The Effect of Eavesdroppers on Network Connectivity: A Secrecy Graph Approach

Satashu Goel*, Vaneet Aggarwal, Aylin Yener, and A. Robert Calderbank

***Abstract*—This paper investigates the effect of eavesdroppers on network connectivity, using a wiretap model and percolation theory. The wiretap model captures the effect of eavesdroppers on link security. A link exists between two nodes only if the secrecy capacity of that link is positive. Network connectivity is defined in percolation sense, i.e., connectivity exists if an infinite connected component exists in the corresponding *secrecy graph*. We consider uncertainty in location of eavesdroppers, which is modeled directly at the *network level* as correlated failures in the secrecy graph. Our approach attempts to bridge the gap between physical layer security under uncertain channel state information and network level connectivity under secrecy constraints. For square and triangular lattice secrecy graphs, we obtain bounds on the percolation threshold, which is the critical value of the probability of occurrence of an eavesdropper, above which network connectivity does not exist. For Poisson secrecy graphs, degree distribution and mean value of upper and lower bounds on node degree are obtained. Further, inner and outer bounds on the achievable region for network connectivity are obtained. Both analytic and simulation results show that uncertainty in location of eavesdroppers has a dramatic effect on network connectivity in a secrecy graph.**

EDICS: SEC-NETW (Network security), MOD-SECU (Security and privacy models), MOD-CHAN (Channel and network models)

I. Introduction

In the recent years, there has been growing interest in employing information theoretic methods to provide secrecy in wireless networks. In his seminal paper [1], Wyner introduced the wiretap channel and formalized the rate at which messages to the intended receiver can be reliably communicated over a discrete memoryless channel while keeping them confidential from an eavesdropper (wiretapper) that receives the signals from a degraded channel. Csiszár and Körner in [2] provided a general secrecy capacity result for the non-degraded wiretap channel. This framework has been successfully applied to networks with one hop communication, such as broadcast, e.g., [3, 4], multiple access, e.g., [5], and two-hop communication with relays, e.g., [6, 7].

Recently, information theoretic techniques have been used to provide end-to-end secrecy in large networks. The concept of *secrecy graph* was introduced in [8], which models the communication network and the effect of eavesdroppers on network security. Link connectivity in a secrecy graph is determined using the wiretap model. A link is considered to be connected if the secrecy capacity of the link is positive. The secrecy graph is analyzed for network connectivity using tools from percolation theory [8, 9]. Thus, network connectivity is defined in percolation sense, i.e., network connectivity exists if an infinite connected component exists in the secrecy graph. Scaling laws for secrecy capacity in large networks have also been investigated in [10, 11]. In [10], a random network was considered where the legitimate nodes and eavesdroppers are placed in a square region of area n according to independent Poisson point processes (PPPs). It was shown that secrecy requirement does not lead to a loss in throughput, in terms of scaling, if the intensity of eavesdroppers is $O((\log n)^{-2})$ while the intensity of the legitimate nodes is 1. In [11], a similar result was shown for mobile ad-hoc networks (MANETs) with n legitimate nodes and a delay constraint of D, if the number of eavesdroppers scales as $o(\sqrt{nD})$.

In references [8–11] the channel gains of all the eavesdroppers are assumed to be known precisely. This assumption may not be realistic, especially for a passive eavesdropper, since it may not be possible to ascertain even the presence of such an entity. For wiretap channel models with a few nodes, the uncertainty of the eavesdropper channel can be modeled using a compound channel model [12, 13]. Noise injection techniques [14] can be used if the channel is unknown in multiple antenna wiretap models. In [15], it was shown that secrecy is possible even if the eavesdropper's channel is arbitrarily varying. In contrast to these results on small networks, we want to characterize the effect of uncertainty in location of eavesdroppers on *network level connectivity*, for large networks.

In this paper, we present a secrecy graph approach where the locations of eavesdroppers are uncertain, and this uncertainty results in node and link failures in a secrecy graph. The main challenge is that these failures are *correlated*, and hence,

S. Goel is with Qualcomm Inc., San Deigo, CA 92121 (email: satashu@cmu.edu). He was with Wireless Communications and Networking Laboratory, Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802, USA, when this work was done. A. Yener is with Wireless Communications and Networking Laboratory, Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802, USA (email: yener@engr.psu.edu). V. Aggarwal is with AT&T Labs Research, 180 Park Avenue - Building 103, Florham Park, NJ 07932, USA (email: vaneet@research.att.com). A. R. Calderbank is with Departments of Computer Science, Mathematics, and Electrical & Computer Engineering, Duke University, Durham, NC 27708, USA (email: robert.calderbank@duke.edu). V. Aggarwal and A. R. Calderbank were with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA, when this work was done. A preliminary version of part of this work was presented at the IEEE International Symposium on Information Theory, Austin, TX, June 2010. The work of S. Goel and A. Yener is supported in part by the National Science Foundation grants CNS-0716325, CCF-0964362, and DARPA ITMANET program through grant W911NF-07-11-0028. The work of V. Aggarwal and R. Calderbank is supported in part by NSF under grant DMS 0701226, by ONR under grant N00173-06-1-G006, and by AFOSR under grant FA 9550-09-1-0643.

the techniques from percolation theory must be extended to account for these correlations. We assume a communication model where a node is aware of only those legitimate and eavesdropper nodes that are located within a distance r_v from the node. We consider square and triangular lattice secrecy graphs which model regular placement of legitimate nodes. We also consider Poisson secrecy graphs which model random placement of legitimate nodes in $\mathbb{R}^2$ according to a Poisson point process. We assume uniform node distribution for analytical tractability [16], since analytical results are known for only a handful of stochastic network models.

Percolation threshold is the critical value of probability of occurrence of an eavesdropper, above which an infinite connected component does not exist in the secrecy graph, almost surely. Exact results are not known even for a square lattice with independent link and node failures. Hence, this paper provides bounds on percolation threshold for square and triangular lattices, which provide insight into the effect of uncertainty in eavesdropper's location on the percolation properties of lattice secrecy graphs.

For the Poisson secrecy graph, distributions and mean values of upper and lower bounds on the degree of a legitimate node are obtained. Given the intensity of legitimate nodes and the radius of communication r_v, the pair (λ, r_E) of the intensity of eavesdropper nodes and the radius of uncertainty is achievable if percolation occurs in the corresponding secrecy graph. We obtain inner and outer bounds on the achievable (λ, r_E) region. In [17], degree distribution and mean value of bounds on node degree in a Poisson secrecy graph were characterized, in the special case when r_v is infinite. In this paper, we provide a tighter upper bound on the percolation threshold of the triangular lattice, compared to the result in [17]. Both analytical and simulation results demonstrate the dramatic effect of location uncertainty of eavesdroppers on network connectivity in a secrecy graph.

The remainder of this paper is organized as follows. In Section II, the connectivity problems considered in this paper are presented formally. In Section III, our results on percolation in square and triangular lattices are presented. The Poisson secrecy graph is considered in Section IV. Bounds on the mean node degree, and inner and outer bounds on the achievable (λ, r_E) region are presented. In Section V, numerical results on percolation probability in lattice secrecy graphs, and bounds on mean node degree and achievable (λ, r_E) region are presented. Finally, Section VI concludes the paper.

II. Model and Formulation

We denote the function $(x)^+ \triangleq \max(0, x)$. Let $\hat{G} = (\phi, \hat{E})$ denote a geometric graph in $\mathbb{R}^d$, where $\phi = \{x_i\} \subset \mathbb{R}^d$ is the set of locations of legitimate nodes. $\hat{E}$ is the set of links over which reliable communication is possible. Link reliability is modeled using Gilbert's disk graph model [18]. We assume that the radius of communication, or range of view, is r_v. Two nodes are connected in the geometric graph if the distance between them is at most r_v. A node is unaware of the presence of any eavesdropper outside the circle of radius r_v centered at the node. Each eavesdropper is located within a known *finite* area, however, the precise location is unknown. Let y_i denote the location of the center of the area which contains eavesdropper i. Let A_i denote the corresponding area. The set $\psi = \bigcup_i A_i \subset \mathbb{R}^d$ thus describes the area in which eavesdroppers exist. If the locations of the nodes come from a stochastic point process, we denote the corresponding random variables by Φ and Ψ.

We define secrecy graphs (SGs) based on $\hat{G}$ and ψ. A link exists in the secrecy graph if the link exists in the underlying geometric graph and the secrecy capacity of the link is positive. We assume that the wireless medium introduces path loss, with exponent α, and that the noise introduced by the receivers is Additive White Gaussian Noise (AWGN). If a source transmits a signal with power P_s to a receiver at distance d_R, and the eavesdropper is located at distance d_E, the secrecy capacity is given by [19]

$$C_s = \left(\log\left(1 + \frac{P_s}{d_R^\alpha}\right) - \log\left(1 + \frac{P_s}{d_E^\alpha}\right)\right)^+ . \qquad (1)$$

The AWGN power is assumed to be unity for both the channels. If the destination is closer than the eavesdropper, i.e., $d_R < d_E$, the secrecy capacity is positive and it is zero otherwise. It should be noted that in this paper, we will utilize this link metric for simplicity. In general, it is difficult to make any claims on the secrecy capacity region of a sizeable network, given the complex interactions that can take place between the network nodes to manage and utilize interference for secrecy [5, 20]. However, since our goal in this paper is to understand and demonstrate the effect of eavesdroppers on connectivity without the knowledge of their channels, it is fitting to sacrifice the network information theoretic rigor, and instead use this metric for the sake of obtaining a tractable problem. We will employ two secrecy graphs in this paper - *directed secrecy graph* and *basic secrecy graph* [8]. In a directed secrecy graph $\vec{G}$, a link (edge) exists from x_i to x_j if $\|x_i - x_j\| < \|x_i - y_k\|$ for all $y_k \in \psi$. In a basic secrecy graph G, a link exists between x_i and x_j if a directed link exists from x_i to x_j and also from x_j to x_i in $\vec{G}$.

