Cooperative Jamming in MIMO Ad-Hoc Networks

Jianqi Wang and A. Lee Swindlehurst
The Henry Samueli School of Engineering
University of California, Irvine
Irvine, CA 92697

***Abstract*—In this work, we investigate cooperative jamming schemes for the transmission of confidential messages in ad-hoc networks. By letting mobile units (the helpers) in the vicinity of a legitimate receiver send out jamming signals while a transmitter communicates with the receiver, an environment that is hostile to any eavesdroppers can be established. Meanwhile, the jamming signals are designed in an intelligent way such that the interference that the legitimate receiver experiences is kept low. Two particular approaches are considered, namely, Uncoordinated Cooperative Jamming (UCJ) and Coordinated Cooperative Jamming (CCJ). For both approaches, we present simulation results of the secrecy rate with respect to the node density of the network, the area the helpers occupy, and the number of transmit/receive antennas.**

***Index Terms*—Secrecy capacity, MIMO, ad hoc networks, cooperative jamming**

I. Introduction

Due to the broadcast nature of the wireless channel, secure transmission of information for wireless systems is receiving considerable attention. Wyner's pioneering paper [1] indicates that, when the channel between the transmitter (Alice) and an eavesdropper (Eve) is a degraded version of the channel between Alice and the legitimate receiver (Bob), Alice can send secret messages to Bob with non-zero rate while keeping Eve completely ignorant of the messages. Along this line, extensive research from an information theoretic perspective has been carried out [2], [3]. The majority of this work focuses on characterizing the fundamental limit of the information rate for various scenarios.

For systems equipped with multiple antennas, the additional spatial degrees of freedom provide us a facility to design a practical method to approach the secrecy capacity. A typical method employs artificial interference, in which the transmitter tries to degrade the eavesdropper's channel condition by sending jamming signals together with the confidential messages [3]–[5]. The transmit signal is designed such that the jamming interference and the confidential messages received by Bob are orthogonal to each other. Bob can easily remove the jamming interference by projecting the received signal to the signal subspace.

Most of the artificial interference approaches work best when the transmitter has some information about the eavesdropper's channel. This assumption, however, is not realistic when the eavesdropper is passive and wants to avoid detection. Without knowledge of the eavesdropper's channel, the only possible way to use jamming is to uniformly spread the jamming power along all the spatial dimensions [5]. The drawback is that not only that some of the jamming power will be wasted but also that some of the jamming power will be leaked to the main channel and degrade the channel of the legitimate receiver.

In this paper, we consider the artificial interference approach for ad hoc networks. In ad hoc networks, there are typically many nodes in a given area that share the same bandwidth. As pointed out in [6], assuming a common transmitter, the wireless channels for receivers with distinct spatial locations exhibit statistically independent characteristics. This is especially true for channels that experience significant multipath fading. For ad hoc networks, the consequence is that the channel from any node to the eavesdropper and the channel to the legitimate receiver will be very different. This proves to be advantageous for secret communication applications when the nodes in the network can synchronize their transmission with the transmitter. Specifically, when one pair of nodes is communicating with each other, those nodes surrounding the legitimate receiver can act as an interferer to the eavesdropper by sending jamming signals. We assume that the helpers know their channels to the legitimate user, and that they design their interference signals in such a way that the received interference at Bob is much less than that at Eve or can be easily removed by the legitimate user.

The main contributions of this paper are two cooperative jamming approaches that explore the spatial independency of the channels in ad hoc networks and the randomness in positions of the nodes that constitute the network. Other approaches that explore cooperation in ad hoc networks to improve physical layer security can be found in [7], [8], where the helpers in the network are used as relay nodes. In [8], a distributed algorithm is proposed to group the users into clusters to exploit these gains.

The organization of this paper is as follows. Section II provides the system model we use throughout this paper. In Section III, the approaches of coordinated cooperative jamming and uncoordinated cooperative jamming are presented. Their performance is discussed in Section IV-A and Section IV-B, respectively. Simulation results are given in Section V, and Section VI concludes the paper.

