Secret Communication in Large Wireless Networks without Eavesdropper Location Information

Cagatay Capar*, Dennis Goeckel*, Benyuan Liu†, and Don Towsley*
* University of Massachusetts Amherst, Amherst, MA, 01003
† University of Massachusetts Lowell, Lowell, MA, 01854

***Abstract*—We present achievable scaling results on the per-node secure throughput that can be realized in a large random wireless network of n legitimate nodes in the presence of m eavesdroppers of unknown location. We consider both one-dimensional and two-dimensional networks. In the one-dimensional case, we show that a per-node secure throughput of order $1/n$ is achievable if the number of eavesdroppers satisfies $m = o(n/\log n)$. We obtain similar results for the two-dimensional case, where a secure throughput of order $1/\sqrt{n \log n}$ is achievable under the same condition. The number of eavesdroppers that can be tolerated is significantly higher than previous works that address the case of unknown eavesdropper locations. The key technique introduced in our construction to handle unknown eavesdropper locations forces adversaries to intercept a number of packets to be able to decode a single message. The whole network is divided into regions, where a certain subset of packets is protected from adversaries located in each region. In the one-dimensional case, our construction makes use of artificial noise generation by legitimate nodes to degrade the signal quality at the potential locations of eavesdroppers. In the two-dimensional case, the availability of many paths to reach a destination is utilized to handle collaborating eavesdroppers of unknown location.**

I. Introduction

Consider the transmission of a message from one party (Alice) to another (Bob), such that it is kept secret from an eavesdropping adversary (Eve). Cryptographic solutions assume that Eve will intercept the transmitted signal cleanly but impose a hard mathematical problem on Eve that is beyond her computational power to solve. Information-theoretic solutions do not rely on computational assumptions, but exploit the relative signal quality achieved at Bob compared to Eve. Specifically, if the signal quality is better at Bob than it is at Eve, a number of secret bits can be delivered to Bob [1] that is a function of the difference in signal qualities. Whether information-theoretic or cryptographic secrecy is employed in a system, there is utility in enhancing reception by the desired party while inhibiting reception by eavesdroppers. For information-theoretic security, the need is apparent, since a positive secrecy capacity relies on such. From the viewpoint of cryptographic security, inhibiting Eve's reception of the encrypted signal can be used to hide its existence or characteristics, or may be part of a defense-in-depth approach to information security. Hence, here we consider constructions that achieve a high signal quality at system nodes while providing a low signal quality to potential eavesdroppers. If a given high signal-to-interference-plus-noise ratio (SINR) threshold is exceeded at the system nodes while the eavesdroppers are unable to achieve a given (lower) SINR threshold, the communication will be deemed secret.

Here, we consider the secrecy problem in large wireless networks, both in the one-dimensional (1-D) and the two-dimensional (2-D) cases. 2-D networks are used for modeling nodes distributed to an open region, while 1-D networks are more suitable for nodes confined to a linear structure like valleys or highways [2]. In this paper, we are interested in the amount of information that can be carried by n (legitimate) nodes in a network while being kept secret from m eavesdroppers also present in the network. This problem can be seen as a security extension of the original problem of capacity scaling in large wireless networks [3], where an achievable per-node throughput that scales as $O(1/\sqrt{n \log n})$ is shown for a 2-D random network of n nodes. Since then, different strategies for achieving similar scaling results and also upper bounds on the capacity have been shown [4], [5]. When considering secrecy in large networks, the ability of network nodes to be securely *connected* (i.e., without any constraint on the throughput value) is studied under the framework of the *secrecy graph* [6], [7]. The scaling of secrecy throughput in a network with mobile nodes is studied in [8] using a one-hop transmission scheme [9]. The secrecy capacity scaling with static nodes, as assumed in this paper, is studied in [10], where it is shown that if the eavesdropper locations are known, the eavesdroppers can be effectively routed around, and a secure per-node throughput of order $(1/\sqrt{n})$ is feasible as long as the number of eavesdroppers in the network is $o(n/(\log n)^2)$. The case of eavesdroppers of unknown location is addressed in [11], where it is shown that a secure throughput on the order of $(1/\sqrt{n \log n})$ is achieved if the number of eavesdroppers is on the order of $(\log n)^c$, for some $0 < c < 1$. The construction in [11] uses artificial noise generation by legitimate nodes to degrade the signal quality at the potential eavesdropper locations, and uses a multi-user diversity effect exploiting the fading characteristics of the wireless channel. A similar construction using concurrent transmissions in the network as noise instead of artificial noise generation is studied in [12], while [13] addresses the secrecy capacity problem under a different, outage-based formulation. Secrecy problem has also been studied for small networks such as a single source-destination pair with a number of relays [14], [15], [16].

A common assumption in most of the previous works in secrecy scaling is that the locations of the eavesdroppers are

known. However, this assumption is highly undesirable especially for passive eavesdroppers [17]. In this paper, we address the issue of unknown eavesdropper locations by requiring each source node to generate multiple "packets" for a single message such that the message can only be decoded if all packets are received, and no information about the message can be gained if even only one of the packets is missing [18], [19]. These packets are sent in separate transmissions such that each packet is delivered to the destination but kept secure from potential eavesdroppers in a certain region of the network. Therefore, an eavesdropper anywhere in the network is guaranteed to miss some non-empty subset of the packets, and hence cannot decode the message. In the two-dimensional case, this is done by sending each packet on a different path, and maintaining sufficient separation between paths. In other words, the "path diversity" available in the network is utilized [20] to provide resilience against the lack of knowledge of the eavesdropper locations. From a graphical view, the eavesdropper has access to only a subset of the edges connecting the source-destination pair, hence it is possible to deliver secret bits by doing secret sharing at the source node and sending the pieces over different edges [21], [18]. In the one-dimensional case, only a single path exists between a source-destination pair, hence the one-dimensional network itself is partitioned into segments, where each packet is kept secure from eavesdroppers located in its corresponding segment.

