Percolation in the Secrecy Graph

Amites Sarkar
Department of Mathematics
Western Washington University
Bellingham, WA 98225, USA
Email: amites.sarkar@wwu.edu

Martin Haenggi
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556, USA
Email: mhaenggi@nd.edu

***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.**

I. 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 [5].

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.

II. Model

Our model is as follows. Let $\mathcal{P}$ and $\mathcal{P}'$ be independent Poisson processes, of intensities 1 and λ 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* $\vec{G}_{\rm sec}$, 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 [5], where the model was originally defined.

Our main aim in this paper is to study the critical value(s) of λ for various types of percolation in $\vec{G}_{\rm sec}$ 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 $\vec{G}_{\rm sec}$ have been obtained in [12] and [5] respectively. We summarize the results below.

Theorem 1: The outdegree distribution in $\vec{G}_{\rm sec}$ is geometric with mean $1/\lambda$, and the indegree distribution 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

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

The result follows. ∎

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

III. 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 below.) Since $\vec{G}_{\rm sec}$ 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 $G_{\rm sec}$ for the undirected graph obtained from $\vec{G}_{\rm sec}$ by removing the orientations of the edges and replacing any resulting double edges by single edges, and $G'_{\rm sec}$ for the undirected graph obtained from $\vec{G}_{\rm sec}$ by including only those edges xy for which both $\vec{xy} \in \vec{G}_{\rm sec}$ and $\vec{yx} \in \vec{G}_{\rm sec}$. We write **U** for the event that $G_{\rm sec}$ has an infinite component, **O** for the event that $\vec{G}_{\rm sec}$ has an infinite out-component, **I** for the the event that $\vec{G}_{\rm sec}$ has an infinite in-component, **S** for the event that $\vec{G}_{\rm sec}$ has an infinite strongly connected subgraph, and **B** for the event that $G'_{\rm sec}$ 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:

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

Let X denote any of $\mathbf{U}, \mathbf{O}, \mathbf{I}, \mathbf{S}$ or $\mathbf{B}$, and let $p_{\mathbf{X}}(\lambda, d) = \mathbb{P}(X)$.

Theorem 2: For all values of λ and d, and all choices of X, $p_{\mathbf{X}}(\lambda, d)$ is either 0 or 1.

Proof: Let E be the event that $\vec{G}_{\rm sec}$ has an infinite $\mathbf{X}$-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_ε from O that is not prohibited by $\mathcal{P}'$ from sending a directed edge to some vertex within K of the origin is less than ε. 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 ε by suitable choice of L. Note that this probability is taken over the restriction of $\mathcal{P} \cup \mathcal{P}'$ to $\mathbb{R}^d \setminus D(O, K)$.

Now, for each choice of $\mathbf{X}$, $\mathbf{X}$-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 $\vec{G}_{\rm sec}$ by removing all vertices of $\mathcal{P}$ inside $B(O, K_\varepsilon)$ and all edges incident with them. But, with probability $1 - \varepsilon$, taken over the restriction of $\mathcal{P} \cup \mathcal{P}'$ to $\mathbb{R}^d \setminus B(O, K)$, this does not depend on points within distance K of the origin. Since this holds for all $\varepsilon > 0$, 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. ■

Since, for a fixed instance of $\mathcal{P}$, adding points to $\mathcal{P}'$ can only remove edges from $\vec{G}_{\rm sec}$, the probability $p_{\mathbf{X}}(\lambda, d)$ is non-increasing in λ. Define the *critical intensity* $\lambda_{\mathbf{X},d}$ by the formula

$$\lambda_{\mathbf{X},d} = \inf\{\lambda : p_{\mathbf{X}}(\lambda, d) = 0\} = \sup\{\lambda : p_{\mathbf{X}}(\lambda, d) = 1\}$$

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

$$\lambda_{\mathbf{B}} \le \lambda_{\mathbf{S}} \le \min\{\lambda_{\mathbf{I}}, \lambda_{\mathbf{O}}\}, \qquad \max\{\lambda_{\mathbf{I}}, \lambda_{\mathbf{O}}\} \le \lambda_{\mathbf{U}}. \tag{2}$$

Our first aim is to provide bounds on $\lambda_{\mathbf{X}}$. While doing this, we survey various methods that have been used for other continuum percolation models. All of these are from [4], [8] and [11], on percolation in the Gilbert disc model, and from [2] and [7], on percolation in the k-nearest neighbour model.

