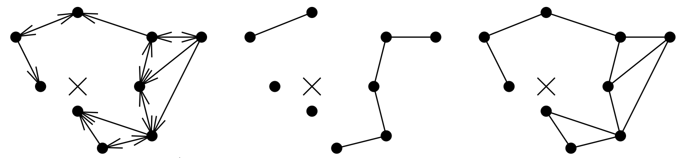
The Secrecy Graph and Some of its Properties

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

***Abstract*—A new random geometric graph model, the so-called *secrecy graph*, is introduced and studied. The graph represents a wireless network and includes only edges over which secure communication in the presence of eavesdroppers is possible. The underlying point process models considered are Poisson point processes. In the Poisson case, the node degrees are determined and percolation is studied using analytical bounds and simulations. It turns out that a small density of eavesdroppers already has a drastic impact on the connectivity of the secrecy graph.**



(a) Directed SG $\vec{G}$ (b) Basic SG G (c) Enhanced SG G'

Fig. 1. Example for secrecy graphs. The dots are the good guys, the cross the eavesdropper. The underlying graph is assumed to be fully connected so that the secrecy graphs include all edges along which secure communication is possible.

I. Introduction

There has been growing interest in information-theoretic secrecy. To study the impact of the secrecy constraint on the connectivity of ad hoc networks, we introduce a new type of random geometric graph, the so-called *secrecy graph*, that represents the network or communication graph including only links over which secure communication is possible. We assume that a transmitter can choose the rate very close to the capacity of the channel to the intended receiver, so that any eavesdropper further away than the receiver cannot intercept the message. This translates into a simple geometric constraint for secrecy which is reflected in the secrecy graph. In this initial investigation, we study some of the properties of the secrecy graph.

II. The Secrecy Graph

Let $\hat{G} = (\phi, \hat{E})$ be a geometric graph in $\mathbb{R}^d$, where $\phi = \{x_i\} \subset \mathbb{R}^d$ represents the locations of the nodes, also referred to as the "good guys". We can think of this graph as the unconstrained network graph that includes all possible edges over the good guys could communicate if there were no secrecy constraints.

Take another set of points $\psi = \{y_i\} \subset \mathbb{R}^d$ representing the locations of the eavesdroppers or "bad guys". These are assumed to be known to the good guys.

Let $D_x(r)$ be the (closed) d-dimensional ball of radius r centered at x, and let $\delta(x,y) = \|x-y\|$ be a distance metric, typically Euclidean distance. Further, let $\phi(A)$ and $\psi(A)$ denote the number of points of ϕ or ψ falling in $A \subset \mathbb{R}^d$.

Based on $\hat{G}$, we define the following secrecy graphs (SGs):

The directed secrecy graph: $\vec{G} = (\phi, \vec{E})$. Replace all edges in $\hat{E}$ by two directional edges. Then remove all edges $\overrightarrow{x_i x_j}$ for which $\psi\left(D_{x_i}(\delta(x_i,x_j))\right) > 0$, *i.e.*, there is at least one eavesdropper in the ball.

From this directed graph, two undirected graphs are derived:

The basic secrecy graph: $G = (\phi, E)$, where the (undirected) edge set E is

$$E \triangleq \{x_i x_j \,:\, \overrightarrow{x_i x_j} \in \vec{E} \text{ and } \overrightarrow{x_j x_i} \in \vec{E}\}\,.$$

The enhanced secrecy graph: $G' = (\phi, E')$, where

$$E' \triangleq \{x_i x_j \,:\, \overrightarrow{x_i x_j} \in \vec{E} \text{ or } \overrightarrow{x_j x_i} \in \vec{E}\}\,.$$

Clearly, $E \subset E'$. The difference is that edges in E permit secure bidirectional communication while edges in E' only allow secure communication in one direction. However, this one-way link may be used to transmit a one-time pad so that the other node can reply secretly. In doing so, the link capacity would drop from $1/2$ in each direction to $1/3$. Fig. 1 shows an example in $\mathbb{R}^2$ for the three types of secrecy graphs. based on the same underlying fully connected graph $\hat{G}$.

