Security Versus Capacity Trade-offs in Large Wireless Networks Using Keyless Secrecy

Sudarshan Vasudevan
University of Massachusetts
Amherst
svasu@cs.umass.edu

Dennis Goeckel
University of Massachusetts
Amherst
goeckel@ecs.umass.edu

Don Towsley
University of Massachusetts
Amherst
towsley@cs.umass.edu

ABSTRACT

We investigate the scalability of a class of algorithms that exploit the dynamics of wireless fading channels to achieve secret communication in a large wireless network of n randomly located nodes. We describe a construction in which nodes transmit *artificial noise* to suppress eavesdroppers and ensure secrecy of messages transported across the network. Under a model in which eavesdroppers operate independently, we show that for some constant c such that $0 < c < 1$, the network can tolerate $\Omega\left(\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)^{2c}\right)$ eavesdroppers while ensuring that the aggregate rate at which eavesdroppers intercept packets goes to 0, where $\Psi(n)$ denotes the achievable per-node throughput and lies in the interval $(1/n, 1/\sqrt{n})$. The result clearly establishes a trade-off between the achievable throughput and the allowable number of eavesdroppers. Under a collaborating eavesdropper model and a similar constraint on the eavesdropper throughput, we show that the network can tolerate a single eavesdropper with $\Omega\left(\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)^{1-\epsilon}\right)$ antennas, $\forall \epsilon > 0$. We also establish sufficient conditions on the number of eavesdroppers to achieve a non-zero throughput.

1. INTRODUCTION

The idea of **keyless secrecy** (also called, *physical layer secrecy*) has attracted considerable attention recently as a method for key distribution in systems based on traditional computational cryptography, or as an alternative that, in contrast to the computational approach, assumes that eavesdroppers have **infinite computational power**. In wireless systems, for instance, a number of recent proposals exploit differences in the received signal across different nodes to achieve secret communication. Examples of such schemes include [7, 8], which exploit common information in fading channel characteristics, and, [19] which exploits independent packet loss of Eve and Bob. Other schemes [3, 17] use **artificial noise generation** to ensure that the eavesdropper(s) receives a degraded version of the signal received by a legitimate receiver so as to ensure a positive rate of secure bits [18]. The scheme proposed in [3], for instance, uses beamforming and interference cancellation, while the scheme in [17] exploits multi-user diversity to generate noise and confuse the eavesdroppers.

In this paper, we study the scalability of keyless secrecy in large wireless networks, as opposed to the two hop setting generally considered in prior literature. Similar to [17], we use artificial noise generation to ensure secrecy of packets. In particular, for each packet hop, we select nearby nodes to generate noise that ensures maximal ambiguity at the eavesdroppers, while allowing the packet to be decoded by a legitimate receiver. Intuitively, the greater the number of nodes generating noise, the greater the number of eavesdroppers that can be tolerated at the cost of reducing the source-destination throughput. Thus, there is an inherent trade-off between the achievable throughput of a node and the security of a wireless system.

We therefore pose the fundamental question: *for a desired source-destination throughput, what is the number of eavesdroppers that can be tolerated, while ensuring that with high probability (w.h.p) the aggregate rate at which eavesdroppers intercept packets (henceforth referred to as the combined eavesdropper throughput) goes to 0?* In this paper, we study the security versus capacity trade-offs for a class of algorithms that artificially generate noise to ensure message secrecy. The results obtained in this paper can be employed for network design in wireless systems that wish to guarantee a given secrecy rate per session (w.h.p), hence addressing the difficult problem of secrecy rate selection when eavesdropper locations are unknown. The results can also be used underneath network-level approaches that, for example, split a message into several smaller messages each of which is encoded and transmitted along different routes to avoid their capture.

The efficient use of artificial noise generation for secrecy has been considered in two-hop relay networks in [3, 17] and for arbitrary (but known) finite network topologies in [14]. Only a few works have considered secrecy in large networks. Reference [9] considers the density of eavesdroppers that can be tolerated while maintaining the per-node throughput of [2], and [6] considers the connectivity graph of large wireless networks when insecure links are removed. However, the results of [9] and [6] are for networks where eavesdropper locations are known to system nodes, and, hence, the network is able to route around eavesdroppers. The security of large mobile networks without delay or buffer constraints, where the mobility simplifies the problem by reducing it to a two-phase construction as in [4], has been considered in [10]. Hence, we are unaware of any prior work that has considered the achievable security of asymptotically large static networks where eavesdropper locations are unknown.

1.1 Main Results

We consider a large wireless network, in which nodes are distributed according to a 2D Poisson point process of unit intensity over a square of area n. Also present in the network are a collection of eavesdroppers placed according to a

Poisson process with intensity $\lambda_e(n)$.

In this setting, we propose a construction in which nodes transmit artificial noise to ensure the secrecy of messages from the eavesdroppers. Our construction can achieve any desired per-node throughput $\Psi(n)$ inside the interval $(1/n, 1/\sqrt{n})$, while yielding the following scaling laws for the number of eavesdroppers:

1. When eavesdroppers operate independently i.e. do not collude with each other, the network can tolerate $\Omega\left(\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)^{2c_1}\right)$ eavesdroppers, where $0 < c_1 < 1$, while ensuring that the combined eavesdropper throughput, denoted as $\Psi_{\mathbf{E}}(n)$, goes to 0 as $n \to \infty$.

   An identical scaling law is derived, even when eavesdroppers have multiple (but, a fixed number of) antennas.

2. We also consider a collaborating eavesdropper model in which a single eavesdropper is allowed to have a number of antennas that scales with n. Under this model, we show that $\forall \epsilon > 0$, an eavesdropper with $\Omega\left(\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)^{1-\epsilon}\right)$ antennas can be tolerated while ensuring that $\Psi_{\mathbf{E}}(n)$ goes to 0.

3. Finally, we derive sufficient conditions for the number of eavesdroppers to achieve a non-zero $\Psi_{\mathbf{E}}(n)$. In particular, we show that when eavesdroppers operate independently, then $O\left(\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)^{2c_2}\right)$ eavesdroppers suffice to achieve a non-zero $\Psi_{\mathbf{E}}(n)$, for some constant $c_2 > 1$. Also, an eavesdropper with $O\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)$ antennas suffices to achieve a non-zero $\Psi_{\mathbf{E}}(n)$.

Thus, our results imply that there is an inherent trade-off between the per-node throughput and achievable secrecy. Our results show, for instance, that when a per-node throughput of $\Psi(n) = \Omega((n \ln n)^{-1/2})$ is desired, we can tolerate up to $\Omega((\ln n)^{c_1})$ independent eavesdroppers or a single eavesdropper with $\Omega((\ln \ln n)^{1-\epsilon})$ antennas. Higher node throughputs can be achieved while reducing the allowable number of eavesdroppers. At the other extreme, we can tolerate up to $\Omega(n^{c_1})$ independent eavesdroppers while achieving only a per-node throughput guarantee of $\omega(1/n)$. Finally, we note that the scaling laws for the sufficient number of eavesdroppers to achieve a non-zerp $\Psi_{\mathbf{E}}(n)$ show that the bounds for allowable number of eavesdroppers are tight up to a polynomial factor.

The rest of the paper is organized as follows. Section 2 presents the system assumptions. In Section 3, we describe our construction for achievable node throughput in presence of artificial noise. In Section 4, we analyze the number of independent eavesdroppers that can be tolerated in the network. In Section 5, we carry out a similar analysis for the case of collaborating eavesdroppers. Section 6 carries a discussion of our results while Section 7 presents our conclusions.

2. SYSTEM MODEL AND ASSUMPTIONS

1. We consider a collection of static nodes placed according to a Poisson point process of unit intensity over a square $\mathcal{B}_n = [0, \sqrt{n}] \times [0, \sqrt{n}]$.

2. Also present in the 2D plane is a set $\mathbf{E}$ of passive eavesdroppers distributed according to a Poisson process of intensity $\lambda_e(n)$.

3. We choose uniformly at random a matching of source-destination pairs, so that each node is the destination of exactly one source.

4. All links experience frequency-nonselective Rayleigh fading. The fading is assumed to be *quasi-static*, which is defined here as being constant over the transmission of a single secure message. The fading across different links and between transmissions on the same link are assumed independent.

5. Let $\mathcal{T}$ be the subset of nodes transmitting at a given time instant. Let d_{ij} denote the distance between an arbitrary pair of nodes i and j. Then, a transmission from node i is successfully received by node j only if the signal to interference plus noise ratio (SINR) at node j (denoted as $\mathcal{S}_j$) exceeds a fixed decoding threshold γ i.e.

$$\mathcal{S}_j = \frac{P|h_{ij}|^2 {d_{ij}}^{-\alpha}}{N_0 + \sum\limits_{k \in \mathcal{T} \setminus \{i\}} P|h_{kj}|^2 {d_{kj}}^{-\alpha}} \geq \gamma, \quad \gamma > 1$$

   where P denotes the transmit power and $|h_{ij}|^2$ denotes the fading gain, a non-negative random variable that models fading on link $i \to j$. N_0 is the ambient noise power at the receiver.

6. Throughout this paper, we assume *channel reciprocity* i.e. $|h_{ij}|^2 = |h_{ji}|^2$, for any two nodes i and j. Further, the Rayleigh fading assumption implies that the fading gain $|h_{ij}|^2$ follows an exponential distribution for all node pairs i, j. We also assume that node i can perfectly estimate the channel to another node j, as is commonly done in commercial systems using pilot signals [16, pg. 53]. Without loss of generality, we take $E[|h_{ij}|^2] = 1$.

3. ACHIEVABLE PER-NODE THROUGHPUT

In this section, we describe a construction which yields a per-node throughput $\Psi(n) = \Omega\left((nf(n))^{-1/2}\right)$, where $f(n)$ is any arbitrary function satisfying:

$$\omega(1) \leq f(n) \leq o(n) \tag{1}$$

The conditions for $f(n)$ thus allow us to achieve any desired throughput in the interval $(1/n, 1/\sqrt{n})$. On the flip side, it is easy to note that the same conditions forbid us from achieving the per-node throughput of $\Omega(n^{-1/2})$, as obtained in [2, 13]. But as we will see later, the asymptotic reduction in throughput allows us to tolerate an asymptotically large number of eavesdroppers.

Similar to [2, 13], our construction uses percolation theory to show the achievability result. However, our construction differs from those in [2, 13] in two crucial aspects:

- Our construction allows system nodes to artificially transmit noise to ensure secrecy of messages transported across the network. Hence, the construction needs to ensure successful delivery of messages to legitimate nodes in presence of this added interference.

- As we will see later, the fact that links experience time varying fading in our model necessitates a substantially different relay selection algorithm from those described in [2, 13].

Our result implies that as $f(n)$ grows, the per-node throughput decreases. However, we will see later that this results in a greater number eavesdroppers being allowed. Expressing the per-node throughput in terms of $f(n)$ therefore provides us a better understanding of the trade-offs between security and the achievable throughput.

Our capacity construction involves three major steps:

1. Construction of a highway system,
2. Specification of a routing protocol, and
3. Specification of a transmission scheduling scheme

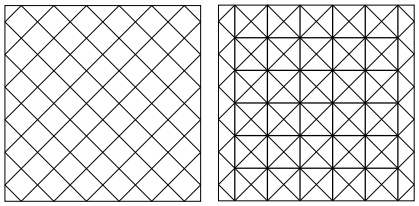

Figure 1: Construction of the bond percolation model. The figure on the left hand side corresponds to division of the unit square into smaller cells. The figure on the right hand side is obtained by associating an edge with each cell, traversing it diagonally.