A. Secrecy in Square and Triangular Lattice

We consider square and triangular lattices, shown in Fig. 1 and Fig. 3, respectively. A legitimate node is present at each vertex of the lattice, and each node is connected to its nearest neighbors. We assume that the probability that a square (or a triangular) region contains an eavesdropper is p_E. We assume that the links bounding each eavesdropper's location are known. For example, assume that the square S_1 in Fig. 1 contains an eavesdropper. In the basic secrecy graph, nodes a, b, c and d will not have any links, and thus, these nodes are considered to have *failed*. Notice that the node failures are correlated, since all nodes of a given square fail together. Thus, we can model the uncertainty in an eavesdropper's location at the *network level*, by employing a physical layer model for secrecy. This approach can be extended to include scenarios where each eavesdropper is located within a finite but arbitrary area. For example, assume that an eavesdropper is present within the squares S_2, S_3 or S_4, in Fig. 1. Then all the nodes

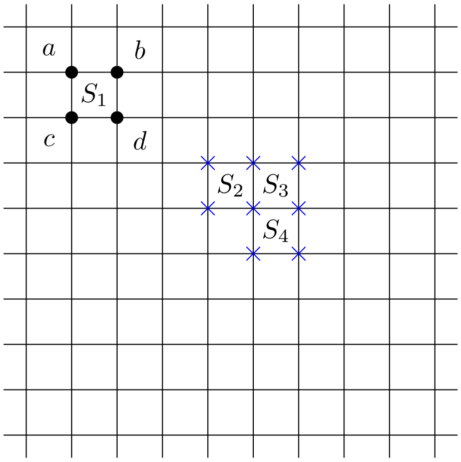


Fig. 1. Failures in square lattice

marked × fail. A similar model is used for the triangular lattice, where nodes on all the vertices of a triangle fail if an eavesdropper is present within that triangle.

B. Secrecy in Poisson graph

We assume that the locations of legitimate nodes follow a Poisson point process (PPP) Φ with intensity 1. Each eavesdropper is known to be located within a circle of radius r_E. The radius r_E captures the uncertainty in an eavesdropper's location. The center of the circles follow a PPP with intensity λ. We denote the directed and basic secrecy graphs by $\vec{G}_{\lambda,r_v,r_E}$ and G_{λ,r_v,r_E}, respectively.

C. Percolation Threshold

The concept of percolation was introduced by Broadbent and Hammersley [21], to model the diffusion process in materials. Percolation is said to occur if an infinite connected component exists in the corresponding graph. It was shown that a phase transition exists, i.e., there exists a critical threshold, below which all connected components are finite, almost surely, and above which an infinite connected component exists, almost surely. Similar results exist on connectivity in random graphs [22]; an area initiated by the work of Erdős and Réyni [23]. In an Erdős-Réyni graph, the probability of existence of a link between any two nodes is independent of the spatial positions of the nodes, and hence, it does not consider network geometry. Therefore, *geometric* random graphs [24] are used instead, to model wireless networks [25, 26]; where connectivity is analyzed using tools from continuum percolation [27].

Let us denote the number of nodes in the connected component containing the origin by $|C|$. First, we consider lattice secrecy graphs where probability of an eavesdropper occupying a square or triangular region is p_E. The percolation probability $\theta(p_E)$ and percolation threshold p_E^c are defined as

$$\theta(p_E) = P(|C| = \infty) \qquad (2)$$

$$p_E^c = \inf\{p_E : \theta(p_E) = 0\}. \qquad (3)$$

Roughly, p_E^c is the smallest value of p_E for which an infinite component does not exist in the secrecy graph. In other words, for any $p_E < p_E^c$, the secrecy graph will have an infinite connected component containing the origin, almost surely. However, the origin is part of the infinite component with probability $\theta(p_E)$, and not with probability 1 [28]. In Poisson secrecy graphs, we assume that the intensity of the legitimate nodes and the radius of communication r_v are fixed, and define the percolation probability as

$$\theta(\lambda, r_E) = P(|C| = \infty). \qquad (4)$$

The percolation threshold pairs (λ_c, r_E^c) are defined as

$$\lambda_c = \inf\{\lambda : \theta(\lambda, r_E^c) = 0\}, \quad r_E^c \geq 0. \qquad (5)$$

III. Square and Triangular Lattices

In this section, we will present bounds on the percolation threshold of square and triangular lattices, where the eavesdroppers are known to be located within square and triangular areas, respectively. We note that the percolation thresholds are known precisely only for a few lattices. For example, for a triangular lattice, where a node appears at each vertex *independently* with probability p, the critical probability is $p_c = 1/2$ [29]. However, the corresponding percolation threshold for a square lattice is not known [28]. Notice that in the secrecy graphs considered in this paper, failures are *correlated*, and hence, the corresponding problems of determining the percolation threshold are expected to be intractable. Therefore, we focus on obtaining upper and lower bounds on the percolation threshold that are as tight as possible. The bounds are obtained by considering a square lattice with different link probabilities for horizontal and vertical links. The following lemma from [30] is useful in obtaining the bounds.

Lemma 1. *(Sykes and Essam [30]): For a square lattice with link probabilities p_1 and p_2 for horizontal and vertical links, respectively, the critical probability satisfies*

$$p_1 + p_2 = 1. \qquad (6)$$

Let the distance between the nearest neighbors in a square or triangular lattice be s. We will assume that $r_v > s$, since percolation can occur in square and triangular lattices only if $r_v > s$.

We first consider the square lattice, where the probability that a square region bounded by links in the lattice contains an eavesdropper is p_E. It is known which squares contain an eavesdropper, however, the exact locations of the eavesdroppers within the squares are unknown. The following theorem presents bounds on the critical eavesdropper probability, for a square lattice.

Theorem 1. *For a square lattice where nodes are located on the vertices of the lattice and eavesdroppers are located in square regions of the lattice with probability p_E, the percolation threshold for the basic secrecy graph, denoted by p_E^c, satisfies*

$$1 - \frac{1}{\sqrt[16]{2}} \leq p_E^c \leq \frac{3 - \sqrt{5}}{2}. \qquad (7)$$

Proof: The existence of critical probability follows from [28]. The percolation threshold in the given square lattice $\mathcal{S}_1$ is denoted by p_E^c.

For the upper bound on the percolation threshold, assume that no eavesdroppers are present in the squares $(2i, 2j)$ for all integers i and j, and eavesdroppers are present in the remaining squares with probability p_E. Now assume that each square $(2i+1, 2j+1)$ is a node in a new square lattice $\mathcal{S}_2$, and the node fails when there is an eavesdropper in the corresponding square. Further, the nodes in $\mathcal{S}_2$ corresponding to squares $(2i+1, 2i+1)$ and $(2i+3, 2i+1)$ are connected if and only if there is no eavesdropper in square $(2i+2, 2i+1)$. Similarly, the nodes in $\mathcal{S}_2$ corresponding to squares $(2i+1, 2i+1)$ and $(2i+1, 2i+3)$ are connected if and only if there is no eavesdropper in square $(2i+1, 2i+2)$. Thus, in the square lattice $\mathcal{S}_2$, the probability of existence of a node and a link are denoted as $p_n = 1 - p_E$ and $p_l = 1 - p_E$, respectively. Notice that the failures in $\mathcal{S}_2$ are independent and identically distributed (i.i.d.). However, we have a mixed site-bond percolation problem [31], and the percolation threshold for that problem is not known. To obtain a bond percolation problem with independent bond (link) probabilities, we map a node failure to the failure of the horizontal link connected to that node on the left. Notice that this underestimates the number of link failures, since a node failure would actually result in the failure of all the links connected to it. Thus, we obtain a new square lattice $\mathcal{S}_3$ in which node probability is 1 and link probabilities for horizontal and vertical links are $p_1 = (1-p_E)^2$ and $p_2 = (1-p_E)$, respectively. Let the critical threshold of p_E for the square lattices $\mathcal{S}_2$ and $\mathcal{S}_3$ be $p_E^{S_2}$ and $p_E^{S_3}$, respectively. For a fixed p_E, if percolation does not occur in the square lattice $\mathcal{S}_3$, it cannot occur in the square lattice $\mathcal{S}_2$ either. Further, removing eavesdroppers from squares $(2i, 2j)$ in the square lattice $\mathcal{S}_1$ can only increase the critical threshold. Hence, the percolation thresholds of the lattices $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ satisfy

$$p_E^c \le p_E^{S_2} \le p_E^{S_3} \tag{8}$$

The percolation threshold of the square lattice $\mathcal{S}_3$ can be found using Lemma 1, where link probabilities are $(1-p_E)^2$ and $(1-p_E)$. This gives the upper bound in the statement of the theorem.

For the lower bound, consider a tiling in $\mathbb{R}^2$ where each tile is a square region consisting of 16 squares. Adjacent rows of tiles are offset by two squares, as shown in Fig. 2(a). Each tile is mapped to a node in a triangular lattice, which fails when any of the squares in that tile contains an eavesdropper. This results in a triangular lattice with node probability $(1-p_E)^{16}$ and link probability 1. Note that we are over-counting the number of eavesdroppers, and this results in a lower bound on the percolation threshold. Percolation occurs in the triangular lattice if

$$(1-p_E)^{16} > p_{c,n}^T \tag{9}$$

where $p_{c,n}^T = 1/2$ is the node (site) percolation threshold for a triangular lattice [29]. Thus, the percolation threshold for the square lattice S_1 must me at least $1 - 1/\sqrt[16]{2}$. ■

For the square lattice, the probability of a node failure is related to p_E as

$$p_{fail} = p_E(2(1-p_E)(2 - p_E + p_E^2) + p_E^3). \tag{10}$$

We contrast this with the scenario where nodes occur on the vertices of a square lattice independently with probability p. Let the threshold probability in that case be p_c. In the secrecy graph model, adjacent nodes fail together, and hence, the failures are *clustered*. Intuitively, a larger number of node failures can be tolerated in the secrecy graph before connectivity is lost, and hence, we expect that $p_{fail} > (1 - p_c)$. Further, we expect that $p_E < (1-p_c)$, since more than one node failures may occur due to the presence of one eavesdropper. Numerical results in Section V will validate this intuition.

Now, consider the placement of nodes on the vertices of the triangular lattice and eavesdroppers inside triangular regions of the lattice. Suppose that a triangular region contains an eavesdropper with probability p_E. The critical eavesdropper probability can be bounded as in the following theorem.

