A COOPERATIVE JAMMING PROTOCOL FOR PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS

Nicholas Kolokotronis[*], *Kyriakos Fytrakis*[†], *Alexandros Katsiotis*[†], *and Nicholas Kalouptsidis*[†]

[*]Dept. of Informatics and Telecomm., University of Peloponnese, 22100 Tripolis, Greece
[†]Dept. of Informatics and Telecomm., University of Athens, 15784 Athens, Greece

ABSTRACT

A cooperative jamming protocol is studied in this paper and its ability to protect the communications of a pair of users in the presence of an eavesdropper. Communication of users is assisted by many helping interferers, assuming knowledge of channel state information. Closed form expressions are given for the optimal weights and power allocation maximizing the difference in the SNR between destination and eavesdropper; these are determined under transmit, reliability, and security constraints. Simulations show that noticeable improvements, of more than 30 dB, may be attained in the SNR difference compared to the non–cooperative case.

Index Terms— Cooperative jamming, wireless networks, physical layer security, fractional optimization.

1. INTRODUCTION

Physical (PHY) layer security approaches have received over the last decade considerable attention [1, 2, 23]. They exploit the characteristics of the wireless medium to allow legitimate nodes communicate securely in the presence of eavesdroppers that can intercept transmissions due to the broadcast nature of the wireless communication networks. This line of research was introduced by Wyner who proved that the communication between a source and a destination is perfectly secure when the source–eavesdropper channel is a degraded version of the source–destination channel [27]. The maximum achievable secrecy rate, i.e. the rate at which information is transmitted with perfect secrecy from the source to the destination is said to be the secrecy capacity, and is the performance measure to use [19, 21]. The work of Wyner has been extended to other cases, e.g. the transmission over the broadcast and the scalar Gaussian wiretap channel, etc. [4, 15, 16, 25].

This work was supported by the research projects ART–IN–SPACE and HANDiCAMS. The project ART–IN–SPACE is co–financed by the European Union (European Social Fund) and Greek national funds through the operational program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) — Research funding program ARISTEIA I, grant no. 1115. The project HANDiCAMS acknowledges the financial support of the Future and Emerging Technologies (FET) programme, within the 7th Framework Programme for Research of the European Commission, under FET–Open grant no. 323944.

The use of multiple antennas [9, 12, 18], or willingness to cooperate [6, 26], can help to overcome the limitations of the single–antenna systems. Cooperative transmission protocols which are commonly considered in the literature include the decode–and–forward (DF) [26], amplify–and–forward (AF) [7], and cooperative jamming (CJ) [6, 26] protocol. In CJ the helpers transmit noise in order to degrade the eavesdropper's channel. In most cases, the availability of global channel state information (CSI) is assumed [17, 24, 28]; works that do not require eavesdropper's CSI, or need only have statistical information include [8, 11, 20, 22]. Deriving the optimal relay (or helper) weights in closed form for a single eavesdropper is in general not easy, and becomes quite hard to solve if more eavesdroppers are assumed.

In this paper, nodes are assumed to cooperate via the CJ protocol under perfect knowledge of the global CSI. Instead of aiming at information–theoretic security, motivated by the work in [13, 14], we maximize the difference of destination's signal–to–noise ratio (SNR) and the eavesdropper's SNR. We assume the presence of a single eavesdropper, and impose a number of constraints related to the total power, security, and reliability. To solve the problem, we employ techniques from fractional programming, and derive closed–form expressions for the optimal jamming weights and the fraction of the power that should be allocated for jamming. Simulations have been performed that validate the theoretical analysis.

The rest of the paper is organized as follows. In Section 2 we discuss modeling aspects of the wireless network, and the CJ protocol. A detailed treatment of the protocol and optimal solutions in closed–form are derived in Section 3. Simulation results and concluding remarks are given in Sections 4, 5.

2. MODELING ASPECTS AND COOPERATION

The following notation is used hereinafter. Letters in boldface are column vectors $\boldsymbol{x}$ if lowercase, or matrices $\boldsymbol{X}$ otherwise. Conjugate and conjugate transpose are written as $\boldsymbol{x}^*$ and $\boldsymbol{x}^\dagger$, whereas $\|\boldsymbol{x}\|^2 = \boldsymbol{x}^\dagger\boldsymbol{x}$. The notation $\boldsymbol{X} \succ 0$ (resp. $\boldsymbol{X} \succcurlyeq 0$) is for positive definite (resp. semi–definite) matrices [10], and $\boldsymbol{I}_N$ for the order N identity matrix. The circularly symmetric complex Gaussian distribution with mean μ and variance σ^2 is denoted as $\mathcal{CN}(\mu, \sigma^2)$.