One way to assess the impact of the secrecy requirement is to determine the *secrecy ratios*

$$\eta = \frac{|E|}{|\hat{E}|} = \frac{\bar{N}}{\bar{\hat{N}}}\,; \qquad \eta' = \frac{|E'|}{|\hat{E}|} = \frac{\bar{N}'}{\bar{\hat{N}}}\,, \tag{1}$$

where $\bar{N}$, $\bar{N}' \geqslant \bar{N}$, and $\bar{\hat{N}}$ are the average node degrees of the respective graphs. For $\eta \approx 1$, the impact of the secrecy requirement is negligible while for small η it severely prunes the graph.

For the directed graph, the mean in- and out-degrees are equal, so we define $\vec{N} \triangleq \bar{N}^{\text{out}} = \bar{N}^{\text{in}} = |\vec{E}|/|\phi|$. Since the edge sets of G and G' are a partition of the edge set of the undirected multigraph containing all edges in $\vec{G}$, the following holds:

Fact 1 *The mean degrees are related by*

$$\bar{N} + \bar{N}' = 2\bar{N}^{\text{in}} = 2\bar{N}^{\text{out}}\,. \tag{2}$$

Furthermore, the degrees of all nodes $x \in \phi$ are bounded by

$$N_x \leqslant \min\{N_x^{\rm in}, N_x^{\rm out}\} \leqslant \max\{N_x^{\rm in}, N_x^{\rm out}\} \leqslant N'_x \leqslant N_x^{\rm in} + N_x^{\rm out}\,. \quad (3)$$

In the example in Fig. 1, (2) yields $10/9 + 22/9 = 32/9$.

These graphs become interesting if the locations of the vertices are stochastic point processes. We will use Φ and Ψ as the corresponding random variables.

Our goal is to study the properties of the resulting random geometric graphs, including degree distributions and percolation thresholds. We will consider two cases, lattices and Poisson point processes.

A. Lattice model

Let the underlying graph be the standard square lattice in $\mathbb{Z}^2$, *i.e.*, $\hat{G} = \mathbb{L}^2$, where edge exists between all pairs of points with Euclidean distance 1. Let Ψ be obtained from random independent thinning of a regular point set where each point exists with probability p, independently of all others. Let the corresponding secrecy graphs be denoted as $\vec{G}_p$, G_p, and G'_p. Let $\theta(p)$ be the probability that the component containing the origin is infinite[1]. Then the percolation threshold is defined as

$$p_c = \inf\{p \,:\, \theta(p) = 0\}\,. \quad (4)$$

B. Poisson model

Let the underlying graph be Gilbert's disk graph $\hat{G}_r$ [1], where Φ is a Poisson point process (PPP) of intensity 1 in $\mathbb{R}^2$ and two vertices are connected if their distance is at most r. Ψ is another, independent, PPP of intensity λ. Denote the secrecy graphs by $\vec{G}_{\lambda,r}$, $G_{\lambda,r}$, and $G'_{\lambda,r}$. With $\theta(\lambda, r)$ being the probability that the component containing the origin (or any arbitrary fixed node) is infinite, the percolation threshold radius for $\vec{G}_r$ is

$$r_{\rm G} \triangleq \sup\{r \,:\, \theta(0, r) = 0\} \approx 1.198\,, \quad (5)$$

where the subscript G indicates that this is Gilbert's critical radius which is not known exactly but the bounds $1.1979 < r_c < 1.1988$ were established with 99.99% confidence in [2]. For radii larger than $r_{\rm G}$, we define

$$\lambda_c(r) \triangleq \inf\{\lambda \,:\, \theta(\lambda, r) = 0\}\,, \quad r > r_{\rm G}. \quad (6)$$

For the analyses, we assume that there is a node in Φ at the origin. This does not affect the distributional properties of the PPP.

The parameter r indicating the maximum range of transmission can be related to standard communication parameters as follows: Assume a standard path loss law with attenuation exponent α, a transmit power P, a noise floor W, and a minimum SNR Θ for reliable communication. Then

$$r = \left(\frac{P}{\Theta W}\right)^{1/\alpha}\,. \quad (7)$$

[1] In the directed case, to be precise, we consider oriented percolation and let $\theta(p)$ be the probability that the out-component is finite, *i.e.*, that there are directed paths from the origin to an infinite number of nodes. Alternatively (or in addition) we could consider the in-component of the origin.