3.1 Highway Construction

As shown in the left side of Figure 1, we divide the square $\mathcal{B}_n$ into cells of dimensions $c(n) \times c(n)$ where

$$c(n) = \sqrt{f(n)} \tag{2}$$

The number of nodes inside a given cell is therefore a Poisson random variable with parameter $f(n)$.

As shown in Figure 2, for each cell, we define eight regions $\mathcal{H}_1 - \mathcal{H}_8$, each having an area $f(n)/2$. The reason for defining these regions will become apparent when we discuss relay selection in Section 3.2. For now, we show that each cell has

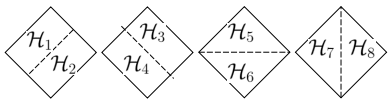

Figure 2: Regions $\mathcal{H}_1 - \mathcal{H}_8$ associated with each cell $\hat{c}_i$.

a large number of nodes inside each of its regions $\mathcal{H}_1 - \mathcal{H}_8$.

LEMMA 3.1. *Let N_{ij} be the number of nodes in region $\mathcal{H}_j, j = 1, \ldots, 8$ of a given cell $\hat{c}_i$. Let E_i denote the event $\{f(n)/4 \leq N_{ij} \leq f(n), \ \ \forall j\}$. Then,*

$$p(n) \equiv P(E_i) > 1 - 16\left(\frac{2}{e}\right)^{f(n)/4}$$

PROOF. Let E_i denote the event:

$$\left\{f(n)/4 \leq N_i^j \leq f(n), \ \ \forall j\right\}$$

Then, E_i^c denotes the event:

$$\left\{\exists j : \{N_{ij} < f(n)/4\} \bigcup \{N_{ij} > f(n)\}\right\}$$

From Theorem A.1, for a fixed j,

$$P(N_{ij} < f(n)/4) \leq e^{-f(n)/2}(2e)^{f(n)/4} = \left(\frac{2}{e}\right)^{f(n)/4}$$

Similarly,

$$P(N_{ij} > f(n)) \leq \left(\frac{e}{4}\right)^{f(n)/2} \leq \left(\frac{2}{e}\right)^{f(n)/4}$$

Using the *union bound* twice,

$$P(E_i^c) \leq 16\left(\frac{2}{e}\right)^{f(n)/4}$$

Lemma 3.1 now follows immediately. □

We declare a cell $\hat{c}_i$ *open*, if E_i holds, and *closed* otherwise. From Lemma 3.1, it is easy to see that the probability $p(n)$ that a given cell is open goes to 1 as $n \to \infty$.

Similar to [2], we map the constructed lattice to a *bond percolation model*. As shown on the right side of Figure 1, we draw a horizontal edge traversing a cell diagonally across half of the cells and a vertical edge across the remaining half. In this way, we obtain a grid of horizontal and vertical edges, each edge being open with probability $p(n)$, independently of all other edges.

For convenience of exposition, we introduce a quantity $m(n)$ that denotes the number of (horizontal or vertical) edges composing the side length of the box $\mathcal{B}_n$. Then,

$$m(n) = \frac{\sqrt{n}}{\sqrt{2}c(n)} \tag{3}$$

Notice that $m(n) \to \infty$ as $n \to \infty$.

We divide the box $\mathcal{B}_n$ into rectangular slabs of dimensions $\sqrt{n} \times \sqrt{2}c(n)(\kappa \ln m(n) - \epsilon_n)$, where $\kappa > 0$. Let R_n^i denote the i-th slab, where $i \leq \frac{m(n)}{\kappa \ln m(n) - \epsilon_n}$. We choose $\epsilon_n > 0$ as the smallest value such that the number of rectangular slabs $\frac{m(n)}{\kappa \ln m(n) - \epsilon_n}$ is an integer. As noted in [2], $\epsilon_n = o(1)$ as $n \to \infty$. Let C_n^i denote the maximal number of edge-disjoint left-to-right crossing paths of rectangle R_n^i and let $N_n = \min_i C_n^i$.

We then have the following theorem which shows the existence of a large number of crossing paths in each of the rectangular slabs of $\mathcal{B}_n$.

THEOREM 3.2. *For all $\kappa > 0$, there exists a δ satisfying $0 < \delta < \kappa$ such that*

$$\lim_{n \to \infty} P(N_n \leq \delta \ln m(n)) = 0$$

PROOF. The proof follows from Theorem 5 in [2] by noting that $p(n) > 5/6$ for large enough n. Taking limits as $n \to \infty$, the inequality (16) in [2] yields the condition $0 < \delta < \kappa$. □

Thus, Theorem 3.2 shows not only that each rectangular slab has a large number of crossing paths but also that each

node is at most $\kappa \ln m(n)$ away from a crossing path. Similarly, by dividing $\mathcal{B}_n$ into vertical rectangular slabs of sides $\sqrt{2}c(n)(\kappa \ln m(n) - \epsilon_n) \times \sqrt{n}$, we can show that there exist $\delta \ln m(n)$ top-to-bottom crossing paths inside each vertical slab. Using the union bound, we conclude that there exist $\Omega(m(n))$ left-to-right and top-to-bottom crossing paths (also called *highways*) of $\mathcal{B}_n$ w.h.p.

We conclude the discussion on highway construction by deriving a *uniform* bound on the probability that a cell is open, for a sufficiently large $f(n)$. This is in contrast to Lemma 3.1, which only bounds the probability that a given cell is open. Once again, let N_{ij} denote the number of nodes in the region $\mathcal{H}_j$ of cell $\hat{c}_i$.

LEMMA 3.3. *When $f(n) \geq k \ln n$, where $k = 4 \log_{e/2} e$*

$$\lim_{n\to\infty} P(f(n)/4 \leq N_{ij} \leq f(n) \ \ \forall i,j) = 1$$

PROOF. Applying Lemma 3.1 and the union bound, we get

$$\begin{aligned} P(f(n)/4 \leq N_{ij} \leq f(n) \ \ \forall i,j) &\geq 1 - \frac{16n}{f(n)} \left(\frac{2}{e}\right)^{f(n)/4} \\ &\geq 1 - \frac{16n}{f(n)} \left(\frac{1}{e/2}\right)^{\log_{\frac{e}{2}} n} \\ &\geq 1 - \frac{16}{f(n)} \to 1 \end{aligned}$$

as $n \to \infty$. □

Thus, when $f(n) \geq k \ln n$, all cells are open w.h.p. In other words, each node is located on a highway w.h.p.

Finally, we uniformly bound the number of nodes per cell when $f(n) < k \ln n$, where $k = 4 \log_{e/2} e$. Let N_i denote the number of nodes in cell $\hat{c}_i$. Then,

LEMMA 3.4.

$$\lim_{n\to\infty} P(N_i \leq 2k \ln n \ \ \forall i) = 1$$

PROOF. The proof follows from an application of the Chernoff and union bounds.

$$\begin{aligned} P(N_i \leq 2k \ln n \ \ \forall i) &\geq 1 - \frac{n}{f(n)} P(N_i > 2k \ln n) \\ &\geq 1 - \frac{n}{f(n)} e^{-f(n)} \left(\frac{ef(n)}{2k \ln n}\right)^{2k \ln n} \\ &\geq 1 - \frac{n}{f(n)} e^{-f(n)} \left(\frac{e}{8 \log_{e/2} e}\right)^{2k \ln n} \\ &\geq 1 - \frac{n}{f(n)} e^{-f(n)} \left(\frac{1}{e}\right)^{2k \ln n} \to 1 \end{aligned}$$

as $n \to \infty$. □

3.2 Routing Protocol

Similar to [2, 13], our routing protocol involves three phases:

1. The *draining phase* in which a source transmits a packet to a nearby "entry point" situated on a horizontal crossing path.

2. The *highway phase* in which the packet is moved first along a horizontal crossing path and then along a vertical crossing path until it arrives at an "exit point", which is suitably close to the destination node.

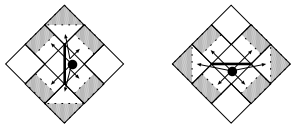

Figure 3: Relay selection for each of cell containing horizontal edge and vertical edge. Only nodes inside the shaded area are eligible for relay selection. The shaded regions correspond to the regions $\mathcal{H}_1 - \mathcal{H}_8$ defined earlier.

3. The *delivery phase* in which the packet is transmitted from the exit point to the destination node via an intermediate relay node.

Note that the draining and delivery phases are employed only when $f(n) < k \ln n$, where $k = 4 \log_{e/2} e$. When $f(n) \geq k \ln n$, we know from Lemma 3.3 that each node is located on a highway w.h.p and hence, the routing protocol involves only the highway phase.

In contrast to the routing strategy in [2, 13] where the nodes on a routing path are fixed over the entire set up, we opportunistically choose a relay node at each hop and with a sufficiently large fading gain. As a result, for the same source-destination pair, the routing paths may vary from one packet transmission to the next.

3.2.1 Relay Selection in Highway Phase

As shown in Figure 3, in the highway phase, a packet is forwarded from a node i in an open cell $\hat{c}_i$ to another node j in an adjacent open cell $\hat{c}_j$ which is chosen as follows:

1. Node i broadcasts a pilot signal and announces the co-ordinates of its cell $\hat{c}_i$ as well as those of its adjacent cell $\hat{c}_j$ to which the packet is next destined.

2. Depending on $\hat{c}_i$ and $\hat{c}_j$'s co-ordinates, only nodes inside one of the eight regions $\mathcal{H}_1 - \mathcal{H}_8$ of $\hat{c}_j$ (see Figure 3), are eligible to participate in relay selection. Each eligible node j then measures its fading gain, $|h_{ij}|^2$, from i's pilot.

3. Let $\hat{n} = f(n)/4$. Then, a node j announces itself the relay if $|h_{ij}|^2 > \ln \hat{n}$.

4. In case no relay is chosen, in keeping with the quasi-static Rayleigh fading assumption, node i once again broadcasts a pilot signal and steps 1-3 are repeated.

The probability that exactly one node announces itself as the relay is therefore

$$p_s = N_r \frac{1}{\hat{n}} \left(1 - \frac{1}{\hat{n}}\right)^{N_r - 1} \geq \hat{n} \frac{1}{\hat{n}} \left(1 - \frac{1}{\hat{n}}\right)^{8\hat{n}} = \frac{1}{e^8} > 0$$

where N_r is the number of eligible relay nodes and from Lemma 3.1 lies in the range $[\hat{n}, 8\hat{n}]$. Thus, the probability of a successful relay selection is a constant bounded away from 0. In other words, a relay j is chosen in a finite expected time (equal to e^8) such that $|h_{ij}|^2 > \ln(f(n)/4)$.

We note that the lower bound on p_s can be significantly improved by employing more time slots for relay selection. However, these improvements do not change the asymptotic results obtained in this paper.

When $f(n) \geq k \ln n$, where $k = \log_{e/2} e$, we note that each packet is routed along the highways until it reaches

the destination cell $\hat{c}_d$. The packet is then delivered to the destination d in two steps via an intermediate relay node r. This relay r is chosen from one of the adjacent cells of $\hat{c}_d$ and is at least $c(n)/2$ away from d. The relay selection is discussed in detail in Section3.2.4.

3.2.2 Draining Phase

As mentioned earlier, the draining phase is employed only when $f(n) < k \ln n$, where $k = 4 \log_{e/2} e$. The objective of the draining phase is for a source node to determine an entry point situated on a horizontal crossing path to which it can transmit directly. Before choosing an entry point, each source node is mapped to a horizontal crossing path and a set of eligible entry points chosen as follows.

