process dies out, so this gives an upper bound on the probability that $O$ belongs to an infinite component. Gilbert also notes the following improvement. The discs surrounding a point of $\mathcal{P}$ and its descendant in $\mathcal{P}$ always intersect in an area of at least $\alpha = \left(\frac{2}{3} \pi - \frac{3}{2} \sqrt{3}\right) r^2$, so we can compare with a branching process whose offspring size distribution is just $\text{Po}((\pi - \alpha)r^2)$. This leads to the improved lower bound of $\frac{\pi}{\pi - \alpha} \approx 1.642$, which was further improved to 2.184 by Hall [11] using multitype branching processes.

This method can be used to give an upper bound of $\lambda O \leq 1$ for the secrecy graph model. In fact, for oriented out-percolation, we have the following result.

**Proposition 3.** The probability $\theta_O(\lambda)$ that $O$ belongs to an infinite out-component in the secrecy graph satisfies

$$\theta_O(\lambda) \leq \max\{0, 1 - \lambda\}.$$ 

**Proof.** As in the above proof sketch, we compare the growing cluster, starting at a black point $p \in \mathcal{P}$, with a branching process. The number of children in the first generation has distribution given by a geometric random variable with mean $1/\lambda$. After the $n^{th}$ generation has been completed, we order the points of the $n^{th}$ generation in order of distance from $p$, and begin growing a ball around each point in turn (according to the order). For each black point $x$, there are two possibilities. First, the ball corresponding to $x$ might encounter a red point which has already been encountered. If not, the ball will certainly outgrow the region $R$ already scanned (by points in previous generations, or the current generation). In this case, the number of black points outside the region $R$ that we encounter before the first red point (which stops the ball) will again have a geometric distribution with mean $1/\lambda$. Consequently, the number of children of a black point is always stochastically dominated by a geometric random variable with mean $1/\lambda$, and generating function $f(x) = \frac{\lambda}{1 + \lambda - x}$. A branching process whose offspring size distribution is given by this geometric random variable has extinction probability 1 if $\lambda \geq 1$, and extinction probability $\lambda$ if $\lambda \leq 1$. (When $\lambda < 1$, the extinction probability is given by the smallest root of $x = f(x)$.) Consequently, the cluster stops growing with probability at least $\lambda$, and so $\theta_O(\lambda) \leq 1 - \lambda$. \hfill $\square$
In higher dimensions, the cluster is approximated better and better by the appropriate branching process, at least for the Gilbert and \( k \)-nearest neighbour models. This is because the distances from a point \( p \in \mathcal{P} \) to its two nearest neighbours in \( \mathcal{P} \) converge in distribution to a (common) deterministic limit, and because the overlap between the balls centered at a parent and at its child gets smaller and smaller, as \( d \to \infty \). There is a slight complication in that the error (between the model and a branching process) is only asymptotically negligible over finitely many generations. Therefore, in both [10] and [15], oriented lattice percolation is brought in to establish asymptotic thresholds for percolation. The results are that in sufficiently high dimension, \( k = 2 \) gives percolation for the \( k \)-nearest neighbour model, and that the critical volume in the Gilbert model tends to 1 as \( d \to \infty \).

For the secrecy graph, we have

**Theorem 4.** If \( \lambda \geq 1 \), then, for all \( d \), \( \theta_{O,d}(\lambda) = 0 \). If \( \lambda < 1 \), then \( \theta_{O,d}(\lambda) \to 1 - \lambda \) as \( d \to \infty \).

The first part of the theorem follows from the above proposition, so we assume from now on that \( \lambda < 1 \).

We will prove this theorem in a series of steps, and we will utilize five different branching random walks. The first is the process \( (X^d_n) \). We define \( X^d_0 \) to be the single point at the origin in \( \mathbb{R}^d \), which we will suppose belongs to \( \mathcal{P} \). \( X^d_1 \) is the set of points of \( \mathcal{P} \) that are closer to \( X^d_0 \) than any point of \( \mathcal{P}' \), ordered according to modulus. Thus the points in \( X^d_1 \) are the out-neighbours of \( X^d_0 \) in \( \vec{G}_{\text{sec}} \). We generate the set \( X^d_2 \) by examining the points of \( X^d_1 \) in order, and growing a ball around each one, capturing black points until the first red point is encountered. We call this *scanning* around the points of \( X^d_1 \). After we have scanned around each point of \( X^d_1 \), the newly-captured black points (i.e., those not in \( X^d_0 \cup X^d_1 \)) form \( X^d_2 \). Thus \( X^d_2 \) is the set of out-neighbours of the points of \( X^d_1 \) in \( \vec{G}_{\text{sec}} \) that are not out-neighbours of \( X^d_0 \). This time, we order the points of \( X^d_2 \) according to the order in which they were captured, i.e., they inherit the order of their parents in \( X^d_1 \), and, within sibling groups, they are ordered by distance to the parent. The set \( X^d_3 \), of not-already encountered out-neighbours of \( X^d_2 \), is generated in the same way, and the same ordering is imposed upon its members. Continuing in this manner we obtain \( (X^d_n) \). Of course, it is entirely possible that this process terminates after a finite number of steps.

As we have already remarked, as \( d \to \infty \), this process more and more resembles the following one. We set \( Y^d_0 \) to be the single point at the origin in \( \mathbb{R}^d \), as before. The set \( Y^d_1 \) is the set of out-neighbours of \( Y^d_0 \) in \( \vec{G}_{\text{sec}} \), again as before. However, to generate \( Y^d_2 \), we use a different procedure. Examining the points of \( Y^d_1 \) in order of modulus, for each point, we generate entirely fresh copies of \( \mathcal{P} \) and \( \mathcal{P}' \), and for each point \( y \in Y^d_1 \), the children of \( y \) in \( Y^d_2 \) are the out-neighbours of \( y \) in this new copy of \( \vec{G}_{\text{sec}} \), once again ordered by distance to the parent. We continue in this manner to obtain \( (Y^d_n) \); each time we scan around a new point, we use a fresh copy of \( \mathcal{P} \) and \( \mathcal{P}' \), and the ordering on the points within each generation is as before. This process might also terminate.
Let first term. Moreover, the extinction probability is $n^{-1}$ when encountering an old red point, from the original instance of the first red point of the new instance of Lemma 6. To the origin in Lemma 5.