Theorem 2. *For a triangular lattice where nodes are located on the vertices of the lattice and eavesdroppers are located in triangular regions of the lattice with probability p_E, the percolation threshold for the basic secrecy graph, denoted by p_E^c, satisfies*

$$1 - \frac{1}{\sqrt[24]{2}} \le p_E^c \le \frac{4}{3} - \frac{1}{3}\left(\sqrt[3]{\frac{25-\sqrt{621}}{2}} + \sqrt[3]{\frac{25+\sqrt{621}}{2}}\right). \tag{11}$$

Proof: We denote the given triangular lattice by $\mathcal{T}_1$. For the upper bound, assume that there are no eavesdroppers in the triangles $(3i+1, 3j+1)$, $(3i+1, 3j+2)$, $(3i+2, 3j+1)$, $(3i+2, 3j+2)$ for all integers i and j and the eavesdroppers are present in the remaining triangles with probability p_E. The indexing of triangles is shown in Fig. 3. Now assume that each triangle $(3i, 3j)$ is a node of a new square lattice $\mathcal{S}_1$ which fails when there is an eavesdropper in that triangle. Further, nodes in $\mathcal{S}_1$ corresponding to triangles $(3i, 3i)$ and $(3i+3, 3i)$ are connected if and only if there is no eavesdropper in any of the triangles $(3i+1, 3i)$ and $(3i+2, 3i)$. Similarly, nodes in $\mathcal{S}_1$ corresponding to triangles $(3i, 3i)$ and $(3i, 3i+3)$ are connected if and only if there is no eavesdropper in any of the triangles $(3i, 3i+1)$ and $(3i, 3i+2)$. Thus, in the square lattice $\mathcal{S}_1$, the probability of existence of a node and a link is $p_n = 1 - p_E$ and $p_l = (1-p_E)^2$ respectively. We obtain a bond (link) percolation problem with independent link probabilities by mapping a node failure to the failure of the horizontal link connected to the node on the left. Thus, we obtain a new square lattice $\mathcal{S}_2$ with node probability 1 and link probabilities for horizontal and vertical links $p_1 = (1-p_E)^3$ and $p_2 = (1-p_E)^2$, respectively. Let the critical threshold of p_E for square lattices $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$ be p_E^c, $p_E^{S_2}$ and $p_E^{S_3}$, respectively. For a fixed p_E, if percolation does not occur in the square lattice $\mathcal{S}_3$, it cannot occur in the square lattice $\mathcal{S}_2$, and in turn it cannot occur in the square lattice $\mathcal{S}_1$. Hence,

$$p_E^c \le p_E^{S_2} \le p_E^{S_3}. \tag{12}$$

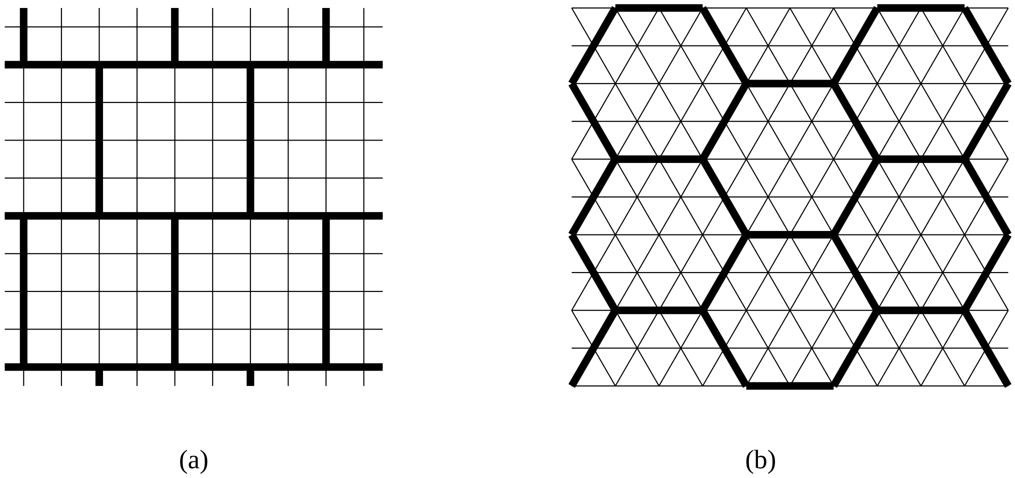


Fig. 2. (a) Tiling in square lattice for lower bound (b) Tiling in triangular lattice for lower bound

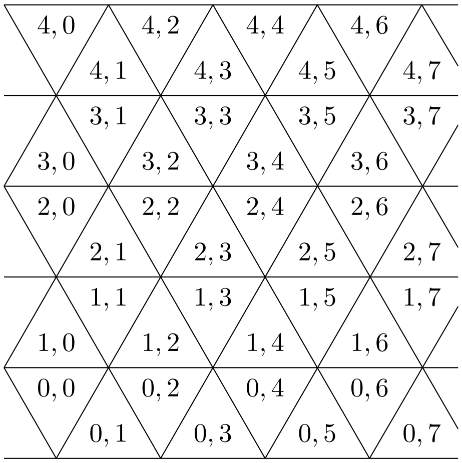


Fig. 3. Indices in triangular lattice

The percolation threshold $p_E^{S_3}$ can be found using Lemma 1, where link probabilities are $(1-p_E)^3$ and $(1-p_E)^2$.

For the lower bound, consider a tiling in $\mathbb{R}^2$ where each tile consists of 24 triangular regions, as shown in Fig. 2(b). Each tile is mapped to a node in a triangular lattice, which fails when any of the triangular regions in that tile contains an eavesdropper. This results in a triangular model with node probability $(1-p_E)^{24}$ and link probability 1. Following the arguments in the proof of Theorem 1, it can be shown that the percolation threshold of the triangular lattice $\mathcal{T}$ must me at least $1-1/\sqrt[24]{2}$. ■

IV. Poisson secrecy graph

In this section, we consider a Poisson model where Φ is a Poisson point process (PPP) of intensity 1 in $\mathbb{R}^2$ (Intensity of a point process denotes the density of nodes per unit area.). The eavesdroppers are located in known circular regions. The centers of circular regions are located in $\mathbb{R}^2$ according to a Poisson point process Ψ of intensity λ, which is independent of Φ. The radius of the circular regions is denoted by r_E. We assume that a legitimate node is aware of only those circular regions containing eavesdroppers whose centers lie within the circle of radius r_v, centered at the node.

For simplicity, we consider the node located at the origin, denoted by o. Let N denote the number of bi-directional links of node o. An analytic computation of N is difficult because it requires characterization of the intersection of two regions - a circular region which determines the out-degree of node o, and a polygonal region which determines the in-degree of node o. The polygonal region is the interior of the region formed by the intersection of bisectors of the line segments which join the origin to the eavesdroppers. Let N^{out} denote the number of directed links out of node o. Assume that the center of a circular region containing an eavesdropper, which is closest to the origin, is located at a distance R from it. Then N^{out} is the number of legitimate nodes in the circle $C(\mathbf{0}, (\min(r_v, R) - r_E)^+)$. Clearly, $N \leq N^{out}$, and thus, we have an upper bound on the node degree. A lower bound can be obtained by considering the circle $C(\mathbf{0}, (\min(r_v, R) - r_E)^+/2)$, since the origin has a bi-directional link to all the nodes in this region. Let $\tilde{N}$ denote the number of legitimate nodes in $C(\mathbf{0}, (\min(r_v, R) - r_E)^+/2)$. Clearly, $\tilde{N} \leq N$. In the following, we will present results on the probability mass function (p.m.f.) and mean values of N^{out} and $\tilde{N}$. The p.m.f. of node degree characterizes the connectivity properties in a Poisson secrecy graph. In Poisson graphs without secrecy constraints, the mean degree is sufficient to characterize the percolation threshold. We will show that a bound on the mean degree can be used to obtain an outer bound on the achievable (λ, r_E) region.

A. Degree distributions

We now present the degree distributions of N^{out} and $\tilde{N}$ by computing $P(N^{out} = n)$ and $P(\tilde{N} = n)$, both of which can be expressed in terms of the same set of functions $\{f_n(x, y)\}$.

Let $f_n(x,y)$ be defined for all $n \in \{0,1,\ldots\}$ as follows.

$$\begin{aligned}
f_0(x,y) \;=\;& 1 - e^{-xyr_E^2} + e^{-xyr_v^2} e^{-x(r_v - r_E)^2} \\
&+ \frac{y}{1+y} e^{-x\frac{y}{1+y}r_E^2} \bigl(e^{-x(1+y)r_E^2(\frac{y}{1+y})^2} \\
&- e^{-x(1+y)(r_v - r_E/(1+y))^2} \bigr) \\
&+ xye^{-x\frac{y}{1+y}r_E^2} \frac{r_E}{(1+y)^{3/2}} \sqrt{\frac{\pi}{x}} \cdot \\
&\Biggl(-\operatorname{erf}\left(\sqrt{x(1+y)} r_E \frac{y}{1+y} \right) \\
&+ \operatorname{erf}\Biggl(\sqrt{x(1+y)} \left(r_v - \frac{r_E}{1+y} \right) \Biggr) \Biggr) \qquad (13)
\end{aligned}$$

$$\begin{aligned}
f_n(x,y) \;=\;& \frac{y}{n!} \frac{1}{(1+y)^{n+1}} e^{-x\frac{r_E^2 y}{1+y}} \Biggl(\sum_{k=0}^{2n+1} \binom{2n+1}{k} \cdot \\
&\Biggl(\Gamma\Biggl(\frac{k+1}{2}, x(1+y)\left(r_v - \frac{r_E}{1+y} \right)^2 \Biggr) \\
&- \Gamma\Biggl(\frac{k+1}{2}, x(1+y)\left(r_E - \frac{r_E}{1+y} \right)^2 \Biggr) \Biggr) \cdot \\
&\left(-\frac{r_E y \sqrt{x}}{\sqrt{1+y}} \right)^{2n+1-k} + r_E\sqrt{x(1+y)} \sum_{k=0}^{2n} \binom{2n}{k} \cdot \\
&\Biggl(\Gamma\Biggl(\frac{k+1}{2}, x(1+y)\left(r_v - \frac{r_E}{1+y} \right)^2 \Biggr) \\
&- \Gamma\Biggl(\frac{k+1}{2}, x(1+y)\left(r_E - \frac{r_E}{1+y} \right)^2 \Biggr) \Biggr) \cdot \\
&\left(-\frac{r_E y \sqrt{x}}{\sqrt{1+y}} \right)^{2n-k} \Biggr) + e^{-xyr_v^2} e^{-x(r_v - r_E)^2} \\
&\frac{x^n (r_v - r_E)^{2n}}{n!} \text{ for } n \geq 1, \qquad (14)
\end{aligned}$$

where

$$\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \qquad (15)$$

is the Gauss error function, and

$$\Gamma(s,x) = \int_x^\infty t^{s-1} e^{-t} dt \qquad (16)$$

is the upper incomplete gamma function.