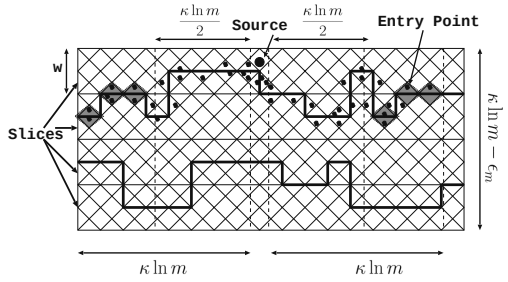

Figure 4: Entry Point Selection. Only nodes in cells with a horizontal edge and which are located at least $\frac{\kappa \ln m}{2}$ and at most $\kappa \ln m$ from the cell containing the source (i.e. shaded cells) are eligible for selection.

1. **Division of $\mathcal{B}_n$ into rectangular slabs:** We divide the square $\mathcal{B}_n$ into an integer number of rectangular slabs of size $m \times \kappa \ln m(n) - \epsilon_n$, where $m(n) = \sqrt{n}/(\sqrt{2}c(n))$. Figure 4 shows a portion of a rectangular slab. We choose a κ such that there are at least $\lceil \delta \ln m(n) \rceil$ crossing paths inside each rectangular slab. These crossing paths are numbered $1, \ldots, N_n$.

2. **Mapping source node to a horizontal crossing path:** We next divide each rectangular slab into $\lceil \delta \ln m(n) \rceil$ smaller *slices*, each of dimensions $n \times w\sqrt{2}c(n)$, where w is a constant. Figure 4 depicts the case where $w = 2$. Each source node in the i-th slice is then mapped to the i-th horizontal crossing path and therefore, chooses an entry point located along the i-th path. Note that as depicted in Figure 4, a crossing path could potentially traverse multiple slices. Further, even though a source node may be located on a crossing path, the mapping scheme can potentially lead the source node to access an entry point on an entirely different crossing path. The main goal of our mapping scheme is to achieve "load-balancing" by distributing source nodes across different crossing paths in a rectangular slab. In fact, we next prove Lemma 3.5 which shows that each crossing path has a bounded number of source nodes accessing it.

   Lemma 3.5 *uniformly* bound the number of streams carried by a highway. We know that the number of streams carried by a highway is bounded by the number of nodes, N_s, in a rectanglular slice s of dimensions $\sqrt{n} \times w\sqrt{2}c(n)$. There are $w\sqrt{nf(n)}$ slices in total, each of which has an area $\sqrt{n} \times \sqrt{2}c(n)w = w\sqrt{2nf(n)}$. Then,

   LEMMA 3.5.

   $$\lim_{n \to \infty} P(N_s \leq 2w\sqrt{2nf(n)}, \quad \forall s) = 1$$

   PROOF. Using the Chernoff and union bounds, we get

   $$P(N_s \leq 2w\sqrt{2nf(n)}, \forall s) \geq 1 - w\sqrt{nf(n)} \left(\frac{e}{4}\right)^{w\sqrt{2nf(n)}}$$

   $$\rightarrow 1$$

   as n tends to infinity. □

3. **Determining eligible entry points:** Once the source nodes are mapped to crossing paths, the set of eligible entry points for each source are determined as follows: Only nodes located inside open cells at a *horizontal* distance is in the range $[(\kappa \ln m(n))/2, \kappa \ln m(n)]$ from the cell containing the source node are eligible for selection. Further, the entry points are chosen from only those open cells containing a horizontal edge. For instance, in Figure 4, only nodes in the shaded cells are eligible to function as entry points.

   Thus, the number of eligible cells (i.e. shaded cells in Figure 4) is at least $(\kappa \ln m(n))/2 - 1$ (occurs when a source is on the boundary of a slab) and at most $\kappa \ln m(n)$. From Lemma 3.1, we therefore conclude that the number of eligible entry points is in the range $[(\kappa \ln m(n) - 2)f(n)/4, 2f(n)\kappa \ln m(n)]$.

   Note that steps 1-3 are performed only once and not repeated every time a source needs to transmit a packet. Finally, we are ready to choose an entry point for a source node i.

4. **Entry point selection:** An entry point j is chosen from the set of eligible points using the scheme described in Section 3.2.1 by setting $\hat{n} = (\kappa \ln m(n) - 2)f(n)/4$ in Step 2 of the relay selection scheme. Once again, it can be easily verified that the probability of successful entry point selection is at least $1/e^9$ i.e. a constant bounded away from 0. Further, the chosen entry point j has a fading gain $|h_{ij}|^2 > \ln \hat{n}$ to the source i.

3.2.3 Delivery Phase

Once gain, the delivery phase is employed only when $f(n) < k \ln n$, where $k = 4 \log_{e/2} e$. The mapping of destinations to vertical crossing paths is analogous to the mapping described in Section 3.2.2. In this section, we therefore focus only on exit point selection and the subsequent delivery of packets to destination nodes.

Exit Point Selection: A packet destined for a node d located in cell $\hat{c}_d$ is forwarded along a vertical crossing path, until it arrives at a node p located in cell $\hat{c}_p$ whose *vertical* distance to $\hat{c}_d$ is $\kappa \ln m(n)$. Node p then becomes the exit point for destination d. For illustration, one can rotate Figure 4 clockwise by 90^o and treat the node labeled "Source" as the destination node d instead. Assuming that the packet for d is moving from left to right in Figure 4 (or top-to-bottom in the rotated figure), the leftmost shaded cell in Figure 4 is the cell $\hat{c}_p$.

Eligible Relay Nodes: Once an exit point p is chosen, the packet is delivered to node d by p via an intermediate relay node from a set of eligible relay nodes. A node r located in cell $\hat{c}_r$ is eligible for relay selection if it satisfies the following conditions:

1. The cell $\hat{c}_r$ must lie between $\hat{c}_p$ and $\hat{c}_d$ i.e. its y-coordinate must lie between those of $\hat{c}_p$ and $\hat{c}_d$.
2. The cell $\hat{c}_r$ must contain a vertical edge
3. The vertical distance between cells $\hat{c}_r$ and $\hat{c}_p$ must be at least $\frac{\kappa \ln m(n)}{4}$, and
4. The vertical distance between cells $\hat{c}_r$ and $\hat{c}_d$ must also be at least $\frac{\kappa \ln m(n)}{4}$.

It is easy to see that there are $\frac{\kappa \ln m(n)}{2}$ cells satisfying the above criteria. From Lemma 3.1, we conclude that the number of eligible relay nodes N_r satisfies $\frac{f(n)\kappa \ln m(n)}{4} \leq N_r \leq f(n)\kappa \ln m(n)$.

Relay Selection: Finally, the relay r^* is chosen as follows:

1. p transmits a pilot signal. Each eligible node r measures its fading gain, $|h_{rp}|^2$ to p.
2. Next, d transmits a pilot signal and once again, each eligible node r measures its fading gain $|h_{rd}|^2$ to node d.
3. Finally, a node r^* satisfying $\min(|h_{r^*p}|^2, |h_{r^*d}|^2) > (\ln \hat{n})/2$, where $\hat{n} = \frac{f(n)\kappa \ln m(n)}{4}$, announces itself as the relay.

Since the minimum of 2 iid exponential random variables with mean 1 is also an exponential random variable with mean 1/2, it is easy to check that the probability that a node r^* announces itself as the relay is $1/\hat{n}$. proceeding as before, the probability of a successful relay selection is

$$p_s = N_r \frac{1}{\hat{n}} \left(1 - \frac{1}{\hat{n}}\right)^{N_r - 1} \geq \hat{n} \frac{1}{\hat{n}} \left(1 - \frac{1}{\hat{n}}\right)^{4\hat{n}} \geq \frac{1}{e^4} > 0$$

Once again, p_s is a constant bounded away from 0. Further, the selected relay r^* satisfies: $\min(|h_{rp}|^2, |h_{rd}|^2) > (\ln \hat{n})/2 = \ln\left(\frac{f(n)\kappa \ln m(n)}{4}\right)/2$.

3.2.4 Delivery to Destination

When $f(n) \geq k \ln n$, where $k = 4 \log_{e/2} e$, we know from Lemma 3.3 that each cell is open w.h.p and each node is located along a highway. As mentioned earlier, we therefore do not employ the draining and delivery phases in our routing algorithm and each packet destined for a node d is routed first along a horizontal crossing path and then along a vertical crossing path until it reaches a node t inside the destination cell $\hat{c}_d$. The node is then delivered from t to d in two steps via an intermediate relay node, chosen in a manner similar to that described in Section 3.2.3.

The process of delivering the packet from node t to node d is illustrated in Figure 5. The relay selection algorithm operates as follows:

1. Node t broadcasts a pilot signal and the co-ordinates of the cell $\hat{c}_d$. Each node r in a cell adjacent to $\hat{c}_d$ and located inside the corresponding shaded area as shown in Figure 5, measures its fading gain $|h_{tr}|^2$.

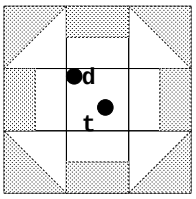

Figure 5: Delivery to Destination. The cell in the middle is the destination cell. The packet is currently at node t and needs to be delivered to node d. This is accomplished via a relay node chosen from the shaded areas of the adjacent cells.

2. Next, the destination node d broadcasts a pilot signal and once again, each node r in the shaded areas of the adjacent cells measure $|h_{dr}|^2$.
3. Let $\hat{n} = \frac{3f(n)}{4}$. Then, an eligible relay node r^* announces itself as the relay node only if $min(|h_{tr^*}|^2, |h_{dr^*}|^2) > \ln \hat{n}/2$.
4. If no relay is chosen, then steps 1-3 are repeated all over again.

Since the number of eligible relay nodes N_r lies in the range $[\hat{n}, 8\hat{n}]$, once again, it follows that the probability of a successful relay selection is at least $\frac{1}{e^8}$, and is thus, bounded away from 0. Finally, we note that a relay r^* with a fading gain at least $(\ln \hat{n})/2$ to each of nodes t and r is chosen in a finte expected time.

3.3 Transmission Scheduling Scheme

We finally describe our transmission scheduling scheme illustrated in Figure 6. The key idea as in [2, 13] is to space simultaneous transmissions sufficiently far apart such that each transmission succeeds w.h.p. Unique to our transmission scheme, however, is a mechanism for choosing noise-generating nodes and is discussed next.

Let the simultaneous transmissions be spaced $2d$ cells apart, where the value of d will be determined for each of the phases. Further, each node in our construction transmits with a power $P_n(d) \propto (dc(n))^\alpha$. As we will see, the value of d varies between the highway and draining/delivery phases, and hence, nodes employ separate transmit powers for the different phases.

Remark: Notice from the expression for $P_n(d)$ that we increase the density of the network (number of nodes per cell) by increasing the transmit power of nodes, as opposed to increasing the number of nodes per unit area [5]. As we will see in Section 6, increasing network density by increasing transmit powers avoids the near-field effects of electromagnetic propagation and results in a realistic model. If near-field effects can be neglected and independent fading can be assumed, as is done in the dense network models of [5, 15], we note that our construction would also employ a constant power setting and identical results would be obtained.

