On Secrecy Capacity Scaling in Wireless Networks

O. Ozan Koyluoglu, C. Emre Koksal, and Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University
Columbus, OH 43210, USA
Email: {koyluogo, koksal, helgamal}@ece.osu.edu

***Abstract*—We study a random extended network, where the legitimate and eavesdropper nodes are assumed to be placed according to Poisson point processes in a square region of area n. It is shown that, when the legitimate nodes have unit intensity, $\lambda = 1$, and the eavesdroppers have an intensity of $\lambda_e = O\left((\log n)^{-2}\right)$, almost all of the nodes achieve a perfectly secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$. 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). Remarkable, under these assumptions, securing the transmissions of nodes does not entail a loss in the per-node throughput in terms of scaling.**

I. Introduction

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. The scaling laws of wireless networks under the assumption of **pre-distributed** private keys was studied in [1]. 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 these limitations by adopting an information theoretic framework for secrecy in wireless networks. In particular, we 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 for point-to-point noiseless channels [2]. This line of work was later extended by Wyner [3] to noisy channels. 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). However, according to the best of our knowledge, information theoretical secrecy analysis of large wireless networks has not been studied in the literature before.

Large networks is studied in the seminal work of Gupta and Kumar ([4]). It is shown that the randomly located nodes can achieve at most a rate that scales like $\frac{1}{\sqrt{n}}$, as $n \to \infty$, under an interference-limited channel model. The authors have further established the achievability of the same scaling behavior when the nodes are arbitrarily placed in the network. In random networks, however, the proposed multi-hop scheme of [4] only achieves a scaling of $\frac{1}{\sqrt{n \log n}}$ per node. This gap was recently closed in [5] using tools from the percolation theory, 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.

This paper considers a random extended network, where the legitimate nodes and eavesdroppers are distributed according to Poisson point processes with intensity $\lambda = 1$ and $\lambda_e = O\left((\log n)^{-2}\right)$, respectively, over a square region of area n. In such a network, we follow the footsteps steps of [5] to construct a highway backbone, which achieves a constant rate and serves $O(\sqrt{n})$ nodes. However, in addition to the interference constraint considered in [5], our multi-hop forwarding strategy is 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. This allows the legitimate nodes to create an advantage over the eavesdroppers, which is, then, exploited to secure transmissions. Furthermore, *an independent randomization signal* is injected in each hop to ensure maximal ambiguity at the eavesdropper(s). We then proceed to show that in this dependent edge model, the network still percolates and many highway paths can be constructed. This construction allows us to show that the highways can carry data of each source-destination pair of rate $\Omega\left(\frac{1}{\sqrt{n}}\right)$ securely. Finally, using the fact that each node has an $O(\log n)$ distance to the closest highway, we show that almost all nodes can access the highways with a secure rate that scales better than $\Omega\left(\frac{1}{\sqrt{n}}\right)$, if the eavesdropper intensity satisfies $\lambda_e = O\left((\log n)^{-2}\right)$. Combining these two results establishes the achievability of a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$ for almost all source-destination pairs. This implies that, under these assumptions, securing the network does not entail a loss in the per-node throughput in terms of scaling.

The rest of this paper is organized as follows. Section II provides our system model and notations. Section III develops our main result via several helper lemmas. Finally, concluding remarks are given in Section IV.

II. System Model and Notation

Our extended network model is a square of side-length $\sqrt{n}$. 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 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 listening 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:

$$\begin{aligned} Y_j(t) &= \sum_{i \in \mathcal{T}(t)} \sqrt{d_{i,j}^{-\alpha}} X_i(t) + N_j(t) \\ Y_e(t) &= \sum_{i \in \mathcal{T}(t)} \sqrt{d_{i,e}^{-\alpha}} X_i(t) + N_e(t), \end{aligned}$$

where $N_j(t)$ and $N_e(t)$ are i.i.d. $\mathcal{N}(0, N_0)$ noise samples at the legitimate node j and at the eavesdropper e, respectively; $\alpha > 2$ is the path loss exponent; and the distance between node i and node j is denoted by d_{ij}.

