Physical Layer Security from Inter-Session Interference in Large Wireless Networks

Azadeh Sheikholeslami*, Dennis Goeckel*, Hossein Pishro-Nik* and Don Towsley†
* Electrical and Computer Engineering Department, University of Massachusetts, Amherst, MA
†Computer Science Department, University of Massachusetts, Amherst, MA
* {sheikholesla,goeckel,pishro}@ecs.umass.edu,†towsley@cs.umass.edu

***Abstract*—Physical layer secrecy in wireless networks in the presence of eavesdroppers of unknown location is considered. In contrast to prior schemes, which have expended energy in the form of cooperative jamming to enable secrecy, we develop schemes where multiple transmitters send their signals in a cooperative fashion to confuse the eavesdroppers. Hence, power is not expended on "artificial noise"; rather, the signal of a given transmitter is protected by the aggregate interference produced by the other transmitters. We introduce a two-hop strategy for the case of equal path-loss between all pairs of nodes, and then consider its embedding within a multi-hop approach for the general case of an extended network. In each case, we derive an achievable number of eavesdroppers that can be present in the region while secure communication between all sources and intended destinations is ensured.**

I. Introduction

Because of the broadcast nature of wireless networks, any node in the coverage range of a source can overhear any message that it transmits. Consequently, one of the most important and difficult considerations in wireless networks is secrecy. The traditional approach to secrecy is encryption of the plain message by means of special functions that are assumed to be computationally infeasible for the adversary to decrypt [1]. However, because of improvements in processors and methods of breaking such encryption systems, there are concerns that these assumptions no longer suffice. Especially in sensitive applications requiring everlasting secrecy, users might prefer a higher level of secrecy. Here we consider methods of network design that inhibit the reception of the transmitted signal at an eavesdropper. This might be used in conjunction with traditional cryptographic approaches, as part of a defense in depth approach, or it might enable information theoretic secrecy, as described next.

In 1949, Shannon introduced the notion of perfect secrecy [2]: if the eavesdropper's uncertainty (entropy rate) about the plain message after seeing the transmitted signal is equal to the eavesdropper's uncertainty about the message before seeing the transmitted signal, then "perfect secrecy" is said to be achieved. Based on this, Wyner introduced the wiretap channel and showed that, in a degraded wiretap channel, adding randomness to the codebook and using channel uncertainty can protect the secure message from being intercepted by the eavesdropper [3]. Later, the idea of the wiretap channel was extended to more general cases [4], [5].

In all cases, the key to a positive secrecy rate is to have a better channel from the transmitter to the intended receiver than to the eavesdropper. However, in many cases the eavesdropper's channel is better than the legitimate channel; for example, the eavesdropper might have a much better receiver than that of the intended recipient or the eavesdropper might be much closer to the transmitter than the intended receiver. Furthermore, in many situations the location of the eavesdroppers are unknown to the legitimate nodes.

To combat these problems, one must design algorithms to produce the required advantage for the intended recipient over the eavesdroppers. Negi and Goel introduced the idea of adding artificial noise to the system by means of a multiple antenna transmitter or a single antenna transmitter with some helper nodes [6], [7]. The artificial noise is placed in the null space of the channel from the transmitter to the intended recipient and consequently does not affect the intended recipient while at the same time degrading the eavesdropper's channel with high probability. Subsequently, cooperative jamming (by producing artificial noise) [8]–[10] and using helper nodes [11] to improve physical layer secrecy in small networks has been extensively investigated.

However, in many network scenarios there are simultaneous ongoing data flows between source-destination pairs. The effect of their interference on the secrecy of wiretap channels and methods to increase the secrecy rate region for small networks consisting of at most two senders, two receivers and one external eavesdropper have also been studied in recent years [12]–[15].

The primary focus of this paper is to propose cooperative strategies that use the mixed signal from the simultaneous transmissions of multiple transmitters to hide each signal from passive but intelligent and powerful eavesdroppers.

Although considerable research has been devoted to physical layer secrecy in scenarios with a few nodes, e.g. one transmitter, one receiver, one eavesdropper and a few helper nodes

This research was sponsored by the National Science Foundation under grants CNS-1018464, CCF-0728970, CCF-0844725, and by the U.S. Army Research Laboratory and the U.K. Ministry of Defence under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

that relay the message or generate artificial noise to help obtain secrecy, rather less attention has been paid to security in large multi-hop wireless networks with a large number of legitimate nodes and eavesdroppers. In this case, the asymptotic results for large networks are often obtained as estimates for the utility of approaches in finite size wireless networks. Consequently, secrecy in large networks has recently been considered in the work of [16] by introducing the secrecy-graph, which has been extended in [17]–[19]. Furthermore, connectivity [20], [21], coverage [22], scalability [23]–[26] and cooperative jamming [27] in large wireless networks have been studied.

In this paper, we consider a cooperative strategy to improve physical layer secrecy in large wireless networks with a large number of sources, destinations, relay nodes and eavesdroppers. In contrast to other cooperative scenarios where helper nodes generate artificial noise, here each node transmits its own (independent) message to the corresponding destination in the presence of passive eavesdroppers. The signal of each transmitter is concealed from the eavesdroppers by interference produced from the aggregate signal of other transmitters. As in [27], legitimate nodes do not perform any interference alignment or interference cancellation.

The legitimate nodes communicate with each other in such a way that intended receivers receive the signal with signal-to-interference-plus-noise-ratio (SINR) higher than a threshold required to decode the message with arbitrarily low probability of error, while at the same time keeping the SINR at the eavesdroppers lower than another arbitrary threshold. This approach is beneficial from different perspectives. From a practical point of view, because the thresholds are separate, the system designer has the freedom to choose threshold values based on available equipment and security requirements. The required SINR threshold for the eavesdropper can be chosen so small that even a smart eavesdropper equipped with a suitable modern decoder would not be able to decode the signal. From an information theoretic point of view, the required SINR thresholds at the legitimate and eavesdropper nodes can be chosen such that the legitimate channel always has a required advantage over the eavesdropper's channel with probability approaching one. This guarantees that we always can achieve a desired secrecy rate from each source to its corresponding destination.

In the literature of physical layer secrecy in large wireless networks, usually geometric approaches based on the relative location of legitimate and eavesdropper nodes have been considered and then the effect of multi-path fading on the received signal has been ignored (e.g. [16]–[20]); however, in our method, the presence of fading is very important for the scheme to work properly. While in most other schemes for enhancing physical layer secrecy, the location of the eavesdroppers and/or channel state information (CSI) of the source to eavesdropper channels are assumed to be known by the legitimate nodes, we assume that the locations of eavesdroppers are not known and legitimate nodes are not aware of this CSI.