3.3.1 Artificial Noise Generation

Unlike the constructions in [2, 13], the primary objective in our work is to achieve message secrecy in the presence of eavesdroppers. To guard against the message being succesfully decoded by an eavesdropper, we require a subset

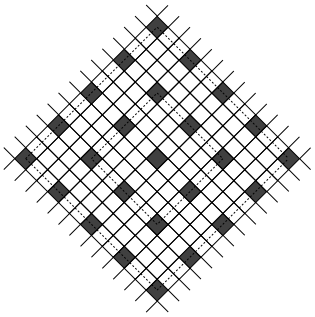

Figure 6: Transmission Scheduling. Simultaneous transmissions (by nodes in shaded cells) are at least $2d$ cells apart. In the figure, $d = 1$.

of system nodes to generate noise simultaneously with the message transmissions.

Regardless of which phase a transmission occurs in, we observe that greater the number of noise-generating nodes the greater will be the number of eavesdroppers that are unable to decode a given transmission. At the same time, the chance that a legitimate node decodes the transmission is also reduced. Ideally, we want to maximize the amount of generated noise, while ensuring that a legitimate receiver decodes a transmission w.h.p.

Consider a transmission from a node R_i in cell $\hat{c}_i$ to a next hop node R_j. Regardless of the phase, the set of noise-generating nodes are chosen according to the following rule: *Nodes inside cell $\hat{c}_i$ within a radius*

$$r(n) = \ln\left(\frac{f(n)}{4}\right)^{\nu/2} \tag{4}$$

from R_i transmit noise, where $\nu = 1/(2^{3+5\alpha/2}\pi\gamma)$.

The rationale behind the choice of $r(n)$ will become clear, when we show that the receive SINR $\mathcal{S}_j$ at node R_j exceeds γ, for both the highway and the draining/delivery phases. Intuitively, choosing noise-generating nodes close to R_i serves two purposes: (i) noise-generating nodes are far away from the receiving node R_j, and (ii) eavesdroppers close to R_i receive sufficient interference to keep them from decoding R_i's transmission.

3.3.2 Receive SINR in Highway Phase

Consider a transmission from a node R_i to another node R_j and let $\mathcal{S}_j$ be R_j's received SINR. Then,

$$\mathcal{S}_j = \frac{P_n(d)|h_{ij}|^2/d_{ij}^{\alpha}}{N_0 + P_n(d)\mathcal{I}_{near} + P_n(d)\mathcal{I}_{far}}$$

where $P_n(d)$ denotes R_i's transmit power, $\mathcal{I}_{near}$ denotes the "near-cell" interference at R_j caused by noise-generating nodes in cell $\hat{c}$ and $\mathcal{I}_{far}$ denotes the interference from the rest of the network. From Section 3.2.1, we know that $|h_{ij}|^2 > \ln\left(\frac{f(n)}{4}\right)$. Further, in the highway phase $d_{ij} \leq 2\sqrt{2}c(n)$. Hence,

$$\mathcal{S}_j \geq \frac{P_n(d)\ln\left(\frac{f(n)}{4}\right)/(2\sqrt{2}c(n))^{\alpha}}{N_0 + P_n(d)\mathcal{I}_{near} + P_n(d)\mathcal{I}_{far}} \tag{5}$$

I_{near} is upper bounded as

$$I_{near} \leq \sum_{R_k \in \mathcal{R}} \frac{|h_{kj}|^2}{(c(n)/2)^{\alpha}}$$

where $\mathcal{R}$ denotes the set of noise-generating nodes inside $\hat{c}$. The term in the denominator follows immediately by observing Figure 3 and by imagining R_j located inside one of the shaded areas.

The area over which noise-generating nodes are located is upper bounded by $\pi r^2(n)$. Hence, $P(|\mathcal{R}| > a) \leq P(N > a), \ \forall a$, where $N \sim \text{Poisson}(\sigma(n))$. Here, $\sigma(n) = \pi r^2(n) = \ln\left(\frac{f(n)}{4}\right)^{\pi/\nu}$. From Theorem A.1, we conclude

$$P\left(|\mathcal{R}| > 2\sigma(n)\right) < (e/4)^{\sigma(n)}$$

The right hand side goes to 0 as $n \to \infty$. Hence, w.h.p., the sum $\sum_{R_k \in \mathcal{R}} |h_{kj}|^2$ is upper bounded by a sum of $2\sigma(n)$ iid exponential random variables. Noting that the sum of iid exponential random variables is an Erlang random variable and employing Chernoff bounds for the same (see Appendix A.2), we obtain

$$P\left(\sum_{R_k \in \mathcal{R}} |h_{kj}|^2 > 4\sigma(n)\right) < (2/e)^{2\sigma(n)}$$

Thus,

$$I_{near} \leq 4\sigma(n) = \frac{\ln\left(\frac{f(n)}{4}\right)}{2\gamma(2\sqrt{2}c(n))^{\alpha}} \tag{6}$$

with probability at least

$$1 - (e/4)^{\sigma(n)} - (2/e)^{2\sigma(n)}$$

which goes to 1 as $n \to \infty$, since $\sigma(n) \to \infty$.

We next derive an upper bound for I_{far}. We first note that relative to node R_j, the transmitters in the eight closest cells (i.e. the shaded cells in Figure 6) from R_j are at Euclidean distance at least $dc(n)$, where d is a constant and will be determined later. The transmitters in the 16 next closest cells are at Euclidean distance at least $3dc(n)$ and so on. In other words, relative to R_j, the other transmitters are located along the boundaries of concentric squares of increasing size. Therefore,

$$\mathcal{I}_{far} \leq \sum_{t=1}^{\infty} \sum_{R_k \in \mathcal{R}^{(t)}} \frac{|h_{kj}|^2}{((2t-1)dc(n))^{\alpha}}$$

where $\mathcal{R}^{(t)}$ denotes the set of noise-generating nodes located along the boundary of the t-th concentric square from R_i. Once again, it is easy to see that $P(|\mathcal{R}^{(t)}| > a) \leq P(N > a), \forall a$ where $N \sim \text{Poisson}\,(8t\sigma(n))$. From Theorem A.1, we conclude

$$\mathcal{I}_{far} \leq \frac{32\sigma(n)}{(dc(n))^{\alpha}} \sum_{t=1}^{\infty} \frac{t}{(2t-1)^{\alpha}}$$

Notice that the sum converges for $\alpha > 2$. A trite calculation shows that this sum can be upper bounded by $\beta = 1 + 1/(2(\alpha - 2))$ and hence,

$$\mathcal{I}_{far} \leq \frac{4\beta\ln\left(\frac{f(n)}{4}\right)}{(2\sqrt{2}dc(n))^{\alpha}} \tag{7}$$

Letting $\mathcal{A}$ denote the event $\left\{\mathcal{I}_{far} > \frac{4P_n(d)\beta \ln \frac{f(n)}{4}}{(2\sqrt{2}dc(n))^{\alpha}}\right\}$ and using the union bound, we get

$$\begin{aligned} P(\mathcal{A}) &< \sum_{t=1}^{\infty} \left((e/4)^{8t\sigma(n)} + (2/e)^{16t\sigma(n)}\right) \\ &= \frac{(e/4)^{8\sigma(n)}}{1-(e/4)^{8\sigma(n)}} + \frac{(2/e)^{16\sigma(n)}}{1-(2/e)^{16\sigma(n)}} \to 0 \end{aligned}$$

as $n \to \infty$.

Substituting from (6) and (7) into (5) and further simplification yields:

$$\mathcal{S}_j \geq \frac{1}{N_0 \frac{(2\sqrt{2}c(n))^{\alpha}}{P_n(d)\ln\left(\frac{f(n)}{4}\right)} + \frac{1}{2\gamma} + \frac{4\beta}{d^{\alpha}}} \quad \text{w.h.p}$$

Noting that $P_n(d) \propto (dc(n))^{\alpha}$ and setting $d \geq (8\beta\gamma)^{1/\alpha}$, we get

$$\lim_{n\to\infty} \mathcal{S}_j \geq \gamma \quad \text{w.h.p}$$

3.3.3 Receive SINR in Draining and Delivery Phases

Using an analysis very similar to the one in previous section, we show that the receive SINR in the draining and delivery phases exceeds γ. The following analysis applies to both draining and delivery phases.

From Section 3.2.2 and Section 3.2.3, we know that any transmitter-receiver pair is separated by a Euclidean distance at most $2\sqrt{2}\kappa c(n)\ln m$. Further, the fading again on each transmitter-receiver link is at least $\left(\ln\left(\frac{\kappa f(n)\ln m}{4}\right)\right)/2$.

Consider a node R_i transmitting to another node R_j. Let $\mathcal{S}_j$ denote the SINR at R_j. Then,

$$S_j \geq \frac{P_n(d)\ln\left(\frac{\kappa f(n)\ln m}{4}\right)/(2\sqrt{2}\kappa c(n)\ln m)^{\alpha}}{2N_0 + 2P_n(d)I_{near} + 2P_n(d)I_{far}}$$

Further, the distance from noise-generating nodes to R_j in each phase is guaranteed to be at least $\frac{\kappa c(n)\ln m}{8}$. Proceeding exactly as in Section 3.3.2, we obtain

$$I_{near} \leq \frac{2^{2\alpha}\ln\left(\frac{f(n)}{4}\right)}{2\gamma(2\sqrt{2}\kappa c(n)\ln m)^{\alpha}} \quad \text{w.h.p}$$

and

$$I_{far} \leq \frac{4\beta\ln\left(\frac{f(n)}{4}\right)}{(2\sqrt{2}dc(n))^{\alpha}} \quad \text{w.h.p}$$

where β is as defined in Section 3.3.2. Letting $d = \kappa\ln m$ and noting that $m = (n/f(n))^{1/2}$, it can easily be checked that

$$\lim_{n\to\infty} S_j \geq \lim_{n\to\infty} \frac{\ln\left(\frac{\kappa f(n)\ln m}{4}\right)}{\ln\left(\frac{f(n)}{4}\right)^{\frac{2^{2\alpha}}{\gamma}} + \ln\left(\frac{f(n)}{4}\right)^{\frac{4\beta}{2^{\alpha/2}}}} \to \infty \text{ w.h.p}$$

Note that the above choice of d ensures that simultaneous transmissions are $2d = 2\kappa\ln m$ cells apart, which is sufficient to ensure a 1:1 mapping between a source node and its eligible entry points and also between an exit point and eligible relay nodes, as discussed in Sections 3.2.2 and 3.2.3 respectively.

Remark: Note that unlike [2, 13], we require that a given rate R and thus corresponding SINR γ be achieved on each link. Hence, our construction employs separate transmit powers for the highway and draining/delivery phases, as would the construction in [2, 13] under a similar constraint (as noted in [2, 13]).

3.4 Time Division Multiplexing Scheme

Finally, we achieve a per-node throughput of $\Omega((nf(n))^{-1/2})$ using the following TDM scheme:

1. We divide time into *frames*, each frame comprising one or more time *slots*. When $f(n) > k \geq n$, where $k = \log_{e/2} e$, we allocate a fraction 1/3 of total time frames to each of draining, highway and delivery phases. Else, all slots are allocated for the highway phase. Each frame consists of $4d^2$ time slots, where d varies depending on the phase. Each time slot in turn includes the time for relay selection followed by data transmission.

2. The draining and delivery phases are employed only when $f(n) < k\ln n$. Each cell transmits in at least one out of $4d^2 = \Theta(\ln^2 m(n)) = O(\ln^2 n)$ time slots. From Lemma 3.3, we know that each cell has fewer than $\ln n$ nodes w.h.p. Hence, the per-node throughput during each of draining and delivery phases is $\Omega(\ln^{-3} n)$ w.h.p.

