Secure Communications With Cooperative Jamming: Optimal Power Allocation and Secrecy Outage Analysis

Kanapathippillai Cumanan, *Member, IEEE*, George C. Alexandropoulos, *Senior Member, IEEE*, Zhiguo Ding, *Senior Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—This paper studies the secrecy rate maximization problem of a secure wireless communication system in the presence of multiple eavesdroppers. The security of the communication link is enhanced through cooperative jamming with the help of multiple jammers. First, a feasibility condition is derived to achieve a positive secrecy rate at the destination. Then, we solve the original secrecy rate maximization problem, which is not convex in terms of power allocation at the jammers. To circumvent this nonconvexity, the achievable secrecy rate is approximated for a given power allocation at the jammers, and the approximated problem is formulated into a geometric programming one. Based on this approximation, an iterative algorithm has been developed to obtain the optimal power allocation at the jammers. Next, we provide a bisection approach, based on 1-D search, to validate the optimality of the proposed algorithm. In addition, by assuming Rayleigh fading, the secrecy outage probability (SOP) of the proposed cooperative jamming scheme is analyzed. More specifically, a single-integral form expression for the SOP is derived for the most general case, as well as a closed-form expression for the special case of two cooperative jammers and one eavesdropper. Simulation results have been provided to validate the convergence and the optimality of the proposed algorithm, as well as the theoretical derivations of the presented SOP analysis.**

***Index Terms*—Cooperative jamming, Convex optimization, physical layer security, secrecy outage analysis.**

I. Introduction

PHYSICAL (PHY) layer security has recently received considerable attention as a significant candidate to enhance the quality of secure communication in emerging and future wireless networks, including the fifth-generation standard [1]. In this new paradigm, the propagation characteristics of wireless channels are exploited against passive eavesdroppers and active attacks through PHY layer secret key generation and authentication schemes, while complementing the conventional cryptographic methods [2]. The fundamental concept of information-theoretic security was first investigated in [3] and [4], where it was shown that secure communication is feasible when the channel quality of legitimate parties is better than that of the eavesdropper. However, in practice, this is not always possible, and therefore, the performance of PHY layer security is limited.

In order to circumvent the performance limitations introduced by the unfavorable wireless channel conditions, cooperative jamming has been proposed as an enabler of secrecy communication [5]–[14]. Under this approach, jamming signals are transmitted to improve the secrecy rate performance, by introducing interference at the eavesdroppers. In [15], different secrecy rate optimization problems have been solved for a relay network based on cooperative jamming, where the relays transmit noise to confound the eavesdroppers. However, these optimization problems have been considered with a total relay power constraint. For the same network, a cooperative jamming scheme has been proposed in [16] with no interference leakage to the legitimate user. Furthermore, in [17], opportunistic cooperative jamming and relay chatting schemes have been developed, without the knowledge of eavesdropper channel state information (CSI), and the performance of these schemes has been evaluated through the secrecy outage probability (SOP) criterion. On the other hand, in [18], an uncoordinated cooperative jamming scheme with multiantenna relays has been investigated by nulling the interference leakage at the destination, and the corresponding SOP has been quantified with eavesdroppers' statistical CSI. In [19], an optimal cooperative jamming scheme has been proposed with multiple relays in the presence of a single eavesdropper, where the optimal relay coefficients have been obtained through an 1-D search scheme.

The SOP of a multiuser wireless communication system, which consists of multiple users who transmit to a base station, while multiple eavesdroppers attempt to tap their transmissions, has been analyzed over Rayleigh fading channels in [20]. In [21], a closed-form expression of the SOP was derived for Rayleigh fading channels in a secrecy network with a multi-antenna source and a single-antenna destination in the presence

Manuscript received March 21, 2016; revised August 8, 2016; accepted December 4, 2016. Date of publication January 24, 2017; date of current version August 11, 2017. The work of K. Cumanan and Z. Ding was supported by H2020-MSCARISE-2015 under Grant 690750. The work of Z. Ding was supported by the Engineering and Physical Sciences Research Council, U.K., under Grant EP/L025272/1. The review of this paper was coordinated by Dr. C. Xing.

K. Cumanan is with the Department of Electronics, University of York, York YO10 5DD, U.K. (e-mail: kanapathippillai.cumanan@york.ac.uk).

G. C. Alexandropoulos is with the Mathematical and Algorithmic Sciences Laboratory, France Research Center, Huawei Technologies France, 92100 Boulogne-Billancourt, France (e-mail: george.alexandropoulos@huawei.com).

Z. Ding is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mail: z.ding@lancaster.ac.uk).

G. K. Karagiannidis is with the Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece (e-mail: geokarag@auth.gr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2017.2657629

of a single-antenna eavesdropper. Finally, in [22], the SOP performance of the multiple-input multiple-output wiretap channel, employing transmit antenna selection and receive generalized selection combining, has been analyzed over Nakagami-m fading channels.