$d$-dimensional ball. This doesn’t affect the graph following [10] and [15], scale the processes will use the following well-known lemmas. To simplify their statements, we will, fixed $d$, we can essentially let the percolation probability 1

Consequently (see, for instance [19]),

$$
\Pr(\lvert Y^n_d \rvert = j) = \begin{cases} 
\frac{\mu^n - 1}{\mu^n + 1 - 1} & \text{if } j = 0 \\
\frac{\mu^n (\mu - 1)^2}{\mu^n + 1 - 1} \left( \frac{\mu^n + 1 - 1}{\mu^n + 1 - 1} \right)^{j-1} \sim \frac{\mu^n (\mu - 1)^2}{\mu^n + 1 - 1} \exp \left( -j(\mu - 1) \right) & \text{if } j \geq 1.
\end{cases}
$$

(Here, the asymptotics are as $n \to \infty$, with $\mu$ and $j$ fixed.) The expected size of the $n$th generation is $\mu^n$, and its mass function is geometric, except for the first term. Moreover, the extinction probability is $\lambda = 1/\mu$, corresponding to the percolation probability $1 - \lambda$. The idea of the rest of the argument is that we can essentially let $k \to \infty$ in the preceding discussion, even though, for any fixed $d$, the processes $(X^n_d)$ and $(Y^n_d)$ will eventually differ with probability 1.

To compare the processes $(X^n_d)$ and $(Y^n_d)$ over the first $k$ generations, we will use the following well-known lemmas. To simplify their statements, we will, following [10] and [15], scale the processes $\mathcal{P}$ and $\mathcal{P}'$ so that they have intensities $1/\alpha_d$ and $\lambda/\alpha_d$ respectively, where $\alpha_d = \pi^{d/2}/\Gamma(1 + d/2)$ is the volume of a unit $d$-dimensional ball. This doesn’t affect the graph $\hat{G}_{sec}$.

Lemma 5. Let $d_i$, for $1 \leq i \leq t$, be the distance of the $i$th nearest point of $\mathcal{P}$ to the origin in $\mathbb{R}^d$. Then, as $d \to \infty$, $d_i \to 1$ in probability.

Lemma 6. Let $B_1$ and $B_2$ be balls in $\mathbb{R}^d$ of radii $r_1, r_2 \in (0.9, 1.1)$. Suppose that the centers of the $B_i$ are at least 0.9 units apart. Then, as $d \to \infty$, the proportion of the volume of $B_1$ which lies inside $B_2$ tends to zero.
Let us see how these lemmas are applied. Fix $y \in Y^d_n$. Firstly, by Lemma 5, all the children $y_1, \ldots, y_t$ of $y$ lie at distance approximately 1 from $y$, as $d \to \infty$. Secondly, by Lemma 6, the $y_i$ are at distance more than 1 from each other, and from the nearest red point $z$ (which is also at distance about 1 from $y$). Write $B = B(y, ||z - y||)$, so that $B$ is the ball generated about $y$ while scanning for children. Now, while scanning around the children $y_i$ of $y$, we generate certain balls $B_i$ of radius approximately 1, centered at the $y_i$, which are stopped by red points $z_i$. The balls $B_i$ will intersect each other, and naturally they will all intersect $B$. However, again by Lemma 6, the volumes of all these intersections will be negligible compared to the volumes of the balls themselves. Consequently, the $y_i$ are very likely to have disjoint sets of children, all born outside $B$, and each of the balls $B_i$ will be stopped by a different point $z_i \neq z$, which will also lie outside $B$. This argument can clearly be carried out for a fixed number $k$ of generations. (Incidentally, the edge between a child and its parent will be almost orthogonal to each of the edges joining the same child to its own children, so the points of $Y^d_n$ will all lie at about distance about $\sqrt{k}$ from $Y^d_0$, when $d$ is large.)

The upshot of this is the following fact, which will be central to all that follows.

**Lemma 7.** Fix $\epsilon > 0$ and $k \geq 1$. If $d \geq d_0(\epsilon, k)$, then the probability that $(X^d_n)$ and $(Y^d_n)$ differ in the first $k$ generations is less than $\epsilon$.

The next step is to project the points of $(Y^d_n)$ onto $\mathbb{R}^2$ using the map $L : \mathbb{R}^d \to \mathbb{R}^2$ defined by

$$L(x_1, \ldots, x_d) = \sqrt{d}(x_1, x_2).$$

The reason for the factor $\sqrt{d}$ is the following lemma, taken from [10].

**Lemma 8.** Suppose $Y$ is uniformly distributed on the surface of the ball of radius 1 in $\mathbb{R}^d$. Then, as $d \to \infty$, the random variable $Z = L(Y)$ converges in distribution to the bivariate normal distribution $N(0, I)$ with mean zero and covariance matrix equal to the $2 \times 2$ identity matrix $I$. In other words, the density function of $Z$ converges pointwise to

$$f(z_1, z_2) = \frac{1}{2\pi} \exp \left(-\frac{z_1^2 + z_2^2}{2}\right)$$

as $d \to \infty$.

**Proof.** The proof of an almost identical statement appears in [15], and the result is well-known, but we sketch the proof nonetheless. If $X_1, X_2, \ldots, X_d$ are independent $N(0,1)$ random variables, then the $d$-dimensional random vector $X = (X_1, X_2, \ldots, X_d) \in \mathbb{R}^d$ has density function

$$f_d(x_1, x_2, \ldots, x_d) = \frac{1}{(2\pi)^{d/2}} \exp \left(-\frac{x_1^2 + x_2^2 + \cdots + x_d^2}{2}\right),$$

which is radially symmetric. Moreover, using Chebyshev's inequality, we see that $\frac{1}{d} |X|^2 = \frac{1}{d} (X_1^2 + \cdots + X_d^2)$ converges in probability to 1 as $d \to \infty$, and
so \( \frac{1}{\sqrt{n}} X \) converges in distribution to \( Y \). Consequently, the distribution of the first two coordinates of \( \sqrt{d} Y \) converges (in distribution) to that of \((X_1, X_2)\), as stated in the lemma.

Write \((Z_n)\) for the result of projecting the process \((Y_{2n}^d)\) from \(\mathbb{R}^d\) to \(\mathbb{R}^2\) using the map \(L\), and write \((Z_n^\infty)\) for the process in which the offspring size distribution agrees with that of \((Z_n)\) and \((Y_{2n}^d)\) (i.e., is geometric with mean \(1/\lambda\)), but where the offsets of each child are independent \(N(0, I)\) random variables. The preceding lemma shows that the processes \((Z_n)\) and \((Z_n^\infty)\) resemble each other more and more as \(d \to \infty\). Consequently, we will study the process \((Z_n^\infty)\) first, and draw conclusions about the other processes later.