We propose two protocols to enhance physical layer secrecy in the network described above and study their asymptotic performance. First, we consider the case of equal path-loss between all pairs of nodes. This scheme is applicable to the situation when eavesdroppers cannot be closer to transmitters than a specific distance or in networks where each transmitter is able to deactivate the eavesdroppers within a neutralization region around itself [19]. We consider a two-hop strategy and propose a protocol to select a messaging relay for each source-destination pair in such a way that the selected relay has good links to both that source and that destination. In each time period, a number of sources simultaneously transmit their message to corresponding destinations using their selected relay. The interference from the signals of other transmitters hides the message of each transmitter from the eavesdroppers.

Next, we consider the general case, when all nodes are placed uniformly and randomly in a square of area n. We consider the employment of the proposed scheme within each cell to support a multi-hop construction within the Gupta-Kumar framework [28]. By using the proposed protocol, nodes of each cell choose suitable relays from the next cell in such a way that each selected relay has a good link to its previous node. Again the message of each transmitter is concealed from eavesdroppers by interference from the communication of other nodes. We find an achievable number of allowable eavesdroppers that the network can tolerate in the region of the cell as a function of the number of system nodes, while guaranteeing a required level of reliability and secrecy.

The rest of the paper organized as follows. Section 2 describes the model and problem formulation. In Sections 3 and 4, the protocols for the case of equal path-loss between all pairs of nodes and the general case are described and analyzed, respectively. Discussion, ideas for future work and conclusions are provided in Sections 5 and 6.

II. Model and Problem Formulation

A. Model

We consider an extended wireless network consisting of n legitimate nodes placed uniformly at random on a 2-D plane of area $[0, \sqrt{n}]^2$. Each node is a source or destination of one stream and source-destination pairs are randomly assigned.

In addition m eavesdroppers, $E_1, ..., E_m$ are placed uniformly at random on this surface (Figure 1). The locations of eavesdroppers and the CSI of channels from legitimate nodes to eavesdropper nodes are assumed to be unknown to the legitimate nodes.

Denote the k^{th} symbol transmitted by node A by $x_k^{(A)}$. All nodes transmit with the same power E_S. The k^{th} signal received by node B is denoted by $y_k^{(B)}$, and the distance between nodes A and B is denoted by $d_{A,B}$. We also denote the noise at receiver B by $n_k^{(B)}$ and the frequency-nonselective multi-path fading from a transmitter A to a receiver B by $h_{A,B}$. Based on this model, the k^{th} signal received at node B from node A when all nodes in a group of nodes, $\mathcal{S}_1$, transmit

their signals is:

$$y_k^{(B)} = \frac{h_{A,B}}{d_{A,B}^{\alpha/2}}\sqrt{E_S}x_k^{(A)} + \sum_{A_i\in\mathcal{S}_1, A_i\neq A}\frac{h_{A_i,B}}{d_{A_i,B}^{\alpha/2}}\sqrt{E_S}x_k^{(A_i)} + n_k^{(B)}$$

where $\alpha > 2$ is the path loss exponent. The noise at each receiver is assumed to be i.i.d complex Gaussian with $E[|n_k^{(B)}|^2] = N_0$. The multi-path fading $h_{A,B}$ is assumed to follow a Rayleigh distribution, which remains constant during the transmission of each packet. Then, $|h_{A,B}|^2$ is exponentially distributed with mean $E[|h_{A,B}|^2]$ and, without loss of generality, we assume that $E[|h_{A,B}|^2] = 1$. We also exploit channel reciprocity, i.e. $h_{A,B} = h_{B,A}$. The SINR from node A to node B for any two nodes in the network is denoted by $C_{A,B}$:

$$C_{A,B} = \frac{E_S.|h_{A,B}|^2 d_{A,B}^{-\alpha}}{\sum_{i\in\mathcal{S}_1, i\neq j} E_s|h_{A_i,B}|^2 d_{A_i,B}^{-\alpha} + {}^{N_0}/_2}$$

B. Problem Formulation

Our goal is to propose protocols to enhance physical layer secrecy in the wireless networks described above and find the achievable number, $m(n)$, of eavesdroppers in the system as a function of the number of nodes, that can be tolerated while guaranteeing reliable and secure communication between all source-destination pairs.

Transmission is *reliable* provided that each packet is delivered from a positive fraction of sources to corresponding destinations with high probability as $n \to \infty$, i.e. a positive fraction of legitimate nodes (relays or destinations) receive packets with signal-to-interference-plus-noise-ratio (SINR) greater than a predefined threshold γ, which is required for successful decoding (with arbitrarily small probability of error) at a legitimate node. Let $P_{OUT}^{(S\to D)}$ denote the probability of the event $\{C_{S,D} < \gamma\}$. For any source S that transmits a message, reliable communication with destination D is ensured if $P_{OUT}^{(S\to D)} \to 0$.

Transmission is *secure* provided that, with high probability, no eavesdropper can achieve a target SINR γ_E from any of the sources or relays as $n \to \infty$, i.e. all eavesdroppers are in outage w.h.p. for large n; where, $P_{OUT}^{(E)}$ is the probability of the event $\left(\bigcap_{j=1}^{n}\{C_{S_j,E_1} < \gamma_E\} \cap ... \cap \{C_{S_j,E_m} < \gamma_E\}\right)$.

III. Equal Path Loss Between All Pairs of Nodes

In this section we consider the case that there is equal path loss between all pairs of nodes. This assumption also applies when we know that the eavesdroppers cannot come closer to each transmitter (source or relay) than a specified distance or each transmitter can deactivate the eavesdroppers within an area around it. Without loss of generality, we assume that the distance between all pairs of nodes is unity (i.e. $d_{A,B} = 1$, for all $A \neq B$).

Among n system nodes, during each time period, ${}^{2\log n}/_t$ of them are designated as sources and destinations, and the other system nodes are the assisting nodes. Here t is a constant to be determined later. We first propose a protocol to convey messages from a positive fraction of designated sources to corresponding destinations reliably and securely. Then, we analyze the system and find the maximum number of eavesdroppers that can be tolerated while secrecy is maintained for all transmitted messages.

