Percolation on the Information Theoretic Secure SINR Graph: Upper and Lower Bounds

Rahul Vaze
Tata Institute of Fundamental Research
School of Technology and Computer Science
Homi Bhabha Road, Mumbai 400005
email: vaze@tcs.tifr.res.in

Srikanth Iyer
Indian Institute of Science,
Department of Mathematics,
Bangalore, 560012,
e-mail: skiyer@math.iisc.ernet.in

***Abstract*—Connectivity in an information-theoretically secure graph is considered where both the legitimate and the eavesdropper nodes are distributed as Poisson point processes. To allow concurrent transmissions from multiple legitimate nodes, a signal-to-interference plus noise ratio secure graph is introduced, and its percolation (having an unbounded connected component) properties are studied. It is shown that for a fixed eavesdropper node density, percolation happens for large enough (but finite) legitimate node density and small enough interference suppression parameter of the legitimate nodes. Conversely, a concrete bound is obtained that shows that if the legitimate node density is below a fixed threshold, then the probability of percolation is zero.**

I. Introduction

Ensuring connectivity in wireless multi-hop networks is a challenging problem. Several seminal results have been obtained in this area [1], [2] starting with [3]. The problem is complicated because of the network topology, dynamic nature of connection between any pair of nodes, large range interdependency for connections between different pair of nodes, short range and long range fading etc. Another critical limitation of the wireless network is its broadcast nature that makes it vulnerable to eavesdropping. Through cryptographic techniques one can try to secure the communication, however, ensuring a feasible non-breakable cryptographic protocol over a large distributed wireless network is a daunting task. To avoid the complexities/limitations of a cryptographic protocol, we turn our attention to the information theoretic notion of secrecy that assumes the presence of eavesdropper with infinite capability and even then ensures that the randomness about the message at any eavesdropper does not change with the knowledge of the signal transmitted by the source [4].

Wyner [4] in his work on information theoretic security, showed that non-zero rate of secure communication is possible as long the channel to the eavesdropper is *weaker* compared to the intended receiver, even if the eavesdropper has infinite capability. This notion of security has been widely used for answering some basic fundamental questions in wireless communication [5]–[8].

Typically, connectivity in wireless networks is studied using the tools of percolation theory, e.g. in [9] for the SINR graph, where two nodes are connected if the SINR between them is greater than a threshold, and the random connection model in [10], where two nodes are connected with some probability that depends on the distance between them independently of other nodes. In recent work, connectivity in an information theoretic secure graph has been studied in [11]–[15], where two legitimate/licensed nodes i and j are connected, if node j is closer to node i than its nearest eavesdropper. The graph resulting out of this connection model is referred to as the *secrecy graph*. Following [4], with this model, communication between two legitimate nodes is secure from any eavesdropper with arbitrary capability.

The secrecy graph model of [11], [12], [14], [15], assumes that all legitimate nodes transmit in non-overlapping time/frequency slots, and their signals do not interfere with each other. For large number of legitimate nodes, this is not always feasible and severely limits the spatial capacity. To model the more realistic scenario that allows concurrent transmissions from legitimate nodes, we introduce and analyze the SINR secure graph (SSG) model, where a link between two legitimate nodes exists if the signal-to-interference ratio plus noise (SINR) between them is more than SINR between the legitimate node and any eavesdropper.

For this new model, we restrict ourselves to the path-loss model of wireless signal propagation (similar to [11]–[15]) with finite support and ignore multi-path fading. The SSG model is characterized by a parameter $\gamma, 0 < \gamma \leq 1$ which represents the interference suppression capability of any legitimate node. For example, if each legitimate node is using a CDMA system, then γ corresponds to the imperfect orthogonality of the codes used in CDMA, where $\gamma = 0$ implies perfect orthogonality between different legitimate users. Hence γ is multiplied to the total interference while computing the SINR at any legitimate node. An important aspect of SSG is that the interference suppression is not available at any eavesdropper, which corresponds to the *weaker* signal at the eavesdropper compared to the intended receiver in [4].

978-3-901882-63-0/2014

Similar to our SSG model, recently, capacity scaling laws of wireless networks in the presence of eavesdropper with the SINR model have been derived in [6]–[8]. For deriving capacity scaling laws of wireless networks, however, two nodes are defined to be connected even if the individual links on the connected path between the two nodes are not active simultaneously. In comparison, while considering connectivity/percolation, we ask for the existence of an unbounded connected component where all links are active simultaneously. Thus results obtained in [6]–[8] do not apply for studying percolation on the SSG graph.

II. Our Contributions

- (Super-Critical Regime) For the SSG, when the distance based path-loss or signal attenuation function has a finite support, we show that for small enough γ, there exists a large enough legitimate node density for which the SSG percolates for any value of eavesdropper node density. By percolation, we mean there is an unbounded size connected component in the network. This result is similar in spirit to [9], [16], where percolation is shown to happen in the SINR graph, where two nodes are connected if the SINR between them is more than a fixed threshold β, (without the secrecy constraint due to eavesdroppers) for small enough γ with finite and infinite support signal attenuation function, respectively. The major difference between the SSG and SINR graph [9], [16], is that with SSG, the threshold for connection between two nodes (maximum of SINRs received at all eavesdroppers) is a random variable that depends on both the legitimate and eavesdropper density, in contrast to the SINR graph, where the threshold is a fixed constant.
- (Sub-Critical Regime) For the SSG, when the distance based signal attenuation function has a finite support, we derive a lower bound on the critical density of legitimate nodes required for percolation. We show that if the density of legitimate nodes is less than $\frac{1}{C\pi\mathbb{E}\{\rho^2\}}$, ρ is the random variable representing the maximum distance to which any legitimate node can connect directly to any other legitimate node in the SSG, and C is a constant, then the probability of percolation is zero. We use the technique developed in [17] for studying percolation on the random Boolean model, where nodes are spatially distributed as a Poisson point process (PPP), and balls with i.i.d. radius are centered at each node of the PPP. The random Boolean model is said to percolate if the area of the region spanned by the union of overlapping (connected) balls is unbounded. We show that for the distance based signal attenuation function with finite support, we can adapt the proof of [17] to obtain a lower bound of on the critical density.