2.1. System Model

The wireless network considered is shown in Fig. 1, where a pair of nodes desire to communicate securely in the presence of an eavesdropper. The communication is assisted by $N \geq 1$ helpers that utilize the CJ cooperative protocol. All nodes are equipped with a single omni–directional antenna and operate in half–duplex mode. The source and the helping nodes are indexed by $i = 0$ and $i = 1, \ldots, N$ respectively.

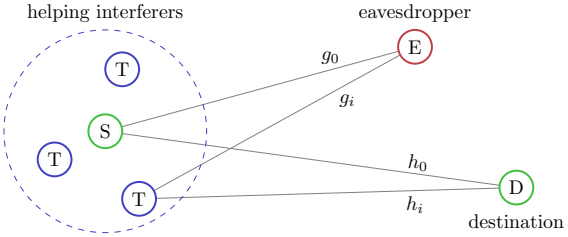

Fig. 1. The system model.

Global CSI is assumed to be available at the trusted nodes [6, 7, 17, 24]; that is, the channels gains h_0^*, g_0^* (resp. h_i^*, g_i^*) from the source (resp. ith helper) to the destination and the eavesdropper are known to allow for coordination. When the source transmits a symbol x using power P, the signal at the destination and the eavesdropper is given by

$$\begin{aligned} y_{\mathsf{D}} &= \sqrt{P} h_0^* x + \eta_{\mathsf{D}} \\ y_{\mathsf{E}} &= \sqrt{P} g_0^* x + \eta_{\mathsf{E}} \end{aligned} \tag{1}$$

where $\mathbb{E}[|x|^2] = 1$ is assumed and $\eta_{\mathsf{D}}, \eta_{\mathsf{E}} \sim \mathcal{CN}(0, \sigma^2)$. This corresponds to the case of direct transmission (DT) where the source uses all its power budget for transmitting the signal to the destination. The SNR at the destination and eavesdropper is $\gamma_{\mathsf{D}} = P|h_0|^2/\sigma^2$ and $\gamma_{\mathsf{E}} = P|g_0|^2/\sigma^2$ respectively.

2.2. Cooperative Protocol

The helpers cooperate with the source via the CJ protocol to securely transmit information to the destination. It is assumed that the existence and number N of helpers is a priori known. In addition, we suppose that the destination and the helping nodes have knowledge of the common jamming signal z to be used, where likewise we let $\mathbb{E}[|z|^2] = 1$.

More precisely, assuming that P is the power available for transmitting both signals x and z, the trusted nodes decide on allocating αP power, $\alpha \in [0, 1)$, for the jamming signal and the remaining $(1-\alpha)P$ power for transmitting the symbol x. The ith helping node transmits a weighted version $w_i z$ of the common jamming signal while the source transmits x. Then, the signal received at the destination and the eavesdropper is

$$\begin{aligned} y_{\mathsf{D}} &= \sqrt{(1-\alpha)P} h_0^* x + \sqrt{\alpha P} \boldsymbol{h}^\dagger \boldsymbol{w} z + \eta_{\mathsf{D}} \\ y_{\mathsf{E}} &= \sqrt{(1-\alpha)P} g_0^* x + \sqrt{\alpha P} \boldsymbol{g}^\dagger \boldsymbol{w} z + \eta_{\mathsf{E}} \end{aligned} \tag{2}$$

where $\boldsymbol{w}^\dagger = (w_1^* \cdots w_N^*)$ contains the weights being used by the helping interferers with $\|\boldsymbol{w}\| = 1$ and $\boldsymbol{h}^\dagger = (h_1^* \cdots h_N^*)$; the vector $\boldsymbol{g}$ is similarly defined. The SNR at the destination and the eavesdropper becomes