III. Properties of the Poisson Secrecy Graphs

A. Isolation probabilities for $r = \infty$

Fact 2 *The probability that the origin o cannot talk to anyone in $\vec{G}_{\lambda,\infty}$ (out-isolation) is*

$$\mathbb{P}[N^{\rm out} = 0] = \frac{\lambda}{\lambda + 1}\,. \quad (8)$$

In $G_{\lambda,\infty}$:

$$\mathbb{P}[N = 0] = \frac{c\lambda}{c\lambda + 1} \quad (9)$$

where $c = \frac{4}{3} + \frac{\sqrt{3}}{2\pi} = 1.609$.

For the directed graph, this is simply the probability that the nearest neighbor in the combined process $\Phi \cup \Psi$ (of density $1 + \lambda$) is an eavesdropper. In the basic graph, let x denote the origin's nearest neighbor in Φ and let $R = \|x\|$. For $N > 0$, we need $D_o(R) \cup D_x(R)$ to be free of eavesdroppers. The area of the two intersecting disks is $c\pi R^2$ for $c = 4/3 + \sqrt{3}/(2\pi)$, and the probability density (pdf) of R is $p_R(r) = 2\pi r \exp(-\pi r^2)$ (Rayleigh with mean 1/2). So

$$\mathbb{P}[N > 0] = \mathbb{E}_R[\exp(-\lambda c\pi R^2)] = \frac{1}{c\lambda + 1}\,. \quad (10)$$

The probability of in-isolation $\mathbb{P}[N^{\rm in} = 0]$ is smaller than $\mathbb{P}[N^{\rm out} = 0]$, since for each node $x \in \Phi\backslash\{o\}$, there must be at least one bad guy in $D_x(\|x\|)$. Clearly, this probability is smaller compared to (8) where only the nearest eavesdropper matters. On the other hand, the in-degree is less likely than the out-degree to be large since a significantly larger area needs to be free of bad guys. The isolation probability $\mathbb{P}[N' = 0]$ is the smallest of all isolation probabilities.

B. Degree distributions

Proposition 3 *The out-degree of o in $\vec{G}_{\lambda,\infty}$ is geometric with mean $1/\lambda$.*

Proof: Consider the sequence of nearest neighbors of o in the combined process $\Phi \cup \Psi$. $N^{\rm out} = n$ if the closest n are in Φ and the $(n+1)$-st is in Ψ. Since these are independent events,

$$\mathbb{P}[N^{\rm out} = n] = \frac{\lambda}{1 + \lambda}\left(\frac{1}{1 + \lambda}\right)^n. \quad (11)$$

∎

Alternatively, the distribution can be obtained as follows: Let R be the distance to the closest *bad* guy, *i.e.*, $R = \min_{y \in \Psi} \|y\|$. We have

$$\mathbb{P}[N^{\rm out} = n] = \mathbb{E}_R\left[\exp(-\pi R^2)\frac{(\pi R^2)^n}{n!}\right]\,, \quad (12)$$

where the pdf of R is $p_R(r) = 2\pi r\lambda \exp(-\pi\lambda r^2)$.

For general r, we have:

Proposition 4 *The out-degree distribution of $\vec{G}_{\lambda,r}$ is*

$$\mathbb{P}[N^{\rm out} = n] = \frac{\lambda\left(1 - \frac{\Gamma(n,a)}{\Gamma(n)}\right) + \exp(-a)\frac{a^n}{n!}}{(\lambda + 1)^{n+1}}\,, \quad (13)$$

where $a = \pi r^2(\lambda + 1)$, and $\Gamma(\cdot,\cdot)$ is the upper *incomplete gamma function. The probability of out-isolation is*

$$\mathbb{P}[N^{\text{out}} = 0] = \frac{\exp(-\pi r^2(\lambda+1)) + \lambda}{1+\lambda}\,, \tag{14}$$

and the mean out- and in-degrees are

$$\mathbb{E}N^{\text{out}} = \mathbb{E}N^{\text{in}} = \frac{1}{\lambda}(1 - \exp(-\lambda\pi r^2))\,. \tag{15}$$

The mean degree of the basic graph $G_{\lambda,r}$ is

$$\mathbb{E}N = \frac{1}{c\lambda}(1 - \exp(-c\lambda\pi r^2))\,, \tag{16}$$

where $c = \frac{4}{3} + \frac{\sqrt{3}}{2\pi}$.