3. As shown in Lemma 3.5, each highway is accessed by at most $2\sqrt{nf(n)}$ nodes. This yields a per-node throughput of $\Omega\left((nf(n))^{-1/2}\right)$ in the highway phase.

From the above it is clear that the highway phase is the bottleneck phase, and hence, the per-node achievable throughput is $\Omega\left((nf(n))^{-1/2}\right)$.

4. INDEPENDENT EAVESDROPPERS

We next derive conditions on the allowable number of eavesdroppers while ensuring that the combined eavesdropper throughput goes to 0. We start with the case where eavesdroppers are *independent* and consider the case of *collaborating eavesdroppers* in Section 5.

4.1 Eavesdropping Model

We make the following assumptions about eavesdropper capabilities.

1. Each eavesdropper has infinite computational power and can potentially decode messages anywhere in the network. Further, each eavesdropper can decode multiple messages at the same time.

2. An eavesdropper cannot use looks from multiple hops to jointly decode a message, but rather has to obtain a received SINR greater than γ for some hop of a given message. One mechanism for ensuring this is described in [9].

4.2 Upper Bound on Eavesdropper Throughput

Our approach towards deriving an upper bound on the combined eavesdropper throughput, $\Psi_{\mathbf{E}}(n)$, is to first determine the probability that an individual eavesdropper e can decode a given transmission. The sum of these probabilities over all transmissions in the network in a given time slot yields an upper bound on the throughput of the eavesdropper, denoted as $\Psi_e(n)$. The product of $\Psi_e(n)$ and the total

number of eavesdroppers, therefore, yields an upper bound on $\Psi_{\mathbf{E}}(n)$. We note that the upper bound on $\Psi_{\mathbf{E}}(n)$ is the same across all time slots.

Let $\mathcal{S}_e$ denote the received SINR at an eavesdropper e due to transmission by a node i located inside cell $\hat{c}_i$. Then,

$$\mathcal{S}_e = \frac{P_n(d)|h_{ie}|^2/d_{ie}^{\alpha}}{N_0 + P_n(d)\sum_{k\in\mathcal{R}}|h_{ke}|^2/d_{ke}^{\alpha}} \leq \frac{|h_{ie}|^2/d_{ie}^{\alpha}}{\sum_{k\in\mathcal{R}}|h_{ke}|^2/d_{ke}^{\alpha}}$$

where $\mathcal{R}$ denotes the set of noise-generating nodes in the entire network. In order to derive an upper bound on $\mathcal{S}_e$, we need to derive a lower bound for the sum in the denominator.

We next derive $P(\mathcal{S}_e > \gamma)$ i.e. the probability that e decodes i's transmission. We will see that the bound we derive for $P(\mathcal{S}_e > \gamma)$ is independent of the phase of operation. We consider the following two cases separately:

C1 i is located at a Euclidean distance at most $2\sqrt{2}dc(n)$ from e, where $c(n)$ is the side length of a cell and is defined in (2). We call i's transmission a *near transmission* and the denote the receive SINR at e to be $\mathcal{S}_e^{near}$ and the corresponding outage probability as $P(\mathcal{S}_e^{near} > \gamma)$.

C2 i is located at a Euclidean distance greater than $2\sqrt{2}dc(n)$ from e.

We begin with the analysis of case **C1**.

$$\mathcal{S}_e^{near} \leq \frac{|h_{ie}|^2/d_{ie}^{\alpha}}{\sum_{k\in\mathcal{R}^{(i)}}|h_{ke}|^2/d_{ke}^{\alpha}}$$

where $\mathcal{R}^{(i)}$ denotes only the noise-generating nodes inside cell $\hat{c}_i$. For any two events $\mathcal{A}$ and $\mathcal{B}$, we know that $P(\mathcal{B}) = P(\mathcal{B}|\mathcal{A})P(\mathcal{A}) + P(\mathcal{B}|\mathcal{A}^c)P(\mathcal{A}^c) \leq P(\mathcal{A}) + P(\mathcal{B}|\mathcal{A}^c)$. Letting $\mathcal{A}$ denote the event $\{d_{ie} \leq r(n)\}$ and $\mathcal{B}$ denote the event $\{\mathcal{S}_e^{near} > \gamma\}$,

$$P(\mathcal{S}_e^{near} > \gamma) = P(d_{ie} \leq r(n)) + P\left(\mathcal{S}_e^{near} > \gamma | d_{ie} > r(n)\right)$$

where $r(n)$ is defined in (4). $P(d_{ie} \leq r(n))$ is upper bounded as

$$P(d_{ie} \leq r(n)) \leq \frac{\pi r^2(n)}{c^2(n)} = \frac{\ln\left(\frac{f(n)}{4}\right)}{2^{3+5\alpha/2}\gamma f(n)}$$

Thus,

$$P(\mathcal{S}_e^{near} > \gamma) \leq \frac{\ln\left(\frac{f(n)}{4}\right)}{2^{3+5\alpha/2}\gamma f(n)} + P\left(\mathcal{S}_e^{near} > \gamma | d_{ie} > r(n)\right) \tag{8}$$

We observe that when $d_{ie} > r(n)$, it follows that $d_{ke} < 2d_{ie}, \forall k \in \mathcal{R}^{(i)}$. Thus, conditioned on $d_{ie} > r(n)$,

$$\mathcal{S}_e^{near} \leq \frac{|h_{ie}|^2 2^{\alpha}}{\sum_{k\in\mathcal{R}^{(i)}}|h_{ke}|^2} \tag{9}$$

We now derive a lower bound for the sum $\sum_{k\in\mathcal{R}^{(i)}}|h_{ke}|^2$. Recall from Section 3.3.1 that the noise-generating nodes inside cell $\hat{c}_i$ are located within a distance of $r(n)$ from node i. Further, the actual number of noise-generating nodes depends on node i's location. In the worst-case, i could be located at one of the corners of $\hat{c}_i$, yielding the smallest number of noise-generating nodes (in expectation). Clearly, $P\left(|\mathcal{R}^{(i)}| > a\right) > P(N > a)\ \forall a$, where $N \sim \text{Poisson}(\pi r^2(n)/4)$.

Similar to the analysis in Section 3.3.2, we can show using Chernoff bounds that

$$\sum_{k\in\mathcal{R}^{(i)}}|h_{ke}|^2 \geq \frac{\pi r^2(n)}{16} = \ln\left(\frac{f(n)}{4}\right)^{\nu_1} \tag{10}$$

with probability at least

$$1 - \left(\frac{4}{f(n)}\right)^{\nu_2} - \left(\frac{4}{f(n)}\right)^{\nu_3}$$

where $\nu_1 = 1/(2^{7+5\alpha/2}\gamma)$, $\nu_2 = 4\nu_1\ln(e/2)$ and $\nu_3 = 2\nu_1\ln(2/\sqrt{e})$. It is easy to see that this probability goes to 1 as $n \to \infty$. From (9) and (10), we conclude that

$$P\left(\mathcal{S}_e^{near} > \gamma | d_{ie} > r(n)\right) \leq \left(\frac{4}{f(n)}\right)^{\nu_4}$$

where $\nu_4 = 1/(2^{7+7\alpha/2})$. Substituting into (8) yields

$$P\left(\mathcal{S}_e^{near} > \gamma\right) \leq \frac{\ln\left(\frac{f(n)}{4}\right)^{16\nu_1}}{f(n)} + \left(\frac{4}{f(n)}\right)^{\nu_4}$$

Noting that $16\nu_1 < 1$, we can upper bound the right hand side of the above as

$$\begin{aligned} P\left(\mathcal{S}_e^{near} > \gamma\right) &\leq \frac{\ln\left(\frac{f(n)}{4}\right)^{16\nu_1}}{f(n)^{16\nu_1}f(n)^{1-16\nu_1}} + \left(\frac{4}{f(n)}\right)^{\nu_4} \\ &\leq \frac{1}{f(n)^{1-16\nu_1}} + \left(\frac{4}{f(n)}\right)^{\nu_4} \end{aligned}$$

Noting that $1 - 16\nu_1 > \nu_4$ is satisfied for all $\gamma > 1$, we conclude that

$$P\left(\mathcal{S}_e^{near} > \gamma\right) \leq \left(\frac{5}{f(n)}\right)^{\nu_4} \tag{11}$$

We now proceed to analyze case **C2**. We observe that excluding the 8 nearest transmissions from e, the next 16 transmitters are located at Euclidean distance at least $2dc(n)$, the next 32 transmitters at Euclidean distance at least $4dc(n)$ and so on. Thus, relative to e the transmitters are placed along boundaries of concentric squares of increasing size, such that the transmitters on the boundary of the t-th ($t > 1$) square have distance at least $2(t-1)dc(n)$ from e.

Hence, the receive SINR at e due to a transmission from a node i located on the boundary of the t-th concentric square ($t > 1$) is upper bounded as

$$\mathcal{S}_e^{(t)} \leq \frac{|h_{ie}|^2/(2(t-1)dc(n))^{\alpha}}{\sum_{k\in\mathcal{R}}|h_{ke}|^2/d_{ke}^{\alpha}}$$

Noting that there is at least one transmitting cell $\hat{c}_j$ within Euclidean distance at most $2\sqrt{2}dc(n)$ from e and letting $\mathcal{R}^{(j)}$ denote the noise generating nodes inside $\hat{c}_j$, we get

$$\begin{aligned} \mathcal{S}_e^{(t)} &\leq \frac{|h_{ie}|^2/(2(t-1)dc(n))^{\alpha}}{\sum_{k\in\mathcal{R}^{(j)}}|h_{ke}|^2/(2\sqrt{2}dc(n))^{\alpha}} \\ &\leq \frac{|h_{ie}|^2 2^{\alpha}}{(t-1)^{\alpha}\sum_{k\in\mathcal{R}^{(j)}}|h_{ke}|^2} \end{aligned}$$

Once again the sum in the denominator can be bounded by (10) yielding

$$\mathcal{S}_e^{(t)} \leq \frac{|h_{ie}|^2 2^{\alpha}}{(t-1)^{\alpha}\ln\left(\frac{f(n)}{4}\right)^{\nu_1}}, \quad \text{and}$$

$$P\left(\mathcal{S}_e^{(t)} > \gamma\right) \leq \frac{1}{(f(n))^{\nu_4(t-1)^\alpha}} \leq \frac{1}{(f(n))^{\nu_4(t-1)^2}}$$

Hence, the aggregate rate at which e intercepts packets (for each of the phases) is upper bounded (w.h.p) as

$$\begin{aligned}
\Psi_e(n) &\leq 8P\left(\mathcal{S}_e^{near} > \gamma\right) + \sum_{t=1}^{\infty} \frac{8(t+1)}{(f(n))^{\nu_4 t^2}} \leq \frac{8^{\nu_4+1}}{\nu_4 (f(n))^{\nu_4}} \\
&\leq 8\left(\frac{5}{f(n)}\right)^{\nu_4} + \frac{16}{(f(n))^{\nu_4}} + \int_{t=1}^{\infty} \frac{8(t+1)dt}{(f(n))^{\nu_4 t^2}} \\
&\leq 8\left(\frac{5}{f(n)}\right)^{\nu_4} + \frac{16}{(f(n))^{\nu_4}} + \frac{8}{\nu_4 (f(n))^{\nu_4}} \\
&\leq \frac{8^{\nu_4+1}}{\nu_4 (f(n))^{\nu_4}}
\end{aligned}$$

where the second inequality follows from (11) and using integration to bound the sum.

