# Percolation and Connectivity in the Intrinsically Secure Communications Graph

Pedro C. Pinto, *Member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

***Abstract*—The ability to exchange secret information is critical to many commercial, governmental, and military networks. The intrinsically secure communications graph ($i\mathcal{S}$-graph) is a random graph which describes the connections that can be securely established over a large-scale network, by exploiting the physical properties of the wireless medium. This paper aims to characterize the global properties of the $i\mathcal{S}$-graph in terms of 1) percolation on the infinite plane, and 2) full connectivity on a finite region. First, for the Poisson $i\mathcal{S}$-graph defined on the infinite plane, the existence of a phase transition is proven, whereby an unbounded component of connected nodes suddenly arises as the density of legitimate nodes is increased. This shows that long-range secure communication is still possible in the presence of eavesdroppers. Second, full connectivity on a finite region of the Poisson $i\mathcal{S}$-graph is considered. The exact asymptotic behavior of full connectivity in the limit of a large density of legitimate nodes is characterized. Then, simple, explicit expressions are derived in order to closely approximate the probability of full connectivity for a finite density of legitimate nodes. These results help clarify how the presence of eavesdroppers can compromise long-range secure communication.**

***Index Terms*—Connectivity, percolation, physical-layer security, stochastic geometry, wireless networks.**

## I. Introduction

CONTEMPORARY security systems for wireless networks are based on cryptographic primitives that generally ignore two key factors: 1) the physical properties of the underlying communication channels, and 2) the spatial configuration of both the legitimate and malicious nodes. These two factors are important since they affect the propagation channels between the nodes, which in turn determine the fundamental secrecy potential of a wireless network. In fact, the randomness introduced both by the physics of the wireless medium and by the spatial location of the nodes can be leveraged to strengthen the overall security of the communications infrastructure.[1]

Manuscript received June 15, 2010; revised July 17, 2011; accepted September 09, 2011. Date of current version February 29, 2012. This work was supported in part by the Portuguese Science and Technology Foundation under Grant SFRH-BD-17388-2004, the MIT Institute for Soldier Nanotechnologies, the Office of Naval Research under Presidential Early Career Award for Scientists and Engineers N00014-09-1-0435, and the National Science Foundation under Grant ECS-0636519.

The authors are with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: pedro.pinto@epfl.ch; moewin@mit.edu).

Communicated by M. Franceschetti, Associate Editor for Communication Networks.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2011.2173726

[1]In the literature, the term "security" typically encompasses three different characteristics: *secrecy* (or privacy), *integrity*, and *authenticity*. This paper does not consider the issues of integrity or authenticity, and the terms "secrecy" and "security" are used interchangeably.

The basis for information-theoretic security, which builds on the notion of perfect secrecy [1], was laid in [2] and later in [3] and [4]. More recently, there has been a renewed interest in information-theoretic security over wireless channels, from the perspective of space-time communications [5], multiple-input multiple-output communications [6]–[10], eavesdropper collusion [11], [12], cooperative relay networks [13], fading channels [14]–[18], strong secrecy [19], [20], secret key agreement [21]–[25], code design [26]–[28], among other topics. A fundamental limitation of this literature is that it only considers scenarios with a small number of nodes. To account for large-scale networks composed of multiple legitimate and eavesdropper nodes, *secrecy graphs* were first introduced in [29] from a geometrical perspective, and in [30] from an information-theoretic perspective. The local connectivity of secrecy graphs was extensively characterized in [31], [32], while the scaling laws of the secrecy capacity were presented in [33] and [34].

Percolation theory studies the existence of phase transitions in random graphs, whereby an infinite cluster of connected nodes suddenly arises as some system parameter is varied. Various percolation models have been considered in the literature. The Poisson Boolean model was introduced in [35], which derived the first bounds on the critical density, and started the field of continuum percolation. The Poisson random connection model was introduced and analyzed in [36]. The Poisson nearest neighbor model was considered in [37]. The signal-to-interference-plus-noise ratio (SINR) model was characterized in [38]. A comprehensive study of the various models and results in continuum percolation can be found in [39].

The connectivity of large but finite networks has also received attention in the literature. The asymptotic behavior of partial connectivity of the Poisson Boolean model restricted to a finite box was studied in [40]. The asymptotic full connectivity of the same model was analyzed in [41] and [42], which obtained the rate of growth of the radius that ensures full connectivity. The asymptotic full connectivity in finite nearest neighbor networks was considered in [43] and [44].

In this paper, we characterize long-range secure connectivity in wireless networks by considering the *intrinsically secure communications graph* ($i\mathcal{S}$-graph). The $i\mathcal{S}$-graph describes the connections that can be established with information-theoretic security over a large-scale network. While in [31] and [32], we characterized the *local* (i.e., single-hop) properties of the $i\mathcal{S}$-graph, including the degrees and maximum rate of a typical node with respect to its neighbors, here we focus on the *global* (i.e., multihop) properties of the $i\mathcal{S}$-graph. The main contributions of this paper are as follows.

1) *Percolation in the $i\mathcal{S}$-graph:* We prove the existence of a phase transition in the Poisson $i\mathcal{S}$-graph defined on the

TABLE I
NOTATION AND SYMBOLS

| Symbol | Usage |
|---|---|
| $\mathbb{E}\{\cdot\}$ | Expectation operator |
| $\mathbb{P}\{\cdot\}$ | Probability operator |
| $H(X)$ | Entropy of $X$ |
| $\Pi_\ell = \{x_i\}, \Pi_\mathrm{e} = \{e_i\}$ | Poisson processes of legitimate nodes and eavesdroppers |
| $\lambda_\ell, \lambda_\mathrm{e}$ | Spatial densities of legitimate nodes and eavesdroppers |
| $\Pi\{\mathcal{R}\}$ | Number of nodes of process $\Pi$ in region $\mathcal{R}$ |
| $N_\mathrm{in}, N_\mathrm{out}$ | In-degree and out-degree of a node |
| $\mathcal{B}_x(\rho)$ | Ball centered at $x$ with radius $\rho$ |
| $\mathcal{D}(a,b)$ | Annular region between radiuses $a$ and $b$, centered at the origin |
| $\mathbb{A}\{\mathcal{R}\}$ | Area of region $\mathcal{R}$ |
| $\mathcal{K}^\diamond(x)$ | Out, in, weak, or strong component of node $x$ |
| $p_\infty^\diamond$ | Percolation probability associated with component $\mathcal{K}^\diamond(0)$ |
| $\lambda_\mathrm{c}^\diamond$ | Critical density associated with component $\mathcal{K}^\diamond(0)$ |
| $\#S$ | Number of elements in the set $S$ |
| $\mathcal{N}(\mu, \sigma^2)$ | Gaussian distribution with mean $\mu$ and variance $\sigma^2$ |

infinite plane, whereby an unbounded component of connected nodes suddenly arises as we increase the density of legitimate nodes. This shows that long-range communication is still possible in a wireless network when a secrecy constraint is present.

2) *Full connectivity in the $i\mathcal{S}$-graph:* We analyze secure full connectivity on a finite region of the Poisson $i\mathcal{S}$-graph. We characterize the exact asymptotic behavior of full connectivity in the limit of a large density of legitimate nodes. Then, we obtain simple, explicit expressions that closely approximate the probability of full connectivity for a finite density of legitimate nodes.

This paper is organized as follows. Section II describes the system model. Section III characterizes continuum percolation in the Poisson $i\mathcal{S}$-graph. Section IV analyzes full connectivity in the Poisson $i\mathcal{S}$-graph. Section V concludes the paper and summarizes important findings.

## II. System Model

We start by describing our system model and defining our measures of secrecy. The notation and symbols are summarized in Table I, at the top of the page.

### A. Wireless Propagation Characteristics

Given a transmitter node $x_i \in \mathbb{R}^d$ and a receiver node $x_j \in \mathbb{R}^d$, we model the received power $P_\mathrm{rx}(x_i, x_j)$ associated with the wireless link $\overrightarrow{x_i x_j}$ as

$$P_\mathrm{rx}(x_i, x_j) = P \cdot g(x_i, x_j) \tag{1}$$

where $P$ is the transmit power, and $g(x_i, x_j)$ is the power gain of the link $\overrightarrow{x_i x_j}$. The gain $g(x_i, x_j)$ is considered constant (quasi-static) throughout the use of the communications channel, corresponding to channels with a large coherence time. Furthermore, the function $g$ is assumed to satisfy the following conditions, which are typically observed in practice: 1) $g(x_i, x_j)$ depends on $x_i$ and $x_j$ only through the link length $|x_i - x_j|$;[2] 2) $g(r)$ is continuous and strictly decreasing with $r$; and 3) $\lim_{r\to\infty} g(r) = 0$.

[2]With abuse of notation, we can write $g(r) \triangleq g(x_i, x_j)|_{|x_i - x_j| \to r}$.

### B. $i\mathcal{S}$-Graph

Consider a wireless network where the legitimate nodes and the potential eavesdroppers are randomly scattered in space, according to some point processes. The $i\mathcal{S}$-graph is a convenient representation of the links that can be established with information-theoretic security on such network. In the following, we introduce a precise definition of the $i\mathcal{S}$-graph, based on the notion of strong secrecy.

*Definition 2.1 ($i\mathcal{S}$-Graph [31]):* Let $\Pi_\ell = \{x_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of legitimate nodes, and $\Pi_\mathrm{e} = \{e_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of eavesdroppers. The *$i\mathcal{S}$-graph* is the directed graph $G = \{\Pi_\ell, \mathcal{E}\}$ with vertex set $\Pi_\ell$ and edge set

$$\mathcal{E} = \{\overrightarrow{x_i x_j} : \mathcal{R}_\mathrm{s}(x_i, x_j) > \varrho\} \tag{2}$$

where $\varrho$ is a threshold representing the prescribed infimum secrecy rate for each communication link; and $\mathcal{R}_\mathrm{s}(x_i, x_j)$ is the maximum secrecy rate (MSR) of the link $\overrightarrow{x_i x_j}$, given by

$$\mathcal{R}_\mathrm{s}(x_i, x_j) = \left[\log_2\left(1 + \frac{P_\mathrm{rx}(x_i, x_j)}{\sigma_\ell^2}\right) - \log_2\left(1 + \frac{P_\mathrm{rx}(x_i, e^*)}{\sigma_\mathrm{e}^2}\right)\right]^+ \tag{3}$$

in bits per complex dimension, where $[x]^+ = \max\{x, 0\}$; $\sigma_\ell^2$, $\sigma_\mathrm{e}^2$ are the noise powers of the legitimate users and eavesdroppers, respectively, and $e^* = \arg\max_{e_k \in \Pi_\mathrm{e}} P_\mathrm{rx}(x_i, e_k)$.[3]

This definition presupposes that the eavesdroppers are not allowed to *collude* (i.e., they cannot exchange or combine information), and therefore, only the eavesdropper with the strongest received signal from $x_i$ determines the MSR between $x_i$ and $x_j$. The effect of eavesdropper collusion on the local connectivity of the $i\mathcal{S}$-graph is analyzed in [32].

In the remainder of this paper, we consider that the noise powers of the legitimate users and eavesdroppers are equal, i.e., $\sigma_\ell^2 = \sigma_\mathrm{e}^2 = \sigma^2$. In such case, we can combine (1)–(3) to obtain the following edge set:

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : g(|x_i - x_j|) > 2^\varrho g(|x_i - e^*|) + \frac{\sigma^2}{P}(2^\varrho - 1)\right\} \tag{4}$$

[3]This definition uses *strong secrecy* as the condition for information-theoretic security. See [19] and [31] for more details.

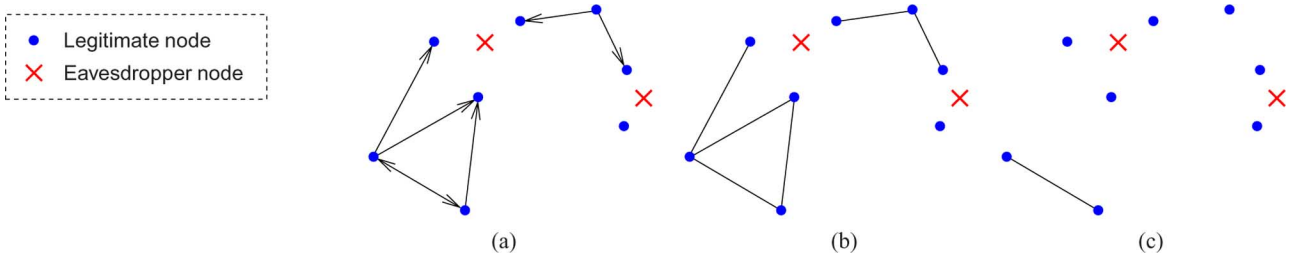


Fig. 1. Three different types of $i\mathcal{S}$-graphs on $\mathbb{R}^2$, considering that $\varrho = 0$ and $\sigma_\ell^2 = \sigma_\ell^2 = \sigma_e^2$ (a) $i\mathcal{S}$-graph $G$ (directed). (b) Weak $i\mathcal{S}$-graph $G^{\text{weak}}$. (c) Strong $i\mathcal{S}$-graph $G^{\text{strong}}$.

where $e^* = \arg\min_{e_k \in \Pi_e} |x_i - e_k|$ is the eavesdropper closest to the transmitter $x_i$. Note that the particular case of $\varrho = 0$ corresponds to considering the *existence* of secure links, in the sense that an edge $\overrightarrow{x_i x_j}$ is present iff $\mathcal{R}_s(x_i, x_j) > 0$. In such case, the edge set in (4) simplifies to

$$\mathcal{E} = \left\{ \overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|, \ e^* = \arg\min_{e_k \in \Pi_e} > |x_i - e_k| \right\} \tag{5}$$

which corresponds to the geometrical model proposed in [29]. Fig. 1(a) shows an example of such an $i\mathcal{S}$-graph on $\mathbb{R}^2$.