Proof: If there is no bad guy inside $D_x(r)$ — which is the case with probability $P_0 = \exp(-\lambda\pi r^2)$ — then the number is simply Poisson with mean πr^2. If there is a bad guy at distance R, the number is Poisson with mean πR^2. So we have

$$\begin{aligned}\mathbb{P}[N^{\text{out}} = n] =& P_0 \exp(-\pi r^2)\frac{(\pi r^2)^n}{n!} \\ &+ (1-P_0)\mathbb{E}_{R<r}\left[\exp(-\pi R^2)\frac{(\pi R^2)^n}{n!}\right]\,,\end{aligned}$$

which, after some manipulations, yields (13). The mean is obtained more directly using Campbell's theorem [3] which says that for stationary point processes with intensity μ in $\mathbb{R}^2$ and non-negative measurable f,

$$\mathbb{E}\left[\sum_{x\in\Phi} f(x)\right] = \mu\int_{\mathbb{R}^2} f(x)\mathrm{d}x\,.$$

Applied to the mean out-degree ($\mu = 1$) we obtain

$$\begin{aligned}\mathbb{E}N^{\text{out}} &= \sum_{x\in\Phi}\mathbb{P}(\overrightarrow{ox} \in \vec{E}) = \mathbb{E}\sum_{\substack{x\in\Phi\setminus\{o\}\\ \|x\|<r}} \exp(-\lambda\pi\|x\|^2) \\ &= 2\pi\int_0^r x\exp(-\lambda\pi x^2)\mathrm{d}x\,. \end{aligned}\tag{17}$$

By replacing the area πr^2 by $c\pi r^2$ (area of two overlapping disks of radius r and distance r), the same calculation yields (16). ∎

The probability of isolation can directly be obtained from considering the two possibilities for isolation: Either there is no node at all within distance r or there is one node (or more) within r and the nearest one is bad. So, using a as in the proposition, $\mathbb{P}[N^{\text{out}} = 0] = \exp(-a) + (1-\exp(-a))\lambda/(1+\lambda)$. Since Φ has intensity 1, the isolation probability equals the density of isolated nodes.

As $\lambda \to 0$, we obtain the Poisson isolation probability and for $r \to \infty$ we get the geometric isolation probability (11). Also in (13) we can observe the expected behavior in the limits $\lambda, r \to 0$ and $\lambda, r \to \infty$. So the two-parameter distribution (13) includes the Poisson distribution and the geometric distribution as special cases. Fig. 2 shows an example of the resulting distributions for $r = 1$ and $\lambda = 1/5$.

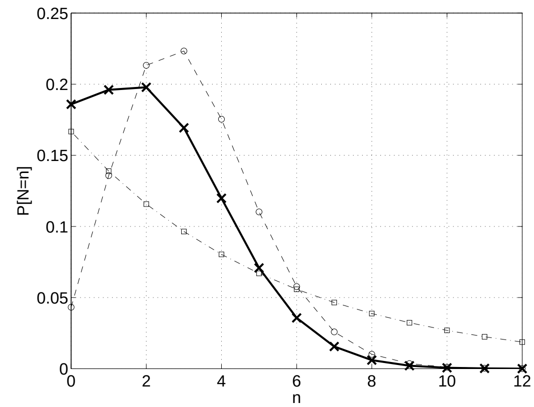


Fig. 2. Distribution of the node degree with and without power constraints. The solid bold curve shows the distribution (13) for $r = 1$ and $\lambda = 1/5$. The dashed curve is the Poisson distribution with mean π (which results when $r = 1$, $\lambda = 0$), and the dash-dotted curve is the geometric distribution with mean 5 (which results when $\lambda = 1/5$, $r \to \infty$).