III. System Model

In this section, we introduce the SSG, which generalizes the secrecy graph considered in [11], by allowing all legitimate nodes to transmit at the same time/frequency and interfere with each other's communication. We restrict ourselves to the path-loss model of signal propagation and ignore multi-path fading. Let Φ be the set of legitimate nodes, and Φ_E be the set of eavesdropper nodes. Let x_i and x_j, $x_i, x_j \in \Phi$, want to communicate secretly, i.e. without providing any knowledge of their communication to any node in Φ_E. Let the distance between x_i and x_j be denoted as d_{ij}. Then to send a message m, x_i sends a signal $\mathbf{s}_i = (s_i(1), \dots, s_i(n))$ to x_j over n time slots. The received signals at x_j denoted by y_j, and at $e \in \Phi_E$ denoted by y_e, are

$$y_j(t) = \ell(x_i, x_j)s_k(t) + \sqrt{\gamma} \sum_{x_k \in \Phi,\ k \neq i} \ell^{1/2}(x_k, x_j)s_k(t) + v_{ij}(t),$$

and

$$y_e(t) = \ell(x_i, e)s_i(t) + \sum_{x_k \in \Phi,\ k \neq i} \ell^{1/2}(x_k, e)s_k(t) + v_{ie}(t),$$

for $t = 1, 2, \dots, n$, respectively, where $\ell(x_i, x_j) = \ell(|x_i - x_j|) = \ell(d_{ij})$ is the signal attenuation function that is a decreasing function of distance d_{ij} between x_i and x_j, $0 < \gamma \leq 1$ is the processing gain of the system (interference suppression parameter) which depends on the transmission/detection strategy. For example, on orthogonality between codes used by different legitimate nodes during simultaneous transmissions, e.g. CDMA system [18], and $v_{ij}(t)$ and $v_{ie(t)}$ are additive White Gaussian noise terms with zero mean and unit variance. No processing gain is, however, available at any of the eavesdroppers. We assume that the signal attenuation function $\ell(.)$ has a finite support, i.e. $\ell(x) = 0$ for $x > \eta, \eta > 0$ for reasons described in Remark 5. Finite support signal attenuation functions have been considered in prior work on percolation on SINR graph [16].

We assume that $\mathbf{s}_i, v_{ij}(t), v_{ie}(t)$ are independent of each other. Without loss of generality, we assume an average power constraint of unity at each node in Φ. Then the SINR between x_i and x_j is

$$\mathsf{SINR}_{ij} := \frac{\ell(x_i, x_j)}{\gamma \sum_{x_k \in \Phi,\ k \neq i} \ell(x_k, x_j) + 1},$$

and between x_i and e is

$$\mathsf{SINR}_{ie} := \frac{\ell(x_i, e)}{\sum_{x_k \in \Phi,\ k \neq i} \ell(x_k, e) + 1}.$$

From [4], [6], the maximum rate of reliable communication between x_i and x_j such that an eavesdropper e gets no knowledge about message m, is

$$R_{ij}(e) := \left[\log_2\left(1 + \mathsf{SINR}_{ij}\right) - \log_2\left(1 + \mathsf{SINR}_{ie}\right)\right]^+, \quad (1)$$

and the maximum rate of communication between x_i and x_j that is secured from all the eavesdropper nodes of Φ_E,

$$R_{ij}^{\mathsf{SINR}} := \min_{e \in \Phi_E} R_{ij}(e).$$

We note that the information theoretic secure rate $R_{ij}(e)$ depends on modeling assumptions, however, the basic structure of the secure rate function $R_{ij}(e)$ (1) remains unchanged. In any case, the focus of this paper is to develop techniques to study the percolation behavior of random graphs originating from secure models of communication with simultaneous communication between all nodes, that remains valid for a wide class of secure rate functions.

Definition 1: SINR Secrecy graph (SSG) is a directed graph $SSG(\theta) := \{\Phi, \mathcal{E}\}$, with vertex set Φ, and edge set $\mathcal{E} := \{(x_i, x_j) : R_{ij}^{\mathsf{SINR}} > \theta\}$, where θ is the minimum rate of secure communication required between any two nodes of Φ.

Similar to [11], [12], [14], in this paper we assume that the locations of Φ and Φ_E are distributed as independent homogenous Poisson point processes (PPPs) with intensities λ and λ_E, respectively.

Definition 2: We define that a node x_i can *connect* to x_j (or there is a link/connection between them) if $(x_i, x_j) \in SSG$.

Definition 3: We define that there is a *path* from node $x_i \in \Phi$ to $x_j \in \Phi$ if there is a connected path from x_i to x_j in the SSG. A path between x_i and x_j on SSG is represented as $x_i \to x_j$.

Definition 4: The connected component of any node $x_j \in \Phi$, is defined as $C_{x_j} := \{x_k \in \Phi, x_j \to x_k\}$, with cardinality $|C_{x_j}|$.

Remark 1: Note that because of stationarity of the PPP, the distribution of $|C_{x_j}|$ does not depend on j, and we consider a typical mark x_1 located at the origin for the purposes of defining connected components.

In this paper we are interested in studying the percolation properties of the SSG. In particular, we are interested in finding the minimum value of λ, λ_c, for which the probability of having an unbounded connected component in SSG is greater than zero as a function of λ_E, i.e. $\lambda_c := \min\{\lambda : P(|\mathcal{C}_{x_1}| = \infty) > 0\}$. The event $\{|\mathcal{C}_{x_1}| = \infty\}$ is also referred to as *percolation* on SSG, and we say that percolation happens if $P(\{|\mathcal{C}_{x_1}| = \infty\}) > 0$, and does not happen if $P(\{|\mathcal{C}_{x_1}| = \infty\}) = 0$. The regime of $\lambda < \lambda_c$ is known as the *sub-critical* regime, while the $\lambda > \lambda_c$ regime is known as the *super-critical* regime.

Remark 2: Note that $SSG(\theta) \subseteq SSG(0)$ for $\theta > 0$. Therefore if $SSG(0)$ does not percolate then $SSG(\theta)$ also cannot percolate, hence considering the sub-critical regime for $SSG(0)$ is sufficient. For the super-critical regime, we will only show the existence of percolation for $SSG(0)$ for large enough λ and small enough γ. The same result can be shown to hold for $SSG(\theta)$ for $\theta > 0$ using the same technique.
Thus, for simplicity of the exposition, we will consider $\theta = 0$ for the rest of the paper, and represent $SSG(0)$ as SSG. With $\theta = 0$, $SSG := \{\Phi, \mathcal{E}\}$, with edge set $\mathcal{E} := \{(x_i, x_j) : \mathsf{SINR}_{ij} > \mathsf{SINR}_{ie}, \ \forall \ e \in \Phi_E\}$.