We assume only path loss for the wireless channel, which means when a message is transmitted, it cannot be securely received by another legitimate node if an eavesdropper is closer to the transmitter compared to the receiver, since in that case, the SINR condition for secrecy cannot be satisfied. This makes achieving secret communication in the one-dimensional case especially challenging, since an eavesdropper located on a point on the line blocks any communication that has to be securely routed through this point. Therefore, even a single eavesdropper causes secret communication between all legitimate nodes in the network to be impossible, resulting in zero secure throughput. In our paper, we make use of the fact that enabling *cooperative jamming* makes secret communication possible in the one-dimensional network [22]. In cooperative jamming [15], [23], a legitimate node transmits artificial noise to degrade the signal quality at the potential nearby eavesdroppers. However, a legitimate node located far away from the jammer node can still achieve the required SINR, hence the transmission can "jump over" the eavesdroppers near the jammer to reach its destination. We present a construction that utilizes cooperative jamming to keep packets secure from eavesdroppers located in the corresponding segment. If the number of eavesdroppers satisfies $m(n) = o(n/\log n)$, with this construction, almost all source-destination pairs achieve secure throughput of order $(1/n)$ with high probability, i.e., with probability one as the number of nodes n goes to infinity.

In the two-dimensional case, a fundamental advantage is the availability of many paths connecting a single source-destination pair. We present a construction that utilizes this path diversity and the fact that an eavesdropper cannot decode the packets that are transmitted over far-away paths. Using our construction, we show that in a two-dimensional network of n nodes, source-destination pairs can achieve a secure throughput on the order of $(1/\sqrt{n \log n})$ if the number of eavesdroppers satisfies $m(n) = o(n/\log n)$. Furthermore, the throughput remains secure up to any constant number of eavesdroppers collaborating by combining their received packets. Note that cooperative jamming is not used in the construction in the two-dimensional case since the eavesdroppers with some minimum distance to a path cannot achieve the SINR threshold. However, this assumes a certain minimum noise level in the eavesdropper receivers, which may not be a desirable assumption in all cases. This can be avoided by using cooperative jamming for the transmissions on the paths, so that a noise floor is established at the potential eavesdroppers regardless of the quality of their receivers.

The rest of the paper is organized as follows. We describe the network and channel models in the next section, which are used in our main results presented in Section III for the 1-D networks, and in Section IV for the 2-D case. A number of issues relevant to our results is discussed in Section V. Section VI is the conclusion.

II. Model

A. Network and Channel Model

The wireless network is composed of legitimate nodes and eavesdroppers inside the interval $[0, n]$ in the one-dimensional case, and inside the square region $[0, \sqrt{n}] \times [0, \sqrt{n}]$ in the two-dimensional case. Legitimate nodes are distributed according to a homogeneous Poisson point process with intensity $\lambda = 1$. All nodes are assumed to be static. Legitimate nodes are matched into source-destination pairs uniformly at random, such that each node is the destination of exactly one source node, and the source for exactly one destination node. For each pair, we associate a *stream* of information that needs to flow from the source to the destination. Eavesdroppers are assumed to be passive, and in the one-dimensional case, operating independently of each other, i.e., they do not collaborate by sharing their observations.

Only path loss is assumed for the wireless channels between transmitter and receiver nodes. Hence, whenever a node A transmits with some transmit power P, the received power at node B is modeled as

$$P_{\text{rcv},B} = P/d_{AB}^{\alpha},$$

where d_{AB} is the distance between nodes A, B, and $\alpha > 1$ in 1-D, $\alpha > 2$ in 2-D, is the path loss exponent. This model may be appropriate for a wideband system where fading is averaged out due to frequency diversity, or an environment without significant multipath effects. The case of fading is further discussed in Section V.

We adopt a threshold model here, as motivated for both practical and information-theoretic security in [14]. Thus, we assume a message is successfully decoded if the received

signal-to-interference-plus-noise ratio (SINR) exceeds a certain threshold $\gamma > 0$. In other words, node B successfully decodes node A's message if

$$\text{SINR}_B \triangleq \frac{P_{\text{rcv},B}}{N_0 + I_B} > \gamma, \tag{1}$$

where N_0 is the power in the additive white Gaussian noise (AWGN) at the receiver, and I_B is the interference received at node B due to other transmissions in the network. In our case, this interference may be due to other legitimate signal transmissions and/or artificial noise generated by legitimate nodes.

As mentioned above, for a message to be *securely* received at B in the presence of an eavesdropper E, we require the SINR at the eavesdropper SINR_E to be smaller than SINR_B. Furthermore, it may be desirable to have some positive *SINR gap* between nodes B and E. Hence, for some γ_e such that $0 < \gamma_e < \gamma$, in our model, we require $\text{SINR}_E < \gamma_e$, where γ_e can be selected to be arbitrarily small. Note that, from an information-theoretic secrecy perspective, this also allows choosing some positive secrecy rate R_s given as [24]

$$R_s = \frac{1}{2}\big(\log(1+\text{SINR}_B) - \log(1+\text{SINR}_E)\big).$$

Therefore, for some region $\mathcal{R}$ in the network, a message is decoded by B while being secret from eavesdroppers inside $\mathcal{R}$ if (1) $\text{SINR}_B > \gamma$, and (2) any eavesdropper E inside $\mathcal{R}$ has $\text{SINR}_E < \gamma_e$. For multi-hop transmission from a source node to a destination node, if this SINR condition is satisfied at every hop, we refer to the rate of information as the *secure throughput* achieved by this pair. Note that secrecy at each hop over a multi-hop path is shown to be sufficient for end-to-end secrecy in [10].

B. Performance Metrics

The network carries information streams to be delivered from the source nodes to their respective destinations. We consider the network's ability to carry these streams at a certain per-node throughput in the presence of eavesdroppers. Our performance metric is the number of eavesdroppers that can be tolerated while legitimate nodes maintain some *secure* throughput with high probability (w.h.p.), i.e., with probability one as the size of the network, n, goes to infinity.

III. One-dimensional Networks

The following theorem establishes security in the absence of eavesdroppers near the source-destination nodes, which is then used in Theorem 2 to establish the number of eavesdroppers that can be tolerated.

Theorem 1: Consider the one-dimensional network inside the interval $[0, n]$, where the eavesdroppers are arbitrarily distributed. The locations of the eavesdroppers are unknown, and they are assumed not to collaborate. Legitimate nodes can maintain a throughput of $\Theta\big(1/n\big)$ w.h.p. for all source-destination pairs, for any number of eavesdroppers. For some fixed positive constant r, the throughput achieved is secure for the source-destination pairs that satisfy the condition that no eavesdropper is placed within a distance $r \log n$ to the source and to the destination node.