A. Branching processes ([4], [7], [8], [11])

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 $\mathcal{P}$, 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 $\mathcal{P}$. First pick the points of $\mathcal{P}$ 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 $\mathrm{Po}(\pi r^2)$, 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 [4], Gilbert argues that if $\pi r^2 \le 1$, 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 $\alpha = (\frac{2}{3}\pi - \frac{\sqrt{3}}{2})r^2$, so we can compare with a branching process whose offspring size distribution is just $\mathrm{Po}(\pi - \alpha)r^2$. This leads to the improved lower bound of $\frac{\pi}{\pi-\alpha} \approx 1.642$, which was further improved to 2.184 by Hall [8] using multitype branching processes. In Hall's method, the type of a child is just the Euclidean distance to its parent: children of higher types are likely to have more descendants. We include a brief description of Hall's modification later.

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

Proposition 3: The probability $\theta_{\mathbf{O}}(\lambda)$ that O belongs to an infinite out-component in the secrecy graph satisfies

$$\theta_{\mathbf{O}}(\lambda) \leq 1 - \lambda.$$

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 disc around each point in turn (according to the order). For each black point x, there are two possibilities. First, the disc corresponding to x might encounter a red point which has already been encountered. If not, the disc 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 disc) 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 λ 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 λ, and so $\theta_{\mathbf{O}}(\lambda) \leq 1 - \lambda$. ∎

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 [7] and [11], 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: $\lambda_{\mathbf{O},d} \to 1$ as $d \to \infty$.

Proof: (Sketch) The proof of [7] goes through, except that we compare with a much simpler branching process, namely the one where the offspring size distribution is geometric with mean $1/\lambda$, as above. There is no need to have two types of offspring.

The first step is to show that, over finitely many (say k) generations, the number of descendants of a black point p in its cluster tends to the number of descendants of p in the above branching process, as $d \to \infty$. This follows since, as $d \to \infty$, the edges in the cluster have asymptotically identical lengths, and are asymptotically orthogonal. Consequently, the first possibility in the above proof, where an expanding disc is stopped by a previously encountered red point, occurs with probability tending to zero over the first k generations. The extension to infinitely many generations is accomplished by truncation and comparison with oriented site percolation, as in [7] and [11]. ∎

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 $d \to \infty$.

B. Lattice percolation ([4], [7], [8], [13], [14])

Two variants of the basic method, applied to the Gilbert model, are described in Gilbert's original paper [4]. 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 $\mathcal{P}$ 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 $r/\sqrt{13}$, and make the state of a hexagon open iff it contains a point of $\mathcal{P}$, 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 πr_c^2 of about 17.4 and 10.9, respectively. The latter value was improved to 10.588 by Hall [8] using "rounded hexagons".

Häggström and Meester [7] used this method to show that, for fixed d, percolation occurs in the k-nearest neighbour model for sufficiently large k. Pinto and Win [13] (see [14] for more details) applied it to show that percolation occurs in all versions of the secrecy graph model when λ 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 $\lambda_{\mathbf{U}}$, also using lattice percolation. Their method is to tile the plane with regular hexagons, each of side length δ. 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 $G_{\rm sec}$ cannot cross a closed circuit, and so percolation will not occur in $G_{\rm sec}$ 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 λ, we maximize $g(\lambda, \delta)$ by setting

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

so the smallest value of λ 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 $\lambda_{\mathbf{U}}$. The last equation can be solved numerically to yield the bound $\lambda_{\mathbf{U}} \leq 40.9$. The method can easily be modified to give bounds for the other $\lambda_{\mathbf{X}}$, 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 λ is sufficiently large.

C. 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 πr_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. However, we will use a slight modification of it to give a lower bound for $\lambda_{\mathbf{B}}$, the percolation threshold for the graph $G'_{\rm sec}$ consisting of bidirectional edges.