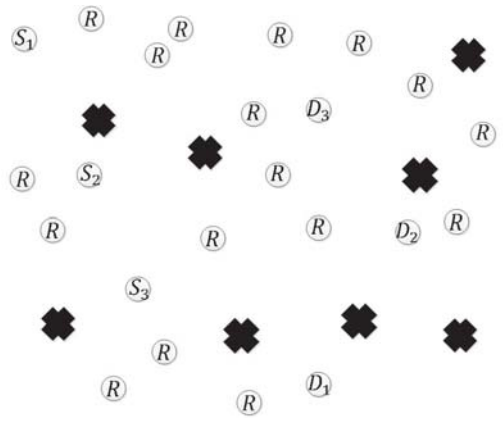

Fig. 1. Multiple sources, multiple destinations and relay nodes (circles) in presence of a number of eavesdroppers (crosses)

A. Protocol

The following protocol is employed by sets of ${}^{\log n}/_t$ source-destination (S-D) pairs to set up secure links between each source and its corresponding destination.

1) *Source-destination pair selection*: Each of the assisting nodes (relays) chooses one of the active ${}^{\log n}/_t$ source-destination pairs uniformly at random and waits to receive a pilot from that S-D pair. This results in $n_j,\ j = 1, ..., {}^{\log n}/_t$ assisting nodes waiting for a pilot from the j^{th} S-D pair. We term the group of nodes waiting to receive pilots from the j^{th} S-D pair, the j^{th} "waiting group" and denote it by $A_j,\ j = 1, ..., {}^{\log n}/_t$.
2) *Channel measurement between sources and relays*: Each source S_j broadcasts a pilot signal. Each node in A_j measures its channel to S_j: $h_{S_j,R_i},\ \forall i, j$ such that $R_i \in A_j$ and $j = 1, ..., {}^{\log n}/_t$. Each eavesdropper also measures the link between itself and its randomly selected source. These measurements are assumed to be perfect.
3) *Channel measurement between destinations and relays*: Each destination D_j broadcasts a pilot signal. Each node in A_j measures its channel to D_j: $h_{R_i,D_j}\ \forall i, j$ such that $R_i \in A_j$ and $j = 1, ..., {}^{\log n}/_t$. Each eavesdropper also measures the link between itself and its randomly selected destination. These measurements are assumed to be perfect.
4) *Relay selection*: In each waiting group of nodes, $A_j\ j = 1, ..., {}^{\log n}/_t$, the relays with $\min\left\{|h_{S_j,R_i}|^2, |h_{R_i,D_j}|^2\right\} > \frac{1}{2}\log\left(\frac{nt}{\log n}\right)$ are the designated relays. For the j^{th} S-D pair, let M_j denote

the number of designated relays and B_j the group of designated relays. For each S-D pair, relay selection is successful if exactly one designated relay exists, i.e. $M_j = 1$. Each relay in the group B_j sends a pilot to S_j. Hence, relay selection for S_j is successful if it receives exactly one pilot. We indicate the group of sources with successful relay selection by $\mathcal{S}_1$ and the messaging relay for the j^{th} S-D pair by R_j.

5) *Message transmission from S_j to R_j*: In this step, each source in $\mathcal{S}_1$ (source with a successful relay selection) transmits its message to the corresponding messaging relay. Relay R_j receives the signal:

$$y_k^{(R_j)} = h_{S_j,R_j}\sqrt{E_S}x_k^{(S_j)} + \sum_{S_i\in\mathcal{S}_1, i\neq j} h_{S_i,R_j}\sqrt{E_S}x_k^{(S_i)} + n_k^{(R_j)}$$

and eavesdropper $E_l,\ l = 1,\ldots,m-1$, receives:

$$y_k^{(E_l)} = h_{S_j,E_l}\sqrt{E_S}x_k^{(S_j)} + \sum_{S_i\in\mathcal{S}_1, i\neq j} h_{S_i,E_l}\sqrt{E_S}x_k^{(S_i)} + n_k^{(E_l)}$$

6) *Message transmission from relay R_j to destinations D_j*: In this step, each messaging relay transmits its message to the intended destination in a manner similar to the previous step.

B. Analysis

We first analyze the source-destination pair selection step. The size of each waiting group is described in the following lemma.

Lemma 3.1. With high probability, the number of relays in each and every waiting group satisfies $\{\frac{tn}{2\log n} < n_j < \frac{3tn}{2\log n}\}$.

Proof: Since $\log n/t$ S-D pairs exist, the probability that a given relay belongs to a given waiting group is $\frac{t}{\log n}$; thus, the number of nodes in each waiting group $n_j \sim$ Binomial$(n, \frac{t}{\log n})$. Using a Chernoff bound for binomial random variables:

$$P(n_j > (1+\delta)\frac{tn}{\log n}) < e^{-\frac{\delta^2 tn}{2\log n}}$$

and

$$P(n_j < (1-\delta)\frac{tn}{\log n}) < e^{-\frac{\delta^2 tn}{4\log n}}$$

then, setting $\delta = \frac{1}{2}$,

$$P\Big((n_j > \frac{3tn}{2\log n}) \cup (n_j < \frac{tn}{2\log n})\Big) < e^{-\frac{tn}{8\log n}}$$

Now we want to bound the number of nodes in each of the waiting groups uniformly. Using a union bound yields:

$$P\Big(\bigcup_{j=1}^{\log n/t}\Big[(n_j > \frac{3tn}{2\log n}) \cup (n_j < \frac{tn}{2\log n})\Big]\Big) < \frac{\log n}{t}e^{-\frac{tn}{8\log n}} \to 0.$$

■

Now consider the relay selection step. The following lemma shows that relay selection is successful for a positive fraction of source-destination pairs. The approach used to prove this lemma is similar to the approach used in [25].

Lemma 3.2. Let N_1 denote the total number of source-destination pairs with $M_j = 1$. Then, for the j^{th} source-destination pair,

$$\Pr(M_j = 1) \to \frac{1}{e} > 0 \quad \text{as} \quad n \to \infty$$

and $\frac{\log n}{2et} < N_1 < \frac{3\log n}{2et}$ with probability approaching one.

