Western Washington University
Western CEDAR

Mathematics | College of Science and Engineering

2010

Secrecy Coverage (Conference Proceeding)

Amites Sarkar
Western Washington University, amites.sarkar@wwu.edu

Martin Haenggi

Follow this and additional works at: http://cedar.wwu.edu/math_facpubs

 Part of the Mathematics Commons

Recommended Citation
Sarkar, Amites and Haenggi, Martin, "Secrecy Coverage (Conference Proceeding)" (2010). *Mathematics*. 89.
http://cedar.wwu.edu/math_facpubs/89

This Conference Proceeding is brought to you for free and open access by the College of Science and Engineering at Western CEDAR. It has been accepted for inclusion in Mathematics by an authorized administrator of Western CEDAR. For more information, please contact westerncedar@wwu.edu.

Secrecy Coverage

Amites Sarkar
Department of Mathematics
Western Washington University
Bellingham, WA 98225, USA

Martin Haenggi
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556, USA

***Abstract*—Motivated by information-theoretic secrecy, geometric models for secrecy in wireless networks have begun to receive increased attention. The general question is how the presence of eavesdroppers affects the properties and performance of the network. Previously the focus has been mostly on connectivity. Here we study the impact of eavesdroppers on the coverage of a network of base stations. The problem we address is the following. Let base stations and eavesdroppers be distributed as stationary Poisson point processes in a disk of area n. If the coverage of each base station is limited by the distance to the nearest eavesdropper, what is the maximum density of eavesdroppers that can be accommodated while still achieving full coverage, asymptotically as $n \to \infty$?**

I. Introduction

A. Motivation and related work

While coverage problems have been studied for several decades from a purely mathematical perspective, they have recently begun to attract significant attention by the engineering and computer science communities due to the advent of wireless networks, in particular sensor networks. The standard problem formulation is the following. Place a number n of nodes randomly in a certain set $B \subset \mathbb{R}^d$ and equip each node with the capability of covering (sensing) a disk or sphere of radius r around itself. How large should n be to guarantee coverage of B with probability $1-\epsilon$? Or, if the area or volume of B is scaled in proportion to n, which $r(n)$ guarantees coverage with high probability as $n \to \infty$?

In the mathematical literature, one of the early and now classical coverage problems is the coverage of a sphere with circular caps introduced in [1] and solved in [2]. Extensions to k dimensions were considered by Hall in [3] and Janson in [4]. Hall later provided a detailed account of coverage processes in his book [5]. Many generalizations have been considered since, see, *e.g.*, [6], [7] for coverage problems in $\mathbb{R}^d$.

Here we focus on a coverage problem that is inspired by secrecy constraints. We assume an information-theoretic model for secrecy, in which a communication is secure from eavesdroppers if the intended receiver is closer to the transmitter than all eavesdroppers. Based on this model, the *secrecy graph*, a random geometric graph that only includes edges along which secure communication is possible was introduced and studied in [8]. [9] extended the analysis to more elaborate physical layer models, while [10] considered the effects of uncertainty in the eavesdroppers' locations. This line of work is based on graph models and focuses on connectivity. In contrast, there is no prior work on the related coverage problem, which is the theme of the present paper.

Base stations and eavesdroppers are distributed randomly on the plane, and the base stations can cover circular areas with radii determined by the distance to the nearest eavesdroppers. The question is what density of eavesdroppers can be accommodated while still guaranteeing that the entire area or volume of interest is covered securely? This would ensure that mobile stations could roam around everywhere and be reached securely by a base station. Hence the downlink is intrinsically secure, while the uplink (from the mobile to the base station) has to be secured by transmission of a one-time pad via the downlink.

B. Problem formulation

To make the problem concrete, we assume that the base stations and eavesdroppers form independent Poisson point processes of intensities 1 and λ, respectively, in $\mathbb{R}^d$. We will denote the process of base stations by $\mathcal{P}$ and call its points *black points*, and the process of eavesdroppers by $\mathcal{P}'$ and call its points *red points*. Now place an open ball $D(p, r_p)$ 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 $p' \in \mathcal{P}'$ to p. We thus obtain a random set $\mathcal{A}_\lambda^d \subset \mathbb{R}^d$ which is the union of balls centered at the points of $\mathcal{P}$. Fig. 1 shows a 2-dimensional example for $\lambda = 0.1$. Our aim is to study properties of $\mathcal{A}_\lambda^d$, in particular the covered volume fraction (Section 2) and the asymptotic conditions for complete coverage in one (Section 3) and two (Section 4) dimensions.

