Energy Efficiency of Cooperative Jamming Strategies in Secure Wireless Networks

Mostafa Dehghan*, Dennis L. Goeckel*, Majid Ghaderi†, and Zhiguo Ding‡

*Department of Electrical and Computer Engineering, University of Massachusetts Amherst, USA

†Department of Computer Science, University of Calgary, Canada

‡Department of Electrical, Electronic, and Computer Engineering, Newcastle University, UK

Abstract

Energy efficient secure communication in wireless networks in the presence of eavesdroppers is considered. For a secure transmission to the destination, a set of intermediate "jammer" nodes are chosen to generate artificial noise that confuses the eavesdropper. We consider two jamming strategies: beamforming and cooperative diversity. Previous research has focused largely on cooperative beamforming strategies, but we demonstrate a number of scenarios where a cooperative diversity strategy is desirable. This motivates approaches which selectively switch between the two strategies, from which significant energy savings can often be realized. In our simulations, energy savings of up to 60% are observed in the simulated networks.

Index Terms

Wireless security, cooperative diversity, cooperative beamforming, energy efficiency.

This research was sponsored by the National Science Foundation under grants CNS-0721861, ECS-0725616, and CNS-1018464, 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.

I. INTRODUCTION

The secure transmission of a message from a sender to a receiver in the presence of an adversary is a major concern in ad hoc networks. Therefore, the problem of secure communication in wireless networks has attracted considerable attention, with the purpose of enabling the authorized receiver to successfully obtain the information, while preventing the adversary from eavesdropping and obtaining the source information.

In cooperative schemes, authenticated relay nodes are used to enhance secrecy against adversaries. Cooperative secrecy schemes are divided into two main categories, based on the role of the relaying nodes. In the first category, relays employ techniques such as decode-and-forward and amplify-and-forward to improve the achievable secrecy rate. In the second category, known as cooperative jamming, the source node transmits the encoded signal while relays generate an artificial noise signal with the purpose of confusing the eavesdropper.

Most of the studies in the second category use beamforming to exploit interference cancelation at the destination node while allowing for artificial noise to impinge on the eavesdropper. While there are numerous examples of such works (see [1]–[10]), there are only a few that exploit cooperative diversity effects and do not require distributed beamforming (*e.g.*, [11], [12]). Whereas the difficulty of achieving distributed beamforming is well understood, we ask here *whether it is always desirable even when possible*. Whereas its avoidance of jamming impinging on the receiver is desirable, such avoidance may lead to a system that is less robust in inhibiting eavesdropper reception. In particular, the *diversity* of the jamming in a cooperative jamming system may offset the performance loss caused by the extra interference at the receiver. It is this tradeoff that we consider in this work.

In this paper, the beamforming and diversity schemes are evaluated from an energy efficiency perspective. Because we adopt a slow fading model, an outage formulation is appropriate: we put constraints on the success probability of the destination and the eavesdropper, meaning that the destination should be able to decode the source message with a success probability that is greater than a target probability, given that the probability that the eavesdropper successfully decodes the message is below some specific threshold. For each of the two schemes, we find

the minimum transmission power that satisfies the secrecy constraints.

Note that our notion of secrecy is different from what might have been expected. Here, we consider constraints on two individual success probabilities for the main receiver and the eavesdropper, namely, $P(S,D) = P(\gamma_{SD} \geq \text{SINR}_{\min})$ and $P(S,E) = P(\gamma_{SE} \leq \text{SINR}_{\min})$,[1] rather than the secrecy outage probability defined as $P\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE}} < 2^{\lambda}\right)$ with λ being the required secrecy rate. We note that the secrecy rate is an event that depends on the ordered pair $(\gamma_{SD}, \gamma_{SE})$. However, when considering maximizing the probability of such an event, note that there does not exists a "universal" wiretap code of rate λ that will work for any point $(\gamma_{SD}, \gamma_{SE})$ in that event. Rather, a wiretap code (or the practical codes used for secrecy) depend on both γ_{SD} and γ_{SE}; that is, if both thresholds are not met, the code "fails". For example, if the received signal-to-noise ratio at the eavesdropper is higher than that for which the code was designed, the code is not secure, even if the signal-to-noise ratio at the receiver is high enough such that the secrecy rate equation is still satisfied. The cost of "failure" is also often different for the two thresholds. If the desired SINR is not realized at the receiver, a retransmission can be initiated. However, if the eavesdropper is able to obtain an SINR higher than the planned threshold, information is leaked – a much more significant failure. Hence, assuming a single code is used throughout the system implies a pair of thresholds that must be met, and, recognizing the quite different costs of failing to meet the thresholds, indicates that a separate failure probability constraint be assigned to each threshold. The fundamental question posed in this paper is then: *for specific success probability constraints on the destination and the eavesdropper, does the beamforming scheme always consumes less energy? If not, how much energy can be saved by exploiting a strategy that selectively switches between the two schemes?*

