Modeling Location Uncertainty for Eavesdroppers: A Secrecy Graph Approach

Satashu Goel[1], Vaneet Aggarwal[2], Aylin Yener[1], A. Robert Calderbank[2]
goel@psu.edu, vaggarwa@princeton.edu, yener@engr.psu.edu, calderbk@math.princeton.edu
[1]Electrical Engineering, The Pennsylvania State University, University Park, PA 16802
[2]Electrical Engineering, Princeton University, Princeton, NJ 08544

***Abstract*—In this paper, we consider end-to-end secure communication in a large wireless network, where the locations of eavesdroppers are uncertain. Our framework attempts to bridge the gap between physical layer security under uncertain channel state information of the eavesdropper and network level connectivity under security constraints, by modeling location uncertainty directly at the *network level* as *correlated* node and link failures in a secrecy graph. Bounds on the percolation threshold are obtained for square and triangular lattices, and bounds on mean degree are obtained for Poisson secrecy graphs. Both analytic and simulation results show the dramatic effect of uncertainty in location of eavesdroppers on connectivity in a secrecy graph.**

I. Introduction

In the recent years, there has been growing interest in employing information theoretic methods to characterize the secrecy capacity of wireless networks. In a seminal paper [1], Wyner introduced the wire-tap channel and formalized an information theoretic setting for communicating a confidential message to the intended receiver while keeping the eavesdropper completely ignorant of the confidential message. Csiszar and Korner [2] generalized this formulation to a broadcast channel, where the transmitter has a common message for both the users along with a confidential message for one of them. This framework has been successfully applied to networks with one hop communication, such as broadcast, e.g., [3], multiple access, e.g., [4], and two-hop communication with relays, e.g., [5]. However, it is not as clear how the information theoretic techniques can be used to guarantee end-to-end secrecy in large networks.

Recently, the concept of *secrecy graph* was introduced in [6], where physical layer secrecy is captured using an abstract model, which is integrated with network layer models. Essentially, link connectivity is determined using information theoretic secrecy models resulting in a *secrecy graph*, which is analyzed for connectivity [6, 7], using tools from percolation theory. Scaling laws for secrecy capacity in large networks have also been investigated in [8, 9]. In [8], a random network was considered where the legitimate nodes and eavesdroppers are placed in a square region of area n according to independent Poisson point processes (PPPs). It was shown that secrecy requirement does not lead to a loss in throughput, in terms of scaling, if the intensity of eavesdroppers is $O((\log n)^{-2})$ while the intensity of the legitimate nodes is 1. In [9], a similar result was shown for mobile ad-hoc networks (MANETs) with n legitimate nodes and a delay constraint of D, if the number of eavesdroppers scales as $o(\sqrt{nD})$.

In references [6–9] the channel gains of all the eavesdroppers are assumed to be known. However, this assumption is unrealistic, especially for a passive eavesdropper, since it may not be possible to ascertain even the presence of such an entity. For communication over a single link, a compound channel model [10] can be used if the eavesdropper's channel is uncertain, and noise injection techniques can be used if the channel is unknown [11]. In contrast, we want to characterize the effect of uncertainty in location of eavesdroppers on the *network level connectivity*, instead of capacity of individual links.

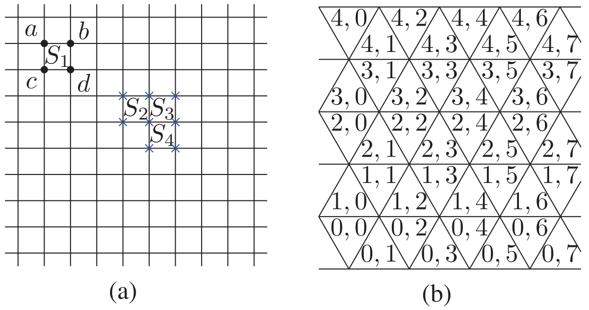
In this paper, we introduce a secrecy graph model where the locations of eavesdroppers are uncertain, and the uncertainty is modeled in terms of node and link failures in a secrecy graph. We study the percolation thresholds and node degree distributions under these failures. Thus, our model captures the uncertainty in eavesdroppers' locations at the *network level*, and provides a realistic model for guaranteeing end-to-end security. The main challenge is that the failures are correlated, and hence, the techniques from percolation theory must be extended to account for these correlations. Numerical results show that location uncertainty of eavesdroppers has a dramatic effect on connectivity in a secrecy graph. Though this is somewhat expected, it is surprising to observe how soon the effect sets in.

