

On Secrecy Capacity Scaling in Wireless Networks

O. Ozan Koyluoglu, *Student Member, IEEE*, C. Emre Koksal, *Member, IEEE*, and Hesham El Gamal, *Fellow, IEEE*

Abstract

This work studies the achievable secure rate per source-destination pair in wireless networks. First, a path loss model is considered, where the legitimate and eavesdropper nodes are assumed to be placed according to Poisson point processes with intensities λ and λ_e , respectively. It is shown that, as long as $\lambda_e/\lambda = o((\log n)^{-2})$, almost all of the nodes achieve a perfectly secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ for the extended and dense network models. Therefore, under these assumptions, securing the network does not entail a loss in the per-node throughput. The achievability argument is based on a novel multi-hop forwarding scheme where randomization is added in every hop to ensure maximal ambiguity at the eavesdropper(s). Secondly, an ergodic fading model with n source-destination pairs and n_e eavesdroppers is considered. Employing the ergodic interference alignment scheme with an appropriate secrecy pre-coding, each user is shown to achieve a constant positive secret rate for sufficiently large n . Remarkably, the scheme does not require eavesdropper CSI (only the statistical knowledge is assumed) and the secure throughput per node increases as we add more legitimate users to the network in this setting. Finally, the effect of eavesdropper collusion on the performance of the proposed schemes is characterized.

I. INTRODUCTION

A. Background

In their seminal work [1] Gupta and Kumar have shown that the randomly located nodes can achieve at most a rate that scales like $\frac{1}{\sqrt{n}}$, as the number of nodes $n \rightarrow \infty$, under an interference-limited channel model. However, the proposed multi-hop scheme of [1] only achieves a scaling of $\frac{1}{\sqrt{n \log n}}$ per node. This gap was recently closed in [2], where the authors proposed a *highway* based multi-hop forwarding protocol that achieves $\frac{1}{\sqrt{n}}$ rate per source-destination pair in random networks. In this approach, a set of connected highways, which span the network both horizontally and vertically, are constructed. Then, each source-destination pair communicates via a time-division strategy, where the source first transmits its message to the closest horizontal highway. Then, the message is transported in multi-hop fashion to the appropriate vertical highway, which carries the message as close to the destination as possible. Finally, the message is delivered to the destination node from the vertical highway. The existence of highways, which satisfy certain desirable properties, is established by borrowing tools from percolation theory. Contrary to this multi-hop approach, a single-hop scheme called as ergodic interference alignment [3] (see also [4], [5]) is recently employed in [6] and, with arbitrary node placement and arbitrary traffic pattern, the unicast and multicast capacity regions of dense networks are characterized (up to a factor of $\log n$) under the Gaussian fading channel model. These line of works assumed an interference-limited channel model, where the interference is considered as noise (the focus of this work as well). Contrary to this model, [7] considered Gaussian fading channel model and proposed hierarchical cooperation schemes that can increase the per-node rate. This approach is further improved in the follow-up works (see, e.g., [8], [9], and references therein).

The broadcast nature of the wireless communication makes it susceptible to eavesdropping. This motivates considering *secrecy* as a quality of service (QoS) constraint that must be accounted for in the network design. State of the art cryptographic approaches can be broadly classified into public-key and private-key protocols. Public-key cryptography assumes that the eavesdropper(s) has limited computational power, whereas the decryption requires a significant complexity without the knowledge of the key [10]. Private-key approaches, on the other hand, assume that a random key is shared in private between the legitimate transmitter and receiver. This key is used to secure the transmitted information from potential eavesdropper(s). One of the earliest examples of private-key cryptography is the Vernam's one time pad scheme [11], where the transmitter sends the XOR of the message bits and key bits. The legitimate receiver can decode the messages by XORing the shared key with the received sequence. In [12], Shannon showed that this scheme achieves perfect secrecy **if and only if** the two nodes share a key of the same length as the message. The scaling laws of wireless networks under the assumption of **pre-distributed** private keys was studied in [13]. However, it is important to note that, the key agreement step of the cryptographic protocols is arguably the most challenging part and this step becomes even more daunting as the network size grows. Our work avoids the aforementioned limitations by adopting an information theoretic framework for secrecy in wireless networks. In particular, we

This work is submitted to the IEEE Transactions on Information Theory.

The authors are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA. Email: {koyluogo, koksal, helgamal}@ece.osu.edu.

This work is partially supported by Los Alamos National Labs (LANL) and by National Science Foundation (NSF).

assume the presence of eavesdropper(s) with **infinite computational power** and characterize the scaling laws of the network secrecy capacity while **relaxing the idealistic assumption of pre-distributed keys**.

The notion of information theoretic secrecy was introduced by Shannon to study secure communication over point-to-point noiseless channels [12]. This line of work was later extended by Wyner [14] to noisy channels. Wyner's degraded wiretap channel assumes that the eavesdropper channel is a degraded version of the one seen by the legitimate receiver. Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper, in terms the lower noise level, can be exploited to transmit secret bits using random binning codes. This *keyless secrecy* result was then extended to a more general (broadcast) model in [15] and to the Gaussian setting in [16]. Recently, there has been a renewed interest in wireless physical layer security (see, e.g., Special Issue on Information Theoretic Security, *IEEE Trans. Inf. Theory*, June 2008 and references therein). The secrecy in stochastic networks is studied in [17], where it is shown that even a small density of eavesdroppers has a drastic impact on the connectivity of the secrecy graph. Connectivity in stochastic networks with secrecy constraints is also studied in [18], [19], where the node degree distribution is analyzed. However, according to the best of our knowledge, information theoretical analysis of secrecy capacity scaling in large wireless networks has not been studied in the literature before.

B. Contributions

This paper considers wireless networks with secrecy constraints. We study two different channel models: 1) Static path loss model, and 2) ergodic fading model. For the first model, we consider a stochastic node placement on a square region, where the legitimate nodes and eavesdroppers are distributed according to Poisson point processes with intensity λ and λ_e , respectively. (For extended networks, the area of the region is n and $\lambda = 1$; and, for dense networks, area of the region is 1 and $\lambda = n$.) The path loss is modeled with a power loss exponent of $\alpha > 2$. This model suits for the scenarios where the channel gains are mostly determined by path losses. In the second model, n source-destination pairs and n_e eavesdroppers are considered, where the gain of each link is assumed to follow some fading process. (The assumptions on the fading processes will be clear in the next section. Here, we note that our model includes a large set of fading distributions.) Arguably, this model suits for (dense) networks in which the inter node distances have a negligible effect on the channel gains compared to that of the underlying fading processes.

The results of this work can be summarized as follows.

1) For the path loss model, we construct a "highway backbone" similar to [2]. However, in addition to the interference constraint considered in [2], our backbone construction and multi-hop forwarding strategy are designed to ensure secrecy. More specifically, an edge can be used in the highway if and only if there is a legitimate node within the corresponding square of the edge and if there is no eavesdropper within a certain *secrecy zone* around the node. We show that the network still percolates in this *dependent* edge model, and many highway paths can be constructed. Here, in addition to the careful choice of the secrecy zone, our novel multi-hop strategy, which enforces the usage of an *independent randomization* at each hop, allows the legitimate nodes to create an advantage over the eavesdroppers, which is, then, exploited to transmit secure bits over the highways. This way, we show that, as long as $\lambda_e/\lambda = o((\log n)^{-2})$, almost all source-destination pairs achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ with high probability, implying that the secrecy constraint does not entail a loss in the per-node throughput (in terms of the scaling). (Note that $\lambda = 1$ for extended networks and $\lambda = n$ for dense networks.) In these scenarios, the proposed scheme, which uses independent randomization at the transmitter of each hop, is the crucial step to obtain the results.

2) For the ergodic fading model, employing the ergodic interference alignment scheme ([3], [4], [5]) with an appropriate secrecy pre-coding we show that each user can achieve secrecy. Here, the secrecy rate per user is shown to be positive for most of the relevant fading distributions. In particular, in the high SNR regime, the proposed scheme allows each user to achieve a secure degrees of freedom of $\eta = [\frac{1}{2} - \frac{1}{n}]^+$ even with the absence of eavesdropper CSI. We observe that, per node performance of users *increase* as we add more legitimate users in the network for this scenario compared to the result obtained for the path loss model.

3) Finally, we focus on the eavesdropper collusion, where the eavesdroppers are assumed to share their observations freely. For the extended networks with the path loss model, the same scaling result is shown to hold for the colluding eavesdropper scenario when $\lambda_e = O((\log n)^{-2(1+p)})$ for any $p > 0$. For the ergodic fading model, extensions to many eavesdropper collusion scenarios are discussed. In the extreme case, where all the eavesdroppers collude, it is shown that the proposed scheme allows each user to achieve a secure degrees of freedom of $\eta = [\frac{1}{2} - \frac{n_e}{n}]^+$. We note that, for the path loss model under the stated assumptions, the eavesdropper collusion does not affect the performance of our multi-hop scheme (in terms of scaling). On the contrary, for the ergodic fading model, the eavesdropper collusion has a clear effect on the achievable performance of our ergodic interference alignment scheme.

C. Organization

The rest of this paper is organized as follows. Section II introduces the two network models (path loss and ergodic fading models). In Section III, we consider the path loss model and develop our novel multi-hop secret encoding scheme. Section IV

focuses on the ergodic fading scenario and proposes ergodic interference alignment scheme for security applications. In Section V, we focus on the colluding eavesdropper scenarios. Concluding remarks are given in Section VI, and, to enhance the flow of the paper, some of technical lemmas and proofs are relegated to the Appendix.

II. NETWORK MODELS

The set of legitimate nodes is denoted by \mathcal{L} , whereas the set of eavesdroppers is represented by \mathcal{E} . During time slot t , the set of transmitting nodes are denoted by $\mathcal{T}(t) \subset \mathcal{L}$, where each transmitting user $i \in \mathcal{T}(t)$ transmits the signal $X_i(t)$. The received signals at receiving node $j \in \mathcal{L} - \mathcal{T}(t)$ and at eavesdropper $e \in \mathcal{E}$ are denoted by $Y_j(t)$ and $Y_e(t)$, respectively:

$$Y_j(t) = \sum_{i \in \mathcal{T}(t)} h_{i,j}(t)X_i(t) + Z_j(t) \quad (1)$$

$$Y_e(t) = \sum_{i \in \mathcal{T}(t)} h_{i,e}(t)X_i(t) + Z_e(t), \quad (2)$$

where receivers are impaired by zero-mean circularly symmetric complex Gaussian noises with variance N_0 . We denote this distribution by $\mathcal{CN}(0, N_0)$. Assuming that each transmitter is active over N channel uses, the average power constraint on channel inputs at each transmitter is given by $\frac{1}{N} \sum_{t=1}^N |X_i(t)|^2 \leq P$. Note that, for i.i.d. $\mathcal{CN}(0, P)$ input distribution, $\text{SNR} \triangleq \frac{P}{N_0}$ is the signal-to-noise ratio per complex symbol.

A. Static Path Loss Model with Stochastic Node Distribution

In the path loss model we consider, the signal power decays with the distance d as $d^{-\alpha}$ for some $\alpha > 2$; and the distance between node i and node j is denoted by $d_{i,j}$. The path loss is modeled in (1) and (2) with

$$h_{i,j}(t) = \sqrt{d_{i,j}^{-\alpha}}, \quad h_{i,e}(t) = \sqrt{d_{i,e}^{-\alpha}}. \quad (3)$$

The set of all observations at eavesdropper e is denoted by $\mathbf{Y}_e \triangleq \{Y_e(t), \forall t\}$.

The extended network model is a square of side-length \sqrt{n} (the area of the region is n). The legitimate nodes and eavesdroppers are assumed to be placed randomly according to Poisson point processes of intensity $\lambda = 1$ and λ_e , respectively. The transmitters are assumed to know *a-priori* whether there is any eavesdropper within some neighborhood or not (the size of the neighborhood will be clear in later parts of the text). We are aware of the idealistic nature of this assumption, but believe that it allows for extracting valuable insights in the problem. To analyze the worst case scenario from a security perspective, the legitimate receivers are assumed to consider interference as noise, whereas no such assumption is made on the eavesdroppers, all of which are assumed to be informed with the network topology perfectly.