The remainder of the paper is organized as follows. Section II presents the system mode and assumptions, and derives expressions for success probabilities of the destination and the eavesdropper for the cooperative beamforming and diversity schemes. In Section III, performance of the two cooperative approaches is evaluated through simulation. Finally, Section IV concludes

[1] We define γ_{SD} and γ_{SE} as the signal-to-interference-plus-noise ratio at the main receiver and the eavesdropper, respectively. Also, $\text{SINR}_{\min}$ denotes the minimum SINR required at a receiving node to decode a transmitted message. Note that different thresholds on γ_{SD} and γ_{SE} are similarly considered with no change in methodology.

the paper.

II. MODEL

Consider a configuration with a source node S, a destination node D, an eavesdropper E, and a set of jammer nodes $J = \{J_1, J_2, \ldots, J_N\}$ that (potentially) jam the eavesdropper. We assume that the location of the eavesdropper is known, but channel state estimates to the eavesdropper are unknown.

A. Channel Model

Consider the discrete-time equivalent channel for a transmission from node t_i to node r_j. Let x_i be the normalized (unit-power) symbol stream to be transmitted by t_i, and let y_j be the received signal at node r_j. We assume that transmitter t_i is able to control its power p_i, in arbitrarily small steps, up to some limit $\mathrm{P}_{\max}$. Let η_j denote the noise received at r_j, where η_j is a complex Gaussian random variable with $\mathbb{E}\left[|\eta_j|^2\right] = N_0$. The received signal at receiver r_j is expressed as follows

$$y_j = \sqrt{p_i} h_{ij} x_i + \eta_j,$$

where h_{ij} is the complex channel gain between t_i and r_j. The channel gain is modeled as $h_{ij} = |h_{ij}|e^{\theta_{ij}}$, where $|h_{ij}|$ is the channel gain magnitude and θ_{ij} is the phase. We assume a non line-of- sight (LOS) environment, implying that $|h_{ij}|$ has a Rayleigh distribution, and that $\mathbb{E}[|h_{ij}|^2] = \frac{1}{d_{ij}^{\alpha}}$, where d_{ij} is the distance between the transmitting and the receiving nodes t_i and r_j, and α is the path-loss exponent.

Let γ_{ij} denote the instantaneous signal-to-noise-ratio (SNR) at receiver r_j due to t_i transmitting with power p_i. Then,

$$\gamma_{ij} = \frac{p_i |h_{ij}|^2}{N_0}\,. \tag{1}$$

Since $|h_{ij}|$ is Rayleigh distributed, $|h_{ij}|^2$ is exponentially distributed with mean $1/d_{ij}^{\alpha}$. Consequently, γ_{ij} is exponentially distributed with decay rate $\mu_{ij} = N_0 \frac{d_{ij}^{\alpha}}{p_i}$.

B. Cooperative Beamforming

In the cooperative beamforming scheme, we assume that the jamming nodes transmit an artificial Gaussian distributed common noise signal z, and are able to adjust their power and phase such that the interfering signals at the receiver cancel out, *i.e.*, they transmit z in the null space of $\mathbf{h}_D$, where

$$\mathbf{h}_D = [h_{J_1,D}, h_{J_2,D}, \ldots, h_{J_N,D}]^{\mathrm{T}}.$$

Hence, the signal transmitted by the jammers can be expressed as

$$\mathbf{s}_J = \mathbf{h}_D^{\perp} z,$$

where $\mathbf{h}_D^{\perp}$ is a Gaussian random vector in the null space of $\mathbf{h}_D$. We note that the total transmitting power from the jammers equals

$$P_J = \| \mathbf{h}_D^{\perp} \|^2 \ . \tag{2}$$

Also, assuming that the source node transmits with power P_S, the signal transmitted by the source node is expressed as

$$s = \sqrt{P_S} x_S, \tag{3}$$

where the data is encoded in signal x_S.