The spatial location of the legitimate and eavesdropper nodes can be modeled either deterministically or stochastically. In many cases, the node positions are unknown to the network designer *a priori*, so they may be treated as uniformly random according to a Poisson point process [45]–[47].

*Definition 2.2 (Poisson $i\mathcal{S}$-Graph):* The Poisson $i\mathcal{S}$-graph is an $i\mathcal{S}$-graph where $\Pi_\ell$, $\Pi_e \subset \mathbb{R}^d$ are mutually independent, homogeneous Poisson point processes with densities $\lambda_\ell$ and $\lambda_e$, respectively.

In the remainder of this paper (unless otherwise indicated), we focus on Poisson $i\mathcal{S}$-graphs in $\mathbb{R}^2$.

## III. Percolation in the Poisson $i\mathcal{S}$-Graph

Percolation theory studies the behavior of the connected components in random graphs. Typically, a continuum percolation model consists of an underlying point process defined on the infinite plane, and a rule that describes how connections are established between the nodes [39]. A main property of all percolation models is that they exhibit a *phase transition* as some parameter is varied. If this parameter is the density $\lambda$ of nodes, then the phase transition occurs at some critical density $\lambda_c$. When $\lambda < \lambda_c$, denoted as the *subcritical phase*, all the clusters are a.s. bounded.[4] When $\lambda > \lambda_c$, denoted as the *supercritical phase*, the graph exhibits a.s. an unbounded cluster of nodes, or in other words, the graph *percolates*.

Percolation theory plays an important role in the study of connectivity in multihop wireless networks, where the formation of an infinite component of connected nodes is desirable for communication over arbitrarily long distances. In the literature, percolation—and therefore long-range communication—were shown to occur in various important models, including the Boolean model [35], the random connection model [36], the nearest neighbor model [37], and the SINR model [38].

[4]We say that an event occurs "almost surely" (a.s.) if its probability is equal to one.

In this section, we focus on the $i\mathcal{S}$-graph model, and show that long-range communication with information-theoretic security is feasible in the presence of eavesdroppers. The mathematical characterization of the $i\mathcal{S}$-graph presents two challenges: 1) the $i\mathcal{S}$-graph is a directed graph, which leads to the study of *directed percolation*; and 2) the $i\mathcal{S}$-graph exhibits dependences between the state of different edges, which leads to the study of *dependent percolation*. We start by introducing some definitions, then present and prove the main theorem, and finally illustrate the percolation phenomenon with various simulation results.

### A. Definitions

*Graphs:* As before, we use $G = \{\Pi_\ell, \mathcal{E}\}$ to denote the (directed) $i\mathcal{S}$-graph with vertex set $\Pi_\ell$ and edge set given in (2). In addition, we define two undirected graphs: the *weak $i\mathcal{S}$-graph* $G^{\text{weak}} = \{\Pi_\ell, \mathcal{E}^{\text{weak}}\}$, where

$$\mathcal{E}^{\text{weak}} = \{\overline{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho \vee \mathcal{R}_s(x_j, x_i) > \varrho\}$$

and the *strongi$\mathcal{S}$-graph* $G^{\text{strong}} = \{\Pi_\ell, \mathcal{E}^{\text{strong}}\}$, where

$$\mathcal{E}^{\text{strong}} = \{\overline{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho \wedge \mathcal{R}_s(x_j, x_i) > \varrho\}.$$

The graph $G^{\text{weak}}$ represents the links where secure *unidirectional* communication is possible with an MSR greater than $\varrho$. The graph $G^{\text{strong}}$, on the other hand, represents the links where secure *bidirectional* communication is possible with an MSR greater than $\varrho$. The various types of $i\mathcal{S}$-graphs are illustrated in Fig. 1.

*Graph Components:* While the notion of "component" is unambiguous in undirected graphs, some subtleties arise in directed graphs. Specifically, the notion of component is not clear in a directed graph, because even if node $x$ can reach node $y$ through a sequence of directed edges, it does not imply $y$ can reach $x$. We can, however, generalize the notion of component associated with undirected graphs by defining four different graph components for the $i\mathcal{S}$-graph.

We use the notation $x \overset{G}{\rightarrow} y$ to represent a path from node $x$ to node $y$ in a directed graph $G$, and $x \overset{G^*}{—} y$ to represent a path between node $x$ and node $y$ in an undirected graph $G^*$. We define four components

$$\mathcal{K}^{\text{out}}(x) \triangleq \{y \in \Pi_\ell : \exists\, x \overset{G}{\rightarrow} y\} \tag{6}$$

$$\mathcal{K}^{\text{in}}(x) \triangleq \{y \in \Pi_\ell : \exists\, y \overset{G}{\rightarrow} x\} \tag{7}$$

$$\mathcal{K}^{\text{weak}}(x) \triangleq \{y \in \Pi_\ell : \exists\, x \overset{G^{\text{weak}}}{—} y\} \tag{8}$$

$$\mathcal{K}^{\text{strong}}(x) \triangleq \{y \in \Pi_\ell : \exists\, x \overset{G^{\text{strong}}}{—} y\}. \tag{9}$$

From these definitions, it is clear that for a given realization of $\Pi_\ell$ and $\Pi_e$, the following properties hold for any $x$: [5]

$$\mathcal{K}^{\text{strong}}(x) \subseteq \mathcal{K}^{\text{out}}(x) \subseteq \mathcal{K}^{\text{weak}}(x) \tag{10}$$

$$\mathcal{K}^{\text{strong}}(x) \subseteq \mathcal{K}^{\text{in}}(x) \subseteq \mathcal{K}^{\text{weak}}(x). \tag{11}$$

*Percolation Probabilities:* To study the percolation in the $i\mathcal{S}$-graph, it is useful to define percolation probabilities associated with the four graph components. Specifically, let $p_\infty^{\text{out}}$, $p_\infty^{\text{in}}$, $p_\infty^{\text{weak}}$, and $p_\infty^{\text{strong}}$, respectively, be the probabilities that the in, out, weak, and strong components containing node $x = 0$ have an infinite number of nodes, i.e.[6]

$$p_\infty^\diamond(\lambda_\ell, \lambda_e, \varrho) \triangleq \mathbb{P}\{|\mathcal{K}^\diamond(0)| = \infty\}$$

where $\diamond \in \{\text{out}, \text{in}, \text{weak}, \text{strong}\}$.[7] Our goal is to study the properties and behavior of these percolation probabilities.

### B. Main Result

We now investigate the percolation phenomenon in the $i\mathcal{S}$-graph. Specifically, we prove the existence of a phase transition in the $i\mathcal{S}$-graph, whereby an unbounded component of securely connected nodes suddenly arises as we increase the density of legitimate nodes.[8] The result is given by the following main theorem.

*Theorem 3.1 (Phase Transition in the $i\mathcal{S}$-Graph):* For any $\lambda_e > 0$ and $\varrho$ satisfying

$$0 \le \varrho < \varrho_{\max} \triangleq \log_2\left(1 + \frac{P \cdot g(0)}{\sigma^2}\right) \tag{12}$$

there exist critical densities $\lambda_c^{\text{out}}$, $\lambda_c^{\text{in}}$, $\lambda_c^{\text{weak}}$, and $\lambda_c^{\text{strong}}$ satisfying

$$0 < \lambda_c^{\text{weak}} \le \lambda_c^{\text{out}} \le \lambda_c^{\text{strong}} < \infty \tag{13}$$

$$0 < \lambda_c^{\text{weak}} \le \lambda_c^{\text{in}} \le \lambda_c^{\text{strong}} < \infty \tag{14}$$

such that

$$p_\infty^\diamond = 0, \quad \text{for } \lambda_\ell < \lambda_c^\diamond \tag{15}$$

$$p_\infty^\diamond > 0, \quad \text{for } \lambda_\ell > \lambda_c^\diamond \tag{16}$$

[5]In the literature, the weak and strong components of node $x$ are sometimes defined differently as

$$\mathcal{K}^{\text{weak}}(x) \triangleq \{y \in \Pi : \exists\, x \overset{G}{\to} y \vee \exists\, y \overset{G}{\to} x\} = \mathcal{K}^{\text{out}}(x) \cup \mathcal{K}^{\text{in}}(x)$$

and

$$\mathcal{K}^{\text{strong}}(x) \triangleq \{y \in \Pi : \exists\, x \overset{G}{\to} y \wedge \exists\, y \overset{G}{\to} x\} = \mathcal{K}^{\text{out}}(x) \cap \mathcal{K}^{\text{in}}(x).$$

In this paper, we prefer the definitions in (8) and (9), since they only depend on the respective undirected graphs $G^{\text{weak}}$ and $G^{\text{strong}}$, and do not require explicit knowledge of $G$. As we shall see, this choice will simplify many of the derivations, namely by allowing us to translate an analysis of *directed* graphs into one of *undirected* graphs.

[6]We condition on the event that a legitimate node is located at $x = 0$. According to Slivnyak's theorem [48, Sec. 4.4], apart from the given point at $x = 0$, the probabilistic structure of the conditioned process is identical to that of the original process.

[7]Except where otherwise indicated, in the rest of this paper we use the symbol $\diamond$ to represent the out, in, weak, or strong component.

[8]Note that the existence of a phase transition was previously conjectured in [29], for the case of $\varrho = 0$.

for any $\diamond \in \{\text{out}, \text{in}, \text{weak}, \text{strong}\}$. Conversely, if $\varrho > \varrho_{\max}$, then $p_\infty^\diamond = 0$ for any $\lambda_\ell$, $\lambda_e$.

To prove the theorem, we introduce the following three lemmas.

*Lemma 3.1:* For any $\lambda_e > 0$ and $\varrho$ satisfying (12), there exists an $\epsilon > 0$ such that $p_\infty^{\text{weak}}(\lambda_\ell) = 0$ for all $\lambda_\ell < \epsilon$.

*Proof:* Due to its length, the proof is postponed to Section III-C. □

*Lemma 3.2:* For any $\lambda_e > 0$ and $\varrho$ satisfying (12), there exists a $\zeta < \infty$ such that $p_\infty^{\text{strong}}(\lambda_\ell) > 0$ for all $\lambda_\ell > \zeta$.

*Proof:* Due to its length, the proof is postponed to Section III-D. □

*Lemma 3.3:* For any $\lambda_e > 0$ and $\varrho \ge 0$, the percolation probability $p_\infty^\diamond(\lambda_\ell)$ is a nondecreasing function of $\lambda_\ell$.

*Proof:* See the Appendix. □

With these lemmas, we are now in condition to prove Theorem 3.1.

*Proof of Theorem 3.1:* We first show that if $\varrho > \varrho_{\max}$, then $p_\infty^\diamond = 0$. The MSR $\mathcal{R}_s$ of a link $\overrightarrow{x_i x_j}$, given in (3), is upper bounded by the channel capacity $\mathcal{R}$ of a link with zero length, i.e., $\mathcal{R}_s(x_i, x_j) \le \mathcal{R}(x_i, x_i) = \log_2\left(1 + \frac{P \cdot g(0)}{\sigma^2}\right)$. If the threshold $\varrho$ is set such that $\varrho > \varrho_{\max}$, the condition $\mathcal{R}_s(x_i, x_j) > \varrho$ in (2) for the existence of the edge $\overrightarrow{x_i x_j}$ is never satisfied by any $x_i$, $x_j$. Thus, the $i\mathcal{S}$-graph $G$ has no edges and cannot percolate. We now consider the case of $0 \le \varrho < \varrho_{\max}$. From properties (10) and (11), we have $p_\infty^{\text{strong}} \le p_\infty^{\text{out}} \le p_\infty^{\text{weak}}$ and $p_\infty^{\text{strong}} \le p_\infty^{\text{in}} \le p_\infty^{\text{weak}}$. Then, Lemmas 3.1, 3.2, and 3.3 imply that each curve $p_\infty^\diamond(\lambda_\ell)$ departs from the zero value at some critical density $\lambda_c^\diamond$, as expressed by (15) and (16). Furthermore, these critical densities are nontrivial in the sense that $0 < \lambda_c^\diamond < \infty$. The ordering of critical densities in (13) and (14) follows from similar coupling arguments. □

We now present some remarks on Theorem 3.1. The theorem shows that each of the four components of the $i\mathcal{S}$-graph experiences a phase transition at some critical density $\lambda_c^\diamond$. As we increase the density $\lambda_\ell$ of legitimate nodes, the component $\mathcal{K}^{\text{weak}}(0)$ percolates first, then $\mathcal{K}^{\text{out}}(0)$ or $\mathcal{K}^{\text{in}}(0)$, and finally $\mathcal{K}^{\text{strong}}(0)$. Furthermore, percolation can occur for any prescribed infimum secrecy rate $\varrho$, as long as it is below the channel capacity of a link with zero length, i.e., $\varrho_{\max}$. This has different implications depending on the type of propagation function $g(r)$.

1) If $g(0) = \infty$, percolation can occur for any arbitrarily large secrecy requirement $\varrho$, as long as the density $\lambda_\ell$ of legitimate nodes is made large enough.
2) If $g(0) < \infty$, percolation cannot occur if the threshold $\varrho$ is set above $\varrho_{\max} = \log_2(1 + \mathsf{SNR} \cdot g(0))$, where $\mathsf{SNR} \triangleq \frac{P}{\sigma^2}$. To ensure percolation for such $\varrho$, the $\mathsf{SNR}$ must be increased until $\varrho_{\max}(\mathsf{SNR})$ decreases below the desired $\varrho$. At that point, the density $\lambda_\ell$ can then be increased to achieve percolation.