$$\begin{aligned} \gamma_{\mathsf{D}}^{\mathsf{CJ}} &= \gamma_{\mathsf{D}} \cdot (1-\alpha)\sigma^2 / (\alpha P \boldsymbol{w}^\dagger \boldsymbol{h}\boldsymbol{h}^\dagger \boldsymbol{w} + \sigma^2) \\ \gamma_{\mathsf{E}}^{\mathsf{CJ}} &= \gamma_{\mathsf{E}} \cdot (1-\alpha)\sigma^2 / (\alpha P \boldsymbol{w}^\dagger \boldsymbol{g}\boldsymbol{g}^\dagger \boldsymbol{w} + \sigma^2) \end{aligned} \tag{3}$$

under the assumption that $\boldsymbol{h}^\dagger \boldsymbol{w}$ (resp. $\boldsymbol{g}^\dagger \boldsymbol{w}$) and η_{D} (resp. η_{E}) are independent random variables. From (3) we immediately obtain $\gamma_{\mathsf{D}}^{\mathsf{CJ}} \leq \gamma_{\mathsf{D}}$ and $\gamma_{\mathsf{E}}^{\mathsf{CJ}} \leq \gamma_{\mathsf{E}}$, due to the fact that $\boldsymbol{h}\boldsymbol{h}^\dagger \succcurlyeq 0$ and $\boldsymbol{g}\boldsymbol{g}^\dagger \succcurlyeq 0$ respectively, where both upper bounds hold with equality if and only if $\alpha = 0$. The jamming signal's to noise power ratio $\varepsilon_{\mathsf{D}} = P\|\boldsymbol{h}\|^2/\sigma^2$ at the destination is defined, and corresponds to the case where all power goes to jamming (i.e. $\alpha = 1$) and the angle between $\boldsymbol{h}, \boldsymbol{w}$ equals $0, \pm\pi$. Likewise, we define $\varepsilon_{\mathsf{E}} = P\|\boldsymbol{g}\|^2/\sigma^2$ at the eavesdropper.

3. SYSTEM DESIGN

Let $\Gamma_{\mathsf{D}}^{\mathsf{CJ}}$ and $\Gamma_{\mathsf{E}}^{\mathsf{CJ}}$ denote the values of $\gamma_{\mathsf{D}}^{\mathsf{CJ}}, \gamma_{\mathsf{E}}^{\mathsf{CJ}}$ in dB. Our goal is to maximize the difference $\Delta\Gamma^{\mathsf{CJ}} = \Gamma_{\mathsf{D}}^{\mathsf{CJ}} - \Gamma_{\mathsf{E}}^{\mathsf{CJ}}$, referred to as the security gap in [13, 14]. In other words, the transmitting nodes need to determine the optimal power allocation $\alpha^\star$ and the weights $\boldsymbol{w}^\star$ that maximize the security gap

$$\begin{aligned} (\alpha^\star, \boldsymbol{w}^\star) &= \arg\max_{\alpha, \boldsymbol{w}} \gamma_{\mathsf{D}}^{\mathsf{CJ}} / \gamma_{\mathsf{E}}^{\mathsf{CJ}} && (4) \\ &= \arg\max_{\alpha, \boldsymbol{w}} \frac{\gamma_{\mathsf{D}}}{\gamma_{\mathsf{E}}} \cdot \frac{\alpha P \boldsymbol{w}^\dagger \boldsymbol{g}\boldsymbol{g}^\dagger \boldsymbol{w} + \sigma^2}{\alpha P \boldsymbol{w}^\dagger \boldsymbol{h}\boldsymbol{h}^\dagger \boldsymbol{w} + \sigma^2} \\ \text{s.t.} \quad & \alpha \in [0, 1) && (4a) \\ & \|\boldsymbol{w}\| = 1 && (4b) \\ & \gamma_{\mathsf{D}}^{\mathsf{CJ}} \geq \gamma^+ && (4c) \\ & \gamma_{\mathsf{E}}^{\mathsf{CJ}} \leq \gamma^- && (4d) \end{aligned}$$

The above constraints pertain to power allocation (4a)–(4b), reliability (4c), as well as, security (4d). The minimum SNR at the destination is denoted by γ^+ and is chosen so that high communication reliability is attained, and γ^- corresponds to the maximum desirable SNR at the adversary. An interesting approach to determine a suitable value for γ^-, assuming that eavesdroppers have bounded resources (computational, time, and memory), has been recently proposed in [14].