Remark 3: Assuming that all legitimate nodes can transmit in orthogonal time/frequency slots, secrecy graph SG was introduced in [11], where two legitimate nodes are connected if the received signal power between them is more than the received signal power at the nearest eavesdropper, i.e. $SG := \{\Phi, \mathcal{E}\}$, with vertex set Φ, and edge set $\mathcal{E} := \{(x_i, x_j) : \ell(x_i, x_j) > \ell(x_i, e), \ \forall \ e \in \Phi_E\}$. Percolation properties of SG were studied in [12], [14], where in [14] it was shown that if $\lambda < \lambda_E$, then there is no percolation, while [12] showed the existence of λ for any fixed λ_E for which the SG percolates. The graph structure of SSG is more complicated compared to SG because of the presence of interference power terms corresponding to simultaneously transmitting legitimate nodes, and hence the results of [12], [14] do not apply for SSG. For example, consider the case of $\gamma = 0$ where it is possible that two legitimate nodes x_i and x_j, with $d_{ij} > \min_{e \in \Phi_E} d_{ie}$ can connect to each other in the SSG, however, x_i and x_j cannot connect to each other in the SG. Similarly, if x_j is closer to x_i than any other eavesdropper node, then x_i is connected to x_j in SG, however, that may not be the case in SSG.

Remark 4: Without the presence of eavesdropper nodes, percolation on the SINR graph, where the vertex set is Φ, and edge set $\mathcal{E} := \{(x_i, x_j) : \mathsf{SINR}_{ij} \geq \beta, x_i, x_j \in \Phi\}$ for some fixed threshold β, has been studied in [9], [16], [19]. The results of [9], [16], [19], however, do not apply for the SSG, since for SSG, $\beta = \mathsf{SINR}_{ie}$ is a random variable that depends on both Φ and Φ_E.

Remark 5: The graph structure of SSG is more complicated compared to secrecy graph [11], since the connection between any two legitimate nodes not only depends on all the eavesdropper nodes, but also on all the legitimate nodes through the interference they cause. For analytical tractability and to obtain meaningful insights, similar to [16], we assume that the signal attenuation function $\ell(x)$ has a finite support, i.e. $\ell(x) = 0$ for $x > \eta, \eta > 0$. This assumption is primarily made to limit the dependency of link formation between x_i and x_j to a finite area around x_i and x_j, $x_i, x_j \in \Phi$. Without this assumption, an eavesdropper node e that is far away from x_i and x_j can influence the link formation between them.

Remark 6: Note that we have defined SSG to be a directed graph, and the connected component of x_1 is its out-component, i.e. the set of nodes with which x_1 can communicate secretly. Since $x_i \to x_j, \ x_i, x_j \in \Phi$, does not imply $x_j \to x_i \ x_i, x_j \in \Phi$, one can similarly define in-component $C_{x_j}^{in} := \{x_k \in \Phi, x_k \to x_j\}$, bi-directional component $C_{x_j}^{bd} := \{x_k \in \Phi, x_k \to x_j \text{ and } x_k \to x_j\}$, and either one-directional component $C_{x_j}^{ed} := \{x_k \in \Phi, x_k \to x_j \text{ or } x_k \to x_j\}$. Percolation on $C_{x_j}^{in}$, $C_{x_j}^{bd}$ and $C_{x_j}^{ed}$ is in principle similar to the percolation on out-component, and is presently out of scope of this paper.

IV. Percolation on the SSG

A. Sub-Critical Regime

In this section, we are interested in obtaining a lower bound on λ_c as a function of λ_E for which percolation does not happen. For the sub-critical regime, we consider the case of $\gamma = 0$, where x_i and x_j are connected in the SSG if

$$\ell(d_{ij}) > \frac{\ell(x_i, e)}{1 + \sum_{j \neq i} \ell(x_j, e)}, \ \forall \ e \in \Phi_E, \tag{2}$$

for $d_{ij} \leq \eta$, since $\ell(x) = 0, x > \eta$. For $\gamma = 0$, if we can show that the critical density $\lambda_c > \lambda_0$ for some fixed $\lambda_0 \in \mathbb{R}^+$, then since SSG with $\gamma > 0$ is contained in SSG with $\gamma = 0$, we have that for all $\gamma > 0$, $\lambda_c > \lambda_0$. So the lower bound of λ_0 on λ_c obtained with $\gamma = 0$ serves as a universal lower bound on the critical density λ_c required for percolation.

For the case of $\gamma = 0$, we proceed as follows.

Definition 5: For a node $x_i \in \Phi$, we define the maximum distance to which it can have a connection in SSG as $\rho(x_i) = \sup \{d : \ \ell(d) > \max_{e \in \Phi_E} \mathsf{SINR}_{ie}\}$. Therefore, if $(x_i, x_j) \in SSG$ then following (2), x_j is such that $d_{ij} < \rho(x_i)$.

Remark 7: Note that $\rho(x_i) \leq \eta, \ \forall \ x_i$, since the signal power received at a distance x, $\ell(x)$, is zero for $x > \eta$. With the PPP assumption on both Φ and Φ_E, it follows that $\rho(x_i)$ is identically distributed for all $x_i \in \Phi$, and we represent it as ρ, and drop the index of node x_i where ever possible. The probability density function of ρ is denoted as ω_ρ. Since $\rho \leq \eta$, $\mathbb{E}\{\rho^m\} < \infty$ for a fixed m, however, finding $\mathbb{E}\{\rho^m\}$ explicitly is not straightforward, since it depends on the signal attenuation function $\ell(.)$.

Remark 8: From the definition of ρ (5), it is immediate that ρ is a non-decreasing (stochastic) function of λ, since $\mathsf{SINR}_{ie}, \ \forall \ e \in \Phi_E$ decreases with increasing λ, and a non-increasing function of λ_E, since $\max_{e \in \Phi_E} \mathsf{SINR}_{ie}$ increases with increasing λ_E.

Let D_m be the square box with side $2m$ centered at the origin, i.e. $D_m = [-m \ m] \times [-m \ m]$. For $r \geq \eta$, consider any node $x_1 \in \Phi \cap D_r$,[1] and let $\mathcal{C}_{x_1}$ be its connected component. Let $x_L \in \mathcal{C}_{x_1}$ be the farthest node from x_1 in terms of Euclidean distance as shown in Fig. 1.

Definition 6: Let $E(q, r), \ q \in \mathbb{R}^2$, be the event that there is a path from a node $x \in \Phi \cap (q + D_r)$ to a node $w \in \Phi \cap (q + D_{9r} \backslash q + D_{8r})$. Note that due to stationarity $P(E(q, r)) = P(E(\mathbf{0}, r))$.