Rather than consider the entire process \((Z_n^\infty)\), we will use a “truncated” version, and compare with oriented site percolation on the lattice \(\Lambda = \{(i, j) \in \mathbb{Z}^2 : i \geq 0, |j| \leq i, i + j \in 2\mathbb{Z}\}\), with oriented edges from \((i, j)\) to \((i + 1, j \pm 1)\). Each site \((i, j)\) of \(\Lambda\) will correspond to a square

\[
S_{i,j} = [M(i - 1/2), M(i + 1/2)] \times [M(j - 1/2), M(j + 1/2)]
\]

in \(\mathbb{R}^2\), where \(M\) is a large integer which we will choose later. Since the oriented percolation probability is left-continuous at 1 (see [6], for instance), we may choose \(\delta > 0\) such that, for oriented site percolation on \(\Lambda\) with parameter \(p \geq 1 - 3\delta\), the oriented percolation probability (of the event that there is an infinite directed path starting from the origin) is greater than \(1 - \epsilon/2\).

A site \((i, j)\) in the oriented percolation process will be deemed \(Z^\infty\)-open if we can proceed to both \((i + 1, j - 1)\) and \((i + 1, j + 1)\) from it. However, “proceed” will mean different things in the cases \(ij = 0\) and \(ij \neq 0\). Assume, as before, that the point \(Z_0^\infty\) lies at the origin. The site \((0, 0)\) will be \(Z^\infty\)-open if and only if \(Z_0^\infty\) has at least \(m\) descendants in generation \(k_1\) within the square \(S_{1, -1}\), and at least \(m\) descendants, also in generation \(k_1\), within the square \(S_{1, 1}\). We will only test a subsequent site \((i, j)\) for \(Z^\infty\)-openness if at least one of \((i - 1, j + 1)\) or \((i + 1, j - 1)\) is \(Z^\infty\)-open. If at least one of these two sites is \(Z^\infty\)-open, then we know that there are \(m\) points \(z_1, \ldots, z_m\) of \((Z_n^\infty)\) in \(S_{i,j}\). (If there are more than \(m\) such points, for definiteness let \(z_1, \ldots, z_m\) be the closest ones to the center of the square.) Site \((i, j)\) will be \(Z^\infty\)-open if and only if \(z_1, \ldots, z_m\) have at least \(m\) descendants in generation \(k_2\) (counted from the \(z_i\), not from \(Z_0^\infty\)) in \(S_{i+1, j-1}\), and at least \(m\) descendants in generation \(k_2\) in \(S_{i+1, j+1}\). We require lower bounds on the probabilities of sites being \(Z^\infty\)-open, and these are provided by the following lemmas.

**Lemma 9.** Fix \(\lambda < 1, \delta > 0\) and \(m \geq 1\). There exist positive integers \(k_1(\lambda, \delta, m)\) and \(M(\lambda, \delta, m)\) such that, with the above definitions, the probability that \((0, 0)\) is \(Z^\infty\)-open is at least \(1 - \lambda - \delta\).

**Proof.** Since the proof of an almost identical statement appears in [10] (only the offspring size distribution is different), we will just sketch the argument. For \(\lambda < 1\), the branching process is supercritical, and by (3) we can find a generation \(k_3(\lambda, \delta, m)\) so that the probability that there are, say, \(N = N(\lambda, \delta, m)\) members
in generation $k_3$ is at least $1 - \lambda - \delta / 4$. These $N$ individuals $z_1, \ldots, z_N$ will all be at distance about $\sqrt{k_3}$ from the origin, and we can ensure that, with probability $1 - \lambda - \delta / 2$, they all lie within distance $M = [2\sqrt{k_3}]$ of the origin. If we run the process for another $M^2$ generations, then about $\lambda N$ of the $z_i$ will not have any descendants in generation $k_3 + M^2$. However, if we pick a random descendant of each remaining $z_j$ in generation $k_3 + M^2$, there is a constant probability that it will land in $S_{1,1}$ or $S_{1,-1}$, since this descendant will lie about distance $M$ from $z_j$, which in turn lies within distance $M$ from the origin. Consequently, from the independence, if $N$ is large enough, we will have, with probability at least $1 - \lambda - \delta$, at least $m$ descendants of $Z_{\infty}$ in generation $k_1 = k_3 + M_2$ in each of $S_{1,1}$ and $S_{1,-1}$.

A similar argument establishes the following lemma.

**Lemma 10.** Fix $\lambda < 1$ and $\delta > 0$. Then there exist positive integers $m(\lambda, \delta), k_1(\lambda, \delta), k_2(\lambda, \delta)$ and $M(\lambda, \delta)$ such that, with the above definitions, the probability that $(0,0)$ is $Z_{\infty}$–open is at least $1 - \lambda - \delta$, and the probability that a site $(i, j)$ with $ij \neq 0$ is $Z_{\infty}$–open is at least $1 - \delta$.

Define $Z$–openness in the obvious manner, using the process $(Z_n)$ rather than $(Z_{\infty})$. The following lemma follows from Lemma 10 and Lemma 8.

**Lemma 11.** Fix $\lambda < 1$ and $\delta > 0$. Then there exist positive integers $m(\lambda, \delta), k_1(\lambda, \delta), k_2(\lambda, \delta), M(\lambda, \delta)$ and $d(\lambda, \delta)$ such that, with the above definitions, the probability that $(0,0)$ is $Z$–open is at least $1 - \lambda - \delta$, and the probability that a site $(i, j)$ with $ij \neq 0$ is $Z$–open is at least $1 - \delta$.

If we could draw the same conclusion for the projection of the process $(X_n^d)$, we would be done. However, the process $(X_n^d)$ is harder to analyze, owing to possible interference between steps. To be specific, denote by “step $(i, j)$” the procedure whereby we determine, for the projection of the process $(X_n^d)$, whether or not the site $(i, j)$ is $W$–open. (Here, $(W_n)$ will be the projection of a suitably modified version of $(X_n^d)$.) It is possible that, during step $(i, j)$, a black point (or a red point) is born in a region that was scanned as part of a previous step $(i', j')$. It is also possible that a red point, discovered in some previous step $(i', j')$, is encountered in step $(i, j)$. We need to show that both of these possibilities can be neglected.