Now, consider any random source-destination pair, where the source s wishes to transmit the message $W_{s,d}$ securely to the intended destination d . In our multi-hop strategy, each transmission consists of N channel uses per hop. We say that the secret rate of R is achievable for almost all the source-destination pairs (s, d) , if

- The error probability of decoding the intended message at the intended receiver can be made arbitrarily small as $N \rightarrow \infty$, and
- The information leakage rate associated with the transmissions of the message over the entire path, i.e., $\frac{I(W_{s,d}; \mathbf{Y}_e)}{N}$, can be made arbitrarily small $\forall e \in \mathcal{E}$ as $N \rightarrow \infty$,

for almost all (s, d) .

If there are H hops carrying the message $W_{s,d}$, one only needs to consider the associated channel observations at the eavesdropper when evaluating our security constraint. Hence, our second condition is satisfied if $\frac{I(W_{s,d}; \mathbf{Y}_e(1), \dots, \mathbf{Y}_e(H))}{N}$ can be made arbitrarily small for sufficiently large block lengths, where $\mathbf{Y}_e(h)$ denotes the length- N channel output vector at eavesdropper $e \in \mathcal{E}$ during hop h ¹.

To derive our asymptotic scaling results, we use the following probabilistic version of Landau's notation. We say $f(n) = O(g(n))$ w.h.p., if there exists a constant k such that

$$\lim_{n \rightarrow \infty} \Pr \{f(n) \leq kg(n)\} = 1.$$

We also say that $f(n) = \Omega(g(n))$ w.h.p., if w.h.p. $g(n) = O(f(n))$. We denote $f(n) = \Theta(g(n))$, if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. Lastly, we say $f(n) = o(g(n))$, if $\frac{f(n)}{g(n)} \rightarrow 0$, as $n \rightarrow \infty$.

We also analyze a dense networks with the path loss model and stochastic node distribution similar to above, where we assume that the network is deployed on a square region of unit area. In this case, we assume that the legitimate nodes have an intensity of $\lambda = n$.

¹ We note that the length of the observation vector \mathbf{Y}_e regarding message $W_{s,d}$ is NH for H hops and N channel uses per hop. Therefore, to analyze the mutual information leakage rate per channel use one might be tempted to use $\frac{I(W_{s,d}; \mathbf{Y}_e(1), \dots, \mathbf{Y}_e(H))}{NH}$ in the secrecy constraint. However, as H hops carry the same message $W_{s,d}$, the overall information accumulation at the eavesdropper might be large even if $\frac{I(W_{s,d}; \mathbf{Y}_e(1), \dots, \mathbf{Y}_e(H))}{N}$ is made arbitrarily small.

B. Ergodic Fading Model

Fading process for the link from i to k , denoted by $h_{i,k}(t)$, is assumed to be drawn i.i.d. across time according to some ergodic fading process. The ergodic fading is modeled in (1) and (2) with the following two assumptions:

- The channel gains for the legitimate users, $h_{i,j}$, are assumed to be drawn from independent distributions (for each $i, j \in \mathcal{K}$) that are symmetric around zero (that is $\Pr\{h_{i,j} = h\} = \Pr\{h_{i,j} = -h\}$); and
- The fading process for eavesdropper $e \in \mathcal{E}$, i.e., $h_{i,e}$, is assumed to be drawn independently from the same distribution $\forall i \in \mathcal{K}$.

Note that, as we assume a certain distribution for any given transmitter-receiver pair, the location of the nodes are not relevant in this model. In addition, the second assumption on the fading processes ensures that each eavesdropper has statistically the same channel to each transmitter.

We denote $\mathbf{Y}_e \triangleq \{Y_e(1), \dots, Y_e(N)\}$, $\mathbf{H}(t) \triangleq \{h_{i,j}(t), \forall i, j \in \mathcal{K}\}$, $\mathbf{H} \triangleq \{\mathbf{H}(1), \dots, \mathbf{H}(N)\}$, $\mathbf{H}_e(t) \triangleq \{h_{i,e}(t), \forall i \in \mathcal{K}, \forall e \in \mathcal{E}\}$, and $\mathbf{H}_e \triangleq \{\mathbf{H}_e(1), \dots, \mathbf{H}_e(N)\}$. Here, \mathbf{H} is assumed to be known at legitimate users, whereas eavesdroppers are assumed to know both \mathbf{H} and \mathbf{H}_e .

We assume that each transmitter in the network has an arbitrary and distinct receiver and the set of legitimate nodes, i.e., \mathcal{L} , consists of n source-destination pairs. For notational convenience, we enumerate each transmitter-receiver pair using an element of $\mathcal{K} = \{1, \dots, n\}$, and denote the channel gain process associated with transmitter-receiver pair i with $h_{i,i}(t)$. In this model, transmitter-receiver pair $i \in \mathcal{K}$ tries to communicate a secret message $W_i \in \mathcal{W}_i$. Denoting the decoding error at the receiver by $P_{e,i}$, we say that the secret rate R_i is achievable, if for any $\epsilon > 0$, 1) $|\mathcal{W}_i| \geq 2^{NR_i}$, 2) $P_{e,i} \leq \epsilon$, and 3) $\frac{1}{N}I(W_i; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \leq \epsilon$, $\forall e \in \mathcal{E}$, for sufficiently large N . We finally say that the symmetric secure degrees of freedom (DoF) (per orthogonal dimension) of η is achievable, if the rate R_i is achievable for pair $i \in \mathcal{K}$ and

$$\eta \leq \lim_{\text{SNR} \rightarrow \infty} \frac{R_i}{\log(\text{SNR})}, \forall i \in \mathcal{K}. \quad (4)$$

III. THE PATH LOSS MODEL

In this section, we first focus on extended networks with a path loss model ($\alpha > 2$) and stochastic node distribution (Poisson point processes) as detailed in Section II-A. Our achievability argument is divided into the following four key steps:

- 1) Lemma 1 uses the idea of **secrecy zone** to guarantee the secrecy of the communication over a single hop.
- 2) In Lemma 2, we introduce our novel multi-hop forwarding strategy which uses independent randomization signal in each hop. This strategy is shown to allow for hiding the information from an eavesdropper which listens to the transmissions over **all** hops.
- 3) Using tools from percolation theory, we show the existence of a sufficient number of horizontal and vertical highways in Lemma 3, and we characterize the rate assigned to each node on the highway in Lemma 4.
- 4) The accessibility of highways for **almost all** the nodes in the networks with the appropriate rates is established in Lemma 5.

Our main result, i.e., Theorem 6, is then proved by combining the aforementioned steps with a multi-hop routing scheme (Fig. 1).

We partition the network area into squares of constant side length c . We further divide the area into larger squares of side $f_t d c$, each of which contains $(f_t d)^2$ small squares. These small squares take turn over a Time-Division-Multiple-Access (TDMA) frame of size $(f_t d)^2$ slots. In each slot, a transmitter within each active small square can transmit to a receiver that is located at most d squares away as illustrated in Fig. 2. On the same figure, we also show the secrecy zone, around a transmitting square, consisting of squares that are at most $f_e d$ squares away. Our first result establishes an achievable **secure** rate per **a single hop**, active over N channel uses, under the assumption of a single eavesdropper on the boundary of the secrecy zone.

Lemma 1 (Secure Rate per Hop): In a communication scenario depicted in Fig. 2, the secure rate, simultaneously achievable between any active transmitter-receiver pair is:

$$R_{TR} = \frac{1}{(f_t d)^2} \left[\log(1 + \underline{\text{SNR}}_{TR}) - \log(1 + \overline{\text{SNR}}_{e^*}) \right], \quad (5)$$

where

$$\underline{\text{SNR}}_{TR} \triangleq \frac{P(d+1)^{-\alpha} c^{-\alpha} (\sqrt{2})^{-\alpha}}{N_o + P 8 (f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha)}, \quad (6)$$

$$S(\alpha) \triangleq \sum_{i=1}^{\infty} i(i-0.5)^{-\alpha}, \quad (7)$$

$$\overline{\text{SNR}}_{e^*} \triangleq \frac{P(f_e)^{-\alpha} d^{-\alpha} c^{-\alpha}}{N_o}, \quad (8)$$

$$f_t \geq \frac{2(d+1)}{d}, \quad (9)$$

and

$$\frac{(d+1)^\alpha(\sqrt{2})^\alpha}{(d)^\alpha} \left[1 + \frac{P}{N_o} 8(f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha) \right] < (f_e)^\alpha. \quad (10)$$

Here, secrecy is guaranteed assuming the presence of an eavesdropper on the boundary of the secrecy zone.

Proof: In Fig. 2, consider that one node per filled square is transmitting. Assuming that there is a transmission from every such square, we denote the interference set seen by our designated legitimate receiver as \mathcal{I} . Since the legitimate receivers simply consider other transmissions as noise in our model, we obtain the following SNR at the legitimate receiver.

$$\text{SNR}_{TR} = \frac{P d_{TR}^{-\alpha}}{N_o + \sum_{i \in \mathcal{I}} P d_{iR}^{-\alpha}}, \quad (11)$$

where the distance between the transmitter and receiver is denoted as d_{TR} and that between interferer $i \in \mathcal{I}$ and our receiver is denoted by d_{iR} .

We now consider an eavesdropper $e \in \mathcal{E}$ listening to the transmission and upper bound its received SNR by the following.

$$\text{SNR}_e \leq \frac{P d_{Te}^{-\alpha}}{N_o}, \quad (12)$$

where the distance between the transmitter and the eavesdropper e is denoted by d_{Te} . Here, the upper bound follows by eliminating the interference at the eavesdropper. The construction in Fig. 2 allows for showing that

$$d_{TR} \leq (d+1)c\sqrt{2}, \quad (13)$$

$$d_{Te} \geq f_e d c, \quad (14)$$

and

$$\begin{aligned} \sum_{i \in \mathcal{I}} d_{iR}^{-\alpha} &= \sum_{i=1}^{\infty} 8i(i f_t d - (d+1))^{-\alpha} c^{-\alpha} \\ &\stackrel{(a)}{\leq} 8(f_t d c)^{-\alpha} \sum_{i=1}^{\infty} i(i-0.5)^{-\alpha} \\ &= 8(f_t d c)^{-\alpha} S(\alpha), \end{aligned} \quad (15)$$

where (a) follows by choosing

$$f_t d \geq 2(d+1), \quad (16)$$

and the last equality follows by defining

$$S(\alpha) \triangleq \sum_{i=1}^{\infty} i(i-0.5)^{-\alpha}, \quad (17)$$

which converges to some finite value as $\alpha > 2$.

Using (13), (14), (15) in (11) and (12), we obtain the followings.

$$\text{SNR}_{TR} \geq \underline{\text{SNR}}_{TR} \triangleq \frac{P(d+1)^{-\alpha} c^{-\alpha} (\sqrt{2})^{-\alpha}}{N_o + P 8(f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha)}, \quad (18)$$

and

$$\text{SNR}_e \leq \overline{\text{SNR}}_{e^*} \triangleq \frac{P(f_e)^{-\alpha} d^{-\alpha} c^{-\alpha}}{N_o}. \quad (19)$$

Hence, $\text{SNR}_{TR} > \text{SNR}_e$ for every eavesdropper e , once we choose f_e such that

$$\frac{(d+1)^\alpha(\sqrt{2})^\alpha}{(d)^\alpha} \left[1 + \frac{P}{N_o} 8(f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha) \right] < (f_e)^\alpha. \quad (20)$$

We then construct the secrecy codebook at the transmitter by considering an eavesdropper that observes the signals of the transmission of **this hop only** with an SNR of $\overline{\text{SNR}}_{e^*}$. Based on the Gaussian wiretap channel capacity [16], one can easily show that the following **perfectly secure** rate is achievable

$$R_{TR} = \frac{1}{(f_t d)^2} \left[\log(1 + \underline{\text{SNR}}_{TR}) - \log(1 + \overline{\text{SNR}}_{e^*}) \right], \quad (21)$$

where the $(f_t d)^2$ term is due to time-division described above. ■

Next we introduce our novel multi-hop *randomization* strategy which ensures secrecy over the *entire path*, from a source to a destination node, at *every* eavesdropper observing *all* transmissions.