Recall that the quantity of interest is $P(|\mathcal{C}_{x_1}| = \infty)$. Let the complement of set $A \subset \mathbb{R}^2$ be denoted by $\bar{A} = \mathbb{R}^2 \backslash A$. Clearly, $P(|\mathcal{C}_{x_1}| = \infty) \leq \lim_{r \to \infty} P(x_L \in \bar{D}_{10r})$, since infinitely many nodes of a PPP cannot lie in a finite region. Thus, to upper bound $P(|\mathcal{C}_{x_1}| = \infty)$, it is sufficient to upper bound $P(x_L \in \bar{D}_{10r})$, which can be done as follows.

Lemma 1:

$$P(x_L \in \bar{D}_{10r}) \leq P(E(\mathbf{0}, r)).$$

[1] Without loss of generality we can assume that x_1 is located at the origin.

Proof: Since the maximum distance between any two connected legitimate nodes $\rho(x) \leq \eta$, where $r \geq \eta$, if the farthest node x_L of $\mathcal{C}_{x_1}$ lies in $\bar{D}_{10r}$, then there is at least one node on the connected path between x_1 and x_L that lies in $D_{mr} \backslash D_{(m-1)r}$ for each $m = 2, \ldots, 10$. In particular, there is a path from $x_1 \in D_r$ to some node $w \in D_{9r} \backslash D_{8r}$, i.e. $E(\mathbf{0}, r)$ occurs. Hence $P(x_L \in \bar{D}_{10r}) \leq P(E(\mathbf{0}, r))$.

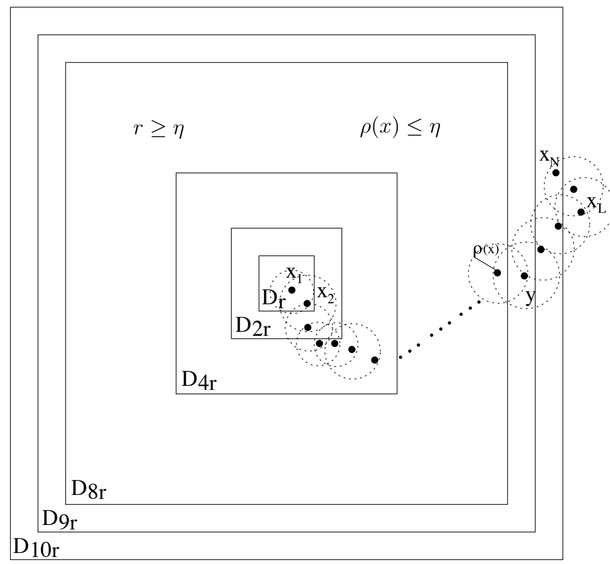

Fig. 1. Illustration of connected component of x_1 (origin) and event $E(\mathbf{0}, r)$.

Hence to show that $\lim_{r \to \infty} P(x_L \in \bar{D}_{10r}) = 0$ for $\lambda < \lambda_0$, using Lemma 1, it is sufficient to show that $P(E(\mathbf{0}, r))$ goes to zero as $r \to \infty$ for $\lambda < \lambda_0$, which is proved in the next Lemma.

Lemma 2: For $\lambda < \frac{1}{C\pi\mathbb{E}\{\rho^2\}}$, where C is a constant, $P(E(\mathbf{0}, r)) \to 0$ as $r \to \infty$.

Proof: See Appendix A.

The main Theorem of this subsection is as follows.

Theorem 1: The critical density $\lambda_c \geq \frac{1}{C\pi\mathbb{E}\{\rho^2\}}$, where C is a constant.

Proof: From Lemma 1, $P(|\mathcal{C}_{x_1}| = \infty) \leq \lim_{r \to \infty} P(E(\mathbf{0}, r))$. From Lemma 2, for $\lambda \leq \frac{1}{C\pi\mathbb{E}\{\rho^2\}}$, $\lim_{r \to \infty} P(E(\mathbf{0}, r)) = 0$.

From Remark 8, we can let $\mathbb{E}\{\rho^2\} := g(\lambda, \lambda_E)$, where g is a non-decreasing function of λ, and a non-increasing function of λ_E. Thus, Theorem 1 states that if $\lambda g(\lambda, \lambda_E) < \frac{1}{\pi C}$, then the connected component of x_1 is bounded for any $x_1 \in \Phi$.

The main ingredient of the proof of Theorem 1 is Lemma 2 that is proved in Appendix A using ideas similar to [17], where a lower bound on the critical density is derived for a random Boolean model. In a random Boolean model, nodes are spatially distributed as a PPP, and balls with i.i.d. radius are centered at each node of the PPP. The quantity of interest is the region spanned by the union of overlapping balls (also called the connected component). Percolation on the SSG is similar to the random Boolean model, however, where two nodes x_i and x_j have an edge in SSG if $\ell(d_{ij}) > \frac{\ell(x_i,e)}{1+\sum_{j\neq i}\ell(x_j,e)}$, $\forall\, e \in \Phi_E$. Thus, with SSG, for two different nodes $x_i, x_k \in \Phi$, the distance to which they can connect to other nodes of Φ is correlated, and hence the proof of [17] does not apply directly.

Discussion: In this section, we obtained a universal lower bound on the critical intensity λ_c required for percolation in the SINR secure graph, where all nodes are allowed to transmit simultaneously with $\gamma = 0$. As discussed before, the lower bound with $\gamma = 0$ holds for all $\gamma > 0$ as well. Our proof is an adaptation of [17], for the non-independent radii of connectivity under the finite support signal attenuation function. The main idea behind the proof is that if λ is below a threshold (the derived lower bound), the probability that there is a path between two legitimate nodes at a distance r from each other goes to zero as $r \to \infty$. Therefore with probability one, if λ is below a threshold, the connected component of any node lies inside a bounded region, and since infinitely many nodes of a PPP do not lie in a bounded region, the connected component of any node is finite.

In prior work, a lower bound of $\lambda_c > \lambda_E$ has been derived in [11] for the secrecy graph model, where each legitimate node can communicate with any other node without causing interference to any other node by using non-overlapping time/frequecy slot. The results of [11], are derived using the branching process arguments on the out-degree distribution, similar to [20]. With the SSG, however, it is difficult to find even the marginal distribution of the out-degree distribution for any legitimate node. Hence, we used an alternate technique developed in [17] for the random Boolean model.

B. Super-Critical Regime

In this section, we are interested in the super-critical regime and want to find an upper bound on λ_c. Towards that end, we will tie up the percolation on SSG to a bond percolation on the square lattice, and show that bond percolation on the square lattice implies percolation in the SSG.