In the sequel we assume that $\alpha \neq 0$ for the analysis of CJ protocol to be meaningful. Note that DT is obtained from (2) for $\alpha = 0$, in which case (4) gives $\gamma_{\mathsf{D}}^{\mathsf{CJ}}/\gamma_{\mathsf{E}}^{\mathsf{CJ}} = \gamma_{\mathsf{D}}/\gamma_{\mathsf{E}}$ whereas $\gamma_{\mathsf{D}}^{\mathsf{CJ}} < \gamma_{\mathsf{D}}$ and $\gamma_{\mathsf{E}}^{\mathsf{CJ}} < \gamma_{\mathsf{E}}$ from (3). Let us define

$$b_j(x) = \frac{\gamma_j - x}{\gamma_j + \varepsilon_j x} \quad \text{and} \quad c_j(x) = \frac{\gamma_j - x}{\gamma_j} \tag{5}$$

for $j \in \{\mathsf{D}, \mathsf{E}\}$, where both functions map all $x \in (0, \gamma_j)$ into the interval $(0, 1)$ and $b_j(x) < c_j(x)$ holds. In order to solve (4), we reformulate the fractional optimization problem based

on an approach due to Dinkelbach [5] as follows ($\gamma_{\mathsf{D}}/\gamma_{\mathsf{E}}$ does not depend on $\alpha, \boldsymbol{w}$ and can therefore be omitted):

$$\begin{aligned} F(t) &= \max_{\alpha,\boldsymbol{w}} f(t,\alpha,\boldsymbol{w}) \qquad (6)\\ &= \max_{\alpha,\boldsymbol{w}} \alpha P \boldsymbol{w}^\dagger \big(\boldsymbol{g}\boldsymbol{g}^\dagger - t\boldsymbol{h}\boldsymbol{h}^\dagger\big)\boldsymbol{w} + \big(1-t\big)\sigma^2 \\ \text{s.t.}\quad & \alpha \in (0,1) \qquad (6a)\\ & \boldsymbol{w}^\dagger\boldsymbol{w} = 1 \qquad (6b)\\ & \boldsymbol{w}^\dagger\boldsymbol{h}\boldsymbol{h}^\dagger\boldsymbol{w} \le q_{\mathsf{D}}(\alpha) \qquad (6c)\\ & \boldsymbol{w}^\dagger\boldsymbol{g}\boldsymbol{g}^\dagger\boldsymbol{w} \ge q_{\mathsf{E}}(\alpha) \qquad (6d) \end{aligned}$$

where the reliability and security constraints are expressed in terms of the functions $q_{\mathsf{D}}(x) = (c_{\mathsf{D}}(\gamma^+) - x)|h_0|^2/\gamma^+ x$ and $q_{\mathsf{E}}(x) = (c_{\mathsf{E}}(\gamma^-) - x)|g_0|^2/\gamma^- x$. The next lemma is easy to prove using (5) and the definitions of $q_{\mathsf{D}}, q_{\mathsf{E}}$.

Lemma 1. *The conditions* (a) $\gamma^+ < \gamma_{\mathsf{D}}$, (b) $\gamma^- < \gamma_{\mathsf{E}}$ *and* (c) $\gamma^+ < p(\gamma^-)$[1] *must hold for a nonempty feasibility set in* (6)*.*

It is known that the original problem (4) and the one in (6) are related via the following result.

Proposition 1 ([17])**.** *With the above notation, $F(t)$ is strictly decreasing and $F(t) = 0$ has a unique root $t^\star$. Moreover, the optimal $(\alpha^\star, \boldsymbol{w}^\star)$ of* (6) *associated with $t^\star$ is also the solution of the original problem* (4)*, and $t^\star\gamma_{\mathsf{D}}/\gamma_{\mathsf{E}}$ is the optimal value taken by the objective function.*