Lemma 2 (Securing a Multi-Hop Path): Securing each hop from an eavesdropper that is located on the boundary of the secrecy zone is sufficient to ensure secrecy from any eavesdropper which listens the transmissions from all the hops and lie outside the secrecy zones of transmitters of hops.

Proof: We consider a source s , a destination d , and an eavesdropper e in the network. Without loss of generality, we assume that the multi-hop scheme uses H hops to route the message. We design the secrecy codebook at each transmitter according to highest possible eavesdropper SNR assumption for each hop. In our multi-hop routing scenario, each code of the ensemble at the transmitter of hop i generates $2^{N(R_i + R_i^x - \frac{\epsilon_1}{H})}$ codewords each entry with i.i.d. $\mathcal{CN}(0, P)$, for some $\epsilon_1 > 0$, and distributes them into 2^{NR_i} bins. Each codeword is, therefore, represented with the tuple $(w_{s,d}, w_i^x)$, where $w_{s,d}$ is the bin index (secret message) and w_i^x is the codeword index (randomization message). To transmit the message $w_{s,d}$, the encoder of transmitter i will randomly choose a codeword within the bin $w_{s,d}$ according to a uniform distribution. This codeword, i.e., $\mathbf{X}_i(w_{s,d}, w_i^x)$, is sent from transmitter i . It is clear now that each transmitter on the path adds *independent* randomness, i.e., the codeword index w_i^x is independent of w_j^x for $i \neq j$.

We consider an eavesdropper at the boundary of the secrecy zone around the transmitter of the hop i , and denote it by e_i^* . We subtract all the interference seen by this virtual node and denote its observations for hop i as $\mathbf{Y}_{e_i^*}$. Omitting the indices $(w_{s,d}, w_i^x)$, for simplicity, we denote the symbols transmitted from the transmitter i as \mathbf{X}_i ; and set $R_i^x = I(X_i; Y_{e_i^*}) = \log(1 + \overline{\text{SNR}}_{e_i^*})$. (Note that this is the rate loss in (5).) We continue as below.

$$\begin{aligned}
I(W_{s,d}; \mathbf{Y}_e) &= I(W_{s,d}; \mathbf{Y}_e(1), \dots, \mathbf{Y}_e(H)) \\
&\stackrel{(a)}{\leq} I(W_{s,d}; \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}) \\
&= I(W_{s,d}, W_1^x, \dots, W_H^x; \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}) - I(W_1^x, \dots, W_H^x; \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*} | W_{s,d}) \\
&\stackrel{(b)}{\leq} I(\mathbf{X}_1, \dots, \mathbf{X}_H; \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}) - H(W_1^x, \dots, W_H^x | W_{s,d}) + H(W_1^x, \dots, W_H^x | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}, W_{s,d}) \\
&\stackrel{(c)}{=} \sum_{i=1}^H I(\mathbf{X}_1, \dots, \mathbf{X}_H; \mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}) - H(W_1^x, \dots, W_H^x) \\
&\quad + \sum_{i=1}^H H(W_i^x | W_{s,d}, \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}, W_1^x, \dots, W_{i-1}^x) \\
&= \sum_{i=1}^H \left[I(\mathbf{X}_i; \mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}) + I(\mathbf{X}_1, \dots, \mathbf{X}_{i-1}, \mathbf{X}_{i+1}, \dots, \mathbf{X}_H; \mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}, \mathbf{X}_i) \right. \\
&\quad \left. - NR_i^x + N \frac{\epsilon_1}{H} + H(W_i^x | \mathbf{Y}_{e_i^*}, W_{s,d}) \right] \\
&\stackrel{(d)}{\leq} \sum_{i=1}^H \left[H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}) - H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}, \mathbf{X}_i) - NR_i^x + N \frac{\epsilon_1 + \epsilon_2}{H} \right] \\
&\stackrel{(e)}{\leq} \sum_{i=1}^H \left[H(\mathbf{Y}_{e_i^*}) - H(\mathbf{Y}_{e_i^*} | \mathbf{X}_i) - NR_i^x + N \frac{\epsilon_1 + \epsilon_2}{H} \right] \\
&= \sum_{i=1}^H \left[I(\mathbf{X}_i; \mathbf{Y}_{e_i^*}) - NR_i^x + N \frac{\epsilon_1 + \epsilon_2}{H} \right] \\
&\stackrel{(f)}{\leq} \sum_{i=1}^H \left[NI(X_i; Y_{e_i^*}) - NR_i^x + N \frac{\epsilon_1 + \epsilon_2}{H} \right] \\
&= N(\epsilon_1 + \epsilon_2),
\end{aligned}$$

where (a) is due to the fact that $\mathbf{Y}_{e_i^*}$ is an enhanced set of observations compared to that of $\mathbf{Y}_e(i)$, (b) is due to the data processing inequality and the Markov chain $\{W_{s,d}, W_1^x, \dots, W_H^x\} \rightarrow \{\mathbf{X}_1, \dots, \mathbf{X}_H\} \rightarrow \{\mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_H^*}\}$, (c) follows since $W_{s,d}$ and W_i^x are independent, (d) is due to fact that the second term in the sum is zero and due to Fano's inequality (as we choose $R_i^x \leq I(X_i; Y_{e_i^*})$, the binning codebook construction allows for decoding randomization message at the eavesdropper given the bin index for almost all codebooks in the ensemble): We define the decoding error probability as $P_{e, e_i^*} \triangleq \Pr\{\hat{W}_i^x \neq W_i^x\}$, where \hat{W}_i^x is the estimate of the randomization message W_i^x given $(\mathbf{Y}_{e_i^*}, W_{s,d})$, and bound

$$H(W_i^x | \mathbf{Y}_{e_i^*}, W_{s,d}) \leq N \left(\frac{H(P_{e, e_i^*})}{N} + P_{e, e_i^*} R_i^x \right) \leq N \frac{\epsilon_2}{H} \quad (22)$$

with some $\epsilon_2 \rightarrow 0$ as $N \rightarrow \infty$, (e) follows by the fact that conditioning does not increase the entropy and the observation that $H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \dots, \mathbf{Y}_{e_{i-1}^*}, \mathbf{X}_i) = H(\mathbf{Y}_{e_i^*} | \mathbf{X}_i)$, and (f) is due to the fact that $I(\mathbf{X}_i; \mathbf{Y}_{e_i^*}) = \sum_{t=1}^N I(\mathbf{X}_i; Y_{e_i^*}(t) | Y_{e_i^*}(1), \dots, Y_{e_i^*}(t-1))$

$$1)) \leq \sum_{t=1}^N H(Y_{e_i^*}(t)) - H(Y_{e_i^*}(t)|X_i(t)) = NI(X_i; Y_{e_i^*}).$$

After setting, $\epsilon = \epsilon_1 + \epsilon_2$, we obtain our result: For any given $\epsilon > 0$, $\frac{I(W_{s,d}; \mathbf{Y}_e)}{N} < \epsilon$ as $N \rightarrow \infty$. ■

Note that, the number of hops scale as $H = O(\sqrt{n})$ and in (22) we have P_{e_i, e_i^*} decays exponentially in N . Thus, we can say that the multi-hop transmissions require larger block lengths, as n gets large, to assure secrecy with this scheme.

The following result uses tools from percolation theory to establish the existence of a sufficient number of **secure highways** in our network.

Lemma 3 (Secure Highways): There exist a sufficient number of *secure* vertical and horizontal highways such that, as $n \rightarrow \infty$, each secure highway is required to serve $O(\sqrt{n})$ nodes and an entry (exit) point has w.h.p. a distance of at most $\kappa' \log n$ away from each source (respectively, destination) for some finite constant $\kappa' > 0$, if $c \geq c_0$ for some finite constant $c_0 > 0$ and $\lambda_e \rightarrow 0$.

Proof: We first describe the notion of secure highway and the percolation model we use in the proof. We note that most of this percolation based construction is developed in [2], [20] and here we generalize it for secrecy. We say that each square is "open" if the square has at least one legitimate node and there are no eavesdroppers in the secrecy zone around the square. We denote the probability of having at least one legitimate node in a square by p . It is evident that

$$p = 1 - e^{-c^2},$$

and hence, p can be made arbitrarily close to 1 by increasing c . For any given transmitting square, we denote the probability of having an eavesdropper-free secrecy zone by q . The number of eavesdroppers within a secrecy zone is a Poisson random variable with parameter $\lambda_e(2f_e d + 1)^2 c^2$, and hence,

$$q = e^{-\lambda_e(2f_e d + 1)^2 c^2}.$$

Thus, q gets arbitrarily close to 1, as $n \rightarrow \infty$, since $\lambda_e \rightarrow 0$ with n (f_e , d , and c are some finite numbers for the highway construction).

We then map this model to a discrete edge-percolation model (a.k.a. bond percolation on the random square grid [21]) by drawing horizontal and vertical edges over the open squares, where an edge is called open if the corresponding square is open (see Fig. 3). We are interested in characterizing (horizontal and vertical) open paths that span the network area. Such open paths are our *horizontal and vertical highways*. We only focus on horizontal highways for the rest of the section as the results hold, due to symmetry, for the vertical highways. We remark that, in our model, the status of edges are not statistically independent due to the presence of associated secrecy zones that intersect for successive squares. Notice that the status of two edges would be independent if their secrecy zones did not intersect, which happens if there were at least $2f_e d$ squares between two edges. Therefore, this dependent scenario is referred to as finite-dependent model, as f_e and d are some finite numbers. Due to Lemma 12, given in Appendix A, this dependent model *stochastically dominates* an independent model, in which edges are independently open with probability p' , where p' can be made arbitrarily high if pq can be made arbitrarily high. This independent scenario can be constructed by following the steps provided in [22]. Therefore, after proving the percolation of the network with some desirable properties under the independence assumption, the network will also percolate with the same properties under the finite dependence model as both p and q can be made sufficiently large.

Using the independent edge model, applying Lemma 13, given in Appendix A, with edge openness probability of p' , and noting the fact that $m = \frac{\sqrt{n}}{c\sqrt{2}}$ (Fig. 3), we obtain the following: There are w.h.p. $\Omega(\sqrt{n})$ horizontal paths, which, for any given $\kappa > 0$, can be grouped into disjoint sets of $\lceil \delta \log n \rceil$ highways that span a rectangle area of size $(\kappa \log n - \epsilon) \times \sqrt{n}$, for some $\delta > 0$, and some $\epsilon \rightarrow 0$ as $n \rightarrow \infty$ if p' is high enough. Then, the network area is sliced into slabs of side length w , chosen so that the number of slabs match with the number of highways in each rectangle. Then, each source (destination) in the i th horizontal (vertical) slab will access the corresponding highway (Fig. 4). This way, each highway is required to serve at most $2w\sqrt{n}$ nodes and an entry (exit) point has w.h.p. a distance of at most $\kappa' \log n$ away from each source (respectively, destination) for some finite constant $\kappa' > 0$. The former claim follows by an application of Chernoff bound, given in Lemma 14, and union bound (see [2, Lemma 2] or [20, Lemma 5.3.5] for details) and the latter incorporates the negligible horizontal distance (at most $c\sqrt{2}$) in addition to the vertical distance, which scales as $\kappa \log n$. Finally, due to the statistical domination argument given above, these percolation results will also hold for our finite-dependent model, as pq can be made arbitrarily large as $n \rightarrow \infty$. Formally, $\exists c_0 \in (0, \infty)$ such that, for any $c \geq c_0$, pq can be made sufficiently high if $\lambda_e \rightarrow 0$ as $n \rightarrow \infty$. This translates to high enough p' by Lemma 12, which shows that the dependent model has the property given in Lemma 13 as well. ■

With the following lemma we conclude the discussion of highways.