We tile $\mathbb{R}^2$ into a square lattice $\mathbf{S}$ with side s. Let $\mathbf{S}' = \mathbf{S} + (\frac{s}{2}, \frac{s}{2})$ be the dual lattice of $\mathbf{S}$ obtained by translating each edge of $\mathbf{S}$ by $(\frac{s}{2}, \frac{s}{2})$. For any edge $\mathbf{a}$ of $\mathbf{S}$, let $S_1(\mathbf{a})$ and $S_2(\mathbf{a})$ be the two adjacent squares to $\mathbf{a}$. See Fig. 2 for a pictorial description. Let $\{a_i\}_{i=1}^4$ denote the four vertices of the rectangle $S_1(\mathbf{a}) \cup S_2(\mathbf{a})$. Let $Y(\mathbf{a})$ be the smallest square containing $\cup_{i=1}^4 \mathbf{B}(a_i, \eta)$, and $Z(\mathbf{a})$ be the smallest square containing $\cup_{i=1}^4 \mathbf{B}(a_i, \sqrt{5}s)$. In the sequel, we will let s to be small enough, so without loss of generality, let $\eta > s$.

Definition 7: Any edge $\mathbf{a}$ of $\mathbf{S}$ is defined to be open if

1) there is at least one node of Φ in both the adjacent squares $S_1(\mathbf{a})$ and $S_2(\mathbf{a})$,
2) there are no eavesdropper nodes in $Z(\mathbf{a})$,
3) and for any pair of legitimate nodes $x_i, x_j \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$, the interference received at x_j from all legitimate nodes Φ other than x_i, $I_j^i := \sum_{k\in\Phi, k\neq i} \ell(x_k, x_j) \leq \frac{\epsilon}{\gamma}$, and for any eavesdropper node $e \in \Phi_E \cap Y(\mathbf{a})$, the interference received from legitimate nodes Φ other than $x_i \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$, $I_e^i := \sum_{k\in\Phi, k\neq i} \ell(x_k, x_e) > \epsilon$ for any fixed $\epsilon > 0$.

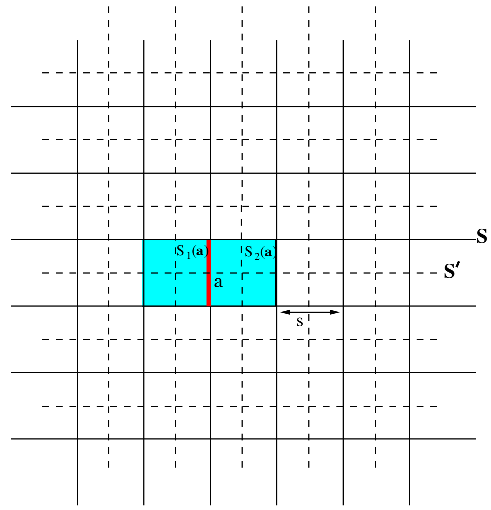

Fig. 2. Square lattice and its dual lattice with side s.

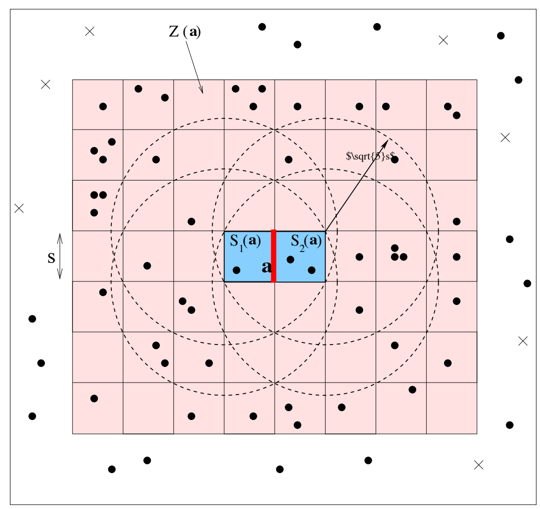

Fig. 3. Open edge definition where black dots represent a legitimate node while a cross represents an eavesdropper node.

An open edge is pictorially described in Fig. 3 by red edge a, where the black dots represent a legitimate node while a cross represents an eavesdropper node.

The next Lemma allows us to tie up the continuum percolation on SSG to the bond percolation on the square lattice, where we show that if an edge $\mathbf{a}$ is open, then all legitimate nodes lying in $S_1(\mathbf{a}) \cup S_2(\mathbf{a})$ can connect to each other.

Lemma 3: If an edge $\mathbf{a}$ of $\mathbf{S}$ is open, then any node $x_i \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$ can connect to any node $x_j \in$

$\Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$ in SSG.

Proof: First note that since $\ell(x) = 0$ for $x > \eta$, $\mathsf{SINR}_{ie} = 0$ for $x_i \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$ and $e \in \Phi_E \cap \bar{Y}(\mathbf{a})$. Now for $x_i, x_j \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$, by definition of an open edge $\mathsf{SINR}_{ij} \geq \frac{\ell(\sqrt{5}s)}{1+\epsilon}$, while for $x_i \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$ and $e \in \Phi_E \cap Y(\mathbf{a})$, $\mathsf{SINR}_{ie} \leq \frac{\ell(\sqrt{5}s)}{1+\epsilon}$, since there is no eavesdropper node in $Z(\mathbf{a})$. Thus, clearly, $(x_i, x_j) \in SSG$, if $x_i, x_j \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$.

Definition 8: An open component of $\mathbf{S}$ is the sequence of connected open edges of $\mathbf{S}$.

Definition 9: A circuit in $\mathbf{S}$ or $\mathbf{S}'$ is a connected path of $\mathbf{S}$ or $\mathbf{S}'$ which starts and ends at the same point. A circuit in $\mathbf{S}$ or $\mathbf{S}'$ is defined to be open/closed if all the edges on the circuit are open/closed in $\mathbf{S}$ or $\mathbf{S}'$.

Some important properties of $\mathbf{S}$ and $\mathbf{S}'$ which are immediate are as follows.

Lemma 4: If the cardinality of the open component of $\mathbf{S}$ containing the origin is infinite, then $|C_{x_1}| = \infty$.

Proof: Follows from Lemma 3.

Lemma 5: [21] The open component of $\mathbf{S}$ containing the origin is finite if and only if there is a closed circuit in $\mathbf{S}'$ surrounding the origin.

Hence, if we can show that the probability that there exists a closed circuit in $\mathbf{S}'$ surrounding the origin is less than one, then it follows that an unbounded connected component exists in $\mathbf{S}$ with non-zero probability. Moreover, having an unbounded connected component in the square lattice $\mathbf{S}$ implies that there is an unbounded connected component in SSG from Lemma 3. Next, we show that if λ is large enough and γ is small enough, then probability of having a closed circuit in $\mathbf{S}'$ surrounding the origin is less than one for any fixed value of λ_E. This is a standard approach used for establishing the existence of percolation in discrete graphs.