Overview of the Proof

We prove Theorem 1 by providing a construction summarized by the following steps:

1) In order to handle unknown eavesdropper locations, we partition the network into a finite number t of interlaced regions $\{\Gamma_i, i = 1, \cdots, n\}$. We refer to this partitioning as "coloring" the network, and treat each region (color) one by one, assuming each time that eavesdroppers are all confined to that particular region.
2) For each message to be delivered to the destination node, the source node generates t "packets". These packets are generated in a way that ensures the message cannot be decoded by a node unless all t packets are successfully received. Packets are delivered in separate transmissions such that the i-th packet is protected from eavesdroppers in Γ_i, thus guaranteeing that an eavesdropper located anywhere in the network misses at least one of the t packets.
3) We provide an algorithm that routes packets from source to destination in a multi-hop fashion, and ensures each packet is kept secure from potential eavesdroppers inside its corresponding region at each hop. This is achieved by legitimate nodes inside the region acting as "jammers" by transmitting random noise to prevent eavesdroppers in that region from decoding the packet.
4) We use time division multiplexing, where time is considered as a sequence of "periods". Each period consists of t "frames", and packets corresponding to color $i, i \in \{1, 2, \cdots, t\}$, are transmitted in the ith frame. Each frame is further divided into slots, where a standard spatial reuse scheme (as in [3]) is employed.

The proof is completed by showing that this construction achieves the stated throughput properties w.h.p.

Proof:

Our construction is given in detail in the following. This construction is then proved to achieve a per-node secure throughput of $\Theta\big(1/n\big)$ w.h.p. for the source-destination pairs with no very nearby eavesdroppers.

A. Coloring the Network

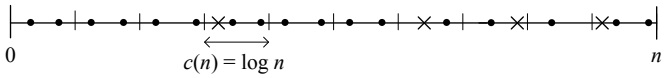

Fig. 1. The one-dimensional network consists of legitimate nodes (represented by dots) and eavesdroppers (represented by crosses) placed in the interval $[0, n]$, divided into cells of length $c(n) = \log n$, as part of the signaling construction.

We divide $[0, n]$ into sub-intervals referred to as "cells", each of length $c(n) = \log n$ (Fig. 1). Let $s_i(n)$ denote the ith cell, $i = 1, \cdots, n/\log n$, with $s_1(n) = [0, \log n]$.

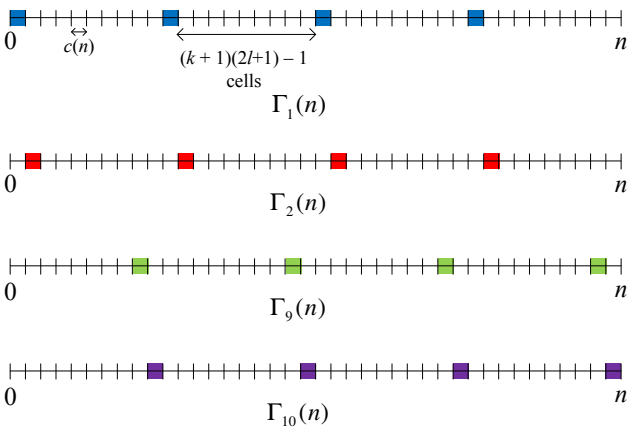

Fig. 2. The network is partitioned into regions (colors), where each region is a collection of cells regularly sampled in the linear grid. Cells in a region are spaced $(k+1)(2l+1)-1$ cells apart ($k=1$, $l=2$ in the figure). Hence, the network consists of $t=(k+1)(2l+1)$ regions ($t=10$ in the figure). The network is shown here with four of those 10 different regions highlighted.

We partition these cells into non-overlapping subsets, which we refer to as "coloring" the network. Specifically, we divide the network into $t=(k+1)(2l+1)$ regions (colors), where $k \geqslant 1$ and $l \geqslant 2$ are integers to be defined later. Denote the collection of regions as:

$$\{\Gamma_i(n), i=1,2,\cdots,t\}$$

Each region is a collection of non-contiguous cells regularly sampled in the grid as shown in Fig. 2. Specifically, cells in $\Gamma_i(n)$ are spaced $t-1$ cells apart. In other words,

$$\Gamma_i(n) \triangleq \bigcup_{j=1}^{\frac{n/\log n}{t}} s_{i+(j-1)t}(n). \tag{2}$$

For convenience, we denote the j-th cell of region $\Gamma_i(n)$ as $\mathcal{C}_i^j(n)$. In other words,

$$\mathcal{C}_i^j(n) \triangleq s_{i+(j-1)t}(n).$$

The whole network is the union of the t regions:

$$[0,n] = \bigcup_{i=1}^{t} \Gamma_i(n)$$

Note that the number of regions t is independent of the size of the network n.

We refer to $\Gamma_i(n)$ and each of its cells $\mathcal{C}_i^j(n)$ as belonging to the i-th color. Also, we use the notation $\Gamma_i, \mathcal{C}_i^j$ in what follows, keeping in mind that the number of cells in a region, and the cell sizes depend on n. As will be clear in the description of the routing algorithm, the cells in a region can be thought of as potential locations of eavesdroppers corresponding to that region. For each cell $\mathcal{C}_i^j$, we define an interval called the "neighborhood" of this cell, and denote it by $N(\mathcal{C}_i^j)$. This neighborhood consists of $(2l+1)$ cells, with $\mathcal{C}_i^j$ being the middle cell (Fig. 3). These neighborhoods are separated by $k(2l+1)$ cells.

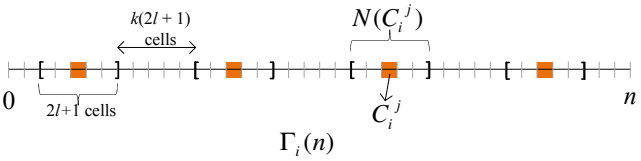

Fig. 3. The network is shown with one region Γ_i highlighted as done in Fig. 2. $\mathcal{C}_i^j$ denotes the jth cell in region Γ_i. Around each cell, the "neighborhood" of that cell $N(\mathcal{C}_i^j)$ is defined as the interval with $(2l+1)$ cells ($l=2$ above). So, neighborhoods are separated by $k(2l+1)$ cells ($k=1$ above).

It is also useful to define the "periphery" and the "interior" of a neighborhood. We define the *periphery* of $N(\mathcal{C}_i^j)$ as the two cells at the two ends of the neighborhood, and the *interior* of $N(\mathcal{C}_i^j)$ as the smaller interval that consists of $(2l-1)$ cells centered at $\mathcal{C}_i^j$.