Lemma 4 (Rate per Node on the Highways): Each node on the constructed highways can transmit to their next hop at a constant secure rate. Furthermore, the number of nodes each highway serves is $O(\sqrt{n})$, and therefore each highway can w.h.p. carry a per-node secure throughput of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Proof: The highways are constructed such that there is at least one legitimate node per square and there are no eavesdroppers within the secrecy zone around the squares of the highway. We choose one legitimate node per square as a member of the highway, and compute the rate that can be achieved with the multi-hop strategy. From Lemma 1 (with $d = 1$) and Lemma 2,

one can see that highways can carry data *securely* with a *constant positive rate*. As each highway carries the data for $O(\sqrt{n})$ nodes due to Lemma 3, the achievable rate per node on highways is $\Omega\left(\frac{1}{\sqrt{n}}\right)$. ■

Our final step is to show that almost all the nodes can access the highways simultaneously with high probability with a rate scaling higher than $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Lemma 5 (Access Rate to Highways): Almost all source (destination) nodes can w.h.p. simultaneously transmit (receive) their messages to (from) highways with a secure rate of $\Omega((\log n)^{-3-\alpha})$, if $\lambda_e = o((\log n)^{-2})$.

Proof: To calculate the rate of each node transmitting to the closest horizontal highway, we follow the same procedure given in the proof of Lemma 4. However, this time we choose $d = \kappa'' \log n$ in Lemma 1 for some finite $\kappa'' > 0$, as the nodes within each transmitting squares need to transmit to a receiver at a distance of at most $\kappa'' \log n$ squares away (due to Lemma 3). (Here, we can choose smallest number $\kappa'' \geq \frac{\kappa'}{c}$ making $\kappa'' \log n$ integer.) In addition, compared to Lemma 4, where only one node per square is transmitting, here all legitimate nodes within small squares should access the highways w.h.p., which is accomplished with a TDMA scheme.

As $d = \kappa'' \log n \rightarrow \infty$, we see from (6), (8), (5) that a per-node rate of $\Omega((\log n)^{-2-\alpha})$ is achievable. Note that, to satisfy (10) and thus (5), any choice of $f_e > \sqrt{2}$ suffices as $n \rightarrow \infty$. However, for this case, due to time division between nodes within squares this rate needs to be further modified. Again applying the Chernoff bound (Lemma 14) and the union bound one can show that there are w.h.p. $O(\log n)$ legitimate nodes in each square (see [2, Lemma 1] or [20, Lemma 5.3.4] for details). Therefore, w.h.p. the secure rate $\Omega((\log n)^{-3-\alpha})$ is achievable to the associated highway from a source node, if there is **no eavesdropper** in the associated secrecy zone. Next, we show that this will happen with a very high probability if $\lambda_e = o((\log n)^{-2})$ asymptotically (as $n \rightarrow \infty$).

From Fig. 2, it is clear that the presence of an eavesdropper eliminates the possibility of secure access to a highway from a region of area $A = (2f_e d + 1)^2 c^2$. We denote the total number of eavesdroppers in the network as $|\mathcal{E}|$ (Poisson r.v. with parameter $\lambda_e n$), and the total number of legitimate users in the network as $|\mathcal{L}|$ (Poisson r.v. with parameter $\lambda n = n$). Let the total area in which the eavesdroppers make it impossible to reach a highway be $A_{\mathcal{E}}$. Clearly, $A_{\mathcal{E}} \leq A|\mathcal{E}|$. Let us further denote the number of legitimate users in an area of $A|\mathcal{E}|$ as $|\mathcal{L}_{A|\mathcal{E}}|$. Then, using the Chebyshev inequality (please refer to Lemma 15 in Appendix A), we obtain

$$\begin{aligned} |\mathcal{E}| &\leq (1 + \epsilon)\lambda_e n, \\ |\mathcal{L}| &\geq (1 - \epsilon)n, \\ |\mathcal{L}_{A|\mathcal{E}}| &\leq (1 + \epsilon)A|\mathcal{E}|, \end{aligned} \tag{23}$$

for any $\epsilon \in (0, 1)$ with high probability (as $n \rightarrow \infty$). We denote the fraction of users that can not transmit to highways due to eavesdroppers as F which can be upper bounded by

$$F \leq \frac{|\mathcal{L}_{A|\mathcal{E}}|}{|\mathcal{L}|} \leq \frac{(1 + \epsilon)^2 (2f_e d + 1)^2 c^2 \lambda_e n}{(1 - \epsilon)n} \rightarrow 0 \tag{24}$$

with high probability (as $n \rightarrow \infty$). The first inequality follows since the eavesdroppers can have intersecting secrecy regions, the second inequality follows from (23), and the limit holds as $d = \kappa'' \log(n)$ and $\lambda_e = o((\log n)^{-2})$. This argument shows that almost all of the nodes are connected to the highways as $n \rightarrow \infty$.

Similar conclusion can be made for the final destination nodes: Any given destination node can w.h.p. receive data from the highways securely with a rate of $\Omega((\log n)^{-3-\alpha})$. ■

Now we are ready to state our main result.

Theorem 6: If the legitimate nodes have unit intensity ($\lambda = 1$) and the eavesdroppers have an intensity of $\lambda_e = o((\log n)^{-2})$ in an extended network, almost all of the nodes can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ with high probability.

Proof: In our multi-hop routing scheme, each user has a dedicated route (due to the time division scheme described below) with each hop sending the message to the next hop over N channel uses. The secrecy encoding at each transmitter is designed assuming an eavesdropper on the boundary of the secrecy zone and listening to this hop (observations of length N) only. This way, a transmitter can achieve the rate reported in Lemma 1. Then, we can argue that this secrecy encoding scheme will ensure secrecy from an eavesdropper that listens to the transmissions of every hop due to Lemma 2.

Now, the main result follows by Lemma 4 and Lemma 5 by utilizing a time division approach. That is the total transmission time of the network is divided into four phases, as shown in Fig. 1. During the first phase, the sources that are not affected by eavesdroppers (i.e., almost all of them due to Lemma 5) will w.h.p. transmit their messages to the closest highway entry point. Then, the secret messages of all nodes are carried through the horizontal highways and then the vertical highways (Lemma 4). During the final phase, the messages are delivered from the highways to almost all of the destinations (Lemma 5). Hence, by Lemma 4 and Lemma 5, as the secrecy rate scaling per node is limited by the transmissions on the highway, we can see that almost all of the nodes achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ with high probability. This concludes the proof. ■

Few remarks are now in order.

1) The expected number of legitimate nodes is n , whereas the expected number of eavesdroppers is $n_e = o(n(\log n)^{-2})$ in this extended network. Note that n_e satisfies $n_e = O(n^{1-\epsilon})$ for any $\epsilon > 0$, and hence network can endure eavesdroppers as long as total number of eavesdroppers scale slightly lower than that of legitimate nodes.

2) Utilizing the upper bound of [1] for the capacity of wireless networks, we can see that Theorem 6 establishes the achievability of the same **optimal scaling law** with and without security constraints. It is worth noting that, in our model, the interference is considered as noise at the legitimate receivers. As shown in [7], more sophisticated cooperation strategies achieve the same throughput for the case of extended networks with $\alpha \geq 3$. This leads to the conclusion that cooperation in the sense of [7] does not increase the secrecy capacity when $\alpha \geq 3$ and $\lambda_e = o((\log n)^{-2})$.

3) $\lambda_e = o(1)$ **is tolerable if each node shares key only with the closest highway member**. If each node can share a secret key with *only* the closest highway member, then the proposed scheme can be combined with a one-time pad scheme (see, e.g., [11] and [12]) for accessing the highways, which results in the same scaling performance for any $\lambda_e \rightarrow 0$ as $n \rightarrow \infty$.

4) **Can network endure $\lambda_e = o(1)$ without key sharing?** Note that in our percolation theory result, we have chosen squares of side length c (edge length in the square lattice was $c\sqrt{2}$, see Fig. 3) satisfying $c \geq c_0$ to make pq sufficiently large in order to have $p' > \frac{5}{6}$ for Lemma 13. We remark that for independent percolation with edge probability p' in a random grid, for any $\gamma \in (0, 1)$, $\exists p^*(\gamma)$ such that for $p' > p^*(\gamma)$, the random grid contains a connected component of at least γn^2 vertices (see, e.g., [20, Theorem 3.2.2]). Thus, as long as $\lambda_e = o(1)$, for some $\epsilon', \epsilon^* > 0$, we can choose a very large, but constant, c (to make sure that pq is very close to 1) to have $p' = 1 - \epsilon' > p^*(1 - \epsilon^*)$, which implies that there are w.h.p. $(1 - \epsilon^*)n^2$ connected vertices. Therefore, we conjecture that, for any given $\epsilon > 0$ and for $\lambda_e = o(1)$, per-node secure throughput of $\Omega(1/\sqrt{n})$ is achievable for $(1 - \epsilon)$ fraction of nodes (we conjecture that these are the nodes that have constant distances to highways).

We now focus on the dense network scenario. The stochastic node distribution for this scenario can be modeled by assuming that the legitimate and eavesdropper nodes are distributed as Poisson point processes of intensities $\lambda = n$ and λ_e , respectively, over a square region of unit area. The proposed scheme in the previous section can be utilized for this topology and the same scaling result can be obtained for dense networks as formalized in the following corollary.

Corollary 7: Under the stochastic modeling of node distribution (Poisson point processes) in a dense network (on a unit area region) with the path loss model (with $\alpha > 2$), if the legitimate nodes have an intensity of $\lambda = n$ and the eavesdropper intensity satisfies $\frac{\lambda_e}{\lambda} = o((\log n)^{-2})$, then almost all of the nodes can simultaneously achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Proof: The claim can be proved by following the same steps of the proof of Theorem 6 with scaling the transmit power from P to $\frac{P}{(\sqrt{n})^\alpha}$ at each transmitter, and scaling each distance parameter by dividing with \sqrt{n} . Note that, with these scalings, signal to interference and noise ratio (SINR) calculations and percolation results remain unchanged. ■

IV. THE ERGODIC FADING MODEL

We now focus on the ergodic fading model described in Section II-B and utilize the ergodic interference alignment for secrecy. Frequency selective slow fading channels are studied in [23], where each symbol time $t = 1, \dots, N$ corresponds to F frequency uses and the channel states of each sub-channel remain constant for a block of N' channel uses and i.i.d. among B blocks ($N = N'B$). For such a model, one can obtain the following high SNR result by utilizing the interference alignment scheme [4].

Theorem 8 (Theorem 3 of [23]): For n source-destination pairs with n_e number of external eavesdroppers, a secure DoF of $\eta = \left[\frac{1}{2} - \frac{1}{n}\right]^+$ per frequency-time slot is achievable at each user in the ergodic setting, in the absence of the eavesdropper CSI, for sufficiently high SNR, N , and F .

This interference alignment scheme is shown to achieve a secure DoF of $\left[\frac{1}{2} - \frac{n_e}{n}\right]^+$ per orthogonal dimension at each user when all the eavesdroppers collude [24]. Remarkably, with this scheme, the network is secured against colluding eavesdroppers and only a statistical knowledge of the eavesdropper CSI is needed at the network users. However, the proposed scheme only establishes a high SNR result in terms of secure DoF per user. In addition, the stated DoF gain is achieved in the limit of large number of sub-channels, which is unrealistic in practice for large number of users, n . (The result is achieved when the design parameter m gets large, where $F = \Omega(m^{n^2})$ [23], [24].)