In this paper, we consider a PHY layer security network with single-antenna nodes, where a source–destination pair establishes secured communication, with the help of multiple jammers in the presence of multiple eavesdroppers. For this network setup, we first present a feasibility condition to achieve a positive secrecy rate at the destination. Then, the secrecy rate maximization problem is solved to determine the optimal power allocation at the jammers, which is a nonconvex problem in nature. In order to overcome the nonconvexity of the secrecy rate function, we approximate it for a given power allocation at the jammers and formulate the problem into a geometric programming one. Based on this approximation, an iterative algorithm is developed by updating a better power allocation at each iteration. To validate the optimality of the presented results, we use 1-D search based on bisection to determine the optimal power allocation of the original secrecy rate maximization problem. Both the proposed and the 1-D search algorithms yield identical results, which confirms the optimality of the proposed algorithm. Moreover, the SOP of the proposed scheme is analyzed over Rayleigh fading channels. A single-integral form expression for the SOP is presented for the most general scenario, whereas a closed-form expression is derived for the special case of two cooperative jammers and one eavesdropper. Finally, numerical and simulation results have been provided to validate the theoretical derivations.

The remainder of this paper is organized as follows. The system model and the secrecy rate maximization problem formulation are presented in Section II. A feasibility condition to achieve positive secrecy rate is provided in Section III, whereas Section IV presents an iterative approach for an approximated secrecy rate maximization problem. In Section V, the optimality of the proposed scheme is validated through 1-D search. The SOP analysis is derived in Section VI for Rayleigh fading channels, whereas Section VII provides numerical and simulation results to validate the performance of the proposed algorithm and the derived theoretical SOP expressions. Finally, Section VIII concludes this paper.

Notations: We use lowercase boldface letters for vectors. $(\cdot)^T$ and $|\cdot|$ denote the transpose of a vector and absolute value of a complex number, respectively. $[x]^+$ represents $\max\{\mathrm{x}, 0\}$, whereas $E\{\cdot\}$, $\Pr[\cdot]$, and $\nabla(\cdot)$ denote expectation, probability, and gradient operator, respectively. The cumulative distribution function (CDF) and the probability density function (PDF) of a random variable (RV) X are represented as $F_X(\cdot)$ and $f_X(\cdot)$, respectively. $\mathrm{Ei}(\cdot)$ is the exponential integral [23, eq. (8.211/1)].

II. System Model

We consider a secrecy network, as shown in Fig. 1, with one source S, which communicates with a destination D and N cooperative jammers $J_1, J_2, \ldots, J_N$ in the presence of M eavesdroppers $E_1, E_2, \ldots, E_M$. The source S wishes to transmit secured information to destination D. It is assumed that all network nodes are equipped with a single antenna. The channel coefficient between S and D is denoted by h_D, whereas h_{Em} represents the channel gain between S and the mth eavesdropper E_m, with $m = 1, 2, \ldots, M$. In addition, the channel coefficients between the nth cooperative jammer J_n and D as well as E_m are denoted by $g_D^{(n)}$ and $g_{Em}^{(n)}$, respectively. The CSI between all nodes is assumed to be perfectly available at S, D, and E_m $\forall m$. The source S transmits signals to destination D, whereas all jammers send interference signals to confound the eavesdroppers.

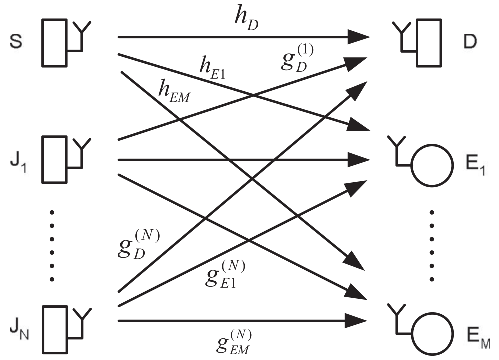


Fig. 1. Considered secrecy network with one source, one destination, and multiple jammers in the presence of multiple eavesdroppers.

The received signals at D and E_m can be mathematically expressed, respectively, as

$$y_D = \sqrt{P_s} h_D x_s + \sum_{i=1}^{N} \sqrt{P_i} g_D^{(i)} x_c^{(i)} + \eta_D \tag{1}$$

$$y_{Em} = \sqrt{P_s} h_{Em} x_s + \sum_{i=1}^{N} \sqrt{P_i} g_{Em}^{(i)} x_c^{(i)} + \eta_{Em} \tag{2}$$

where x_s $(\mathbb{E}\{|x_s|^2\} = 1)$ and $x_c^{(i)}$ $(\mathbb{E}\{|x_c^{(i)}|^2\} = 1)$ denote the transmitted signal from S to D and the jamming signal from the ith jammer J_i, respectively. In addition, η_D $(\mathbb{E}\{|\eta_D|^2\} = \sigma_D^2)$ and η_{Em} $(\mathbb{E}\{|\eta_{Em}|^2\} = \sigma_{Em}^2)$ represent the noise at node D and mth eavesdropper E_m, respectively. The power allocation at J_i and S are denoted by P_i and P_s, respectively. Assuming white Gaussian noise, the achievable secrecy rate at D is defined as

$$R_s = \left[\log_2(1 + \gamma_D) - \log_2(1 + \gamma_{E_{\max}})\right]^+ \tag{3}$$

where $\gamma_{E_{\max}} = \max\{\gamma_{E1}, \gamma_{E2}, \ldots, \gamma_{EM}\}$, and γ_D and γ_{Em} are the signal-to-interference plus noise ratios at D and E_m, respectively, given by

$$\gamma_D = \frac{P_s |h_D|^2}{\sum_{i=1}^{N} P_i |g_D^{(i)}|^2 + \sigma_D^2} \tag{4}$$

$$\gamma_{Em} = \frac{P_s |h_{Em}|^2}{\sum_{i=1}^{N} P_i |g_{Em}^{(i)}|^2 + \sigma_{Em}^2}. \tag{5}$$