First we upper bound the probability that any edge $\mathbf{a}$ of $\mathbf{S}$ is closed. Let $\mathcal{F}_1 := \left\{I_j^i \leq \frac{\epsilon}{\gamma},\ \forall\ x_i, x_j \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))\right\}$, and $\mathcal{F}_2 := \left\{I_e^i > \epsilon,\ \forall\ x_i \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a})), e \in \Phi_E \cap Y(\mathbf{a})\right\}$. From Definition 7, $P(\mathbf{a}$ is closed$)$

$$\begin{aligned}
&= P\left(\{|S_1(\mathbf{a})|_\Phi = 0 \cup |S_2(\mathbf{a})|_\Phi = 0\}\right.\\
&\qquad \left.\cup \{|Z(\mathbf{a})|_{\Phi_E} > 0\} \cup \bar{\mathcal{F}}_1 \cup \bar{\mathcal{F}}_2\right),\\
&\stackrel{(a)}{\leq} P\left(\{|S_1(\mathbf{a})|_\Phi = 0 \cup |S_2(\mathbf{a})|_\Phi = 0\}\right)\\
&\qquad + P\left(\{|Z(\mathbf{a})|_{\Phi_E} > 0\}\right) + P\left(\bar{\mathcal{F}}_1\right) + P\left(\bar{\mathcal{F}}_2\right)\\
&= 1 - (1 - e^{-\lambda s^2})^2 + 1 - e^{-2\lambda_E \nu(Z(\mathbf{a}))}\\
&\qquad + P\left(I_j^i > \frac{\epsilon}{\gamma} \text{ for any } x_i, x_j \in \Phi \cap (S_1(\mathbf{a}) \cup S_2(\mathbf{a}))\right)\\
&\qquad + P\left(I_e^i \leq \epsilon \text{ for any } x_i \in \Phi \cap S_1(\mathbf{a}) \cup S_2(\mathbf{a}),\right.\\
&\qquad \left. e \in \Phi_E \cap Y(\mathbf{a})\right), \qquad (3)
\end{aligned}$$

where (a) follows from the union bound.

For any edge $\mathbf{a}$, let $X(\mathbf{a})$ be the smallest square containing $\cup_{i=1}^4 \mathbf{B}(a_i, \sqrt{5}s + 2\eta)$, where $a_i, i = 1, \ldots, 4$, are the four vertices of the rectanlge $\mathbf{S}_1(\mathbf{a}) \cup \mathbf{S}_2(\mathbf{a})$. Now consider a sequence of edges (or path) $\mathcal{P}_n := \{\mathbf{a}_i\}_{i=1}^n$ of $\mathbf{S}$. We want to upper bound $P(\mathcal{P}_n$ is closed$)$.

Lemma 6: $P(\mathcal{P}_n$ is closed$) \leq q^{n/\psi}$, where $q := P(\mathbf{a}$ is closed$)$, and ψ is a positive integer independent of λ, λ_E.

Proof: The states (open/closed) of any two edges of $\mathcal{P}_n$, $\mathbf{a}_i$ and $\mathbf{a}_j$ are independent if $X(\mathbf{a}_i) \cap X(\mathbf{a}_j) = \phi$, since $\ell(x) = 0$ for $x > \eta$. Consider a subset of path $\mathcal{P}_n^s \subset \mathcal{P}_n$ where $\mathcal{P}_n^s = \{\mathbf{a}_i\}_{i \in \mathcal{I}}$, where for any $n, m \in \mathcal{I}$, $X(\mathbf{a}_n) \cap X(\mathbf{a}_m) = \phi$. Since $X(\mathbf{a})$ occupies at most $\left(L + \left\lceil \frac{2\eta}{s} \right\rceil\right) \times \left(L + 1 + \left\lceil \frac{2\eta}{s} \right\rceil\right)$ squares of lattice $\mathbf{S}$, where $L = 2\left\lceil \sqrt{5} \right\rceil$, it follows that $|\mathcal{I}| \geq \frac{n}{\psi}$, where $\psi = 8\left(L + \left\lceil \frac{2\eta}{s} \right\rceil\right)^2 - 1$. Thus, $P(\mathcal{P}_n$ is closed$) \leq q^{n/\psi}$, where $q = P(\mathbf{a}_i$ is closed$)$ for any $\mathbf{a}_i \in \mathbf{S}$.

Using the Peierl's argument, the next Lemma characterizes an upper bound on q for which having a closed circuit in $\mathbf{S}$ surrounding the origin is less than one.

Lemma 7: If $q < \left(\frac{11 - 2\sqrt{10}}{27}\right)^\psi$, then the probability of having a closed circuit in $\mathbf{S}'$ surrounding the origin is less than one.

Proof: From [21], the number of possible circuits of length n around the origin is less than or equal to $4n3^{n-2}$. From Lemma 6, we know that the probability of a closed circuit of length n is upper bounded by $q^{n/\psi}$. Thus,

$$\begin{aligned}
P(\text{closed circuit around the origin}) &\leq \sum_{n=1}^{\infty} 4n3^{n-2} q^{n/\psi},\\
&= \frac{4q^{1/\psi}}{3(1 - 3q^{1/\psi})^2},
\end{aligned}$$

which is less than 1 for $q < (\frac{11 - 2\sqrt{10}}{27})^\psi$.

Now we are ready to state and prove the main Theorem of this section as follows.

Theorem 2: For the signal attenuation function $\ell(x)$ with finite support, for any λ_E, there exists $\lambda' < \infty$ and a function $\gamma'(\lambda, \lambda_E) > 0$, such that $P(|C_{x_1}| = \infty) > 0$ in the SSG for $\lambda > \lambda'$, and $\gamma < \gamma'(\lambda, \lambda_E)$.

Proof: Using Lemmatas 4, 5, and 7, to conclude the result we just need to show that $q = P(\mathbf{a}$ is closed$)$ can be made arbitrarily small for large enough λ and small enough γ. Recall that an upper bound on q has been derived in (3). Consider the four terms in the R.H.S. of (3). Clearly, the second term, $1 - e^{-2\lambda_E \nu(Z(\mathbf{a}))}$, can be made arbitrarily small by choosing a small enough s (the side of the lattice). Now depending on the choice of s, the first term, $1 - (1 - e^{-\lambda s^2})^2$, can be made arbitrarily small for large enough λ. For the third and fourth term, note that both $(S_1(\mathbf{a}) \cup S_2(\mathbf{a}))$ and $\mathbf{Y}(\mathbf{a})$ have finite areas and hence only finitely many nodes of Φ and Φ_E can lie in them, respectively. Therefore, the fourth term can also be made arbitrarily small by choosing small enough ϵ, and depending on the choice of ϵ, choosing small enough γ, the third term can be made as small as required. Note that both ϵ and γ could possibly depend on λ, λ_E.