We now proceed with the analysis of (6) by first defining the associated Lagrangian and then determining the Karush–Kuhn–Tucker (KKT) conditions that must be satisfied by any optimal solution [3]. From (6), its Lagrangian is given by

$$\begin{aligned} \mathcal{L}(t,\alpha,\boldsymbol{w},\boldsymbol{\lambda}) = &- f(t,\alpha,\boldsymbol{w}) + \lambda_{\mathsf{D}}\big(\boldsymbol{w}^\dagger\boldsymbol{h}\boldsymbol{h}^\dagger\boldsymbol{w} - q_{\mathsf{D}}(\alpha)\big) \\ &+ \lambda_{\mathsf{P}}\big(\boldsymbol{w}^\dagger\boldsymbol{w} - 1\big) - \lambda_{\mathsf{E}}\big(\boldsymbol{w}^\dagger\boldsymbol{g}\boldsymbol{g}^\dagger\boldsymbol{w} - q_{\mathsf{E}}(\alpha)\big) \end{aligned}$$

where $\boldsymbol{\lambda} = (\lambda_{\mathsf{P}}\ \lambda_{\mathsf{D}}\ \lambda_{\mathsf{E}})$ is the vector of Lagrange multipliers corresponding to the constraints (6b)–(6d). By using the KKT conditions, it is not difficult to show that the constraint

$$\lambda_{\mathsf{D}}^\star \frac{|h_0|^2}{\gamma^+} = \lambda_{\mathsf{E}}^\star \frac{|g_0|^2}{\gamma^-} + \lambda_{\mathsf{P}}^\star \qquad (7)$$

is obtained on the optimal value $\boldsymbol{\lambda}^\star$ of Lagrange multipliers. Then, from (7) and the fact that $\lambda_{\mathsf{P}}^\star \neq 0$ and $\lambda_{\mathsf{D}}^\star, \lambda_{\mathsf{E}}^\star \ge 0$ should hold, we conclude that at least one of the multipliers $\lambda_{\mathsf{D}}^\star, \lambda_{\mathsf{E}}^\star$ is nonzero, therefore proving the following result.

Proposition 2. *The optimal solution $(\alpha^\star, \boldsymbol{w}^\star)$ of* (6) *is such that either* (6c) *or* (6d) *is satisfied with equality.*

Next, we suppose that the reliability constraint (6c) holds with equality and determine the unique optimal solution. The analysis for the case where the optimal solution satisfies (6d) with equality is similar (it is omitted due to space limitations). Substituting $\boldsymbol{w}^\dagger\boldsymbol{h}\boldsymbol{h}^\dagger\boldsymbol{w} = q_{\mathsf{D}}(\alpha)$ into the objective function of (6) we see that the function $F(t)$ is written as

$$F(t) = \big(1-t\big)\sigma^2 + P\max_{\alpha}\ \alpha\big(-tq_{\mathsf{D}}(\alpha) + \max_{\boldsymbol{w}} |\boldsymbol{g}^\dagger\boldsymbol{w}|^2\big)$$

and therefore we first proceed to solve the quadratic problem $\boldsymbol{w}^\star = \arg\max_{\boldsymbol{w}} \boldsymbol{w}^\dagger\boldsymbol{g}\boldsymbol{g}^\dagger\boldsymbol{w}$ subject to (6b)–(6d) where (6c) is satisfied with equality. It is readily shown using $\boldsymbol{h}\boldsymbol{h}^\dagger \succcurlyeq 0$ and $\boldsymbol{g}\boldsymbol{g}^\dagger \succcurlyeq 0$ that for the constraints (6c) and (6d) to hold we need to have $\alpha \in \mathscr{A} = [b_{\mathsf{E}}(\gamma^-), c_{\mathsf{D}}(\gamma^+)]$.

Theorem 1. *Let $\theta = \boldsymbol{h}\angle\boldsymbol{g}$ be the angle between $\boldsymbol{h}, \boldsymbol{g}$ and let $\gamma^+ > p'(\gamma^-)$[2]. For all $\alpha \in \mathscr{A}$, the optimal solution $\boldsymbol{w}^\star$ of*

$$\max_{\boldsymbol{w}} \boldsymbol{w}^\dagger\boldsymbol{g}\boldsymbol{g}^\dagger\boldsymbol{w} \quad \text{s.t.} \begin{cases} \boldsymbol{w}^\dagger\boldsymbol{w} = 1 \\ \boldsymbol{w}^\dagger\boldsymbol{h}\boldsymbol{h}^\dagger\boldsymbol{w} = q_{\mathsf{D}}(\alpha) \\ \boldsymbol{w}^\dagger\boldsymbol{g}\boldsymbol{g}^\dagger\boldsymbol{w} \ge q_{\mathsf{E}}(\alpha) \end{cases} \qquad (8)$$