For the secrecy network studied in this paper, we consider secrecy rate maximization with a transmit power constraint. In particular, we intend to maximize the achievable secrecy rate at the destination node D, with the available transmit power at the source node and all N available jammers. The secrecy rate maximization problem can be, therefore, formulated as

$$\begin{aligned} \text{P1}: \quad & \max_{\mathbf{p}\succeq\mathbf{0}} \quad R_s \\ & \text{s.t.} \quad P_i \leq \bar{P}_i \quad \forall i \end{aligned} \tag{6}$$

where $\bar{P}_i$ is the maximum available transmit power at J_i and $\mathbf{p} = [P_1\, P_2\, \cdots\, P_N]^T$.

III. Feasibility Conditions for a Positive Secrecy Rate

The optimization problem P1, formulated in (6), is valid or worth to solve only when it is possible to achieve a positive secrecy rate for a given set of channels and transmit powers at D and J_is. Through verifying these feasibility conditions, the source can make a decision whether to solve the secrecy rate maximization to obtain a positive secrecy rate at the destination. Hence, we first investigate the feasibility conditions. From (3), the following conditions need to be satisfied for $m = 1, 2, \ldots, M$:

$$\frac{P_s|h_D|^2}{\sum_{i=1}^N P_i|g_D^{(i)}|^2 + \sigma_D^2} > \frac{P_s|h_{Em}|^2}{\sum_{i=1}^N P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2}. \tag{7}$$

By arranging the terms in (7), the following equality needs to hold $\forall m$:

$$|h_D|^2\left(\sum_{i=1}^N P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2\right) > |h_{Em}|^2\left(\sum_{i=1}^N P_i|g_D^{(i)}|^2 + \sigma_D^2\right)$$

which can be expressed as

$$\mathbf{p}^T\left(|h_D|^2\mathbf{g}_{Em} - |h_{Em}|^2\mathbf{g}_D\right) > |h_{Em}|^2\sigma_D^2 - |h_D|^2\sigma_{Em}^2 \tag{8}$$

where

$$\begin{aligned} \mathbf{g}_{Em} &= \left[|g_{Em}^{(1)}|^2 \quad |g_{Em}^{(2)}|^2 \quad \cdots \quad |g_{Em}^{(N)}|^2\right]^T \\ \mathbf{g}_D &= \left[|g_D^{(1)}|^2 \quad |g_D^{(2)}|^2 \quad \cdots \quad |g_D^{(N)}|^2\right]^T. \end{aligned} \tag{9}$$

The feasibility conditions given by (8) can be formulated into the following linear programming problem [24]:

$$\begin{aligned} & \min_{\mathbf{p}\succeq 0} \ \mathbf{1}^T\mathbf{p} \\ & \text{s.t.}\ \mathbf{p}^T\left(|h_D|^2\mathbf{g}_{Em} - |h_{Em}|^2\mathbf{g}_D\right) > |h_{Em}|^2\sigma_D^2 - |h_D|^2\sigma_{Em}^2 \\ & \qquad \forall m. \end{aligned} \tag{10}$$

The above convex problem can be easily solved using existing convex optimization software [24], [25]. A positive secrecy rate can be only achieved at the destination node, if the problem in (10) is feasible. In the following section, we solve the secrecy rate maximization problem, with the assumption that a positive secrecy rate is achievable.

IV. Iterative Approach for the Solution of the Secrecy Rate Maximization Problem

The secrecy rate maximization problem P1 given by (6) is nonconvex due to the nonconvex secrecy rate function, and therefore, it is challenging to obtain the optimal solution. In this section, we develop an iterative algorithm for the power allocation $\mathbf{p}$ at the jammer nodes, which is based on an approximation to the original problem P1. By reformulating (6) and introducing a new slack variable τ, the original secrecy maximization problem P1 can be written as

$$\begin{aligned} \text{P2}: \quad & \min_{\mathbf{p}\succeq\mathbf{0},\tau\geq 0} \quad \tau \\ & \text{s.t.} \quad \Gamma_{Em}(\mathbf{p}) \triangleq \frac{\Phi_{Em}(\mathbf{p})}{\Psi_{Em}(\mathbf{p})} \leq \tau, \forall m \\ & \qquad P_i \leq \bar{P}_i, \forall i \end{aligned} \tag{11}$$

where

$$\begin{aligned} \Psi_{Em}(\mathbf{p}) \triangleq & \left(\sum_{i=1}^N P_i|g_D^{(i)}|^2 + P_s|h_D|^2 + \sigma_D^2\right) \\ & \times\left(\sum_{i=1}^N P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2\right) \triangleq \sum_k \psi_{Em}^{(k)} \end{aligned} \tag{12}$$

and

$$\begin{aligned} \Phi_{Em}(\mathbf{p}) \triangleq & \left(\sum_{i=1}^N P_i|g_{Em}^{(i)}|^2 + \sigma_{Em}^2 + P_s|h_{Em}|^2\right) \\ & \times\left(\sum_{i=1}^N P_i|g_D^{(i)}|^2 + \sigma_D^2\right). \end{aligned} \tag{13}$$