In this paper, we use lowercase boldface letters to denote vectors and uppercase bold letters to denote matrices. $\|\cdot\|$ denotes the Euclidean norm of a vector. The symbol $(\cdot)^T$ denotes matrix transposition, and $(\cdot)^H$ denotes the matrix Hermitian transpose. Furhtermore, $\mathbb{E}\{\cdot\}$ will denote expectation, and $|\cdot|$ the absolute value.

978-1-4244-5827-1/09/$26.00 ©2009 IEEE

II. System Model

In this paper, we consider MIMO ad-hoc networks with one transmitter (Alice), one intended receiver (Bob), one eavesdropper (Eve), and N helpers. The basic assumptions that are used throughout this paper are:

1) We assume that Alice has full knowledge of its channel to Bob.
2) The helpers do not have the channel state information (CSI) of the main channel (the channel between Alice and Bob).
3) Similarly, each helper is assumed to have CSI for its outgoing channel to Bob, but the helpers do not share this CSI with each other.
4) In addition, we assume that neither Alice nor the helpers have any knowledge of the presence of Eve nor her CSI.
5) Finally, we assume that transmissions by Alice and the helpers are synchronized.

Note that in TDD systems, these assumptions guarantee that Eve does not know any additional channel information other than her own. The central idea behind these assumptions is that we want to limit the amount of channel state information that could be leaked to Eve. Moreover, these assumptions make it possible to accommodate more than one eavesdropper in the system.

We assume Alice, Bob and Eve have M_A, M_B, and M_E antennas, respectively. Helper i is equipped with $M_{H,i}$ antennas. All nodes are assumed to be in an environment of deep fading. In this paper, we adopt the model where the channel gain is inversely proportional to the distance between the transmitter and the receiver. Specifically, let $\boldsymbol{H}_{B,i} \in \mathbb{C}^{M_B \times M_{H,i}}$ and $\boldsymbol{H}_{E,i} \in \mathbb{C}^{M_E \times M_{H,i}}$ be the channels from helper i to Bob and Eve, respectively. The elements of $\boldsymbol{H}_{B,i}$ are i.i.d. and have a circularly symmetric complex Gaussian distribution with zero mean and variance $\frac{\sigma_h^2}{d_{B,i}^2}$. Similarly, the elements of $\boldsymbol{H}_{E,i}$ are i.i.d. and follow a circularly symmetric complex Gaussian distribution with zero mean and variance $\frac{\sigma_h^2}{d_{E,i}^2}$. Note that $d_{B,i}$ and $d_{E,i}$ are the distance from helper i to Bob and Eve, respectively.

The cooperative jamming scheme works as follows: while Alice is communicating with Bob, the N helpers transmit artificial interference in an effort to disrupt Eve's ability to decode Alice's signal to Bob. The received signals for the intended receiver and the eavesdropper can be written as

$$\begin{aligned} \boldsymbol{y} &= \sqrt{P_S}\boldsymbol{H}_{B,0}\boldsymbol{x} + \sum_{i=1}^{N} \sqrt{P_I}\boldsymbol{H}_{B,i}\boldsymbol{q}_i + \boldsymbol{n}_B, \\ \boldsymbol{z} &= \sqrt{P_S}\boldsymbol{H}_{E,0}\boldsymbol{x} + \sum_{i=1}^{N} \sqrt{P_I}\boldsymbol{H}_{E,i}\boldsymbol{q}_i + \boldsymbol{n}_E, \end{aligned} \tag{1}$$