The signals received at the destination and the eavesdropper are, respectively,

$$y_D = \sqrt{P_S} h_{S,D} x_S + \eta_D,$$

$$y_E = \sqrt{P_S} h_{S,E} x_S + \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} z + \eta_E,$$

where $\mathbf{h}_E = [h_{J_1,E}, h_{J_2,E}, \ldots, h_{J_N,E}]^{\mathrm{T}}$ represents the channel gain vector between the jammers and the eavesdropper, and η_D and η_E denote the complex Gaussian noise at the destination and the eavesdropper, respectively, with $\mathbb{E}\left[|\eta_D|^2\right] = \mathbb{E}\left[|\eta_E|^2\right] = N_0$.

Let $\mathrm{SINR}_{\min}$ denote the minimum signal-to-interference-plus-noise ratio required at a receiving node to decode the transmitted message at some desired rate λ. Assuming optimal coding, the

capacity formula of the additive white Gaussian noise (AWGN) yields $\mathrm{SINR}_{\min} = 2^{\lambda} - 1$. Due to fading, the communication link may not be able to sustain the rate λ, resulting in outage. Let $P(S, D)$ denote the probability that link $\langle S, D\rangle$ is not in outage when the source power is P_S, *i.e.*, the transmission from source to destination is successful. Because we want to focus on the use of beamforming versus cooperative jamming by the relays under equivalent assumptions on the source to destination link, we assume h_{SD} is not known or not used by the source for power allocation. From (1) we obtain that:

$$\begin{aligned} P(S,D) &= \mathbb{P}(\gamma_{SD} \geq \mathrm{SINR}_{\min}) \\ &= e^{-N_0 \mathrm{SINR}_{\min} \frac{d_{SD}^{\alpha}}{P_S}}. \end{aligned} \tag{4}$$

Now, let $P(S, E)$ denote the probability that the eavesdropper successfully decodes the transmitted signal, when the source power is P_S, and the total jamming power equals P_J. We have

$$\begin{aligned} P(S,E) &= \mathbb{P}(\gamma_{SE} \geq \mathrm{SINR}_{\min}) \\ &= \mathbb{E}_{\mathbf{h}_E}\left[P_{h_{S,E}}\left(\frac{P_S |h_{S,E}|^2}{N_0 + \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} {\mathbf{h}_D^{\perp}}^{\mathrm{T}} \mathbf{h}_E} > \mathrm{SINR}_{\min} \mid \mathbf{h}_E \right) \right] \\ &= e^{-\frac{N_0 \mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S}} \mathbb{E}_{\mathbf{h}_E}\left[e^{-\frac{\mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S} \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} {\mathbf{h}_D^{\perp}}^{\mathrm{T}} \mathbf{h}_E} \right], \end{aligned}$$

where $\mathbb{E}_{\mathbf{h}_E}$ means expectation with respect to unknown channel gains $\mathbf{h}_E$, and $P_{h_{S,E}}$ denotes probability with respect to the random variable $h_{S,E}$. Now using the results from [13] (see Eq. 14) to calculate the expectation, we can write the success probability of the eavesdropper as follows ($\mathbf{I}_N$ is the identity matrix of size N)

$$\begin{aligned} P(S,E) &= \frac{e^{-\frac{N_0 \mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S}}}{|\mathbf{I}_N + \frac{\mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S} \mathbb{E}\{\mathbf{h}_E \mathbf{h}_E^{\mathrm{T}}\} \mathbf{h}_{\mathbf{D}}^{\perp} {\mathbf{h}_{\mathbf{D}}^{\perp}}^{\mathrm{T}}|} \\ &= \frac{e^{-\frac{N_0 \mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S}}}{|\mathbf{I}_1 + \frac{\mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S} \mathbf{h}_D^{\perp\,\mathrm{T}} \mathbb{E}\{\mathbf{h}_E \mathbf{h}_E^{\mathrm{T}}\} \mathbf{h}_{\mathbf{D}}^{\perp}|} \\ &= \frac{e^{-N_0 \mathrm{SINR}_{\min} \frac{d_{SE}^{\alpha}}{P_S}}}{1 + \frac{\mathrm{SINR}_{\min} d_{SE}^{\alpha}}{P_S} \sum \frac{P_i}{d_{J_i,E}^{\alpha}}}, \end{aligned} \tag{5}$$