In (12), $\psi_{Em}^{(k)}$ represents the individual term in the summation, obtained by expanding function $\Psi_{Em}(\mathbf{p})$. The constraint in (11) is a quadratic fractional nonconvex function. However, the problem in (11) can be converted into a series of geometric programming problems by exploiting the single condensation method [26]. A fractional constraint with a posynomial numerator and a monomial denominator is convex. The idea of approximating the denominator posynomial with a monomial was presented in [24] in order to convert the aforementioned constraint to a convex one. We hereinafter adopt this idea, and we approximate $\Psi_{Em}(\mathbf{p})$ [i.e., denominator of the constraint in (11)] to the best monomial, for a given set of $\mathbf{p}$. The following lemma is required.

Lemma 1: For a posynomial $g(\mathbf{x})$, the following inequality holds:

$$g(\mathbf{x}) = \sum_{k=1}^K w_k(\mathbf{x}) \geq \hat{g}(\hat{\mathbf{x}}) = \prod_{k=1}^K \left[\frac{w_k(\mathbf{x})}{a_k}\right]^{a_k} \tag{14}$$

where $a_k > 0$ and $\sum_{k=1}^K a_k = 1$. Notation $\hat{g}(\hat{\mathbf{x}})$ represents the best approximation of $g(\hat{\mathbf{x}})$ at $\hat{\mathbf{x}}$ with $a_k = w_k(\hat{\mathbf{x}})/g(\hat{\mathbf{x}})$, and the inequality in (14) holds with an equality at this point.

Proof: The proof is provided in Appendix A. ■

Algorithm A: Secrecy Rate Maximization.

```
Step 1: Initialization of power allocation vector $\mathbf{p}$
Step 2: Repeat
  1) Calculate $\Psi_{Em}(\mathbf{p}), \forall m$ using (12).
  2) Calculate $\alpha_k^{(m)}, \forall k, m$ using (16).
  3) Determine $\hat{\Psi}_{Em}(\mathbf{p}), \forall m$ by using (15).
  4) Solve the standard geometric programming problem in (17).
Step 3: Until required accuracy is achieved or the maximum number of iterations is reached.
```

Based on Lemma 1, the denominator polynomial function $\Psi_{Em}(\mathbf{p})$ in (11) can be approximated as $\hat{\Psi}_{Em}(\mathbf{p})$

$$\Psi_{Em}(\mathbf{p}) \approx \hat{\Psi}_{Em}(\mathbf{p}) \triangleq \prod_{k=1}^{K} \left[\frac{\psi_{Em}^{(k)}}{\alpha_k^{(m)}}\right]^{\alpha_k^{(m)}} \tag{15}$$

where

$$\alpha_k^{(m)} \triangleq \frac{\psi_{Em}^{(k)}}{\hat{\Psi}_{Em}(\mathbf{p})} \ \forall k. \tag{16}$$

Using the approximation given by (15), problem P2 can be reformulated for a given set of power allocation $\mathbf{p}$ as

$$\begin{aligned} \text{P3}: \ & \min_{\mathbf{p}\succeq\mathbf{0},\tau\geq 0} \ \tau \\ & \text{s.t.} \ \hat{\Gamma}_{Em}(\mathbf{p}) \triangleq \frac{\Phi_{Em}(\mathbf{p})}{\hat{\Psi}_{Em}(\mathbf{p})} \leq \tau, \forall m \\ & P_i \leq \bar{P}_i, \forall i. \end{aligned} \tag{17}$$

The above optimization problem P3, which is an approximation of the original P1, can now be formulated into a standard geometric programming one. The iterative algorithm A is developed for P3, where the power allocation $\mathbf{p}$ is updated at each iteration.

The solution of the proposed Algorithm A satisfies the Karush–Kuhn–Tucker (KKT) conditions. This can be validated by proving the following three conditions [27].

1) $\Gamma_{Em}(\mathbf{p}) \leq \hat{\Gamma}_{Em}(\mathbf{p}), \forall m, \mathbf{p}$, where $\Gamma_{Em}(\mathbf{p}) = \frac{\Phi_{Em}(\mathbf{p})}{\Psi_{Em}(\mathbf{p})}$.
2) $\Gamma_{Em}(\tilde{\mathbf{p}}) = \hat{\Gamma}_{Em}(\tilde{\mathbf{p}}), \forall m$, where $\tilde{\mathbf{p}}$ denotes the power allocation obtained from the previous iteration of Algorithm A.
3) $\nabla\Gamma_{Em}(\tilde{\mathbf{p}}) = \nabla\hat{\Gamma}_{Em}(\tilde{\mathbf{p}}), \forall m$.