respectively, where $\boldsymbol{H}_{B,0} \in \mathbb{C}^{M_B \times M_A}$ and $\boldsymbol{H}_{E,0} \in \mathbb{C}^{M_E \times M_A}$ are the channels from Alice to Bob and Eve, respectively. We assume that $\boldsymbol{x}$ is the transmitted signal and $\|\boldsymbol{x}\| = 1$. The covariance matrix of $\boldsymbol{x}$ is $\mathrm{E}[\boldsymbol{x}\boldsymbol{x}^H] = \boldsymbol{C}$. $\boldsymbol{q}_i$ is the artificial interference from helper i and $\|\boldsymbol{q}_i\| = 1$ for all i. $\boldsymbol{n}_B$ and $\boldsymbol{n}_E$ are white Gaussian noise. We assume proper normalization is performed so that $\boldsymbol{n}_B$ and $\boldsymbol{n}_E$ can be modeled as $\boldsymbol{n}_B, \boldsymbol{n}_E \sim \mathcal{CN}(0, \boldsymbol{I})$. P_S is the transmission power at Alice. P_I is the transmission power at each helper.

III. Cooperative Jamming Algorithms

In this section, we present the general framework for the two jamming approaches we present in this paper, namely, the approach of uncoordinated cooperative jamming (UCJ) and coordinated cooperative jamming (CCJ). In a nutshell, CCJ provides a mechanism for Alice, Bob, and the helpers to coordinate in the design of the confidential messages and the jamming signals using the publicized information on the secrecy and jamming subspace. In contrast, with UCJ, Alice, Bob, and the helpers do not have such information. They act autonomously. Each party makes their best endeavor based on their knowledge of their individual channels.

A. Coordinated Cooperative Jamming

With CCJ, the whole signal space for Bob is divided into two subspaces, the secrecy subspace and the jamming subspace. Information about these two subspaces are made public. All the participants including Alice, Bob, and the helpers are aware of this information, and Eve may know this information as well. However, this information does not benefit Eve since the helpers know $\boldsymbol{H}_{B,i}$, their channels to Bob, and they can properly design their signals such that the interference received at Bob is perfectly aligned in the jamming subspace. Bob can completely remove the interference by projecting the received signal to the secrecy subspace. On the other hand, the interference at Eve goes through a channel that is different from $\boldsymbol{H}_{B,i}$, which she is unaware of. As a consequence, the interference Eve experiences will in general span the whole received signal space. Even though Eve knows the public information about the secrecy subspace, she has no means to remove the interference.

Specifically, the CCJ approach divides the signal space at Bob into two subspaces, the secrecy subspace $\mathcal{S} = \mathrm{span}\{\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_{l_1}\}$ and the jamming subspace $\mathcal{J} = \mathrm{span}\{\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{l_2}\}$, where $\boldsymbol{\eta}_1, \cdots, \boldsymbol{\eta}_d, \boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{l_2}$ are orthogonal to each other with unit norm. We also require that $l_1 + l_2 = M_B$. The jamming signal generated by helper i should satisfy

$$\boldsymbol{H}_{B,i}\boldsymbol{q}_i \in \mathcal{J}. \tag{2}$$

The jamming signal at Bob's end can be completely removed by projecting Bob's signal into the secrecy subspace $\mathcal{S}$. Let $\boldsymbol{W} = [\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_{l_1}]$. The received signal at Bob after the projection is

$$\begin{aligned} \hat{y} &= \sqrt{P_s}\boldsymbol{W}^H\boldsymbol{y} \\ &= \sqrt{P_s}\boldsymbol{W}^H(\boldsymbol{H}_{B,0}\boldsymbol{x} + \sum_{i=1}^{N} \sqrt{P_I}\boldsymbol{H}_{B,i}\boldsymbol{q}_i + \tilde{n}_B) \\ &= \sqrt{P_s}\tilde{\boldsymbol{H}}_{B,0}\boldsymbol{x} + \tilde{n}_B, \end{aligned} \tag{3}$$

where $\tilde{\boldsymbol{H}}_{B,0} = \boldsymbol{W}^H\boldsymbol{H}_{B,0}$. It can be seen that, if we use beamforming, the beamforming vector should be the principle eigenvector of $\tilde{\boldsymbol{H}}^H\tilde{\boldsymbol{H}}$. The received signal at Eve is the same as in (1). Although she has information about the jamming

subspace $\mathcal{J}$, she does not know $\boldsymbol{H}_{B,i}$. Therefore, she can not recover and remove $\boldsymbol{q}_i$.