Note that the theorem holds for any channel gain function $g(r)$ satisfying Conditions 1–3 in Section II-A, including bounded and unbounded models. Concerning the density $\lambda_e$ of eavesdroppers, the theorem says that as long as $\varrho < \varrho_{\max}$, percolation

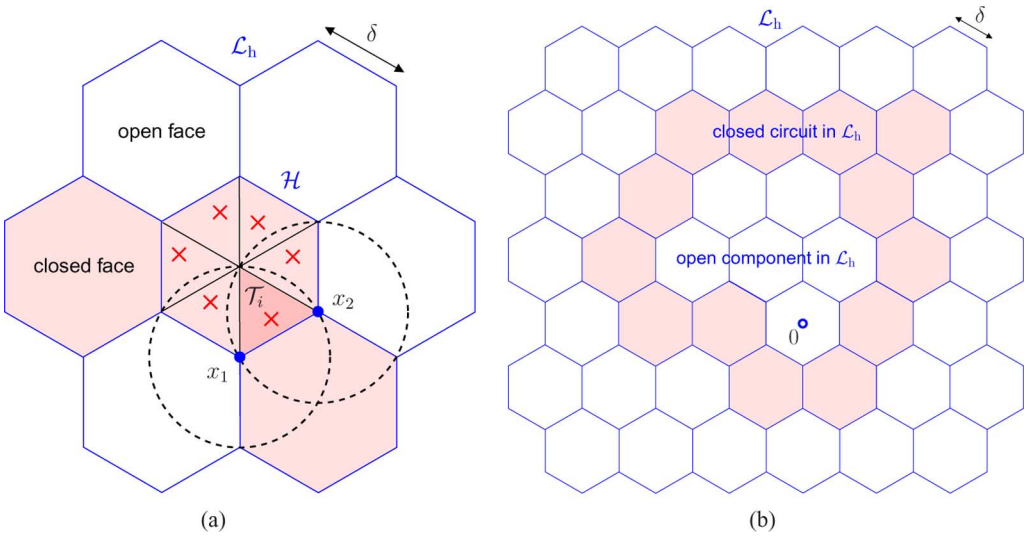


Fig. 2. Auxiliary diagrams for proving Lemma 3.1. (a) Conditions for a face $\mathcal{H}$ in $\mathcal{L}_h$ to be closed, according to Definition 3.1: each of the six triangles in $\mathcal{H}$ must have at least one eavesdropper node each, and $\mathcal{H}$ must be free of legitimate nodes. (b) Finite open component at the origin, surrounded by a closed circuit.

can occur even in scenarios with arbitrarily dense eavesdroppers. This can be achieved by just deploying more legitimate nodes, so that $\lambda_\ell$ is large enough.

Operationally, the theorem is important because it shows that long-range secure communication over multiple hops is still feasible, even in the presence of arbitrarily dense eavesdroppers. In particular, if we limit communication to the secure links whose MSR exceeds $\varrho$ (chosen such that $\varrho < \varrho_{\max}$), then for $\lambda_\ell$ large enough, a component with an infinite number of securely connected nodes arises. Those nodes are able to communicate with strong secrecy at a rate greater than $\varrho$ bits per complex channel use. The specific type of the secure connection (e.g., unidirectional or bidirectional) depends on the graph component under consideration: out, in, weak, or strong component.

### C. Proof of Lemma 3.1

In this proof, it is sufficient to show that $G^{\rm weak}$ does not percolate for sufficiently small $\lambda_\ell$ in the case of $\varrho = 0$, since for larger $\varrho$ the connectivity is worse and $G^{\rm weak}$ certainly does not percolate either.[9] We then proceed in two intermediate steps. First, we map the continuous $i\mathcal{S}$-graph $G$ onto a discrete hexagonal lattice $\mathcal{L}_{\rm h}$, and declare a face in $\mathcal{L}_{\rm h}$ to be closed in such a way that the absence of face percolation in $\mathcal{L}_{\rm h}$ implies the absence of continuum percolation in $G^{\rm weak}$. Second, we show that discrete face percolation does not occur in $\mathcal{L}_{\rm h}$ for sufficiently small (but nonzero) $\lambda_\ell$.

*Mapping on a Lattice:* We start with some definitions. Let $\mathcal{L}_{\rm h}$ be a hexagonal lattice as depicted in Fig. 2(a), where each face is a regular hexagon with side length $\delta$. Each face has a *state*, which can be either *open* or *closed*. A set of faces (e.g., a path or a circuit) in $\mathcal{L}_{\rm h}$ is said to be open iff all the faces that form the set are open. We now define when a face is *closed* based on how the processes $\Pi_\ell$ and $\Pi_{\rm e}$ behave inside that face.

*Definition 3.1 (Closed Face in $\mathcal{L}_{\rm h}$):* A face $\mathcal{H}$ in $\mathcal{L}_{\rm h}$ is said to be *closed* iff all the following conditions are met:

1) Each of the six equilateral triangles $\{\mathcal{T}_i\}_{i=1}^6$ that compose the hexagon $\mathcal{H}$ has at least one eavesdropper.
2) The hexagon $\mathcal{H}$ is free of legitimate nodes.

The aforementioned definition was chosen such that discrete face percolation in $\mathcal{L}_{\rm h}$ can be tied to continuum percolation in $G^{\rm weak}$, as given by the following proposition.

*Proposition 3.1 (Circuit Coupling):* If there exists a closed circuit in $\mathcal{L}_{\rm h}$ surrounding the origin, then the component $\mathcal{K}^{\rm weak}(0)$ is finite.

*Proof:* Assume there is a closed circuit $\mathcal{C}$ in $\mathcal{L}_{\rm h}$ surrounding the origin, as depicted in Fig. 2(b). This implies that the open component in $\mathcal{L}_{\rm h}$ containing 0, denoted by $\mathcal{K}^{\mathcal{L}_{\rm h}}(0)$, must be finite. Since the area of the region $\mathcal{K}^{\mathcal{L}_{\rm h}}(0)$ is finite, the continuous graph $G^{\rm weak}$ has a finite number of vertices falling inside this region. Thus, to prove that $\mathcal{K}^{\rm weak}(0)$ is finite, we just need to show that no edges of $G^{\rm weak}$ cross the circuit $\mathcal{C}$. Consider Fig. 2(a), and suppose that the shaded faces are part of the closed circuit $\mathcal{C}$. Let $x_1$, $x_2$ be two legitimate nodes such that $x_1$ falls on an open face on the inner side of $\mathcal{C}$, while $x_2$ falls on the outer side of $\mathcal{C}$ (note that Definition 3.1 specifies that the closed faces in $\mathcal{C}$ cannot contain legitimate nodes). Clearly, the most favorable situation for $x_1$, $x_2$ being able to establish an edge across $\mathcal{C}$ is the one depicted in Fig. 2(a). The edge $\overline{x_1x_2}$ exists in $G^{\rm weak}$ iff either $\mathcal{B}_{x_1}(\delta)$ or $\mathcal{B}_{x_2}(\delta)$ are free of eavesdroppers.[10] This condition does not hold, since Definition 3.1 guarantees that at least one eavesdropper is located inside the triangle $\mathcal{T}_i \subset \mathcal{B}_{x_1}(\delta) \cap \mathcal{B}_{x_2}(\delta)$. Thus, no edges of $G^{\rm weak}$ cross the circuit $\mathcal{C}$, which implies that $\mathcal{K}^{\rm weak}(0)$ has finite size. □

[9] A simple coupling argument shows that the percolation probabilities $p_\infty^\diamond(\lambda_\ell, \lambda_{\rm e}, \varrho)$ are nonincreasing functions of $\varrho$.

[10] We use $\mathcal{B}_x(\rho) \triangleq \{y \in \mathbb{R}^2 : |y - x| \le \rho\}$ to denote the closed 2-D ball centered at point $x$, with radius $\rho$.

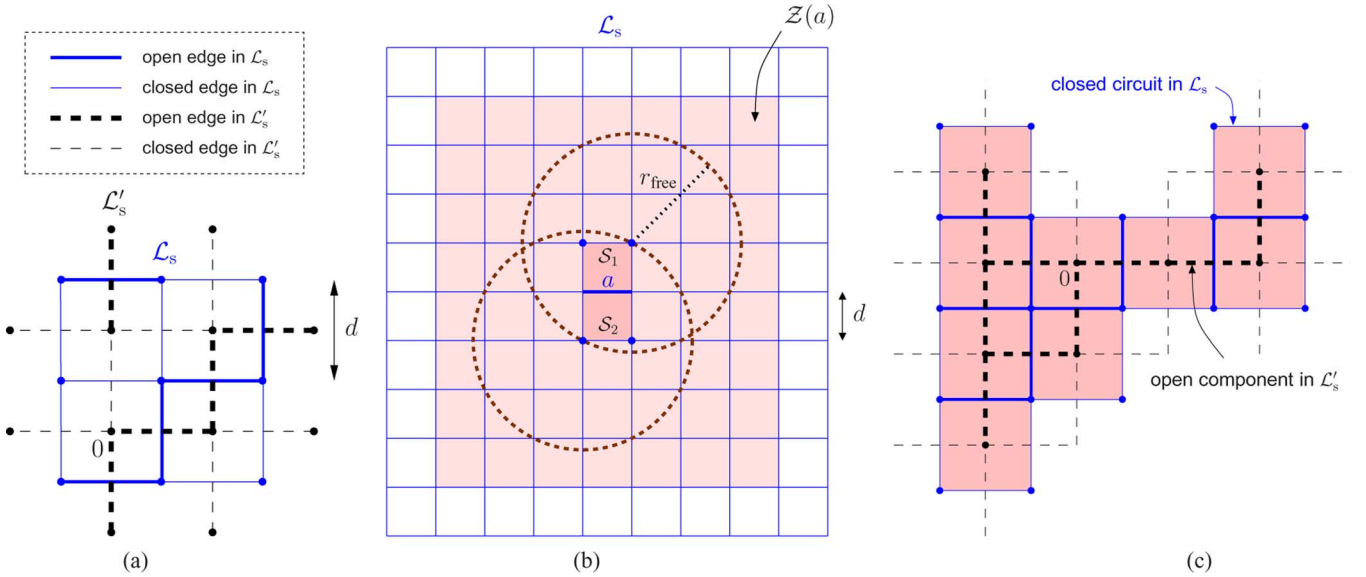


Fig. 3. Auxiliary diagrams for proving Lemma 3.2. (a) Square lattice $\mathcal{L}_s = d \cdot \mathbb{Z}^2$ and its dual $\mathcal{L}'_s = \mathcal{L}_s + \left(\frac{d}{2}, \frac{d}{2}\right)$. We declare an edge of $\mathcal{L}'_s$ to be open iff its dual edge in $\mathcal{L}_s$ is open. (b) Conditions for an edge $a$ in $\mathcal{L}_s$ to be open, according to Definition 3.2: the squares must have at least one legitimate node each, and the rectangle must be free of eavesdroppers. The radius $r_{\text{free}}$ increases with $\varrho$. The figure plots the case of $\varrho = 0$. (c) Finite open component at the origin, surrounded by a closed circuit in the dual lattice.

*1) Discrete Percolation:* Having performed an appropriate mapping from a continuous to a discrete model, we now analyze discrete face percolation in $\mathcal{L}_{\text{h}}$.

*Proposition 3.2 (Discrete Percolation in $\mathcal{L}_{\text{h}}$):* If the parameters $\lambda_\ell$, $\lambda_{\text{e}}$, $\delta$ satisfy

$$\left(1 - e^{-\lambda_{\text{e}} \frac{\sqrt{3}}{4} \delta^2}\right)^6 \cdot e^{-\lambda_\ell \frac{3\sqrt{3}}{2} \delta^2} > \frac{1}{2} \tag{17}$$

then the origin is a.s. surrounded by a closed circuit in $\mathcal{L}_{\text{h}}$.

*Proof:* The model introduced in Section III-C1 can be seen as a face percolation model on the hexagonal lattice $\mathcal{L}_{\text{h}}$, where each face is closed independently of other faces with probability

$$\begin{aligned} p &\stackrel{\triangle}{=} \mathbb{P}\{\text{face } \mathcal{H} \text{ of } \mathcal{L}_{\text{h}} \text{ is closed}\} \\ &= \mathbb{P}\left\{\left(\bigwedge_{i=1}^{6} \Pi_{\text{e}}\{\mathcal{I}_i\} \geq 1\right) \wedge \Pi_\ell\{\mathcal{H}\} = 0\right\} \\ &= \left(1 - e^{-\lambda_{\text{e}} \frac{\sqrt{3}}{4} \delta^2}\right)^6 \cdot e^{-\lambda_\ell \frac{3\sqrt{3}}{2} \delta^2}. \end{aligned} \tag{18}$$

Face percolation on the hexagonal lattice can be equivalently described as site percolation on the triangular lattice. In particular, recall that if

$$\mathbb{P}\{\mathcal{H} \text{ is open}\} < \frac{1}{2} \tag{19}$$

then the open component in $\mathcal{L}_{\text{h}}$ containing the origin is a.s. finite [49, Ch. 5, Th. 8], and so the origin is a.s. surrounded by a closed circuit in $\mathcal{L}_{\text{h}}$. Combining (18) and (19), we obtain (17). □

We now use the propositions to finalize the proof of Lemma 3.1, whereby $p_\infty^{\text{weak}}(\lambda_\ell) = 0$ for sufficiently small (but nonzero) $\lambda_\ell$.

*2) Proof of Lemma 3.1:* For any fixed $\lambda_{\text{e}}$, it is easy to see that condition (17) can always be met by making the hexagon side $\delta$ large enough, and the density $\lambda_\ell$ small enough (but nonzero). For any such choice of parameters $\lambda_\ell$, $\lambda_{\text{e}}$, $\delta$ satisfying (17), the origin is a.s. surrounded by a *closed* circuit in $\mathcal{L}_{\text{h}}$ (by Proposition 3.2), and the component $\mathcal{K}^{\text{weak}}(0)$ is a.s. finite (by Proposition 3.1), i.e., $p_\infty^{\text{weak}}(\lambda_\ell) = 0$. □

### D. Proof of Lemma 3.2

We proceed in two intermediate steps. First, we associate with our continuous $i\mathcal{S}$-graph $G$ a discrete square lattice $\mathcal{L}_{\text{s}}$ as well as its dual $\mathcal{L}'_{\text{s}}$, and declare an edge in $\mathcal{L}_{\text{s}}$ to be open in such a way that discrete edge percolation in $\mathcal{L}'_{\text{s}}$ implies continuum percolation in $G^{\text{strong}}$. Second, we show that discrete edge percolation occurs in $\mathcal{L}'_{\text{s}}$ for sufficiently large (but finite) $\lambda_\ell$.