From the weak law of large numbers, we know that the number of eavesdroppers $E(n) \leq (1+\epsilon) n \lambda_e(n),\ \forall \epsilon > 0$ w.h.p. Hence, the combined eavesdropper throughput $\Psi_{\mathbf{E}}(n)$ is upper bounded (w.h.p) as

$$\Psi_{\mathbf{E}}(n) \leq \frac{8(1+\epsilon) n \lambda_e(n)}{\nu_4} \left(\frac{8}{f(n)}\right)^{\nu_4},\ \forall \epsilon > 0 \qquad (12)$$

4.3 Scaling Laws for Allowable Number of Eavesdroppers

We now derive scaling laws for $E(n)$ under various constraints on the total eavesdropper throughput $\Psi_{\mathbf{E}}(n)$.

We first obtain the following theorem that follows immediately from (12).

THEOREM 4.1. *When $\lambda_e(n) = o((f(n))^{\nu_4}/n)$, $\Psi_{\mathbf{E}}(n) = 0$ w.h.p., where $0 < \nu_4 < 1$.*

Theorem 4.1 in turn yields the following relationship that directly captures the trade-off between the per-node throughput $\Psi(n)$ and the allowable number of eavesdroppers $E(n)$.

COROLLARY 4.2. *When $E(n) = \Omega\left(\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)^{2c_1}\right)$, where $c_1 < \nu_4$, it follows that $\Psi_{\mathbf{E}}(n) = 0$ w.h.p.*

We can similarly derive a sufficient condition for $E(n)$ under a more lenient metric than the one considered above and which allows $\Psi_{\mathbf{E}}(n)$ to be bounded by a constant $\mu > 0$. Once again, we obtain the following result directly from (12).

THEOREM 4.3. *When $E(n) \leq \left(\frac{K}{\sqrt{n}\ \Psi(n)}\right)^{2\nu_4}$, it follows that $\Psi_{\mathbf{E}}(n) \leq \mu$ w.h.p., for some constant $\mu > 0$.*

where $K = \left(\nu_4/(1+\epsilon)8^{\nu_4+1}\right)^{1/2\nu_4}$ and $\epsilon > 0$.

Finally, we consider an even more lenient metric than the one above and only restrict $\Psi_{\mathbf{E}}(n)$ to grow more slowly than $\Psi_{\mathbf{S}}(n)$, where $\Psi_{\mathbf{S}}(n) = \sum_i \Psi_i(n)$ denotes the overall network capacity and is equal to $\Omega\left(n \times (nf(n))^{-1/2}\right) = \Omega\left((n/f(n))^{1/2}\right)$.

Once gain, from (12), we get the following result.

THEOREM 4.4. *When $E(n) = \Omega\left(\left(\frac{n^{1/2c_1 - 1/2}}{\Psi(n)^{1-1/2c_1}}\right)^{2c_1}\right)$, it follows that $\Psi_{\mathbf{E}}(n)/\Psi_{\mathbf{S}}(n) = 0$ w.h.p., for some constant $c_1 < \nu_4$.*

4.4 Eavesdroppers With Multiple Antennas

We next allow the eavesdropper e to have more than one receive antenna. In particular, we let each eavesdropper have access to a fixed number of, say q, antennas. Similar to Section 4.2, we define the events $\mathcal{A} = \{d_{ie} \leq r(n)\}$ and $\mathcal{B} = \{S_E^{near} > \gamma\}$. Then,

$$\begin{aligned}
P(\mathcal{B}) &\leq P(\mathcal{A}) + P(\mathcal{B}|\mathcal{A}^c) \\
&\leq \frac{1}{(f(n))^{\nu_4}} + P\left(\mathcal{B}|\mathcal{A}^c\right)
\end{aligned}$$

Similar to (11) in Section 4.2, we obtain by conditioning on $\mathcal{A}^c$ that

$$\mathcal{S}_e^{near} \leq \frac{\sum_{l=1}^{q} |h_{il}|^2 2^\alpha}{\ln\left(\frac{f(n)}{4}\right)^{\nu_1}}$$

where $|h_{il}|^2$ denotes the fading gain from node i to the l-th antenna of e. Noting that sum of q iid exponential random variables is a q-stage Erlang random variable and applying Chernoff bounds for the same (see Appendix A.2), we obtain

$$\begin{aligned}
P(\mathcal{B}|\mathcal{A}^c) &\leq \left(\frac{e \ln\left(\frac{f(n)}{4}\right)^{\frac{\nu_1\gamma}{2^\alpha q}}}{(f(n))^{\frac{\nu_1\gamma}{2^\alpha q}}}\right)^q \\
&\leq \frac{e^q}{(f(n))^{\nu_5}}
\end{aligned}$$

where $\nu_5 = \nu_1\gamma/2^{\alpha+1}$ and the second inequality follows from the fact [11] that

$$\frac{\ln x}{x} \leq \frac{1}{\sqrt{x}},\quad \forall x > 0$$

Hence,

$$\begin{aligned}
P(S_E^{near} > \gamma) &\leq \frac{1}{(f(n))^{\nu_4}} + \frac{e^q}{(f(n))^{\nu_5}} \\
&\leq \frac{e^q + 1}{(f(n))^{\nu_5}}
\end{aligned}$$

Once again, the analysis in Section 4.2 can be trivially extended to show that, for $t > 1$

$$\mathcal{S}_e^{(t)} \leq \frac{\sum_{l=1}^{q} |h_{il}|^2 2^\alpha}{(t-1)^\alpha \ln\left(\frac{f(n)}{4}\right)^{\nu_1}}$$

Therefore,

$$P\left(\mathcal{S}_e^{(t)} > \gamma\right) \leq \frac{1}{(f(n))^{\nu_5(t-1)^\alpha}} \leq \frac{1}{(f(n))^{\nu_5(t-1)^2}}$$

and

$$\Psi_e(n) \leq \frac{8(e^q+4)}{\nu_5 (f(n))^{\nu_5}}$$

Therefore the combined eavesdropper throughput $\Psi_{\mathbf{E}}(n)$ is upper bounded (w.h.p) as:

$$\Psi_{\mathbf{E}}(n) \leq \frac{8(1+\epsilon)\lambda_e(n)(e^q+4)}{\nu_5 (f(n))^{\nu_5}},\quad \forall \epsilon > 0$$

From the above expression, it is adequately clear that apart from a change in constants, the scaling laws derived in Section 4.3 trivially extend to the case when nodes have q antennas.

4.5 Lower Bound on Eavesdropper Throughput

So far, we focused on deriving conditions for $E(n)$ that guarantee the secrecy of the system as per the various secrecy metrics considered. We next derive conditions on $E(n)$ that is sufficient to "break" the secrecy of the system.

In particular, we obtain sufficient conditions for $E(n)$ such that:

$$\lim_{n\to\infty} P(\Psi_{\mathbf{E}}(n) = \mu) = 1$$

for some constant $\mu > 0$.

Once again, we will see that $\Psi_{\mathbf{E}}(n)$ is independent of d and hence the phase of operation. Notice that regardless of e's position, at every time slot there exists at least one transmitting node, i, such that $d_{ie} \leq 2\sqrt{2}dc(n)$. A lower bound for $\Psi_{\mathbf{E}}(n)$ immediately follows from a lower bound on the probability that e decodes i's transmission i.e $P(\mathcal{S}_e > \gamma)$, where

$$\mathcal{S}_j = \frac{P_n(d)|h_{ij}|^2/d_{ij}^{\alpha}}{N_0 + P_n(d)I_{near} + P_n(d)I_{far}} \tag{13}$$

where

$$\begin{aligned} I_{near} &= \sum_{R_k\in\mathcal{R}^{(d)}} \frac{|h_{kj}|^2}{d_{kj}^{\alpha}} \\ I_{far} &= \sum_{R_k\in\mathcal{R}} \frac{|h_{kj}|^2}{d_{kj}^{\alpha}} \end{aligned}$$

$\mathcal{R}^{(d)}$ and $\mathcal{R}$ denote the set of noise-generating nodes at Euclidean distance at most $2\sqrt{2}dc(n)$ and the rest of the network respectively.

Letting $\mathcal{A}$ denote the event $\left\{d_{j,e} > 2r(n),\ \forall j \in \mathcal{T}^{(d)}\right\}$, where $r(n)$ is defined in (4) and $\mathcal{T}^{(d)}$ denotes the set of all the transmitting nodes j such that $d_{je} \leq 2\sqrt{2}dc(n)$, we can write

$$P(\mathcal{S}_e > \gamma) \geq P(\mathcal{S}_e > \gamma|\mathcal{A})P(\mathcal{A}) \tag{14}$$

We thus consider only the event when e is sufficiently far away from each of the "near transmitters". We thus avoid having to derive an upper bound on the interference at e, when e is very close to any of the transmitting (and hence, to the noise-generating) nodes, by assuming outage (i.e. $\mathcal{S}_e < \gamma$), when $\mathcal{A}^c$ is true.

Noting that $|\mathcal{T}| \leq 8$ and applying the union bound, we get

$$P(\mathcal{A}) \geq 1 - 8\frac{4\pi r^2(n)}{c(n)^2} = 1 - \frac{\ln\left(\frac{f(n)}{4}\right)}{2^{5\alpha/2-2}f(n)} > \frac{7}{8} \tag{15}$$

We next derive $P(\mathcal{S}_j > \gamma|\mathcal{A})$ by obtaining a lower bound on $\mathcal{S}_j$ under the condition that the event $\mathcal{A}$ holds. When $\mathcal{A}$ holds, it is easy to see that $d_{kj} > d_{ij}/2,\ \forall R \in \mathcal{R}^{(d)}$. Hence,

$$I_{near} \leq \frac{2^{\alpha+3}}{d_{ij}^{\alpha}} \sum_{R_k\in\mathcal{R}^{(d)}} |h_{kj}|^2$$

Similar to the analysis in Section 4.2, we can show that the sum

$$\sum_{R_k\in\mathcal{R}^{(d)}} |h_{kj}|^2 \leq 32\pi r^2(n) = \ln\left(\frac{f(n)}{4}\right)^{\nu_6}$$

with probability at least

$$1 - \left(\frac{4}{f(n)}\right)^{\nu_7} - \left(\frac{4}{f(n)}\right)^{\nu_8}$$

where $\nu_6 = 1/(2^{5\alpha/2-2}\gamma)$, $\nu_7 = (\nu_6\ln(4/e))/4$ and $\nu_8 = (\nu_6\ln(e/2))/2$. Therefore,

$$I_{near} \leq \frac{2^{\alpha+3}}{d_{ij}^{\alpha}} \ln\left(\frac{f(n)}{4}\right)^{\nu_6} \tag{16}$$

We next derive an upper bound on I_{far}. Once again, we observe that relative to E_j, the transmitting nodes are placed along the boundaries of concentric squares of inreasing size. Let $I_{far}^{(t)}$ denote the interference due to nodes located along the t-th square. Letting $\mathcal{R}^{(t)}$ represent the set of these nodes, we get

$$I_{far}^{(t)} \leq \sum_{R_k\in\mathcal{R}^{(t)}} |h_{kj}|^2/d_{kj}^{\alpha}$$

The transmission scheme described in Section 3.3 ensures that there are at most $8t$ transmitting nodes along the t-th concentric square, each of which is at a distance at least $(t-1)dc(n)$ from E_j. Applying Chernoff bounds, we obtain

$$I_{far}^{(t)} \leq \frac{32t\pi r^2(n)}{((t-1)dc(n))^{\alpha}} = \frac{t\ln\left(\frac{f(n)}{4}\right)^{\nu_6}}{((t-1)dc(n))^{\alpha}}$$

with probability at least

$$1 - \left(\frac{4}{f(n)}\right)^{t\nu_7} - \left(\frac{4}{f(n)}\right)^{t\nu_8}$$

Hence,

$$I_{far} \leq \sum_{t=1}^{\infty} \frac{(t+1)\ln\left(\frac{f(n)}{4}\right)^{\nu_6}}{(tdc(n))^{\alpha}} = \frac{\ln\left(\frac{f(n)}{4}\right)^{\nu_6}\zeta}{(dc(n))^{\alpha}} \tag{17}$$

for some constant ζ. The equality follows from the fact that the sum $\sum_t (t+1)/t^{\alpha}$ converges for $\alpha > 2$.