where P_i is the transmission power of the ith jammer. The second expression is derived using Sylvester's determinant theorem:

$$\det(\mathbf{I}_m + \mathbf{AB}) = \det(\mathbf{I}_n + \mathbf{BA}),$$

for $\mathbf{A}$ and $\mathbf{B}$ being $m \times n$ and $n \times m$ matrices, respectively. The final equation is derived noting that $\mathbb{E}\{\mathbf{h}_E \mathbf{h}_E^{\mathrm{T}}\}$ equals the diagonal matrix $\mathbf{diag}(\frac{1}{d^{\alpha}_{J_1,E}}, \frac{1}{d^{\alpha}_{J_2,E}}, \ldots, \frac{1}{d^{\alpha}_{J_N,E}})$, and that the jamming powers are embedded in $\mathbf{h}_D^{\perp}$ (see (2)).

C. Cooperative Diversity

In the cooperative diversity scheme, we also assume that the source node transmits the encoded data with power P_S, and hence the transmitted signal, s, is the same as in (3). Here we assume that the jamming nodes transmit i.i.d. Gaussian artificial noise signals z_i, and each jammer J_i transmits with power P_i. Hence, the signal transmitted by the jamming nodes can be expressed as

$$\mathbf{s}_J = \mathbf{diag}(\sqrt{P_1}, \sqrt{P_2}, \ldots, \sqrt{P_N})\mathbf{z},$$

where $\mathbf{z} = (z_1, z_2, \ldots, z_N)$. Note that the total transmitting power by the jammers is given by $P_J = \sum_{i=1}^{N} P_i$.

The received signal at the receiver and the eavesdropper can now be written as

$$y_D = h_{S,D}\sqrt{P_S}x_S + \sum_{i=1}^{N} h_{J_i,D}\sqrt{P_i}z_i + \eta_D,$$

and

$$y_E = h_{S,E}\sqrt{P_S}x_S + \sum_{i=1}^{N} h_{J_i,E}\sqrt{P_i}z_i + \eta_E,$$

where η_D and η_E denote complex Gaussian noise at the destination and the eavesdropper, respectively. Because of the similarity of the expressions for the destination and the eavesdropper, we will use R to refer to a receiving node (either E or D) in the remainder of this section.

With the expressions obtained for the received signal at a receiving node R, the probability of a successful transmission can be found as follows. Let $P(S, R)$ denote the probability that a

receiving node R successfully decodes the transmitted signal, when the source node transmits with power P_S, and the jammers transmit i.i.d. Gaussian signals, each with power P_i. We have

$$\begin{aligned} P(S,R) &= \mathbb{P}(\gamma_{SR} \geq \mathrm{SINR}_{\min}) \\ &= \mathbb{E}_{\mathbf{h}_R}\left[P_{h_{S,R}}\left(\frac{P_S|h_{S,R}|^2}{N_0 + \sum_{i=1}^{N} P_i|h_{J_i,R}|^2} > \mathrm{SINR}_{\min} \mid \mathbf{h}_R \right) \right] \\ &= e^{-\frac{N_0 \mathrm{SINR}_{\min} d_{SR}^{\alpha}}{P_S}} \mathbb{E}_{\mathbf{h}_R}\left[e^{-\frac{\mathrm{SINR}_{\min} d_{SR}^{\alpha}}{P_S} \sum_{i=1}^{N} P_i|h_{J_i,R}|^2} \right] \\ &= e^{-\frac{N_0 \mathrm{SINR}_{\min} d_{SR}^{\alpha}}{P_S}} \prod_{i=1}^{N} \frac{1}{1 + \frac{\mathrm{SINR}_{\min} d_{SR}^{\alpha}}{P_S} \frac{P_i}{d_{J_i,R}^{\alpha}}} \,. \end{aligned} \tag{6}$$

D. Energy Efficiency

In both of the cooperation schemes described above, the source node transmits with power P_S, and the total transmission consumed by the jamming nodes equals P_J. Hence, the total transmission power in both cases equals $P_S + P_J$. Per above, we need to keep the success probability at the eavesdropper below a threshold $\wp_E$, and the success probability at the destination above some threshold $\wp_D$. Hence, we can write the problem of energy efficient secure communication as the following optimization problem:

$$\begin{aligned} &\min P_S + P_J, \\ &\text{s.t.} \quad P(S,D) \geq \wp_D, \\ &\qquad P(S,E) \leq \wp_E \,. \end{aligned} \tag{7}$$

III. Numerical Analysis

Consider a scenario where a source transmits to a destination in the presence of a single eavesdropper. For each of the cooperative schemes, we compute the total transmission power per (7). We will solve this problem numerically to find optimal power allocation for jammers. We used the interior method implemented in Matlab to solve the optimization problems.