For any source-destination pair $S-D$, let w be the b-bit message to be delivered from S to D. S generates $(t-1)$ random b-bit packets $w_1,\cdots,w_{t-1}$ and then sets w_t such that the message w satisfies

$$w = w_1 \oplus w_2 \oplus \cdots \oplus w_t, \tag{3}$$

where $\oplus$ denotes bit-wise XOR operation. We refer to packet w_i as belonging to the i-th color. The basic idea is that w_i is transmitted such that it is *protected* from eavesdroppers located in Γ_i. Note that any node that receives all t packets can compute w, while any node that misses one or more packets acquires no information about w.

B. Routing Algorithm

For the transmission of a packet of any color i from a source node S to its destination node D, S transmits the packet to a relay in the next cell on the route. Each relay that receives the packet does the same until the packet reaches the first neighborhood $N(\mathcal{C}_i^j)$ on the route. Inside $N(\mathcal{C}_i^j)$, we assign two nodes to act as relays, and one node to act as a jammer: A relay node A is selected from the cell where the route enters $N(\mathcal{C}_i^j)$, a jammer node J is selected from $\mathcal{C}_i^j$, and a relay node B is selected from the cell at the end of neighborhood (Fig. 4 (b)). A receives the message from outside the neighborhood, and then transmits to B while J transmits random noise. Therefore, inside a neighborhood, the message is transmitted across a number of cells in one slot. A jammer is only active when there is a transmission inside its corresponding neighborhood. Therefore, each packet is carried in a repeating sequence of single-cell hops followed by one multi-cell hop until it reaches D (Fig.4 (a)). When D receives all t packets, it decodes the message by performing the operation in (3).

Note that packets of color i are routed in a way that prevents it from entering the interiors of neighborhoods $N(\mathcal{C}_i^j)$, except possibly at the start or the end of the route. To see this, consider a source node S inside $\mathcal{C}_i^j$. S will generate a packet

w_i of color i. This packet is first routed in single-cell hops, and follows the above scheme only after it reaches outside $N(\mathcal{C}_i^j)$. Similarly, deliveries to destination nodes inside neighborhoods are also done in a sequence of single-cell hops (see Fig. 4 (a)).

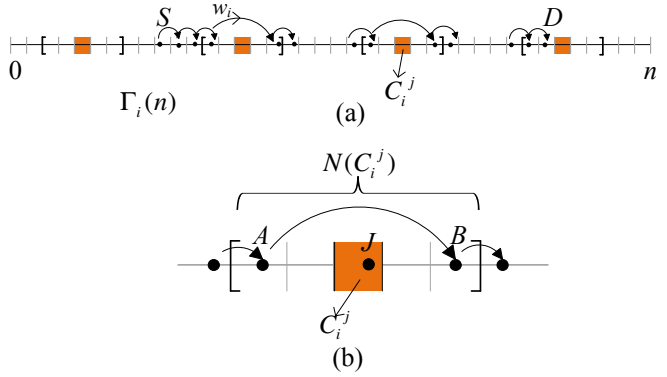

Fig. 4. (a) The route followed by a packet w_i from a source node S to a destination node D is shown. At each hop, the packet is delivered to the next cell on the route except inside the neighborhoods, $N(\mathcal{C}_i^j)$, where the packet is transmitted such that it reaches over multiple cells at once. (b) Inside $N(\mathcal{C}_i^j)$, a transmitting relay A in the first cell transmits to a receiving relay B in the last cell, while a jammer node J in $\mathcal{C}_i^j$ transmits artificial noise. Hence, packets of color i are routed in a way that avoids entering the interiors of neighborhoods $N(\mathcal{C}_i^j)$. The only exception is possibly at the start or the end of the route, as the source or the destination node may be located inside the interior of a neighborhood (destination node D is inside the interior of a neighborhood in (a)).

C. Time Division Multiplexing Scheme

Time is divided into a sequence of "periods". In the i-th frame, only packets belonging to the i-th color are transmitted. In each frame, a spatial reuse scheme is employed such that in the i-th frame, every cell in the network transmits a packet of color i once. This is done by further dividing each frame into t time slots. In each slot, transmitting cells are $t-1$ cells apart (see Fig. 5). During the i-th frame, jammer nodes inside Γ_i become active only in the time slots where multiple-cell hops take place.

The throughput achieved per stream is constrained due to the fact that streams arriving to a cell take turns being relayed. Each cell has to relay information for at most a constant factor of n streams w.h.p., hence a throughput of $\Theta\big(1/n\big)$ per stream is achieved w.h.p.

In order to consider the secrecy of the achieved throughput, note that the route of a packet contains the following types of hops: (1) single-cell hop outside neighborhoods, (2) multiple-cell hop inside a neighborhood, (3) single-cell hop inside a neighborhood if it contains either the source or destination (see Fig. 4 (a)). In Appendix I, we show that the first two types of hops are achieved securely. We show that there exist constants k, l for coloring the network, and transmit power values for relays and jammer nodes, such that for any stream of color i, the destination node and the eavesdroppers inside Γ_i satisfy the SINR requirement for secure transmission for these hops. Hence, the only possible insecure transmissions are in the close proximity of the source and destination nodes (i.e., the third type above). For a source-destination pair, if no eavesdropper is within a distance $rc(n)$, $r = l$, to the source and to the destination, then these hops will also be secure, hence the result follows.

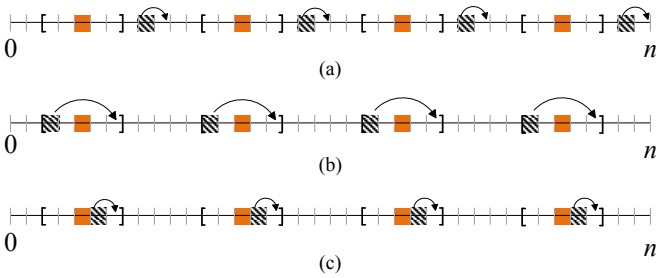

Fig. 5. One period is divided into t frames. In the i-th frame, packets of color i are transmitted according to the routing protocol corresponding to Γ_i (see Fig. 4). Each frame further consists of t time slots ($t = 10$ in the figure). Cells transmitting simultaneously (dashed cells) in one slot are $t-1$ cells apart. For the i-th frame, three time slots are shown above: (a) shows a time slot with single-cell transmissions outside neighborhoods, (b) shows a time slot with multi-cell hops over the neighborhoods (with all jammers active), (c) shows a time slot with transmissions inside neighborhoods. Note that cells in the periphery of the neighborhoods also do "occasional" single-cell hops for deliveries to destinations inside neighborhoods, with all jammers passive (not shown above).