The upper bound on I_{far} holds with probability at least

$$1 - \sum_{t=1}^{\infty}\left(\left(\frac{4}{f(n)}\right)^{t\nu_7} + \left(\frac{4}{f(n)}\right)^{t\nu_8}\right)$$

Noting that each of the summands above is a geometric series and upon further simplification, it is easy to see that the above probability goes to 1 as $n \to \infty$.

Substituting from (16) and (17) into (13) and further simplification yields:

$$\begin{aligned} \mathcal{S}_j &\geq \frac{|h_{ij}|^2}{\frac{N_0 d_{ij}^{\alpha}}{P_n(d)} + 2^{\alpha+3}\ln\left(\frac{f(n)}{4}\right)^{\nu_6} + \frac{d_{ij}^{\alpha}\ln\left(\frac{f(n)}{4}\right)^{\nu_6}\zeta}{(dc(n))^{\alpha}}} \\ &\geq \frac{|h_{ij}|^2}{N_0(\sqrt{2})^{\alpha} + 2^{\alpha+1}(\zeta+8)\ln\left(\frac{f(n)}{4}\right)^{\nu_6}} \end{aligned}$$

We thus see that the lower bound of $\mathcal{S}_j$ is independent of d. Therefore,

$$P(\mathcal{S}_j > \gamma|\mathcal{A}) \geq e^{-\gamma N_0(\sqrt{2})^{\alpha}}\left(\frac{4}{f(n)}\right)^{\nu_9} \tag{18}$$

where $\nu_9 = (\zeta+8)/2^{3\alpha/2-2}$. Substituting from (18) and (15) into (14), we get

$$P(\mathcal{S}_j > \gamma) \geq \frac{7e^{-\gamma N_0(\sqrt{2})^\alpha}}{8}\left(\frac{4}{f(n)}\right)^{\nu_9}$$

From the above, we immediately obtain the following theorem.

THEOREM 4.5. *When $\lambda_e(n) = O\left((f(n))^{\nu_9}/n\right)$, it follows that $\Psi_{\mathbf{E}}(n) \geq \mu$ w.h.p, for some constant $\mu > 0$.*

In terms of the number of eavesdroppers $E(n)$ and the per-node throughput $\Psi(n)$, it can be easily verified that the above theorem leads to the following result.

COROLLARY 4.6. *When $E(n) = O\left(\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)^{2\nu_9}\right)$, it follows that $\Psi_{\mathbf{E}}(n) \geq \mu$ w.h.p, for some constant $\mu > 0$.*

5. COLLABORATING EAVESDROPPERS

A natural extension of our analysis in Section 4 is to consider the case of collaborating eavesdroppers. In this paper, we consider the special case of a single eavesdropper e with $\Gamma(n)$ antennas and assume that the eavesdropper employs maximum ratio combining [16] to maximize the signal-to-noise ratio at the combiner output, hence ignoring the correlation in the chatter observed across the antennas. The consideration of other receiver approaches and spatially-distributed eavesdroppers are interesting open problems.

5.1 Upper Bound on Combined Eavesdropper Throughput

Consider a transmission by a node i. Let $\mathcal{S}_e$ denote the combined SINR at all eavesdroppers and is expressed thus:

$$\begin{aligned}\mathcal{S}_e &= \sum_{j=1}^{\Gamma(n)} \frac{P_n(d)|h_{i,j}|^2/d_{i,e}^\alpha}{N_0 + P_n(d)\sum_{k\in\mathcal{R}}|h_{k,j}|^2/d_{k,e}^\alpha} \\ &\leq \sum_{j=1}^{\Gamma(n)} \frac{|h_{i,j}|^2/d_{i,e}^\alpha}{\sum_{k\in\mathcal{R}^{(d)}}|h_{k,j}|^2/d_{k,e}^\alpha}\end{aligned}$$

where $|h_{i,j}|^2$ denotes the fading gain from i to the j-th antenna of eavesdropper e and $\mathcal{R}^{(d)}$ denotes the set of noise-generating nodes at a distance at most $2\sqrt{2}dc(n)$.

Proceeding exactly in Section 4.2, we *uniformly* bound the total interference at each of the $\Gamma(n)$ antennas of eavesdropper e. More formally, from (10) and the union bound we get

$$\sum_{k\in\mathcal{R}^{(d)}}|h_{ke}|^2 \geq \frac{\pi r^2(n)}{16} = \ln\left(\frac{f(n)}{4}\right)^{\nu_1},\ \forall j = 1,\ldots,\Gamma(n)$$

with probability at least

$$1 - \Gamma(n)\left(\frac{4}{f(n)}\right)^{\nu_2} - \Gamma(n)\left(\frac{4}{f(n)}\right)^{\nu_3}$$

$$P(\mathcal{S}_e^{near} > \gamma) \leq \frac{1}{(f(n))^{\nu_4}} + P\left(\frac{\sum_{j=1}^{\Gamma(n)}|h_{i,j}|^2 2^\alpha}{\ln\left(\frac{f(n)}{4}\right)^{k_1}} > \gamma\right)$$

Applying Markov Inequality to bound the probability on the right hand side, we get

$$P(\mathcal{S}_e^{near} > \gamma) \leq \frac{1}{(f(n))^{\nu_4}} + \frac{\Gamma(n)}{\ln\left(\frac{f(n)}{4}\right)^{\nu_4}} \simeq \frac{\Gamma(n)}{\ln\left(\frac{f(n)}{4}\right)^{\nu_4}}$$

Similarly, we can show that

$$P\left(\mathcal{S}_e^{(t)} > \gamma\right) \leq \frac{\Gamma(n)}{\ln\left(\frac{f(n)}{4}\right)^{\nu_4(t-1)^\alpha}}$$

Similar to our analyses in Section 4, we note that the upper bounds on the probability that e decodes a message is independent of the phase of operation. Hence, the aggregate rate at which e intercepts packets (for each of the phases) is upper bounded (w.h.p) as

$$\begin{aligned}\Psi_e(n) &\leq 8P\left(\mathcal{S}_e^{near} > \gamma\right) + \sum_{t=1}^{\infty} 8(t+1)P\left(\mathcal{S}_e^{(t+1)} > \gamma\right) \\ &\leq \frac{24\Gamma(n)}{\ln\left(\frac{f(n)}{4}\right)^{\nu_4}} + \frac{8\Gamma(n)}{\nu_4\ln\left(\frac{f(n)}{4}\right)^{\nu_4}} \\ &\leq \frac{32\Gamma(n)}{\nu_4\ln\left(\frac{f(n)}{4}\right)^{\nu_4}}\end{aligned}$$

5.1.1 Scaling Laws For Allowable Number of Antennas

Based on the analysis in Section 5.1, we can easily derive the following scaling laws for $\Gamma(n)$.

THEOREM 5.1. *When $\Gamma(n) = \Omega\left((\ln f(n))^{1-\epsilon}\right)$, $\forall\epsilon > 0$, it follows that $\Psi_{\mathbf{E}}(n) = 0$ w.h.p.*

In terms of $\Gamma(n)$ and $\Psi(n)$ the above theorem implies the following result

COROLLARY 5.2. *When $\Gamma(n) = \Omega\left(\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)^{1-\epsilon}\right)$, it follows that $\Psi_{\mathbf{E}}(n) = 0$ w.h.p.*

THEOREM 5.3. *When $\Gamma(n) \leq \frac{\nu_4^2\mu}{32}\ln\left(\frac{f(n)}{4}\right)$, it follows that $\lim_{n\to\infty}\Psi_{\mathbf{E}}(n) \leq \mu$ w.h.p, for some constant $\mu > 0$.*

In terms of $\Gamma(n)$ and $\Psi(n)$, we obtain the following result

COROLLARY 5.4. *When $\Gamma(n) = \frac{\nu_4^2\mu}{32}\left(\ln\left(\frac{1}{4\sqrt{n}\ \Psi(n)}\right)\right)$, it follows that $\Psi_{\mathbf{E}}(n) = 0$ w.h.p.*

THEOREM 5.5. *When $\Gamma(n) = \Omega\left(\left(\frac{n}{f(n)}\right)^{1/2}\ln f(n)\right)$, it follows that $\frac{\Psi_{\mathbf{E}}(n)}{\Psi_{\mathbf{S}}(n)} = 0$ w.h.p.*

Once again, in terms of $\Gamma(n)$ and $\Psi(n)$, the above theorem implies the following result.

COROLLARY 5.6. *When $\Gamma(n) = \Omega\left(\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)^{1-\epsilon} n\Psi(n)\right)$, it follows that $\frac{\Psi_{\mathbf{E}}(n)}{\Psi_{\mathbf{S}}(n)} = 0$ w.h.p.*

5.2 Lower Bound on Eavesdropper Throughput

Similar to Section 4.5, we again derive sufficient conditions on $\Gamma(n)$ to achieve a desired eavesdropper throughput. Once again, we know that at every time slot there is a transmitting node i within a distance of $\sqrt{2}dc(n)$ from e. Rewriting (13) for the case of an eavesdropper with $\Gamma(n)$ antennas, we get

$$\mathcal{S}_e = \sum_{j=1}^{\Gamma(n)} \frac{P_n(d)|h_{i,j}|^2/d_{i,e}^{\alpha}}{N_0 + P_n(d)\sum\limits_{k\in\mathcal{R}^{(d)}} \frac{|h_{k,j}|^2}{d_{k,e}^{\alpha}} + P_n(d)\sum\limits_{k\in\mathcal{R}} \frac{|h_{k,j}|^2}{d_{k,e}^{\alpha}}}$$

where $\mathcal{R}^{(d)}$ and $\mathcal{R}$ denote the interference from noise-generating nodes at Euclidean distance at most $2\sqrt{2}dc(n)$ and the rest of the network respectively.

