Secrecy coverage in two dimensions

Amites Sarkar*

January 12, 2013

Abstract

Let $\mathcal{P}$ and $\mathcal{P}'$ be independent Poisson processes, of intensities 1 and λ respectively, in $\mathbb{R}^2$. Place an open disc $D(p, r_p)$ of radius r_p around each point $p \in \mathcal{P}$, where r_p is maximal so that $D(p, r_p) \cap \mathcal{P}' = \emptyset$. We thus obtain a random set $\mathcal{A}_\lambda \subset \mathbb{R}^2$ which is the union of discs centered at the points of $\mathcal{P}$. Now let $B_n \subset \mathbb{R}^2$ be a fixed disc of area n, and set $\mathcal{A}_\lambda(B_n) = \mathcal{A}_\lambda \cap B_n$. Write $B_\lambda(n)$ for the event that $\mathcal{A}_\lambda(B_n)$ covers B_n (except for the points of $\mathcal{P}'$), and set $p_\lambda(n) = \mathbb{P}(B_\lambda(n))$. Extending results in [7], we show that if $\lambda^3 n \log n \to \infty$, then $p_\lambda(n) \to 0$, while if $\lambda^3 n \log n (\log \log n)^2 \to 0$, then $p_\lambda(n) \to 1$.

1 Introduction

Place discs of radius r in $\mathbb{R}^2$ so that their centers form a Poisson process of intensity 1, and let $B(n) \subset \mathbb{R}^2$ be a disc of area $n \gg r^2$. What is the probability that $B(n)$ is covered by the small discs? This question, inspired by biology [6], has a long history, and many detailed results are known about it [3, 5]. For instance, writing

$$\pi r^2 = \log n + \log \log n + t,$$

Svante Janson proved in 1986 [5] that coverage occurs with probability asymptotically $e^{e^{-t}}$, as $n \to \infty$. One approach to this result [1, 2] uses the fact that the obstructions to coverage are small uncovered regions, which essentially form their own Poisson process, of intensity e^{-t}. Although these uncovered regions may be of different shapes, they are all roughly the same size (with probability tending to one). Here we study a related natural coverage process, where there are many different potential obstructions of many different sizes.

To define the process, let $\mathcal{P}$ and $\mathcal{P}'$ be independent Poisson processes, of intensities 1 and λ respectively, in $\mathbb{R}^2$. We will call the points of $\mathcal{P}$ *black points* and the points of $\mathcal{P}'$ *red points*. Place an open disc $D(p, r_p)$ of radius r_p around each black point $p \in \mathcal{P}$, where r_p is maximal so that $D(p, r_p) \cap \mathcal{P}' = \emptyset$. In other words, r_p is the distance from the black point p to the nearest red point $p' \in \mathcal{P}'$

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

to p. p' is almost surely unique, and we will refer to it as the *stopping point* of the disc centered at p, or of p itself. We thus obtain a random set $\mathcal{A}_\lambda \subset \mathbb{R}^2$ which is the union of discs centered at the points of $\mathcal{P}$. Now let $B_n \subset \mathbb{R}^2$ be a fixed disc of area n, and set $\mathcal{A}_\lambda(B_n) = \mathcal{A}_\lambda \cap B_n$. Write $B_\lambda(n)$ for the event that $\mathcal{A}_\lambda(B_n)$ covers B_n (except for the points of $\mathcal{P}'$), and set $p_\lambda(n) = \mathbb{P}(B_\lambda(n))$. Since adding red points makes coverage less likely, $p_\lambda(n)$ is a non-increasing function of λ, for fixed n. In addition, $p_\lambda(n)$ is non-increasing in n, with λ fixed, because increasing n corresponds to examining the random set A_λ over a larger area.

This model, based on the *secrecy graph* [4], was inspired by the issue of security in wireless networks, and was studied in [7]. Our ultimate goal is to determine $p_\lambda(n)$ asymptotically. In this paper, we refine the results in [7] to provide a new condition under which $p_\lambda(n)$ tends to zero, and a corresponding new condition under which $p_\lambda(n)$ tends to one. These can be thought of as improved upper and lower bounds, respectively, on the value of λ such that $p_\lambda(n) = 1/2$, and will be referred to as such in what follows. Due to the divergence of a certain integral, the proofs strongly suggest that there are obstructions on a range of scales, and we hope to investigate this further in the future.