Providing secure transmission guarantees for users at any SNR with finite number of dimensions is of definite interest. In this section, we utilize the ergodic interference alignment scheme [3] to satisfy this quality of service (QoS) requirement at the expense of large coding delays. Ergodic interference alignment can be summarized as follows. Suppose that we can find some time indices in $\{1, \dots, N\}$, represented by t_1, t_2, \dots and their complements $\tilde{t}_1, \tilde{t}_2, \dots$, such that $h_{i,i}(t_m) = h_{i,i}(\tilde{t}_m), \forall i \in \mathcal{K}$, and $h_{i,j}(t_m) = -h_{i,j}(\tilde{t}_m), \forall i, j \in \mathcal{K}$ with $i \neq j$, for $m = 1, 2, \dots, N_1$. Now, consider that we sent the same codeword over the resulting channels, i.e., we set $X_i(t_m) = X_i(\tilde{t}_m), \forall m$. Then, by adding the observations seen by destination i for these two time instance sequences, the effective channel can be represented as

$$\tilde{Y}_i(t_m) = 2h_{i,i}(t_m)X_i(t_m) + Z_i(t_m) + Z_i(\tilde{t}_m), \quad (25)$$

whereas the eavesdropper e observes

$$\tilde{\mathbf{Y}}_e(t_m) = \sum_{i=1}^n \begin{bmatrix} h_{i,e}(t_m) \\ h_{i,e}(\tilde{t}_m) \end{bmatrix} X_i(t_m) + \begin{bmatrix} Z_e(t_m) \\ Z_e(\tilde{t}_m) \end{bmatrix}, \quad (26)$$

for $m = 1, 2, \dots, N_1$. Remarkably, while the interference is canceled for the legitimate users, it still exists for the eavesdropper, whose effective channel becomes multiple access channel with single input multiple output antennas (SIMO-MAC). By taking advantage of this phenomenon together with exploiting the ergodicity of the channel, secure transmission against each eavesdropper is made possible at each user for any SNR (depending on the underlying fading processes) as reported in the following theorem, which is the main result of this section.

Theorem 9: For $t = 1, 2, \dots$, let

$$\tilde{Y}_i(t) \triangleq 2h_{i,i}(t)X_i(t) + Z_i(t) + \tilde{Z}_i(t), \quad (27)$$

$$\tilde{\mathbf{Y}}_e(t) \triangleq \sum_{i=1}^n \tilde{\mathbf{H}}_{i,e}(t)X_i(t) + \tilde{\mathbf{Z}}_e(t), \quad (28)$$

$\tilde{\mathbf{H}}_{i,e}(t) \triangleq [h_{i,e}(t)\tilde{h}_{i,e}(t)]^T$, and $\tilde{\mathbf{Z}}_e(t) \triangleq [Z_e(t)\tilde{Z}_e(t)]^T$, where, $\forall i \in \mathcal{K}$ and $\forall e \in \mathcal{E}$, \tilde{Z}_i and \tilde{Z}_e are i.i.d. as Z_i and Z_e , respectively; and $\tilde{h}_{i,e}$ is i.i.d. as $h_{i,e}$. Then, source destination pair $i \in \mathcal{K}$ can achieve the secret rate

$$R_i = \left[\frac{1}{2}E[I(X_i; \tilde{Y}_i|\mathbf{H})] - \frac{1}{2n}E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] \right]^+, \quad (29)$$

on the average, where the expectations are over underlying fading processes.

Proof: We first need to quantize the channel gains to have a finite set of possible matrices. (These steps are given in [3] and provided here for completeness.) Let $\epsilon' > 0$. Choose $\tau > 0$ such that $\Pr\{\cup_{i,j}\{|h_{i,j}| > \tau\}\} \leq \epsilon'$. This will ensure a finite quantization set. For $\gamma > 0$, the γ -quantization of $h_{i,j}$ is the point among $\gamma(\mathbb{Z} + j\mathbb{Z})$ that is closest to $h_{i,j}$ in Euclidean distance. The γ -quantization of channel gain matrix $\mathbf{H}(t)$ is denoted by $\mathbf{H}_\gamma(t)$, where each entry is γ -quantized. Thus, γ -quantized channel alphabet \mathcal{H}_γ has size satisfying $(\frac{\sqrt{2}\tau}{\gamma})^{2n^2} \leq |\mathcal{H}_\gamma| \leq (\frac{2\tau}{\gamma})^{2n^2}$. We denote each channel type with \mathbf{H}_γ^b , for $b = 1, \dots, B = |\mathcal{H}_\gamma|$. The complement of the channel \mathbf{H}_γ^b is denoted by $\mathbf{H}_\gamma^{\bar{b}}$, whose diagonal elements are the same as \mathbf{H}_γ^b and the remaining elements are negatives of that of \mathbf{H}_γ^b .

We next utilize strong typicality [25] to determine the number of channel uses for each type. Consider any i.i.d. sequence of quantized channel matrices $\mathbf{H}_\gamma(1), \dots, \mathbf{H}_\gamma(N)$. Such a sequence is called δ -typical, if

$$N(\Pr\{\mathbf{H}_\gamma^b\} - \delta) \leq \#\{\mathbf{H}_\gamma^b|\mathbf{H}_\gamma(1), \dots, \mathbf{H}_\gamma(N)\} \leq N(\Pr\{\mathbf{H}_\gamma^b\} + \delta), \quad (30)$$

where $\#\{.\}$ operator gives the number of blocks of each type. The set of such strong typical sequences is denoted by $\mathcal{A}_\delta^{(N)}$. By the strong law of large numbers, we choose sufficiently large N to have $\Pr\{\mathcal{A}_\delta^{(N)}\} \geq 1 - \epsilon'$.

Assuming that the realized sequence of quantized channel gain matrices, i.e., $\mathbf{H}_\gamma(1), \dots, \mathbf{H}_\gamma(N)$, is δ -typical, we use the first $N_b \triangleq N(\Pr\{\mathbf{H}_\gamma^b\} - \delta)$ channel uses for each channel type b . This causes a loss of at most $2\delta NB$ channel uses out of N , which translates to a negligible rate loss. With again a negligible loss in the rate, we choose each N_b as even. Note that the complement block of b is \bar{b} , which lasts for $N_{\bar{b}} = N_b$ channel uses, as $\Pr\{\mathbf{H}_\gamma^{\bar{b}}\} = \Pr\{\mathbf{H}_\gamma^b\}$.

We now describe the coding scheme, which can be viewed as an ergodic interference alignment coding scheme with a secrecy pre-coding. For each secrecy codebook in the ensemble of transmitter i , we generate $2^{N(R_i + R_i^x)}$ sequences each of length $\sum_{b=1}^B \frac{N_b}{2}$, where entries are chosen such that they satisfy the long term average power constraint of P . We assign each codeword to 2^{NR_i} bins each with $2^{NR_i^x}$ codewords. Given w_i , transmitter randomly chooses a codeword in bin i according to the uniform distribution, which is denoted by $\mathbf{X}_i(w_i, w_i^x)$, where w_i^x is the randomization index to confuse the eavesdroppers. The codeword is then divided into B blocks each with a length of $\frac{N_b}{2}$ symbols. The codeword of block b is denoted by $\{X_i^b(t), t = 1, \dots, \frac{N_b}{2}\}$ and is repeated during the last $\frac{N_b}{2}$ channel uses of the block \bar{b} , i.e., $X_i^b(t) = X_i^{\bar{b}}(\frac{N_b}{2} + t)$, for $t = 1, \dots, \frac{N_b}{2}$. The channel gains, additive noises, and the received symbols is denoted with the same block, i.e., channel type, notation. Here, the effective channels during block b is given by

$$\tilde{Y}_i^b(t) = 2h_{i,i}^b(t)X_i^b(t) + Z_i^b(t) + Z_i^{\bar{b}}\left(\frac{N_b}{2} + t\right), \quad (31)$$

and

$$\tilde{\mathbf{Y}}_e^b(t) = \sum_{i=1}^n \begin{bmatrix} h_{i,e}^b(t) \\ h_{i,e}^{\bar{b}}(\frac{N_b}{2} + t) \end{bmatrix} X_i^b(t) + \begin{bmatrix} Z_e^b(t) \\ Z_e^{\bar{b}}(\frac{N_b}{2} + t) \end{bmatrix}, \quad (32)$$

for $t = 1, 2, \dots, \frac{N_b}{2}$.

We essentially code over the above two fading channels seen by destinations and eavesdroppers. Here, to satisfy both the secrecy and the reliability constraints, we choose the rates as follows.

$$R_i = \frac{1}{2}E[I(X_i; \tilde{Y}_i|\mathbf{H})] - \frac{1}{2n}E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] - \epsilon \quad (33)$$

$$R_i^x = \frac{1}{2n}E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)], \quad (34)$$

where the expectation is over the ergodic channel fading, and the channel outputs \tilde{Y}_i and $\tilde{\mathbf{Y}}_e$ are given by the transformations (27) and (28), respectively.

For any $\epsilon > 0$, we choose sufficiently small δ . Then, in the limit of $N \rightarrow \infty$, $\tau \rightarrow \infty$, $\gamma \rightarrow 0$, each legitimate receiver i can decode W_i and W_i^x with high probability (covering a-typical behavior of the channel sequence as well) as

$$R_i + R_i^x = \frac{1}{2}E[I(X_i; \tilde{Y}_i | \mathbf{H})] - \epsilon, \quad (35)$$

where ϵ covers for quantization errors and unused portion of the channel uses.

For the secrecy constraint we first consider each expression on the right hand side of the following equality.

$$\begin{aligned} \frac{1}{N}I(W_{\mathcal{K}}; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) &= \frac{1}{N}I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) + \frac{1}{N}H(W_{\mathcal{K}}^x | W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ &\quad - \frac{1}{N}H(W_{\mathcal{K}}^x | W_{\mathcal{K}}, \mathbf{H}, \mathbf{H}_e), \end{aligned} \quad (36)$$

where we denote $W_{\mathcal{K}} \triangleq \{W_i, \forall i \in \mathcal{K}\}$ and $W_{\mathcal{K}}^x \triangleq \{W_i^x, \forall i \in \mathcal{K}\}$.

We have

$$\begin{aligned} \frac{1}{N}I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) &= \frac{1}{N}I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e | \mathbf{H}, \mathbf{H}_e) \\ &\stackrel{(a)}{\leq} \frac{1}{N}I(\{X_i^b(t), \forall i, b, t\}; \{\tilde{\mathbf{Y}}_e^b(t), \forall b, t\} | \mathbf{H}, \mathbf{H}_e) \\ &\stackrel{(b)}{\leq} \frac{\sum_{b=1}^B \frac{N_b}{2}}{N} \left(E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e | \mathbf{H}, \mathbf{H}_e)] - \epsilon_1 \right) \\ &\stackrel{(c)}{=} \frac{(1 - \epsilon_2)}{2} \left(E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e | \mathbf{H}, \mathbf{H}_e)] - \epsilon_1 \right) \\ &\leq \frac{1}{2}E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e | \mathbf{H}, \mathbf{H}_e)] + \epsilon_1 \epsilon_2, \end{aligned} \quad (37)$$

where (a) is due to the coding scheme and the data processing inequality, (b) is due to ergodicity with some $\epsilon_1 \rightarrow 0$ as $N \rightarrow \infty$, (c) is due to unused portion of channel uses with some $\epsilon_2 \rightarrow 0$ as $N \rightarrow \infty$.

Secondly, due to the ergodicity and the symmetry among transmitters, the rate assignment implies the following: The rates satisfy

$$\sum_{i \in \mathcal{S}} R_i^x \leq \frac{1}{2}E[I(X_{\mathcal{S}}; \tilde{\mathbf{Y}}_e | X_{\mathcal{K}-\mathcal{S}}, \mathbf{H}, \mathbf{H}_e)], \quad (38)$$

for any $\mathcal{S} \subseteq \mathcal{K}$. (Please refer to Lemma 8 of [23] for details.) Thus, the randomization indices $W_{\mathcal{K}}^x$ can be decoded at the eavesdropper e given the bin indices $W_{\mathcal{K}}$. Then, utilizing Fano's inequality and averaging over the ensemble of the codebooks, we have

$$\frac{1}{N}H(W_{\mathcal{K}}^x | W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \leq \epsilon_3, \quad (39)$$

with some $\epsilon_3 \rightarrow 0$ as $N \rightarrow \infty$.