In two dimensions, the radius R of each disk is given by the nearest-neighbor distance, distributed as

$$f_R(x) = 2\pi x\lambda \exp(-\lambda\pi x^2)\,.$$

Note that this coverage problem is rather different from the case where the covering disks have *independent* radii drawn from f_R. The difference is that in our case, the disk radii of nearby nodes are strongly correlated, which leads to drastically different conditions for coverage compared with the independent case. Indeed, for the standard model with random independent disk radius, a disk of area n is covered a.s. if[1]

$$\pi\mathbb{E}(R^2) = (1+\varepsilon)\log n$$

[1]This condition is not the sharpest possible.

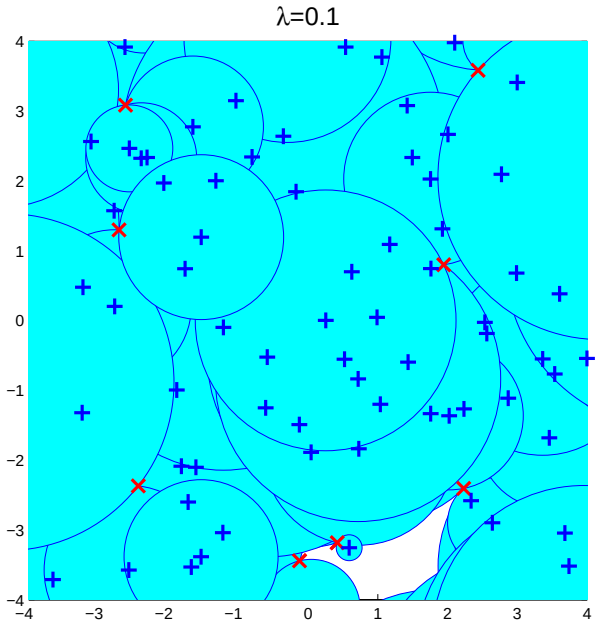


Fig. 1. Example for coverage of an 8×8 square for $\lambda = 0.1$. The base stations are marked by $+$, the eavesdroppers by $\times$, and the covered area is grey shaded.

for any $\varepsilon > 0$. Since $\mathbb{E}(R^2) = (\lambda\pi)^{-1}$, this translates to

$$\lambda = [(1+\varepsilon)\log n]^{-1},$$

which indicates that λ may decrease rather slowly with n while still achieving full coverage. In the secrecy case, however, λ has to decrease much faster, at a rate of about $n^{-1/3}$, as we will show.

II. Covered volume fraction

For $\lambda > 0$, write

$$C^d(\lambda) = \mathbb{P}(O \in \mathcal{A}_\lambda^d).$$

By stationarity of the model, $C^d(\lambda)$ can also be interpreted as the fraction of $\mathbb{R}^d$ which is covered by $\mathcal{A}_\lambda^d$, known as the *covered volume fraction*.

Theorem 1.

$$C^d(\lambda) = 1 - \mathbb{E}(e^{-V_d/\lambda}) = 1 - \int_0^\infty f_d(t) e^{-t/\lambda}\, dt,$$

where $f_d(t)$ is the probability density function for the volume V_d of a randomly chosen cell in a Voronoi tessellation associated with a unit intensity Poisson process in $\mathbb{R}^d$.

Proof: We rescale the model so that $\mathcal{P}$ and $\mathcal{P}'$ have intensities $1/\lambda$ and 1 respectively. This does not affect $C^d(\lambda)$. Now $O \notin \mathcal{A}_\lambda^d$ if and only if there are no points of $\mathcal{P}$ in the Voronoi cell C defined by $\mathcal{P}' \cup \{O\}$ containing O. If C has volume V, then $\mathbb{P}(C \cap \mathcal{P} = \emptyset) = e^{-V/\lambda}$. ∎