*1) Mapping on a Lattice:* We start with some definitions. Let $\mathcal{L}_{\text{s}} \stackrel{\triangle}{=} d \cdot \mathbb{Z}^2$ be a square lattice with edge length $d$. Let $\mathcal{L}'_{\text{s}} \stackrel{\triangle}{=} \mathcal{L}_{\text{s}} + \left(\frac{d}{2}, \frac{d}{2}\right)$ be the dual lattice of $\mathcal{L}_{\text{s}}$, depicted in Fig. 3(a). We make the origin of the coordinate system coincide with a vertex of $\mathcal{L}'_{\text{s}}$. Each edge has a *state*, which can be either *open* or *closed*. We declare an edge $a'$ of $\mathcal{L}'_{\text{s}}$ to be open iff its dual edge $a$ in $\mathcal{L}_{\text{s}}$ is open. Furthermore, a set of edges (e.g., a path or a circuit) in $\mathcal{L}_{\text{s}}$ or $\mathcal{L}'_{\text{s}}$ is said to be open iff all the edges that form the set are open.

We now specify when an edge of $\mathcal{L}_{\text{s}}$ (and therefore of $\mathcal{L}'_{\text{s}}$) is *open* based on how the processes $\Pi_\ell$ and $\Pi_{\text{e}}$ behave in the neighborhood of that edge. Consider Fig. 3(b), where $a$ denotes an edge in $\mathcal{L}_{\text{s}}$, and $\mathcal{S}_1(a)$ and $\mathcal{S}_2(a)$ denote the two squares adjacent to $a$. Let $\{v_i\}_{i=1}^4$ denote the four vertices of the rectangle $\mathcal{S}_1(a) \cup \mathcal{S}_2(a)$. We then have the following definition.

*Definition 3.2 (Open Edge in $\mathcal{L}_{\text{S}}$):* An edge $a$ in $\mathcal{L}_{\text{s}}$ is said to be *open* iff all the following conditions are met.

1) Each square $\mathcal{S}_1(a)$ and $\mathcal{S}_2(a)$ adjacent to $a$ has at least one legitimate node.

2) The region $\mathcal{Z}(a)$ is free of eavesdroppers, where $\mathcal{Z}(a)$ is smallest rectangle such that $\bigcup_{i=1}^{4}\mathcal{B}_{v_i}(r_{\text{free}}) \subset \mathcal{Z}(a)$ with[11]

$$r_{\text{free}} \triangleq g^{-1}\left(2^{-\varrho}g(\sqrt{5}d) - \frac{\sigma^2}{P}(1-2^{-\varrho})\right) \tag{20}$$

The aforementioned definition was chosen such that discrete edge percolation in $\mathcal{L}'_{\text{s}}$ can be tied to continuum percolation in $G^{\text{strong}}$, as given by the following two propositions.

*Proposition 3.3 (Two-Square Coupling):* If $a$ is an open edge in $\mathcal{L}_{\text{s}}$, then all legitimate nodes inside $\mathcal{S}_1(a)\cup\mathcal{S}_2(a)$ form a single connected component in $G^{\text{strong}}$. □

*Proof:* If two legitimate nodes $x_1, x_2$ are to be placed inside the region $\mathcal{S}_1(a)\cup\mathcal{S}_2(a)$, the most unfavorable configuration in terms of MSR is the one where the distance $|x_1-x_2|$ is maximized, i.e., $x_1, x_2$ are on opposite corners of the rectangle $\mathcal{S}_1(a)\cup\mathcal{S}_2(a)$ and thus $|x_1-x_2|=\sqrt{5}d$. In such configuration, we see from (4) that the edge $\overrightarrow{x_1x_2}$ exists in $G$ iff

$$|x_1-e^*| > g^{-1}\left(2^{-\varrho}g(\sqrt{5}d) - \frac{\sigma^2}{P}(1-2^{-\varrho})\right) \triangleq r_{\text{free}}$$

where $e^*$ is the eavesdropper closest to $x_1$. As a result, the edge $\overline{x_1x_2}$ exists in $G^{\text{strong}}$ iff both $\mathcal{B}_{x_1}(r_{\text{free}})$ and $\mathcal{B}_{x_2}(r_{\text{free}})$ are free of eavesdroppers. Now, if $\mathcal{Z}(a)$ is the smallest rectangle containing the region $\bigcup_{i=1}^{4}\mathcal{B}_{v_i}(r_{\text{free}})$, the condition $\Pi_{\text{e}}\{\mathcal{Z}(a)\}=0$ ensures the edge $\overline{x_ix_j}$ exists in $G^{\text{strong}}$ for any $x_i, x_j \in \mathcal{S}_1(a)\cup\mathcal{S}_2(a)$. Thus, all legitimate nodes inside $\mathcal{S}_1(a)\cup\mathcal{S}_2(a)$ form a single connected component in $G^{\text{strong}}$. □

*Proposition 3.4 (Component Coupling):* If the open component in $\mathcal{L}'_{\text{s}}$ containing the origin is infinite, then the component $\mathcal{K}^{\text{strong}}(0)$ is also infinite.

*Proof:* Consider Fig. 3(c). Let $\mathcal{P}=\{a'_i\}$ denote a path of open edges $\{a'_i\}$ in $\mathcal{L}'_{\text{s}}$. By the definition of dual lattice, the path $\mathcal{P}$ uniquely defines a sequence $\mathcal{S}=\{\mathcal{S}_i\}$ of adjacent squares in $\mathcal{L}_{\text{s}}$, separated by open edges $\{a_i\}$ (the duals of $\{a'_i\}$). Then, each square in $\mathcal{S}$ has at least one legitimate node (by Definition 3.2), and all legitimate nodes falling inside the region associated with $\mathcal{S}$ form a single connected component in $G^{\text{strong}}$ (by Proposition 3.3). Now, let $\mathcal{K}^{\mathcal{L}'_{\text{s}}}(0)$ denote the open component in $\mathcal{L}'_{\text{s}}$ containing 0. Because of the argument just presented, we have $|\mathcal{K}^{\mathcal{L}'_{\text{s}}}(0)| \le |\mathcal{K}^{\text{strong}}(0)|$. Thus, if $|\mathcal{K}^{\mathcal{L}'_{\text{s}}}(0)|=\infty$, then $|\mathcal{K}^{\text{strong}}(0)|=\infty$. □

*2) Discrete Percolation:* Having performed an appropriate mapping from a continuous to a discrete model, we now analyze discrete edge percolation in $\mathcal{L}'_{\text{s}}$. Let $N_{\text{s}}$ be the number of squares that compose the rectangle $\mathcal{Z}(a)$ introduced in Definition 3.2. We first study the behavior of paths in $\mathcal{L}_{\text{s}}$ with the following proposition.

*Proposition 3.5 (Geometric Bound):* The probability that a given path of $\mathcal{L}_{\text{s}}$ with length $n$ is *closed* is bounded by

$$\mathbb{P}\{\text{path of } \mathcal{L}_{\text{s}} \text{ with length } n \text{ is closed}\} \le q^{n/N_e} \tag{21}$$

where $N_e$ is a finite integer and

$$q = 1-(1-e^{-\lambda_\ell d^2})^2\cdot e^{-\lambda_{\text{e}}N_{\text{s}}d^2} \tag{22}$$

is the probability that an edge of $\mathcal{L}_{\text{s}}$ is closed.

*Proof: (Outline):* Using Definition 3.2, we can write

$$\begin{aligned} q &\triangleq \mathbb{P}\{\text{edge } a \text{ in } \mathcal{L}_{\text{s}} \text{ is closed}\} \\ &= 1-\mathbb{P}\{\Pi_\ell\{\mathcal{S}_1(a)\}\ge 1\wedge\Pi_\ell\{\mathcal{S}_2(a)\}\ge 1\wedge\Pi_{\text{e}}\{\mathcal{Z}(a)\}=0\} \\ &= 1-(1-e^{-\lambda_\ell d^2})^2\cdot e^{-\lambda_{\text{e}}N_{\text{s}}d^2}. \end{aligned}$$

Now, let $\mathcal{P}=\{a_i\}_{i=1}^{n}$ denote a path in $\mathcal{L}_{\text{s}}$ with length $n$ and edges $\{a_i\}$. Even though the edges $\{a_i\}$ do not all have independent states (in which case we would have $\mathbb{P}\{\mathcal{P} \text{ is closed}\}=q^n$), it is possible to show that $\mathbb{P}\{\mathcal{P} \text{ is closed}\} \le q^{n/N_e}$ for a finite integer $N_e$, by finding a subset $\mathcal{Q}\subseteq\mathcal{P}$ of edges with independent states (see [38] and [50] for various examples). □

Having obtained a geometric bound on the probability of a path of length $n$ being closed, we can now use a Peierls argument to study the existence of an infinite component.[12]

*Proposition 3.6 (Discrete Percolation in $\mathcal{L}'_{\text{S}}$):* If the probability $q$ satisfies

$$q < \left(\frac{11-2\sqrt{10}}{27}\right)^{N_e} \tag{23}$$

then

$$\mathbb{P}\{\text{open component in } \mathcal{L}'_{\text{s}} \text{ containing 0 is infinite}\} > 0. \tag{24}$$

*Proof:* We start with the key observation that the open component in $\mathcal{L}'_{\text{s}}$ containing 0 is finite iff there is a closed circuit in $\mathcal{L}_{\text{s}}$ surrounding 0. This is best seen by inspecting Fig. 3(c), where the origin is surrounded by a necklace of closed edges in $\mathcal{L}'_{\text{s}}$, which block all possible routes in $\mathcal{L}_{\text{s}}$ from the origin to infinity. Thus, the inequality in (24) is equivalent to $\mathbb{P}\{\exists \text{ closed circuit in } \mathcal{L}_{\text{s}} \text{ surrounding } 0\} < 1$. Let $\rho(n)$ denote the possible number of circuits of length $n$ in $\mathcal{L}_{\text{s}}$ surrounding 0 (a deterministic quantity). Let $\kappa(n)$ denote the number of closed circuits of length $n$ in $\mathcal{L}_{\text{s}}$ surrounding 0 (a random variable). From combinatorial arguments, it can be shown [52, eq. (1.17)] that $\rho(n)\le 4n3^{n-2}$. Then, for a fixed $n$

$$\begin{aligned} \mathbb{P}\{\kappa(n)\ge 1\} &\le \rho(n)\mathbb{P}\{\text{path of } \mathcal{L}_{\text{s}} \text{ with length } n \text{ is closed}\} \\ &\le 4n3^{n-2}q^{n/N_e} \end{aligned}$$

where we used the union bound and Proposition 3.5. Also

$$\begin{aligned} &\mathbb{P}\{\exists \text{ closed circuit in } \mathcal{L}_{\text{s}} \text{ surrounding } 0\} \\ &\quad = \mathbb{P}\{\kappa(n)\ge 1 \text{ for some } n\} \\ &\quad \le \sum_{n=1}^{\infty} 4n3^{n-2}q^{n/N_e} = \frac{4q^{1/N_{\text{e}}}}{3(1-3q^{1/N_e})^2} \end{aligned} \tag{25}$$

for $q<\left(\frac{1}{3}\right)^{N_e}$. We see that if $q$ satisfies (23), then (25) is strictly less than one, and (24) follows. □

[11]To ensure that $r_{\text{free}}$ in (20) is well defined, in the rest of this paper we assume that $d$ is chosen such that $d<\frac{1}{\sqrt{5}}g^{-1}\left(\frac{\sigma^2}{P}(2^{\varrho}-1)\right)$.

[12]A "Peierls argument," so-named in honor of R. Peierls and his 1936 article on the Ising model [51], refers to an approach based on enumeration.

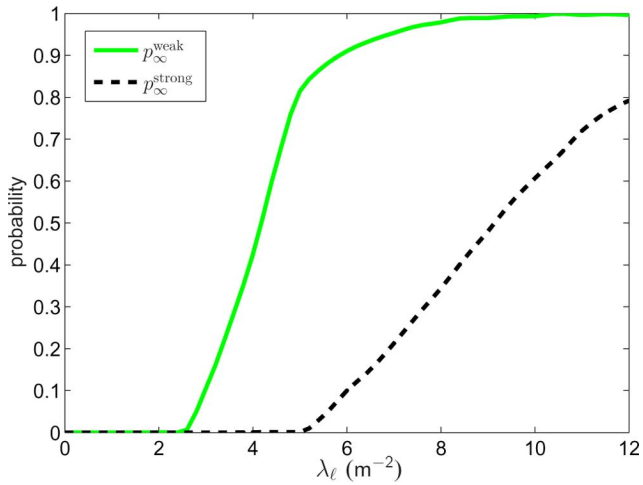


Fig. 4. Simulated percolation probabilities for the weak and strong components of the $i\mathcal{S}$-graph, versus the density $\lambda_\ell$ of legitimate nodes ($\lambda_e = 1$ m$^{-2}$, $\varrho = 0$).