Third, as $W_{\mathcal{K}}^x$ is independent of $\{W_{\mathcal{K}}, \mathbf{H}, \mathbf{H}_e\}$ and as each W_i^x is independent, we have

$$\frac{1}{N}H(W_{\mathcal{K}}^x | W_{\mathcal{K}}, \mathbf{H}, \mathbf{H}_e) = \frac{1}{N}H(W_{\mathcal{K}}^x) = \frac{1}{N} \sum_{i=1}^n H(W_i^x) = \frac{1}{N} \sum_{i=1}^n N R_i^x = \frac{1}{2}E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_e | \mathbf{H}, \mathbf{H}_e)]. \quad (40)$$

Finally, using (37), (39), and (40) in (36), we obtain

$$\frac{1}{N}I(W_{\mathcal{K}}; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \leq \epsilon, \quad (41)$$

which implies that

$$\frac{1}{N}I(W_i; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \leq \epsilon, \forall i \in \mathcal{K} \quad (42)$$

with some $\epsilon \rightarrow 0$ as $N \rightarrow \infty$, which establishes the claim. \blacksquare

Note that for i.i.d. complex Gaussian input distribution, i.e., when $X_i(t) \sim \mathcal{CN}(0, P), \forall i, t$, the proposed scheme achieves

$$R_i = \left[\frac{1}{2}E \left[\log \left(1 + \frac{2P|h_{i,i}|^2}{N_0} \right) \right] - \frac{1}{2n}E \left[\log \det \left(\mathbf{I}_2 + \frac{P}{N_0} \sum_{i=1}^n \tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* \right) \right] \right]^+, \quad (43)$$

for user $i \in \mathcal{K}$. Here, for any non-degenerate fading distribution, e.g., Rayleigh fading where $h_{i,k} \sim \mathcal{CN}(0, 1), \forall i \in \mathcal{K}, \forall k \in \mathcal{K} \cup \mathcal{E}$, the second term of (43) diminishes as n gets large. In particular, as $n \rightarrow \infty$, R_i scales as

$$R_i = \left[\frac{1}{2} E \left[\log \left(1 + \frac{2P|h_{i,i}|^2}{N_0} \right) \right] - \frac{O(\log(n))}{n} \right]^+,$$

and hence we can say that each user can achieve at least a positive constant secure rate for any given SNR for sufficiently large n . (Please refer to Appendix B.)

To quantify the behavior of the scheme in the high SNR regime, we now focus on the achievable secure DoF per user, which can be characterized by dimension counting arguments. The proposed scheme achieves $\eta = \left[\frac{1}{2} - \frac{1}{n} \right]^+$ secure DoF per user for any given non-degenerate fading model. (This can be shown by dividing both sides of (43) with $\log \text{SNR}$ and taking the limit $\text{SNR} \rightarrow \infty$ for any given n .) Note that the pre-log gain of the proposed scheme is the same as that of [23]. But, remarkably, ergodic interference alignment allows us to attain secrecy at any SNR by only requiring a statistical knowledge of the eavesdropper CSI. We note that this gain is obtained at the expense of large coding delay (at least exponential in the number of users).

V. EAVESDROPPER COLLUSION

In a more powerful attack, eavesdroppers can *collude*, i.e., they can share their observations. Securing information in such a scenario will be an even more challenging task compared to non-colluding case [19], [26]. Interestingly, even with colluding eavesdroppers, we show that the scaling result for the path loss model remains the same with the proposed multi-hop scheme with almost the same eavesdropper intensity requirement.

Theorem 10: If the legitimate nodes have unit intensity ($\lambda = 1$) and the colluding eavesdroppers have an intensity of $\lambda_e = O((\log n)^{-2-\rho})$ for any $\rho > 0$ in an extended network, almost all of the nodes can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ under the static path loss channel model.

Proof: Please refer to Appendix C. ■

We note that, in the colluding eavesdropper scenario, the result requires only a slightly modified eavesdropper intensity condition compared to the non-colluding case. Also, for the highway construction of the non-colluding case, the secrecy zone with an area of $(2df_e + 1)^2 c^2$ with $f_e > \sqrt{2}$ was sufficient. However, for the colluding eavesdropper scenario, legitimate nodes need to know whether there is an eavesdropper or not within the first layer zone, which has an area of $(2df_{l_1} + 1)^2 c^2$ with $f_{l_1} = \delta' \log(n)$, where δ' can be chosen arbitrarily small (see (62)). Hence, securing the network against colluding eavesdroppers requires more information regarding the eavesdroppers compared to the non-colluding case. But, remarkably, the optimal scaling law (see [2]) is achieved even when the eavesdroppers collude under these assumptions.

For the ergodic fading model, the eavesdropper collusion decreases the achievable performance. Let us add independent observations to the received vector given in (28) of Theorem 9 according to eavesdropper collusion and denote colluding eavesdroppers' observations by $\tilde{\mathbf{Y}}_{e^*}$ for $e^* \in \mathcal{E}^* \triangleq \{e_1^*, e_2^*, \dots\}$. For example, if e_1 and e_2 colludes, their cumulative observations is denoted by $\tilde{\mathbf{Y}}_{e_1^*}$ (SIMO-MAC with 4 receive antennas). In such a scenario, the proposed scheme can be used to achieve the following rate.

Corollary 11: For a given eavesdropper collusion set \mathcal{E}^* , source-destination pair $i \in \mathcal{K}$ achieves the following rate with the proposed ergodic interference alignment scheme for the ergodic fading channel model:

$$R_i = \min_{e^* \in \mathcal{E}^*} \left[\frac{1}{2} E[I(X_i; \tilde{\mathbf{Y}}_i | \mathbf{H})] - \frac{1}{2n} E[I(X_1, \dots, X_n; \tilde{\mathbf{Y}}_{e^*} | \mathbf{H}, \mathbf{H}_e)] \right]. \quad (44)$$

Note that the proposed scheme achieves $\eta = \left[\frac{1}{2} - \frac{n_e}{n} \right]^+$ secure DoFs per user for non-degenerate fading distributions when all the eavesdroppers collude. (This can be shown from (44) by setting $\mathcal{E}^* = \mathcal{E}$, choosing the input distribution as i.i.d. $\mathcal{CN}(0, P)$, dividing both sides by $\log \text{SNR}$, and taking the limit $\text{SNR} \rightarrow \infty$ for any given n_e and n .)

VI. CONCLUSION

In this work, we studied the scaling behavior of the capacity of wireless networks under secrecy constraints. For extended networks with the path loss model (the exponent is assumed to satisfy $\alpha > 2$), the legitimate nodes and eavesdroppers were assumed to be randomly placed in the network according to Poisson point processes of intensity $\lambda = 1$ and λ_e , respectively. It is shown that, when $\lambda_e = o((\log n)^{-2})$, almost all of the nodes achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$, showing that securing the transmissions does not entail a loss in the per-node throughput for our model, where transmissions from other users are considered as noise at receivers. Our achievability argument is based on novel secure multi-hop forwarding strategy where forwarding nodes are chosen such that no eavesdroppers exist in appropriately constructed *secrecy zones* around them and independent randomization is employed in each hop. Tools from percolation theory were used to establish the existence of a sufficient number of *secure highways* allowing for network connectivity. Finally, a time division approach was used to accomplish an end-to-end secure connection between almost all source-destination pairs. The same scaling result is also

obtained for the dense network scenario when $\frac{\lambda_\epsilon}{\lambda} = o((\log n)^{-2})$. We note that, in the proposed scheme, we assumed that nodes know whether an eavesdropper exist in a certain zone (secrecy zone) or not. An analysis of a more practical scenario, in which legitimate nodes have no (or more limited) eavesdropper location information, would be interesting.

We next focused on the ergodic fading model and employed ergodic interference alignment scheme with an appropriate secrecy pre-coding at each user. This scheme is shown to be capable of securing each user at any SNR (depending on the underlying fading distributions), and hence provides performance guarantees even for the finite SNR regime compared to previous work. For the high SNR scenario, the scheme achieves $[\frac{1}{2} - \frac{1}{n}]^+$ secure DoFs per orthogonal dimension at each user. Remarkably, the results for the ergodic fading scenarios do not require eavesdropper CSI at the legitimate users, only a statistical knowledge is sufficient. However, this gain is obtained at the expense of large coding delays.

Lastly, the effect of the eavesdropper collusion is analyzed. It is shown that, for the path loss model, the same per-node throughput scaling, i.e., $\Omega(\frac{1}{\sqrt{n}})$, is achievable under almost the same eavesdropper intensity requirement. For the fading model, the proposed model is shown to endure various eavesdropper collusion scenarios. In particular, when all the eavesdroppers collude, a secure DoF of $[\frac{1}{2} - \frac{\alpha_\epsilon}{n}]^+$ is shown to be achievable.

We list several future directions here: 1) Characterizing the full trade-off between secure throughput vs. eavesdropper node intensity is of definite interest. 2) We have not exploited cooperation techniques to enhance security in this work. Cooperation in the sense of [7] may be helpful. For example, in the extended network scenario, hierarchical cooperation might increase the per-node throughput for $\alpha < 3$ or achieve the optimal throughput for $\alpha \geq 3$ even with higher eavesdropper intensities. In addition, cooperation for secrecy strategies (see, e.g., [27], [28] and references therein) may be beneficial in enhancing the scaling results. 3) A uniform rate per user is considered in this work. Arbitrary traffic pattern can be considered for users with distinct quality of service constraints. 4) Eavesdroppers are assumed to be passive (they only listen the transmissions). An advanced attack might include active eavesdroppers, which may jam the wireless channel. Securing information in such scenarios is an interesting avenue for further research.

APPENDIX A LEMMAS USED IN SECTION III

Lemma 12 (Theorem 7.65, [21]): Let $d, k \geq 1$. Consider random variables Y_x and Z_x^π taking values in $\{0, 1\}$, for $x \in \mathbb{Z}^d$. Denote $Z^\pi = \{Z_x^\pi : x \in \mathbb{Z}^d\}$ as a family of independent random variables satisfying $\Pr\{Z_x^\pi = 1\} = 1 - \Pr\{Z_x^\pi = 0\} = \pi$. Also, denote Euclidean distance in \mathbb{Z}^d as $d(\cdot, \cdot)$.

If $Y = \{Y_x : x \in \mathbb{Z}^d\}$ is a k -dependent family of random variables, i.e., if any two sub-families $\{Y_x : x \in \mathcal{A}\}$ and $\{Y_{x'} : x' \in \mathcal{A}'\}$ are independent whenever $d(x, x') > k$, $\forall x \in \mathcal{A}, \forall x' \in \mathcal{A}'$, such that

$$\Pr\{Y_x = 1\} \geq \delta, \forall x \in \mathbb{Z}^d,$$

then there exist a family of independent random variables $Z^{\pi(\delta)}$ such that Y statistically dominates $Z^{\pi(\delta)}$, where $\pi(\delta)$ is a non-decreasing function $\pi : [0, 1] \rightarrow [0, 1]$ satisfying $\pi(\delta) \rightarrow 1$ as $\delta \rightarrow 1$.