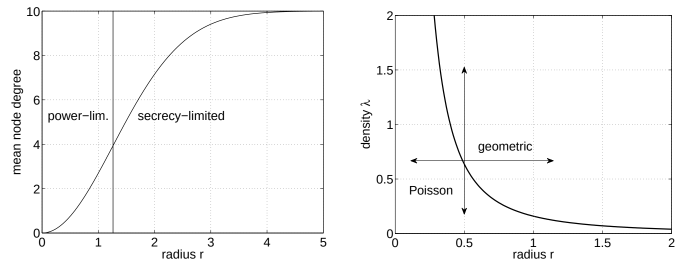


Fig. 3. Left: Mean out-degree of $\vec{G}_{1/10,r}$. The vertical line goes through the inflection point and indicates the boundary between the power-limited and the secrecy-limited regime. At the inflection point, $r = r_T = (2\pi\lambda)^{-1/2} = \sqrt{5/\pi} \approx 1.26$. Right: The curve $\lambda = (2\pi r^2)^{-1}$ bordering the power-limited and the secrecy-limited regimes. As $r \to \infty$ or $\lambda \to \infty$, the network becomes secrecy-limited and the degree distribution is geometric. As $r \to 0$ or $\lambda \to 0$, the network is power-limited and the degree distribution is Poisson.

As a function of r, the mean degree increases approximately as πr^2 for small r (this is the region where the degree is power-limited) and has a cap at $1/\lambda$ (due to the secrecy condition). Hence there exists a power-limited and a secrecy-limited regime, and the inflection point of $\mathbb{E}N(r)$, which is $r_T = (2\pi\lambda)^{-1/2}$ is a suitable boundary. This is illustrated in Fig. 3. Generally, the curve $2\pi r^2 = 1/\lambda$ separates the two regimes. Note that in the *po*wer-limited regime, the distribution is close to *Po*isson, whereas in the secrecy-limited regime, it is closer to geometric. Using the maximum slope s of $\mathbb{E}N^{\text{out}}(r)$, a simple piecewise linear upper bound on the mean degree is

$$\mathbb{E}N^{\text{out}}(r) < \min\{sr, \frac{1}{\lambda}\}\,, \quad s \triangleq \sqrt{\frac{2\pi}{e\lambda}}\,. \tag{18}$$

This bound is reasonably tight for λ not too small.

As a function of λ, the mean degree is monotonically decreasing from πr^2 to 0, upper bounded by $1/\lambda$.

The transmission range (power) needed to get within ϵ of the maximum mean out-degree (for $r = \infty$) is

$$r_\epsilon = \sqrt{\frac{-\log\epsilon}{\lambda\pi}} \tag{19}$$

For example, $r_{0.01} = 1.21/\sqrt{\lambda}$ achieves a mean out-degree of $0.99/\lambda$.

Next we establish bounds on the node degree distribution in the basic graph $G_{\lambda,\infty}$. Let R be the distance of the nearest bad guy. If the second-nearest bad guy is at distance at least $2R$, which happens with probability $\exp(-\lambda\pi 3R^2)$, then bidirectional secure communication is possible to any good guy in the area $a\pi R^2$ where $a = 2/3 + \sqrt{3}/(4\pi) \approx 0.80$ (circle minus a segment of height $R/2$). As a lower bound, we consider the circle of radius $R/2$. For sure bidirectional communication is possible to any node within that distance. (This bound would be tight if there were many more bad guys, all at the same distance R.) So we have

$$\sum_{k=0}^{n} \mathbb{E}_R \left[\exp(-A)\frac{A^k}{k!}\right] < \mathbb{P}[N \leqslant n] < \sum_{k=0}^{n} \mathbb{E}_R \left[\exp(-B)\frac{B^k}{k!}\right]$$

where $A = a\pi R^2$ and $B = b\pi R^2$ with $b = 1/4$. The bounds are geometric:

$$1 - \left(\frac{a}{a+\lambda}\right)^{n+1} < \mathbb{P}[N \leqslant n] < 1 - \left(\frac{b}{b+\lambda}\right)^{n+1} \qquad (20)$$

Since $\mathbb{E}N = \sum \mathbb{P}[N > n]$, the bounds $a/\lambda > \mathbb{E}N > b/\lambda$ for the mean degree follow. From (16) we already know that $\mathbb{E}N = 1/(\lambda c) \approx 0.62/\lambda$.

Lastly, in this subsection, we consider the enhanced graph.