In the next theorem, we present the p.m.f. of N^{out}, the number of out-going links from the node located at the origin. This p.m.f. characterizes the connectivity properties in the directed Poisson secrecy graph. The result is obtained for $r_v > r_E$, since if $r_v \leq r_E$, nodes will be unaware of eavesdroppers that are located arbitrarily close to them, and no secure communication will be possible in that case.

Theorem 3. *In the directed secrecy graph $\vec{G}_{\lambda,r_v,r_E}$ with radius of uncertainty for an eavesdropper's location r_E and radius of communication $r_v > r_E$, the probability mass function of the number of out-going links at the origin N^{out} is given by*

$$P(N^{out} = n) = f_n(\pi, \lambda) \qquad (17)$$

Proof: Assume that the center of the circular region containing an eavesdropper, that is closest to the origin, is located at a distance R from it. Then, the origin can securely transmit to any node within a circle of radius $(\min(r_v, R) - r_E)^+$. Averaging the probability of having n legitimate nodes in that circle over R results in the statement of the theorem. For details, see Appendix A. ∎

The above result can be specialized to two regimes of interest. In the first regime, the uncertainty in the location of eavesdroppers is small, i.e., $r_E \to 0$. In the second regime, the communication radius is large, i.e., $r_v \to \infty$. It is clear that when either $r_E \to \infty$ or $r_v \to 0$, no secure communication is possible.

Corollary 3.1. *If the uncertainty in location of the eavesdroppers is small,*

$$\lim_{r_E \to 0} P(N^{out} = 0) = \frac{\lambda}{1+\lambda} + \frac{1}{1+\lambda} e^{-\pi(1+\lambda)r_v^2}. \qquad (18)$$

Clearly, isolation probability decreases as the radius of communication r_v increases. If r_E is finite and the radius of communication r_v is infinite,

$$\begin{aligned}
\lim_{r_v \to \infty} P(N^{out} = 0) \;=\;& 1 - \frac{1}{1+\lambda} e^{-\pi\lambda r_E^2} + \frac{\pi\lambda r_E}{(1+\lambda)^{3/2}} \\
&\left(1 - \operatorname{erf}\left(\lambda r_E \sqrt{\frac{\pi}{1+\lambda}} \right) \right). \quad (19)
\end{aligned}$$

Notice that (18) which is obtained by letting r_E tend to zero, is the same expression obtained in [8], where it is assumed that the locations of the eavesdroppers are known precisely. In the directed Poisson secrecy graph, the node degree is characterized by obtaining the p.m.f. of N^{out}. In the following theorem, the p.m.f. of $\tilde{N}$ is presented, which is a lower bound on node degree in the basic Poisson secrecy graph.

Theorem 4. *In the basic secrecy graph G_{λ,r_v,r_E} with radius of uncertainty for eavesdropper's location r_E and radius of communication $r_v > r_E$, the probability mass function of $\tilde{N}$, which is a lower bound on the number of bi-directional links at the origin, is given by*

$$P(\tilde{N} = n) = f_n\left(\frac{\pi}{4}, 4\lambda \right) \qquad (20)$$

Proof: The proof is similar to that of Theorem 3, but nodes within the circle of radius $(\min(r_v, R) - r_E)^+/2$ are considered. For details, see Appendix B. ∎

Notice that the probability mass functions of $\tilde{N}$ and N^{out} are given by the same set of functions $\{f_n(x,y)\}$, albeit with different parameters. This is because the ratio of the areas considered for obtaining $\tilde{N}$ and N^{out} is constant regardless of the distance to the closest eavesdropper. Once again, we specialize the results for $r_E \to 0$ and $r_v \to \infty$ as follows.

Corollary 4.1. *If the uncertainty in location of the eavesdroppers is small,*

$$\lim_{r_E \to 0} P(\tilde{N} = 0) = \frac{4\lambda}{1+4\lambda} + \frac{1}{1+4\lambda} e^{-(\pi/4)(1+4\lambda)r_v^2}. \quad (21)$$

If r_E is finite and the radius of communication r_v is infinite,

$$\lim_{r_v \to \infty} P(\tilde{N} = 0) = 1 - \frac{1}{1+4\lambda} e^{-\pi\lambda r_E^2} + \frac{\pi \lambda r_E}{(1+4\lambda)^{3/2}} \left(1 - \operatorname{erf}\left(4\lambda r_E \sqrt{\frac{\pi/4}{1+4\lambda}}\right)\right). \quad (22)$$

Thus, we have characterized $\tilde{N}$ and N^{out} by obtaining their p.m.f.s, which show important trends with respect to r_v, λ and r_E. The trends are easy to notice in the regimes $r_E \to 0$ and $r_v \to \infty$. In these regimes, isolation probability increases with λ and r_E and decreases with r_v, as expected. Isolation probability is an important parameter, since it represents the proportion of nodes in the secrecy graph that cannot communicate securely with any other node. To further our intuition, we next characterize $P(\tilde{N} = 0)$ and $P(N^{out} = 0)$ when two of the parameters λ, r_E and r_v take extreme values.

Remark 1. For the directed secrecy graph,

$$\lim_{r_v \to \infty, r_E \to 0} P(N^{out} = 0) = \frac{\lambda}{1+\lambda} \quad (23)$$

$$\lim_{r_v \to \infty, r_E \to \infty} P(N^{out} = 0) = 1. \quad (24)$$

Similarly, for the upper bound on isolation probability,

$$\lim_{r_v \to \infty, r_E \to 0} P(\tilde{N} = 0) = \frac{4\lambda}{1+4\lambda} \quad (25)$$

$$\lim_{r_v \to \infty, r_E \to \infty} P(\tilde{N} = 0) = 1. \quad (26)$$

Thus, in both the cases, none of the nodes have any links, almost surely, in either the directed or basic secrecy graph, if the locations of the eavesdroppers are not known at all. For $r_E \to 0$, we obtain the probability of isolation of a node when locations of all the eavesdroppers are known precisely, which match the results in [8] where $r_E = 0$ was assumed. Note that for small values of λ both $\lim_{r_v \to \infty, r_E \to 0} P(N^{out} = 0)$ and $\lim_{r_v \to \infty, r_E \to 0} P(\tilde{N} = 0)$ increase linearly with λ.

Remark 2. As the eavesdroppers' intensity λ goes to zero,

$$\lim_{r_v \to \infty, \lambda \to 0} P(N^{out} = 0) = 0 \quad (27)$$

$$\lim_{r_v \to \infty, \lambda \to 0} P(\tilde{N} = 0) = 0, \quad (28)$$

meaning that all the nodes have at least one link, almost surely. As the eavesdroppers' intensity λ goes to infinity,

$$\lim_{r_v \to \infty, \lambda \to \infty} P(N^{out} = 0) = 1 \quad (29)$$

$$\lim_{r_v \to \infty, \lambda \to \infty} P(\tilde{N} = 0) = 1, \quad (30)$$

meaning that none of the nodes have any links, almost surely, regardless of the radius of uncertainty for eavesdroppers r_E and even if the communication radius is infinite.

B. Mean degree and percolation threshold

We now present results on the mean degree and percolation threshold for the Poisson secrecy graph. In a Poisson graph with intensity of nodes λ and communication radius r, where no secrecy constraints are imposed, the node degree distribution, and hence, connectivity properties are characterized by the term $a \triangleq \lambda \pi r^2$, which is the mean node degree in the graph. A critical value a_c exists such that if $a > a_c$ an infinite connected component exists in the graph with probability 1. If $a < a_c$, no infinite connected component exists, with probability 1. In the following theorem, we obtain bounds on the mean degree in the basic Poisson secrecy graph, and then obtain necessary and sufficient conditions for percolation to occur. The necessary condition is obtained in terms of a bound on the mean degree.

Theorem 5. *The mean degree of a node in the basic Poisson secrecy graph with secure bi-directional links is bounded as,*

$$\mathbf{E}[\tilde{N}] \le \mathbf{E}[N] \le \mathbf{E}[N^{out}], \quad (31)$$

where

$$\mathbf{E}[\tilde{N}] = \frac{1}{4\lambda}\left(e^{-\lambda\pi r_E^2} - e^{-\lambda\pi r_v^2}\right) - \frac{\pi r_E}{4\sqrt{\lambda}}\left(\operatorname{erf}(\sqrt{\lambda\pi} r_v) - \operatorname{erf}(\sqrt{\lambda\pi} r_E)\right) \quad (32)$$

$$\mathbf{E}[N^{out}] = 4\mathbf{E}[\tilde{N}] \quad (33)$$

Proof: The regions corresponding to $\tilde{N}$ and N^{out} were chosen so that $\tilde{N} \le N \le N^{out}$. By taking expectation, we obtain (31). The lower bound is obtained as follows. Let the center of the circular region containing an eavesdropper, that is closest to the origin, be located at a distance R from it. The lower bound is computed using the law of total expectation $\mathbf{E}[\tilde{N}] = \underset{R}{\mathbf{E}}[\mathbf{E}[\tilde{N}|R]]$. The upper bound is obtained in a similar manner. For details, see Appendix C. ■

Notice that the ratio $\mathbf{E}[N^{out}]/\mathbf{E}[\tilde{N}]$ is constant since the ratio of areas considered for obtaining N^{out} and $\tilde{N}$ is fixed. Thus, the bounds are expected to be tight when the mean degree is small. We now specialize the above result for $r_E \to 0$ and $r_v \to \infty$.

Corollary 5.1. *If the uncertainty in the location of eavesdroppers is small,*

$$\lim_{r_E \to 0} \mathbf{E}[\tilde{N}] = \frac{1}{4\lambda}\left(1 - e^{-\lambda\pi r_v^2}\right). \quad (34)$$

As expected, the mean degree increases as r_v increases. Further, for small λ and r_v finite, $\lim_{r_E \to 0} \mathbf{E}[\tilde{N}] \approx \pi r_v^2/4$, and hence, the mean degree depends only on r_v. If r_E is finite and the radius of communication r_v is infinite,

$$\lim_{r_v \to \infty} \mathbf{E}[\tilde{N}] = \frac{1}{4\lambda} e^{-\lambda\pi r_E^2} - \frac{\pi r_E}{4\sqrt{\lambda}}\left(1 - \operatorname{erf}(\sqrt{\lambda\pi} r_E)\right). \quad (35)$$

The mean degree decreases exponentially with the term $\lambda\pi r_E^2$.