II. Model and Formulation

Let $\hat{G} = (\phi, \hat{E})$ denote a geometric graph in $\mathbb{R}^d$, where $\phi = \{x_i\} \subset \mathbb{R}^d$ is the set of locations of legitimate nodes. E is the set of links over which reliable communication is possible. $\psi = \{y_i\} \subset \mathbb{R}^d$ denotes the set of locations of eavesdroppers. We assume that each eavesdropper is located within a known finite area and the precise location is uncertain. If the locations of the nodes come from a stochastic point process, we denote the corresponding random variables by Φ and Ψ.

We define secrecy graphs (SGs) based on $\hat{G}$ and ψ. The existence of links in the secrecy graphs is determined based on secrecy capacity of the links. We assume that the wireless medium introduces only path loss, with exponent α, and that the noise introduced by the receivers is Additive White Gaussian Noise (AWGN). If the source transmits a signal with power P_s to a receiver at distance d_R, and the eavesdropper is

978-1-4244-7891-0/10/$26.00 ©2010 IEEE



(a) (b)

Fig. 1. (a) Failures in square lattice (b) Indices in triangular lattice

located at distance d_E, the secrecy capacity is given by [12]

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

where the AWGN power is assumed to be 1 for both the channels. If the destination is closer than the eavesdropper, i.e., $d_R < d_E$, the secrecy capacity is positive and it is zero otherwise. We will employ two secrecy graphs in this paper - *directed secrecy graph* and *basic secrecy graph* [6]. A directed edge exists from x_i to x_j in the directed secrecy graph $\vec{G}$ if $\|x_i - x_j\| < \|x_i - y_k\|$ for all $y_k \in \psi$. An undirected edge exists in the basic secrecy graph G if a directed edge exists from x_i to x_j and also from x_j to x_i in $\vec{G}$.

A. Secrecy in Square and Triangular Lattice

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

B. Secrecy in Poisson graph

We assume that the locations of legitimate nodes follow a Poisson point process (PPP) Φ with intensity 1. Two nodes are connected if the distance between them is at most r, resulting in Gilbert's disk graph [13]. Each eavesdropper is known to be located within a circle of radius r_E. The radius r_E captures the uncertainty in an eavesdropper's location. The center of the circles follow a PPP with intensity λ. We denote the directed and basic secrecy graphs by $\vec{G}_{\lambda,r}$ and $G_{\lambda,r}$, respectively.

C. Percolation Threshold

Percolation was introduced by Broadbent and Hammersley [14], to model the diffusion process in materials. They used regular lattices to model a material, where each node is present with probability p. Percolation is said to occur if an infinite component exists in the corresponding graph. It was shown that a phase transition exists, i.e., there exists a critical threshold, below which all components are finite, almost surely, and above which an infinite component exists, almost surely. Let us denote the number of nodes in the component containing the origin by $|C|$. Then, the percolation probability is defined as

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

The percolation threshold is defined as

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

Roughly, p_E^c is the smallest value of p_E for which an infinite component does not exist in the secrecy graph. In other words, for any $p_E < p_E^c$, the secrecy graph will have an infinite component containing the origin almost surely.

III. Square and Triangular Lattices

In this section, we present bounds on the percolation threshold of square and triangular lattices. We note that exact solutions for percolation probability exist only for a few lattices. For example, for a triangular lattice, where each node occurs with probability p, $p_c = 1/2$. However, the corresponding percolation threshold for a square lattice is not known [15]. Notice that in the models considered in this paper, failures are *correlated*, and hence, the corresponding problems of determining the percolation threshold are expected to be intractable. Therefore, we concentrate our effort in obtaining tight upper and lower bounds on the percolation threshold. The following lemma from [16] is useful.