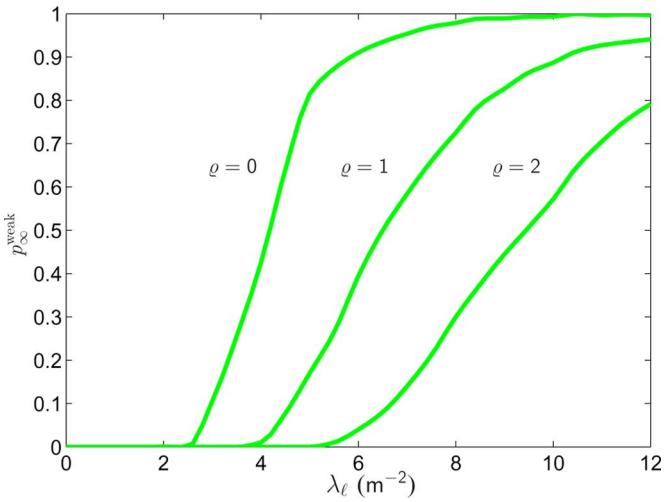


Fig. 5. Effect of the secrecy rate threshold $\varrho$ on the percolation probability $p_\infty^{\text{weak}}$ ($\lambda_e = 1$ m$^{-2}$, $g(r) = \frac{1}{r^{2b}}$, $b = 2$, $P_\ell/\sigma^2 = 10$).

We now use the propositions to finalize the proof of Lemma 3.2, whereby $p_\infty^{\text{strong}}(\lambda_\ell) > 0$ for sufficiently large (but finite) $\lambda_\ell$.

*3) Proof of Lemma 3.2:* For any fixed $\lambda_e$, it is easy to see that the probability $q$ in (22) can be made small enough to satisfy condition (23), by making the edge length $d$ sufficiently small, and the density $\lambda_\ell$ sufficiently large (but finite). For any such choice of parameters $\lambda_\ell$, $\lambda_e$, $d$ satisfying (23), the open component in $\mathcal{L}'_s$ containing 0 is infinite with positive probability (by Proposition 3.6), and the component $\mathcal{K}^{\text{strong}}(0)$ is also infinite with positive probability (by Proposition 3.4), i.e., $p_\infty^{\text{strong}}(\lambda_\ell) > 0$. □

### E. Simulation Results

In this section, we obtain additional insights about percolation in the $i\mathcal{S}$-graph via Monte Carlo simulation. Specifically, we aim to evaluate the percolation probabilities $p_\infty^\diamond$ as a function of the density $\lambda_\ell$ of legitimate nodes, and thus estimate the corresponding critical densities $\lambda_c^\diamond$.

In our simulation procedure, we consider a square $\mathcal{R}$ with dimensions $\sqrt{A} \times \sqrt{A}$. The area $A$ is adjusted according to $A = \frac{N_\ell}{\lambda_\ell}$, where the average number $N_\ell$ of legitimate nodes in $\mathcal{R}$ is kept fixed. We use $N_\ell = 5000$ nodes and $\lambda_e = 1$ m$^{-2}$. We first place $\Pi_\ell\{\mathcal{R}\} \sim \mathcal{P}(\lambda_\ell A)$ legitimate nodes and $\Pi_e\{\mathcal{R}\} \sim \mathcal{P}(\lambda_e A)$ legitimate nodes inside $\mathcal{R}$, uniformly and independently.[13] The $i\mathcal{S}$-graph $G = \{\Pi_\ell, \mathcal{E}\}$ is then established using as edge set

$$\mathcal{E} = \left\{ \overrightarrow{x_i x_j} : g(d(x_i, x_j)) > 2^\varrho g(d(x_i, e^*)) + \frac{\sigma^2}{P}(2^\varrho - 1) \right\} \tag{26}$$

where $e^* = \arg\min_{e_k \in \Pi_e} d(x_i, e_k)$, and $d(\cdot,\cdot)$ is a toroidal distance metric [53], [54] used to reduce boundary effects. We then determine the various components in $G$, $G^{\text{weak}}$, and $G^{\text{strong}}$, and directly compute each percolation probability as the covered fraction of the corresponding unbounded cluster.[14]

[13]We use $\mathcal{P}(\mu)$ to denote a discrete Poisson distribution with mean $\mu$.

[14]We consider that a component is *unbounded* when it contains a loop around the torus, in any direction.

Fig. 4 shows the simulated percolation probabilities for the weak and strong components of the $i\mathcal{S}$-graph, versus the density $\lambda_\ell$ of legitimate nodes. It considers the simplest case of $\varrho = 0$, for which the percolation probabilities depend only on the ratio $\frac{\lambda_\ell}{\lambda_e}$. As predicted by Theorem 3.1, the curves $p_\infty^{\text{weak}}$ and $p_\infty^{\text{strong}}$ steeply depart from zero as the density $\lambda_\ell$ is increased, suggesting that $\lambda_c^{\text{weak}} \approx 2.6$ m$^{-2}$ and $\lambda_c^{\text{strong}} \approx 5.2$ m$^{-2}$, for the case of $\lambda_e = 1$ m$^{-2}$ and $\varrho = 0$. Operationally, this means that if long-range bidirectional secure communication is desired in a wireless network, the density of legitimate nodes must be at least 5.2 times that of the eavesdroppers. In practice, this ratio must be even larger, because a security requirement greater than $\varrho = 0$ is typically required.[15] Furthermore, increasing $\lambda_\ell$ also leads to an increased average fraction of nodes $p_\infty^{\text{strong}}$ which belong to the infinite component, thus ensuring better connectivity of the network.

Fig. 5 illustrates the dependence of the percolation probability $p_\infty^{\text{weak}}$ on the secrecy rate threshold $\varrho$. As expected, we observe that the critical density $\lambda_c^{\text{weak}}$ is increasing with respect to $\varrho$. This is because as we increase the threshold $\varrho$, the requirement $\mathcal{R}_s(x_i, x_j) > \varrho$ for any two nodes $x_i$, $x_j$ to be securely connected becomes stricter. Thus, the connectivity of the $i\mathcal{S}$-graph becomes worse and a higher density of legitimate nodes is needed for percolation.

Fig. 6 illustrates the subcritical and supercritical phases of the $i\mathcal{S}$-graph. In Fig. 6(a), we have $\frac{\lambda_\ell}{\lambda_e} = 2$, and the $i\mathcal{S}$-graph exhibits only small, bounded clusters of legitimate nodes. This is in agreement with Fig. 6(b), which suggests that for a ratio of $\frac{\lambda_\ell}{\lambda_e} = 2$, all four out, in, weak, and strong components are subcritical. In Fig. 6(b), we have $\frac{\lambda_\ell}{\lambda_e} = 15$, and the $i\mathcal{S}$-graph exhibits a large cluster of connected nodes. This also agrees with Fig. 4, which suggests that for a ratio of $\frac{\lambda_\ell}{\lambda_e} = 15$, all four components are supercritical.

## IV. Full Connectivity in the Poisson $i\mathcal{S}$-Graph

In the previous sections, we studied percolation in the $i\mathcal{S}$-graph defined over the infinite plane. We showed that for

[15]The critical densities $\lambda_c^\diamond(\lambda_e, \varrho)$ are nondecreasing functions of $\lambda_e$ and $\varrho$, as can be shown using a coupling argument similar to the proof of Lemma 3.3.

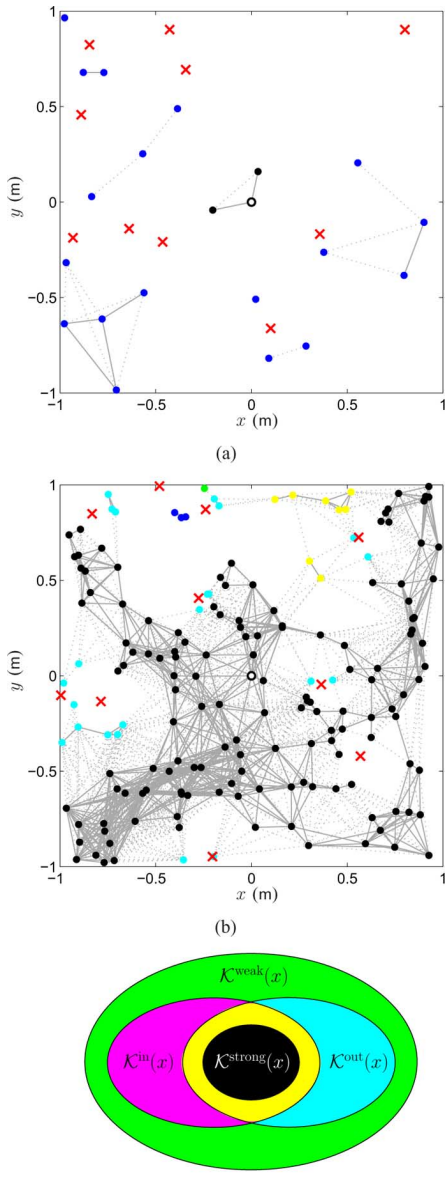


Fig. 6. Percolation in the $iS$-graph for $\varrho = 0$. The solid lines represent the edges in $G^{\text{strong}}$, while the dotted lines represent the edges in $G^{\text{weak}}$. (a) Subcritical graph $(\lambda_\ell/\lambda_e = 2)$. (b) Supercritical graph $(\lambda_\ell/\lambda_e = 15)$. (c) Structure and color legend of the various graph components of node $x = 0$.

some combinations of the parameters $(\lambda_\ell, \lambda_{\text{e}}, \varrho)$, the regime is supercritical and an infinite component arises. However, the existence of an infinite component does not ensure connectivity between any two nodes, and in this sense percolation ensures only *partial connectivity* of the network. In some scenarios, it is of interest to guarantee *full connectivity*, i.e., that all nodes can communicate with each other, possibly through multiple hops. Note, however, that for networks defined over an infinite region, the probability of full connectivity is exactly zero. Thus, to study of full connectivity, we need to restrict our attention to a finite region $\mathcal{R}$.

Throughout this section, we consider the simplest case of $\varrho = 0$, i.e., the *existence* of secure links with a positive (but possibly small) MSR. Because this scenario is characterized by the simple geometric description in (5), it provides various insights that are useful in understanding more complex scenarios.[16] Furthermore, the case of $\varrho = 0$ represents the most favorable scenario in terms of full connectivity, since a higher security requirement $\varrho$ leads to degraded connectivity.

In what follows, we start by defining full connectivity in the $i\mathcal{S}$-graph. We then characterize the exact asymptotic behavior of full connectivity in the limit of a large density of legitimate nodes. Finally, we derive simple, explicit expressions that closely approximate the probability of full in- and out-connectivity for a finite density of legitimate nodes, and determine the accuracy of such approximations using simulations.

### A. Definitions

Since the $i\mathcal{S}$-graph is a directed graph, we start by distinguishing between full out- and in-connectivity with the following definitions.

*Definition 4.1 (Full Out-Connectivity):* A legitimate node $x_i \in \Pi_\ell \cap \mathcal{R}$ is *fully out-connected* with respect to a region $\mathcal{R}$ if in the $i\mathcal{S}$-graph $G = \{\Pi_\ell, \mathcal{E}\}$ there exists a directed path from $x_i$ to *every* node $x_j \in \Pi_\ell \cap \mathcal{R}$, for $x_j \neq x_i$.

*Definition 4.2 (Full In-Connectivity):* A legitimate node $x_i \in \Pi_\ell \cap \mathcal{R}$ is *fully in-connected* with respect to a region $\mathcal{R}$ if in the $i\mathcal{S}$-graph $G = \{\Pi_\ell, \mathcal{E}\}$ there exists a directed path to $x_i$ from *every* node $x_j \in \Pi_\ell \cap \mathcal{R}$, for $x_j \neq x_i$.[17]

Since the $i\mathcal{S}$-graph is a random graph, we can consider the probabilities of a node $x_i$ being fully out- or in-connected. For analysis purposes, we consider that probe legitimate node (node 0) placed at the origin of the coordinate system, i.e., $x_{\text{probe}} = 0 \in \mathcal{R}$. We then define $p_{\text{out}-\text{con}}$ and $p_{\text{in}-\text{con}}$ as the probability that node 0 is, respectively, fully out- and fully in-connected. These probabilities are a deterministic function of the densities $\lambda_\ell$ and $\lambda_{\text{e}}$, and the area $A$ of region $\mathcal{R}$. Our goal is to characterize $p_{\text{out}-\text{con}}$ and $p_{\text{in}-\text{con}}$.

### B. Full Connectivity: Asymptotic Regime

In this section, we focus on the asymptotic behavior of secure connectivity as we increase the density of legitimate nodes. Specifically, for a fixed region of area $A$ and a fixed density $\lambda_{\text{e}}$ of eavesdroppers, we would like to determine if by increasing $\lambda_\ell \to \infty$, we can asymptotically achieve full in- and out-connectivity with probability one.[18]

[16]Specifically, the case of $\varrho = 0$ brings the following mathematical simplifications. First, the $i\mathcal{S}$-graph is completely independent of channel gain function $g(r)$; thus, no assumptions about the propagation model are needed. Second, there exist simple (often closed form) expressions for characterizing local connectivity [31] which will be useful in analyzing full connectivity.

[17]Note that these two definitions imply that legitimate nodes *outside* the region $\mathcal{R}$ can act as relays between legitimate nodes *inside* $\mathcal{R}$. Essentially, we are considering the $i\mathcal{S}$-graph defined on the infinite plane, but are only interested in the full connectivity of the nodes inside an observation region $\mathcal{R}$. In this paper, we will refer to this as the *observation model*. In the literature, other models for finite networks include 1) the *restriction model*, where the network graph is strictly limited to a finite square, with no nodes outside the square (e.g., [40]), and 2) the *toroidal model*, where the network graph is defined over a torus (e.g., [41]). The main advantage of the observation and toroidal models is their homogeneity, since they eliminate boundary effects associated with the restriction model, leading to mathematically more elegant results.

[18]We say that an event occurs "asymptotically almost surely" (a.a.s.) if its probability approaches one as $\lambda_\ell \to \infty$.

