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 lattices and Poisson point processes. In the lattice case, analogies to standard bond and site percolation can be exploited to determine percolation thresholds. 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.

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 \( \psi = \{y_j\} \subset \mathbb{R}^d \) representing the locations of the eavesdroppers or “bad guys”. These are assumed to be known to the good guys.

Let \( D_s(r) \) 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 \( \phi \) or \( \psi \) falling in \( A \subset \mathbb{R}^d \).

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

The directed secrecy graph: \( \hat{G} = (\phi, \hat{E}) \). Replace all edges in \( \hat{E} \) by two directional edges. Then remove all edges \( \overrightarrow{x_i,x_j} \) for which \( \psi(D_s(\delta(x_i,x_j))) > 0 \), 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

\[
E \triangleq \{x_i x_j : \overrightarrow{x_i,x_j} \in \hat{E} \text{ and } \overrightarrow{x_j,x_i} \in \hat{E}\}.
\]

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

\[
E' \triangleq \{x_i x_j : \overrightarrow{x_i,x_j} \in \hat{E} \text{ or } \overrightarrow{x_j,x_i} \in \hat{E}\}.
\]

Clearly, \( E \subset E' \). The difference is that edges in \( E \) permit secure unidirectional 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

\[
\eta = \frac{|E|}{|\hat{E}|} = \frac{\bar{N}}{\bar{N}}; \quad \eta' = \frac{|E'|}{|\hat{E}|} = \frac{\bar{N}'}{\bar{N}}, \quad (1)
\]

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

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

**Fact 1** The mean degrees are related by

\[
\bar{N} + \bar{N}' = 2\bar{N}^{\text{in}} = 2\bar{N}^{\text{out}}. \quad (2)
\]
Furthermore, the degrees of all nodes $x \in \phi$ are bounded by

$$N_x \leq \min\{N_x^{\text{in}}, N_x^{\text{out}}\} \leq \max\{N_x^{\text{in}}, N_x^{\text{out}}\} \leq N_x' \leq N_x^{\text{in}} + N_x^{\text{out}}.$$  \(3\)

In the example in Fig. 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 $\Phi$ and $\Psi$ 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., $G = \mathbb{L}^2$, where edge exists between all pairs of points with Euclidean distance 1. Let $\Psi$ 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 $G_p, G'_p$, and $G''_p$. Let $\theta(p)$ be the probability that the component containing the origin is infinite. Then the percolation threshold is defined as

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

B. Poisson model

Let the underlying graph be Gilbert's disk graph $G_r$, where $\Phi$ is a Poisson point process (PPP) of intensity 1 in $\mathbb{R}^2$ and two vertices are connected if their distance is at most $r$. $\Psi$ is another, independent, PPP of intensity $\lambda$. Denote the secrecy graphs by $G_{\lambda, r}$, $G'_{\lambda, r}$, 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 $G_r$ is

$$r_G \triangleq \sup\{r : \theta(0, r) = 0\} \approx 1.198,$$  \(5\)

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 $r_G$, we define

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

For the analyses, we assume that there is a node in $\Phi$ 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 $\alpha$, a transmit power $P$, a noise floor $W$, and a minimum SNR $\Theta$ for reliable communication. Then

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

III. PROPERTIES OF THE LATTICE SECRECY GRAPHS

Consider first the graph $G'_p$ for the case where a bad guy is placed (with probability $p$) in the middle of each edge in $\mathbb{L}^2$, i.e.,

$$\Psi = \{x \in (\mathbb{Z}^2 + (1/2, 0)) \cup (\mathbb{Z}^2 + (0, 1/2)) : U_x < p\},$$  \(8\)

where $U_x$ is iid uniformly distributed in $[0, 1]$.

This case is analogous to bond percolation on the two-dimensional square lattice [3], so:

Fact 2 The percolation threshold for $G'_p$ is $p_c = 1/2$.

For $p = 1/2$, the density of bad guys is 1, the same as the density of good guys. So the density of bad guys only needs to be a factor $1 - \epsilon$ smaller than the density of good guys, and the graph still percolates, for any $\epsilon > 0$. Close to that threshold $\eta' = 1/2$.

If we put the bad guys on the lattice points themselves (with probability $p$), the situation is analogous to site percolation on $\mathbb{L}^2$, for which the critical probability is unknown but estimated to be around 0.59, so $p_c \approx 0.41$. In this case the maximum density of bad guys is only 0.41.

So it seems having the eavesdroppers at the locations indicated in (8) causes the least “damage” to the connectivity of the secrecy graph among all regular $\Psi$.