Proposition 5 *The mean degree $\mathbb{E}N'$ in the enhanced graph $G'_{\lambda,r}$ is*

$$\mathbb{E}N' = \frac{2}{\lambda}(1-\exp(-\lambda\pi r^2)) - \frac{1}{c\lambda}(1-\exp(-c\lambda\pi r^2))\,. \quad (21)$$

Proof: This follows by combining (2), (15), and (16). ∎

C. Secrecy ratios

Using the mean degree established in (16) we obtain

$$\eta(\lambda, r) = \frac{1-\exp(-c\lambda\pi r^2)}{c\lambda\pi r^2}\,. \qquad (22)$$

$\eta(\lambda, r)$ is decreasing in both r and λ. $\eta'(\lambda, r)$ follows from (21). Of interest are also the relative edge densities of the enhanced and basic graphs:

Fact 6 *At least a fraction $3\pi/(5\pi+3\sqrt{3}) \approx 0.45$ of the edges in the enhanced graph $G'_{\lambda,r}$ are present in the basic graph $G_{\lambda,r}$.*

The ratio $\mathbb{E}N/\mathbb{E}N'$ is 1 for small λr^2 and reaches its minimum as $\lambda r^2 \to \infty$, where it is $(2c-1)^{-1}$ with c as in (16). The consequence is that in some graphs, more than 50% of the links can only be used securely in one direction (unless one-time pads are used).

D. Edge lengths

We consider the distribution of the length of the edges in $\vec{G}_{\lambda,\infty}$. For each node, its nearest bad guy determines the maximum length of an out-edge. So we intuitively expect the edge length distribution to approximately inherit the distribution of the distance to the nearest bad guy. Simulation studies reveal that indeed the edge length distribution is very close to Rayleigh with mean $1/(2\sqrt{\lambda})$, with only very slightly higher probabilities for longer edges—which is expected since nodes whose nearest bad guy is far will have many long edges on average and thus skew the distribution.

In the power-limited regime, with r finite and $\lambda \to 0$, the edge length pdf converges to the usual $2x/r^2$, $0 \leqslant x \leqslant r$.

E. Oriented percolation of $\vec{G}_{\lambda,r}$

We are studying oriented out-percolation in $\vec{G}_{\lambda,r}$, *i.e.*, the critical region in the (λ, r)-plane for which there is a positive probability that the out-component containing the origin has infinite size.

Fact 7 *$\lambda_c(r)$ is monotonically increasing for $r > r_{\mathrm{G}}$, and we have*

$$0 < \lim_{r\to\infty} \lambda_c(r) < 1\,. \qquad (23)$$

In other words, there exists a $\lambda_\infty < 1$ such that for $\lambda > \lambda_\infty$, $G'_{\lambda,r}$ does not percolate for any r.

This follows from the facts that for fixed r the mean degree is continuously decreasing to 0 as a function of λ, and for $\lambda < 1$, the mean degree is smaller than 1 even for $r = \infty$, so percolation is impossible. We will use λ_∞ to denote the limit in (23). For intensities smaller than that, we define

$$r_c(\lambda) \triangleq \sup\{r \,:\, \theta(\lambda, r) = 0\}\,, \quad \lambda \leqslant \lambda_\infty\,. \qquad (24)$$

From the monotonic decrease of the mean degree in λ follows:

Fact 8 *The percolation radius $r_c(\lambda)$ is monotonically increasing with λ and has a vertical asymptote at λ_∞.*

Conjecture 9 *$r_c(\lambda)$ is convex (and, consequently, $\lambda_c(r)$ is concave):*

$$\frac{\mathrm{d}^2 r_c(\lambda)}{\mathrm{d}\lambda^2} > 0 \quad \forall\, 0 \leqslant \lambda < \lambda_\infty \qquad (25)$$

It follows that

$$r_c(\lambda) \geqslant r_{\mathrm{G}} + c\lambda\,, \quad \textit{where } c \triangleq \left.\frac{\mathrm{d}r_c(\lambda)}{\mathrm{d}\lambda}\right|_{\lambda=0}. \qquad (26)$$

Simulation results show that $\lambda_\infty \approx 0.1499$ with a standard deviation of $5.8 \cdot 10^{-4}$ over 200 runs.