Note that the effective channel matrix $\tilde{\boldsymbol{H}}_{B,0}$ is of dimension $l_1 \times M_B$. In essence, CCJ sacrifices l_2 degrees of freedom to achieve jamming-free communication between Alice and Bob. For Eve, because she experiences different channels, her capacity can be severely degraded by the jamming signals sent from the helpers.

B. Uncoordinated Cooperative Jamming

In the scenario we consider in this section, we do not use a public jamming subspace. Instead, Alice uses the principle singular vector of her channel to Bob as the beamforming vector to achieve the maximum transmission gain for the desired signal. Because the helpers know their channel to Bob, they can minimize the interference to Bob by sending the jamming signals along the right singular vector that correspond to the smallest singular value of their channel to Bob. Due to the randomness of their location, we have $\boldsymbol{H}_{E,i} \neq \boldsymbol{H}_{B,i}$ for any i. Therefore, there is no average reduction of the interference that Eve experiences.

More precisely, for Helper i, let the singular value decomposition for its channel matrix $\boldsymbol{H}_{B,i}$ be

$$\boldsymbol{H}_{B,i} = \boldsymbol{U}_{B,i}\boldsymbol{\Lambda}_{B,i}\boldsymbol{V}_{B,i}^H,$$

where $\boldsymbol{U}_{B,i} = [\boldsymbol{u}_{B,i}^1, \cdots, \boldsymbol{u}_{B,i}^{M_B}]$ and $\boldsymbol{V}_{B,i} = [\boldsymbol{v}_{B,i}^1, \cdots, \boldsymbol{v}_{B,i}^{M_B}]$. $\boldsymbol{\Lambda} = \text{diag}\{\sqrt{\lambda_{B,i}^1}, \ldots, \sqrt{\lambda_{B,i}^{M_B}}\}$ is a diagonal matrix containing its singular values in decreasing order, i.e., $\lambda_{B_i}^1 \geq \cdots \geq \lambda_{B,i}^{M_B}$. The interference sent by helper i is $\boldsymbol{q}_i = \boldsymbol{v}_{B,i}^{M_B} t_i$, for some complex white Gaussian interference, i.e., $t_i \sim \mathcal{CN}(0,1)$.

With this choice for $\boldsymbol{x}$ and $\boldsymbol{q}_i$, the received signal can be written as

$$\begin{aligned} \boldsymbol{y} &= \sqrt{P_S}\boldsymbol{H}_{B,0}\boldsymbol{x} + \sum_{i=1}^{N}\sqrt{P_I}\boldsymbol{H}_{B,i}\boldsymbol{v}_{B,i}^{M_B} + \boldsymbol{n}_B, \\ \boldsymbol{z} &= \sqrt{P_S}\boldsymbol{H}_{E,0}\boldsymbol{x} + \sum_{i=1}^{N}\sqrt{P_I}\boldsymbol{H}_{E,i}\boldsymbol{v}_{B,i}^{M_B} + \boldsymbol{n}_E. \quad (4) \end{aligned}$$

Similar to the case of CCJ, the transmitted signal $\boldsymbol{x}$ can be designed using water-filling.

Equivalently,

$$\begin{aligned} \boldsymbol{y} &= \sqrt{P_S}\boldsymbol{H}_{B,0}\boldsymbol{x} + \sum_{i=1}^{N}\sqrt{P_I\lambda_{B,i}^M}\boldsymbol{u}_{B,i}^{M_B} + \boldsymbol{n}_B, \\ \boldsymbol{z} &= \sqrt{P_S}\boldsymbol{H}_{E,0}\boldsymbol{x} + \sum_{i=1}^{N}\sqrt{P_I}\boldsymbol{H}_{E,i}\boldsymbol{v}_{B,i}^{M_B} + \boldsymbol{n}_E. \quad (5) \end{aligned}$$

IV. Performance Analysis

In this section, we analyze the performance of the two approaches presented in last section. The main interest of this section is to study how the helpers can improve the secrecy capacity. To simplify the analysis, we mainly focus on beamforming techniques. We also let $M_A = M_B = M_E = M_{H,i} = M$. Proofs of the lemmas and theorems presented below will not be included due to space limitations.