Corollary 2. *In one dimension, we have*

$$C^1(\lambda) = \frac{1+4\lambda}{(1+2\lambda)^2}.$$

Proof: Let $\mathcal{P}$ be a unit intensity Poisson process in $\mathbb{R}$. The distribution of the gap lengths between points of $\mathcal{P}$ has density e^{-t}, but the distribution of the length of the gap containing a fixed point, such as the origin O, has density te^{-t}. (This is known as the *waiting time paradox*.) Consequently, the density function for the length of the Voronoi cell defined by $\mathcal{P}$ containing the origin is $4te^{-2t}$, so that by Theorem 1

$$C^1(\lambda) = 1 - \int_0^\infty 4te^{-2t-t/\lambda}\, dt = \frac{1+4\lambda}{(1+2\lambda)^2}.$$

∎

Remark. This corollary can also be proved as follows. Let L be the event that the origin O is covered by points of $\mathcal{P}$ lying only to the left of O, and let R be the event that O is covered by points of $\mathcal{P}$ lying only to the right of O. Then L and R are independent, and

$$\begin{aligned} C^1(\lambda) &= 1 - (1-\mathbb{P}(L))(1-\mathbb{P}(R)) \\ &= 1 - (1-\mathbb{P}(R))^2 \\ &= 2\mathbb{P}(R) - \mathbb{P}(R)^2, \end{aligned}$$

by symmetry. Now R occurs if and only if the closest black point to the right of O is at distance t, and there are no red points in the interval $[0, 2t]$, for some $t > 0$. Thus

$$\mathbb{P}(R) = \int_0^\infty e^{-t} e^{-2\lambda t}\, dt = \frac{1}{2\lambda+1},$$

which gives the desired result.

III. Probability of total coverage in one dimension

In this and the next section, we study the following problem. With $\mathcal{P}, \mathcal{P}'$ and $\mathcal{A}_\lambda^d$ as before, let $B_n^d \subset \mathbb{R}^d$ be a fixed ball of volume n, and set $\mathcal{A}_\lambda^d(B_n^d) = \mathcal{A}_\lambda^d \cap B_n^d$. Write $B_\lambda^d(n)$ for the event that $\mathcal{A}_\lambda^d(B_n^d)$ covers B_n^d (except for the points of $\mathcal{P}'$), and set $p_\lambda^d(n) = \mathbb{P}(B_\lambda^d(n))$. Our principal goal is to estimate $p_\lambda^d(n)$ for arbitrary d.

Let us first consider the case $d = 1$. In this case, $I = B_n^1$ is simply an interval of length n, containing some black and red points. We place an interval centered at each black point of maximal length subject to containing no red points, and ask for the probability $p_\lambda^1(n) \to 0$ that I is covered by such intervals.

In the one-dimensional case, we have the following sharp result.

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

Proof: To simplify our analysis, let us suppose that $\mathcal{P}$ and $\mathcal{P}'$ are placed on a circle T of circumference n rather than an interval of length n: there is asymptotically no difference. Our strategy is to place the red points $\mathcal{P}'$ first, partitioning the circle T into $M \sim \mathrm{Po}(n\lambda)$ arcs A_i. Now place the black points $\mathcal{P}$. For each arc A_i, let C_i be the event that A_i is covered by the smaller arcs associated with the black points in A_i. The events C_i are independent, and this will enable us to estimate $p_\lambda^1(n)$.

Suppose A_i has length ℓ, and let m_i be the midpoint of A_i. Let x be the distance of the closest black point to m_i lying on the left of m_i, and let y be the distance of the closest black point to m_i lying on the right of m_i. Whether or not C_i occurs, i.e., whether or not A_i is covered by small arcs, is determined solely by x and y. In fact, it is easy to see that

- C_i occurs if and only if $x + y \leq \ell/2$.

Now $x + y$ has the gamma distribution with density function te^{-t}, and consequently

$$\begin{aligned}\mathbb{P}(C_i \mid A_i \text{ has length } \ell) &= \int_0^{\ell/2} te^{-t}\,dt \\ &= 1 - e^{-\ell/2}(1+\ell/2). \qquad (1)\end{aligned}$$

Further, since the black and red points are independent, and the length ℓ has an exponential distribution with density function $\lambda e^{-\lambda t}$, we have

$$\begin{aligned}\mathbb{P}(C_i) &= \int_0^\infty \lambda e^{-\lambda\ell}(1 - e^{-\ell/2}(1+\ell/2))\,d\ell \\ &= \frac{1}{(1+2\lambda)^2}.\end{aligned}$$