is given by $\boldsymbol{w}^\star = v_{\mathsf{D}}\,\boldsymbol{h} + v_{\mathsf{E}}\,\boldsymbol{g}$, and $\forall\,\phi \in [0, 2\pi)$ we have

$$v_{\mathsf{D}} = \tfrac{1}{\|\boldsymbol{h}\|^2}\big(|v_{\mathsf{E}}|\,|\boldsymbol{h}^\dagger\boldsymbol{g}| - \sqrt{q_{\mathsf{D}}(\alpha)}\big)\cdot e^{j\phi} \qquad (9a)$$

$$v_{\mathsf{E}} = \tfrac{1}{\rho}\sqrt{\|\boldsymbol{h}\|^2 - q_{\mathsf{D}}(\alpha)}\cdot e^{j(\phi-\theta+\pi)} \qquad (9b)$$

where $\rho = \|\boldsymbol{h}\|\|\boldsymbol{g}\|\,|\sin\theta\,|$.

The solution $\boldsymbol{w}^\star$ provided by Theorem 1 (whose proof is extensive and will be included in the full paper) depends on α according to (9). Let us define $k = |h_0|^2(|\boldsymbol{h}^\dagger\boldsymbol{g}|^2 - \rho^2)/\|\boldsymbol{h}\|^4$ and $l = 2\rho|h_0|^2|\boldsymbol{h}^\dagger\boldsymbol{g}|/\|\boldsymbol{h}\|^4$. Substitution of $\boldsymbol{w}^\star$ yields

$$f(x,\alpha) = r - \big(1-\alpha\big)\,x + \sqrt{s(\alpha)} \qquad (10)$$

where r, and the coefficients of the quadratic function $s(\alpha) = -s_0 + s_1\alpha - s_2\alpha^2$, are provided below

$$r = \frac{\rho^2}{\|\boldsymbol{h}\|^2} + \frac{|h_0|^2}{\gamma_{\mathsf{D}}} + k\left(\frac{2}{\gamma^+} - \frac{1}{\gamma_{\mathsf{D}}}\right) \qquad (11a)$$

$$s_0 = l^2\left(\frac{1}{\gamma^+} - \frac{1}{\gamma_{\mathsf{D}}}\right)^2 \qquad (11b)$$

$$s_1 = l^2\left(\frac{1}{\gamma^+} - \frac{1}{\gamma_{\mathsf{D}}}\right)\left(\frac{\|\boldsymbol{h}\|^2}{|h_0|^2} + \frac{2}{\gamma^+}\right) \qquad (11c)$$

$$s_2 = l^2\left(\frac{\|\boldsymbol{h}\|^2}{|h_0|^2} + \frac{1}{\gamma^+}\right)\frac{1}{\gamma^+} \qquad (11d)$$

and the change of variables $x = \frac{1}{\|\boldsymbol{h}\|^2}\rho^2 + \frac{1}{\gamma^+}(k + t|h_0|^2)$ is performed to simplify the resulting expression. To determine the optimal $\alpha^\star$ maximizing (10), we need to consider the case $\theta = 0, \pm\pi$ separately, since then $s(\alpha)$ is identically zero (due to $l = 0$), and the derivative of the square root is not defined. As f becomes a linear function of α in this case, we clearly have that $\alpha^\star \in \{b_{\mathsf{E}}(\gamma^-), c_{\mathsf{D}}(\gamma^+)\}$ and the particular value of

[1] $p(x) = \gamma_{\mathsf{D}}(x + \varepsilon_{\mathsf{E}}x)/(\gamma_{\mathsf{E}} + \varepsilon_{\mathsf{E}}x)$

[2] $p'(x) = \gamma_{\mathsf{D}}(x + \varepsilon_{\mathsf{E}}x)/(\gamma_{\mathsf{E}} + \varepsilon_{\mathsf{E}}x + \varepsilon_{\mathsf{D}}(\gamma_{\mathsf{E}} - x)\cos^2\theta)$