Proof: The proof is given in [22], where the authors also provide a construction of the independent model. See also [21]. ■

Lemma 13 (Theorem 5, [2]): Consider discrete edge percolation with edge existence probability p on a square grid of size $m \times m$ (number of edges). For any given $\kappa > 0$, partition the area into $\frac{m}{(\kappa \log m - \epsilon_m)}$ rectangles of size $m \times (\kappa \log m - \epsilon_m)$, where $\epsilon_m = o(1)$ as $m \rightarrow \infty$ and is chosen to have integer number of rectangles. Denote the maximal number of edge-disjoint left to right crossings of the i th rectangle as C_m^i and let $N_m \triangleq \min_i C_m^i$. Then, $\forall \kappa > 0$ and $\forall p \in (\frac{5}{6}, 1)$ satisfying $\kappa \log(6(1-p)) < -2$, $\exists \delta > 0$ such that

$$\lim_{m \rightarrow \infty} \Pr\{N_m \leq \delta \log m\} = 0. \quad (45)$$

Proof: The proof is given in [2, Appendix I]. See also [20, Theorem 4.3.9]. ■

Lemma 14: Consider a Poisson random variable X of parameter λ . Then,

$$P(X \geq x) \leq \frac{e^{-\lambda}(e\lambda)^x}{x^x}, \text{ for } x > \lambda. \quad (46)$$

Proof: The proof follows by an application of the Chernoff bound. Please refer to [2, Appendix II] or [20, Appendix]. ■

Lemma 15: Consider a Poisson random variable X of parameter λ . Then, for any $\epsilon \in (0, 1)$,

$$\lim_{\lambda \rightarrow \infty} P(X \leq (1 - \epsilon)\lambda) = 0, \quad (47)$$

and

$$\lim_{\lambda \rightarrow \infty} P(X \leq (1 + \epsilon)\lambda) = 1. \quad (48)$$

Proof: The proof follows by utilizing the Chebyshev's inequality. ■

APPENDIX B

$R_i > R$ FOR SOME CONSTANT $R > 0$ IN (43) AS $n \rightarrow \infty$

Consider that the statistics of $h_{i,e}s$ are given by 1) $q \triangleq E[\Re\{h_{i,e}\}] + jE[\Im\{h_{i,e}\}]$ is a complex number with finite real and imaginary parts, and 2) $s \triangleq E[|h_{i,e}|^2]$ is a finite real number, $\forall i \in \mathcal{K}, e \in \mathcal{E}$. Let us further assume that $\mathbf{I}_2 + \frac{P}{N_0} \sum_{i=1}^n \tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^*$ is a positive definite matrix. Focusing on the second term of (43), we obtain

$$\frac{1}{2n} E \left[\log \det \left(\mathbf{I}_2 + \frac{P}{N_0} \sum_{i=1}^n \tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* \right) \right] \stackrel{(a)}{\leq} \frac{1}{2n} \log \det \left(\mathbf{I}_2 + \frac{P}{N_0} \sum_{i=1}^n E \left[\tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* \right] \right) \quad (49)$$

$$\stackrel{(b)}{=} \frac{1}{2n} \log \left(1 + \frac{P}{N_0} 2ns + \frac{P^2}{N_0^2} n^2 (s^2 - |q|^4) \right) \quad (50)$$

$$= \frac{O(\log(n))}{n}, \quad (51)$$

where (a) is due to Jensen's inequality as $\log \det(\cdot)$ function is concave in positive definite matrices, and (b) follows from

$$\tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* = \begin{pmatrix} |h_{i,e}|^2 & h_{i,e} \tilde{h}_{i,e}^* \\ \tilde{h}_{i,e} h_{i,e}^* & |\tilde{h}_{i,e}|^2 \end{pmatrix},$$

which implies

$$E \left[\tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* \right] = \begin{pmatrix} s & |q|^2 \\ |q|^2 & s \end{pmatrix}.$$

Thus, the second term of (43) becomes insignificant, $o(1)$ as $n \rightarrow \infty$; and $\exists R > 0$ such that $R_i > R, \forall i \in \mathcal{K}$ for sufficiently large n . Note that the assumption that $\mathbf{I}_2 + \frac{P}{N_0} \sum_{i=1}^n \tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^*$ is a positive definite matrix holds in the limit of large n almost surely. (Here, due to strong law of large numbers, the sum converges to $nE \left[\tilde{\mathbf{H}}_{i,e} \tilde{\mathbf{H}}_{i,e}^* \right]$ with probability 1.)

APPENDIX C

PROOF OF THEOREM 10

The proof follows along the same lines of the proof of Theorem 6 by generalizing the secrecy zone approach to multi-level zones, where the area of each zone is carefully chosen to obtain a (statistically) working bound for the SNR of the colluding eavesdropper.

In Fig. 5, we show the *zones* around a transmitting square: Zone of level k for $k \in \{1, \dots, L\}$ has an area of A_{l_k} , and the associated distance is denoted with $f_{l_k} d$ with some $f_{l_k} \geq 1$ and $f_{l_k} \geq f_{l_{k-1}}$. Note that, we take f_{l_k} as a design parameter. We will choose f_{l_k} differently, depending on whether a node is forwarding data over a highway or accessing to/accessed by a highway. Furthermore, d and f_{l_k} may depend on n , i.e., expected number of users.

We now provide generalization of Lemma 1 to the colluding eavesdropper case.

Lemma 16 (Secure Rate per Hop): In a communication scenario depicted in Fig. 5 (no eavesdroppers in the first zone), the rate

$$R_{TR} = \frac{1}{(f_t d)^2} \left[\log(1 + \underline{\text{SNR}}_{TR}) - \log(1 + \overline{\text{SNR}}_{\mathcal{E}^*}) \right]^+, \quad (52)$$

where

$$\underline{\text{SNR}}_{TR} \triangleq \frac{P(d+1)^{-\alpha} c^{-\alpha} (\sqrt{2})^{-\alpha}}{N_o + P8(f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha)}, \quad (53)$$

$$S(\alpha) \triangleq \sum_{i=1}^{\infty} i(i-0.5)^{-\alpha}, \quad (54)$$

$$\overline{\text{SNR}}_{\mathcal{E}^*} \triangleq \frac{P(1+\epsilon)9c^{2-\alpha}d^{-\alpha}}{N_0} \lambda_e d^2 \sum_{k=2}^L (f_{l_k})^2 (f_{l_{k-1}})^{-\alpha}, \quad (55)$$

$$f_t \geq \frac{2(d+1)}{d}, \quad (56)$$

is w.h.p. securely and simultaneously achievable between any active transmitter-receiver pair if f_{l_k} is chosen such that

$$\lambda_e d^2 (f_{l_k})^2 \rightarrow \infty, \text{ as } n \rightarrow \infty, \text{ for } k = 2, 3, \dots \quad (57)$$

Proof: The steps of the proof are similar to that of Lemma 1. Here, we need to derive a working upper bound for the colluding eavesdropper SNR. In our case, secrecy is guaranteed assuming that the eavesdroppers are located on the boundary of each level of zones. We first bound the number of eavesdroppers at each level. We have

$$A_{l_k} \leq (2df_{l_k} + 1)^2 c^2 \leq 9d^2 (f_{l_k})^2 c^2, \quad (58)$$

as $d \geq 1$ and $f_{l_k} \geq 1$. Hence, the number of eavesdroppers in layer l_k can be bounded, using the Chebyshev's inequality (see Lemma 15), by

$$|\mathcal{E}_{l_k}^*| \leq (1 + \epsilon) \lambda_e 9c^2 d^2 (f_{l_k})^2 \quad (59)$$

w.h.p., for a given $\epsilon > 0$, as long as we choose f_{l_k} to satisfy

$$\lambda_e d^2 (f_{l_k})^2 \rightarrow \infty, \text{ as } n \rightarrow \infty.$$

Now, we place $|\mathcal{E}_{l_k}^*|$ number of eavesdroppers from layer k at distance $f_{l_{k-1}} dc$ for $k = 2, 3, \dots$. This is referred to as configuration \mathcal{E}^* . These colluding eavesdroppers can do maximal ratio combining (this gives the best possible SNR for them) to achieve the following SNR.

$$\begin{aligned} \text{SNR}_{\mathcal{E}^*} &= \frac{P \sum_{k=2}^L |\mathcal{E}_{l_k}^*| (f_{l_{k-1}})^{-\alpha} c^{-\alpha} d^{-\alpha}}{N_0} \\ &\leq \frac{P(1 + \epsilon) 9c^2 d^{-\alpha}}{N_0} \lambda_e d^2 \sum_{k=2}^L (f_{l_k})^2 (f_{l_{k-1}})^{-\alpha} \\ &\triangleq \overline{\text{SNR}_{\mathcal{E}^*}}. \end{aligned} \quad (60)$$

Note that the challenge here is to choose f_{l_k} such that $\overline{\text{SNR}_{\mathcal{E}^*}} < \infty$, and at the same time to satisfy (57). With some appropriate choices of these parameters, we generalize Lemma 4 and Lemma 5 to the colluding eavesdropper case. ■

Lemma 17 (Rate per Node on the Highways): If $\lambda_e = O((\log n)^{-2})$, each node on the constructed highways can transmit to their next hop at a constant secure rate. Furthermore, if the number of nodes each highway serves is $O(\sqrt{n})$, each highway can w.h.p. carry a per-node throughput of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Proof:

We show the result for $\lambda_e = \Theta((\log n)^{-2})$, which will imply the desired result (as lowering the eavesdropper density can not degrade the performance). Consequently, there exists constants $\underline{\Lambda}$, $\overline{\Lambda}$, and n_1 such that

$$\underline{\Lambda} (\log n)^{-2} \leq \lambda_e \leq \overline{\Lambda} (\log n)^{-2}, \text{ for } n \geq n_1, \quad (61)$$

where $\underline{\Lambda} < \overline{\Lambda}$.

We choose each level of zones over the highways by setting

$$f_{l_k} = \left(\frac{\delta}{9\overline{\Lambda}c^2d^2} \right)^{\frac{1}{2}} (\log n)^{\left(\frac{\alpha}{2}\right)^{k-1}}. \quad (62)$$

Here,

$$\lambda_e (2f_{l_1}d + 1)^2 c^2 \leq \lambda_e 9(f_{l_1})^2 d^2 c^2 \quad (63)$$

$$= \lambda_e \frac{\delta (\log n)^2}{\overline{\Lambda}} \quad (64)$$

$$\leq \delta, \text{ for } n \geq n_1. \quad (65)$$

Therefore, due to our percolation result, i.e., Lemma 3, each member of a given highway does not have any eavesdropper within their first level secrecy zone as δ can be chosen arbitrarily small. Now, as the above choice also satisfies

$$\lambda_e d^2 (f_{l_k})^2 \rightarrow \infty, \text{ as } n \rightarrow \infty, \text{ for } k = 2, 3, \dots,$$

we can utilize Lemma 1 to achieve a secrecy rate of

$$R_{TR} = \frac{1}{(f_t d)^2} \left[\frac{1}{2} \log(1 + \overline{\text{SNR}_{TR}}) - \frac{1}{2} \log(1 + \overline{\text{SNR}_{\mathcal{E}^*})} \right]. \quad (66)$$

Now, we provide an upper bound for $\overline{\text{SNR}_{\mathcal{E}^*}}$. First, note that our setup results in

$$(f_{l_k})^2 (f_{l_{k-1}})^{-\alpha} = \left(\frac{\delta}{9\overline{\Lambda}c^2d^2} \right)^{\frac{2-\alpha}{2}}.$$

Hence,

$$\overline{\text{SNR}}_{\mathcal{E}^*} = \frac{P(1+\epsilon)9}{N_0} \lambda_e (L-1) \left(\frac{\delta}{9\bar{\Lambda}} \right)^{\frac{2-\alpha}{2}} \quad (67)$$

$$\leq \frac{P(1+\epsilon)9\bar{\Lambda}}{N_0} (\log n)^{-2} (L-1) \left(\frac{\delta}{9\bar{\Lambda}} \right)^{\frac{2-\alpha}{2}}, \quad (68)$$

for $n \geq n_1$

$$\rightarrow 0, \text{ as } n \rightarrow \infty, \quad (69)$$

where the last step is due to the observation that the number of levels can be upper bounded by

$$L-1 \leq \frac{\log(\log n)}{\log(\frac{\alpha}{2})}. \quad (70)$$

Therefore, there exists n_2 such that for all $n \geq n_2$, the rate expression satisfies $R_{TR} \geq R$ for some constant R . The second claim follows from Lemma 3. ■

Lemma 18 (Access Rate to Highways): Almost all source (destination) nodes can w.h.p. simultaneously transmit (receive) their messages to (from) highways with a secure rate of $\Omega((\log n)^{-3-\alpha})$, if $\lambda_e = O((\log n)^{-(2+\rho)})$ for any $\rho > 0$.