■

Theorem 2: Consider the one-dimensional network inside the interval $[0, n]$, where the eavesdroppers are placed according to a Poisson point process with some density $\lambda_e > 0$, independent of the placement of the legitimate nodes. The locations of the eavesdroppers are unknown, and they are assumed not to collaborate. Then, the fraction of source-destination pairs that can maintain a per-node secure throughput of $\Theta\big(1/n\big)$ is arbitrarily close to one w.h.p, if $\lambda_e = o(1/\log n)$.

Proof:

We use the same construction as that used to prove Theorem 1. For source-destination pairs free from any nearby eavesdroppers, this construction achieves w.h.p. the stated secure throughput. Hence, the proof follows by showing that for $\lambda_e = o(1/\log n)$, the fraction of source-destination pairs that do not have any nearby eavesdroppers is arbitrarily close to one w.h.p.

Let the random variable $m(n)$ be the number of eavesdroppers in the network, which has an expected value of $\lambda_e n$. Let $y_i \in [0, n]$ be the location of the i-th eavesdropper, and define $A_i(n) = [y_i - l\log n, y_i + l\log n]$, with length $\ell(n) \triangleq |A_i(n)| = 2l\log n, \forall i$. Let $A(n)$ be the total region covered by the eavesdroppers, i.e., any source or destination node inside $A(n)$ will not be able to communicate secretly.

$$A(n) \triangleq \bigcup_{i=1}^{m(n)} A_i(n) \tag{4}$$

Let $N_i(n), N_o(n)$ be the random variables denoting the number of legitimate nodes inside and outside $A(n)$, respec-

tively. For some $\varepsilon > 0$, let the event $C^{\varepsilon}(n)$ be defined as

$$C^{\varepsilon}(n) \triangleq \left\{ \frac{N_i(n)}{N_i(n) + N_o(n)} < \varepsilon \right\}. \tag{5}$$

We can write $P(C^{\varepsilon}(n))$ as

$$\begin{aligned} &P(C^{\varepsilon}(n)) = \\ &P(C^{\varepsilon}(n) \,|\, \{|A(n)| \leq 2\lambda_e n\ell(n)\}) P(\{|A(n)| \leq 2\lambda_e n\ell(n)\}) \\ &+P(C^{\varepsilon}(n) \,|\, \{|A(n)| > 2\lambda_e n\ell(n)\}) P(\{|A(n)| > 2\lambda_e n\ell(n)\}) \end{aligned}$$

Define the random variable $X(n)$ as

$$X(n) \triangleq \frac{N_i(n)/n}{N_o(n)/n}.$$

Given $\lambda_e = o(1/\log n)$, and $|A(n)| \leq 2\lambda_e n\ell(n)$,

$$N_i(n)/n \to 0, N_o(n)/n \to 1, \text{ and } X(n) \to 0, \text{ a.s.}$$

Then,

$$\begin{aligned} &P\big(C^{\varepsilon}(n) \,|\, \{|A(n)| \leq 2\lambda_e n\ell(n)\}\big) = \\ &P\left(\frac{X(n)}{1 + X(n)} < \varepsilon \,|\, \{|A(n)| \leq 2\lambda_e n\ell(n)\} \right) \to 1, n \to \infty \end{aligned} \tag{6}$$

By a Chernoff bound,

$$\begin{aligned} P(|A(n)| \leq 2\lambda_e n\ell(n)) &\geq P(m \leq 2\lambda_e n) \\ &\to 1, n \to \infty. \end{aligned}$$

Thus, for any $\varepsilon > 0$, $P(C^{\varepsilon}(n)) \to 1$, as $n \to \infty$. This shows the fraction of nodes inside $A(n)$ is arbitrarily close to zero w.h.p., which readily implies that the fraction of source-destination pairs inside $A(n)$ is arbitrarily close to zero w.h.p. ■

IV. Two-dimensional Networks

Similar to the one-dimensional case, we first establish security in the absence of eavesdroppers near the source-destination nodes in the following theorem. The construction given for this theorem is then used in Theorem 4 to establish the number of eavesdroppers that can be tolerated.

Theorem 3: Consider the two-dimensional network inside the square $[0, \sqrt{n}] \times [0, \sqrt{n}]$, where the eavesdroppers are arbitrarily distributed, and the locations of the eavesdroppers are unknown. Legitimate nodes can maintain a throughput of $\Theta\big(1/\sqrt{n \log n}\big)$ w.h.p. for all source-destination pairs, for any number of eavesdroppers. For some fixed positive constant r, the throughput achieved is secure for the source-destination pairs that satisfy the condition that no eavesdropper is placed within a distance $r\sqrt{\log n}$ to the source and to the destination node. For any given integer $t < \infty$, the throughput remains secure for any number $g < t$ of collaborating eavesdroppers arbitrarily chosen from the network.

Proof:

We present a construction where source nodes generate packets as in the one-dimensional case, but sends these packets over different paths to the destination. The basic idea is that eavesdroppers cannot decode the packets carried on distant paths. By keeping a sufficient spacing between paths, and choosing the number of paths accordingly, it is further ensured that eavesdroppers cannot decode a packet by combining their received packets.

A. Routing Algorithm

We divide $[0, \sqrt{n}] \times [0, \sqrt{n}]$ into a square lattice of cells, each with a side of length $c(n) = \sqrt{\log n}$ (Fig. 6); hence, each cell contains a legitimate node w.h.p. [25]. For each source-destination pair $S-D$, S generates t packets $\{w_1, \cdots, w_t\}$ for each message w to be sent. The packets are generated in the same way as done in the one-dimensional case (see Section III-A).