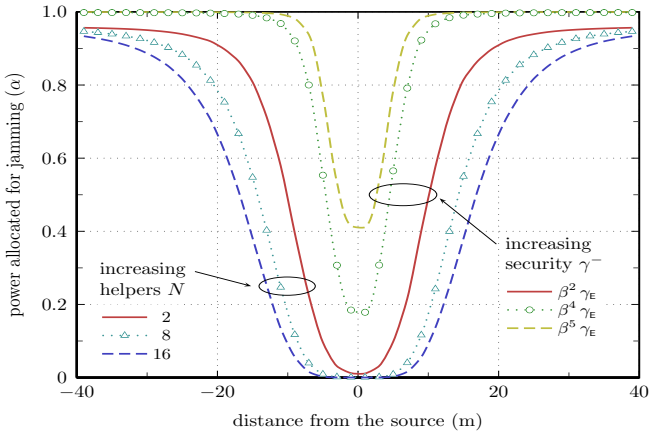

Fig. 2. Fraction α of the power P allocated to jamming for various values of N, γ^- ($\beta = 0.2$, angle $= 0 \cdot \frac{\pi}{8}$)

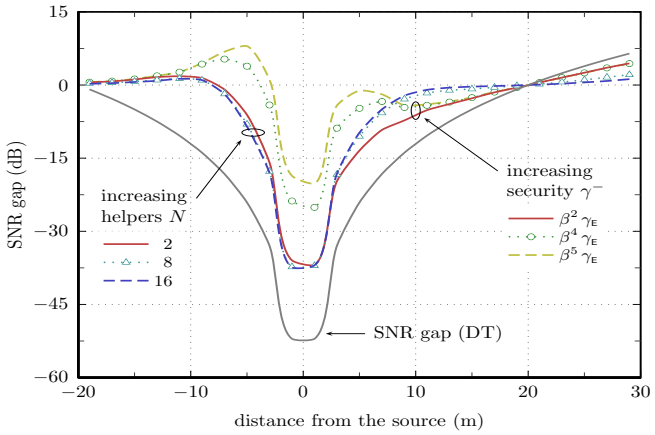

Fig. 3. The SNR gap between destination / eavesdropper for various values of N, γ^- ($\beta = 0.2$, angle $= 0 \cdot \frac{\pi}{8}$)

$\alpha^\star$ depends on the sign of x. It is not difficult to show that we have $s(c_{\mathsf{D}}(\gamma^+)) = 0$ and that the second root of $s(\alpha)$ does not lie in the interval $\mathscr{A}$ under the assumptions of Theorem 1; the value of f at $\alpha = c_{\mathsf{D}}(\gamma^+)$ must be compared with the optimal value derived from Theorem 2.

Theorem 2. *Let $\mathscr{A}^\diamond = \mathscr{A} \setminus \{c_{\mathsf{D}}(\gamma^+)\}$ and $\delta_{\mathsf{S}} = s_1^2 - 4 s_0 s_2$. With the notation of Theorem 1, if $\theta \neq 0, \pm\pi$, the value*

$$\alpha^\star = \frac{s_1}{2 s_2} + \frac{x}{2 s_2} \cdot \frac{\sqrt{\delta_{\mathsf{S}}}}{\sqrt{s_2 + x^2}} \tag{12}$$

is the optimal solution of the problem $F(x) = \max_\alpha f(x, \alpha)$ s.t. $\alpha \in \mathscr{A}^\diamond$, where f is given by (10).

As expected, the solution given by Theorem 2 depends on x (the proof is omitted due to space limitations). To compute the actual values of $(\alpha^\star, \boldsymbol{w}^\star)$ we need to determine the root of $F(x)$ first; the solution is provided in Theorem 3.

Theorem 3. *With the above notation, the equation $F(x) = 0$ has a unique root $x^\star$ that is given by*

$$x^\star = \frac{r\,(s_1 - 2 s_2) - \sqrt{\delta_{\mathsf{S}}} \cdot \sqrt{r^2 - s(1)}}{2\, s(1)} \tag{13}$$

where $s(1)$ is the value of s at $\alpha = 1$; the optimal value of the original problem (4) *is $t^\star = \frac{\gamma_{\mathsf{D}} \gamma^+}{\gamma_{\mathsf{E}} |h_0|^2} \left(x^\star - \frac{\rho^2}{\|\boldsymbol{h}\|^2} - \frac{k}{\gamma^+} \right)$.*