2 Upper bound

Theorem 1. *If $\lambda^3 n \log n \to \infty$, then $p_\lambda(n) \to 0$.*

Proof. Our strategy will be to show that, under the hypothesis, the expected number of *good configurations* (defined below) tends to infinity. A routine application of the second moment method then shows that a good configuration occurs with high probability (probability tending to one). Finally, we show that a good configuration results in an uncovered region of B_n.

First, therefore, we define a good configuration. Such a configuration consists of an ordered triple (p_1, p_2, p_3) of red points in B_n. p_1 and p_2 must lie at distance t, where $n^{-1/12} < t < 1$. p_3 must lie at distance between $50/t$ and $100/t$ of p_1, in such a way that the angle $p_3p_1p_2$ is between $\pi/4$ and $3\pi/4$. (The choice of these angles is somewhat arbitrary: all we need is that the angle $p_3p_1p_2$ is bounded away from 0 and π.) Write ℓ_{ij} for the perpendicular bisector of p_ip_j, and S for the bi-infinite strip of width $||p_1 - p_2||$ centered on ℓ_{12}. For ease of explanation, suppose that the segment p_1p_2 is horizontal, so that S is vertical, and that p_3 lies above the line through p_1 and p_2. ℓ_{13} and ℓ_{23} intersect the boundary ∂S of S in four points; suppose that the highest of these lies at height $h \leq 110/t$ above p_1p_2. Write $R \subset S$ for the rectangle with base p_1p_2 and height $2h$ (containing all four intersections above), and $R' \subset S$ for its reflection in p_1p_2. A good configuration must also have no black points in the rectangular region $R \cup R'$. Note that the area of $R \cup R'$ is at most 440. Consequently, writing X for the number of good configurations, there exist absolute constants C and C' such that

$$\mathbb{E}(X) \sim C \int_{n^{-1/12}}^{1} \lambda n \cdot \lambda t^{-2} \cdot \lambda t \, dt = C' \lambda^3 n \log n \to \infty.$$

Second, we show that we can apply the second moment method to prove that, with high probability, $X \geq 1$. For this to work, we require an *upper* bound on λ; it will suffice to assume $\lambda^3 n \to 0$. Since $p_\lambda(n)$ is decreasing in λ, if we can prove that $p_\lambda(n) \to 0$ under the more restrictive hypotheses, the full result will follow. Tessellate $B(n)$ with squares of side length $n^{1/6}$, and color a square black if both of its "coordinates" are even. (Thus one out of every four squares is black.) We will only consider the black squares, which we label $S_1, S_2, \ldots, S_N$. Let the *apex* of a good configuration be the point furthest from the opposite side (p_3, in the above notation), and write X_i for the number of good configurations with apex in S_i. With high probability, each X_i will be either zero or one. Moreover, since the maximum diameter of a good configuration is $O(n^{1/12})$ by construction, the X_i are independent. Let $X' = \sum X_i$. Then $\mathbb{E}(X') \to \infty$ as above, and since

$$\mathbb{P}(X_i \geq 1) = O(\log n / n^{2/3}) \to 0,$$

it follows that

$$\mathrm{Var}(X') = \sum \mathrm{Var}(X_i) \sim \sum \mathbb{E}(X_i) = \mathbb{E}(X'),$$

and so

$$\mathbb{P}(X = 0) \leq \mathbb{P}(X' = 0) \leq \frac{\mathrm{Var}(X')}{\mathbb{E}(X')^2} \sim \frac{1}{\mathbb{E}(X')} \to 0.$$

Finally, we explain why the presence of a good configuration prohibits full coverage. As above, suppose that p_1p_2 is horizontal, and that p_3, and hence ℓ_{13} and ℓ_{23}, lie above p_1p_2. The idea is that part of ℓ_{12} lying just above p_1p_2 will be uncovered. Write m_0 for the midpoint of p_1p_2, and m_s for the point of ℓ_{12} at height s above p_1p_2. Any black points lying in S and above p_1p_2 are much closer to p_3 than to p_1 or p_2, and so their corresponding discs cannot cover m_0 or m_s, for $s \sim C/t$. Write q_2 for the intersection of ℓ_{13} with ∂S lying above p_1, q_1 for the intersection of ℓ_{23} with ∂S lying above p_2, and q_3 for the midpoint of the opposite side of R' from p_1p_2. The q_i are the best locations to place black points for the purposes of covering points m_s, for small s. However, even their corresponding black discs fail to cover $m_{s'}$, for suitable s'. Specifically, for $i = 1, 2$, write