A. Simulation Parameters

We simulate a wireless network where nodes are distributed uniformly in a square with a density of $\sigma = 2$ nodes per unit area. The noise power is set to $N_0 = 1$, and simulations are performed for path-loss exponents of $\alpha = 2$ and $\alpha = 4$. The success probability at the destination and the eavesdropper are set to $\wp_D = 0.5$ and $\wp_E = 10^{-4}$, respectively, unless otherwise specified. Also, a maximum of 10 jamming nodes are employed for each transmission. Each simulation is performed over ten randomly generated networks by randomly selecting ten seeds for node distribution, and the presented data are the average of results from all simulation runs.

B. Simulation Results

We compare the energy cost of the beamforming scheme with that of a *combined cooperative scheme* which selectively switches between cooperative beamforming and cooperative diversity based on the geometry of the network to minimize the expected energy.

Two sets of simulations are performed. In the first set of experiments, we fix the distance between the source and the destination nodes, and look at the performance of the combined cooperative scheme versus cooperative beamforming. We place the source node at the center of the network, *i.e.*, at location (0, 0), and put the destination at distance 2 from the source at location (2, 0). The eavesdropper node is allowed to be in any point in the square network. Figure 1 answers the first question posed in the introduction, by showing the eavesdropper locations for which switching to cooperative diversity results in energy savings as well as the amount of energy saved for each location.

Figure 1 shows the results for different values of the parameters α, $\wp_D$ and $\wp_E$, to capture the effects of the three parameters. We see that the combined scheme can show a significant performance improvement obtaining close to 90% energy savings for some eavesdropper locations. This is the diversity gain obtained (compare (5) and (6)). Other than showing that cooperative diversity can be useful in reducing the transmission energy in a secure communication, Figure 1 also provides insight about the geometries where the combined scheme shows better performance.

Results from the first set of experiments, presented in Figure 1, give answer to our first

question, as we observe that there are some cases in which cooperative diversity can help to achieve energy gains. This observation leads to the second set of experiments, where we calculate the average energy savings by the combined cooperative scheme over all locations of the eavesdropper. Similar to the first set of simulations, the source node is placed at the center of the square topology. The destination node is placed at different locations along the X-axis in steps of 0.5 away from the source. The energy saving presented for each case is the average over all locations of the eavesdropper with a positive energy saving. Figure 2 shows the results of the simulations for two cases of limited jamming sets with size $|J| = 5$ and $|J| = 10$ nodes, and two different path-loss exponent values, namely $\alpha = 2$ and $\alpha = 4$.

It is observed that, on average, more than 60% energy savings are obtained in some cases. It is also observed that as the distance between the source and the destination is increased, energy saving increases at first until it reaches a maximum point. When the source and destination are close, the source node can satisfy the minimum success probability at the receiver with a lower power level, and hence only a small area is susceptible to eavesdroppers. As the source power is increased, this area becomes larger and there is more need for jamming. Based on Figure 2 employing more nodes for jamming can increase the energy saving.

C. Discussion

It is important to note that both the cooperative diversity and cooperative beamforming have their advantages and disadvantages. Independent of the level of energy consumption, cooperative diversity cannot always be used, as there are cases where there is no feasible solution to the optimization problem in (7). A similar statement is true regarding the beamforming scheme. In particular, in this work, we did not consider a maximum limit on the transmitting power of the nodes. If such a limit is to be assumed, there will be scenarios where beamforming does not provide a feasible solution, while the diversity scheme can be used instead. The points with 80% energy savings in Figure 1 are essentially of this nature.

One also needs to recall that cooperative beamforming faces significant implementation challenges. In the beamforming approach a static environment is assumed where sets of transmitting

nodes are phase-locked and perfect channel state information is available – such synchronization requirements are onerous in a mobile ad hoc network. In general, there are two methods for obtaining the channel state information at a transmitter. In the first method, the receiver measures the channel and transmits a feedback message to the transmitter. In the second method, the transmitter estimates the channel based on channel response estimates calculated from signals received from the receiver. A detailed explanation of the two methods is given in [14].