4. SIMULATION RESULTS

In the simulations, helping nodes are assumed to be randomly distributed in a disk of radius 5m with the source at its center; the destination is fixed at 20m distance from the source, while the eavesdropper is moving on a line that passes through the source at a fixed angle $i \cdot \frac{\pi}{8}$, for $i = 0, \ldots, 4$. A simple line–of–sight model is assumed $h = d^{-\frac{c}{2}} e^{j\varphi}$ between a transmitter and a receiver, where d is their distance, φ their phase offset, and $c = 4$ is the path loss exponent. The noise variance σ^2 is equal to -30dBm. We evaluated the performance of the CJ scheme, by solving problem (4) according to Theorems 1, 2, and 3. The experiments included varying number of helpers and values γ^+, γ^-. Monte–Carlo simulations are performed and each setup is repeated 10^3 times to get average results.

The power devoted to jamming is shown in Fig. 2, versus the distance of the eavesdropper form the source. The helping nodes devote less power whenever the eavesdropper is close to the source (and hence close to their location) as the helper–eavesdropper channel is then not greatly affected by path loss in such cases. Decreasing the upper bound γ^- in the SNR, is shown to increase the fraction α of the power P that goes to jamming even when the eavesdropper is at the proximity of the interferers. On the other hand, an increase in the number N of helpers —although it does not result in a corresponding increase of the SNR gap (as illustrated in Fig. 3)— it utilizes the available power in a more efficient way, attaining about the same security gap with less power on jamming.

N	γ^-	d: -12	-8	-4	4	8	12
2	$\beta^5 \gamma_{\mathsf{E}}$	11.22	21.72	33.07	25.85	13.03	5.27
16	$\beta^2 \gamma_{\mathsf{E}}$	10.00	15.62	15.25	14.55	12.47	8.17

The table shows an SNR gap increase up to 33dB if the eavesdropper is close to the source ($\beta = 0.2$, angle $= 0 \cdot \frac{\pi}{8}$).

5. CONCLUSIONS

A cooperative jamming protocol is presented that allows two wireless nodes to communicate securely in the presence of an eavesdropper. Closed–form expressions have been given for the case of a single eavesdropper. The proposed protocol has shown to perform very well in the case that the S–E channel is superior than that of the S–D channel. Ongoing work focuses on extensions to multiple eavesdroppers.

6. REFERENCES

[1] R. Bassily, E. Ekrem, *et al.*, "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, 2013.

[2] M. Bloch and J. Barros, *Physical–Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

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

[5] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, 1967.

[6] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in proc. *IEEE SSP '09*, pp. 417–420, 2009.

[7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, 2010.

[8] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in proc. *IEEE ICC '11*, pp. 1–5, 2011.

[9] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, 2011.

[10] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 4th ed. Johns Hopkins University Press, 2013.

[11] X. He and A. Yener, "Two–hop secure communication using an untrusted relay: a case for cooperative jamming," in proc. *IEEE GLOBECOM '08*, pp. 1–5, 2008.

[12] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, 2011.

[13] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, 2011.

[14] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "Cooperation for secure wireless communications with resource–bounded eavesdroppers," in proc. *IEEE GLOBECOM '14 — Wksp Physical Layer Security*, pp. 1483–1488, 2014.

[15] L. Lai and H. El Gamal, "The relay–eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[16] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire–tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[17] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, pp. 4985–4997, 2011.

[18] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi–antenna transmission,", in proc. *CISS '07*, pp. 905–910, 2007.

[19] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Now Publishers, 2009.

[20] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical–layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, 2013.

[21] R. Liu and W. Trappe (Eds.), *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[22] S. Luo, J. Li, and A. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1081–1090, 2013.

[23] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[24] R. Negi and S. Goehm, "Secret communication using artificial noise," in proc. *IEEE VTC '05*, vol. 3, pp. 1906–1910, 2005.

[25] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in proc. *IEEE ISIT '07*, pp. 2466–2470, 2007.

[26] L. Tang, X. Gong, J. Wu, and J. Zhang, "Secure wireless communications via cooperative relaying and jamming," in proc. *IEEE GLOBECOM '11 — Wksp Physical Layer Security*, pp. 849–853, 2011.

[27] A. D. Wyner, "The wire–tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[28] G. Zheng, L.-C. Choo, and K.-. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, 2011.