Lemma 1. *(Hori and Kitahara [16]): For a triangular lattice with site probability r and bond probabilities p_1, p_2 and p_3, the critical probability satisfies*

$$r(p_1 + p_2 + p_3 - p_1 p_2 p_3) = 1. \qquad (4)$$

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

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

$$\frac{1}{18} \le p_E^c \le \frac{3-\sqrt{5}}{2}. \qquad (5)$$

Proof: The existence of critical probability follows from [15]. For the upper bound on the percolation threshold, assume that no eavesdroppers are present in the squares $(2i, 2j)$ for all integers i and j, and eavesdroppers are present in the remaining squares with probability p_E. Removing eavesdroppers from squares $(2i, 2j)$ can only increase the critical probability, and thus, results in an upper bound. Now assume that each square $(2i + 1, 2j + 1)$ is a vertex in a new square lattice which fails when there is an eavesdropper in that square. Further, the nodes corresponding to squares $(2i + 1, 2i + 1)$ and $(2i + 3, 2i + 1)$ are connected iff there is no eavesdropper in square $(2i+2, 2i+1)$. Similarly, the nodes corresponding to squares $(2i+1, 2i+1)$ and $(2i+1, 2i+3)$ are connected iff there is no eavesdropper in square $(2i + 1, 2i + 2)$. This produces a new square lattice with the probability of existence of a node and an edge being $1-p_E$ each. Thus, when the probability p_E is less than one minus the percolation probability of the square lattice with equally likely bond and site probability, there exists an infinite connected component with probability 1. Since the percolation probability of a square lattice is greater than that of a triangular lattice, the required critical probability can be upper bounded by one minus the percolation probability of a triangular lattice with equally likely bond and site probability, using Lemma 1. This gives the upper bound in the statement of the theorem.

For the lower bound, consider each square as a node of a triangular lattice which fails when it or any of the neighboring squares contain an eavesdropper. Note that we are over-counting all the eavesdroppers resulting in a lower bound for critical percolation probability. This results in a triangular model with site probability $1 - 9p_E$ and bond probability 1 which yields a lower bound of $1/18$ on p_E^c. ■

Note that, for the square lattice, the probability of a node failure is related to p_E as

$$p_{fail} = p_E(2(1 - p_E)(2 - p_E + p_E^2) + p_E^3). \tag{6}$$

However, the node failures are correlated, and hence, existing results on percolation thresholds cannot be used directly.

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

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

$$1/26 \le p_E^c \le 0.2582. \tag{7}$$

Proof: The existence of the critical probability follows from [15]. For the upper bound, assume that there are no eavesdroppers in the triangles $(3i+1, 3j+1)$, $(3i+1, 3j+2)$, $(3i + 2, 3j + 1)$, $(3i + 2, 3j + 2)$ for all integers i and j and the eavesdroppers are present in the remaining triangles with probability p_E (the indexing of triangles is shown in Fig. 1(b)). Now assume that each triangle $(3i, 3j)$ is a vertex of a new square lattice which fails when there is an eavesdropper in that triangle. Further, nodes corresponding to triangles $(3i, 3i)$ and $(3i + 3, 3i)$ are connected iff there is no eavesdropper in any of the triangles $(3i + 1, 3i)$ and $(3i + 2, 3i)$. Similarly, nodes corresponding to triangles $(3i, 3i)$ and $(3i, 3i + 3)$ are connected iff there is no eavesdropper in any of the triangles $(3i, 3i+1)$ and $(3i, 3i+2)$. This produces a new square lattice with the probability of existence of a vertex and an edge being $1-p_E$ and $(1-p_E)^2$ respectively. Thus, when the probability p_E is less than one minus the percolation probability of this square lattice, there exists an infinite connected component with probability 1. Since the percolation probability of a square lattice is greater than that of a triangular lattice, the required critical probability can be upper bounded by one minus the percolation probability of a triangular lattice with corresponding bond and site probability. This gives the upper bound as one minus the solution of equation $3x^3 - x^5 = 1$ in $(0, 1)$ which is less than 0.2582. The lower bound analysis is similar to the proof in Theorem 1 and is thus omitted. ■

IV. Poisson secrecy graph

In this section, we consider a Poisson model where Φ is a Poisson point process (PPP) of intensity 1 in $\mathbb{R}^2$. The eavesdroppers are located in known circular regions. The centers of circular regions are located according to a Poisson point process Ψ of intensity λ in $\mathbb{R}^2$, which is independent of Φ. The radius of the circular regions is denoted by r_E. For simplifying the notation, we define $A \doteq \lambda\pi r_E^2$.