All legitimate transmitters have an individual peak power constraint, denoted by P. The transmitters are assumed to know *a-priori* whether there is any eavesdropper within some neighborhood or not (the neighborhood is called secrecy zone and the size of it will be clear in later parts of the text). To simulate a 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. Finally, the set of all observations at eavesdropper e is denoted by $\mathbf{Y}_e$.

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. 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 $N \to \infty$, and
- The information leakage rate, i.e., $\frac{I(W_{s,d};\mathbf{Y}_e)}{N}$, can be made arbitrarily small $\forall e \in \mathcal{E}$ as $N \to \infty$.

If there are only 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. (We denote these by $\{\mathbf{Y}_e(1), \cdots, \mathbf{Y}_e(H)\}$.)

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

$$\lim_{n \to \infty} \Pr\{f(n) \le k g(n)\} = 1.$$

We also say that $f(n) = \Omega(g(n))$ w.h.p., if w.h.p. $g(n) = O(f(n))$.

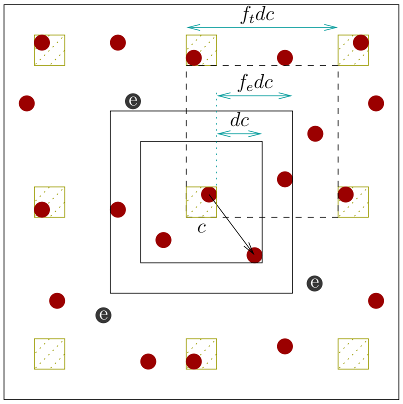

Fig. 1. The time division approach is represented by denoting the squares that are allowed for transmission. It is evident from the dotted square that the time division requires $(f_t\, d)^2$ time slots. The transmitter located at the center of the figure wishes to communicate with a receiver that is 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.

III. The Main Result

To establish the main result of the paper, we first consider the secrecy rate per hop. We partition the network area into squares of constant side length c. We further divide the area into larger squares of side $f_t dc$, 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 a small square can transmit to a receiver that is located at most d squares away as illustrated in Fig. 1. 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. 1, the secure rate, simultaneously achievable between any transmitter-receiver pair is:

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

where $f_t \ge \frac{2(d+1)}{d}$,

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

$$S(\alpha) \triangleq \sum_{i=1}^{\infty} i(i-0.5)^{-\alpha}, \quad \overline{\mathrm{SNR}_{e^*}} \triangleq \frac{P(f_e)^{-\alpha} d^{-\alpha} c^{-\alpha}}{N_o}, \quad (3)$$

$$\frac{(d+1)^{\alpha} (\sqrt{2})^{\alpha}}{(d)^{\alpha}} \left[1 + \frac{P}{N_o} 8 (f_t)^{-\alpha} d^{-\alpha} c^{-\alpha} S(\alpha) \right] < (f_e)^{\alpha}. \quad (4)$$

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

Proof: Please refer to [6]. ■

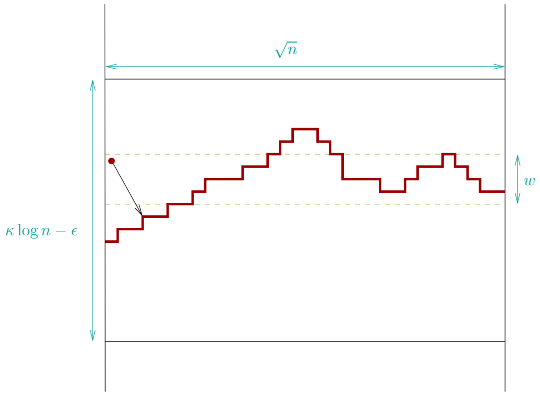

Fig. 2. There are $\lceil \delta \log n \rceil$ number of disjoint highways within each rectangle of size $(\kappa \log n - \epsilon) \times \sqrt{n}$. (Please refer to [5] and [6] for details.) The legitimate users in the slab denoted by dotted line of the depicted rectangle is served by the highway denoted with red bold line. It is clear that the highway serves to $O(\sqrt{n})$ nodes in this setup.