Proof:

We show the result for $\lambda_e = \Theta((\log n)^{-(2+\rho)})$, which will imply the desired result (as lowering the eavesdropper density can not degrade the performance). Consequently, there exists constants $\underline{\Lambda}$, $\bar{\Lambda}$, and n_3 such that

$$\underline{\Lambda}(\log n)^{-(2+\rho)} \leq \lambda_e \leq \bar{\Lambda}(\log n)^{-(2+\rho)}, \text{ for } n \geq n_3, \quad (71)$$

where $\underline{\Lambda} < \bar{\Lambda}$.

At this point, we can upper bound the fraction of nodes that can not access to a highway due to an existence of an eavesdropper in their first secrecy zone. Following the analysis in Lemma 5, as long as we satisfy

$$\lambda_e (f_{l_1})^2 d^2 \rightarrow 0, \text{ as } n \rightarrow \infty, \quad (72)$$

almost all the nodes can access to the highways. To compute the achievable secrecy rate with Lemma 1, we need to satisfy

$$\lambda_e (f_{l_k})^2 d^2 \rightarrow \infty, \text{ as } n \rightarrow \infty, \text{ for } k = 2, 3, \dots. \quad (73)$$

Further, we can show that as long as we satisfy

$$\lambda_e d^2 \sum_{k=2}^L (f_{l_k})^2 (f_{l_{k-1}})^{-\alpha} \leq C, \text{ as } n \rightarrow \infty, \quad (74)$$

for some constant C , the achievable rate R_{TR} in Lemma 16 scales like $\Omega((\log n)^{-2-\alpha})$ as $d = \kappa'' \log n$. Due to time-division among the legitimate nodes accessing the highways (there are w.h.p. $O(\log n)$ nodes within small squares), the secrecy rate per user satisfies $\Omega((\log n)^{-3-\alpha})$.

Here, to satisfy (72), (73), (74) with $d = \kappa'' \log n$, we choose the secrecy zones as

$$f_{l_k} = (\log n)^{r(\frac{\alpha}{2})^{k-1}}, \quad (75)$$

with some r satisfying $\frac{r}{\alpha} < r < \frac{r}{2}$. ■

Note that, Lemma 2 that the per hop security implies the multi-hop security also holds for the colluding eavesdropper scenario. That is, the security obtained for configuration \mathcal{E}^* for each hop is sufficient to ensure secrecy against colluding eavesdroppers listening all the hops. Combining these results with the percolation result given in Lemma 3 concludes the proof.

REFERENCES

- [1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.
- [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 Trans. Inf. Theory*, vol. 53, no. 3, pp. 1009–1018, Mar. 2007.
- [3] B. Nazer, S. A. Jafar, M. Gastpar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. 2009 IEEE International Symposium on Information Theory (ISIT)*, Jun. 2009.
- [4] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom for the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
- [5] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3457–3470, Aug. 2008.
- [6] U. Niesen, "Interference alignment in dense wireless networks," 2009, submitted for publication.
- [7] A. Özgür, O. Lévêque, and D. N. C. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3549–3572, Oct. 2007.
- [8] U. Niesen, P. Gupta, and D. Shah, "On capacity scaling in arbitrary wireless networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3959–3982, Sep. 2009.
- [9] J. Ghaderi, L.-L. Xie, and X. Shen, "Hierarchical cooperation in ad hoc networks: Optimal clustering and achievable throughput," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3425–3436, Aug. 2009.
- [10] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, 2nd ed. Springer, 2007.
- [11] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Elect. Eng.*, vol. 55, pp. 109–115, 1926.
- [12] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.
- [13] V. Bhandari and N. H. Vaidya, "Secure capacity of multi-hop wireless networks with random key pre-distribution," in *Proc. 2008 IEEE INFOCOM Workshops*, Apr. 2008.
- [14] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [15] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [16] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [17] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. 2008 IEEE International Symposium on Information Theory (ISIT)*, Jul. 2008, pp. 539–543.
- [18] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. 11th IEEE Singapore International Conference on Communication Systems (ICCS)*, Nov. 2008, pp. 974–979.
- [19] —, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. 2009 IEEE International Symposium on Information Theory (ISIT)*, Jun. 2009, pp. 2442–2446.
- [20] M. Franceschetti and R. Meester, *Random Networks for Communication: From Statistical Physics to Information Systems*. Cambridge University Press, 2007.
- [21] G. Grimmett, *Percolation*, 2nd ed. Springer, 1999.
- [22] T. M. Liggett, R. H. Schonmann, and A. M. Stacey, "Domination by product measures," *Annals of Probability*, vol. 25, no. 1, pp. 71–95, 1997.
- [23] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, to appear. [Online]. Available: <http://arxiv.org/abs/0810.1187>
- [24] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On the effect of colluding eavesdroppers on secrecy capacity scaling," in *Proc. 16th European Wireless Conference (EW 2010)*, Lucca, Italy, Apr. 2010.
- [25] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley and Sons, Inc., 1991.
- [26] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Military Communications Conference (MILCOM)*, Oct. 2005, pp. 1501–1506.
- [27] O. O. Koyluoglu and H. El Gamal, "On the secrecy rate region for the interference channel," in *Proc. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, Cannes, France, Sep. 2008.
- [28] —, "Cooperative binning and channel prefixing for secrecy in interference channels," *IEEE Trans. Inf. Theory*, submitted for publication.

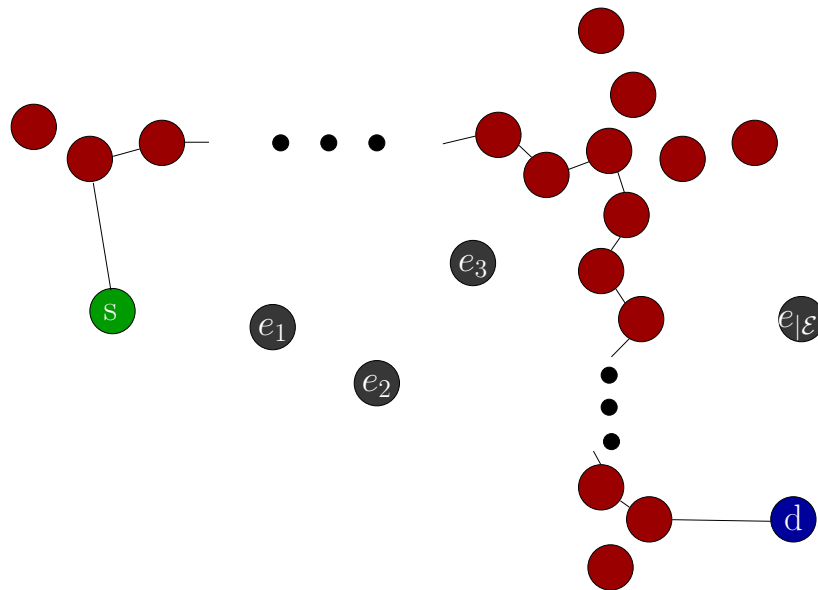


Fig. 1. A typical multi-hop route consists of four transmission phases: 1) From source node to an entry point on the horizontal highway, 2) Across horizontal highway (message is carried until the desired vertical highway member), 3) Across vertical highway (message is carried until the exit node), and 4) From the exit node to the destination node.

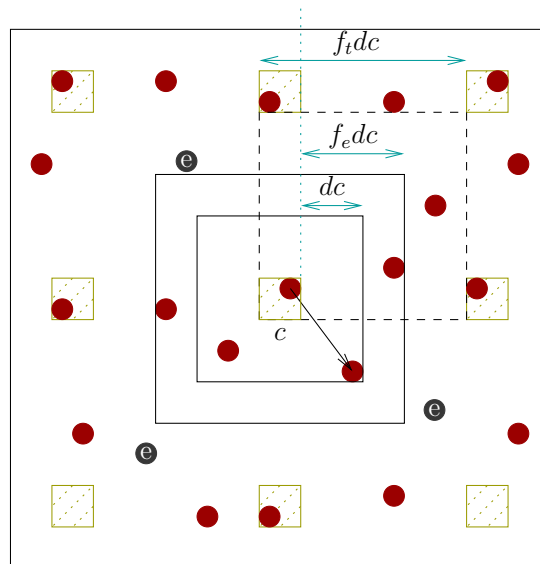


Fig. 2. The transmitter located at the center of the figure wishes to communicate with a receiver that is d squares away. The second square surrounding the transmitter is the secrecy zone, which is the region of points that are at most $f_e d$ squares away from the transmitter. Side length of each square is denoted by c . The time division approach is represented by the shaded squares that are allowed for transmission. It is evident from the dashed square that the time division requires $(f_t d)^2$ time slots.

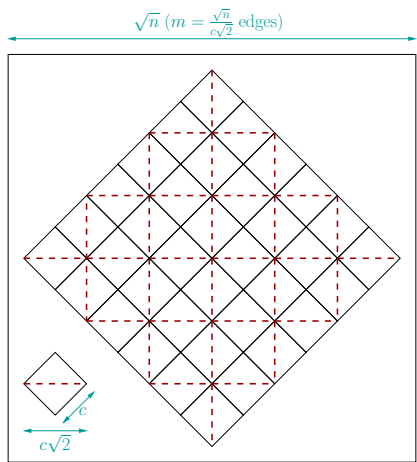


Fig. 3. Horizontal and vertical edges in the discrete bond percolation model are denoted by dotted lines. A dotted edge is open (used for the highway construction) if the corresponding square is open. There are $\Theta(n)$ number of edges in the random graph.

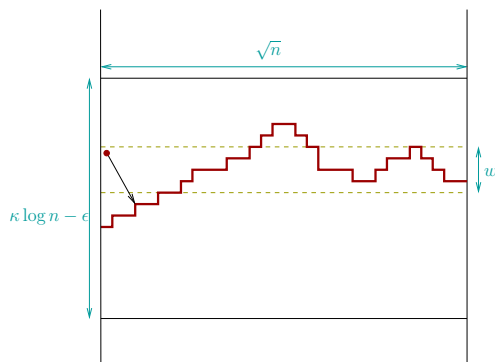


Fig. 4. There are $\lceil \delta \log n \rceil$ number of disjoint highways within each rectangle of size $(\kappa \log n - \epsilon) \times \sqrt{n}$. The legitimate users in the slab, denoted by dotted lines, of the rectangle is served by the highway denoted with red bold line.

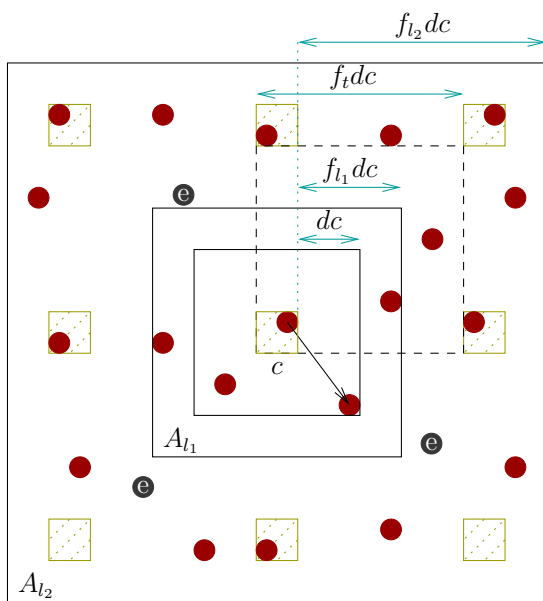


Fig. 5. The second square surrounding the transmitter is the secrecy zone (zone of level 1), which is the region of points that are at most $f_{l_1} d$ squares away from the transmitter. The zone of level k is denoted with distance $f_{l_k} d$ and has an area of A_{l_k} .