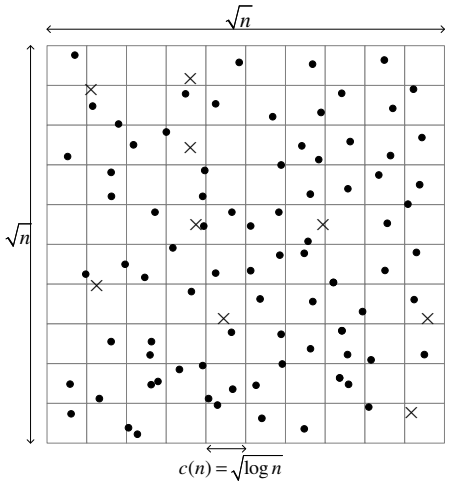

Fig. 6. The two-dimensional network consists of legitimate nodes (represented by dots) and eavesdroppers (represented by crosses) placed in the square $[0, \sqrt{n}] \times [0, \sqrt{n}]$. The whole region is divided into square cells of size $c(n) \times c(n)$, with $c(n) = \sqrt{\log n}$, as part of the signaling construction.

Consider square regions with $(t-1)(2l-1)+1$ cells on each side with S, and D in the center cells. We refer to these as S and D's "bases" (Fig. 7). The value of $t \geq 2$ is determined based on the maximum number of collaborating eavesdroppers assumed, $l \geq 2$ is chosen to ensure secrecy as in the one-dimensional case (see Appendix I). We define t "paths" connecting S to D, and packets of color i are sent on the i-th path. As shown in Fig. 7, each path exits the source base on a horizontal line, then follows a vertical line entering the destination base. The first path exits the edge of the source base from the top cell on the edge. Outside the bases, the paths have a minimum spacing of $(2l-2)$ cells. Inside the source base, a packet is delivered from S to a path following a vertical route. Similarly, when inside the destination base, a packet is delivered to D following a horizontal line. At each hop, the packet is delivered to a relay inside the next cell on the path. When D receives all t packets, it decodes the message by performing the operation in (3).

Note that this routing algorithm (including the definition of source and destination base) is slightly modified for source or destination nodes close to the edges of the network, or when

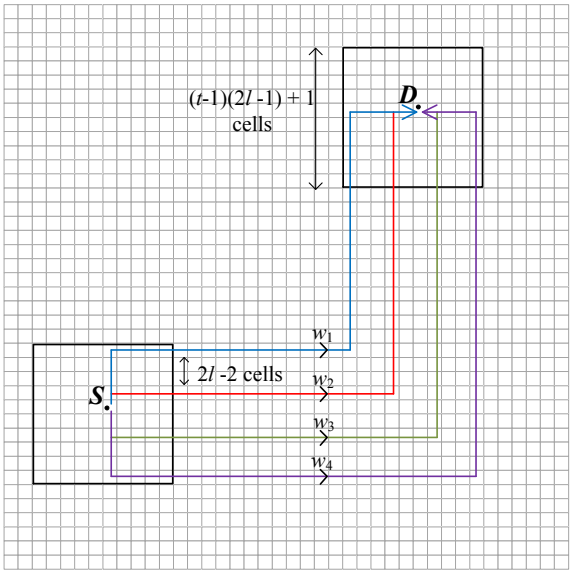

Fig. 7. Around each source and destination node S, D, a square region is defined as the "base" of that node, and consists of $[(t-1)(2l-1)+1]^2$ cells ($t = 4, l = 2$ in the figure). Each source and destination pair $S - D$ is connected by t paths. Outside the source and the destination base, the paths consist of a horizontal line followed by a vertical line, and have a minimum spacing of $(2l-2)$ cells. The t packets generated by S for a single message are carried on these t paths.

the bases are roughly aligned horizontally or vertically. The details are omitted due to space constraints.

B. Time Division Multiplexing Scheme

Time is divided into a sequence of periods, where each period consists of t frames. Only packets of color i are transmitted in the i-th frame. Each frame is further divided into $(h+1)^2$ time slots for some constant h, where nodes with a distance of h cells transmit simultaneously in each time slot (Fig. 8).

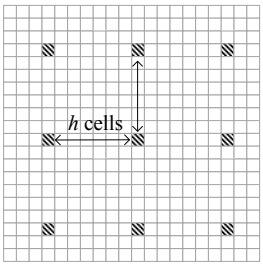

Fig. 8. One period is divided into t frames, where only packets of color i are transmitted in the ith frame. Each frame is further divided into $(h+1)^2$ time slots. Nodes transmitting simultaneously (shaded cells) in a given time slot are h cells apart. In each time slot, relays in the active cells transmit a packet to a relay inside the next cell on the path.

In each cell, streams that have arrived to that cell take turns being relayed. As proved in Appendix II, the number of streams arriving to each cell is at most a constant times $\sqrt{n \log n}$ w.h.p. Hence, a throughput value of $\Theta\big(1/\sqrt{n \log n}\big)$ is achieved for each source-destination pair w.h.p.

For the secrecy of the achieved throughput, consider the transfer of a message w to be carried from node S to D, and focus on the transmission of the packet w_i on its corresponding path. Consider a hop where w_i is transmitted from node A to B. It can be shown that (see Appendix I), the receiving node B, and any eavesdropper E located at least a distance of $(l-1)$ cells from the transmitting cell satisfy the SINR condition for secrecy. This shows that a packet of color i is protected from all the eavesdroppers located outside a strip of width $(2l-1)$ cells surrounding the path carrying that packet. Note that, outside the bases, an eavesdropper can be located less than $(l-1)$ cells to at most one path due to the spacing of the paths. If the source and the destination are free from eavesdroppers inside a radius of $r \log n$, $r \geqslant 2tl$, then the source and destination bases do not contain any eavesdroppers. Hence, an eavesdropper in the network can decode at most one packet out of the t packets. Therefore, any number $g < t$ of collaborating eavesdroppers are not able to decode the message by combining their received packets.

■

A stronger form of collaboration where eavesdroppers combine their received SINRs is discussed in Section V.

Theorem 4: Consider the two-dimensional network inside $[0, \sqrt{n}] \times [0, \sqrt{n}]$, where the eavesdroppers are placed according to a Poisson point process with some density $\lambda_e > 0$, independent of the placement of the legitimate nodes. Then, the fraction of source-destination pairs that can maintain a per-node secure throughput of $\Theta\big(1/\sqrt{n \log n}\big)$ is arbitrarily close to one w.h.p., if $\lambda_e = o(1/\log(n))$, and the throughput achieved remains secure for any number $g < t$ of collaborating eavesdroppers arbitrarily chosen from the network.