The first condition holds due to the fact that $\Psi_{Em}(\mathbf{p}) \leq \hat{\Psi}_{Em}(\mathbf{p})$, which is true from Lemma 1. In addition, the second condition is satisfied from the equality condition in Lemma 1. The third condition can be validated through proving $\nabla\hat{\Psi}_{Em}(\tilde{\mathbf{p}}) = \nabla\Psi_{Em}(\tilde{\mathbf{p}})$ for all m:

$$\nabla\hat{\Psi}_{Em}(\tilde{\mathbf{p}}) = \left[\frac{\partial\hat{\Psi}_{Em}(\tilde{\mathbf{p}})}{\partial P_1}\bigg|_{\tilde{P}_1} \frac{\partial\hat{\Psi}_{Em}(\tilde{\mathbf{p}})}{\partial P_2}\bigg|_{\tilde{P}_2} \cdots \frac{\partial\hat{\Psi}_{Em}(\tilde{\mathbf{p}})}{\partial P_N}\bigg|_{\tilde{P}_N}\right] \ \forall m \tag{18}$$

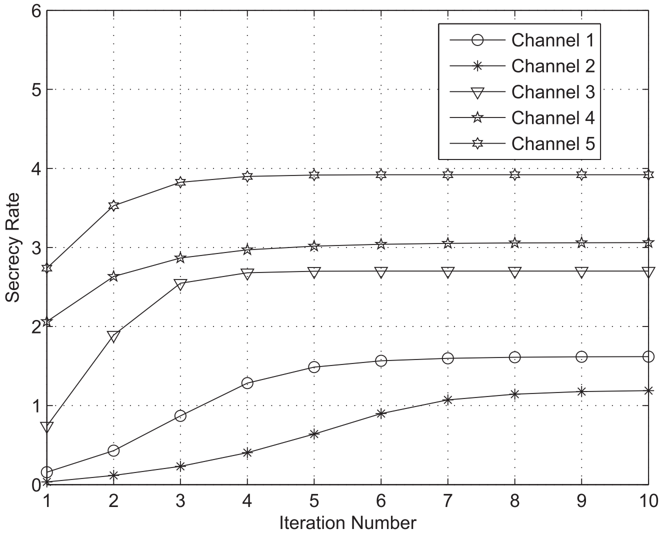


Fig. 2. Convergence of the proposed secrecy rate maximization Algorithm A for different sets of wireless channels.

$$\begin{aligned} \frac{\partial\hat{\Psi}_{Em}}{\partial P_1}\bigg|_{P_1=\tilde{P}_1} &= \prod_k \left[\frac{\psi_{Em}^{(k)}}{\alpha_k^{(m)}}\right]^{\alpha_k^{(m)}} \left[\frac{\sum_k \rho_{Em}^{(k)}}{P_1\hat{\Psi}_{Em}(\tilde{\mathbf{p}})}\right] \\ &= \left[\hat{\Psi}_{Em}(\tilde{\mathbf{p}})\right]^{\sum_k \alpha_k^{(m)}} \frac{\sum_k \rho_{Em}^{(k)}}{P_1\hat{\Psi}_{Em}(\tilde{\mathbf{p}})} \\ &= \frac{\sum_k \rho_{Em}^{(k)}}{P_1} = \frac{\partial\Psi_{Em}}{\partial P_1}\bigg|_{P_1=\tilde{P}_1} \end{aligned} \tag{19}$$

where $\rho_{Em}^{(k)}$ are the differentiated $\psi_{Em}^{(k)}$s with respect to P_1. Similarly, the rest of the partial derivatives in (18) can be derived, and it can be easily proved to be equal to the partial derivatives of $\Psi_{Em}(\tilde{\mathbf{p}})$, with respect to the corresponding power allocation. Hence, the power allocation obtained through Algorithm A satisfies the KKT conditions of the original optimization problem P1. However, it is difficult to analytically prove global optimality. In addition, the geometric programming in Algorithm A can be solved with polynomial time complexity. In order to validate the convergence of the proposed algorithm, simulation results will be provided in Section VII for different sets of wireless channels.

A. Convergence Analysis

The approximated secrecy rate maximization problem P3 given by (17) is convex, and the optimal power allocation $\mathbf{p}^*$ can be obtained by solving (17) for a given set of power allocation $\tilde{\mathbf{p}}$. At each iteration, the power allocation $\tilde{\mathbf{p}}$ is updated from the optimal solution $\mathbf{p}^*$ determined through the previous iteration. Hence, $\tilde{\mathbf{p}}$ is always a feasible solution of the next iteration, and the optimal power allocation $\mathbf{p}^*$ obtained for a given $\tilde{\mathbf{p}}$ will achieve a secrecy rate, which is greater than or equal to that of the previous iteration. This reveals that the achieved secrecy rate will monotonically increase at each iteration, which can be also observed from the simulation results, presented in Fig. 2. Since, the achievable secrecy rate is upper bounded for a given transmit power at the jammers, this algorithm will converge to a solution. Fortunately, the proposed Algorithm A converges to the optimal solution, which is validated through an one-dimensional search, based on bisection and provided in the following section.