We position Bob at the origin $(0,0)$ and Eve at $(d,0)$. Let $A = [-\frac{D}{2}, \frac{D}{2}] \times [-\frac{D}{2}, \frac{D}{2}]$ be a $D \times D$ square area that is centered at the origin. We assume $D >> 1$. Let $A_B = [-1,1] \times [-1,1]$ and $A_E = [d-1, d+1] \times [-1,1]$ be two 2×2 square areas that are centered at Bob and Eve, respectively. In this paper, we are interested in scenarios where the helpers lie in the area $A \cap \bar{A_B} \cap \bar{A_E}$. There are two main reasons for these constraints:

1) Because the helpers need to coordinate with Alice, in this work, we let Bob notify Alice as well as the helpers when he is ready to receive confidential messages. So only helpers that are in the vicinity of Bob are able to receive this notification and send out jamming signals. Moreover, we adopt a more practical assumption where Eve's position is unknown to Alice or Bob. It is therefore impossible to select the helpers around the eavesdropper.
2) Note that with are assumed propagation model, when $d_{E,i}$ or $d_{B,i}$ is decreased toward zero, we actually get infinite channel gains. By forcing the helpers to be outside A_B and A_E, we can ensure the channel gains are finite.

The positions of the helpers follow a 2-D Poisson process with parameter μ. Because $D >> 1$, the number of helpers in this area can be approximated by the following distribution

$$\Pr\{N = n\} = \frac{(\mu D^2)^n e^{-\mu D^2}}{n!}. \quad (6)$$

Moreover, let $(z_{i,1}, z_{i,2})$ be the position of helper i, $(z_{i,1}, z_{i,2})$, which follows a uniform distribution over $A \cap \bar{A_B} \cap \bar{A_E}$. The position of the transmitter is not specified as this paper is focused on studying the benefit of helpers in the ad hoc networks. Before we present the SINR results, we note the fact that the channel gains are inversely proportional to the square of the distance between the transmitter and the receiver. The following Lemma is crucial in calculating the expected channel gains.

Lemma 1: Given a random point $Z = (z_1, z_2)$ that is uniformly distributed in the area $A \cap \bar{A_E}$, where $A = [-\frac{D}{2}, \frac{D}{2}] \times [-\frac{D}{2}, \frac{D}{2}]$, and $A_E = [d-1, d+1] \times [-1,1]$. Let $\rho = \sqrt{(z_1 - d)^2 + z_2^2}$ be the distance between the point Z and the point $(d,0)$, where $|d| < D/2 - 1$. The expected value of $\frac{1}{\rho^2}$ is given by

$$\begin{aligned} \text{E}\left\{\frac{1}{\rho^2}\right\} &= \frac{2}{D^2-4}\left[\varphi\left(\frac{D/2}{D/2+d}, D/2\right)\right. \\ &\quad \left. +\varphi\left(\frac{D/2}{D/2-d}, D/2\right) + 2\varphi\left(\frac{2}{D}, 1\right)\right], \quad (7) \end{aligned}$$

where

$$\varphi(a,b) = \int_a^b \frac{1}{x}\arctan x dx.$$

A. Coordinated Cooperative Jamming

In what follows, we will derive the expected SINR for Bob and Eve, which are summarized in the following theorem:

Theorem 1: With CCJ, the SINRs for Bob and Eve are

$$\begin{aligned} \text{SINR}_B &= P_s\|\tilde{\boldsymbol{H}}_{B,0}\boldsymbol{b}\|^2 \\ \text{SINR}_E &= \frac{P_s\|\boldsymbol{H}_{E,0}\boldsymbol{b}\|^2}{\mu P_I \sigma_h^2 \Phi(d,D) + 1}, \end{aligned}$$

respectively, where

$$\begin{aligned}\Phi(d,D) &= 2\varphi\left(\frac{D/2}{D/2+d}, D/2\right) \\ &\quad +2\varphi\left(\frac{D/2}{D/2-d}, D/2\right)+4\varphi\left(\frac{2}{D},1\right).\end{aligned}$$