The proof is very similar to the proof of Theorem 2, and is omitted.

V. Discussion

1) *Percolation highway:* Our construction for the 2-D network can be extended to achieve a higher secure throughput on the order of $1/\sqrt{n}$ using a "percolation highway" [4] construction, with sources sending packets over different "highways" to reach their destination. This extension does not improve the number of eavesdroppers that can be tolerated, because nodes need to access highways contained in a slab of width on the order of $\log n$ to ensure the highways used are disjoint, and with enough spacing.

2) *Eavesdropper collaboration:* In the 2-D case, we assume collaborating eavesdroppers combine their received packets, and we ensure that an eavesdropper can decode at most one packet out of the t packets. A stronger form of collaboration may be assumed by considering a super-node having access to the observations of the eavesdroppers, and trying to decode the message. This may cause $g < t$ eavesdroppers being able to decode t packets. However, this can be avoided by adjusting the constants used for the minimum spacing of the paths in the construction, with no effect on the scaling results.

3) *Fading:* Secrecy throughput scaling in the case of eavesdroppers of unknown location was recently studied in [11]. However, what is crucial to the results in [11] is the use of multi-user diversity that can only be achieved in a fading environment. Therefore, the construction in [11] cannot be applied to our case. Note that most current networks use wideband communications, where fading can be effectively averaged out, resulting in an AWGN channel between nodes.

4) *2D strip:* An interesting case for future work is to consider secure communication in a 2-D strip to study the trade-off between the 1-D and 2-D networks, which require quite different formulations.

VI. Conclusion

We address the important problem of secure communication in a wireless network in the presence of eavesdroppers. We present achievable scaling results on the rate of information that can be securely carried in a network, when the size of the network becomes large. In contrast to most of the previous work in this area, we assume the locations of the eavesdroppers are unknown. Compared to previous works that consider unknown eavesdropper locations, our construction can achieve the same secure throughput scaling while tolerating a significantly higher number of eavesdroppers.

Appendix I
Secrecy at Each Hop

Consider the transmission of a packet of any color i (see Fig. 4). We show that this packet is securely delivered during (1) single-cell hops outside neighborhoods, (2) multi-cell hops inside the neighborhoods, by showing that, the relays and the eavesdroppers inside Γ_i satisfy the SINR condition for secrecy for given SINR thresholds $0 < \gamma_e < \gamma$.

Assume relays for single-cell hops transmit with some power P (Fig. 4 (a)), the relays for multi-cell hops inside the neighborhoods (node A in Fig. 4 (b)) transmit with power P_A, and jammers transmit with power P_J. We have three transmit power values, P, P_A, P_J, and two constants, k, l to set to satisfy the SINR requirements. We select the following values for P, P_A, P_J, l:

$$P = 4^\alpha c^\alpha \gamma N_0 \qquad l = 1 + 12(\gamma/\gamma_e)^{1/\alpha} \tag{7}$$

$$P_A = 2^\alpha (2l+1)^\alpha c^\alpha \gamma N_0 \qquad P_J = (l-1)^\alpha c^\alpha N_0 \tag{8}$$

Consider the first type of hop, where a packet of color i is transmitted outside the neighborhoods of Γ_i, where a relay R receives the signal from an adjacent cell.

$$\text{SINR}_R = \frac{P_{\text{rcv},R}}{N_0 + I_R},$$

where $P_{\text{rcv},R}$ is the received signal power at R, and I_R is the interference due to other transmissions.

$P_{\text{rcv},R}$ can be lower bounded by noting that the distance between the transmitting and receiving relay cannot exceed $2c$:

$$P_{\text{rcv},R} > \frac{P}{2^\alpha c^\alpha} = \frac{4^\alpha c^\alpha \gamma N_0}{2^\alpha c^\alpha} = 2^\alpha \gamma N_0$$

Considering the interference power I_R, note that jammers are silent., and other transmitting nodes are spaced with larger than $2kl$ cells in between. The two closest interferers are both at a distance larger than $2kl$ to R, the second two closest interferers are $4kl$ cells away, and so on (see Fig. 5). So,

$$I_R < \sum_{i=1}^{\infty} 2\frac{P}{(2iklc)^\alpha} = \frac{P}{k^\alpha l^\alpha c^\alpha}\beta < \frac{1}{k^\alpha}\beta\frac{\gamma_e N_0}{3^\alpha},$$

where $\beta = \sum_{i=1}^{\infty} 2/(2i)^\alpha$. Note that $\beta < \infty$ for $\alpha > 1$. Hence,

$$\text{SINR}_R > \frac{2^\alpha \gamma N_0}{N_0 + \frac{1}{k^\alpha}\beta\frac{\gamma_e N_0}{3^\alpha}} > \gamma, \text{ provided}$$

$$k^\alpha > \frac{\beta\gamma_e}{3^\alpha\left(2^\alpha - 1\right)}. \tag{9}$$

During this single-cell hop for packet i, the SINR value at the closest eavesdropper E inside Γ_i can be bounded as

$$\text{SINR}_E < \frac{P/(l-1)^\alpha c^\alpha}{N_0} = \frac{4^\alpha c^\alpha \gamma N_0}{12^\alpha(\gamma/\gamma_e)c^\alpha N_0} = \frac{\gamma_e}{3^\alpha} < \gamma_e.$$

Therefore, single-cell hops outside the neighborhoods satisfy the SINR requirements (with k satisfying (9)).

Second, consider any multi-cell hop inside a neighborhood $N(\mathcal{C}_i^j)$ (see Fig. 4 (b)), where the transmitting relay A sends the packet to the receiving relay B.

$$\text{SINR}_B = \frac{P_{\text{rcv},B}}{N_0 + I_B + \tilde{I_B}}$$

Here, I_B is the interference due to other relay transmissions, $\tilde{I_B}$ is the jamming noise suffered due to all the active jammer nodes in the network. $P_{\text{rcv},B}$ can be bounded by noting the maximum distance between A and B.

$$P_{\text{rcv},B} \geq \frac{P_A}{(2l+1)^\alpha c^\alpha} = 2^\alpha \gamma N_0$$