For the remainder of the proof, $\delta$ and $\lambda$ will be fixed. Write $k = \max\{k_1, k_2\}$. The first step is to show that we may assume that, in the first $k$ generations of $(X_n^d)$, the total number of descendants is bounded by an absolute constant $N$, the total volume scanned is bounded by an absolute constant $V$, and the distance of the $L$–projection of any point from the origin (in $\mathbb{R}^2$) is at most an absolute
constant $R$. (Here, these “absolute constants” might depend on the (fixed) $\delta$ and $\lambda$, but they don’t depend on $d$.) Indeed, the probabilities of the failures of these conditions can each be made arbitrarily small by taking $N, V$ and $R$ suitably large. If any of them fail, we modify the process $(X_n^d)$ to terminate at the first failure, and deem step $(i, j)$ to be a failure. We denote by $(W_n)$ the $L-$projection of this modified process to $\mathbb{R}^2$. The preceding discussion, together with Lemma 7, proves the following.

**Lemma 12.** Fix $\delta > 0$ and $k \geq 1$. If $d \geq d_1(\delta, k)$, then the probability that $(W_n)$ and $(Z_n)$ differ in the first $k$ generations is less than $\delta$.

To summarize, we have dealt with two ways in which step $(i, j)$ could fail: the processes $(W_n)$ and $(Z_n)$ might differ, or $(Z_n)$ might fail to proceed to both $S_{i+1,j-1}$ and $S_{i+1,j+1}$ for some reason involving only the $k_1$ or $k_2$ generations corresponding to step $(i, j)$. To these we must add two more: the step might fail because a black or red point might be born in a previously scanned region (from a step $(i', j')$), or a previously discovered red point (from a step $(i', j')$) might be encountered. If we can show that the probability of each of these two events can be bounded by $\delta$, we will be done. The following lemma does just this. We modified the process $(X_n^d)$ to facilitate the proof of this lemma.

**Lemma 13.** Let the process $(W_n)$ be defined as above. Then, during the step $(i, j)$, the probability that either a black or a red point is born in a region scanned in a previous step, or that a red point from a previous step is encountered, is at most $\delta$.

**Proof.** Consider a previous step $(i', j')$, and suppose that $(Mi', Mj')$ is at distance $x \gg 2R$ from $(Mi, Mj)$. The total volume scanned in step $(i', j')$ is at most $V$, and, if $x \geq D$ is sufficiently large, at most $\delta'/x^3$ of this volume falls, when projected, within distance $M + R$ from the center $(Mi, Mj)$ of $S_{i,j}$. Summing over all square centers $(Mi', Mj')$ at distance more than $D$ from $(Mi, Mj)$, the total previously scanned volume from these distant steps which falls, after projection, within distance $M + R$ from $(Mi, Mj)$ is at most $\delta'$. Since there are at most $N$ individuals in step $(i, j)$, we can choose $\delta'$ (and hence $D$), so that the probability that a black or red point from step $(i, j)$ is born in this region of volume $\delta'$ is at most $\delta'/3$. Similarly, the probability that, while scanning in step $(i, j)$, we hit a previously encountered red point from a distant step is at most $\delta/3$. For the steps at distance at most $D$, we can bound the probability of failure of either type by $\delta/3$, because only boundedly many steps are involved. \qed

Together, the last three lemmas prove the following one.

**Lemma 14.** Fix $\lambda < 1$ and $\delta > 0$. Then there exist constants

$$m(\lambda, \delta), k_1(\lambda, \delta), k_2(\lambda, \delta), M(\lambda, \delta), N(\lambda, \delta), V(\lambda, \delta), R(\lambda, \delta) \text{ and } d(\lambda, \delta)$$

such that, with the above definitions, the probability that $(0, 0)$ is $W-$open is at least $1 - \lambda - 2\delta$, and the probability that a site $(i, j)$ with $ij \neq 0$ is $W-$open is at least $1 - 3\delta$.
It only remains to put the pieces together. Given $\epsilon > 0$, we choose $\delta < \epsilon/4$ so that, for oriented site percolation on $\Lambda$ with parameter $p \geq 1 - 3\delta$, the oriented percolation probability (of the event that there is an infinite directed path starting from the origin) is greater than $1 - \epsilon/2$. From the previous lemma, we find an infinite directed $W-$path from the origin, corresponding to an infinite out-component in $\tilde{G}_{\text{sec}}$, with probability at least

$$(1 - \lambda - 2\delta)(1 - \epsilon/2) > (1 - \lambda - \epsilon/2)(1 - \epsilon/2) > 1 - \lambda - \epsilon,$$

as required. This completes the proof of Theorem 4.

The method seems to be tailored for oriented out-percolation, so we expect it won’t give bounds for other types of percolation, except via equation (2). In two dimensions, it should be possible to improve the bound in Proposition 3 using Hall’s modification, which, for the disc model, runs as follows. Each offspring $y$ is indexed by its distance $t$ to its parent $x$, and its offspring size distribution is bounded in terms of the area of the lune $D(y, r) \setminus D(x, r)$. In addition, the distribution of the types of these offspring is also bounded in terms of the same lune. Consequently, one can compare the growing cluster with an appropriate multitype branching process (the types are indexed by $t$). For the secrecy graph, there are three parameters one might wish to keep track of (instead of just one). These are: the radius $r$ of the disc centered at $x$, the distance $t$ of $x$ to its offspring $y$, and the location of the red point $z$ on the boundary $\partial D(x, r)$ of $D(x, r)$. Nonetheless, one could in principle compute the appropriate conditional probability distribution and this should result in a slightly improved upper bound.

To summarize, although branching processes are usually employed to show that percolation does not occur in these models, they can also be used to show that percolation does occur for certain fixed values of the parameters, as $d \to \infty$. For the secrecy graph model, it would be interesting to investigate the case $\lambda = 1$, as $d \to \infty$.

### 3.2 Lattice percolation ([7], [10], [11], [17], [18])

Two variants of the basic method, applied to the Gilbert model, are described in Gilbert’s original paper [7]. For both variants, fix a connection radius $r$. First, if we consider the square lattice with bonds of length $r/2$, and make the state of a bond $e$ open iff there is at least one point of $P$ in the square whose diagonal is $e$, then bond percolation in the lattice implies percolation in the Gilbert model. Second, if we consider the hexagonal lattice where the hexagons have side length $r/\sqrt{3}$, and make the state of a hexagon open iff it contains a point of $P$, then face percolation in the hexagonal lattice implies percolation in the Gilbert model. Using the fact that the critical probabilities for both bond percolation in the square lattice and face percolation in the hexagonal lattice are equal to $1/2$, one thus obtains upper bounds on the critical area $\pi r^2$ of about 17.4 and 10.9, respectively. The latter value was improved to 10.588 by Hall [11] using “rounded hexagons”.