Discussion: In this section, we showed that for any eavesdropper node density, percolation happens in the SSG for large enough legitimate node density and small enough γ, when concurrent transmissions are allowed from all legitimate nodes. We mapped the continuum percolation to discrete percolation (percolation on the square grid), for which concrete percolation results can be obtained. We needed the signal attenuation function to have a finite support, since otherwise, nodes (legitimate or eavesdropper) with arbitrarily large distances can interact with each other, thereby introducing long range correlations and complicating the graph structure.

V. Conclusions

In this paper, we considered percolation in a wireless network, where two legitimate nodes can connect/communicate with each other if the SINR between them is more than the SINR at any eavesdropper. This model of communication is complicated since the link formation between any two legitimate nodes depends on all the other legitimate nodes in the network (through their interference contribution) and entails infinite range dependencies. For analytical tractability, we assumed a signal attenuation function that has a finite support, and found existential results on the sub-critical and super critical regimes of percolation. Finding concrete bounds on the critical density remains an open problem.

Appendix A
Proof of Lemma 2

We now prove some intermediate results that are required for proving Lemma 2. The first key element required for proving Lemma 2 is described in the next Lemma.

Lemma 8: Event $E(q, r)$ only depends on $x \in \Phi \cap (q + D_{10r+\eta})$, and $e \in \Phi_E \cap (q + D_{10r+\eta})$.

Proof: By definition, $E(q, r)$ is the event that there is a path from a node $x \in \Phi \cap (q + D_r)$ to a node $w \in \Phi \cap (q + D_{9r} \backslash q + D_{8r})$. With a finite support signal attenuation function $\ell(.)$, $\rho(x) \leq \eta$, and hence connections between legitimate nodes of Φ lying in $(q + D_{10r})$ can most be influenced by nodes of Φ and Φ_E lying in $(q + D_{10r+\eta})$, since $\ell(x) = 0$ for $x > \eta$.

The second key ingredient required for proving Lemma 2 is described in the next Lemma that uses Lemma 8.

Lemma 9: For $r \geq \eta$, $P(E(\mathbf{0}, 10r)) \leq CP(E(\mathbf{0}, r))^2$, where C is a constant that does not depend on r.

Proof: The essential idea here is to show that if $E(\mathbf{0}, 10r)$ occurs, then two small events $E(q_1, r)$ and $E(q_2, r)$ happen, where $||q_2 - q_1|| > 20r + 2\eta$, which makes the two events $E(q_1, r)$ and $E(q_2, r)$ independent following Lemma 8. A rigorous proof is as follows.

Let K and L be two finite discrete subsets of $\mathbb{R}^2$, such that $K \subset \delta D_{10}, L \subset \delta D_{80}$, and $D_{10} \backslash D_9 \subset K + D_1, D_{81} \backslash D_{80} \subset$

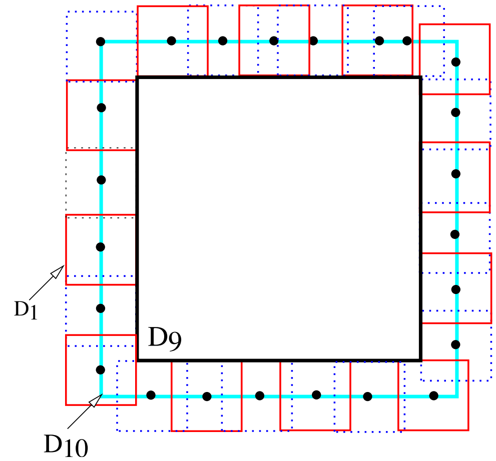

Fig. 4. Covering of $D_{10} \backslash D_9$ by discrete points lying on the boundary (black dots) of D_{10} using D_1.

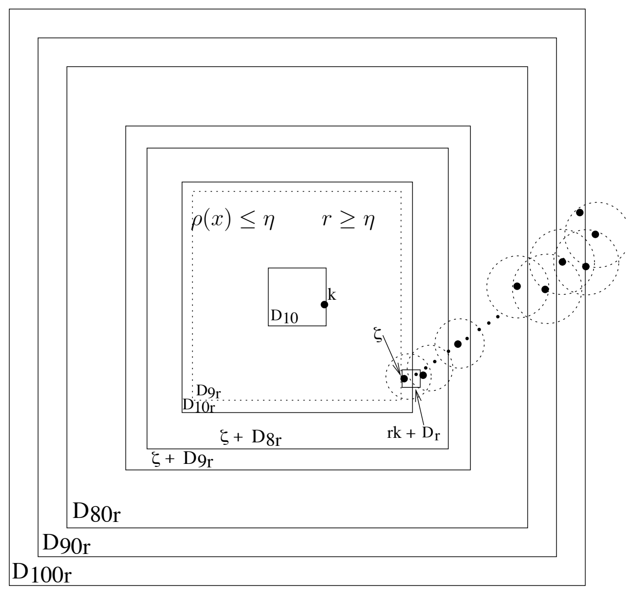

Fig. 5. Picture to illustrate the idea used in Proof of Lemma 9.

$L + D_1$. For example, see Fig. 4 where black dots represent the points of $K \subset \delta D_{10}$ covering $D_{10} \backslash D_9$ using D_1. Let C be the product of the cardinality of K and L.

Assume that $E(\mathbf{0}, 10r)$ occurs for $r \geq \eta$. Thus, there exists a node in D_{10r} that has a connected path to a node in $D_{90r} \backslash D_{80r}$. Since $\rho(x) \leq \eta \leq r$ for any $x \in \Phi$, there exists a node $\zeta \in D_{10r} \backslash D_{9r}$ that has a connected path to a node in $D_{90r} \backslash D_{80r}$. By the definition of K, $\zeta \in rk + D_r$ for some $k \in K$. See Fig. 5 for a pictorial description. Moreover, since $\rho(x) \leq \eta$ for all x, there is a connected path from node ζ to some node in $\zeta + D_{9r} \backslash D_{8r}$. Hence if $E(\mathbf{0}, 10r)$ occurs, then $\cup_{k \in K} E(rk, r)$ happens, where $P(E(rk, r)) = P(E(\mathbf{0}, r))$ for any $k \in K$. Similarly looking at nodes around D_{80r} and using the definition of L we can show that if $E(\mathbf{0}, 10r)$ occurs then $\cup_{\ell \in L} E(r\ell, r)$ happens. Hence if $E(\mathbf{0}, 10r)$ occurs, then $\cup_{k \in K} E(rk, r) \cap \cup_{\ell \in L} E(r\ell, r)$ happens, where $P(E(r\ell, r)) = P(E(\mathbf{0}, r))$ for any $\ell \in L$. From Lemma 8, we know that the event $\cup_{k \in K} E(rk, r)$ depends only upon the nodes of Φ and Φ_E lying in D_{20r}, while the event $\cup_{\ell \in L} E(r\ell, r)$ depends only upon the nodes of Φ and Φ_E lying in $\bar{D}_{69r}$. Since D_{20r} and $\bar{D}_{69r}$ are disjoint, and since Φ are Φ_E are independent PPPs, the events $\cup_{\ell \in L} E(r\ell, r)$ and $\cup_{k \in K} E(rk, r)$ are independent, and hence we get that $P(E(\mathbf{0}, 10r)) \leq CP(E(\mathbf{0}, r))^2$.