$$D_i = D(q_i, r_{q_i}) = D(q_i, ||q_i - p_{2-i}||) = D(q_i, ||q_i - p_3||),$$

and

$$D_3 = D(q_3, r_{q_3}) = D(q_3, ||q_3 - p_1||) = D(q_3, ||q_3 - p_2||).$$

If the distance of q_i from p_1p_2 is c_i/t, then the heights of D_1 and D_2 above m_0 are asymptotically $t^3/8c_i$, and D_3 only covers m_s for $s < t^3/8c_3$ (asymptotically). However, by construction,

$$c_3 \geq \tfrac{3}{2} \max\{c_1, c_2\},$$

so the point $m_{s'}$, for $s' = t^3/7c_3$, will be uncovered by $D_1 \cup D_2 \cup D_3$, and hence by A_λ. □

3 Lower bound

We require a lemma from [7]. This relates to the one-dimensional version of the problem, where we are covering an interval of length n with small intervals centered at black points, which in turn are stopped by red points. In [7], the lemma was used to show that, in one dimension, if $\lambda \to \infty$ and also $\lambda n \to \infty$, then (with obvious notation)

$$p^1_\lambda(n) \sim e^{-4n\lambda^2}. \tag{1}$$

The lemma itself concerns an interval L of length ℓ between two consecutive red points.

Lemma 2. *Let L be an interval of length ℓ between two consecutive red points. Let $\mathcal{P}$ be a Poisson process of intensity 1 in L, and grow an interval I_p centered at each point p of $\mathcal{P}$ until it hits one of the red points at the endpoints of L. Then*

$$\mathbb{P}\left(L \text{ is covered by } \bigcup_{p\in\mathcal{P}} I_p\right) = 1 - e^{-\ell/2}(1+\ell/2).$$

Proof. Let m be the midpoint of L, let x be the distance of the closest black point to m lying on the left of m, and let y be the distance of the closest black point to m lying on the right of m. Then coverage of L is determined solely by x and y. Indeed, coverage occurs if and only if $x + y \le \ell/2$. Now $x + y$ has the gamma distribution with density function te^{-t}, and consequently

$$\mathbb{P}\left(L \text{ is covered by } \bigcup_{p\in\mathcal{P}} I_p\right) = \int_0^{\ell/2} te^{-t}\,dt = 1 - e^{-\ell/2}(1+\ell/2),$$

as required. □

The deduction of (1) from Lemma 2 is straightforward. Firstly, the unconditional probability that the interval between two consecutive red points is covered, obtained by integrating the above probability against the density function of ℓ, is $(1+2\lambda)^{-2} \sim 1-4\lambda$. Second, since there are asymptotically $n\lambda \to \infty$ intervals between consecutive red points, and coverage fails independently in each one with probability asymptotically $4\lambda \to 0$, the number of failures is approximately Poisson with mean $4n\lambda^2$, and (1) follows.

We return to the original two-dimensional problem, for which we have the following bound.

Theorem 3. *If $\lambda^3 n \log n(\log\log n)^2 \to 0$, then $p_\lambda(n) \to 1$.*

Proof. This is a refinement of the proof of Theorem 7 from [7]. Suppose that $n \to \infty$ and also that $\lambda^3 n \log n(\log\log n)^2 \to 0$. First, we show that we need only worry about coverage of parts of $B(n)$ which are close (within distance $\sqrt{8\log n}$) to a red point. To do this, we tessellate $B(n)$ with squares of side length $r = \sqrt{\log n}$. The probability that any small square of the tessellation contains no black point is $e^{-\log n} = n^{-1}$. Since there are $\sim n/\log n$ such squares, the expected number of them containing no black points is asymptotically $1/\log n \to 0$. Consequently, with high probability, every small square contains a black point. Now fix a small square S. If no point of S is within distance $\sqrt{2\log n}$ of a red point, and if S contains a black point, then all of S will be covered by $\mathcal{A}_\lambda$. Therefore, with high probability, any point of $B(n)$ at distance more than $\sqrt{8\log n}$ from all red points will be covered by $\mathcal{A}_\lambda$, and we may assume this from now on.