IV. PROPERTIES OF THE POISSON SECRECY GRAPHS

A. Isolation probabilities for $r = \infty$

Fact 3 The probability that the origin $o$ cannot talk to anyone in $G_{\lambda, \infty}$ (out-isolation) is

$$\mathbb{P}[N^{\text{out}} = 0] = \frac{\lambda}{\lambda + 1}.$$  \(9\)

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

$$\mathbb{P}[N = 0] = \frac{c\lambda}{c\lambda + 1}$$  \(10\)

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 $\Phi$ 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 $\pi R^2$ 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 $1/2$) [4]. So

$$\mathbb{P}[N > 0] = \mathbb{E}_R[\exp(-\lambda c\pi R^2)] = \frac{1}{c\lambda + 1}.$$  \(11\)

The probability of in-isolation $\mathbb{P}[N^{\text{in}} = 0]$ is smaller than $\mathbb{P}[N^{\text{out}} = 0]$, since for each node $x \in \Phi \setminus \{o\}$, there must be at least one bad guy in $D_x(||x||)$. Clearly, this probability is smaller compared to (9) 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 4** The out-degree of \( o \) in \( G_{\lambda,\infty} \) is geometric with mean \( 1/\lambda \).

**Proof:** Consider the sequence of nearest neighbors of \( o \) in the combined process \( \Phi \cup \Psi \). \( N_{\text{out}} \) is \( n \) if the closest \( n \) are in \( \Phi \) and the \( (n+1) \)-st is in \( \Psi \). Since these are independent events,

\[
P[N_{\text{out}} = n] = \frac{\lambda}{1+\lambda} \left( \frac{1}{1+\lambda} \right)^n. \tag{12}
\]

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

\[
P[N_{\text{out}} = n] = \mathbb{E}_R \left[ \exp(-\pi R^2) \left( \frac{\pi R^2}{n!} \right)^n \right], \tag{13}
\]

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

For general \( r \), we have:

**Proposition 5** The out-degree distribution of \( G_{\lambda,r} \) is

\[
P[N_{\text{out}} = n] = \frac{\lambda}{1+\lambda} \left( \frac{1}{1+\lambda} \right)^n \left( 1 - \frac{1}{\Gamma(\lambda)} + \exp(-a) \frac{a^n}{n!} \right), \tag{14}
\]

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

\[
P[N_{\text{out}} = 0] = \frac{\exp(-\pi r^2(\lambda + 1)) + \lambda}{1+\lambda}, \tag{15}
\]

and the mean out- and in-degrees are

\[
\mathbb{E}N_{\text{out}} = \mathbb{E}N_{\text{in}} = \frac{1}{c \lambda} \left( 1 - \exp(-c \lambda \pi r^2) \right). \tag{16}
\]

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

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

which, after some manipulations, yields (14). The mean is obtained more directly using Campbell’s theorem [5] which says that for stationary point processes with intensity \( \mu \) in \( \mathbb{R}^2 \) and non-negative measurable \( f \),

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

By replacing the area \( \pi r^2 \) by \( c \pi r^2 \) (area of two overlapping disks of radius \( r \) and distance \( r \)), the same calculation yields (17).

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, \( P[N_{\text{out}} = 0] = \exp(-a) + (1-\exp(-a))\lambda/(1+\lambda) \).

Since \( \Phi \) 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 (12). Also in (14) we can observe the expected behavior in the...
limits \( \lambda, r \to 0 \) and \( \lambda, r \to \infty \). So the two-parameter distribution \((14)\) includes the Poisson distribution and the geometric distribution as special cases. Fig.2 shows an example of the resulting distributions for \( r = 1 \) and \( \lambda = 1/5 \).

As a function of \( r \), the mean degree increases approximately as \( \pi r^2 \) 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 infection 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 power-limited regime, the distribution is close to Poisson, 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

\[
\mathbb{E}N^{\text{out}}(r) < \min\{sr, \frac{1}{\lambda}\}, \quad s \triangleq \sqrt{\frac{2\pi}{\varepsilon \lambda}}. \tag{19}
\]

This bound is reasonably tight for \( \lambda \) not too small.

As a function of \( \lambda \), the mean degree is monotonically decreasing from \( \pi r^2 \) to 0, upper bounded by \( 1/\lambda \).

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

\[
r_e = \sqrt{-\frac{\log \varepsilon }{\lambda^2}}. \tag{20}
\]

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 this distance. (This bound would be tight if there were many more bad guys, all at the same distance \( R \).) So we have

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

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

\[
1 - \left( \frac{a}{a + \lambda} \right)^{n+1} < \mathbb{P}[N \leq n] < 1 - \left( \frac{b}{b + \lambda} \right)^{n+1}. \tag{21}
\]

Since \( \mathbb{E}N = \sum \mathbb{P}[N > n] \), the bounds \( a/\lambda > \mathbb{E}N > b/\lambda \) for the mean degree follow. From \( (17) \) we already know that \( \mathbb{E}N = 1/(\lambda c) \approx 0.62/\lambda \).