V. Optimality Validation of the Secrecy Rate Maximization Algorithm

In this section, we present an 1-D search approach to validate the optimality of the proposed Algorithm A. The concept behind this approach is to fix the received total interference power at the destination node and find the optimal power allocation at the jammers[19], [28]. The secrecy rate maximization problem P1 can be formulated into the following max–min one:

$$\text{P4}: R^* = \max_{\mathbf{p}} \min_{t_i} \; (t_1, t_2, \ldots, t_M)$$
$$\text{s.t. } \log_2 \left(\frac{1 + \frac{P_s |h_D|^2}{\sum_{i=1}^{N} P_i |g_D^{(i)}|^2 + \sigma_D^2}}{1 + \frac{P_s |h_{Em}|^2}{\sum_{i=1}^{N} P_i |g_{Em}^{(1)}|^2 + \sigma_{Em}^2}} \right) \geq t_m, \forall m$$
$$P_i \leq \bar{P}i, \forall i \tag{20}$$

where R^* is the optimal achieved secrecy rate. By fixing the total received interference (i.e., $\sum_{i=1}^{N} P_i |g_D^{(i)}|^2$) at the destination to a particular value t_0, the following subproblem can be formulated:

$$\text{P5}: \; q^* = \max_{\mathbf{p},t} \; t$$
$$\text{s.t. } \sum_{i=1}^{N} P_i |g_D^{(i)}|^2 = t_0$$
$$R_{Em}(t_0) = \frac{1 + \frac{P_s |h_D|^2}{t_0 + \sigma_D^2}}{1 + \frac{P_s |h_{Em}|^2}{f_m(t_0) + \sigma_{Em}^2}} \geq t, \forall m$$
$$P_i \leq \bar{P}i, \forall i \tag{21}$$

where $f_m(t_0) = \sum_{i=1}^{N} P_i |g_{Em}^{(1)}|^2$. Next, we show that the problem in (21) is quasi-convex in terms of t_0, and therefore, the optimal t_0 can be obtained through 1-D search.

Lemma 2: $R_{Em}(t_0)$ is a quasi-concave function in terms of t_0.

Proof: This can be proved by finding the second derivative of $R_{Em}(t_0)$ with respect to t_0 and easily provided that it is negative for any $t_0 > 0$ [28]. ■

In addition, the pointwise infimum of a set of quasi-concave functions is quasi-concave [24]. Therefore, problem P5 given by (21) is quasi-convex and the optimal power allocation at the jammers can be obtained through Algorithm B.

VI. SOP Analysis Over Rayleigh Fading Channels

In this section, we analyze the SOP performance of the proposed cooperative jamming scheme over Rayleigh fading channels. In particular, for the system model presented in Section II, we assume that h_D as well as $g_D^{(n)}$ $\forall\, n = 1, 2, \ldots, N$ and γ_{E_i} $\forall\, i = 1, 2, \ldots, M$ are standard circularly symmetric complex Gaussian RVs.

Algorithm B: One-Dimensional Search Based on Bisection.

```
Step 1: Initialize $t_0^{(\min)}, t_0^{(\max)}$, and $\epsilon$
Step 2: Solve the problem in P5 given by (21) with
    $t_0 = \frac{t_0^{(\min)} + 3t_0^{(\max)}}{4}$.
Step 3: Set $t^* = t$.
Step 4: Repeat
  1) $t_0 = \frac{t_0^{(\min)} + t_0^{(\max)}}{2}$.
  2) Solve the problem P5 given by (21) and obtain the value of $t$
  3) If $t^* > t$
  4)     $t_0^{(\min)} = \frac{t_0^{(\min)} + t_0^{(\max)}}{2}$
  5) else
  6)     $t_0^{(\max)} = \frac{t_0^{(\min)} + t_0^{(\max)}}{2}$
  7) end
Step 5: Repeat until $t_0^{(\max)} - t_0^{(\min)} \geq \epsilon$.
```

By using the SOP definition of [29], the SOP of the proposed cooperative jamming scheme can be obtained as

$$P_{\text{out}} = \Pr\left[\log_2 \frac{\gamma_D + 1}{\gamma_{E_{\max}} + 1} < \mathcal{R} \Big| \gamma_D > \gamma_{E_{\max}}\right]$$
$$\times \Pr\left[\gamma_D > \gamma_{E_{\max}}\right] + \Pr\left[\gamma_D \leq \gamma_{E_{\max}}\right] \tag{22}$$

where $\mathcal{R}$ denotes the rate in bits per second (bps) per Hertz. With the utilization of the auxiliary positive real parameter $\mu \triangleq 2^{\mathcal{R}}$ and the negative real parameter $\nu \triangleq 2^{-\mathcal{R}} - 1$, (22) can be rewritten, as shown in Appendix B, as

$$P_{\text{out}} = 1 - \Pr\left[\gamma_{E_{\max}} < \frac{\gamma_D}{\mu} + \nu\right]$$
$$= 1 - \mu \int_0^{\infty} F_{\gamma_{E\max}}(x) f_{\gamma_D}(\mu x - \mu\nu) dx. \tag{23}$$