Moreover, in the cooperative diversity scheme, each relay transmits a noise signal that is independent of the other relays. However, in the beamforming scheme, jammer nodes are required to transmit the same noise signal z. The noise signal z should be kept secret from the eavesdroppers, or they will be able to decode the source message. Hence, the common noise signal plays the role of a shared key that needs to be pre-distributed. A description of the schemes for generating artificial noise is presented in [4], [15]. Also a hardware-based Gaussian noise generator is described in [16].

In this work, we did not consider the cost of coordinating the jamming nodes. To choose the best jamming scheme it is necessary to include the coordination overhead of each scheme and calculate the corresponding costs. Other jamming schemes, with less overhead and possibly higher transmission cost, should also be considered to choose the best scheme. One such scheme is selective jamming in which a single jammer, the best one, is selected.

IV. Conclusion

In this work, we considered the problem of energy efficient secure communication in wireless ad hoc networks. We explored the energy efficiency of two cooperative jamming techniques used to improve communication secrecy, namely cooperative beamforming and cooperative diversity. We formulated the minimum energy secure communication based on the constraints on the success probability of the intended and eavesdropping receivers.

Cooperative beamforming has been extensively studied for secrecy purposes. Because of its ability to cancel the interference at the destination, one might expect that beamforming always performs better than cooperative diversity. We showed that this is not always the case, and there

are scenarios where cooperative diversity achieves the same secrecy constraints at the destination and eavesdropper, while consuming 80% less energy.

In this work, we assumed that there is only one eavesdropper in the network, and its location is know to all system nodes. A direction for future work is to consider extending this work for the case where the location of the eavesdropper(s) is unknown, and the relaying nodes cooperate to provide secrecy against a set of eavesdroppers.

REFERENCES

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

[2] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

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

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

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 3, September 2005, pp. 1906–1910.

[6] J. Li, A. Petropulu, and S. Weber, "Transmit power minimization under secrecy capacity constraint in cooperative wireless communications," in *IEEE Workshop on Statistical Signal Processing*, September 2009, pp. 217–220.

[7] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Communications Letters*, vol. 14, no. 10, pp. 885–887, October 2010.

[8] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, October 2010.

[9] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, October 2009.

[10] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[11] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM MobiHoc*, September 2010, pp. 21–30.

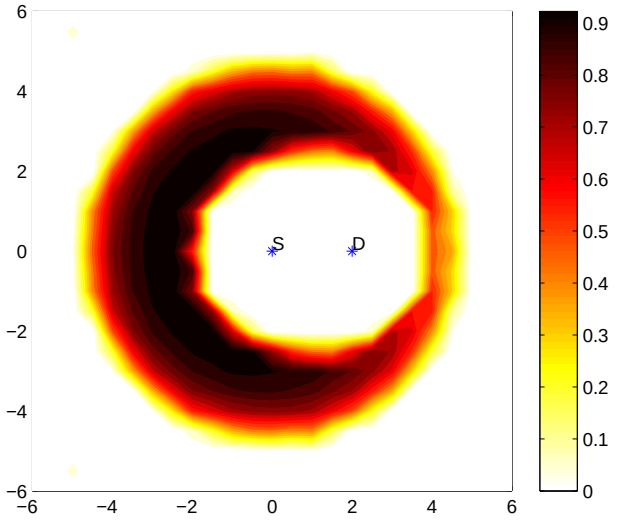
[12] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung, "Multi-user diversity for secrecy in wireless networks," in *Information Theory and Applications Workshop (ITA)*, February 2010, pp. 1–9.

[13] G. L. Turin, "The characteristic function of hermitian quadratic forms in complex normal variables," *Biometrika*, vol. 47, no. 1/2, pp. 199–201, June 1960.