Next we introduce our novel multi-hop *randomization* strategy. This technique 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 located on the boundary of the secrecy zone is sufficient to ensure secrecy from any eavesdropper which listens to the transmissions from all the hops and lie outside the secrecy zones.

Proof: We consider a source s, a destination d, and an eavesdropper e in the network. Without loss of generality, we consider H hops in the multi-hop scheme. 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 has $2^{N(R_i + R_i^x - \frac{\epsilon_1}{H})}$ codewords each entry with i.i.d. $\mathcal{N}(0, P)$, for some $\epsilon_1 > 0$. Each codeword is 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 codeword $\mathbf{X}_i(w_{s,d}, w_i^x)$ is transmitted at transmitter i, where w_i^x is randomly chosen. 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 $R_i^x = I(X_i; Y_{e_i^*}) = \frac{1}{2} \log\left(1 + \overline{\text{SNR}}_{e_i^*}\right)$ (note that this is the rate loss in (1)). We continue as below.

$$
\begin{aligned}
I(W_{s,d}; \mathbf{Y}_e) &= I(W_{s,d}; \mathbf{Y}_e(1), \cdots, \mathbf{Y}_e(H)) \\
&\overset{(a)}{\leq} I(W_{s,d}; \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_H^*}) \\
&\overset{(b)}{\leq} I(\mathbf{X}_1, \cdots, \mathbf{X}_H; \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_H^*}) \\
&\quad - I(W_1^x, \cdots, W_H^x; \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_H^*} | W_{s,d}) \\
&\overset{(c)}{=} \sum_{i=1}^{H} I(\mathbf{X}_1, \cdots, \mathbf{X}_H; \mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_{i-1}^*}) \\
&\quad - H(W_1^x, \cdots, W_H^x) \\
&\quad + \sum_{i=1}^{H} H(W_i^x | W_{s,d}, \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_H^*}, W_1^x, \cdots, W_{i-1}^x) \\
&\overset{(d)}{\leq} \sum_{i=1}^{H} H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_{i-1}^*}) \\
&\quad - H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_{i-1}^*}, \mathbf{X}_i) - NR_{x_i} + N\frac{\epsilon_1 + \epsilon_2}{H} \\
&\overset{(e)}{\leq} \sum_{i=1}^{H} I(\mathbf{X}_i; \mathbf{Y}_{e_i^*}) - NR_{x_i} + N\frac{\epsilon_1 + \epsilon_2}{H} \\
&\overset{(f)}{\leq} \sum_{i=1}^{H} NI(X_i; Y_{e_i^*}) - NR_{x_i} + N\frac{\epsilon_1 + \epsilon_2 + \epsilon_3}{H} \\
&= N(\epsilon_1 + \epsilon_2 + \epsilon_3),
\end{aligned}
$$

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 data processing inequality and the Markov chain $\{W_{s,d}, W_1^x, \cdots, W_H^x\} \rightarrow \{\mathbf{X}_1, \cdots, \mathbf{X}_H\} \rightarrow \{\mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_H^*}\}$, (c) follows since $W_{s,d}$ and W_i^x are independent, (d) is due to Fano's inequality (as we choose $R_i^x \leq I(X_i; Y_{e_i^*})$, the codebook construction allows for decoding randomization message at the eavesdropper given the bin index) with some $\epsilon_2 \rightarrow 0$ as $N \rightarrow \infty$ and due to fact that the second term in the sum is zero, (e) follows by the fact that conditioning does not increase the entropy and the observation that $H(\mathbf{Y}_{e_i^*} | \mathbf{Y}_{e_1^*}, \cdots, \mathbf{Y}_{e_{i-1}^*}, \mathbf{X}_i) = H(\mathbf{Y}_{e_i^*} | \mathbf{X}_i)$, and (f) is due to the fact that $I(\mathbf{X}_i; \mathbf{Y}_{e_i^*}) \leq NI(X_i; Y_{e_i^*}) + N\frac{\epsilon_3}{H}$ for some $\epsilon_3 \rightarrow 0$ as $N \rightarrow \infty$ (see, e.g., [3, Lemma 8]).