In order to solve the integral in (23), we first derive a closed-form expression for the PDF of γ_D as follows. Since $z \triangleq P_s |h_D|^2$ is an exponentially distributed RV and $y \triangleq \sum_{n=1}^{N} P_n |g_{E_i}^{(n)}|^2$ is a generalized chi-squared one, by obtaining the CDF of z and the PDF of y by easily integrating [30, eq. (2.7)] and from [31, eq. (19)] for distinct P_n's, it can be shown that the CDF of γ_D is given by

$$F_{\gamma_D}(x) = \int_{\sigma_D^2}^{\infty} F_z(xw) f_y\left(w - \sigma_D^2\right) dw$$
$$= 1 - \sum_{n=1}^{N} \mathcal{A}_n \exp\left(\frac{\sigma_D^2}{P_n}\right) \int_{\sigma_D^2}^{\infty} \exp\left[-\left(\frac{x}{P_s} + \frac{1}{P_n}\right) w\right] dw$$
$$\overset{(a)}{=} 1 - P_s \exp\left(-\frac{\sigma_D^2 x}{P_s}\right) \sum_{n=1}^{N} \frac{\mathcal{A}_n P_n}{P_n x + P_s} \tag{24}$$

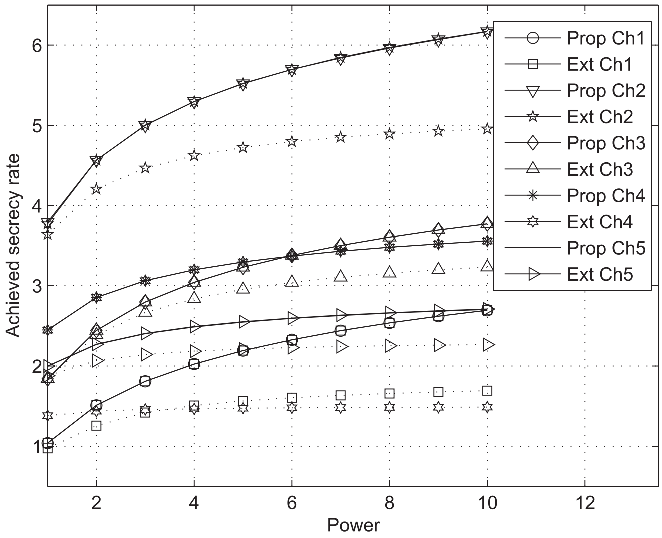


Fig. 3. Achieved secrecy rates of Algorithm A, the scheme in [19], and the best jammer selection scheme for five sets of different wireless channels with different maximum available transmit power. The dotted lines denote the best jammer selection scheme.

where (a) follows after using [23, eq. (3.381/3)] and the definition

$$A_n \triangleq \left[P_n \prod_{j=1, j\neq n}^{N} \left(1 - \frac{P_j}{P_n} \right) \right]^{-1}. \tag{25}$$

By differentiating (24), the PDF of γ_D is easily derived as

$$f_{\gamma_D}(x) = \exp\left(-\frac{\sigma_D^2 x}{P_s} \right) \times \sum_{n=1}^{N} \mathcal{A}_n P_n \left[\frac{\sigma_D^2}{P_n x + P_s} + \frac{P_s P_n}{(P_n x + P_s)^2} \right]. \tag{26}$$

A closed-form expression for the CDF of $\gamma_{E_{\max}}$ can be easily obtained using the marginal CDFs of γ_{E_i} ∀ i and the fact that these RVs are independent. In particular, the latter CDFs are derived in closed form similar to the CDF of γ_D, and each is given by (24) after substituting σ_D^2 with $\sigma_{E_i}^2$. Hence, the CDF of $\gamma_{E_{\max}}$ can be expressed as

$$F_{\gamma_{E\max}}(x) = \prod_{i=1}^{M} \left[1 - P_s \exp\left(-\frac{\sigma_{E_i}^2 x}{P_s} \right) \sum_{n=1}^{N} \frac{\mathcal{A}_n P_n}{P_n x + P_s} \right]. \tag{27}$$

By substituting (26) and (27) into (23), an analytical expression in the form of a single integral for the SOP of the proposed PHY layer security scheme can be obtained as

$$P_{\text{out}} = 1 - \mu \exp\left(\frac{\sigma_D^2 \mu \nu}{P_s} \right) Y \tag{28}$$

where integral Y is given by

$$Y = \int_0^\infty \left\{ \prod_{i=1}^{M} \left[1 - P_s \exp\left(-\frac{\sigma_{E_i}^2 x}{P_s} \right) \sum_{n=1}^{N} \frac{\mathcal{A}_n}{x + \lambda_n} \right] \right\} \times \exp(-\xi x) \sum_{n=1}^{N} \frac{\mathcal{A}_n}{\mu} \left[\frac{\sigma_D^2}{x - \kappa_n} + \frac{P_s}{\mu (x - \kappa_n)^2} \right] dx \tag{29}$$