We are interested in computing the mean degree of a node in the basic secrecy graph. For simplicity, we consider the node located at the origin, denoted by o. Let N denote the number of bi-directional links of node o. An analytic computation of N is difficult because it requires characterization of the intersection of two regions - a circular region which determines the out-degree of node o, and a polygonal region which determines the in-degree of node o. The polygonal region is the interior of the region formed by the intersection of bisectors of the line segments joining the origin to an eavesdropper. Let N^{out} denote the number of directed links out of node o. Clearly, $N \le N^{out}$, and thus, we can obtain an upper bound on the mean degree. Assume that the eavesdropper closest to the origin is located at a distance R from the origin. A lower bound can be obtained by considering the circle $C(\mathbf{0}, (R - r_E)/2)$, since the origin has a bi-directional link to all the nodes in this region. $\tilde{N}$ denotes the number of legitimate nodes in $C(\mathbf{0}, (R - r_E)/2)$. Clearly, $\tilde{N} \le N$.

Lemma 2. *In the directed secrecy graph $\vec{G}_{\lambda,\infty}$ with radius of uncertainty for eavesdropper's location r_E, the probability that the origin is isolated, i.e., it cannot transmit securely to any other node is*

$$P(N^{out}{=}0) = 1 - \frac{e^{-A}}{1+\lambda} + \frac{2\pi\lambda r_E e^{-\frac{A}{1+\lambda}}}{(1+\lambda)^{3/2}} Q\left(\sqrt{\frac{2\lambda A}{1+\lambda}}\right), \tag{8}$$

Proof: Assume that the eavesdropper closest to the origin is located at a distance R from it. Then, the origin can securely transmit to any node within the circle of radius $R - r_E$, centered at the origin. Averaging the probability of having no legitimate nodes in that circle over R results in (8). ∎

Lemma 3. *In the basic secrecy graph $G_{\lambda,\infty}$ with radius of uncertainty for eavesdropper's location r_E, the probability that the origin is isolated, i.e., it does not have a secure bi-directional link to any other node, is lower-bounded by $P(N^{out} = 0)$ and is upper-bounded by $P(\tilde{N} = 0)$, given by,*

$$P(\tilde{N}{=}0){=}1{-}\frac{e^{-A}}{1+4\lambda}{+}\frac{2\pi\lambda r_E e^{-\frac{A}{1+4\lambda}}}{(1/4+\lambda)^{3/2}}Q\left(\sqrt{\frac{2\lambda A}{1/4+\lambda}}\right). \quad (9)$$

Proof: The proof is similar to that of Lemma 2, but nodes in $C(\mathbf{0}, (R - r_E)/2)$ are considered. ∎

Note that for the directed secrecy graph,

$$\lim_{r_E\to 0} P(N^{out}{=}0){=}\frac{\lambda}{1+\lambda}, \quad \lim_{r_E\to\infty} P(N^{out}{=}0){=}1, \quad (10)$$

which match the results in [6] where $r_E = 0$ was assumed. Similarly, for the upper bound,

$$\lim_{r_E\to 0} P(\tilde{N} = 0) = \frac{\lambda}{1/4+\lambda}, \quad \lim_{r_E\to\infty} P(\tilde{N} = 0) = 1. \quad (11)$$

Thus, in both the cases, none of the nodes have any links, almost surely, if the locations of the eavesdroppers are not known at all. For $r_E = 0$, we obtain the probability of isolation of a node when locations of all the eavesdroppers are known precisely. Further, as the eavesdroppers' intensity λ goes to infinity,

$$\lim_{\lambda\to\infty} P(N^{out} = 0) = 1, \lim_{\lambda\to\infty} P(N = 0) = 1, \quad (12)$$

meaning that none of the nodes have any links, almost surely.

Lemma 4. *The distributions of the number of out-going links at the origin N^{out} and the number of bi-directional links to nodes in the circle $C(\mathbf{0}, (R - r_E)/2)$ $\tilde{N}$ are given by,*

$$P(N^{out} = n) = \frac{2\pi^{n+1}\lambda}{n!}e^{-\frac{A}{1+\lambda}}\sum_{k=0}^{2n}\binom{2n}{k}\left(\frac{-\lambda r_E}{1+\lambda}\right)^{2n-k}$$

$$(F_{k+1}(\pi(1+\lambda)) + \frac{r_E}{1+\lambda}F_k(\pi(1+\lambda)), \; n \geq 1, \quad (13)$$