Conditioning on the number of arcs M changes the distribution of the lengths of the A_i, but the difference is asymptotically negligible. Consequently, as $n \to \infty$ with $\lambda \to 0$ but $\lambda n \to \infty$,

$$\begin{aligned}p_\lambda^1(n) &\sim \sum_{m=0}^\infty \mathbb{P}(M=m)(2\lambda+1)^{-2m} \\ &= e^{-4n\lambda^2(\lambda+1)/(2\lambda+1)^2} \\ &\sim e^{-4n\lambda^2}.\end{aligned}$$

So, if $n\lambda^2 \to 0$, $p_\lambda^1(n) \to 1$, and if $n\lambda^2 \to \infty$, $p_\lambda^1(n) \to 0$, as postulated. ∎

IV. Probability of coverage in two dimensions

A. Analysis

A natural step is to generalize these results to arbitrary d. Simple heuristics would suggest that if $\lambda^{d+1}n \to 0$ then $p_\lambda^d(n) \to 1$, and if $\lambda^{d+1}n \to \infty$ then $p_\lambda^d(n) \to 0$. Unfortunately, attempts to generalize the above one-dimensional arguments run into difficulties, mainly due to the lack of an order structure in $\mathbb{R}^d$ for $d \geq 2$.

For the rest of the paper, we restrict attention to the case $d = 2$. It turns out to be useful to consider the *Gilbert disc model* on the red points $\mathcal{P}'$, with an appropriately chosen radius. This model is constructed by simply joining two points of $\mathcal{P}'$ if the distance between them is less than some specified threshold.

Theorem 4. *If $f(n) = \lambda^3 n \to \infty$, then $p_\lambda^2(n) \to 0$.*

Proof: Suppose that $n \to \infty$ and also that $\lambda^3 n \to \infty$. Let $R > 0$ be a large constant. Construct the Gilbert disc model $G = G_R(\mathcal{P}')$ on the red points $\mathcal{P}'$, with radius R (i.e., we join two points of $\mathcal{P}'$ if they are within distance R). Let T be the (random) number of triangles in G which lie entirely within B_n^2. Then, for some absolute constant C_1,

$$\begin{aligned}\mathbb{E}(T) &\sim C_1 e^{-\lambda\pi R^2}(\lambda\pi R^2)^2\lambda n \\ &= \left(C_1\pi^2 R^4 + o(1)\right)\lambda^3 n \to \infty.\end{aligned}$$

Consequently, if T_1 denotes the (random) number of triangles in G which lie entirely inside B_n^2 and have all angles between $\pi/6$ and $\pi/2$, then also $\mathbb{E}(T_1) \to \infty$. Finally, putting in the black points $\mathcal{P}$, and writing T_2 for the number of triangles counted in T_1 which are not within distance $1000R$ of a black point, we have that $\mathbb{E}(T_2) \to \infty$. A simple application of the second moment method shows that $\mathbb{P}(T_2 \geq 1) \to 1$ (this is intuitively obvious from $\mathbb{E}(T_2) \to \infty$ due to the long-range independence of the model). However, any red triangle counted in T_2 will have points in its interior which are not covered by black discs. Since with high probability $T_2 \geq 1$, we have that $p_\lambda^2(n) \to 0$. ∎

The other direction seems to require a more elaborate argument (and a stronger hypothesis):

Theorem 5. *If $g(n) = \lambda^3 n(\log n)^3 \to 0$, then $p_\lambda^2(n) \to 1$.*

Proof: (Sketch.) Suppose that $n \to \infty$ and also that $g(n) = \lambda^3 n(\log n)^3 \to 0$. Once again, we construct the Gilbert disc model $G = G_R(\mathcal{P}')$ on the red points $\mathcal{P}'$, but this time $R = R(n)$ will be a function of n. As long as $R(n)$ is not too large, there will be (up to a constant) λn vertices, $R^2\lambda^2 n$ edges and $R^4\lambda^3 n$ triangles in G inside B_n^2. We will show that $R(n)$ can be chosen so that:

(I) The maximum degree of G is one.

(II) The region of B_n^2 close to points of $\mathcal{P}'$ is covered (by $\mathcal{A}_\lambda^2$).

(III) The rest of B_n^2, far from points of $\mathcal{P}'$, is covered (by $\mathcal{A}_\lambda^2$).