It remains to show that the regions of $B(n)$ within distance $\sqrt{8\log n}$ from a red point are covered by A_λ. Color such regions yellow. In order to facilitate a division into cases, let us construct a graph $G = G(n, \mathcal{P}')$ on the red points by joining two red points if they lie within distance $R = R(n) = \sqrt{128\log n}$ of each other. (Such a graph is usually called a *random geometric graph.*) A routine calculation shows that, with high probability, the connected components of G consist of $o(n^{2/3}(\log n)^{-1/3})$ isolated vertices, $o(n^{1/3}(\log n)^{1/3})$ edges, $o(\log n)$ triangles, and $o(\log n)$ paths of length 2 (i.e., paths with 2 edges). We deal with each of these in turn; it will be convenient to consider a path of length 2 as a triangle, even though one of its edges is "long".

Isolated vertices. Consider the circles of radii $\sqrt{8\log n}$ and $\sqrt{32\log n}$ around each isolated red point, and divide the annulus between these circles into 6 equal "sectors", each of area $4\pi\log n$. With high probability, there is a black point inside each sector, and this black point is closer to the isolated vertex than to any other red point. But then the yellow region surrounding the isolated vertex is covered by A_λ.

Edges. For a fixed red edge $e = p_1p_2$, where we may assume $p_1 = (0,0)$ and $p_2 = (t,0)$, consider the circles of radii $\sqrt{8\log n}$ and $\sqrt{32\log n}$ around p_1 and p_2. Divide each half-annulus, between two concentric circles and lying outside the "critical strip" $S = [0,t] \times \mathbb{R}$, into 3 equal sectors, each of area $4\pi\log n$. With high probability, there is a black point inside each sector, and this black point is closer to the associated p_i than to any other red point. Thus the yellow regions outside S are covered by A_λ. However, coverage of the yellow regions inside the critical strip S is not guaranteed. Indeed, from the upper bound argument in the previous section, such coverage is threatened by the presence of red points at distance $\sim C/t$ from e. G contains edges almost as short as $n^{-1/6}$, so such points may lie almost as far as $n^{1/6}$ from e, almost as much as the typical distance between red points.

In connection with e, consider the region

$$R_1^+ = [0,t] \times [\sqrt{2\log n}, \sqrt{2\log n} + \log n/t] \subset S,$$

and its reflection in the x-axis

$$R_1^- = [0,t] \times [-\sqrt{2\log n}, -\sqrt{2\log n} - \log n/t] \subset S,$$

together with the much smaller regions

$$R_2^+ = [0,t] \times [\sqrt{2\log n}, \sqrt{2\log n} + 5\log\log n/t] \subset S,$$

and

$$R_2^- = [0,t] \times [-\sqrt{2\log n}, -\sqrt{2\log n} - 5\log\log n/t] \subset S.$$

R_1^+ and R_1^- each have area $\log n$, while R_2^+ and R_2^- each have area $5\log\log n$. Call en edge *bad* if some point of $R_1^+ \cup R_1^-$ is closer to a third red point than to p_1 or p_2, *very bad* if some point of $R_2^+ \cup R_2^-$ is closer to a third red point than to p_1 or p_2, and *good* otherwise. Write B for the number of bad edges, and V for the number of very bad edges. For an edge to be bad, there must be a third red point p_3 within distance $C\log n/t$ of e, and, for an edge to be very bad, p_3 must lie within distance $C\log\log n/t$ of e, for some absolute constant C. (Note that, since e is an isolated edge, such a p_3 must lie at distance at least $\sqrt{128\log n}$ from both p_1 and p_2.) Moreover, the expected number of edges of length less than $n^{-1/6}$ is $O(\lambda n \cdot \lambda n^{-1/3}) = o(1)$, so, with high probability, there are no such edges. Consequently,

$$\mathbb{E}(B) \le C' \int_{n^{-1/6}}^{\sqrt{128\log n}} \lambda n \cdot \lambda(\log n)^2 t^{-2} \cdot \lambda t \, dt \le C''\lambda^3 n(\log n)^3 = o(\log n)^2,$$

and

$$\mathbb{E}(V) \le C' \int_{n^{-1/6}}^{\sqrt{128\log n}} \lambda n \cdot \lambda(\log\log n)^2 t^{-2} \cdot \lambda t \, dt \le C''\lambda^3 n \log n(\log\log n)^2 \to 0,$$

for some absolute constants C' and C''. Thus, with high probability, there are no very bad edges, and in fact most edges are good.