12
Häggström and Meester [10] used this method to show that, for fixed $d$, percolation occurs in the $k$-nearest neighbour model for sufficiently large $k$. Pinto and Win [17] (see [18] for more details) applied it to show that percolation occurs in all versions of the secrecy graph model when $\lambda$ is sufficiently small. For the latter application, one needs to use dependent percolation, which means that the bounds are rather weak. In the same paper, Pinto and Win prove an upper bound on $\lambda_U$, also using lattice percolation. Their method is to tile the plane with regular hexagons, each of side length $\delta$. Divide each hexagon into 6 equilateral triangles in the obvious way. Set the state of a hexagon to be closed if it contains no black points and at least one red point in each of its 6 triangles, and open otherwise. If the probability $g(\lambda, \delta)$ of this is at least $1/2$, the critical probability of face percolation on the hexagonal lattice, then the origin will almost surely be surrounded by arbitrarily large closed circuits. It is easy to check that an edge of $G_{sec}$ cannot cross a closed circuit, and so percolation will not occur in $G_{sec}$ if $g(\lambda, \delta) \geq 1/2$. Now

$$g(\lambda, \delta) = \left(1 - e^{-\lambda \sqrt{3} \delta^2 / 4}\right)^6 e^{-3\sqrt{3} \delta^2 / 2},$$

and, for fixed $\lambda$, we maximize $g(\lambda, \delta)$ by setting

$$e^{-\lambda \sqrt{3} \delta^2 / 4} = \frac{1}{1 + \lambda},$$

so the smallest value of $\lambda$ for which

$$\left(\frac{\lambda}{1 + \lambda}\right)^6 \left(\frac{1}{1 + \lambda}\right)^{6/\lambda} \geq \frac{1}{2}$$

will be an upper bound for $\lambda_U$. The last equation can be solved numerically to yield the bound $\lambda_U \leq 40.9$. The method can easily be modified to give bounds for the other $\lambda_X$, but we expect that the results will be rather weak.

In summary, lattice percolation has generally been used to show that percolation does occur in these models, although Pinto and Win also used it to show that percolation does not occur in the secrecy graph if $\lambda$ is sufficiently large.

### 3.3 The rolling ball method ([2])

This is a method designed to show that percolation does occur for certain parameter ranges in various models. It was applied in [2] to prove upper bounds for critical values of $k$ in the $k$-nearest neighbour model. Unfortunately, when applied to the Gilbert disc model, it only yields an upper bound (on $\pi r_c^2$) of about 12, worse than the previously best known bound.

The method involves comparison with 1-independent percolation and carries through almost entirely for the secrecy graph. We will only need to modify some of the equations from [2]: however, for completeness, we include a full account of the method here. First, we state precisely what we mean by a 1-independent percolation model.
Definition 15. A bond percolation model on $\mathbb{Z}^2$ is said to be 1-independent if, whenever $E_1$ and $E_2$ are sets of edges at graph distance at least 1 from each other (i.e., if no edge of $E_1$ is incident to any edge of $E_2$), the state of the edges in $E_1$ is independent of the state of the edges in $E_2$.

We will use the following theorem about such models, proved in [3].

Theorem 16. If every edge in a 1-independent bond percolation model on $\mathbb{Z}^2$ is open with probability at least 0.8639, then, almost surely, there is an infinite open component. Moreover, if $B$ is a bounded region of the plane, there is, almost surely, a cycle of open edges surrounding $B$.

We will use the first part of the theorem for our lower bounds, and the second part for our upper bounds.

For simplicity, let us first consider the case of $B$-percolation. Later, we will indicate the modifications necessary for the other types.

Consider the rectangular region consisting of two adjacent squares $S, T$ shown in Figure 1. Both $S$ and $T$ have side length $2r + 2s$, where $r$ and $s$ are to be chosen later. Also, $T$ may be to the right, left, above or below $S$, in which case Figure 1 should be rotated accordingly. We define the basic good event $E_{B,S,T}$ to be the event that every black point $u$ in the central disc $K$ of $S$ is joined to at least one black point in the central disc $M$ of $T$ by a path in $G_{sec}',$ regardless of the state of the Poisson processes outside $S \cup T$, and moreover that $K$ contains at least one black point.

Now consider the following percolation model on $\mathbb{Z}^2$. Each vertex $(i, j) \in \mathbb{Z}^2$ corresponds to a square $[R_i, R(i+1)] \times [R_j, R(j+1)]$ in $\mathbb{R}^2$, where $R = 2r + 2s$, and an edge is open between adjacent vertices (corresponding to squares $S$ and $T$) if both the corresponding basic good events $E_{B,S,T}$ and $E_{B,T,S}$ hold. Note that this is a 1-independent model on $\mathbb{Z}^2$, and that percolation in this model implies percolation in the original one. Since, by Theorem 16, the critical probability for any 1-independent model is at most 0.8639, if we can show that, for some $r, s, \lambda,$

$$\mathbb{P}(E_{B,S,T}) \geq 0.93195$$

Figure 1: The rolling ball method
it will follow that
\[ \mathbb{P}(E_{B,S,T} \cap E_{B,T,S}) \geq 0.8639 \]
by symmetry, and hence we will have shown that \( \lambda_B \geq \lambda \).

To bound the probability that a basic good event fails, we proceed as follows. Let \( K, L \) and \( M \) be as in Figure 1. (\( L \) is the region between the two discs \( K \) and \( M \).) Define \( E_{B,S,T} \) to be the event that for every black point \( v \in K \cup L \), there is a black point \( u \) such that i) \( uv \in E(G_{sec}') \) ii) \( \|u - v\| \leq s \) and iii) \( u \in D_v \), where \( D_v \) is the disc of radius \( r \) inside \( K \cup L \) with \( v \) on its \( K \)-side boundary (the middle disc in Figure 1). If we let \( F_S \) be the event that there is at least one black point in \( K \), then we have (see [2] for background)

\[ E_{B,S,T} \cap F_S \subset E_{B,S,T} \]

and so
\[ E_{B,S,T}^c \subset (E_{B,S,T})^c \cup F_S^c \]

so that, since \( \mathbb{P}((E_{B,S,T})^c) \) is bounded by the expected number of points \( v \) such that i), ii) or iii) fail,

\[ \mathbb{P}(E_{B,S,T}^c) \leq e^{-\pi r^2} + 2r(2r + 2s)p_{B,r,s} \]

where \( p_{B,r,s} \) is the probability that i), ii) or iii) fail for some fixed \( v \).