Condition **(I)** simply states that G consists of isolated vertices and isolated edges. It is **(II)** and **(III)** which necessitate the stronger hypothesis. We will define a set of *bad events*, which will depend on $\mathcal{P}$ and $\mathcal{P}'$, and show that coverage (by $\mathcal{A}_\lambda^2$) occurs in the absence of bad events. We will then show that the probability of at least one bad event occurring tends to zero.

First, we overlay a grid of squares of side length $r = \sqrt{\log n}$ onto B_n^2. The probability that any small square of the grid contains no point of $\mathcal{P}$ 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 $\mathcal{A}_\lambda^2$. Consequently, with high probability, any point of B_n^2 at distance more than $\sqrt{8\log n}$ from all red points will be covered by $\mathcal{A}_\lambda^2$. Our first type of bad event will be that some square S of the grid contains no black points: if no such event occurs then we may

assume that points at distance $\sqrt{8\log n}$ from $\mathcal{P}'$ are covered. This deals with **(III)**.

Take $R(n) = 1000\sqrt{\log n}$. Our second bad event will be that G contains vertices of degree at least 2. Write W for the number of such vertices in G (within B_n^2). Then

$$\begin{aligned}\mathbb{E}(W) &\sim \frac{1}{2}e^{-\lambda\pi R^2}(\lambda\pi R^2)^2\lambda n \\ &= \left(5\cdot 10^{11}\pi^2(\log n)^2 + o(1)\right)\lambda^3 n \to 0,\end{aligned}$$

so that $\mathbb{P}(W=0)\to 1$. This deals with **(I)**.

It remains to deal with **(II)**. From now on, we may assume that G has only isolated vertices and isolated edges (inside B_n^2). Recall that we need only worry about the coverage of points within distance $\sqrt{8\log n}$ from a red point. We will colour all such points yellow.

First we deal with the isolated vertices. Consider the circles of radii $10\sqrt{\log n}$ and $11\sqrt{\log n}$ around each isolated red point, and divide the annulus between these circles into 10 equal "sectors". With high probability, there is a black point inside each sector. But then the yellow region surrounding the red point is covered.

For the edges, a lengthier argument is needed. We provide a summary. Let $L\subset\mathbb{R}^2$ be the line segment between the two nodes connected by the red edge. The critical event here is coverage of the yellow "sausages" $L\oplus D(0,\sqrt{8\log n})$ around the red edges. By focusing on certain black points at a suitable, carefully chosen, distance from the red edge, it can be shown that such yellow sausages are indeed covered with probability $1-n^{-4}$—if the hypothesis holds. ■

B. Simulation results

Here we provide two simulation results, see Fig. 2, which give an indication of the fraction of the area that remains uncovered if the condition in Theorem 4 holds, and how quickly this fraction goes to zero if the condition in Theorem 5 holds.

V. Conclusions

We have introduced a novel class of coverage problems, where the size of the covering disks is determined by the distance to the nearest point in a second point process. In the Poisson-Poisson case, where black and red points are independent Poisson point processes, we have provided expressions for the covered volume fraction and the probability of complete coverage in the one- and two-dimensional cases.

The main result is the asymptotic threshold for coverage in two dimensions. For

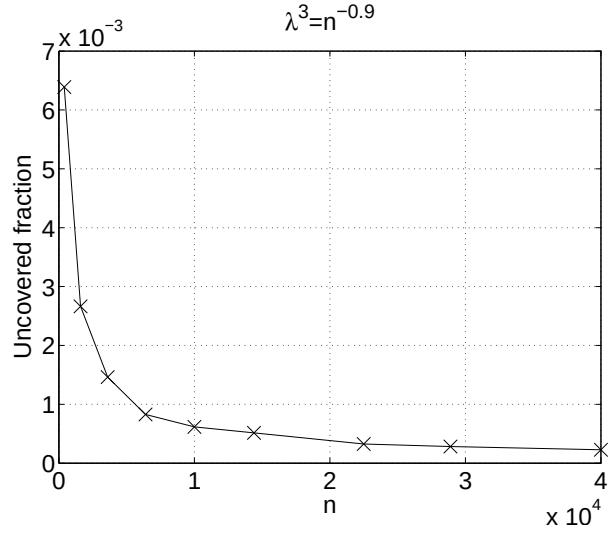
$$\lambda^3 n(\log n)^3 \to 0\,, \quad n\to\infty\,,$$