The interfering relays and jammers (with power P_A, P_J, respectively) are located in the network as in the single-cell hop case. Hence,

$$I_B < \sum_{i=1}^{\infty} 2\frac{P_A}{(2iklc)^\alpha} = \frac{P_A}{k^\alpha l^\alpha c^\alpha}\beta < \frac{1}{k^\alpha}\beta\gamma N_0 6^\alpha,$$

$$\tilde{I_B} < \frac{P_J}{(l-1)^\alpha c^\alpha} + \sum_{i=1}^{\infty} 2\frac{P_J}{(2iklc)^\alpha} \leq N_0 + \frac{1}{k^\alpha}\beta N_0,$$

where the first term in the upper bound for $\tilde{I_B}$ is due to the jammer node inside $\mathcal{C}_i^j$. Hence,

$$\text{SINR}_B > \frac{2^\alpha \gamma N_0}{N_0 + \frac{1}{k^\alpha}\beta\gamma N_0 6^\alpha + N_0 + \frac{1}{k^\alpha}\beta N_0} > \gamma,$$

provided

$$k^\alpha > \frac{\beta(6^\alpha\gamma + 1)}{2^\alpha - 2}. \tag{10}$$

The bound in (10) is stricter than the bound in (9).

The SINR value at an eavesdropper E inside $\mathcal{C}_i^j$ can be bounded as

$$\begin{aligned}\text{SINR}_E &\leq \frac{P_A/(l-1)^\alpha c^\alpha}{P_J/c^\alpha} = \gamma 2^\alpha \left(\frac{2l+1}{l-1}\right)^\alpha \frac{1}{(l-1)^\alpha} \\ &< \frac{6^\alpha}{12^\alpha}\frac{\gamma}{\gamma/\gamma_e} < \gamma_e.\end{aligned}$$

The other eavesdroppers inside Γ_i satisfy the SINR condition due to the active jammers in their cells. Hence, with constants satisfying (7), (8), (10) the secrecy is shown to be achieved for both types of hops.

The secrecy of each hop in the 2-D case can be shown by very similar arguments. Details can be found in [25].

Appendix II
The Number of Streams Arriving to a Cell in 2-D

Consider any stream arriving at a cell $s_{ij}(n)$, on the ith row and jth column in the square lattice, $i, j \in \{1, \cdots, \sqrt{n/\log n}\}$. The source base of this stream should contain cells on the ith row. Therefore, the source node is located on a row i_s such that $(i - z) < i_s < (i + z)$, $z = 4tl$. Hence, the sources of all the streams arriving to $s_{ij}(n)$ is contained in a rectangular region $\mathcal{R}_i$ of size $z\sqrt{\log n} \times \sqrt{n}$. By a similar argument, the destination nodes of all streams are contained in a rectangular region $\mathcal{R}_j$ of size $\sqrt{n} \times z\sqrt{\log n}$. Hence, the number of streams N arriving at $s_{ij}(n)$ can be upper-bounded by the number of nodes inside $\mathcal{R}_i \cup \mathcal{R}_j$. Let N_i, N_j be the number of nodes located in $\mathcal{R}_i, \mathcal{R}_j$, respectively. N_i, N_j are Poisson random variables with parameter $z\sqrt{n \log n}$. Note that $N \leqslant N_i + N_j$. Hence,

$$\begin{aligned}P(N < 4z\sqrt{n\log n}) &\geq P(N_i + N_j < 4z\sqrt{n\log n}) \\ &\geq P\big(\{N_i < 2z\sqrt{n\log n}\} \\ &\quad \cap\{N_j < 2z\sqrt{n\log n}\}\big) \\ &\geq 1 - \big[P(\{N_i \geq 2z\sqrt{n\log n}\}) \\ &\quad + P(\{N_j \geq 2z\sqrt{n\log n}\})\big] \\ &\geq 1 - 2(e/4)^{z\sqrt{n\log n}} \to 1, n \to \infty,\end{aligned}$$

where the third inequality is due to a union bound, and the last inequality is due to a Chernoff bound. This shows $N < 4z\sqrt{n \log n}$ with high probability.

Acknowledgment

This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished 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.

References

[1] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, January 1975.

[2] O. Dousse, P. Thiran, and M. Hasler, "Connectivity in ad-hoc and hybrid networks," in *INFOCOM 2002*, vol. 2, 2002, pp. 1079 – 1088 vol.2.

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

[4] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *Information Theory, IEEE Transactions on*, vol. 53, no. 3, pp. 1009 –1018, march 2007.

[5] O. Leveque and I. Telatar, "Information-theoretic upper bounds on the capacity of large extended ad hoc wireless networks," *Information Theory, IEEE Transactions on*, vol. 51, no. 3, pp. 858 – 865, march 2005.

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

[7] P. Pinto, J. Barros, and M. Win, "Wireless secrecy in large-scale networks," in *ITA 2011*, feb. 2011, pp. 1 –10.

[8] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of manets with malicious nodes," in *ISIT 2009*, 28 2009-july 3 2009, pp. 1189 –1193.

[9] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, pp. 477–486, August 2002.

[10] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, submitted for publication (eprint arXiv:0908.0898).

[11] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. of MobiHoc '10*. New York, NY, USA: ACM, 2010, pp. 21–30.

[12] A. Sheikoleslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," Technical Report (Available: www.ecs.umass.edu/∼sheikholesla).

[13] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *Wireless Communications, IEEE Transactions on*, to be published (eprint arXiv:1012.4552).

[14] 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*, to be published. (Available: www.ecs.umass.edu/∼goeckel/networksecurity.html).

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180 –2189, june 2008.

[16] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *INFOCOM 2009*, april 2009, pp. 1935 –1943.

[17] S. Goel, V. Aggarwal, A. Yener, and A. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *ISIT 2010*, 2010, pp. 2627 –2631.

[18] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, November 1979.

[19] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, pp. 335–348, April 1989.

[20] W. Lou, W. Liu, and Y. Fang, "Spread: enhancing data confidentiality in mobile ad hoc networks," in *INFOCOM 2004*, vol. 4, march 2004, pp. 2404 – 2413 vol.4.

[21] N. Cai and R. Yeung, "Secure network coding," in *ISIT 2002*, p. 323.

[22] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Cooperative jamming to improve the connectivity of the 1-d secrecy graph," in *CISS 2011*, March 2011, pp. 1 –6.

[23] E. Perron, S. Diggavi, and E. Telatar, "On noise insertion strategies for wireless network secrecy," in *ITA 2009*, feb. 2009, pp. 77 –84.

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

[25] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," Technical Report (Available: www.ecs.umass.edu/∼ccapar).