Proof: Suppose that in a given waiting group with n_j nodes, p is the probability that the minimum of fading of $S_j \to R_j$ and $R_j \to D_j$ links for a given S-D pair and given relay R_j is greater than $\frac{1}{2}\log(\frac{nt}{\log n})$, i.e.

$$p = \Pr\left(\min\left\{|h_{S_j,R_i}|^2, |h_{R_i,D_j}|^2\right\} > \frac{1}{2}\log\left(\frac{nt}{\log n}\right)\right)$$

The left side of the inequality is the minimum of two exponential random variables with mean one. Thus, it is an exponential random variable with mean $1/2$. Consequently,

$$p = e^{-2^{\frac{\log(\frac{nt}{\log n})}{2}}} = \frac{\log n}{nt}$$

From the independence of the fading, the probability that exactly one relay $R_j \in A_j$ has this property is:

$$\Pr(M_j = 1) = \left(\frac{nt}{\log n}\right) \times p(1-p)^{(\frac{nt}{\log n})} = \left(\frac{nt}{\log n}\right) \times \frac{1}{(\frac{nt}{\log n})}\left(1 - \frac{1}{(\frac{nt}{\log n})}\right)^{(\frac{nt}{\log n})}$$

$(\frac{nt}{\log n}) \to \infty$ as $n \to \infty$; hence,

$$\Pr(M_j = 1) \to \frac{1}{e} \quad \text{as} \quad n \to \infty$$

Then the number of S-D pairs that have a single relay $N_1 \sim$ Binomial$(\frac{\log n}{t}, \frac{1}{e})$; by using the Chernoff bound for binomial random variables:

$$P(N_1 < (1-\delta)\frac{\log n}{te}) < e^{-\frac{\delta^2\log n}{2e}}$$

and,

$$P(N_1 > (1+\delta)\frac{\log n}{te}) < e^{-\frac{\delta^2\log n}{4e}}$$

Choosing $\delta = 1/2$ and using the union bound:

$$P(\frac{\log n}{2et} < N_1 < \frac{3\log n}{2et}) > 1 - 2e^{-\frac{\log n}{8e}}$$

Thus in the limit, the number of nodes that find a single relay satisfies $\frac{\log n}{2et} < N_1 < \frac{3\log n}{2et}$ with probability approaching 1. ■

Now consider the following lemma, which will be very useful in our analysis [29]:

Lemma 3.3. Let $Y_1, \ldots, Y_n$ be a sequence of n i.i.d. exponential random variables, (more generally, each having an exponential tail $\bar{F}(y) \sim Ke^{-ay}$ where $K, a > 0$). Let $M_n = \max(Y_1, \ldots, Y_n)$. Then, $\lim_{n\to\infty} \frac{M_n}{\log n} = \frac{1}{a}$ a.s.

The following theorem characterizes an achievable number of eavesdroppers such that with high probability a positive fraction of the S-D pairs can communicate and all communications are secure.

Theorem 3.1. Consider the case of equal path-loss between all pairs of nodes. By applying the proposed protocol, $m(n)$ eavesdroppers can be tolerated guaranteeing $P_{OUT}^{(S_j\to D_j)} \to 0$, for each source S_j which transmits a message, and $P_{OUT}^{(E)} \to 1$ as $n \to \infty$, provided:

$$m(n) = o\left(\frac{n^{\frac{\log(1+\gamma_E)}{2et}}}{\log n}\right).$$

Proof: Because the relay-destination transmission is similar to the source-relay transmission, we analyze only the source-relay transmission. Also, by applying a coding technique [24], securing each hop is sufficient to ensure source-destination secrecy.

First consider the probability of outage between a source and its messaging relay, $P_{OUT}^{(S_j\to R_j)}$. The SINR at messaging relay R_j during the transmissions from sources to relays is:

$$C_{S_j,R_j} = \frac{E_S.|h_{S_j,R_j}|^2}{\sum_{i\in\mathcal{S}_1, i\neq j} E_s|h_{S_i,R_j}|^2 + N_0/2}$$

From Lemmas 3.1 and 3.3 with $a = 2$, $|h_{S_j,R_j}|^2 > \frac{\log n_j}{2\sqrt{2}} > \frac{\log n}{4}$ w.h.p. as $n \to \infty$. In the denominator, $\mathcal{S}_1$ is the subset of sources that transmit their message; from Lemma 3.2 , $|\mathcal{S}_1| = N_1 < \frac{3\log n}{2et}$ and thus $\sum_{i\in\mathcal{S}_1, i\neq j} |h_{S_i,R_j}|^2 < \frac{3\log n}{et}$ as $n \to \infty$ by the weak law of large numbers. The interference term is the dominant term in the denominator of C_{S_j,R_j}; hence,

$$C_{S_j,R_j} > \frac{\log n/4}{6\log n/et} > \gamma$$

with high probability if we choose t such that $t > \frac{24\gamma}{e}$; then, $P_{OUT}^{(S_j\to R_j)} \to 0$.

Now consider the eavesdroppers. For each source S_j, given that the group $\mathcal{S}_1$ of sources are transmitting and using a union bound:

$$P_{OUT}^{(S_j\to E)} = 1 - P\left(\bigcup_{i=1}^{m(n)} \{C_{S_j,E_i} \geq \gamma_E\}\right)$$
$$\geq 1 - \sum_{i=1}^{m(n)} P(C_{S_j,E_i} \geq \gamma_E)$$

Then, using the same approach as in [27], for each eavesdropper:

$$\begin{aligned}
&P(C_{S_j,E_i} \geq \gamma_E) \\
&\leq P\left(\frac{E_S|h_{S_j,E_i}|^2}{\sum_{S_k\in\mathcal{S}_r, k\neq j} E_S|h_{S_k,E_i}|^2 + N_0/2} > \gamma_E\right) \\
&< P\left(\frac{E_S|h_{S_j,E_i}|^2}{\sum_{S_k\in\mathcal{S}_r, k\neq j} E_S|h_{S_k,E_i}|^2} > \gamma_E\right) \\
&= E_{\{|h_{S_k,E_i}|^2, S_k\in\mathcal{S}_1\}}\left[P\left(|h_{S_j,E_i}|^2 > \gamma_E \sum_{S_k\in\mathcal{S}_1, k\neq j} |h_{S_k,E_i}|^2\right)\right] \\
&= \prod_{S_k\in\mathcal{S}_1, k\neq j} E_{\{|h_{S_k,E_i}|^2\}}\left[e^{-\gamma_E|h_{S_k,E_i}|^2}\right] \\
&\leq \left(\frac{1}{1+\gamma_E}\right)^{|\mathcal{S}_1|}
\end{aligned}$$

Hence, by the law of total probability and using Lemma 3.2,

$$P(C_{S_j,E_i} \geq \gamma_E) \leq \left(\frac{1}{1+\gamma_E}\right)^{\frac{\log n}{2et}}$$

w.h.p. as $n \to \infty$; and,

$$P_{OUT}^{(E)} \geq 1 - \sum_{i=1}^{m(n)} \left(\frac{1}{1+\gamma_E}\right)^{\frac{\log n}{2et}} \to 1$$

as $n \to \infty$ for any $m(n) = o((1+\gamma_E)^{\frac{\log n}{2et}})$. Using the union bound again, we obtain $P_{OUT}^{(E)}$, the probability that none of the eavesdroppers can achieve the target SINR from any of the transmitting sources. In this case:

$$m(n) = o\left(\frac{(1+\gamma_E)^{\frac{\log n}{2et}}}{\log n}\right) = o\left(\frac{n^{\frac{\log(1+\gamma_E)}{2et}}}{\log n}\right).$$

■

IV. General Case

Now consider the case that the path-loss between pairs of nodes is based on their relative locations. We consider an extended network where n nodes are placed uniformly at random in the 2-D plane on a square of side $\sqrt{n}$. Also m passive eavesdroppers of unknown channels and locations are placed uniformly at random. Our goal is to find the maximum achievable number of eavesdroppers that can be tolerated while maintaining reliability and secrecy.