We now compute the bounds on the mean degree when two of the parameters λ, r_E, r_v take extreme values. We expect the bounds to take large values when λ, r_E are small and r_v is large.

Remark 3. As the radius of uncertainty for eavesdroppers' location r_E takes limiting values,

$$\lim_{r_v \to \infty, r_E \to 0} \mathbf{E}[\tilde{N}] = \frac{1}{4\lambda} \quad (36)$$

$$\lim_{r_v \to \infty, r_E \to \infty} \mathbf{E}[\tilde{N}] = 0. \quad (37)$$

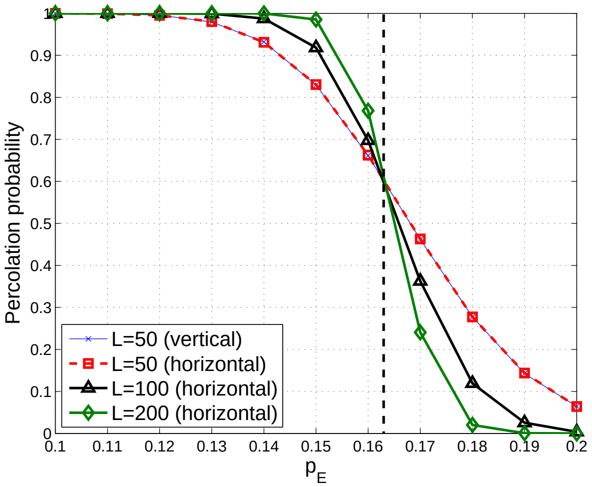


Fig. 4. Percolation threshold for square lattice

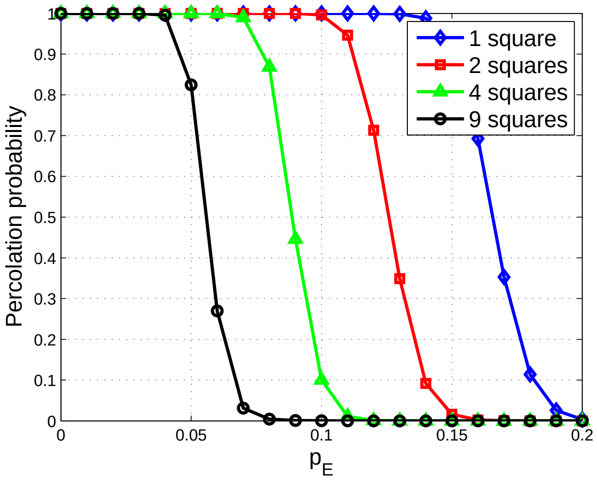


Fig. 5. Percolation threshold versus area

As expected, if the uncertainty in the eavesdroppers is large, no secure communication is possible. If the communication radius is large, and the uncertainty in the location of eavesdroppers is small, the mean degree has an inverse dependence on λ. Hence, it is expected that secure communication will be possible if λ is sufficiently small.

Remark 4. As the intensity of eavesdropper nodes λ takes limiting values,

$$\lim_{r_v\to\infty,\lambda\to 0} \mathbf{E}[\tilde{N}] = \infty \tag{38}$$

$$\lim_{r_v\to\infty,\lambda\to\infty} \mathbf{E}[\tilde{N}] = 0. \tag{39}$$

As the intensity of eavesdroppers (λ) increases, the probability of existence of link decreases, and thus, the mean degree decreases. In the limit of large intensity of eavesdroppers, there is no secure link, almost surely, and thus, the probability that node degree is zero is 1.

We have characterized the lower and upper bounds to the mean degree in a basic Poisson secrecy graph. The above results show that the bounds to mean degree depend crucially on both the radius of uncertainty r_E and the intensity of eavesdropper nodes λ. We will now characterize the pair of values taken by these two parameters for which an infinite connected component exists in the basic Poisson secrecy graph. We will show that an outer bound on the (λ, r_E) region is obtained in terms of the upper bound on the mean degree. We begin by defining the achievable (λ, r_E) region.

Definition 1. *Consider a Poisson secrecy graph with intensity of legitimate nodes 1, radius of communication r_v. The pair (λ, r_E) of the intensity of eavesdroppers and the radius of uncertainty in an eavesdropper's location is achievable if percolation occurs in the corresponding secrecy graph, i.e., if $\theta(\lambda, r_E) = P(|C| = \infty) > 0$.*

A complete characterization of the achievable region requires us to determine the critical pairs (λ_c, r_E^c), which is a difficult problem. In the following theorem, we provide inner and outer bounds for the achievable region. The outer bound is obtained in terms of an upper bound on the mean degree $\mathbf{E}[N^{out}]$.

Theorem 6. *Consider a Poisson secrecy graph G_{λ,r_v,r_E} with density of eavesdroppers λ, radius of uncertainty of the eavesdroppers r_E and radius of communication r_v. Percolation does not occur in the basic Poisson secrecy graph if*

$$\mathbf{E}[N^{out}] < \frac{6\pi}{2\pi + 3\sqrt{3}}, \tag{40}$$

where $\mathbf{E}[N^{out}]$ is given by (33). Further, percolation occurs if

$$\lambda < \frac{1}{L^2(s^*)^2}\left((2L-1)\log(1-e^{-(s^*)^2}) - \log(p_c^{UB})\right), \tag{41}$$

where $L = 7$. p_c^{UB} is an upper bound on site (node) percolation threshold for the square lattice. s^* is chosen as

$$s^* = \underset{s\geq(3+\sqrt{5})r_E/4}{\arg\max} \left(e^{-\lambda L^2 s^2}(1-e^{-s^2})^{2L-1}\right), \tag{42}$$

where $L = 7$. It is assumed that $r_v > \sqrt{5}s^*$.

Proof: The outer bound is obtained by iteratively building the connected component containing the origin and bounding the number of new nodes added at each step. The inner bound is obtained by considering a tiling in $\mathbb{R}^2$ where each tile is mapped to a node in a square lattice. The radius of communication and parameters of the tiling are chosen so that percolation occurs in the square lattice. For details see Appendix D. ■

Thus, we have obtained necessary and sufficient conditions for percolation to occur in the basic Poisson secrecy graph. The outer bound shows that percolation does not occur if the upper bound on the mean degree is smaller than a threshold (≈ 1.642). The inner bound is obtained by assuming a specific structure on the underlying graph and then computing the probability for such a structure to occur. In Section V, the behavior of the inner and outer bounds is explored through numerical results.

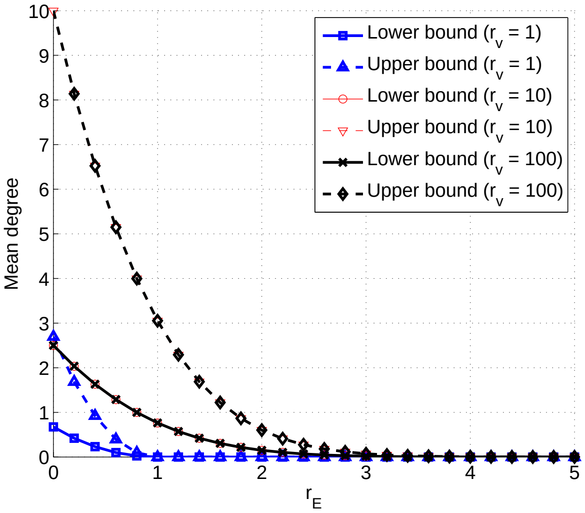


Fig. 6. Mean degree versus r_E in basic Poisson secrecy graph

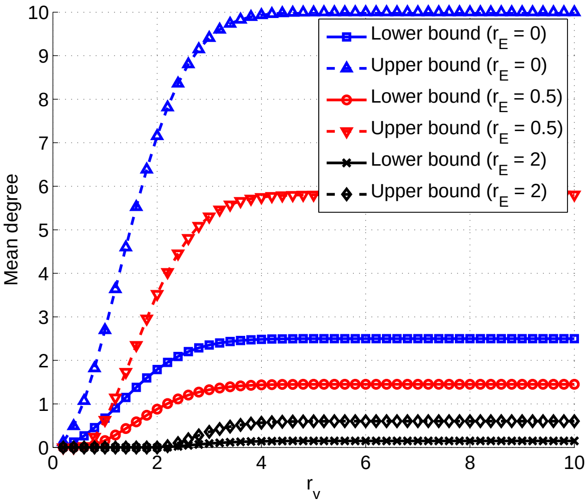


Fig. 7. Mean degree versus r_v in basic Poisson secrecy graph

V. Numerical Results

In this section, we present numerical results for lattice and Poisson secrecy graphs. For lattice secrecy graphs, we present simulation results on the percolation threshold. For Poisson secrecy graphs, we present numerical results on the mean degree, and the inner and outer bounds to the achievable (λ, r_E) region.

A. Lattice secrecy graphs

We estimated the percolation probability $\theta(p_E)$ for $L \times L$ square lattice through Monte-Carlo simulations. Eavesdroppers were placed in the squares randomly and independently, with the probability of a given square having an eavesdropper being p_E. We estimated the probability that a cluster wraps around the periodic boundary conditions. Cluster wrapping can be defined in several ways. We considered the probability of cluster wrapping in the horizontal and vertical directions, denoted by $R_L^{(h)}(p_E)$ and $R_L^{(v)}(p_E)$, respectively [32]. 10^5 random lattices were generated for each estimate. Fig. 4 shows the variation of percolation probability with p_E, for $L = 50, 100, 200$. Notice that in Fig. 4, the percolation probability transitions from a large value (close to 1), to a small value (close to 0). This transition is a typical behavior of percolation probability, and the region of transition becomes narrower as the size of simulated network increases. The percolation threshold can be estimated as the point of intersection of the three curves. Thus, for the square lattice with each eavesdropper located within a square, the percolation threshold is $p_E^c \approx 0.163$. For $p_E = p_E^c$, we obtain $p_{fail} \approx 0.5$ (using (10)) for correlated node failures, whereas for independent node failures, the critical threshold is $p_{fail} \approx 0.41$. Although, a larger proportion of node failures can be tolerated (p_{fail}) in the correlated failure scenario, only 16.3% eavesdroppers can be tolerated in that case.