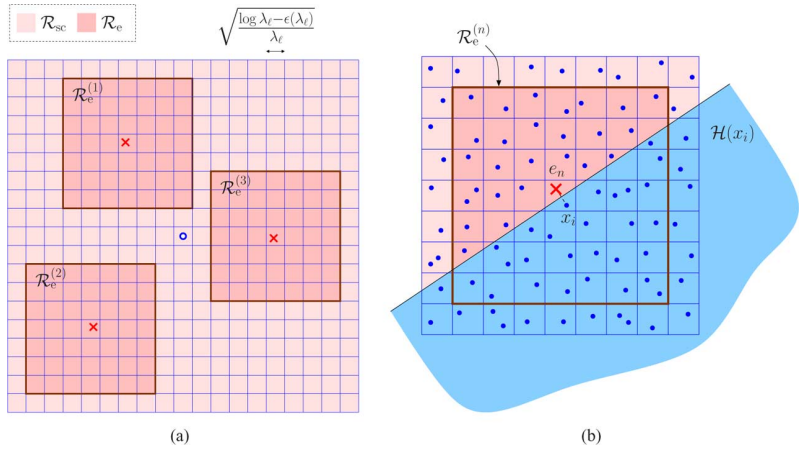


Fig. 7. Auxiliary diagrams for proving that $\lim_{\lambda_\ell\to\infty} p_{\rm out-con} = 1$.

*Definition 4.3 (Asymptotic Out-Connectivity):* A legitimate node $x \in \Pi_\ell \cap \mathcal{R}$ is *asymptotically out-connected* with respect to a region $\mathcal{R}$ with area $A$ if $\lim_{\lambda_\ell\to\infty} p_{\rm out-con} = 1$, for any $\lambda_{\rm e} > 0$ and $A > 0$.

*Definition 4.4 (Asymptotic In-Connectivity):* A legitimate node $x \in \Pi_\ell \cap \mathcal{R}$ is *asymptotically in-connected* with respect to a region $\mathcal{R}$ with area $A$ if $\lim_{\lambda_\ell\to\infty} p_{\rm in-con} = 1$, for any $\lambda_{\rm e} > 0$ and $A > 0$.[19]

The following theorem characterizes the asymptotic out-connectivity in the $i\mathcal{S}$-graph.

*Theorem 4.1 (Asymptotic Out-Connectivity):* For the Poisson $i\mathcal{S}$-graph with $\lambda_{\rm e} > 0$ and $A > 0$, the legitimate node at the origin is asymptotically out-connected.

*Proof:* Without loss of generality, consider that a legitimate node is placed at the origin, and let the region $\mathcal{R}$ be a square of size $\sqrt{A}\times\sqrt{A}$ containing at the origin. Let us partition $\mathcal{R}$ into equal subsquares $\mathcal{S}_i$ of size $\sqrt{\frac{\log\lambda_\ell-\epsilon(\lambda_\ell)}{\lambda_\ell}}\times\sqrt{\frac{\log\lambda_\ell-\epsilon(\lambda_\ell)}{\lambda_\ell}}$, where $\epsilon(\lambda_\ell) > 0$ is the smallest number such that the total number $\frac{A\lambda_\ell}{\log\lambda_\ell-\epsilon(\lambda_\ell)}$ of subsquares is an integer.[20] This partition is depicted in Fig. 7(a). A subsquare is said to be full if it contains at least one legitimate node, and empty otherwise. The probability that a subsquare is full is $1-e^{-\log\lambda_\ell+\epsilon(\lambda_\ell)}$, and the probability that every subsquare of $\mathcal{R}$ is full is

$$\mathbb{P}\left\{\bigwedge_{i=1}^{\frac{A\lambda_\ell}{\log\lambda_\ell-\epsilon(\lambda_\ell)}} \mathcal{S}_i \text{ is full}\right\} = \left(1-e^{-\log\lambda_\ell+\epsilon(\lambda_\ell)}\right)^{\frac{A\lambda_\ell}{\log\lambda_\ell-\epsilon(\lambda_\ell)}} \tag{27}$$

where we used the fact that $\Pi_\ell$ is a Poisson process. When we take the limit $\lambda_\ell\to\infty$, it is easy to see that $\epsilon(\lambda_\ell)\to 0$ and that (27) converges to one. In other words, the described partition of $\mathcal{R}$ ensures that every subsquare $\mathcal{S}_i$ will be full a.a.s.

Next, we analyze the secure connectivity between legitimate nodes belonging to *adjacent* subsquares of $\mathcal{R}$. Recall Fig. 3(b), where $\mathcal{S}_1$ and $\mathcal{S}_2$ denote two adjacent squares. Using an argument analogous to Section III-D-I, we know that if the $7\times 8$ subsquare rectangle [$\mathcal{Z}(a)$ in Fig. 3(b)] is free of eavesdroppers, then all legitimate nodes inside $\mathcal{S}_1\cup\mathcal{S}_2$ form a single strong component.[21] Now consider a region $\mathcal{R}_{\rm sc}\subseteq\mathcal{R}$ constructed in the following way. For every possible pair of adjacent subsquares $(\mathcal{S}_i,\mathcal{S}_j)$ in $\mathcal{R}$, determine whether the associated rectangle $\mathcal{Z}(\mathcal{S}_i,\mathcal{S}_j)$ is free of eavesdroppers. If so, update $\mathcal{R}_{\rm sc}$ such that it now becomes $\mathcal{R}_{\rm sc}\cup\mathcal{S}_i\cup\mathcal{S}_j$. Repeat the process until there are no more pairs of adjacent subsquares. With this definition, it is possible for large enough $\lambda_\ell$ to partition the square $\mathcal{R}$ into two regions as $\mathcal{R} = \mathcal{R}_{\rm sc}\cup\mathcal{R}_e$, where $\mathcal{R}_e = \mathcal{R}\backslash\mathcal{R}_{\rm sc}$ is simply the remaining region of $\mathcal{R}$ after $\mathcal{R}_{\rm sc}$ is constructed as previously. This partition is shown in Fig. 7(a). By construction, it is easy to see that as $\lambda_\ell$ approaches infinity (or, equivalently, the size of the subsquares $\{\mathcal{S}_i\}$ approaches zero) the following properties hold a.s.

1) The region $\mathcal{R}_e$ can be decomposed into nonoverlapping regions as $\mathcal{R}_e = \bigcup_{n=1}^{N_e}\mathcal{R}_e^{(n)}$, where $N_e \triangleq \Pi_{\rm e}\{\mathcal{R}\}$ is the number of eavesdroppers inside $\mathcal{R}$, and $\mathcal{R}_e^{(n)}\subset\mathcal{R}$ is a square of size $7\times 7$ subsquares centered at the $n$th eavesdropper of $\mathcal{R}$. If $N_e = 0$, then $R_e = \oslash$.
2) The origin belongs to $\mathcal{R}_{\rm sc}$.
3) There exists a lattice path (i.e., a path composed only of horizontal and vertical segments inside $\mathcal{R}$) between every two subsquares of $\mathcal{R}_{\rm sc}$, and thus, all legitimate nodes inside $\mathcal{R}_{\rm sc}$ form a single strong component.

We thus conclude that the origin is a.a.s. out-connected to all legitimate nodes inside $\mathcal{R}_{\rm sc}$. It remains to be determined whether it is also out-connected to all legitimate nodes inside $\mathcal{R}_e$. For that purpose, we consider the behavior of the $i\mathcal{S}$-graph in the vicinity of the $n$th eavesdropper of $\mathcal{R}$, which we denote by $e_n$.[22] We know that a node $x_i\in\Pi_\ell\cap\mathcal{R}_e^{(n)}$ will be in-connected iff the corresponding Voronoi cell induced by the process $\Pi_{\rm e}\cup\{x_i\}$ has at least another legitimate node [31]. A little reflection shows that as $\lambda_\ell\to\infty$, this Voronoi cell approaches the half-plane $\mathcal{H}(x_i)\triangleq\{y\in\mathbb{R}^2 : |y-x_i| < |y-e_n|\}$, as depicted in Fig. 7(b). Now, it is easy to see that for every

[19]In our study of asymptotic connectivity, it is irrelevant whether we consider the observational, restriction, or toroidal model. The reason is that, as we shall see, full connectivity is determined by the behavior of the legitimate nodes in the vicinity of the eavesdroppers. Therefore, when we let $\lambda_\ell\to\infty$, there exist enough legitimate nodes between the border of the region $\mathcal{R}$ and any eavesdropper, so the border effects essentially vanish before they can affect the vicinity of the eavesdroppers (and thus, full connectivity).

[20]We have explicitly indicated the dependence of $\epsilon$ on $\lambda_\ell$, and for simplicity omitted its dependence on $A$ (which will be kept fixed).

[21]Note that here we are considering the case of $\varrho = 0$, while the discussion in Section III-D1 was valid for nonzero $\varrho$ as well.

[22]In the trivial case of zero eavesdroppers in $\mathcal{R}$, the origin is out-connected to all legitimate nodes inside $\mathcal{R}$, and the theorem follows.

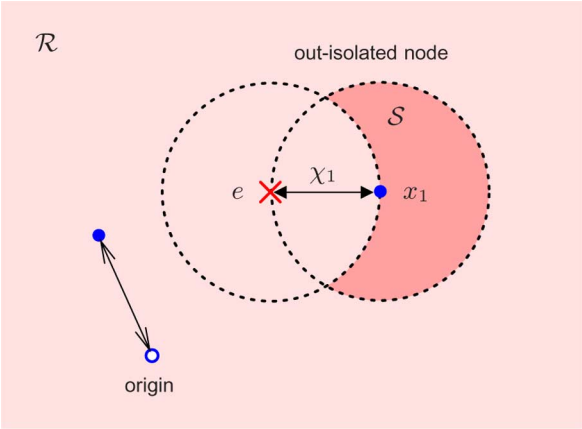


Fig. 8. Auxiliary diagram for proving that $\lim_{\lambda_\ell\to\infty} p_{\text{in}-\text{con}} < 1$.

$x_i \in \Pi_\ell \cap \mathcal{R}_e^{(n)}$, there is a.a.s. at least one legitimate node inside the region $\mathcal{H}(x_i) \cap \mathcal{R}_{\text{sc}}$, and thus, every such node $x_i$ has an in-connection from the strong component in $\mathcal{R}_{\text{sc}}$. This argument holds similarly for every region $\mathcal{R}_e^{(n)}$, $n = 1, \ldots, N_e$, and so we conclude that the origin is a.a.s. out-connected to all legitimate nodes inside $\mathcal{R}_e$, in addition to those in $\mathcal{R}_{\text{sc}}$. □

The following theorem characterizes the asymptotic in-connectivity in the $i\mathcal{S}$-graph.

*Theorem 4.2 (Asymptotic In-Connectivity):* For the Poisson $i\mathcal{S}$-graph with $\lambda_{\text{e}} > 0$ and $A > 0$, we have that

$$\lim_{\lambda_\ell\to\infty} p_{\text{in}-\text{con}} \le 1 - \frac{6\pi}{8\pi + 3\sqrt{3}}(1 - e^{-\lambda_{\text{e}} A}) \qquad (28)$$

i.e., the legitimate node at the origin is *not* asymptotically in-connected.

*Proof:* Consider a region $\mathcal{R}$ with area $A$, where a probe legitimate node (node 0) is placed at the origin. Let $\Pi_\ell\{\mathcal{R}\}$ and $\Pi_{\text{e}}\{\mathcal{R}\}$ denote the number of nodes in $\Pi_\ell \cap \mathcal{R}$ and $\Pi_{\text{e}} \cap \mathcal{R}$, respectively. Consider the event that there is at least one eavesdropper and one legitimate node in region $\mathcal{R}$, as depicted in Fig. 8. Let $\chi_1$ denote the distance between a arbitrarily selected eavesdropper $e$ and its *closest* legitimate node $x_1 \in \mathcal{R}$, i.e., $\chi_1 \stackrel{\triangle}{=} |e - x_1|$. In addition, let $\mathcal{S}$ be the set of possible locations in $\mathbb{R}^2$ where a node can connect to $x_1$, given that $x_1$ is the closest legitimate node to $e$, i.e., $\mathcal{S} \stackrel{\triangle}{=} \mathcal{B}_{x_1}(\chi_1) \backslash \mathcal{B}_e(\chi_1)$. If there are no legitimate nodes inside $\mathcal{S}$, then $x_1$ is *out-isolated*, and the origin is *not* fully in-connected. Thus, we can write

$$p_{\text{in}-\text{con}} \le 1 - (1 - e^{\lambda_{\text{e}} A}) \cdot \mathbb{P}\{\Pi_\ell\{\mathcal{R}\} \ge 1 \wedge \Pi_\ell\{\mathcal{S}\} = 0\} \quad (29)$$

In the limit of $\lambda_\ell \to \infty$, the event $\{\Pi_\ell\{\mathcal{R}\} \ge 1\}$ occurs a.s., and the RV $\zeta \stackrel{\triangle}{=} \chi_1^2$ becomes exponentially distributed with rate $\pi\lambda_\ell$ leading to

$$\mathbb{P}\{\Pi_\ell\{\mathcal{S}\} = 0\} = \mathbb{E}_{\chi_1}\left\{\exp\left(-\lambda\pi\chi_1^2\left(\frac{1}{3} + \frac{\sqrt{3}}{2\pi}\right)\right)\right\} = \frac{6\pi}{8\pi + 3\sqrt{3}}.$$

With this result, (29) becomes (28).

The theorem has the following intuitive explanation. Consider $\lambda_\ell$ (or $A$) large enough that border effects can be ignored. Given that exactly one eavesdropper occurs inside region $\mathcal{R}$, there is a constant probability $\mathbb{P}\{\Pi_\ell\{\mathcal{S}\} = 0\} = \frac{6\pi}{8\pi+3\sqrt{3}} \approx 0.62$ that the legitimate node closest to the eavesdropper is out-isolated, and this probability does not decrease with $\lambda_\ell$. In fact, when $\lambda_\ell$ increased, the area of $\mathcal{S}$ decreases in such a way that $\mathbb{P}\{\Pi_\ell\{\mathcal{S}\} = 0\}$ remains constant. As a result, regardless of how large $\lambda_\ell$ is made, there is a constant probability of $\approx 0.62$ that the nearest node is out-isolated, and therefore, a positive probability that the origin is *not* in-connected.