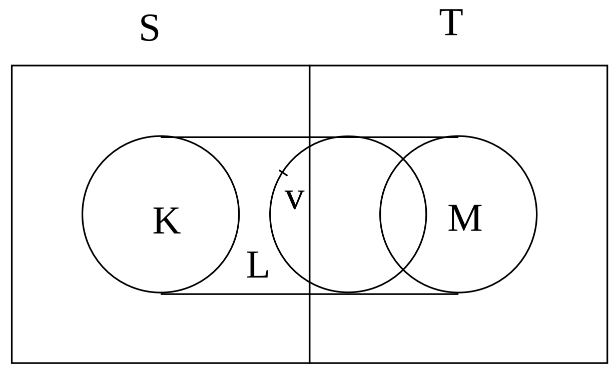

Fig. 1. The rolling ball method

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* $E_{\mathbf{B},S,T}$ 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 $G'_{\rm sec}$, 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 $[Ri, R(i+1)] \times [Rj, R(j+1)]$ 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 $E_{\mathbf{B},S,T}$ and $E_{\mathbf{B},T,S}$ 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 it is known (see [2]) that the critical probability for any 1-independent model is at most 0.8639, if we can show that, for some r, s, λ,

$$\mathbb{P}(E_{\mathbf{B},S,T}) \geq 0.9347$$

it will follow that

$$\mathbb{P}(E_{\mathbf{B},S,T} \cap E_{\mathbf{B},T,S}) \geq 0.8639$$

by symmetry, and hence we will have shown that $\lambda_{\mathbf{B}} \geq \lambda$.

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 $E'_{\mathbf{B},S,T}$ to be the event that for every black point $v \in S \cup L$, there is a black point u such that i) $\|u - v\| \leq s$ and ii) $u \in D_v$, where D_v is the disc of radius r inside $K \cup L \cup M$ 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, and $H_{S,T}$ be the event that there is no red point in $S \cup T$, then we have (see [2] for background)

$$E'_{\mathbf{B},S,T} \cap F_S \cap H_{S,T} \subset E_{\mathbf{B},S,T}$$

and so

$$E^C_{\mathbf{B},S,T} \subset (E'_{\mathbf{B},S,T})^C \cup F^C_S \cup H^C_{S,T}$$

so that

$$\mathbb{P}(E^C_{\mathbf{B},S,T}) \leq e^{-\pi r^2} + 1 - e^{-8\lambda(r+s)^2} + 2r(2r+2s)p_{\mathbf{B},r,s}$$

where $p_{\mathbf{B},r,s}$ is the probability that i) or ii) fails for some fixed v, which is just $e^{-|D_v \cap B(v,s)|}$, so that finally

$$\begin{aligned}\mathbb{P}(E^C_{\mathbf{B},S,T}) &\leq e^{-\pi r^2}+1-e^{-8\lambda(r+s)^2}+2r(2r+2s)e^{-|D_v \cap B(v,s)|} \\ &= f(r,s,\lambda)\end{aligned}$$

which can be minimized over various values of r and s.

A computer calculation shows that when $\lambda = 0.000332$, the minimum of $f(r,s,\lambda)$ is 0.06514, attained at $r = 1.76$ and $s = 2.97$, and consequently, we have the following theorem.

Theorem 5: $\lambda_{\mathbf{B}} \geq 0.000332$.

D. 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, and 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 λ, which we wish to show is a lower bound on one of the percolation thresholds $\lambda_{\mathbf{U}}, \lambda_{\mathbf{O}}$ or $\lambda_{\mathbf{B}}$, we choose r and s as above. Then we generate a random instance of $\mathcal{P} \cup \mathcal{P}'$ 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 $G_{\text{sec}}, \vec{G}_{\text{sec}}$ or G'_{sec} for the cases $\mathbf{X} = \mathbf{U}, \mathbf{O}, \mathbf{B}$) to more than half the black points in M, regardless of the state of $\mathcal{P} \cup \mathcal{P}'$ 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 $\mathcal{P} \cup \mathcal{P}'$ outside $S \cup T$. If these conditions hold with probability at least 0.8639, then percolation occurs.

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 probability of success was less than 0.8639. In all cases p was less that 10^{-50}. It turns out that the method for the $\mathbf{X} = \mathbf{O}$ case actually applies to the cases $\mathbf{X} = \mathbf{S}$ and $\mathbf{X} = \mathbf{I}$ as well, and the results obtained are as follows.

Proposition 6: With high confidence, $\lambda_{\mathbf{B}} \geq 0.08, \lambda_{\mathbf{O}} \geq 0.1, \lambda_{\mathbf{I}} \geq 0.1, \lambda_{\mathbf{S}} \geq 0.1$ and $\lambda_{\mathbf{U}} \geq 0.18$.
Corresponding high confidence upper bounds will appear in a forthcoming paper.