We now show the effect of the uncertainty in the location of eavesdroppers on the percolation threshold. An eavesdropper may be located anywhere within certain N_S squares. N_S captures the amount of uncertainty in an eavesdropper's location. Fig. 5 shows the variation of percolation probability with p_E for $L = 100$ and $N_S = 1, 2, 4, 9$. As expected, this probability reduces as N_S increases, where the decrease quantifies the effect of uncertainty in location on percolation threshold of secrecy graphs.

B. Poisson secrecy graphs: Mean degree

We now present numerical results for the Poisson secrecy graph. Fig. 6 shows the variation of the upper and lower bounds on the mean degree of the node located at the origin in the basic secrecy graph with r_E, for $r_v = 1, 10, 100$. λ was chosen as 0.1 for which percolation occurs at $r_E = 0$ [8]. For a fixed value of r_v, the upper and lower bounds both decrease to zero as r_E increases. As expected, the bounds on the mean degree increase as the radius of communication r_v increases. The figure shows that the mean degree is severely limited if r_v is small. For the range of values of r_E considered here, the bounds on the mean degree are the same for $r_v = 10$ and $r_v = 100$. i.e., for $r_v \geq 10$, the mean degree is limited by the secrecy constraint.

Fig. 7 shows the variation of the upper and lower bounds on the mean degree with r_v, for $r_E = 0, 0.5, 2$, and $\lambda = 0.1$. As expected, the bounds on the mean degree increase with r_v. The figure shows that the bounds on the mean degree converge to the asymptotic value at $r_v \approx 4$. For $r_E = 2$, the mean degree is zero for $r_v < 2$. When $r_v > 2$, the mean degree increases as r_v increases. The figure shows a dramatic reduction in the mean degree as r_E increases. Further, for small values of r_E, the mean degree increases quickly with r_v and then saturates.

Fig. 8 shows the variation of the upper and lower bounds on the mean degree with λ, for $r_E = 0, 0.5, 2$, and $r_v = 10$. As expected, for fixed values of r_v and r_E, the bounds on the mean degree decrease with an increase in λ. The figure shows that for the range of values of r_E considered here, the mean degree decreases sharply as λ increases from 0 to 0.5, and the decrease is moderate when $\lambda > 0.5$.

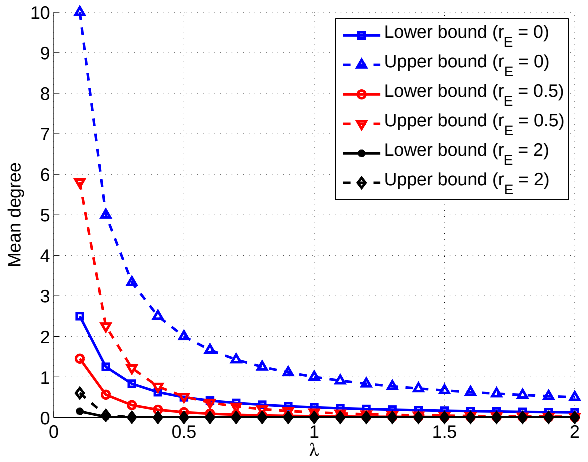


Fig. 8. Mean degree versus λ in basic Poisson secrecy graph

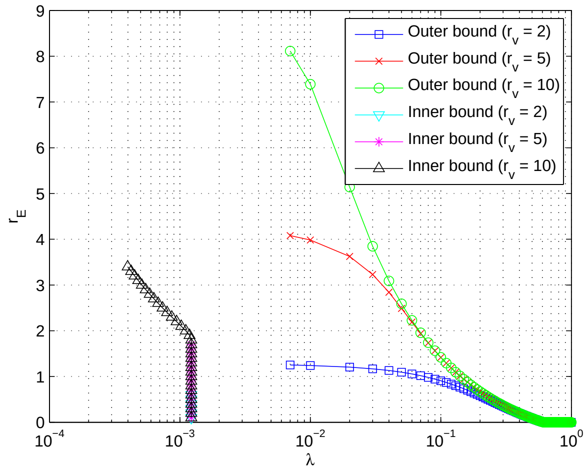


Fig. 9. Inner and outer bounds on achievable (λ, r_E) region

C. Poisson secrecy graphs: Inner and Outer bounds on achievable (λ, r_E) region

The inner and outer bounds on the achievable (λ, r_E) region are shown in Fig. 9. The result in Fig. 9 indicates that perfect secrecy can be attained to the left of the lower bound while cannot be attained to the right of the upper bound. Inner and outer bounds are presented for $r_v = 2, 5, 10$. The outer bound reduces dramatically as r_v is reduced from 10 to 2, showing the need for a large communication radius r_v. Notice that for $r_v = 10$ and small λ, the inner and outer bounds follow a similar trend, although there is a significant gap between the two. The large gap suggests that at least one of the bounds is not tight. The inner bound shows that percolation will occur for large values of r_E as long as λ is sufficiently small. As r_E becomes small, the lower bound remains to the left of $\lambda = 2 \times 10^{-3}$. This is because of the specific structure assumed for deriving the inner bound.

VI. Conclusion

We considered a secrecy graph approach to investigate the effect of eavesdroppers with uncertain locations on network connectivity, which was defined in percolation sense. The communication network and the impact of eavesdroppers on network connectivity were modeled via a secrecy graph. The uncertainty in the location of the eavesdroppers was modeled directly at the network level as correlated failures in the secrecy graph. Bounds on percolation thresholds of square and triangular lattice secrecy graphs were presented. For the Poisson secrecy graph, the degree distribution and mean value of upper and lower bounds on the mean node degree were presented. Inner and outer bounds on the achievable region of pairs of the intensity of eavesdropper nodes and the radius of uncertainty for eavesdroppers locations were obtained. Both analytic and numerical results showed that uncertainty in the location of the eavesdroppers effects connectivity in a secrecy graph dramatically. Future directions include investigating information theoretic secrecy based methods to mitigate the effect of uncertainty in location (CSI) of eavesdroppers, using the secrecy graph approach developed in this paper. In addition, exploring percolation threshold for a fading based model is an important open problem.

Appendix A
Proof of Theorem 3

Probability that the node at origin has n outgoing edges is given by

$$\begin{aligned} P(N^{out} = n) &= \int_{r=0}^{r_v} P(N^{out} = n | R = r) f_R(r) dr \\ &\quad + P(R \geq r_v) P(N^{out} = n | R = r_v), \end{aligned}$$

where

$$\begin{aligned} &P(N^{out} = n | R = r) \\ &= \begin{cases} \mathbf{1}_{\{n=0\}} & \text{if } r \leq r_E, \\ e^{-\pi(r-r_E)^2} \frac{\pi^n (r-r_E)^{2n}}{n!} & \text{if } r > r_E. \end{cases} \end{aligned} \tag{43}$$

and $f_R(r) = 2\pi\lambda r e^{-\pi\lambda r^2}$.

Thus, for $r_v > r_E$,

$$\begin{aligned} &P(N^{out} = n) \\ &= \int_{r=0}^{r_v} P(N^{out} = n | R = r) f_R(r) dr \\ &\quad + e^{-\pi\lambda r_v^2} e^{-\pi(r_v - r_E)^2} \frac{\pi^n (r_v - r_E)^{2n}}{n!}. \end{aligned} \tag{44}$$

The first expression is given by

$$\begin{aligned} &\int_{r=0}^{r_v} P(N^{out} = n | R = r) f_R(r) dr \\ &= 2\pi\lambda \mathbf{1}_{\{n=0\}} \int_{r=0}^{r_E} r e^{-\pi\lambda r^2} dr + \frac{2\pi\lambda\pi^n}{n!} \times \\ &\quad \int_{r=r_E}^{r_v} e^{-\pi(r-r_E)^2} r e^{-\pi\lambda r^2} (r - r_E)^{2n} dr \end{aligned} \tag{45}$$

The second term is given by

$$\begin{aligned}
&\int_{r=r_E}^{r_v} P(N^{out}=n|R=r)f_R(r)dr \\
=\ & \frac{2\pi^{n+1}\lambda}{n!}\int_{r=r_E}^{r_v} r\exp\left(-(1+\lambda)\pi\right. \\
& \left.\left[\left(r-\frac{r_E}{1+\lambda}\right)^2+\frac{r_E^2\lambda}{(1+\lambda)^2}\right]\right)(r-r_E)^{2n}dr \\
=\ & \frac{2\pi^{n+1}\lambda}{n!}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}}\int_{r=r_E}^{r_v} r\exp \\
& \left(-(1+\lambda)\pi\left(r-\frac{r_E}{1+\lambda}\right)^2\right)(r-r_E)^{2n}dr \quad (46)
\end{aligned}$$

Define $t \triangleq \pi(1+\lambda)(r-\frac{r_E}{1+\lambda})^2$, $t_L \triangleq t(r_E)$, $t_U \triangleq t(r_v)$. Then the above integral is given by

$$\begin{aligned}
&\int_{r=r_E}^{r_v} P(N^{out}=n|R=r)f_R(r)dr \\
=\ & \frac{2\pi^{n+1}\lambda}{n!}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}}\int_{t=t_L}^{t_U}\left(\frac{r_E}{1+\lambda}+\sqrt{\frac{t}{\pi(1+\lambda)}}\right)e^{-t} \\
& \frac{\left(\sqrt{\frac{t}{\pi(1+\lambda)}}-\frac{r_E\lambda}{1+\lambda}\right)^{2n}}{2\pi(1+\lambda)\sqrt{\frac{t}{\pi(1+\lambda)}}}dt \\
=\ & \frac{\lambda}{n!}\frac{1}{(1+\lambda)^{n+1}}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}}\int_{t=t_L}^{t_U}\left(\frac{r_E\sqrt{\pi}}{\sqrt{1+\lambda}}+\sqrt{t}\right)e^{-t} \\
& \left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}+\sqrt{t}\right)^{2n}/\sqrt{t}dt \\
=\ & \frac{\lambda}{n!}\frac{1}{(1+\lambda)^{n+1}}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}} \\
& \int_{t=t_L}^{t_U}\left(e^{-t}\left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}+\sqrt{t}\right)^{2n+1}/\sqrt{t}\right. \\
& \quad \left.+r_E\sqrt{\pi(1+\lambda)}e^{-t}\left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}+\sqrt{t}\right)^{2n}/\sqrt{t}\right)dt \\
=\ & \frac{\lambda}{n!}\frac{1}{(1+\lambda)^{n+1}}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}}\int_{t=t_L}^{t_U}\left(e^{-t}\sum_{k=0}^{2n+1}\binom{2n+1}{k}\right. \\
& t^{(k-1)/2}\left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}\right)^{2n+1-k} \\
& \quad +r_E\sqrt{\pi(1+\lambda)}e^{-t}\sum_{k=0}^{2n}\binom{2n}{k}t^{(k-1)/2} \\
& \left.\left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}\right)^{2n-k}\right)dt \\
=\ & \frac{\lambda}{n!}\frac{1}{(1+\lambda)^{n+1}}e^{-\pi\frac{r_E^2\lambda}{1+\lambda}}\left\{\sum_{k=0}^{2n+1}\binom{2n+1}{k}\right. \\
& \left(\Gamma\left(\frac{k+1}{2},\pi(1+\lambda)\left(r_v-\frac{r_E}{1+\lambda}\right)^2\right)\right. \\
& \quad \left.-\Gamma\left(\frac{k+1}{2},\pi(1+\lambda)\left(r_E-\frac{r_E}{1+\lambda}\right)^2\right)\right) \\
& \left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}\right)^{2n+1-k}+r_E\sqrt{\pi(1+\lambda)}\sum_{k=0}^{2n}\binom{2n}{k} \\
& \left(\Gamma\left(\frac{k+1}{2},\pi(1+\lambda)\left(r_v-\frac{r_E}{1+\lambda}\right)^2\right)\right. \\
& \quad \left.-\Gamma\left(\frac{k+1}{2},\pi(1+\lambda)\left(r_E-\frac{r_E}{1+\lambda}\right)^2\right)\right) \\
& \left.\left(-\frac{r_E\lambda\sqrt{\pi}}{\sqrt{1+\lambda}}\right)^{2n-k}\right\} \quad (47)
\end{aligned}$$