We tessellate the square $[0, \sqrt{n}]^2$ into $\frac{n}{N}$ square cells, where $N = k\log n$ and each cell is of side $\sqrt{N} = \sqrt{k\log n}$ (Figure 2). Each source sends its message to a final destination in a multi-hop fashion. Each packet travels cell by cell horizontally until its x dimension equals the final destination's x dimension and then travels vertically until it reaches its final destination. Using this model, each packets take roughly $\sqrt{\frac{n}{\log n}}$ hops; thus, the occurrence of a final destination in each hop is very infrequent. In other words, most of the traffic entering a cell is the "through traffic" and just a small amount is local traffic.

As in the standard Gupta-Kumar approach [28], the cells which are at least $\Delta\sqrt{N}$ apart (Δ is a constant) can transmit simultaneously (see Appendix). Thus, we do not consider the

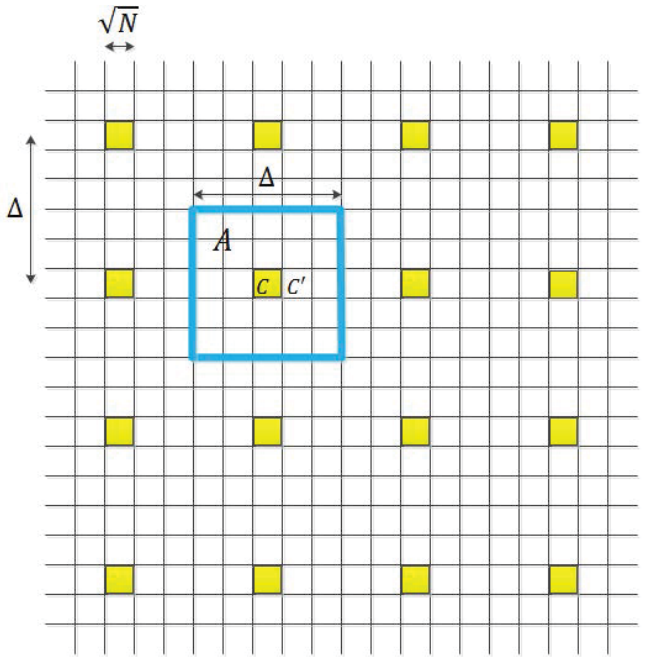

Fig. 2. The whole area is tessellated into squares of side $\sqrt{N}$. The square which is centered at cell C is region A.

interference from outside the cell in our analysis and only focus on the interference from the nodes inside each cell.

As earlier, securing each hop is sufficient to ensure source-destination secrecy [24]. Hence, we focus on the security of the through traffic between two adjacent cells and later discuss its extension to the whole network.

Consider two adjacent cells C and C'. Let N_C and $N_{C'}$ be the number of nodes in cells C and C' respectively. From [30], $1/2N < N_C < 3/2N$ and $1/2N < N_{C'} < 3/2N$ w.h.p. providing that $k > 8$. The cell C is divided into $\frac{N}{c(N)}$ square sub-cells, each of area $c(N) = k_1 \log N$ (Figure 3). The time slot which is assigned to cell C is divided into time periods. During each time period, the nodes in one sub-cell of C choose nodes in cell C' and send their messages securely to them based on the following protocol. If a packet in an active sub-cell has its final destination in C', the other nodes in this sub-cell stop transmitting their messages and, a protocol similar to [27] is employed to deliver the packet to the final destination by using some nodes as chatterers. Then, in the following time period, the protocol described below resumes. Note that, because local traffic (i.e. packets whose destinations are in C') forms a diminishing fraction of the total traffic, the use of the protocol in [27] is so infrequent that it does not impact the power consumption and network throughput.

We denote the number of nodes in the i^{th} sub-cell of C by N_{c_i}. The number of nodes in each sub-cell is characterized by the following lemma. The same approach as in [30] is used here.

Lemma 4.1. With high probability, the number of relays in each and every sub-cell of C satisfies $\frac{c(N)}{4} < N_{c_i} < \frac{9c(N)}{4}$ as $N \to \infty$.

Proof: The probability that a node belongs to a sub-cell c_i is $\frac{c(N)}{N}$. Given that the number of nodes in cell C, $N_C = N'$, $N_{c_i} \sim \text{Binomial}(N', \frac{c(N)}{N})$. Using a Chernoff bound:

$$P(N_{c_i} < (1-\delta)\frac{N'}{N}c(N)) < e^{-\frac{\delta^2 c(N) N'}{2N}}$$

and,

$$P(N_{c_i} > (1+\delta)\frac{N'}{N}c(N)) < e^{-\frac{\delta^2 c(N) N'}{4N}}$$

Where $1/2 < N'/N < 3/2$ with probability approaching 1. Using the law of total probability and choosing $\delta = 1/2$,

$$P\Big((N_{c_i} < \frac{c(N)}{4}) \cup (N_{c_i} > \frac{9c(N)}{4})\Big) < 2e^{-\frac{c(N)}{16}}$$

Using a union bound to bound the number of nodes per sub-cell uniformly:

$$\begin{aligned} &P\Bigg(\Big[\bigcup_{i=1}^{N/c(N)} \Big((N_{c_i} < \frac{c(N)}{4}) \cup (N_{c_i} > \frac{9c(N)}{4})\Big)\Big]\Bigg) \\ &< \frac{N}{c(N)} 2e^{-\frac{c(N)}{16}} \\ &= \frac{2N^{1-k_1/16}}{k_1 \log N} \end{aligned}$$

Hence, provided that $k_1 > 16$, $\frac{c(N)}{4} < N_{c_i} < \frac{9c(N)}{4}$, $\forall i$ w.h.p as $N \to \infty$. ■

The protocol for communication between two adjacent cells is described in the following section.

A. Protocol

Consider two neighboring cells C and C' (Figure 3). When nodes within a sub-cell are transmitting their messages, we refer to these nodes as sources and the nodes in the neighbor cell C' that receive the messages as relays. During each time period, a fraction $1/t$ of the sources in the active sub-cell c_i of cell C choose relays from the region $[\frac{\sqrt{N}}{4}, \sqrt{N}] \times [0, \sqrt{N}]$ of C', where t is a constant to be determined later. Then, the sources transmit their messages securely to these relays.