Once again from (16) and the union bound, we uniformly bound the near interference for all antennas j thus

$$\sum_{k\in\mathcal{R}^{(d)}} |h_{k,j}|^2/d_{k,e}^{\alpha} \leq \ln\left(\frac{f(n)}{4}\right)^{\nu_6}, \forall j = 1,\ldots,\Gamma(n)$$

with probability at least

$$1 - \Gamma(n)\left(\frac{4}{f(n)}\right)^{\nu_7} - \left(\frac{4}{f(n)}\right)^{\nu_8}$$

Similarly from (17) and the union bound, we uniformly bound the far interference for all antennas j thus

$$\sum_{k\in\mathcal{R}} |h_{k,j}|^2/d_{k,e}^{\alpha} \leq \frac{\ln\left(\frac{f(n)}{4}\right)^{\nu_6}\zeta}{(dc(n))^{\alpha}}$$

with probability at least

$$1 - \Gamma(n)\sum_{t=1}^{\infty}\left(\left(\frac{4}{f(n)}\right)^{t\nu_7} + \left(\frac{4}{f(n)}\right)^{t\nu_8}\right)$$

Notice that the uniform bounds on the near and far interference go to 1, so long as $\Gamma(n) = o(f(n))$.

$$\mathcal{S}_e \geq \frac{\sum_{j=1}^{\Gamma(n)}|h_{i,j}|^2}{\frac{N_0 d_{i,e}^{\alpha}}{P_n(d)} + 2^{\alpha}(\beta+8)\ln\left(\frac{f(n)}{4}\right)^{\nu_5}} \text{ w.h.p}$$

Noting that the numerator is a $\Gamma(n)$-stage Erlang random variable and applying Chernoff bounds for the same, we see that

$$\begin{aligned}\mathcal{S}_e &\geq \frac{\Gamma(n)/2}{\frac{N_0 d_{i,e}^{\alpha}}{P_n(d)} + 2^{\alpha}(\beta+8)\ln\left(\frac{f(n)}{4}\right)^{\nu_5}} \text{ w.h.p} \\ &\geq \frac{\Gamma(n)}{2^{\alpha+2}(\beta+8)\ln\left(\frac{f(n)}{4}\right)^{\nu_5}} \text{ w.h.p}\end{aligned}$$

where the second inequality follows from observing that the first summand in the denominator is smaller than the second. We note that if $S_e > \gamma$ w.h.p is sufficient to enable e to achieve a constant throughput.

We thus conclude from the lower bound for $\mathcal{S}_e$ that

THEOREM 5.7. *When $\Gamma(n) = O(\ln f(n))$, then $\Psi_{\mathbf{E}}(n) = \mu$ w.h.p, for some constant $\mu > 0$.*

In terms of $\Psi(n)$, we can re-write the above theorem as

THEOREM 5.8. *When $\Gamma(n) = O\left(\ln\left(\frac{1}{\sqrt{n}\ \Psi(n)}\right)\right)$, it follows that $\Psi_{\mathbf{E}}(n) = \mu$ w.h.p., for some $\mu > 0$ w.h.p.*

6. DISCUSSION

6.1 Other Eavesdropping Models

Since we assume a powerful eavesdropper in our analysis, it might be tempting to ask if the scaling laws improve under weaker adversarial models, for instance, when an eavesdropper can only intercept transmissions a fixed distance away. From our analysis,we note that the probability of an eavesdropper intercepting a message is dominated by the near transmissions and hence, the results do not change even under this weaker model.

Assuming a jamming eavesdropper will likely not change the results because of only a small number of eavesdroppers relative to the legitimate nodes in the network. We also expect no change in our results when we allow eavesdroppers to jointly decode messages across multiple hops. This can be established when there are at least $\ln n$ nodes per cell, yielding straight line routing paths and causing the message to move farther away from an eavesdropper at each hop. Showing this result in the case of winding paths is an interesting open problem.

6.2 Other Secrecy Metrics

Our analysis begs the question of whether we could achieve improvements in the scaling laws under a less stringent metric than the one considered in this paper. An example includes a metric which constrains $\Psi_{\mathbf{E}}(n)$ to grow more slowly than the aggregate network capacity $\Psi_{\mathbf{S}}(n) = \Omega(n/f(n)^{1/2})$. It is easy to see that under this metric we can improve the allowable number of eavesdroppers by a factor of $\Psi_{\mathbf{S}}(n)$.

6.3 Other Fading Models

Although we assume a Rayleigh fading model in our analysis, it is easy to see that our analysis only requires an exponentially decaying tail for the fading gains, a condition that is also satisfied by the Nakagami and Ricean fading models [15].

6.4 Receive Power vs Transmit Power

The traditional dense network model [5], in which nodes are placed in a disk of unit area, ignores the near-field effects and also allows the transmit power to exceed receive power. Assuming independent fading [15] across links in such a model is not realistic since inter-node distances shrink to 0. In contrast, we keep the the number of nodes per unit area fixed while only increasing the density by growing the transmit power with n. This allows us to ignore near-field effects and also to assume independent fading across links. Further, by noting that distances between directly communicating neighbors grows as $\sqrt{f(n)}$ and the fading gain between them is (a.s.) smaller than $\ln f(n)$ [1][pp.176], it is easy to see that the receive power (a.s.) never exceeds transmit power.

6.5 Achievable Secrecy in Limiting Cases

One natural question that stems from our results is can any secrecy be achieved when operating the network at a per-node throughput of $\Omega(n^{-1/2})$ (i.e. when $f(n) = c^2$, for some constant c). Unfortunately, in this case, we cannot employ w.h.p arguments as done in Sections 4 and 5. We however conjecture that for a large enough choice of the constant c, the scaling laws apply with as large as a probability as desired. This implies that a constant number of

eavesdroppers can be tolerated with a probability as large as desired. At the other extreme, when $f(n) = n$, the network consists of a single cell and the problem reduces to a two-hop setting studied in [17]. While [17] assumes equal path-losses between nodes, we conjecture that an analysis accounting for path-losses yields $\Omega(n^{1-\epsilon})$ allowable independent eavesdroppers.

6.6 Secrecy using Power Control

One concern with the artificial noise-generation is the energy consumption of the legitimate nodes. Indeed, it might seem that the fading gain due to multi-user diversity can be exploited to decrease node transmit power by a factor proportional to the gain, and not employ noise-generation at all. In this case, however, the only interference an eavesdropper experiences is from the transmitting nodes. A straightforward calculation reveals that this interference is smaller than that resulting from our noise-generating algorithm by a factor of $\ln f(n)$. Thus, it indicates that noise-generation is essential to allow a number of eavesdroppers growing with n.

6.7 Secrecy Capacity Based Formulation

Although we have adopted a packet loss/interception approach in this paper, the results are easily extended to guarantee a secrecy rate for each link (and, hence, for each source-destination pair[9]). In particular, conditioned on the fading gains, the effective transmitter-receiver-eavesdropper channel for each link is a Gaussian wiretap channel. Hence, one can select SINR thresholds for the receiver and eavesdropper at which a constant secrecy rate R is obtained. It is then straightforward to show that identical scaling results to what have been demonstrated here can be obtained.

7. CONCLUSIONS

This paper presented the first work studying the scalability of keyless secrecy in a generalized network setting when the eavesdropper locations are unknown. We described a construction allowing nodes to generate artificial noise to overcome eavesdroppers and yet achieving a throughput of $\Omega\left((nf(n))^{-1/2}\right)$ w.h.p., where $\omega(1) \leq f(n) \leq o(n)$. We showed that $\Omega(f(n)^c)$ and $\Omega((\ln f(n))^{1-\epsilon})$ independent and collaborating eavesdroppers can be tolerated while ensuring that the eavesdropper throughput goes to 0. We also derived sufficient conditions on the number of eavesdroppers in order to achieve a non-zero throughput. As ongoing work, we seek to improve the constants in the exponent of scaling laws.

8. REFERENCES

[1] P. Embrechts, C. Kluppelberg, and T. Mikosch. *Modelling extremal events for insurance and finance*. Springer-Verlag, 1997.

[2] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran. Closing the gap in the capacity of wireless networks via percolation theory. *IEEE Transactions on Information Theory*, 53:1009–1018, 2007.

[3] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[4] M. Grossglauser and D. Tse. Mobility increases the capacity of ad hoc wireless networks. *IEEE/ACM Transactions on Networking*, 10(8):477–486, August 2002.

[5] P. Gupta and P. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2):388–404, 2000.

[6] M. Haenggi. The secrecy graph and some of its properties. In *IEEE ISIT*, 2008.

[7] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6:207–212, 1996.

[8] J. Hershey, A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43(1):3–6, 1995.

[9] O. Koyluoglu, C. E. Koksal, and H. E. Gamal. On secrecy capacity scaling in wireless networks. *Under submission*, (eprint arXiv:0908.0898), 2009.

[10] Y. Liang, H. Poor, and L. Ying. Secrecy throughput of manets with malicious nodes. In *International Symposium on Information Theory*, 2009.

[11] D. Mitrinovic and P. Vasic. *Analytic Inequalities*. Springer-Verlag, 1970.

[12] M. Mitzenmacher and E. Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[13] Y. Nebat. A lower bound for the achievable throughput in large wireless networks under fixed multipath fading. In *IEEE SpaSWiN*, 2006.

[14] E. Perron, S. N. Diggavi, and E. Telatar. On cooperative wireless network secrecy. In *IEEE INFOCOM*, 2009.

[15] S. Toumpis. *Capacity and Cross-Layer Design of Wireless Ad Hoc Networks*. PhD thesis, Stanford University, 2003.

[16] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[17] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung. Multi-user diversity for secrecy in wireless networks. In *Information Theory and Applications Workshop*, 2009.

[18] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. Journal*, 54:1355–1387, 1975.

[19] S. Xiao, H. Pishro-Nik, and W. Gong. Dense parity check based secrecy sharing in wireless communications. In *IEEE GLOBECOM*, 2007.

APPENDIX

A. CHERNOFF BOUNDS FOR POISSON AND ERLANG RANDOM VARIABLE

We first state the Chernoff bounds for a Poisson random variable, which are proved in [12][pp.97-98].

THEOREM A.1. *Let X be a Poisson random variable with parameter λ.*

1. *If $x > \lambda$, then $P(X \geq x) \leq e^{-\lambda}(e\lambda)^x/x^x$*
2. *If $x < \lambda$, then $P(X \leq x) \leq e^{-\lambda}(e\lambda)^x/x^x$*

Similarly, we can also obtain Chernoff bounds for an Erlang random variable.

THEOREM A.2. *Let X be an Erlang random variable with mean k and let $\varepsilon > 1$. Then,*

1. $P(X > \varepsilon k) \leq \left(\varepsilon/e^{\varepsilon-1}\right)^k$
2. $P(X < k/\varepsilon) \leq \left(e^{1-\frac{1}{\varepsilon}}/\varepsilon\right)^k$

PROOF. We derive a probability bound on the lower tail of a k-stage Erlang random variable X. Using Chernoff bounds for a non-negative random variable,

$$P(X < a) \leq \inf_{t<0} e^{-ta} M_X(t) \tag{19}$$

where $M_X(t) = E[e^{tX}]$ denotes the moment generating function of the random variable X. For a k-stage Erlang random variable X with rate λ:

$$M_X(t) = \left(\frac{\lambda}{\lambda - t}\right)^k$$

Using elementary calculus, the value of t that minimizes the right hand side of (19) can be obtained as:

$$t^* = \lambda - \frac{n}{a}$$

Therefore,

$$P(X < a) \leq e^{-(a\lambda - n)} \left(\frac{a\lambda}{k}\right)^k$$

Setting $a = E[X]/\varepsilon = k/\varepsilon\lambda$, where $\varepsilon > 1$, yields:

$$P(X < \frac{E[X]}{\varepsilon}) \leq \left(\frac{e^{1-\frac{1}{\varepsilon}}}{\varepsilon}\right)^k$$

Since $e^{1-1/\varepsilon}/\varepsilon < 1 \ \ \forall \varepsilon > 1$, the right hand side in the above inequality goes to 0 as $n \to \infty$.

The probability bound for the upper tail can be derived similarly. In particular, for a non-negative random variable X and $a > 0$, we have

$$P(X > a) \leq \inf_{t>0} e^{-ta} M_X(t)$$

Proceeding exactly in the same manner as before, it can be easily shown that

$$P(X > \varepsilon E[X]) \leq \left(\frac{\varepsilon}{e^{\varepsilon-1}}\right)^k$$

For $\varepsilon > 1$, the right hand side goes to 0 as $k \to \infty$. $\square$