The result for $n \geq 1$ is obtained by combining equations (44), (45) and (47). When $n=0$, equations (44) and (45) yield

$$\begin{aligned}
& P(N^{out}=0) \\
=\ & e^{-\pi\lambda r_v^2}e^{-\pi(r_v-r_E)^2}+1-e^{-\pi\lambda r_E^2} \\
& +2\pi\lambda e^{-\pi\frac{\lambda}{1+\lambda}r_E^2}\int_{r=r_E}^{r_v} re^{-\pi(1+\lambda)(r-\frac{r_E}{1+\lambda})^2}dr \quad (48)
\end{aligned}$$

The integral in (48) can be computed as

$$\begin{aligned}
&\int_{r=r_E}^{r_v} re^{-\pi(1+\lambda)(r-\frac{r_E}{1+\lambda})^2}dr \\
=\ & \frac{1}{\pi(1+\lambda)}\left(e^{-\pi(1+\lambda)(\frac{\lambda r_E}{1+\lambda})^2}-e^{-\pi(1+\lambda)(r_v-\frac{r_E}{1+\lambda})^2}\right) \\
& +\frac{\pi}{1+\lambda}\frac{1}{2\sqrt{1+\lambda}}\cdot\left(\mathrm{erf}\left(\sqrt{\pi(1+\lambda)}\frac{\lambda}{1+\lambda}r_E\right)\right. \\
& \left.-\,\mathrm{erf}\left(\sqrt{\pi(1+\lambda)}\left(r_v-\frac{r_E}{1+\lambda}\right)\right)\right) \quad (49)
\end{aligned}$$

which yields the result for $n=0$.

Appendix B
Proof of Theorem 4

Probability that the node at origin has n outgoing edges is given by

$$\begin{aligned}
P(\tilde{N}=n) \ &= \int_{r=0}^{r_v} P(\tilde{N}=n|R=r)f_R(r)dr \\
& \quad +P(R\geq r_v)P(\tilde{N}=n|R=r_v), \quad (50)
\end{aligned}$$

where

$$\begin{aligned}
& P(\tilde{N}=n|R=r) \\
=\ & \begin{cases} \mathbf{1}_{\{n=0\}} & \text{if } r\leq r_E, \\ e^{-\frac{\pi}{4}(r-r_E)^2}\pi^n\frac{(r-r_E)^{2n}}{4^n n!} & \text{if } r>r_E \end{cases} \quad (51)
\end{aligned}$$

and $f_R(r)=2\pi\lambda re^{-\pi\lambda r^2}$.

Note that all the terms in the expression are obtained from the expression of $P(N^{out}=n)$ by replacing π with $\pi/4$ and λ with 4λ and hence the statement of the Theorem holds.

Appendix C
Proof of Theorem 5

Assume that the center of a circular region containing an eavesdropper, which is closest to the origin, is located at a distance R from it. Using the law of total expectation, we obtain

$$\begin{aligned}\mathbf{E}[\tilde{N}] &= \mathop{\mathbf{E}}_{R}[\mathbf{E}[\tilde{N}|R]] && (52)\\ &\overset{a}{=} \mathop{\mathbf{E}}_{R}[\pi((\min(r_v, R) - r_E)^+/2)^2], && (53)\end{aligned}$$

where (*a*) holds because for a fixed R, the mean number of legitimate nodes in the circle $C(\mathbf{0}, (\min(r_v, R) - r_E)^+/2)$ are $\pi((\min(r_v, R) - r_E)^+/2)^2$ (the intensity of the legitimate nodes is assumed to be 1). The distribution of R is $f_R(r) = 2\pi\lambda r e^{-\pi\lambda r^2}$. Thus,

$$\begin{aligned}\mathbf{E}[\tilde{N}] &= \frac{\pi}{4}\left(\int_{r_E}^{r_v} (r - r_E)^2 f_R(r)dr \right.\\ &\quad \left. + \int_{r_v}^{\infty} (r_v - r_E)^2 f_R(r)dr\right)\\ &= \frac{\pi}{4}\left(-(r_v - r_E)^2 e^{-\lambda\pi r_v^2}\right.\\ &\quad + \frac{1}{\lambda\pi}\left(e^{-\lambda\pi r_E^2} - e^{-\lambda\pi r_v^2}\right)\\ &\quad \left. -2r_E\int_{r_E}^{r_v} e^{-\lambda\pi r^2}dr + (r_v - r_E)^2 e^{-\lambda\pi r_v^2}\right)\\ &= \frac{1}{4\lambda}\left(e^{-\lambda\pi r_E^2} - e^{-\lambda\pi r_v^2}\right)\\ &\quad -\frac{\pi r_E}{4\sqrt{\lambda}}\left(\mathrm{erf}(\sqrt{\lambda\pi}r_v) - \mathrm{erf}(\sqrt{\lambda\pi}r_E)\right). && (54)\end{aligned}$$

For the upper bound, we consider all the nodes in the circle $C(\mathbf{0}, (\min(r_v, R) - r_E)^+)$. Therefore,

$$\begin{aligned}\mathbf{E}[N^{out}] &= \mathop{\mathbf{E}}_{R}[\mathbf{E}[N^{out}|R]] && (55)\\ &= \mathop{\mathbf{E}}_{R}[\pi((\min(r_v, R) - r_E)^+)^2] && (56)\\ &= 4\ \mathbf{E}[\tilde{N}] && (57)\end{aligned}$$

APPENDIX D
PROOF OF THEOREM 6

First consider the outer bound. We obtain a necessary condition for percolation in the directed Poisson secrecy graph. If percolation does not occur in this graph, it cannot occur in the basic Poisson secrecy graph either, and hence, an outer bound on the achievable (λ, r_E) region is obtained. The proof for the outer bound closely follows the analysis in [33]. Let C_0 denote the component containing the origin. Consider a sequence of pair of sets (D_t, L_t). At step t, D_t is the set of points that belong to C_0, such that all neighbors of points in D_t also belong to C_0. L_t is the set of points which belong to C_0 but whose neighbors have not been explored. We start with the origin, and initialize $D_0 = \{\phi\}$ and $L_0 = \{\mathbf{0}\}$. The process terminates at step t if $L_t = \{\phi\}$, otherwise a point $X_t \in L_t$ is chosen and we set

$$D_{t+1} = D_t \cup X_t \qquad (58)$$

$$L_{t+1} = N_t \cup L_t \qquad (59)$$

where N_t is the set of neighbors of X_t that are not the neighbors of any points in D_t. Since N_t new nodes are added to the set D_{t-1} at time t, the size of set D_t can be upper bounded as

$$|D_t| - 1 \leq \sum_{i=0}^{t-2} |N_i| \qquad (60)$$

The new nodes belong to a region of area at most

$$\left(\frac{\pi}{3} + \frac{\sqrt{3}}{2}\right)((\min(r_v, R_{t-1}) - r_E)^+)^2 \qquad (61)$$

where R_{t-1} is the distance to the eavesdropper closest to X_{t-1}. Let $Z_0, Z_1, \dots$ be independent Poisson random variables with mean

$$\begin{aligned}\mathbf{E}[Z_0] &= \pi\mathbf{E}[((\min(r_v, R_{t-1}) - r_E)^+)^2] && (62)\\ \mathbf{E}[Z_i] &= \left(\frac{\pi}{3} + \frac{\sqrt{3}}{2}\right)\mathbf{E}[((\min(r_v, R_{t-1}) - r_E)^+)^2]\\ &= \left(\frac{1}{3} + \frac{\sqrt{3}}{2\pi}\right)\mathbf{E}[N^{out}] \doteq b && (63)\end{aligned}$$

The probability that C_0 contains at least k elements can be upper bounded as

$$P(|C_0| \geq k) \leq P(\sum_{i=0}^{k-2} Z_i \geq k - 1) \qquad (64)$$

Percolation does not occur if $\lim_{k\to\infty} P(|C_0| \geq k) = 0$ which occurs if $b < 1$, i.e.,

$$\mathbf{E}[N^{out}] < \frac{6\pi}{2\pi + 3\sqrt{3}} \qquad (65)$$

For the lower bound, consider a tiling in $\mathbb{R}^2$ using square tiles where edge length of each tile is s. A frame consists of $L \times L$ tiles. We map each frame to a node in a square lattice. Consider tiles A and B marked in Fig. 10. The maximum distance between a node in tile A and a node in tile B is $\sqrt{5}s$. Therefore, any node in tile A can communicate securely with any node in tile B if there is no eavesdropper within $(L-1)/2$ tiles on each side, with $L \geq 7$. We choose $L = 7$ to define the frames. Assume that the center of a circular region containing an eavesdropper is present at the boundary of a frame. A node in the center tile of the frame can communicate securely with a node in a neighboring tile only if

$$s \geq \left(\frac{3 + \sqrt{5}}{4}\right) r_E. \qquad (66)$$

Now, consider the square lattice obtained by mapping each frame to a node in the lattice. A node exists in the lattice if the corresponding frame has no eavesdropper and a legitimate node is present in each of the shaded tiles in Fig. 10. Thus, the site probability for the square lattice is given by

$$p = e^{-\lambda L^2 s^2}(1 - e^{-s^2})^{2L-1}. \qquad (67)$$

We maximize p by choosing the optimal value of s,

$$s^* = \mathop{\arg\max}_{s \geq (3+\sqrt{5})r_E/4} \left(e^{-\lambda L^2 s^2}(1 - e^{-s^2})^{2L-1}\right). \qquad (68)$$

and denote the optimal value of p by p^*. Percolation occurs in the square lattice, and hence, in the Poisson secrecy graph,