To bound \( p_{B,r,s} \), we consider the probability that the vertex \( u \) closest to \( v \) inside \( D_v \) fails one of i), ii) or iii) (or does not exist). Suppose some \( u \in D_v \) does exist, and write \( t = \|u - v\|, A = B(v,t), B = B(v,t) \cap D_v \) and \( C = B(u,t) \). Let \( p_B(u) \) be the probability that \( u \) is the closest point to \( v \) inside \( D_v \), but that \( uv \notin G_{sec}' \). Then

\[ p_B(u) = (1 - e^{-\lambda|A \cup C|})e^{-|B|} \tag{4} \]

and also
\[ p_{B,r,s} \leq e^{-|D_v \cap B(v,s)|} \int_{u \in D_v \cap B(v,s)} p_B(u) \, du \]

so that
\[ \mathbb{P}(E_{B,S,T}^c) \leq e^{-\pi r^2} + 2r(2r + 2s) \left( e^{-|D_v \cap B(v,s)|} + \int_{u \in D_v \cap B(v,s)} (1 - e^{-\lambda|A \cup C|})e^{-|B|} \, du \right) \tag{5} \]

and the right hand side can be minimized over all \( r \) and \( s \), with \( \lambda \) fixed. The result is shown in Table 1, in row \( B \).

The calculation for the cases \( U \) and \( O \) is exactly analogous, using the graphs \( G_{sec} \) and \( \tilde{G}_{sec} \) respectively. The analogues of (4) are

\[ p_U(u) = (1 - e^{-\lambda|A|} - e^{-\lambda|C|} + e^{-\lambda|A \cup C|})e^{-|B|} \tag{6} \]

and
\[ p_O(u) = (1 - e^{-\lambda|A|})e^{-|B|} \tag{7} \]

respectively, and the natural analogue of (5) applies. The results of the optimization are shown in Table 1.

As proved in [2], the bound for \( \lambda_O \) in fact applies to \( \lambda_S \) and \( \lambda_I \) as well (see [2] for a proof). In conclusion, we have proved the following theorem.
Theorem 17. $\lambda_U \geq 0.002, \lambda_O \geq 0.0008, \lambda_I \geq 0.0008, \lambda_S \geq 0.0008$ and $\lambda_B \geq 0.0005$.

3.4 High confidence results ([2])

This method gives both upper and lower bounds for percolation thresholds in the $k$-nearest neighbour model. It involves computing a certain high dimensional integral using Monte Carlo methods, and so is not fully rigorous. The approach carries over essentially completely for the secrecy graph.

The lower bound method (corresponding to the upper bound method for the $k$-nearest neighbour model) may be summarized as follows. Given a trial value of $\lambda$, which we wish to show is a lower bound on one of the percolation thresholds $\lambda_U, \lambda_O$ or $\lambda_B$, we choose trial values of $r$ and $s$. Then we generate a random instance of $P \cup P'$ inside $S \cup T$ and test for the following conditions: i) for more than half of the black points $v \in K$, there are paths (in $G_{sec}, \tilde{G}_{sec}$ or $G'_{sec}$ for the cases $X = U, O, B$) to more than half the black points in $M$, regardless of the state of $P \cup P'$ outside $S \cup T$; ii) for more than half of the black points $v \in M$, there are paths to more than half the black points in $K$, regardless of the state of $P \cup P'$ outside $S \cup T$. As before, it is clear that this is a 1-independent model on the bonds joining adjacent squares, and that percolation in this model implies percolation in the original one. Consequently, if these conditions hold with probability at least 0.8639, then percolation occurs. The condition that the path should be independent of the process outside $S \cup T$ is simply obtained by ignoring any edges of $uv \in E(\tilde{G}_{sec}(S \cup T))$ where $\|u - v\| > \text{dist}(u, \partial(S \cup T))$, since only edges $uv$ with $\|u - v\| \leq \text{dist}(u, \partial(S \cup T))$ are guaranteed to exist in $\tilde{G}_{sec}$.

The probability that conditions i) and ii) are satisfied can be expressed as a complicated multiple integral, whose value we would like to be greater than 0.8639, for some $r$ and $s$. This is the integral we estimate using Monte Carlo methods. Using a computer program we generated many instances, and counted the proportion of times these conditions held. From these we calculated the confidence level, i.e., the probability $p$ that these results (or better) could be obtained, if the true value of the integral was less than 0.8639. In all cases $p$ was less than $10^{-25}$: the detailed results appear in Table 2. It turns out that the method for the $X = O$ case actually applies to the cases $X = S$ and $X = I$ as well, and the results obtained are as follows.

Theorem 18. With high confidence, $\lambda_B \geq 0.09, \lambda_O \geq 0.11, \lambda_I \geq 0.11, \lambda_S \geq 0.11$ and $\lambda_U \geq 0.20$.

<table>
<thead>
<tr>
<th>$X$</th>
<th>$\lambda$</th>
<th>$r$</th>
<th>$s$</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>0.002</td>
<td>1.659</td>
<td>3.15</td>
<td>0.0669</td>
</tr>
<tr>
<td>O</td>
<td>0.0008</td>
<td>1.658</td>
<td>3.15</td>
<td>0.0677</td>
</tr>
<tr>
<td>B</td>
<td>0.0005</td>
<td>1.657</td>
<td>3.15</td>
<td>0.0680</td>
</tr>
</tbody>
</table>

Table 1: Upper bounds on $p = \min_{r,s} P(E_{X,S,T}^C)$. (All values of $p$ rounded up.)
The upper bound method (corresponding to the lower bound method for the \( k \)-nearest neighbour model) is as follows. For suitable \( r \) and \( s \), we generate instances of \( P \) and \( P' \) in \( S \cup T \), and check whether, regardless of the state of the processes outside \( S \cup T \), there is no path (in \( G_{sec}, \tilde{G}_{sec} \) or \( G'_{sec} \) for the cases \( X = U, O, B \)) from outside \( S \cup T \) that crosses the line segment joining the center of \( S \) to the center of \( T \) (see Figure 2). We define a 1-independent percolation model on \( \mathbb{Z}^2 \) by declaring an edge open if this condition holds for the corresponding rectangle \( S \cup T \). If an edge is open with probability at least 0.8639, then, from Theorem 16, there are open cycles surrounding any bounded region of the plane. Consequently, if there was an infinite \( X \)-component starting in some such bounded region, it would have to cross an open cycle, and in particular cross the central line segment in one of the rectangles \( S \cup T \) corresponding to an open edge in this cycle. This contradicts the condition for that edge to be open, and so percolation cannot occur if the edges are open with probability at least 0.8639.