IV. Uniqueness of the infinite cluster

Uniqueness of the infinite cluster above the percolation threshold was proved by Harris [9] for bond percolation in $\mathbb{Z}^2$, by Aizenman, Kesten and Newman [1] for connected, transitive and amenable graphs, by Meester and Roy [10] for the Gilbert model, and by Häggström and Meester [7] for the k-nearest neighbour model. The last two results were obtained by modifying a very short and elegant argument of Burton and Keane [3], 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 [7], and so we have the following result.

Theorem 7: For all values of d and for $\mathbf{X} = \mathbf{U}, \mathbf{B}$, if $\lambda < \lambda_{\mathbf{X},d}$, there is exactly one infinite $\mathbf{X}$-component in the secrecy graph.

Proof: (Sketch) Following the account in the survey paper by Häggström and Jonasson [6], we just outline the basic steps.

The first step is to show that, below the percolation threshold, the number of infinite components is almost surely (a.s.) constant (possibly ∞). For example, if the constant is 5, then the probability of getting exactly 5 infinite components is 1. This follows by ergodicity, as for all the other models. One then rules out the possibility that the constant is anything other than 1 or ∞ using the "local modifier". The idea is that any secrecy graph containing 5 components which intersect a large ball can be locally modified so that these components join up. In the case of the secrecy graph the local modifier is particularly simple. Let N be the number of infinite components, and suppose that, for some $n \in \{2, 3 \ldots\}$, $\mathbb{P}(N = n) = 1$. Then there exists some r such that, with positive probability, $D(0,r)$ intersects all n infinite components. Remove all the red points in $D(0,3r)$. In the "local coupling" described in [7], such a new configuration has positive probability (conditional on the original configuration). But, in the new configuration, all n components have joined up, so there is only one infinite component. Consequently, $\mathbb{P}(N = 1) > 0$, contradicting the fact that the number of infinite components is a.s. constant.

The final step is to rule out the possibility that, above the threshold, there are infinitely many infinite components with probability 1. For this, the analogue of Lemma 4.2 of [7] goes through, and the construction in the above paragraph can be used to complete the argument, using the local modifier to produce, with positive probability, a forbidden "trifurcation" from any configuration where three infinite components intersect some ball. Details will appear in a forthcoming paper. ■

V. 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 CNS 04-47869, CCF 728763) and the DARPA/IPTO IT-MANET program (grant W911NF-07-1-0028).

REFERENCES

[1] M. Aizenman, H. Kesten and C.M. Newman, Uniqueness of the infinite cluster and continuity of connectivity functions for short- and long-range percolation, *Comm. Math. Phys.* **111** (1987), 505–532.

[2] P. Balister and B. Bollobás, Percolation in the k-nearest neighbor graph, submitted.

[3] R.M. Burton and M.S. Keane, Density and uniqueness in percolation, *Comm. Math. Phys.* **121** (1989), 501-505.

[4] E.N. Gilbert, Random plane networks, *Journal of the Society for Industrial and Applied Mathematics* **9** (1961), 533–543.

[5] M. Haenggi, The secrecy graph and some of its properties, *2008 IEEE International Symposium on Information Theory (ISIT'08)*, Toronto, Canada, 2008.

[6] O. Häggström and J. Jonasson, Uniqueness and non-uniqueness in percolation theory, *Probability Surveys* **3** (2006), 289–344.

[7] O. Häggström and R. Meester, Nearest neighbor and hard sphere models in continuum percolation, *Random Structures and Algorithms* **9** (1996), 295–315.

[8] P. Hall, On continuum percolation, *Annals of Probability* **13** (1985), 1250–1266.

[9] T.E. Harris, A lower bound for the critical probability in a certain percolation process, *Proc. Cam. Phil. Soc.* **56** (1960), 13–20.

[10] R.W.J. Meester and R. Roy, Uniqueness of unbounded occupied and vacant compenents in Boolean models, *Annals of Applied Probability* **4** (1994), 933-951.

[11] M.D. Penrose, Continuum percolation and Euclidean minimal spanning trees in high dimensions, *Annals of Applied Probability* **6** (1996), 528–544.

[12] P.C. Pinto, J. Barros and M.Z. Win, Physical-layer security in stochastic wireless networks, *Proceedings of the 11th IEEE Singapore International Conference on Communication Systems*, 2008.

[13] P.C. Pinto and M.Z. Win, Continuum percolation in the intrinsically secure communications graph, posted on the arXiv 22 July 2010.

[14] P.C. Pinto and M.Z. Win, Percolation and connectivity in the intrinsically secure communications graph, posted on the arXiv 24 August 2010.