Since $\lambda_c(r)$ is concave and converges to a finite λ_∞, we may conjecture that it can be well approximated by a function of the form:

$$\lambda_c(r) \approx \lambda_\infty - \exp(a - br)\,, \quad r > r_{\mathrm{G}}\,, \qquad (27)$$

where a and b are related through $a = \log\lambda_\infty + br_{\mathrm{G}}$. Indeed simulation results (see Fig. 4) reveal that for $b = 4$, $\lambda_\infty =$

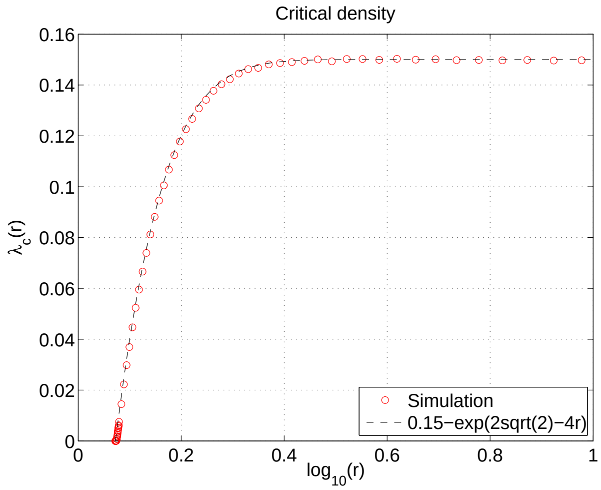


Fig. 4. The simulated critical density $\lambda_c(r)$ vs. $\log_{10}(r)$ together with a simple exponential approximation. Each simulated point is the average of 30 runs.

0.1499, and $a = 2\sqrt{2}$, we obtain an excellent approximation. Similarly,

$$r_c(\lambda) \approx \frac{a}{b} - \frac{1}{b}\log(\lambda_\infty - \lambda)\,, \quad \lambda < \lambda_\infty\,. \tag{28}$$

It follows that the constant c in Conj. 9 is $c = (b\lambda_\infty)^{-1} = 5/3$, and the slope of $\lambda_c(r)$ at $r = r_{\mathrm{G}}^+$ is $3/5$.

For the *critical* graph $\vec{G}_{\lambda, r_c(\lambda)}$, it turns out that both $\mathbb{P}[N = 0]$ and $\mathbb{E}N$ are increasing with λ.

A good empirically derived approximation is

$$\mathbb{P}[N_c^{\mathrm{out}} = 0] \approx \frac{1}{80} + \frac{4}{5}\lambda\,, \quad \lambda < \lambda_\infty\,. \tag{29}$$

For the mean out-degree we have from (15) and (28)

$$\mathbb{E}N_c^{\mathrm{out}}(\lambda) > \pi r_{\mathrm{G}}^2 + \frac{11}{4}\lambda\,. \tag{30}$$

$\mathbb{E}N_c^{\mathrm{out}}(\lambda)$ is convex and reaches $1/\lambda_\infty$ at $\lambda = \lambda_\infty$ per Prop. 3.

So percolation on the secrecy graph requires a higher mean degree than Gilbert's disk graph, as expected since edges are not independent.

IV. Concluding Remarks

We have introduced a new class of random geometric graphs that captures the condition for secure communications in ad hoc networks. For lattice-based models, there exist analogies to bond and site percolation problems. In Poisson-based networks, we have derived the mean node degrees and, in some cases, the distribution. As a byproduct, a two-parameter distribution was found that includes the Poisson and the geometric distribution as special cases. Based on the mean degree, we defined power- and secrecy-limited regions in the (λ, r)-plane. The percolation region $\{(r, \lambda) : \theta(r, \lambda) > 0\}$ was bounded and numerically determined. In conclusion, the presence of eavesdroppers is rather harmful in the random case. A (relative) density of 0.15 is sufficient to make percolation impossible. Many interesting problems remain open; we hope that this initial study sparks further investigations.

Acknowledgments

The author wishes to thank Aylin Yener for the discussions leading to the problem studied in this paper. The support of NSF (grants CNS 04-47869, DMS 505624, and CCF 728763), and the DARPA/IPTO IT-MANET program (grant W911NF-07-1-0028) is gratefully acknowledged.

References

[1] E. Gilbert, "Random plane networks," *Journal of the Society for Industrial Applied Mathematics*, vol. 9, pp. 533–543, 1961.

[2] P. Balister, B. Bollobás, and M. Walters, "Continuum percolation with steps in the square of the disc," *Random Structures and Algorithms*, vol. 26, pp. 392–403, July 2005.

[3] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*. John Wiley & Sons, 1995. 2nd Ed.