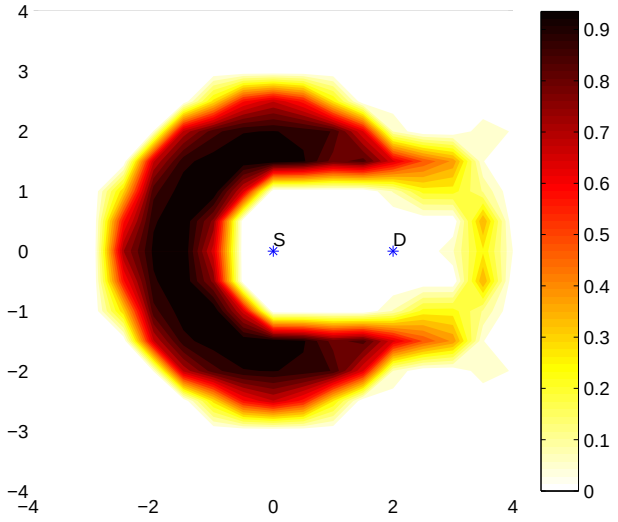
[14] F. Vook, X. Zhuang, K. Baum, T. Thomas, and M. Cudak, "Signaling methodologies to support closed-loop transmit processing in tdd-ofdma," *IEEE C802.16e-04/103r2*, July 2004.

[15] X. Li, M. Chen, and E. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," in *IEEE 6th Workshop on Signal Processing Advances in Wireless Communications*, June 2005, pp. 811–815.

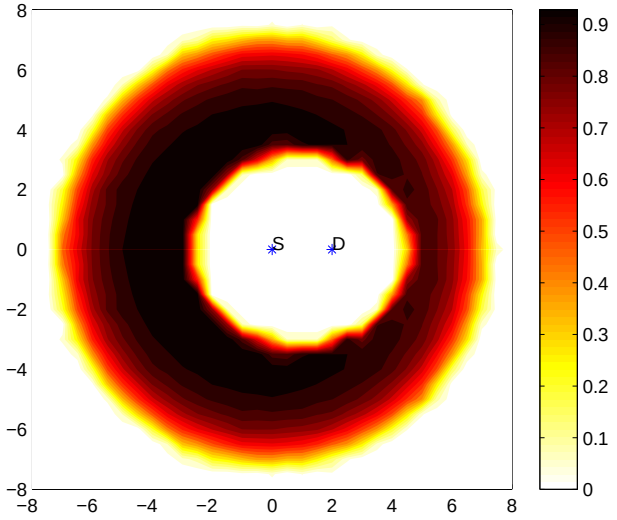
[16] D.-U. Lee, W. Luk, J. Villasenor, and P. Cheung, "A hardware gaussian noise generator for channel code evaluation," in *IEEE Symposium on Field-Programmable Custom Computing Machines*, April 2003, pp. 69–78.



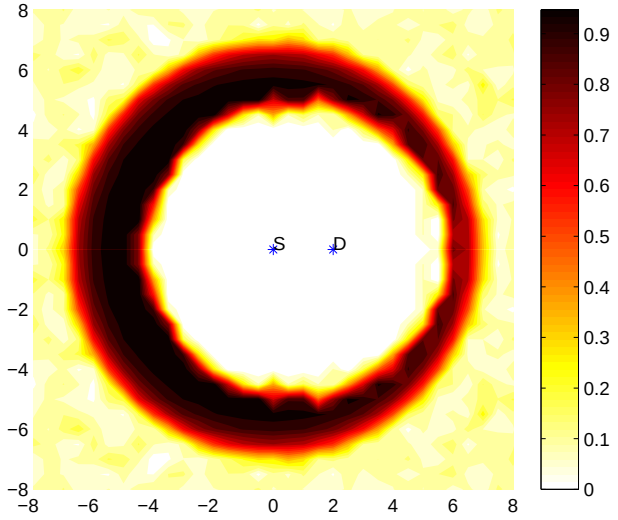
(a) $\alpha = 2, \wp_D = 0.5, \wp_E = 10^{-4}$.



(b) $\alpha = 4, \wp_D = 0.5, \wp_E = 10^{-4}$.