Moreover, for large D, we have

$$\lim_{D\to+\infty}\mathrm{SINR}_E = \frac{P_s\|\boldsymbol{H}_{E,0}\boldsymbol{b}\|^2}{\mu P_I\sigma_h^2(c_1+c_2\log(D^2))+1}, \quad (8)$$

for some constant c_1 and c_2, where D^2 is the area of the rectangular we consider.

Theorem 1 shows that the interference the eavesdropper experiences scales as the logarithm of the area of the rectangle where the helpers reside. The interference by the helpers becomes saturated as we increase the size of the rectangle.

The secrecy rate for this scheme is

$$\begin{aligned}R_{\mathrm{CCJ}} &= [\log_2(1+\mathrm{SNR}_B)-\log_2(1+\mathrm{SNR}_E)]^+ \\ &= \left[\log_2\left(1+P_s\|\tilde{\boldsymbol{H}}_{B,0}\boldsymbol{b}\|^2\right)\right. \\ &\quad \left.-\log_2\left(1+\frac{P_s\|\boldsymbol{H}_{E,0}\boldsymbol{b}\|^2}{\mu P_I\sigma_h^2\Phi(d,D)+1}\right)\right]^+ \quad (9)\end{aligned}$$

We have the following observations.

Remark 1: We can see that as μ or D becomes large, SNR_E converges to zero. More precisely,

$$\lim_{\mu\log(D^2)\to+\infty} R_{\mathrm{CCJ}} = \log_2\left(1+P_s\|\tilde{\boldsymbol{H}}_{B,0}\boldsymbol{b}\|^2\right) \quad (10)$$

Effectively, increasing μ or D is equivalent to increasing the the number of the helpers in the system. A Large number of helpers can eliminate the eavesdropper's ability to intercept Alice's transmissions.

B. Uncoordinated Cooperative Jamming

In this analysis, we focus on beamforming, i.e. $\boldsymbol{x}=\boldsymbol{b}s$, where $\boldsymbol{b}$ is the beamformer. The received signals at Bob and Eve are

$$\begin{aligned}\boldsymbol{y} &= \sqrt{P_S}\boldsymbol{H}_{B,0}\boldsymbol{b}s+\sum_{i=1}^{N}\sqrt{P_I\lambda_{B,i}^M}\boldsymbol{u}_{B,i}^M+\boldsymbol{n}_B, \\ \boldsymbol{z} &= \sqrt{P_S}\boldsymbol{H}_{E,0}\boldsymbol{b}s+\sum_{i=1}^{N}\sqrt{P_I}\boldsymbol{H}_{E,i}\boldsymbol{v}_{B,i}^M+\boldsymbol{n}_E. \quad (11)\end{aligned}$$

Because Bob has the perfect CSI, maximum ratio combining can be used. For Bob, let

$$\boldsymbol{\phi}_B = \frac{\boldsymbol{H}_{B,0}\boldsymbol{b}}{\|\boldsymbol{H}_{B,0}\boldsymbol{b}\|}.$$

We have

$$\begin{aligned}\hat{y} &= \boldsymbol{\phi}_B^H\boldsymbol{y} \\ &= \sqrt{P_S}\|\boldsymbol{H}_{B,0}\boldsymbol{b}\|s+\sum_{i=1}^{N}\sqrt{P_I\lambda_{B,i}^M}\boldsymbol{\phi}_B^H\boldsymbol{u}_{B,i}^M+\boldsymbol{\phi}_B^H\boldsymbol{n}_B.\end{aligned} \quad (12)$$

Note that in cases where Bob knows $\boldsymbol{H}_{B,i}$, he can find the covariance of the interference. In that way, we can do better by pre-whitening the interference plus noise before using MRC. Nevertheless, to simplify the theoretical analysis, we use MRC directly in this paper.