The proposed protocol for conveying the messages securely on each hop consists of:

1) *Channel measurement between sources and relays*: A constant fraction $1/t$ of sources within sub-cell c_i broadcast their pilots to the relays in the next cell. Each node in the region $[\frac{\sqrt{N}}{4}, \sqrt{N}] \times [0, \sqrt{N}]$ of C' and each eavesdropper measure the link between itself and its randomly selected source. These measurements are assumed to be perfect.
2) *Relay selection*: A relay that receives a pilot with fading greater than $\log N$, i.e. $|h_{S_j,R_k}|^2 > \log N$ such that $S_j \in c_i$ and $R_k \in C'$, is a designated relay. We denote the group of designated relays for source S_j by B_j. Each relay in each group B_j sends a pilot to S_j. For S_j, the relay selection step is successful if it receives exactly one pilot, i.e. from only one relay. We denote this relay

as R_j. Let $\mathcal{S}_1$ denote the set of sources that have exactly one relay.

3) *Message transmission from sources to relays*: In this step, each source in $\mathcal{S}_1$ transmits its message to its corresponding relay. Relay R_j receives the following signal:

$$y_k^{(R_j)} = h_{S_j,R_j}\sqrt{E_S}d_{S_j,R_j}^{-\alpha}x_k^{(S_j)} + \sum_{S_i\in\mathcal{S}_1, i\neq j} h_{S_i,R_j}\sqrt{E_S}d_{S_i,R_j}^{-\alpha}x_k^{(S_i)} + n_k^{(R_j)}$$

and eavesdropper E_l, $l = 1,\ldots,m-1$, receives:

$$y_k^{(E_l)} = h_{S_j,E_l}\sqrt{E_S}d_{S_j,E_l}^{-\alpha}x_k^{(S_j)} + \sum_{S_i\in\mathcal{S}_1, i\neq j} h_{S_i,E_l}\sqrt{E_S}d_{S_i,E_l}^{-\alpha}x_k^{(S_i)} + n_k^{(E_l)}$$

B. Analysis

Relay selection only depends on the multi-path fading of the links between sources and relays. Thus from Lemma 3.2, the probability that exactly one relay is selected is greater than $\frac{1}{e} > 0$. Consequently, a positive fraction of nodes can always convey messages. Denote the number of such nodes by $N_1 = |\mathcal{S}_1|$. Furthermore, from Lemmas 3.2 and 4.1 we have $\frac{k_1\log N}{8et} < N_1 < \frac{27k_1\log N}{8et}$.

Recall from the previous section that $P_{OUT}^{(S_j\to R_j)}$ is the probability that the SINR from a given source S_j to its corresponding relay R_j is less than γ. For each active cell C, $P_{OUT}^{(E)}$ is the probability of the event that the SINR at none of the eavesdropper nodes inside a square region A, centered at C and of side $\Delta\sqrt{N}$ (Figure 3) from any of the sources exceeds the required SINR for eavesdroppers, γ_E.

The following theorem characterizes an achievable number of eavesdroppers that the network can tolerate.

Theorem 4.1. Consider the general case with legitimate and eavesdropper nodes placed uniformly and randomly at unknown locations on the square region A. For the proposed protocol, $m(N)$ eavesdroppers can be tolerated while guaranteeing $P_{OUT}^{(S_j\to R_j)} \to 0$ for each source S_j and $P_{OUT}^{(E)} \to 1$ as $N\to\infty$, if:

$$m(N) = o\left(\frac{N^{\frac{\log(1+\gamma_E 2^{-\alpha})}{8et}}}{\log N}\right).$$

Proof: Consider the active sub-cell c_i within C. As mentioned earlier, we denote the group of active nodes in c_i by $\mathcal{S}_1$ and the nodes in $\mathcal{S}_1$ by $S_j, j = 1,...,N_1$. We denote the corresponding messaging relay for source S_j in the neighbor cell C' by R_j. Consider the SINR at each messaging relay:

$$C_{S_j,R_j} = \frac{E_S.|h_{S_j,R_j}|^2 d_{S_j,R_j}^{-\alpha}}{\sum_{S_i\in\mathcal{S}_1, i\neq j} E_S.|h_{S_i,R_j}|^2 d_{S_i,R_j}^{-\alpha} + N_0/2}$$

From Lemma 3.3 with $a = 1$, $|h_{S_j,R_j}|^2 > \frac{\log(3/8N)}{\sqrt{2}}$; thus, $|h_{S_j,R_j}|^2 > \frac{\log N}{2}$ as $N\to\infty$.

Now consider the denominator. For each pair of nodes $S_i \in \mathcal{S}_1$ and R_j, $d_{S_i,R_j} > \frac{\sqrt{N}}{4} \gg 2\sqrt{k_1\log N}$, then we can assume $d_{S_i,R_j} \approx d_{i,j}$, where $d_{i,j}$ is the distance between sub-cell c_i and relay R_j. By the weak law of large numbers, $\sum_{S_i\in\mathcal{S}_1}|h_{S_i,R_j}|^2 < 2N_1$; using Lemmas 3.2 and 4.1, $\sum_{S_i\in\mathcal{S}_1}|h_{S_i,R_j}|^2 < \frac{9k_1\log N}{2et}$ as $N\to\infty$. Furthermore, the noise term in the denominator is constant while the interference grows as N gets large; thus,

$$\begin{aligned} C_{S_j,R_j} &> \frac{E_S.\log(3/8N)d_{i,j}^{-\alpha}}{2.\sum_{S_i\in\mathcal{S}_1} E_S.|h_{S_i,R_j}|^2 d_{i,j}^{-\alpha}} \\ &> \frac{\log N/2}{9k_1\log N/et} \\ &> \gamma \quad \text{as} \quad N\to\infty \end{aligned}$$

w.h.p. provided $t > \frac{18k_1\gamma}{e}$. Consequently, $P_{OUT}^{(S_j,R_j)} \to 0$ as $N\to\infty$.