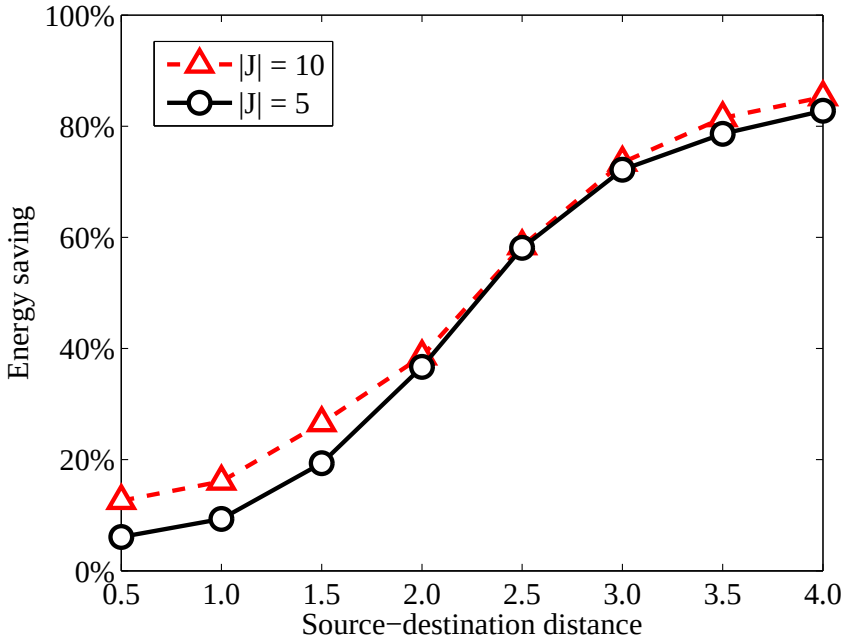


(c) $\alpha = 2, \wp_D = 0.75, \wp_E = 10^{-4}$.

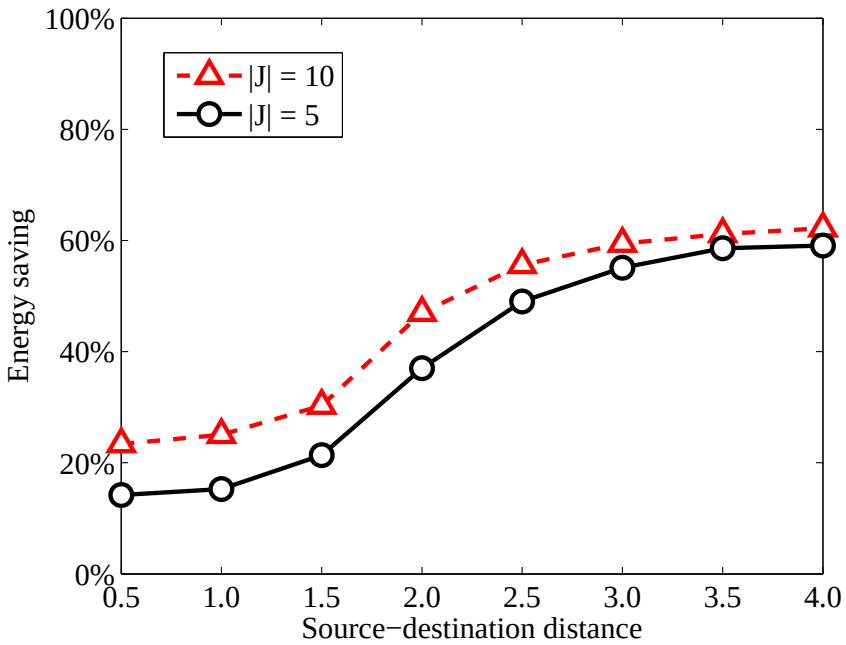


(d) $\alpha = 2, \wp_D = 0.5, \wp_E = 10^{-6}$.

Fig. 1: Square network with colors representing the extent of energy saving by the combined cooperative scheme compared to cooperative beamforming, for different locations of the eavesdropper. Effects of three parameters are considered: path-loss exponent (α), destination success probability ($\wp_D$) and eavesdropper success probability ($\wp_E$). Figure (a) shows the energy savings for the case the parameters are set to their default values. Figures (b), (c) and (d) show the effect of the path-loss exponent, destination success probability and the eavesdropper success probability, respectively. Note that a maximum of 10 jamming nodes are used. It can be seen that significant energy savings are obtained, reaching 90% for some eavesdropper locations.



(a) Path-loss exponent $\alpha = 2$.



(b) Path-loss exponent $\alpha = 4$.

Fig. 2: Average energy savings obtained by the combined cooperative scheme versus cooperative beamforming, based on the distance between the source and the destination. Different cases are considered for jamming sets limited to 5 and 10 nodes, *i.e.*, $|J| = 5$ and $|J| = 10$. Also, different environment conditions are considered with different values for path-loss exponent α. It is observed that up to 80% in energy savings can be achieved by using the combined cooperative scheme.