Theorem 2: Assume UCJ is used and Bob and Eve use maximum ratio combining at the receiver. The SINRs for Bob and Eve are given by

$$\begin{aligned}\mathrm{SINR}_B &= \frac{P_s\|\boldsymbol{H}_{B,0}\boldsymbol{b}\|^2}{\frac{P_I\mu\sigma_h^2\Phi(0,D)}{M^2}+1}, \\ \mathrm{SINR}_E &= \frac{P_s\|\boldsymbol{H}_{E,0}\boldsymbol{b}\|^2}{P_I\mu\sigma_h^2\Phi(d,D)+1}, \quad (13)\end{aligned}$$

respectively.

Denote $G_B=\|\boldsymbol{H}_{B,0}\boldsymbol{b}\|$ and $G_E=\|\boldsymbol{H}_{E,0}\boldsymbol{b}\|$. The secrecy capacity for this scheme is

$$\begin{aligned}C_{\mathrm{UCJ}} &= [\log_2(1+\mathrm{SINR}_B)-\log_2(1+\mathrm{SINR}_E)]^+ \\ &= \left[\log_2\left(1+\frac{P_sG_B^2}{\frac{\mu P_I\Phi(0,D)}{M^2}\sigma_h^2+1}\right)\right. \\ &\quad \left.-\log_2\left(1+\frac{P_sG_E^2}{\mu P_I\sigma_h^2\Phi(d,D)+1}\right)\right]^+. \quad (14)\end{aligned}$$

The condition $\mathrm{SINR}_B>\mathrm{SINR}_E$ can also be written as

$$G_B > \sqrt{\frac{\frac{\mu P_I}{M^2}\Phi(0,D)\sigma_h^2+1}{\mu P_I\Phi(d,D)\sigma_h^2+1}}G_E. \quad (15)$$

Remark 2: Note that $\lim_{D\to+\infty}\Phi(d,D)=\Phi(0,D)$. Then

$$\lim_{\mu,D\to+\infty}\frac{\frac{\mu P_I}{M^2}\Phi(0,D)\sigma_h^2+1}{\mu P_I\Phi(d,D)\sigma_h^2+1}=\frac{1}{M^2}.$$

This shows that the interference Bob receives is roughly $\frac{1}{M^2}$ of what Eve experiences.

On the other hand, both $\log_2(1+\mathrm{SINR}_B)$ and $\log_2(1+\mathrm{SINR}_E)$ will go to zero. Hence

$$\lim_{\mu,D\to+\infty}C_{\mathrm{UCJ}}=0.$$

This shows that increasing μ and D alone cannot improve the secrecy capacity in this case.

In the following Lemma, we show that increasing the number of antennas and interference power can improve the secrecy capacity.

Lemma 2: When $\mu, D, M\to+\infty$ and $\frac{\mu\Phi(0,D)}{M^2}=c$ for some constant c,

$$\lim_{\mu,D,M\to+\infty}C_{\mathrm{UCJ}}=\log_2\left(1+\frac{P_sG_B^2}{cP_I\sigma_h^2+1}\right)$$

with probability 1.

Essentially, this result shows that when the number of helpers is large and the square of the number of antennas is comparable to the number of helpers, we can obtain unlimited capacity by increasing the transmission power.

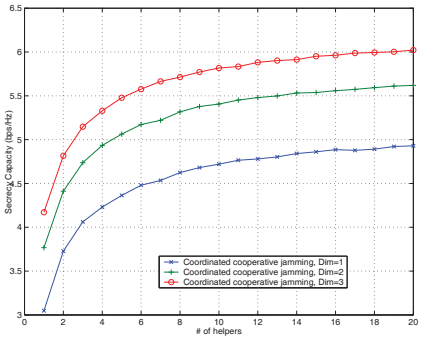

Fig. 1. Secrecy capacity versus the density of users

V. Simulation Results

In this section, we provide numerical results for the two approaches discussed in the previous sections. Throughout this section, we fix $\Phi(d, D)$ to be 10 and vary the density of users μ, which roughly corresponds to $d = 5$ and $D = 50$.