Theorems 4.1 and 4.2 clearly show that increasing the density $\lambda_\ell$ of legitimate nodes is an effective way to improve the full out-connectivity, in the sense that the corresponding probability approaches one. However, the probability of full in-connectivity *cannot* be made arbitrarily close to one by increasing $\lambda_\ell$. In essence, full (in or out) connectivity is determined by the behavior of the legitimate nodes in the vicinity of the eavesdroppers. It is more likely that a legitimate node in such vicinity is *locally* in-connected than out-connected [31, Property 3.2], which is reflected in the fact that the origin achieves full out-connectivity a.a.s., but not full in-connectivity. Operationally, this means a node can a.a.s. *transmit* secret messages to all the nodes in a finite region $\mathcal{R}$, but cannot a.a.s. *receive* secret messages from all the nodes in $\mathcal{R}$.

### C. Full Connectivity: Finite Regime

We now attempt to characterize full connectivity for a finite density of legitimate nodes. We start with the simple observation that if node 0 is fully out-connected, then there are no in-isolated nodes in $\mathcal{R}$. Then, we immediately obtain an upper bound for $p_{\text{out}-\text{con}}$ as

$$p_{\text{out}-\text{con}} \le \mathbb{P}\{\text{no in-isolated nodes in } \mathcal{R}\}. \qquad (30)$$

We would like to express the right-hand side in terms of the individual in-isolation probability determined in [31, eq. 9]. In general, this is nontrivial because the in-isolation events for different nodes are statistically dependent. For example, if legitimate node $x_{\text{A}}$ is in-isolated and node $x_{\text{B}}$ is close to $x_{\text{A}}$, then it is most likely that $x_{\text{B}}$ is also in-isolated. Full connectivity has been previously studied in the case of the Poisson Boolean model for unsecured wireless networks.[23] For such scenario, it has been shown in [36], [55], and [56] that as the average node degree $\pi\lambda r_{\max}^2$ becomes large, two phenomena are observed: 1) the isolation events for different nodes become almost independent; and 2) $\mathbb{P}\{\text{full connectivity}\} \approx \mathbb{P}\{\text{no isolated nodes}\}$, i.e., a bound analogous to (30) becomes tight. These two facts imply that for the Poisson Boolean model, the $\mathbb{P}\{\text{no isolated nodes}\}$ is both a simple and accurate analytical approximation for $\mathbb{P}\{\text{full connectivity}\}$, when $\pi\lambda r_{\max}^2 \to \infty$.

We now investigate under which conditions similar phenomena occur in the $i\mathcal{S}$-graph. For that purpose, we introduce the following definition:

[23]The Poisson Boolean model is an undirected model where each node can establish wireless links to all nodes within a fixed connectivity range $r_{\max}$, but to no other.

$$\widetilde{p}_{\mathrm{out-con}} \triangleq \mathbb{E}_{N_{\mathcal{R}}}\{(1-p_{\mathrm{in-isol}})^{N_{\mathcal{R}}}\} \tag{31}$$

where $N_{\mathcal{R}} = \Pi_{\ell}\{\mathcal{R}\}$ is the random number of legitimate nodes inside the region $\mathcal{R}$ (excluding the probe node at the origin). The quantity $\widetilde{p}_{\mathrm{out-con}}$ represents the probability that none of the $N_{\mathcal{R}}$ legitimate nodes are in-isolated, under the approximation that the in-isolation events are *independent* and have the same probability $p_{\mathrm{in-isol}}$ given in [31, eq. 9]. As we will show later, this quantity can serve as a good approximation of $p_{\mathrm{out-con}}$, with the advantage that it only depends on local characteristics (the isolation probabilities) of the $i\mathcal{S}$-graph and is analytically tractable. This can be shown by rewriting (31) as

$$\begin{aligned}\widetilde{p}_{\mathrm{out-con}} &= \sum_{n=0}^{\infty} \frac{(\lambda_{\ell}A)^n \exp(-\lambda_{\ell}A)}{n!}(1-p_{\mathrm{in-isol}})^n \\ &= \exp(-\lambda_{\ell}A p_{\mathrm{in-isol}}) \\ &= \exp\left(-\lambda_{\ell}A\mathbb{E}\left\{e^{-\frac{\lambda_{\ell}}{\lambda_{\mathrm{e}}}\widetilde{A}}\right\}\right)\end{aligned} \tag{32}$$

where $\widetilde{A}$ is the (random) area of a typical Voronoi cell induced by a unit-density Poisson process. Here, we used the expression for $p_{\mathrm{in-isol}}$ in [31, eq. 9].

For the case of full in-connectivity, we can proceed in a completely analogous way to write

$$p_{\mathrm{in-con}} \leq \mathbb{P}\{\text{no out-isolated nodes in } \mathcal{R}\} \tag{33}$$

and

$$\begin{aligned}\widetilde{p}_{\mathrm{in-con}} &\triangleq \mathbb{E}_{N_{\mathcal{R}}}\{(1-p_{\mathrm{out-isol}})^{N_{\mathcal{R}}}\} \\ &= \exp(-\lambda_{\ell}A\, p_{\mathrm{out-isol}}) \\ &= \exp\left(-A\frac{\lambda_{\ell}\lambda_{\mathrm{e}}}{\lambda_{\ell}+\lambda_{\mathrm{e}}}\right)\end{aligned} \tag{34}$$

where we used the expression for $p_{\mathrm{out-isol}}$ in [31, eq. 14].

Furthermore, according to [31, Property 3.2], we know that $p_{\mathrm{in-isol}} < p_{\mathrm{out-isol}}$ for $\lambda_{\ell} > 0$ and $\lambda_{\mathrm{e}} > 0$, and therefore

$$\widetilde{p}_{\mathrm{out-con}} > \widetilde{p}_{\mathrm{in-con}}.$$

As a result, in the regime where $\widetilde{p}_{\mathrm{in-con}}$ and $\widetilde{p}_{\mathrm{out-con}}$ closely approximate $p_{\mathrm{in-con}}$ and $p_{\mathrm{out-con}}$, respectively, $p_{\mathrm{out-con}}$ will be typically larger than $p_{\mathrm{in-con}}$. Intuitively, it is *easier* for an individual node to be *locally in-connected* than out-connected, and this fact is reflected in the global connectivity properties of the $i\mathcal{S}$-graph, in the sense that it is *easier* for the origin to be *fully out-connected* (reach all nodes) than fully in-connected (be reached by all nodes).

### D. Simulation Results

In this section, we use Monte Carlo simulations to determine under which conditions $p_{\mathrm{in-con}}$ and $p_{\mathrm{out-con}}$ can be accurately approximated by $\widetilde{p}_{\mathrm{in-con}}$ and $\widetilde{p}_{\mathrm{out-con}}$, respectively. Fig. 9 considers full out-connectivity, comparing three different probabilities as a function of $\lambda_{\mathrm{e}}$ and $\lambda_{\ell}$.

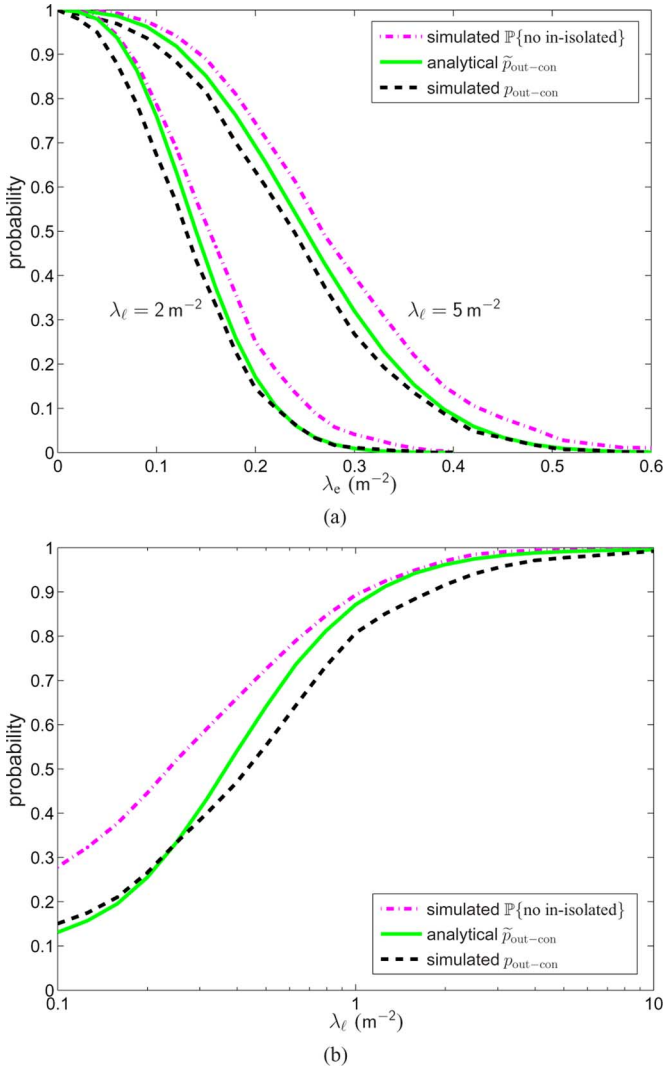


Fig. 9. Full out-connectivity in the Poisson $iS$-graph ($A = 100\ \mathrm{m}^2$, $\varrho = 0$) (a) Connection probabilities versus the eavesdropper density $\lambda_{\mathrm{e}}$, for various values of $\lambda_{\ell}$. (b) Connection probabilities versus the spatial density $\lambda_{\ell}$ of legitimate nodes ($\lambda_e = 0.05\ \mathrm{m}^{-2}$).

1) The simulated $\mathbb{P}\{\text{no in-isolated nodes in } \mathcal{R}\}$, which is an upper bound for $p_{\mathrm{out-con}}$ as given in (30).
2) The analytical $\widetilde{p}_{\mathrm{out-con}}$, whose expression is given in (32).
3) The simulated probability of full out-connectivity, $p_{\mathrm{out-con}}$.

From the plots, we observe that the analytical curve $\widetilde{p}_{\mathrm{out-con}}$ approximates $p_{\mathrm{out-con}}$ surprisingly well for all $\lambda_{\ell}$ and $\lambda_{\mathrm{e}}$, considering the strong approximations associated with $\widetilde{p}_{\mathrm{out-con}}$. Furthermore, the approximation becomes tight in the extreme ranges where $\lambda_{\ell}A \to \infty$ or $\lambda_{\mathrm{e}}A \to 0$ (i.e., $p_{\mathrm{out-con}} \approx 1$). This corresponds to the regime where it is desirable to operate the network in practice, in the sense that secure out-connectivity is achieved with probability very close to one.

Fig. 10 is analogous to Fig. 9, but for the case of full in-connectivity. It compares $\mathbb{P}\{\text{no out-isolated nodes in } \mathcal{R}\}$, $p_{\mathrm{in-con}}$, and $\widetilde{p}_{\mathrm{in-con}}$, as a function of $\lambda_{\mathrm{e}}$ and $\lambda_{\ell}$. We observe that the approximation of $p_{\mathrm{in-con}}$ by $\widetilde{p}_{\mathrm{in-con}}$ becomes tight when $\lambda_{\mathrm{e}}A \to 0$ (i.e., $p_{\mathrm{in-con}} \approx 1$), but *not* when $\lambda_{\ell}A \to \infty$,

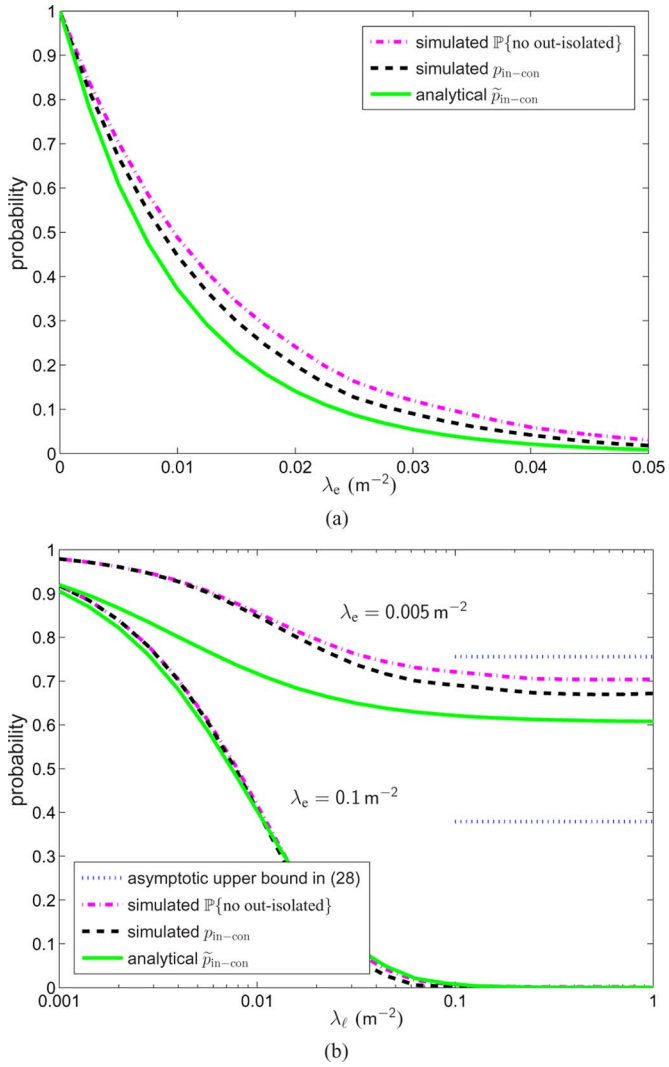


Fig. 10. Full in-connectivity in the Poisson $iS$-graph ($A = 100$ m$^2$, $\varrho = 0$). (a) Connection probabilities versus the eavesdropper density $\lambda_e$ ($\lambda_\ell = 1$ m$^{-2}$). (b) Connection probabilities versus the spatial density $\lambda_\ell$ of legitimate nodes, for various values of $\lambda_e$.

unlike what happens for full out-connectivity. Also, note that the curves *decrease* with $\lambda_\ell$: this is due to the same phenomenon illustrated in Fig. 8, whereby adding more legitimate nodes just increases the chance that some of them will be out-isolated.