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

**Proposition 6** The mean degree \( \mathbb{E}N' \) in the enhanced graph \( G'_{\lambda, r} \) is

\[
\mathbb{E}N' = \frac{2}{\lambda} \left( 1 - \exp(-\lambda \pi r^2) \right) - \frac{1}{c\lambda} (1 - \exp(-c\lambda \pi r^2)). \tag{22}
\]

**Proof:** This follows by combining \((2), (16), \) and \((17)\).

**C. Secrecy ratios**

Using the mean degree established in \((17)\) we obtain

\[
\eta(\lambda, r) = \frac{1 - \exp(-c\lambda \pi r^2)}{c\lambda \pi r^2}. \tag{23}
\]

\( \eta(\lambda, r) \) is decreasing in both \( r \) and \( \lambda \). \( \eta'(\lambda, r) \) follows from \((22)\). Of interest are also the relative edge densities of the enhanced and basic graphs:

**Fact 7** 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 \( \lambda r^2 \) and reaches its minimum as \( \lambda r^2 \to \infty \), where it is \( (2e - 1)^{-1} \) with \( c \) as in \((17)\). 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 \( G'_{\lambda, \infty} \). 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 \( 2x/r^2, 0 \leq x \leq r \).

**E. Oriented percolation of \( G'_{\lambda, r} \)**

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

**Fact 8** \( \lambda_c(r) \) is monotonically increasing for \( r > r_c \), and we have

\[
0 < \lim_{r \to \infty} \lambda_c(r) < 1. \tag{24}
\]

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 \( \lambda \), and for \( \lambda < 1 \), the mean degree is smaller than 1 even for \( r = \infty \), so percolation is impossible. We will use \( \lambda_\infty \) to denote the limit in \((24)\). For intensities smaller than that, we define

\[
r_c(\lambda) \triangleq \sup\{r : \theta(\lambda, r) = 0\}, \quad \lambda \leq \lambda_\infty. \tag{25}
\]

From the monotonic decrease of the mean degree in \( \lambda \) follows:
**Fact 9** The percolation radius \( r_c(\lambda) \) is monotonically increasing with \( \lambda \) and has a vertical asymptote at \( \lambda_\infty \).

**Conjecture 10** \( r_c(\lambda) \) is convex (and, consequently, \( \lambda_c(r) \) is concave): 
\[
\frac{d^2 r_c(\lambda)}{d\lambda^2} > 0 \quad \forall 0 \leq \lambda < \lambda_\infty \tag{26}
\]
It follows that 
\[
r_c(\lambda) \geq r_G + c\lambda, \text{ where } c \equiv \frac{dr_c(\lambda)}{d\lambda}|_{\lambda=0}. \tag{27}
\]
Simulation results show that \( \lambda_\infty \approx 0.1499 \) with a standard deviation of \( 5.8 \times 10^{-4} \) over 200 runs.

Since \( \lambda_c(r) \) is concave and converges to a finite \( \lambda_\infty \), we may conjecture that it can be well approximated by a function of the form:
\[
\lambda_c(r) \approx \lambda_\infty - \exp(a - br), \quad r > r_G, \tag{28}
\]
where \( a \) and \( b \) are related through \( a = \log \lambda_\infty + b r_G \). Indeed, simulation results (see Fig. 4) reveal that for \( b = 4 \), \( \lambda_\infty = 0.1499 \), and \( a = 2\sqrt{2} \), we obtain an excellent approximation. Similarly,
\[
r_c(\lambda) \approx \frac{a}{b} - \frac{1}{b} \log(\lambda_\infty - \lambda), \quad \lambda < \lambda_\infty. \tag{29}
\]
It follows that the constant \( c \) in Conj. 10 is \( c = (b\lambda_\infty)^{-1} = 5/3 \), and the slope of \( \lambda_c(r) \) at \( r = r_G^+ \) is \( 3/5 \).

For the critical graph \( \bar{G}_{\lambda_c(\lambda)} \), it turns out that both \( \mathbb{P}_r[N = 0] \) and \( \mathbb{E}N \) are increasing with \( \lambda \).

A good empirically derived approximation is
\[
\mathbb{P}_r[N_c^{\text{out}} = 0] \approx \frac{1}{80} + \frac{4}{5} \lambda, \quad \lambda < \lambda_\infty. \tag{30}
\]
For the mean out-degree we have from (6) and (25)
\[
\mathbb{E}N_c^{\text{out}}(\lambda) > \pi r_G^2 + \frac{11}{4} \lambda. \tag{31}
\]