It remains to specify how we tested whether an edge of a path (in \( G_{sec}, \tilde{G}_{sec} \) or \( G'_{sec} \) for the cases \( X = U, O, B \)) could come from outside \( S \cup T \) to some \( v \in S \cup T \). In these cases, we must find possible neighbours within \( S \cup T \) of every possible point outside \( S \cup T \). To do this, we used the following algorithm. We mark all the black points falling in a certain region \( R' \), determined by the red points, as possibly having edges from outside \( S \cup T \). First we define the subset \( R \subset R' \) to be the union of various half-discs \( R_i \), described as follows. A point \( x \) moving along the boundary of \( S \cup T \) has, at almost every position, exactly one nearest neighbour in \( P' \cap (S \cup T) \). At some places, there will be a tie for the nearest neighbour of \( x \), so that \( \|x - a\| = \|x - b\| \) for some points \( a, b \in P' \). Draw the disc through \( a \) and \( b \) and centered at \( x \), and let \( R_i \) be the intersection of this disc with \( S \cup T \). \( R \) is just the union of all such regions \( R_i \), and \( R' \) is the union of \( R \) together with the regions at the corners of \( S \cup T \) which lie outside the \( R_i \) (see Figure 3).

To check that this method works, suppose that there is an edge \( xy \in E(\tilde{G}_{sec}) \), where \( x \notin S \cup T \) and \( y \in (S \cup T) \setminus R \). Let \( u \) be the point on \( \partial (S \cup T) \) on the
line joining $x$ and $y$. Then, if $B(u, \|u - y\|)$ contains a red point $a$, so does $B(x, \|x - y\|)$, since

$$\|x - a\| \leq \|x - u\| + \|u - a\| < \|x - u\| + \|u - y\| = \|x - y\|$$

so that it is enough to assume that $x = u$. Moreover, let $v$ be the point on $\partial R$ on the line joining $u$ and $y$. If $B(u, \|u - v\|)$ contains a red point $b$, so does $B(u, \|u - y\|)$, since $B(u, \|u - y\|)$ contains $B(u, \|u - v\|)$. Hence we may also assume that $y = v$. Now, with $u$ fixed, we may assume that $v$ is the closest point of $\partial R$ to $u$, which we may also assume does not coincide with the location of a red point. Draw the disc $B(u, \|u - v\|)$. By construction, this disc is tangent to one of the half-discs $R_i$, centered at $z$, say, and has a strictly smaller radius than that of $R_i$, with probability 1. Therefore, its center, $u$, lies in the interior of the line segment joining $z$ to $v$. Consequently, $u \in S \cup T$, which is a contradiction. Figure 3 shows that the three conditions i) $v$ is the closest point of $\partial R$ to $u$ ii) $\|u - v\| < \min(\|u - a\|, \|u - b\|)$ and iii) $u \in \partial(S \cup T)$ are incompatible, by illustrating a typical situation where i) and ii) are satisfied.

The results of these simulations are also shown in Table 2, and so we have the following result.

**Theorem 19.** With high confidence, $\lambda_B \leq 0.13, \lambda_O \leq 0.17, \lambda_I \leq 0.17, \lambda_S \geq 0.17$ and $\lambda_U \leq 0.27$. 
Table 2: Results of Monte-Carlo simulations. (All confidences rounded up.)

<table>
<thead>
<tr>
<th>X</th>
<th>bound</th>
<th>value</th>
<th>r</th>
<th>s</th>
<th>successes</th>
<th>trials</th>
<th>confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>lower</td>
<td>0.20</td>
<td>90</td>
<td>10</td>
<td>1480</td>
<td>1500</td>
<td>$10^{-66}$</td>
</tr>
<tr>
<td>O</td>
<td>lower</td>
<td>0.11</td>
<td>60</td>
<td>0</td>
<td>963</td>
<td>1000</td>
<td>$10^{-25}$</td>
</tr>
<tr>
<td>B</td>
<td>lower</td>
<td>0.09</td>
<td>80</td>
<td>0</td>
<td>2159</td>
<td>2250</td>
<td>$10^{-51}$</td>
</tr>
<tr>
<td>U</td>
<td>upper</td>
<td>0.27</td>
<td>110</td>
<td>0</td>
<td>4296</td>
<td>4600</td>
<td>$10^{-91}$</td>
</tr>
<tr>
<td>O</td>
<td>upper</td>
<td>0.17</td>
<td>110</td>
<td>0</td>
<td>3689</td>
<td>4000</td>
<td>$10^{-25}$</td>
</tr>
<tr>
<td>B</td>
<td>upper</td>
<td>0.13</td>
<td>125</td>
<td>0</td>
<td>6226</td>
<td>6750</td>
<td>$10^{-45}$</td>
</tr>
</tbody>
</table>

4 Uniqueness of the infinite cluster

Uniqueness of the infinite cluster above the percolation threshold was proved by Harris [12] for bond percolation in $\mathbb{Z}^2$, by Aizenman, Kesten and Newman [1] for connected, transitive and amenable graphs, by Meester and Roy [13] for the Gilbert model, and by Häggström and Meester [10] for the $k$-nearest neighbour model. The last two results were obtained by modifying a very short and elegant argument of Burton and Keane [5], which was originally applied to give a second proof of the Aizenman–Kesten–Newman theorem. The Burton–Keane argument goes through for the secrecy graph, with a considerably simpler proof than in [10]. Before presenting it, we make a few preliminary remarks.