We also need the following upper bound on the $P(E(\mathbf{0}, r))$ to prove Lemma 2.

Lemma 10: $P(E(\mathbf{0}, r)) \leq \lambda \pi \mathbb{E}\{\rho^2\}$.

Proof: Event $E(\mathbf{0}, r)$ implies that for some $x \in \Phi \cap D_r$, there is at least one node in a disc of radius $\rho(x)$. Hence event $E(\mathbf{0}, r)$ implies $|(\Phi \cap \mathbf{B}(x, \rho(x)))| > 0$, i.e., $P(E(\mathbf{0}, r)) \leq P(|(\Phi \cap \mathbf{B}(x, \rho(x)))| > 0)$. Since for any random variable X, $\mathbb{E}\{X\} \geq P(X > 0)$, we get the result by noting that $\mathbb{E}\{|(\Phi \cap \mathbf{B}(x, \rho(x)))|\} = \lambda \pi \mathbb{E}\{\rho^2\}$.

Next, we need a technical result that is similar to Lemma 3.7 [17].

Lemma 11: For $\eta \geq 1$, suppose $f : [\eta, \infty) \to \mathbb{R}^+$ is a non-increasing function such that $f(\eta) = a < 1$, and f satisfies $f(x) \leq f(x/10)^2$ for all $x \geq 10\eta$. Then $f(x) \to 0$ as $x \to \infty$.

Proof: For all $x \geq 10\eta$, we have that $f(x) \leq af(x/10)$. Hence for all integers $n \geq 1$, we have

$$\begin{aligned} f((10\eta)^n) &\leq a^n f(\eta), \\ &\leq a^{n+1}, \end{aligned}$$

Thus, $f((10\eta)^n) \to 0$ as $n \to \infty$. The result now follows since f is non-increasing.

Definition 10: Let $f(r) := CP(E(\mathbf{0}, r))$ for $r \geq \eta$. Then the following is true.

Lemma 12: For $\lambda < \frac{1}{\pi C \mathbb{E}\{\rho^2\}}$, $f(r) < 1$ for $r \geq \eta$.

Proof: From Lemma 10, $f(r) = CP(E(\mathbf{0}, r)) \leq \lambda \pi C \mathbb{E}\{\rho^2\}$. Thus, for $\lambda < \frac{1}{\pi C \mathbb{E}\{\rho^2\}}$, $f(r) < 1$ for $r \geq \eta$.

Finally, we are ready to prove Lemma 2.

Proof: (Lemma 2) Using the definition of $f(r)$, from Lemma 9, $f(r) \leq f(r/10)^2$ for $r \geq \eta$. Moreover, from Lemma 12, $f(r) < 1$ for $r \geq \eta$, and $f(r)$ is non-increasing. Hence using Lemma 11, it follows that $f(r) \to 0$, and using the definition of $f(r)$, $P(E(\mathbf{0}, r)) \to 0$ as $r \to \infty$.

References

[1] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 4, pp. 477–486, 2002.

[2] M. Franceschetti, O. Dousse, D. Tse, and P. Tiran, "Closing the gap in the capacity of random wireless networks," in *Proc. Int. Symp. Information Theory ISIT 2004*, 2004.

[3] P. Gupta and P. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming, W. M. McEneaney, G. Yin, and Q. Zhang (Eds.).* Birkhauser, Boston, 1998.

[4] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, 1975.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[6] O. Koyluoglu, C. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[7] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," vol. special issue in Military Communications and Networking Computers, Dec. 2011.

[8] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *IEEE INFOCOM 2012*, Apr. 2012.

[9] O. Dousse, M. Franceschetti, N. Macris, R. Murlster, and P. P. Thiran, "Percolation in the signal to interference ratio graph," *Journal of Applied Probability*, vol. 43, no. 2, pp. 552–562, 2006.

[10] M. Penrose, "On a continuum percolation model," *Advances in Applied Probability*, vol. 23, no. 3, pp. 536–556, 1991.

[11] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Information Theory ISIT 2008*, 2008, pp. 539–543.

[12] P. Pinto and M. Win, "Percolation and connectivity in the intrinsically secure communications graph," 2010, submitted. Available at http://arxiv.org/abs/1008.4161.

[13] A. Sarkar and M. Haenggi, "Secrecy coverage," *Internet Mathematics*, 2010, submitted. Available at http://www.nd.edu/ mhaenggi/pubs/im10.pdf.

[14] ——, "Percolation in the Secrecy Graph," in *2011 Information Theory and Applications Workshop (ITA'11)*, Feb. 2011, available at http://www.nd.edu/ mhaenggi/pubs/ita11.pdf.

[15] S. Goel, V. Aggarwal, A. Yener, and R. Calderbank, "The effect of eavesdroppers on network connectivity: A secrecy graph approach," *IEEE Trans. Inf. Forensics Security*, 2011, accepted, to be published in 2011.

[16] O. Dousse, F. Baccelli, and P. Thiran, "Impact of interferences on connectivity in ad hoc networks," *IEEE/ACM Trans. Networking*, vol. 13, no. 2, pp. 425 – 436, April 2005.

[17] J. Gouéré, "Subcritical regimes in the poisson boolean model of continuum percolation," *Annals of Probability*, vol. 36, no. 4, pp. 1209–1220, 2008.

[18] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. New York, NY, USA: Cambridge University Press, 2005.

[19] R. Vaze, "Percolation and connectivity on the signal to interference ratio graph," in *Proceedings IEEE INFOCOM, 2012*, Mar. 2012, pp. 513 – 521.

[20] E. Gilbert, "Random plane networks," *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, p. 533, 1991.

[21] G. Grimmett, *Percolation*. Springer-Verlag, 1980.