$$F_k(\alpha) = \begin{cases} (-1)^{k/2}\frac{\partial^{k/2}}{\partial\alpha^{k/2}}\sqrt{\frac{\pi}{\alpha}}Q(\sqrt{2\alpha}\frac{\lambda}{1+\lambda}r_E), \; k \; even \\ (-1)^{(k-1)/2}\frac{\partial^{(k-1)/2}}{\partial\alpha^{(k-1)/2}}\frac{e^{-\alpha\left(\frac{\lambda r_E}{1+\lambda}\right)^2}}{2\alpha}, \; k \; odd \end{cases} \quad (14)$$

$$P(\tilde{N} = n) = \frac{2\pi^{n+1}\lambda}{4^n n!}e^{-\frac{A}{1+4\lambda}}\sum_{k=0}^{2n}\binom{2n}{k}\left(\frac{-\lambda r_E}{1/4+\lambda}\right)^{2n-k}$$

$$(\tilde{F}_{k+1}(\pi(\frac{1}{4}+\lambda)) + \frac{r_E}{1+4\lambda}\tilde{F}_k(\pi(\frac{1}{4}+\lambda)), \; n \geq 1, \quad (15)$$

$$\tilde{F}_k(\alpha) = \begin{cases} (-1)^{k/2}\frac{\partial^{k/2}}{\partial\alpha^{k/2}}\sqrt{\frac{\pi}{\alpha}}Q(\sqrt{2\alpha}\frac{\lambda}{1/4+\lambda}r_E), \; k \; even \\ (-1)^{(k-1)/2}\frac{\partial^{(k-1)/2}}{\partial\alpha^{(k-1)/2}}\frac{e^{-\alpha\left(\frac{\lambda r_E}{1/4+\lambda}\right)^2}}{2\alpha}, \; k \; odd \end{cases} \quad (16)$$

and (8), (9).

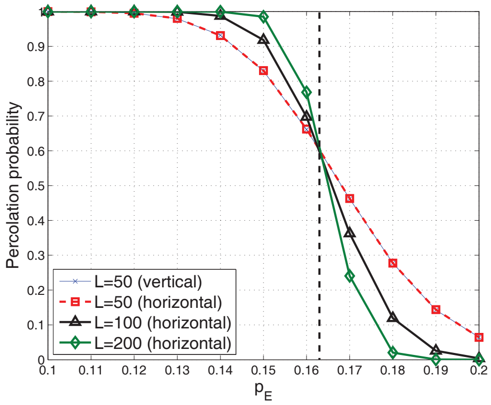


Fig. 2. Percolation threshold for square lattice

Proof: The upper bound is obtained by considering legitimate nodes in the circle $C(0, R{-}r_E)$, while $C(0, (R{-}r_E)/2)$ is considered for the lower bound. ∎

The main result of this section is summarized next.

Theorem 3. *The mean degree of a node in the basic Poisson secrecy graph with secure bi-directional links is bounded as,*

$$\mathbf{E}[\tilde{N}] \leq \mathbf{E}[N] \leq \mathbf{E}[N^{out}], \quad (17)$$

where the distributions of $\tilde{N}$ and N^{out} are given by (9),(15) and (8), (13), respectively.

Proof: The regions corresponding to $\tilde{N}$ and N^{out} were chosen so that $\tilde{N} \leq N \leq N^{out}$. By taking expectation, we obtain (17). ∎

V. Numerical Results

We now present numerical results on percolation thresholds of lattice secrecy graphs and mean degree in Poisson secrecy graphs.

A. Percolation threshold

We estimated the percolation probability $\theta(p_E)$ for $L \times L$ square lattice through Monte-Carlo simulations. Eavesdroppers were placed in the squares randomly and independently, with the probability of a given square having an eavesdropper being p_E. We estimated the probability that a cluster wraps around the periodic boundary conditions. Cluster wrapping can be defined in several ways; we considered the probability of cluster wrapping in the horizontal and vertical directions, denoted by $R_L^{(h)}(p_E)$ and $R_L^{(v)}(p_E)$, respectively [17]. 10^5 random lattices were generated for each estimate. Fig. 2 shows the variation of percolation probability with p_E, for $L = 50, 100, 200$. Notice that in Fig. 2, the percolation probability transitions from a large value (close to 1), to a small value (close to 0). This transition is a typical behavior of percolation probability, and the region of transition becomes narrower as the size of simulated network increases. The percolation threshold can be estimated as the point of intersection of the three curves. Thus,