In general, based on the simulations, we conclude that $\widetilde{p}_{\text{out-con}}$ and $\widetilde{p}_{\text{in-con}}$ are fairly good approximations for the corresponding probabilities of full connectivity, for a wide range of parameters. The main advantage is that $\widetilde{p}_{\text{out-con}}$ and $\widetilde{p}_{\text{in-con}}$ only depend on the *local* characterization of the network, namely on the isolation probabilities, and thus lead to simple analytical expressions which can be used to infer about the *global* behavior of the network. In particular, they are simple enough to be used in first-order dimensioning of the system, providing the network designer with valuable insights on how $p_{\text{out-con}}$ and $p_{\text{in-con}}$ vary with the parameters $\lambda_\ell$, $\lambda_e$, and $A$.

## V. Conclusion

The $i\mathcal{S}$-graph captures the connections that can be established with MSR exceeding a threshold $\varrho$, in large-scale networks. In [31] and [32], we characterized the *local properties* of the $i\mathcal{S}$-graph, including the degrees and MSR of a typical node with respect to its neighbors. In this paper, we have built on that work and analyzed the *global properties* of the $i\mathcal{S}$-graph, namely percolation on the infinite plane, and connectivity on a finite region. Interestingly, some local metrics such as the isolation probability, although quite simple to derive, provide insights into the more complex notion of global connectivity.

We first characterized percolation of the Poisson $i\mathcal{S}$-graph on the infinite plane. We showed that each of the four components of the $i\mathcal{S}$-graph (in, out, weak, and strong) experiences a phase transition at some nontrivial critical density $\lambda_c^\diamond$ of legitimate nodes. Operationally, this is important because it implies that long-range communication over multiple hops is still feasible when a secrecy constraint is present. We proved that percolation can occur for any prescribed infimum secrecy rate $\varrho$ satisfying $\varrho < \varrho_{\max} = \log_2\left(1 + \frac{P \cdot g(0)}{\sigma^2}\right)$, as long as the density of legitimate nodes is made large enough. This implies that for unbounded path loss models, percolation can occur for *any* arbitrarily large secrecy requirement $\varrho$, while for bounded models the desired $\varrho$ may be too high to allow percolation. Our results also show that as long as $\varrho < \varrho_{\max}$, percolation can be achieved even in cases where the eavesdroppers are arbitrarily dense, by making the density of legitimate nodes large enough.

Using Monte Carlo simulations, we obtained estimates for the critical densities $\lambda_c^\diamond$. In the case of $\varrho = 0$, for example, we estimated that if the density of eavesdroppers is larger than roughly 40% that of the legitimate nodes, long-range communication in the weak $i\mathcal{S}$-graph is completely disrupted, in the sense that no infinite cluster arises. In the strong $i\mathcal{S}$-graph, we estimated this fraction to be about 20%. For a larger secrecy requirement $\varrho$, an even more modest fraction of attackers is enough to disrupt the network.

Besides considering the existence of an unbounded component on the infinite plane, we also analyzed the existence of a fully-connected $i\mathcal{S}$-graph on a finite region. Specifically, we characterized the asymptotic behavior of secure full connectivity for a large density $\lambda_\ell$ of legitimate nodes. In particular, we showed $p_{\text{out-con}}$ approaches one as $\lambda_\ell \to \infty$, and therefore, full out-connectivity can be improved as much as desired by deploying more legitimate nodes. Full in-connectivity, however, remains bounded away from one, regardless of how large $\lambda_\ell$ is made. Operationally, this means a node can a.a.s. *transmit* secret messages to all the nodes in a finite region $\mathcal{R}$, but cannot a.s.s. *receive* secret messages from all the nodes in $\mathcal{R}$.

We derived simple expressions that closely approximate $p_{\text{out-con}}$ and $p_{\text{in-con}}$ for a finite density $\lambda_\ell$ of legitimate nodes. The advantage of these approximate expressions is that they only depend on the *local* characterization of the network, namely on the isolation probabilities, and thus lead to simple analytical expressions which can be used to infer about the

*global* behavior of the network. In particular, our expressions show that typically $p_{\mathrm{out-con}} > p_{\mathrm{in-con}}$, i.e., it is easier for a node to be fully out-connected (reach all nodes) than fully in-connected (be reached by all nodes). Our expressions explicitly show that this fact can be directly explained in terms of the *local connectivity*: it is easier for an individual node to be locally in-connected than out-connected, and this is reflected in the behavior of global connectivity described previously. Using Monte Carlo simulations, we showed that the approximate expressions are surprisingly accurate for a wide range of densities $\lambda_\ell$ and $\lambda_{\mathrm{e}}$.

We are hopeful that further efforts in combining stochastic geometry with information-theoretic principles will lead to a more comprehensive treatment of wireless security.

## APPENDIX
## PROOF OF LEMMA 3.3

*Proof:* In what follows, we use a coupling argument. For fixed parameters $\lambda_{\mathrm{e}}$ and $\varrho$, we begin with an $i\mathcal{S}$-graph $G(\lambda_{\ell,2})$ whose underlying process $\Pi_\ell$ has density $\lambda_{\ell,2}$. We then thin this process by keeping each point of $\Pi_\ell$ with probability $\frac{\lambda_{\ell,1}}{\lambda_{\ell,2}}$ where $\lambda_{\ell,1} \leq \lambda_{\ell,2}$, such that when a point is removed, all its in- and out-connections are also removed. Because of the thinning property [45, Sec. 5.1], the resulting process of legitimate nodes has density $\lambda_{\ell,1}$, and we have, therefore, obtained a valid new $i\mathcal{S}$-graph $G(\lambda_{\ell,1})$, with the same parameters $\lambda_{\mathrm{e}}$ and $\varrho$ as before. By construction, the two graphs $G(\lambda_{\ell,1})$ and $G(\lambda_{\ell,2})$ are coupled in such a way that $\mathcal{K}^{\diamond}_{\lambda_{\ell,1}}(0) \subseteq \mathcal{K}^{\diamond}_{\lambda_{\ell,2}}(0)$. As a result, the event $\{|\mathcal{K}^{\diamond}_{\lambda_{\ell,1}}(0)| = \infty\}$ implies that $\{|\mathcal{K}^{\diamond}_{\lambda_{\ell,2}}(0)| = \infty\}$, and it follows that $p^{\diamond}_{\infty}(\lambda_{\ell,1}) \leq p^{\diamond}_{\infty}(\lambda_{\ell,2})$. □

## ACKNOWLEDGMENT

The authors would like to thank J. N. Tsitsiklis, V. K. Goyal, W. Suwansantisuk, and O. Dousse for their helpful suggestions.

## REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.
[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[5] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.
[7] E. Ekrem and S. Ulukus, "Secrecy capacity region of the Gaussian multi-receiver wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 2612–2616.
[8] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
[9] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.
[10] L. Zhang, R. Zhang, Y. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," presented at the presented at the Allerton Conf. Commun., Control, Comput., Monticello, IL, Sep. 2009.
[11] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. Military Commun. Conf.*, Oct. 2005, pp. 1501–1506.
[12] P. C. Pinto, J. O. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jul. 2009, pp. 2442–2446.
[13] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Jul. 2008, pp. 2217–2221.
[14] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.
[15] P. Gopala, L. Lai, and H. E. Gamal, On the secrecy capacity of fading channels 2006, arxiv preprint cs.IT/0610103.
[16] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. Annu. Allerton Conf. Commun., Control Comput.*, Sep. 2006, pp. 841–848.
[17] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[18] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[19] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Lecture Notes Comput. Sci.*, vol. 1807, pp. 351–368, 2000.
[20] J. Barros and M. Bloch, "Strong secrecy for wireless channels," presented at the presented at the Int. Conf. Inf. Theor. Security, Calgary, Canada, Aug. 2008.
[21] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[22] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[23] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[24] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.
[25] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC-based secret key agreement over the Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, 2006, pp. 1179–1183.
[26] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[27] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, Sep. 2007, pp. 337–342.
[28] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, vol. E89-A, no. 7, pp. 2036–2046, Jul. 2006.
[29] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 539–543.
[30] P. C. Pinto, J. O. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Syst.*, Guangzhou, China, Nov. 2008, pp. 974–979.
[31] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
[32] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
[33] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 1189–1193.
[34] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," in *Proc. Inf. Theory Appl. Workshop*, San Diego, CA, Feb. 2010, pp. 1–4.

[35] E. N. Gilbert, "Random plane networks," *J. Soc. Ind. Appl. Math.*, vol. 9, pp. 533–543, 1961.
[36] M. D. Penrose, "On a continuum percolation model," *Adv. Appl. Probabil.*, vol. 23, no. 3, pp. 536–556, 1991.
[37] O. Häggström and R. W. J. Meester, "Nearest neighbor and hard sphere models in continuum percolation," *Random Struct. Algorithm*, vol. 9, no. 3, pp. 295–315, 1996.
[38] O. Dousse, M. Franceschetti, N. Macris, R. Meester, and P. Thiran, "Percolation in the signal to interference ratio graph," *J. Appl. Probabil.*, vol. 43, no. 2, pp. 552–562, 2006.
[39] R. Meester and R. Roy, *Continuum Percolation*. Cambridge, U.K.: Cambridge Univ. Press, 1996.
[40] M. D. Penrose and A. Pisztora, "Large deviations for discrete and continuous percolation," *Adv. Appl. Probabil.*, vol. 28, no. 1, pp. 29–52, 1996.
[41] M. D. Penrose, "The longest edge of the random minimal spanning tree," *Ann. Appl. Probabil.*, vol. 7, no. 2, pp. 340–361, 1997.
[42] P. Gupta and P. Kumar, *Critical power for asymptotic connectivity in wireless networks*, vol. 16, no. 2, pp. 347–358, 1998.
[43] P. Balister, B. Bollobás, A. Sarkar, and M. Walters, "Connectivity of random k-nearest-neighbour graphs," *Adv. Appl. Probabil.*, vol. 37, no. 1, pp. 1–24, 2005.
[44] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *J. Wireless Netw.*, vol. 10, no. 2, pp. 169–181, 2004.
[45] J. Kingman, *Poisson Processes*. London, U.K.: Oxford Univ. Press, 1993.
[46] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.
[47] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
[48] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*. New York: Wiley, 1995.
[49] B. Bollobás and O. Riordan, *Percolation*. Cambridge, U.K.: Cambridge Univ. Press, 2006.
[50] M. Franceschetti and R. Meester, *Random Networks for Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2007.
[51] R. Peierls, "On Ising's model of ferromagnetism," *Proc. Cambridge Phil. Soc.*, vol. 32, pp. 477–481, 1936.
[52] G. Grimmett, *Percolation*. New York: Springer-Verlag, 1999.
[53] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proc. 3rd ACM Int. Symp. Mobile ad hoc Netw. Comput.*, New York, 2002, pp. 80–91, ACM.
[54] N. A. C. Cressie, *Statistics for Spatial Data*. New York: Wiley, 1993.
[55] D. Miorandi and E. Altman, "Coverage and connectivity of ad hoc networks in presence of channel randomness," in *Proc. IEEE Conf. Comput. Commun.*, Mar. 2005, vol. 1, pp. 491–502.
[56] C. Bettstetter and C. Hartmann, "Connectivity of wireless multihop networks in a shadow fading environment," *J. Wireless Netw.*, vol. 11, no. 5, pp. 571–579, Sep. 2005.

**Pedro C. Pinto** (S'04–M'10) received the Licenciatura degree with highest honors in Electrical and Computer Engineering from the University of Porto, Portugal, in 2003. He received the M.S. degree in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT) in 2006. Since 2004, he has been with the MIT Laboratory for Information and Decision Systems (LIDS), where he is now a Ph.D. candidate. His main research interests are in wireless communications and signal processing. He was the recipient of the MIT Claude E. Shannon Fellowship in 2007, the Best Student Paper Award at the IEEE International Conference on Ultra-Wideband in 2006, and the Infineon Technologies Award in 2003.

**Moe Z. Win** (S'85–M'87–SM'97–F'04) received both the Ph.D. in Electrical Engineering and M.S. in Applied Mathematics as a Presidential Fellow at the University of Southern California (USC) in 1998. He received an M.S. in Electrical Engineering from USC in 1989, and a B.S. (magna cum laude) in Electrical Engineering from Texas A&M University in 1987. Dr. Win is an Associate Professor at the Massachusetts Institute of Technology (MIT). Prior to joining MIT, he was at AT&T Research Laboratories for five years and at the Jet Propulsion Laboratory for seven years. His research encompasses developing fundamental theory, designing algorithms, and conducting experimentation for a broad range of real-world problems. His current research topics include location-aware networks, time-varying channels, multiple antenna systems, ultra-wide bandwidth systems, optical transmission systems, and space communications systems. Professor Win is an IEEE Distinguished Lecturer and elected Fellow of the IEEE, cited for "contributions to wideband wireless transmission." He was honored with the IEEE Eric E. Sumner Award (2006), an IEEE Technical Field Award for "pioneering contributions to ultra-wide band communications science and technology." Together with students and colleagues, his papers have received several awards including the IEEE Communications Society's Guglielmo Marconi Best Paper Award (2008) and the IEEE Antennas and Propagation Society's Sergei A. Schelkunoff Transactions Prize Paper Award (2003). His other recognitions include the Laurea Honoris Causa from the University of Ferrara, Italy (2008), the Technical Recognition Award of the IEEE ComSoc Radio Communications Committee (2008), Wireless Educator of the Year Award (2007), the Fulbright Foundation Senior Scholar Lecturing and Research Fellowship (2004), the U.S. Presidential Early Career Award for Scientists and Engineers (2004), the AIAA Young Aerospace Engineer of the Year (2004), and the Office of Naval Research Young Investigator Award (2003).