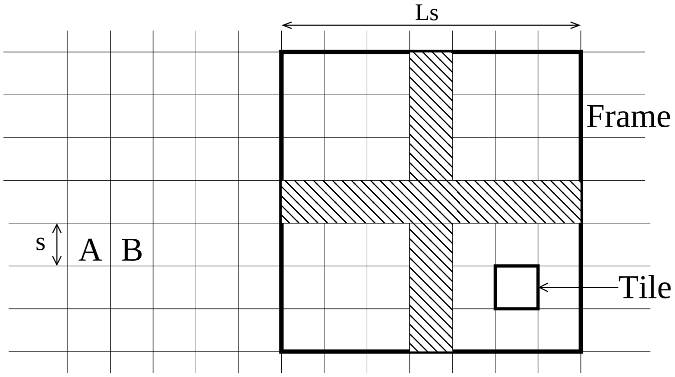


Fig. 10. Tiling in $\mathbb{R}^2$ for achievable (λ, r_E) region

if $p^* > p_c^{UB}$, where $p_c^{UB} = 0.679492$ is an upper bound on the percolation threshold for the square lattice [33]. Thus, percolation occurs in the Poisson secrecy graph if

$$\lambda < \frac{1}{L^2(s^*)^2}\left((2L-1)\log(1-e^{-(s^*)^2}) - \log(p_c^{UB})\right). \tag{69}$$

References

[1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[4] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[5] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[6] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[7] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3801–3827, Aug. 2010.

[8] M. Haenggi, "The secrecy graph and some of its properties," in *Proceedings of IEEE International Symposium on Information Theory*, July 2008, pp. 539–543.

[9] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *IEEE International Conference on Communications Systems*, Nov. 2008, pp. 974–979.

[10] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *Submitted to IEEE Transactions on Information Theory*, 2010, submitted. Also available at [arXiv.org:0908.0898].

[11] Y. Liang, V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proceedings of IEEE International Symposium on Information Theory*, 2009.

[12] Y. Liang, G. Kramer, H. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, 2009.

[13] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Transactions on Information Theory*, submitted. Also available at [arXiv:0910.3033v1].

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[15] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," *IEEE Transactions on Information Theory*, submitted. Also available at [arXiv:1007.4801v1].

[16] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, Mar 2000.

[17] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proceedings of IEEE International Symposium on Information Theory*, 2010, pp. 2627–2631.

[18] E. N. Gilbert, "Random plane networks," *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, no. 4, pp. 533–543, Dec 1961.

[19] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[20] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," *IEEE Transactions on Information Theory*, submitted. Also available at [arXiv:0907.5388].

[21] S. R. Broadbent and J. M. Hammersley, "Percolation processes. I. Crystals and Mazes," in *Proceedings of the Cambridge Philosophical Society*, vol. 53, Jul. 1957, pp. 629–641.

[22] B. Bollobás, *Random Graphs*. Cambridge University Press, 2001.

[23] P. Erdős and A. Réyni, "On the evolution of random graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[24] M. Penrose, *Random Geometric Graphs*. Oxford: Oxford University Press, 2003.

[25] M. Franceschetti and R. Meester, *Random Networks for Communication: From Statistical Physics to Information Systems*. Cambridge, UK: Cambridge University Press, 2007.

[26] F. Baccelli and B. Blaszczyszyn, *Stochastic Geometry and Wireless Networks*. NoW Publishers, 2009.

[27] R. Meester and R. Roy, *Continuum Percolation*. Cambridge, UK: Cambridge University Press, 1996.

[28] G. Grimmett, *Percolation*. Berlin: Springer-Verlag, 1999.

[29] J. Wierman, "Bond percolation on honeycomb and triangular lattices," *Advances in Applied Probability*, pp. 298–313, 1981.

[30] M. F. Sykes and J. W. Essam, "Exact critical percolation probabilities for site and bond problems in two dimensions," *Journal of Mathematical Physics*, vol. 5, no. 8, pp. 1117–1127, 1964.

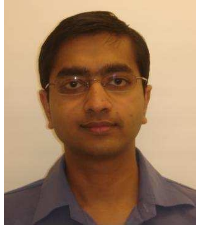
[31] Y. Y. Tarasevich and S. C. van der Marck, "An investigation of site-bond percolation on many lattices," *International Journal of Modern Physics C*, vol. 10, pp. 1193–1204, 1999.

[32] M. E. J. Newman and R. M. Ziff, "Fast Monte Carlo algorithm for site or bond percolation," *Physics Review E*, vol. 64, no. 1, p. 016706, Jun 2001.

[33] B. Bollobás and O. Riordan, *Percolation*. Cambridge University Press, 2006.

Satashu Goel (S'04 - M'10) received the B.Tech. degree in Electrical Engineering in 2003 from the Indian Institute of Technology Delhi, India, and the M.S. and Ph.D. degrees in 2007 and 2010, respectively from Carnegie Mellon University, Pittsburgh, PA, USA, both in Electrical and Computer Engineering.

He is currently a Senior Engineer at Qualcomm Inc., San Diego, CA. His research interests include cross-layer optimization, information theory, coding for communications systems, and physical layer security. Dr. Goel received the Best Paper award from the Communication Theory Symposium in IEEE International Conference on Communications (ICC) in 2009.



Vaneet Aggarwal (S'08 - M'11) received the B.Tech. degree in 2005 from the Indian Institute of Technology, Kanpur, India, and the M.A. and Ph.D. degrees in 2007 and 2010, respectively from Princeton University, Princeton, NJ, USA, all in Electrical Engineering.

He is currently Senior Member of Technical Staff at AT&T Labs-Research, Florham Park, NJ. His research interests are in applications of information and coding theory to wireless systems and quantum error correction. Dr. Aggarwal was the recipient of Princeton University's Porter Ogden Jacobus Honorific Fellowship in 2009.

Aylin Yener (S'91 - M'00) received her two B.Sc. degrees, with honors, in Electrical and Electronics Engineering, and in Physics, from Boğaziçi University, Istanbul, Turkey, in 1991, and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from Rutgers University, NJ, in 1994 and 2000, respectively. During her Ph.D. studies, she was with Wireless Information Network Laboratory (WINLAB) in the Department of Electrical and Computer Engineering at Rutgers University, NJ. From September 2000 to December 2001, she was with the Electrical Engineering and Computer Science Department, Lehigh University, PA, where she was a P.C. Rossin Assistant Professor. In January 2002, she joined the faculty of The Pennsylvania State University, University Park, where she was an Assistant Professor, then Associate Professor, and is currently Professor of Electrical Engineering. During the academic year 2008-2009, she was a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford CA. Her research interests are in information theory, communication theory and network science, with emphasis on fundamental limits of wireless ad hoc networks and information theoretic security.

Dr. Yener received the NSF CAREER award in 2003 and is a member of the team that received the DARPA Information Theory for Mobile Ad Hoc Networks (ITMANET) Young Investigator Team Award in 2006. In 2010, she received the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award, and the Best Paper award from the Communication Theory Symposium in IEEE International Conference on Communications (ICC). Her service to IEEE includes membership in the Technical Program Committees of various annual conferences since 2002. She chaired the Communications Track in the Asilomar Conference on Signals, Systems and Computers in 2005 and in 2008. She served as the Technical Program Co-Chair for the Communication Theory Symposium of the IEEE International Conference on Communications (ICC) 2009 and for the Wireless Communications Symposium of the IEEE International Conference on Communications (ICC) 2008. She currently serves as an editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and for the IEEE TRANSACTIONS ON COMMUNICATIONS. Her service to the IEEE Information Theory Society includes chairing the Student Committee since September 2007. She is the cofounder of the Annual School of Information Theory in North America, and served as the general Co-Chair of the First Annual School of Information Theory that was held at Penn State University, University Park, in June 2008, the Second Annual School of Information Theory at Northwestern University, Evanston, IL, in August 2009, and the Third Annual School of Information Theory at University of Southern California, Los Angeles, in August 2010.

Robert Calderbank (M'89 - SM'97 - F'98) received the B. Sc degree in 1975 from Warwick University, England, the M. Sc degree in 1976 from Oxford University, England, and the Ph. D. degree in 1980 from the California Institute of Technology, all in mathematics.

Dr. Calderbank is Dean of Natural Sciences at Duke University. He was previously Professor of Electrical Engineering and Mathematics at Princeton University where he directed the Program in Applied and Computational Mathematics. Prior to joining Princeton in 2004, he was Vice President for Research at AT&T, responsible for directing the first industrial research lab in the world where the primary focus is data at scale. At the start of his career at Bell Labs, innovations by Dr. Calderbank were incorporated in a progression of voiceband modem standards that moved communications practice close to the Shannon limit. Together with Peter Shor and colleagues at AT&T Labs he showed that good quantum error correcting codes exist and developed the group theoretic framework for quantum error correction. He is a co-inventor of space-time codes for wireless communication, where correlation of signals across different transmit antennas is the key to reliable transmission.

Dr. Calderbank served as Editor in Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY from 1995 to 1998, and as Associate Editor for Coding Techniques from 1986 to 1989. He was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2006 to 2008. Dr. Calderbank was honored by the IEEE Information Theory Prize Paper Award in 1995 for his work on the $\mathbb{Z}_4$ linearity of Kerdock and Preparata Codes (joint with A.R. Hammons Jr., P.V. Kumar, N.J.A. Sloane, and P. Sole), and again in 1999 for the invention of space-time codes (joint with V.Tarokh and N. Seshadri). He received the 2006 IEEE Donald G. Fink Prize Paper Award and the IEEE Millennium Medal, and was elected to the US National Academy of Engineering in 2005.