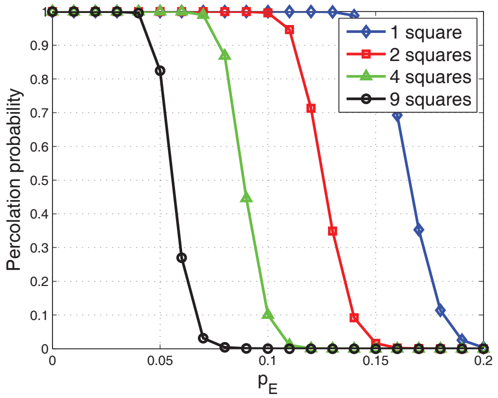


Fig. 3. Percolation threshold versus area

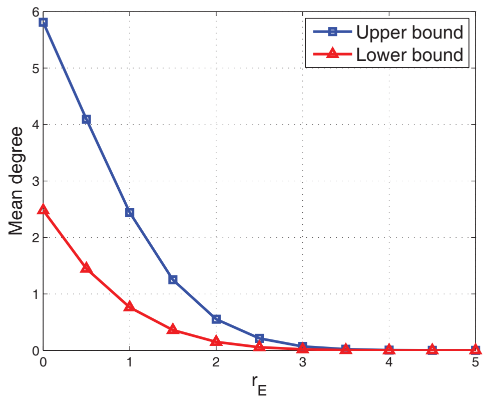


Fig. 4. Mean degree in basic secrecy graph

for the square lattice with each eavesdropper located within a square, the percolation threshold is $p_E^c \approx 0.163$. For $p_E = p_E^c$, we obtain $p_{fail} \approx 0.5$ (using (6)) for correlated node failures, whereas for independent node failures, the critical threshold is $p_{fail} \approx 0.41$. Although, a larger proportion of node failures can be tolerated (p_{fail}) in the correlated failure scenario, only 16.3% eavesdroppers can be tolerated in that case.

B. Effect of uncertainty in location

We now show the effect of the uncertainty in the location of eavesdroppers on the percolation threshold. An eavesdropper may be located anywhere within certain N_S squares. N_S captures the amount of uncertainty in an eavesdropper's location. Fig. 3 shows the variation of percolation probability with p_E for $L = 100$ and $N_S = 1, 2, 4, 9$. As expected, the threshold probability reduces as N_S increases, where the decrease quantifies the effect of uncertainty in location on percolation threshold of secrecy graphs.

Note that in the lattice model, the uncertainty in an eavesdropper's location was represented in terms of the number of squares, resulting in limited resolution. We now present numerical results in the Poisson model, where the radius r_E can take any non-negative real value. Fig. 4 shows the variation of the upper and lower bounds on the mean degree of the origin in the basic secrecy graph. λ was chosen as 0.1, for which percolation occurs at $r_E = 0$ [6]. Notice that both the upper and lower bounds decrease by a more than a factor of $1/2$ as r_E goes from 0 to 1. The gap between the upper and lower bounds reduces with increasing r_E.

VI. Conclusion

We have introduced a new model for secrecy graphs where uncertainty in location of eavesdroppers can be modeled as correlated node and link failures. Our framework captures the uncertainty at the *network level*, allowing the analysis of end-to-end connectivity under uncertainty in eavesdroppers' locations. Bounds on the percolation thresholds of square and triangular lattices were presented. For the Poisson secrecy graph, bounds on the mean node degree were presented. Numerical results showed that uncertainty in location of eavesdroppers effects connectivity in a secrecy graph dramatically. In our future work, we will investigate methods to mitigate the effect of location uncertainty of eavesdroppers, using the framework developed in this paper.

References

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

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[4] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

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

[6] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE ISIT*, July 2008, pp. 539–543.

[7] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE ICCS*, Nov. 2008, pp. 974–979.

[8] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *submitted to IEEE Trans. on Information Theory*, 2010.

[9] Y. Liang, V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE ISIT*, 2009.

[10] Y. Liang, G. Kramer, H. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in *Proc. Allerton Conf. Comm., Contr., and Comput.*, Sept. 2007.

[11] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE VTC Fall 2005*, vol. 3, Sept. 2005, pp. 1906–1910.

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

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

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

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

[16] M. Hori and K. Kitahara, "Percolation thresholds for honeycomb, kagome and triangular lattices," in *Proc. International Conf. Statistical Physics*, 2004.

[17] M. E. J. Newman and R. M. Ziff, "Fast monte carlo algorithm for site or bond percolation," *Phys. Rev. E*, vol. 64, no. 1, p. 016706, Jun 2001.