full coverage is achieved with probability tending to 1. On the other hand, if

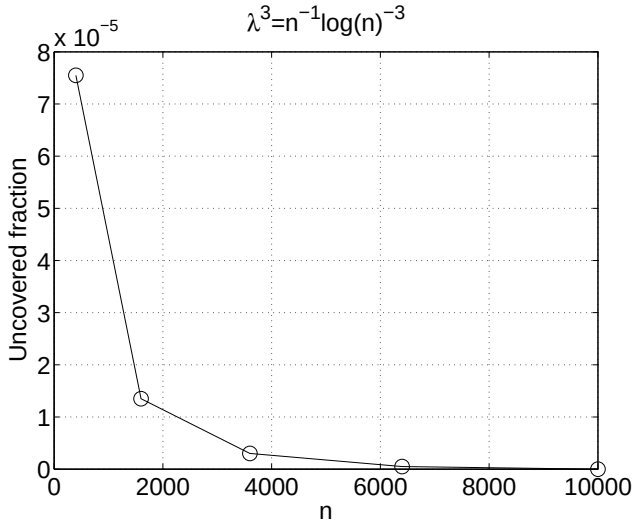
$$\lambda^3 n \to \infty\,, \quad n\to\infty\,,$$

then the probability of full coverage tends to 0.

The model can be viewed as a germ-grain model with germs of random and *correlated* size.



(a) Uncovered fraction for $\lambda^3 = n^{-0.9}$



(b) Uncovered fraction for $\lambda^3 = n^{-1}(\log n)^{-3}$

Fig. 2. Simulation results for Theorems 4 and 5. In (a), per Theorem 4, coverage is not achieved asymptotically. In (b), the function $g(n)$ in Theorem 5 is a constant, and it appears that coverage is achieved. Note that the scale in the axes are different in (a) and (b).

The results have applications in secure wireless networking. If the red points are eavesdroppers and the black point base stations, then full coverage in our model implies that from all points of the plane, messages can be received from at least one base station securely, without any eavesdropping.

Acknowledgment

The work of the second author was partially supported by the DARPA/IPTO IT-MANET program under grant W911NF-07-1-0028.

REFERENCES

[1] P. A. P. Moran and S. F. de St. Groth, "Random circles on a sphere," *Biometrika*, vol. 49, pp. 389–396, 1962.

[2] E. N. Gilbert, "The probability of covering a sphere with n circular caps," *Biometrika*, vol. 56, pp. 323–330, 1965.

[3] P. Hall, "On the coverage of k-dimensional space by k-dimensional spheres," *The Annals of Probability*, vol. 13, pp. 991–1002, Aug. 1985.

[4] S. Janson, "Random coverings in several dimensions," *Acta Mathematica*, vol. 13, pp. 991–1002, 1986.

[5] P. Hall, *Introduction to the Theory of Coverage Processes*. Wiley Series in Probability and Mathematical Statistics, 1988.

[6] S. Athreya, R. Roy, and A. Sarkar, "On the Coverage of Space by Random Sets," *Advances in Applied Probability*, vol. 36, pp. 1–18, 2004.

[7] R. Roy, "Coverage of Space in Boolean Models," *Dynamics & Stochastics*, vol. 48, pp. 119–127, 2006.

[8] M. Haenggi, "The Secrecy Graph and Some of its Properties," in *2008 IEEE International Symposium on Information Theory (ISIT'08)*, (Toronto, Canada), July 2008.

[9] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks." ArXiv http://arxiv.org/abs/1001.3697, Jan. 2010.

[10] S. Goal, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling Location Uncertainty for Eavesdroppers: A Secrecy Graph Approach," in *IEEE Symposium on Information Theory (ISIT'10)*, (Austin, TX), June 2010.

[11] M. Tanemura, "Statistical Distributions of Poisson Voronoi Cells in Two and Three Dimensions," *Forma*, vol. 18, no. 4, pp. 221–247, 2003.

[12] S. A. Zuyev, "Estimates for distributions of the Voronoi polygon's estimates for distributions of the Voronoi polygon's geometric characteristics," *Random Structures and Algorithms*, vol. 3, pp. 149–162, 1992.