There are three main ingredients in proving the uniqueness of the infinite cluster. One is ergodicity, which allows us to show that the number of infinite components is almost surely constant (this constant might be $\infty$). The second is the local modifier, which works as follows. Suppose we know that some event $E$ occurs with positive probability. Suppose also that, by removing a finite number of points from any instance of $P \cup P'$ in which $E$ occurs, we get a configuration in which some other event $F$ always occurs. Then also $P(F) > 0$. This is proved using coupling. The third ingredient is the trifurcation argument, which, roughly speaking, shows that the probability of having some infinite component with three distinct “branches” going off to infinity is zero. Since the ergodicity and trifurcation arguments are fairly standard (see [4, 9, 14] for instance), we will simply state their implications, without proof, and concentrate on the local modifier.

To keep things simple, we will focus on the case $X = B$. In other words, we will work with the graph $G_{sec}'$ of bidirectional edges. From now on, we will call this graph $G$. Versions of the result, with almost identical proofs, exist for the cases $X = U$ and $X = S$; when $X = I$ or $X = O$, things are more complicated, since two maximal infinite components might intersect.

First then, we describe precisely the respective end results of the ergodicity and trifurcation arguments.

**Lemma 20.** For each value of $d$, and for each $\lambda > 0$, the number of infinite components in the graph $G = G_{sec}'$ is almost surely constant. (This constant might be $\infty$.)
Lemma 21. Pick \( r > 0 \) and \( x \in \mathbb{R}^d \). Let \( T(x, r) \) be the event that the ball \( B(x, r) \) is intersected by an infinite component \( C \) of \( G = G_{\text{sec}}' \) in such a way that, if all edges of \( C \) intersecting \( B(x, r) \) are removed, \( C \) falls apart into a number of infinite components, of which at least three are infinite. Then \( \mathbb{P}(T(x, r)) = 0 \).

We next describe a useful coupling. Let \( \mathcal{P}_1 \) and \( \mathcal{P}_2 \) be two independent Poisson processes of intensity 1 in \( \mathbb{R}^d \), and let \( \mathcal{P}_1' \) and \( \mathcal{P}_2' \) be two independent Poisson processes of intensity \( \lambda \), also in \( \mathbb{R}^d \). Given \( R > 0 \), construct two more processes \( \mathcal{P}_3 \) and \( \mathcal{P}_3' \) as follows. Outside \( B(O, 3R) \), let \( \mathcal{P}_3 \) and \( \mathcal{P}_3' \) coincide with \( \mathcal{P}_1 \) and \( \mathcal{P}_1' \) respectively. Inside \( B(O, 3R) \), for \( \mathcal{P}_3 \), include each point of \( \mathcal{P}_1 \cup \mathcal{P}_2 \) with probability \( \frac{1}{2} \), and for \( \mathcal{P}_3' \), include each point of \( \mathcal{P}_1' \cup \mathcal{P}_2' \) with probability \( \frac{1}{2} \). Then \( \mathcal{P}_3 \) and \( \mathcal{P}_3' \) are both Poisson processes in \( \mathbb{R}^d \), of intensities 1 and \( \lambda \), respectively. This coupling will be referred to, following [10], as the special coupling. It shows that, if an event \( E \) occurs for an instance \( (\mathcal{P}_1, \mathcal{P}_1') \), and if an event \( F \) can be made to occur by removing some points of \( (\mathcal{P}_1, \mathcal{P}_1') \) inside \( B(O, 3R) \), then \( \mathbb{P}(E) > 0 \Rightarrow \mathbb{P}(F) > 0 \), since the modified instance occurs with positive probability for \( (\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_1', \mathcal{P}_2') \). Its first application will be in the proof of the following lemma.

Lemma 22. For each value of \( d \), and for each \( \lambda > 0 \), the number of infinite components in the graph \( G = G_{\text{sec}}' \) is either almost surely 0, almost surely 1, or almost surely \( \infty \).

Proof. By Lemma 20, we only have to show that, for each fixed \( k \geq 2 \), it is not the case that \( G \) has, almost surely, exactly \( k \) infinite components. Suppose then, that, for some \( k \geq 2 \), \( G \) has, almost surely, exactly \( k \) infinite components. For some \( r > 0 \), the probability that each of these components \( C_1, \ldots, C_k \) intersects \( B(0, r) \) is strictly positive. Given some configuration in which all \( k \) infinite components \( C_1, \ldots, C_k \) intersect \( B(0, r) \), remove all the red points in \( B(0, 3r) \). The effect of this is that the \( k \) components \( C_1, \ldots, C_k \) merge to form a single infinite component. However, using the special coupling, this shows that the probability of having a single infinite component is strictly positive, contradicting Lemma 20.

We are now ready for our final theorem.

Theorem 23. For each value of \( d \), and for each \( \lambda > 0 \), the number of infinite components in the graph \( G = G_{\text{sec}}' \) is either almost surely 0, or almost surely 1.

Proof. In this proof we may assume that \( \lambda > \lambda_c \), so that there is at least one infinite component, almost surely.

Suppose that, almost surely, \( G \) has infinitely many infinite components. Then there exists an \( r > 0 \) such that, with probability at least 0.99, at least three infinite components intersect \( B(O, r) \). If \( r \) is large enough, one can also show, by the argument in the proof of Theorem 2, that, based on \( \mathcal{P} \cap B(0, 3r)^C \), with probability at least 0.9, there can be no edge from \( \mathcal{P} \cap B(0, 4r)^C \) to \( \mathcal{P} \cap B(0, 3r) \) in \( G \). In other words, the red points outside \( B(O, 3r) \) by themselves prevent an edge of \( G \) from crossing the annulus \( B(O, 4r) \setminus B(O, 3r) \). This also implies
that \( G \cap B(O, 4r)^C \) is unaffected by the red points inside \( B(O, 3r) \). Now let \( C_1, C_2 \) and \( C_3 \) be three of the infinite components intersecting \( B(0, r) \). First, remove all black points not in these components from inside \( B(O, 4r) \). Second, remove all the red points from \( B(O, 3r) \). The effect of this is that \( C_1, C_2 \), and \( C_3 \) merge into a single infinite component \( C \), while none of the other infinite components merge with \( C \). But, in the new configuration, which has positive probability of occurring (by the special coupling), \( T(x, 4r) \) occurs. This contradicts Lemma 21.

\[ \Box \]

5 Concluding Remarks

We have presented several methods to calculate bounds on five percolation thresholds in the Poisson secrecy graph. While the rigorous bounds are still rather loose, the high-confidence lower bounds derived here are much tighter.

Acknowledgments

The work of the second author was in part supported by the U.S. NSF (grants CCF 728763, CNS 1016742) and the DARPA/IPTO IT-MANET program (grant W911NF-07-1-0028).

References