The idea behind the construction of R_1^+, R_1^-, R_2^+ and R_2^- is that, in the absence of very bad edges, we may use the black points in R_1^+ and R_1^- to cover the yellow regions close to good edges, and those in R_2^+ and R_2^- to cover the yellow regions close to bad edges. For the purposes of covering such yellow regions in the critical strip S, only the x-coordinates of black points in R_1^+, R_1^-, R_2^+ and R_2^- matter. (The reason behind the $\sqrt{2\log n}$ term in the definitions of these rectangles is so that coverage of the entire yellow region follows from coverage of e from both sides.) Considering the good edges first, we project the black points in R_1^+ and R_1^- to the edge $e = [0,t]$, where they form two separate Poisson processes, each of intensity $\log n/t$, on an interval of length t. For coverage purposes, these are equivalent to two processes of intensity 1 on an interval of length $\log n$, and so we see from the lemma that full coverage of the relevant yellow regions fails with probability at most

$$2e^{-\log n/2}(1 + \log n/2)) < \frac{2\log n}{\sqrt{n}}.$$

Since we only expect $o(n^{1/3}(\log n)^{1/3})$ edges in G, the yellow regions close to good edges are covered with high probability. Turning to the bad edges, and performing a corresponding projection of the black points in R_2^+ and R_2^-, we see that this time coverage fails with probability at most

$$2e^{-5\log\log n/2}(1 + 5\log\log n/2)) < \frac{10\log\log n}{(\log n)^{5/2}},$$

and, since we only expect $o((\log n)^2)$ bad edges in G, the yellow regions close to bad edges are also covered with high probability. Consequently, with high probability, all yellow regions near all edges of G inside $B(n)$ are fully covered.

Triangles. We expect $o((\log n)^2)$ of these in G. The expected number of them with one edge shorter than $100 \log\log n$ is $O(\lambda^3 n(\log n)(\log\log n)^2) = o(1)$, so we may assume that each edge in each such triangle T is longer than $100 \log\log n$. For simplicity, we deal with the case where each angle of T is less than $80°$, the other cases being, if anything, easier. Let the vertices of T be p_1, p_2 and p_3, and let the circumcenter of T be c. Let Q_i be the rectangle with base $p_{i+1}p_{i+2}$, whose opposite side s from $p_{i+1}p_{i+2}$ contains c (here, subscripts are taken modulo 3), and let Q'_i be the "top half" of Q_i, whose base is halfway from $p_{i+1}p_{i+2}$ to s, and whose opposite side still contains c. Projecting the $\Omega((\log\log n)^2)$ black points in Q'_i to $p_{i+1}p_{i+2}$ as before, we see that the interior of T is covered by A_λ with probability $1 - o((\log n)^{-2})$, so that the interiors of all such triangles are covered with high probability. The exteriors of the triangles are also covered with high probability (this can be seen using such "sectors" as were used in the case of isolated vertices).

Consequently, with high probability, A_λ covers all yellow regions in $B(n)$. Thus, also with high probability, $B(n)$ itself is covered. □

I suspect that the lower bound is closer to the truth.

References

[1] Balister, P., Bollobás, B. and Sarkar, A., Percolation, connectivity, coverage and colouring of random geometric graphs, Handbook of Large-Scale Random Networks, Springer (2009), 117–142.

[2] Balister, P., Bollobás, B., Sarkar, A. and Walters, M., Sentry selection in wireless networks, *Advances in Applied Probability* **42** (2010), 1–25.

[3] E.N. Gilbert, The probability of covering a sphere with N circular caps, *Biometrika* **56** (1965), 323–330.

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

[5] S. Janson, Random coverings in several dimensions, *Acta Mathematica* **156** (1986), 83–118.

[6] P.A.P. Moran and S. Fazekas de St Groth, Random circles on a sphere, *Biometrika* **49** (1962), 389–396.

[7] A. Sarkar and M. Haenggi, Secrecy coverage, *Internet Mathematics*, to appear.