In Figure 1, we plot the secrecy capacity against the density of the users. All the nodes that are involved have 4 transmit antennas. The transmit and jamming power are 10 dB. We can see that the secrecy capacity increases monotonically with the density of the users. Furthermore, we can also see that increasing the dimensionality of the signal space increases the capacity as well. This is because when the signal subspace has higher dimensionality, it is more likely we will obtain a larger eigenvalue for $\tilde{\boldsymbol{H}}_{0,B}$.

In Figure 2, we plot the secrecy capacity of UCJ. Both the transmit power and the jamming power is 10 dB. The number of helpers in the area we consider is M^2, where M is the number of transmit/receive antennas. We can see that with help from the neighboring nodes, the secrecy capacity approaches the channel capacity for a single user where there are no eavesdroppers.

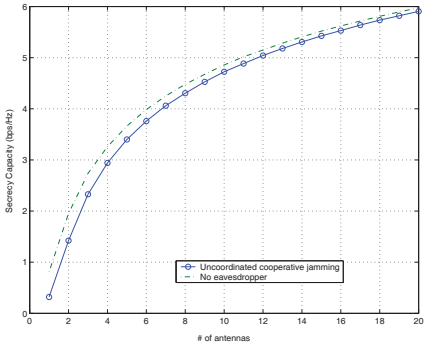

Fig. 2. Secrecy capacity versus the number of transmit antennas M, the number of helpers is M^2.

In Figure 3, we compare the performance of CCJ and UCJ. We can see that while increasing the density of helpers improves the secrecy capacity for CCJ, UCJ tends to work better when the density of helpers is small because UCJ allows Alice to use the principle singular vector of Bob's channel $\boldsymbol{H}_{B,0}$ as the beamforming vector, as opposed to CCJ where only the principle singular vector of the projected channel matrix is used. When the density of the helpers increases, the secrecy capacity for UCJ decreases. This can be clearly observed in (13). As the density of the helpers increases, the SINR of Bob as well as Eve decreases. Correspondingly, the secrecy capacity decreases.

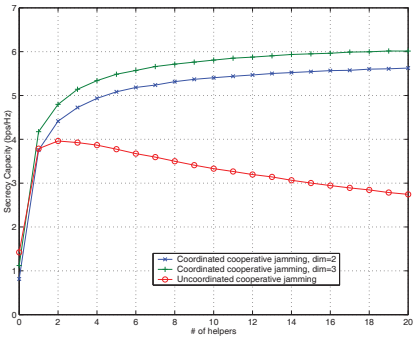

Fig. 3. Secrecy capacity versus the number of helpers.

VI. Conclusion

The spatial independence of wireless fading channels is a resource that we can exploit to improve security at the physical layer. For ad hoc networks, due to the randomness in the location of the nodes, cooperative jamming is a very effective way to utilize this spatial independence for secure communications. The two approaches presented here, coordinated and uncoordinated cooperative jamming, represent one approach to addressing this problem in ad hoc networks. Our simulation results show that both approaches can effectively increase the secrecy capacity by significantly degrading the eavesdropper's channel. When the density of the helpers in the network is small, UCJ is preferable. On the contrary, when the helper density is larger, CCJ is the better choice.

References

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The misome wiretap channel," submitted IEEE Trans. Inform. Theory. [Online]. Available: http://arxiv.org/abs/0708.4219

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[5] A. L. Swindlehurst, "Fixed sinr solutions for the mimo wiretap channel," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2009*, pp. 2437–2440.

[6] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2008*, Mar. 2008, pp. 3013–3016.

[7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communication via cooperation," in *Proc. of Allerton Conference on Communication, Control, and Computing*, Sep. 2008.

[8] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Hjorungnes, "Physical layer security: Coalitional games for distributed cooperation," 2009. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:0906.4827