Now consider the eavesdroppers. For each source S_j, using the union bound for the eavesdroppers in the region A:

$$\begin{aligned} P_{OUT}^{(S_j\to E)} &= 1 - P\left(\bigcup_{l=1}^{m(N)}\{C_{S_j,E_l}\geq\gamma_E\}\right) \\ &\geq 1 - \sum_{l=1}^{m(N)} P(C_{S_j,E_l}\geq\gamma_E) \end{aligned}$$

Assume that sub-cell c_i is active. Considering the eavesdropper E_l, based on its location, we have:

$$\begin{aligned} P(C_{S_j,E_l}\geq\gamma_E) &= P(C_{S_j,E_l}\geq\gamma_E|E_l\in A_1)P(E_l\in A_1) \\ &+ P(C_{S_j,E_l}\geq\gamma_E|E_l\in A_2)P(E_l\in A_2) \\ &+ P(C_{S_j,E_l}\geq\gamma_E|E_l\in A_3)P(E_l\in A_3) \end{aligned}$$

where $A = A_1\cup A_2\cup A_3$, and: A_1 is the circle that is circumscribed around the sub-cell c_i, A_2 is the annulus with the same center with inner radius $\sqrt{\frac{c(N)}{2}}$ and outer radius $3\sqrt{\frac{c(N)}{2}}$ and A_3 is the area of A minus $A_1 + A_2$ (Figure 3).

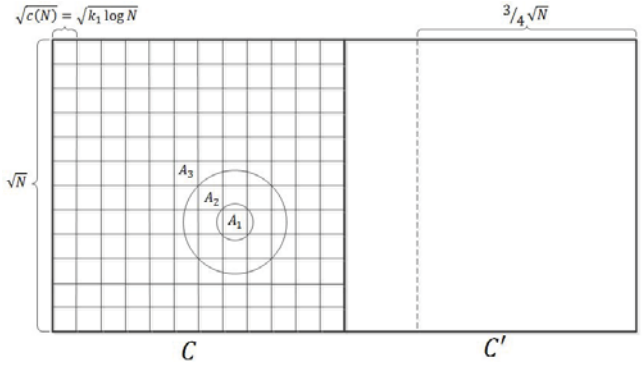

Fig. 3. Two adjacent cells C and C'. During each time period, the nodes in one sub-cell of cell C choose nodes from area $[\frac{\sqrt{N}}{4},\sqrt{N}]\times[0,\sqrt{N}]$ of C' and transmit their messages to them.

Then:

$$\begin{aligned}&P(C_{S_j,E_l} \geq \gamma_E)\\&< 1.\frac{\pi c(N)}{2\Delta^2 N}\\&+ 1.\frac{4\pi c(N)}{\Delta^2 N}\\&+ P(C_{S_j,E_l} \geq \gamma_E | E_l \in A_3)\frac{\Delta^2 N - 4.5\pi c(N)}{\Delta^2 N}\end{aligned}$$

Thus, we have to bound $P(C_{S_j,E_l} \geq \gamma_E | E_l \in A_3)$:

$$\begin{aligned}&P(C_{S_j,E_l} \geq \gamma_E | E_l \in A_3)\\&= P\left(\frac{E_S.|h_{S_j,E_i}|^2 d_{S_j,E_l}^{-\alpha}}{\sum_{S_i \in \mathcal{S}_1} E_S.|h_{S_i,E_l}|^2 d_{S_i,E_l}^{-\alpha} + {N_0}/{2}} \geq \gamma_E | E_l \in A_3\right)\end{aligned}$$

In the denominator of the SINR, removing the noise benefits the eavesdropper. Also, the distance of the interfering sources to the eavesdropper is less than the distance of the closest source to the eavesdropper plus the diagonal of the sub-cell. In addition, recall that the multi-path fading of different links is independent. Given that the nodes in the group $\mathcal{S}_1$ are transmitting:

$$\begin{aligned}&P(C_{S_j,E_l} \geq \gamma_E | E_l \in A_3)\\&= P\Big(\frac{E_S.|h_{S_j,E_l}|^2 d_{S_j,E_l}^{-\alpha}}{\sum_{S_i \in \mathcal{S}_1} E_S.|h_{S_i,E_l}|^2 d_{S_i,E_l}^{-\alpha} + {N_0}/{2}} \geq \gamma_E | E_l \in A_3\Big)\\&< P\Big(\frac{E_S.|h_{S_j,E_l}|^2 d_{S_j,E_l}^{-\alpha}}{\sum_{S_i \in \mathcal{S}_1} E_S.|h_{S_i,E_l}|^2 d_{S_i,E_l}^{-\alpha}} \geq \gamma_E | E_l \in A_3\Big)\\&< P\Big(\frac{|h_{S_j,E_l}|^2 d^{-\alpha}}{\sum_{S_i \in \mathcal{S}_1} |h_{S_i,E_l}|^2 (d + \sqrt{2c(N)})^{-\alpha}} \geq \gamma_E | d > \sqrt{2c(N)}\Big)\\&< E_{\{|h_{S_i,E_l}|^2, S_i \in \mathcal{S}_1\}}\Big[P(|h_{S_j,E_l}|^2 \geq \gamma_E . \sum_{S_i \in \mathcal{S}_1} |h_{S_i,E_l}|^2 2^{-\alpha})\Big]\\&= E_{\{|h_{S_i,E_l}|^2, S_i \in \mathcal{S}_1\}}\Big[e^{-\gamma_E . \sum_{S_i \in \mathcal{S}_1} |h_{S_i,E_l}|^2 2^{-\alpha}}\Big]\\&= \prod_{S_i \in \mathcal{S}_1} E_{\{|h_{S_i,E_l}|^2\}}\Big[e^{-\gamma_E 2^{-\alpha} . |h_{S_i,E_l}|^2}\Big]\\&= \left(\frac{1}{1 + \gamma_E . 2^{-\alpha}}\right)^{|\mathcal{S}_1|}\end{aligned}$$

From Lemmas 3.2 and 4.1, the number of transmitting nodes $N_1 = |\mathcal{S}_1| > \frac{k_1 \log N}{8et}$. Then,

$$\begin{aligned}&P_{OUT}^{(S_j \to E)}\\&\geq 1 - \sum_{i=1}^{m(N)} \left[\frac{4.5\pi \log N}{t\Delta^2 N} + \left(\frac{1}{1 + \gamma_E . 2^{-\alpha}}\right)^{k_1 \log N / 8et}\right]\end{aligned}$$

Using the union bound again, considering that at most $\frac{27 \log N}{8et}$ sources transmit at the same time (Lemma 4.1), an achievable number of eavesdroppers in the region A that cannot intercept the message from any of the sources, as $N \to \infty$, is:

$$\begin{aligned}m(N) &= o\left(\frac{(1 + \gamma_E 2^{-\alpha})^{\frac{k_1 \log N}{8et}}}{\log N}\right)\\&= o\left(\frac{N^{\frac{k_1 \log (1 + \gamma_E 2^{-\alpha})}{8et}}}{\log N}\right).\end{aligned}$$

■

V. Discussion

(a) *Comparison to previous works*: The local region approach taken here, in contrast to the global approach taken in [25], has an impact on various convergences (e.g. the occupancy result in Lemma 4.1 has not been shown to hold uniformly across all sub-cells of the entire network), and hence one needs to be careful in making definitive direct comparisons despite the similarity in form of a number of the results. Furthermore, when considering the achievable number of eavesdroppers $o((\log n)^{c_1}),\ c_1 > 0$, from [25] for the same cell size considered here, it is apparent that the value of c_1, which was not bounded tightly in [25], is critical to the comparison. Improving this comparison by establishing bounds on the value of c_1 and putting both pieces of work in the same mathematical framework is currently under consideration. In performing this comparison, it is important to note that the approach considered here is both more power efficient and allows for the simultaneous transmission of $\log \log n$ transmitters at the considered cell size.