After setting, $\epsilon = \epsilon_1 + \epsilon_2 + \epsilon_3$, we obtain our result: For any given $\epsilon > 0$, $\frac{I(W_{s,d}; \mathbf{Y}_e)}{N} < \epsilon$ as $N \rightarrow \infty$. ■

The following result, using the construction given in [5], shows 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), where κ' can be made arbitrarily small.

Proof: Please refer to [6]. See also Fig. 2. ■

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. Therefore, in addition to the percolation based construction developed in [5], we utilized the result of [7] to establish Lemma 3. 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, as the number of nodes each highway serves is $O(\sqrt{n})$, each highway can w.h.p.

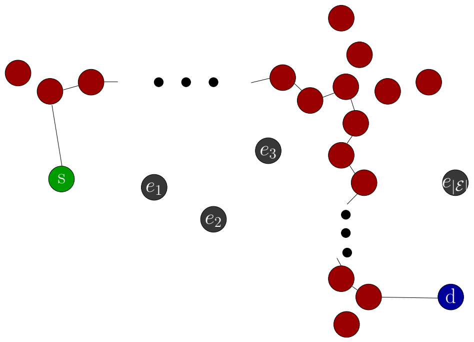

Fig. 3. A typical multi-hop route consists of four transmission phases: 1) From source node to an entry point on the horizontal highway, 2) Across horizontal highway (message is carried until the desired vertical highway member), 3) Across vertical highway (message is carried until the exit node), and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

carry a per-node 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 Lemmas 1 and 2, one can see that highways can carry data *securely* with a *constant positive rate* (we choose $d = 1$). 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 $\Omega\left((\log n)^{-3-\alpha}\right)$, if $\lambda_e = O\left((\log n)^{-2}\right)$.

Proof: The proof follows from Lemma 1, where we choose $d = \kappa' \log(n)$ with arbitrarily small κ' (Lemma 3). Please refer to [6] for details. ■

We now establish the main result of the paper. In our multi-hop routing scheme, each user has a dedicated route with each hop used for N channel uses. The secrecy encoding at each transmitter is designed assuming an eavesdropper on the boundary of the secrecy zone. This way, a transmitter can achieve the rate reported in Lemma 1. We argue that this secrecy encoding scheme will ensure secrecy from an eavesdropper that listens to the transmissions of every hop due to Lemma 2. Then, the main result follows by utilizing the following time division approach. The total transmission time of the network is divided into four phases (see Fig. 3). 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). From the achievable rates given in these lemmas we obtain our main result, which is formalized by the following theorem.

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

Utilizing the upper bound of [4] for the capacity of wireless networks, we see that the proposed scheme achieves the optimal scaling law.

IV. Conclusion

In this work, we considered the problem of securing transmissions of extended wireless networks, where the legitimate nodes and eavesdroppers were assumed to be randomly placed into the extended network according to Poisson point processes of intensity $\lambda = 1$ and λ_e, respectively. It is shown that, when $\lambda_e = O\left((\log n)^{-2}\right)$, almost all of the nodes achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$. Our achievability argument is based on novel secure multi-hop forwarding strategy where 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. Overall, our results show that, as long as $\lambda_e = O\left((\log n)^{-2}\right)$, securing the transmissions does not entail a loss in the per-node throughput.

We note that, the interference is considered as noise at the legitimate receivers in our model. As shown in [8], more sophisticated cooperation strategies achieve the same throughput for the case of extended networks with $\alpha \geq 3$ leading to the conclusion that cooperation in the sense of [8] does not increase the secrecy capacity for $\alpha \geq 3$. Our current investigations aim at extending this analysis to a more practical scenario, in which legitimate nodes have no (or more limited) eavesdropper location information.

References

[1] V. Bhandari and N. H. Vaidya, “Secure capacity of multi-hop wireless networks with random key pre-distribution,” in *Proc. 2008 IEEE INFOCOM Workshops, Workshop on Mission Critical Networking (MCN)*, Apr. 2008.

[2] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[3] A. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 388–404, Mar. 2000.

[5] 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.

[6] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, “On secrecy capacity scaling in wireless networks.” [Online]. Available: http://arxiv.org/abs/0908.0898

[7] 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.

[8] 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.