(b) *Motivating the finite case*: The approach proposed in this paper to physical layer secrecy is also of interest in the finite case. Suppose we have a finite number of nodes in a given area with multiple source-destination pairs among them. By a careful routing and scheduling of flows in the network, the aggregate signals of the flows can be employed to help keep each flow secret from external eavesdroppers while the interference does not destroy the communication between sources and destinations. This is currently under consideration.

VI. Conclusion

In this paper, we employ cooperative transmission and relay nodes to improve secrecy. We first consider a scenario of equal path-loss between all pairs of nodes. A protocol for two-hop communication between a large number of source-destination pairs via one relay for each pair is proposed. It is shown that in this scenario that any $m(n) = o\left(\frac{n^{\frac{\log (1+\gamma_E)}{2et}}}{\log n}\right)$ number of eavesdroppers can be tolerated, where n is the number of system nodes, α is the path-loss exponent, γ_E is the required SINR threshold at each eavesdropper, and t is a constant.

Next, for the general case, we consider the local analysis of a multi-hop strategy in an extended network. In particular, we tessellate the network into small square cells and propose a protocol for communication between two neighboring cells.

In this case, it is shown that $m(N) = o\left(\frac{N^{\frac{\log(1+\gamma_E 2^{-\alpha})}{8et}}}{\log N}\right)$ eavesdroppers inside and around each cell can be tolerated, where N is roughly the number of nodes in each cell and t is a constant different from that employed above.

In contrast to [25], the energy efficiency is improved. In particular, the energy that chattering nodes employ to generate artificial noise in [25] can be more than the energy employed to transmit the message. Here, all the energy is used to transmit messages and hence there is no extra energy required to obtain secrecy. Furthermore, by using the proposed protocol, a large number of nodes share the same bandwidth simultaneously and achieve a higher bandwidth efficiency.

APPENDIX

We denote the out-cell interference from the transmission of nodes in other active cells at relay R_j by $I_{out}^{R_j}$. Then,

$$I_{out}^{R_j} < \sum_{l=1}^{\infty} \sum_{S\in\mathcal{S}_l} E_s.(\Delta\sqrt{N}l)^{-\alpha}|h_{S,R_j}|^2$$
$$= E_S.(\Delta\sqrt{N})^{-\alpha}.\sum_{l=1}^{\infty} l^{-\alpha} \sum_{S\in\mathcal{S}_l} |h_{S,R_j}|^2$$

In each active cell we know that $N_1 < \frac{27\log N}{8et}$ nodes are transmitting. Also, the number of concentric transmitting cells at the distance $l\Delta\sqrt{N}$ is $8l$; then, the number of nodes transmitting from distance $l\Delta\sqrt{N}$ simultaneously: $|\mathcal{S}_l| < \frac{27l\log N}{et}$. Using the law of large numbers $\sum_{S\in\mathcal{S}_l}|h_{S,R_j}|^2 < \frac{27\sqrt{2}l\log N}{et}$. Besides, $\sum_{l=1}^{\infty} l^{-\alpha+1}$ converges to some constant k for $\alpha > 2$; hence,

$$I_{out}^{R_j} < \frac{27\sqrt{2}E_S k}{et\Delta^{\alpha}}\frac{\log N}{N^{\alpha/2}} \to 0 \quad \text{as} \quad N\to\infty.$$

REFERENCES

[1] D. Stinson, *Cryptography: theory and practice*. CRC press, 2006.

[2] C. Shannon, *Communication theory of secrecy systems*. AT & T, 1949.

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

[4] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

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

[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference, 2005*, vol. 62, no. 3, p. 1906.

[7] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *IEEE Military Communications Conference, MILCOM 2005*, pp. 1501–1506.

[8] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE Workshop on Statistical Signal Processing*, 2009, pp. 417–420.

[9] E. Tekin, "The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *IEEE Information Theory and Applications Workshop, 2007*, pp. 404–413.

[10] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[11] I. Krikidis, J. Thompson, P. Grant, and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in *GLOBECOM Workshops , 2010*, pp. 1177–1181.

[12] R. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *International Symposium on Information Theory, ISIT 2008*, pp. 374–378.

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

[14] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference-assisted secret communication," in *Information Theory Workshop, ITW 2008*, pp. 164–168.

[15] O. Koyluoglu and H. El Gamal, "On the secrecy rate region for the interference channel," in *International Symposium on Personal, Indoor and Mobile Radio Communications, 2008*, pp. 1–5.

[16] M. Haenggi, "The secrecy graph and some of its properties," in *International Symposium on Information Theory, ISIT 2008*, pp. 539–543.

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

[18] ——, "Wireless physical-layer security: The case of colluding eavesdroppers," in *International Symposium on Information Theory, ISIT 2009*, pp. 2442–2446.

[19] ——, "Techniques for enhanced physical-layer security," *Arxiv preprint arXiv:1008.3705*, 2010.

[20] P. Pinto and M. Win, "Continuum percolation in the intrinsically secure communications graph," in *International Symposium on Information Theory and its Applications, ISITA 2010*, pp. 349–354.

[21] S. Goel, V. Aggarwal, A. Yener, and A. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *International Symposium on Information Theory Proceedings, ISIT 2010*, pp. 2627–2631.

[22] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Asilomar Conference on Signals, Systems and Computers, 2010*, pp. 42–46.

[23] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of manets with malicious nodes," in *International Symposium on Information Theory Proceedings, ISIT 2009*, pp. 1189–1193.

[24] O. Koyluoglu, E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," in *Information Theory and Applications Workshop (ITA), 2010*, pp. 1–4.

[25] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM international symposium on Mobile ad hoc networking and computing*, 2010, pp. 21–30.

[26] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *INFOCOM 2012*.

[27] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 2067–2076, 2011.

[28] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.

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

[30] S. Toumpis and A. Goldsmith, "Large wireless networks under fading, mobility, and delay constraints," in *INFOCOM 2004*, vol. 1.