with $\xi \triangleq P_s^{-1} \sigma_D^2 \mu$, as well as, for $n = 1, 2, \ldots, N$, $\kappa_n \triangleq P_s / (\mu P_n) - \nu$ and $\lambda_n \triangleq P_s / P_n$. By using the closed-form solution for Y included in Appendix C, a closed-form expression for the SOP of the proposed scheme for arbitrary positive integer values of N and M is given by

$$\begin{aligned} P_{\text{out}} = 1 - \mu \exp(\xi \nu) \Bigg\{ & \sum_{n=1}^{N} \frac{\mathcal{A}_n}{\mu} \Bigg[\sigma_D^2 I_{1,0}(\xi, \kappa_n, 0) \\ & + \frac{P_s}{\mu} I_{2,0}(\xi, \kappa_n, 0) \Bigg] + \sum_{\{\alpha_i\}_{i=1}^{M}} P_s^i \sum_{k_1 + k_2 + \cdots + k_N = i} \frac{i!}{\prod_{n=1}^{N} k_n!} \\ & \times \left(\prod_{t=1}^{N} \mathcal{A}_t^{k_t} \right) \sum_{n=1}^{N} \frac{\mathcal{A}_n}{\mu} \Bigg[\sigma_D^2 I_{1,\{k_n\}_{n=1}^{N}} \left(\psi_i, \kappa_n, \{\lambda_n\}_{n=1}^{N} \right) \\ & + \frac{P_s}{\mu} I_{2,\{k_n\}_{n=1}^{N}} \left(\psi_i, \kappa_n, \{\lambda_n\}_{n=1}^{N} \right) \Bigg] \Bigg\} \end{aligned} \tag{30}$$

where symbol $\sum_{\{\alpha_i\}_{i=1}^{M}}$ is used for short-hand representation of the multiple summation $\sum_{i=1}^{M} \sum_{\alpha_1=1}^{M-i+1} \sum_{\alpha_2=\alpha_1+1}^{M-i+2} \cdots \sum_{\alpha_i=\alpha_{i-1}+1}^{M}$, and the sum $\sum_{k_1+k_2+\cdots+k_N=i}$ is taken over all combinations of nonnegative integer indices k_1 through k_N such that the sum of all k_n is i. Moreover, $I_{\ell,\{k_n\}_{n=1}^{N}}(\alpha_1, \alpha_2, \{\alpha_{3,n}\}_{n=1}^{N})$ is given by (C8) for $\ell = 1, 2$ as well as for k_n being positive integer and α_1, α_2, $\alpha_{3,n} \in \mathbb{R}_+^*$ ∀ $n = 1, 2, \ldots, N$. As an example, for the special case of $N = 2$ and $M = 1$, the latter SOP expression simplifies to

$$\begin{aligned} P_{\text{out}} = & 1 - \mu \exp(\xi \nu) \\ & \times \Bigg\{ \sum_{n=1}^{2} \frac{\mathcal{A}_n}{\mu} \left[\sigma_D^2 I_{1,0}(\xi, \kappa_n, 0) + \frac{P_s}{\mu} I_{2,0}(\xi, \kappa_n, 0) \right] \\ & - \sum_{n=1}^{2} \frac{P_s \mathcal{A}_n^2}{\mu} \left[\sigma_D^2 I_{1,1}(\psi, \kappa_n, \lambda_n) + \frac{P_s}{\mu} I_{2,1}(\psi, \kappa_n, \lambda_n) \right] \\ & - \frac{P_s \mathcal{A}_1 \mathcal{A}_2 \sigma_D^2}{\mu} \left[I_{1,1}(\psi, \kappa_1, \lambda_2) + I_{1,1}(\psi, \kappa_2, \lambda_1) \right] \\ & - \frac{P_s^2 \mathcal{A}_1 \mathcal{A}_2}{\mu^2} \left[I_{2,1}(\psi, \kappa_1, \lambda_2) + I_{2,1}(\psi, \kappa_2, \lambda_1) \right] \Bigg\} \end{aligned} \tag{31}$$

where $\psi \triangleq \xi + P_s^{-1} \sigma_{E_1}^2$,

$$I_{1,0}(\xi, \kappa_n, 0) = -\exp(\xi \kappa_n) \operatorname{Ei}(-\xi \kappa_n) \tag{32a}$$

$$I_{2,0}(\xi, \kappa_n, 0) = \kappa_n^{-1} + \xi \exp(\xi \kappa_n) \operatorname{Ei}(-\xi \kappa_n) \tag{32b}$$

TABLE I
OPTIMAL POWER ALLOCATION AT THE JAMMERS BASED ON ALGORITHMS A AND B FOR DIFFERENT SETS OF WIRELESS CHANNELS

	Algorithm B				Algorithm A			
Channels	P_1	P_2	P_3	Achieved Secrecy Rate	P_1	P_2	P_3	Achieved Secrecy Rate
1	1.00	0	0.50	1.62	1.00	0	0.50	1.62
2	1.00	0	0.17	2.98	1.00	0	0.16	2.98
3	0.47	0	0.35	1.68	0.46	0	0.34	1.68
4	1.00	0.43	0	2.72	1.00	0.42	0	2.73
5	0	0.28	0.31	1.09	0	0.28	0.31	1.09

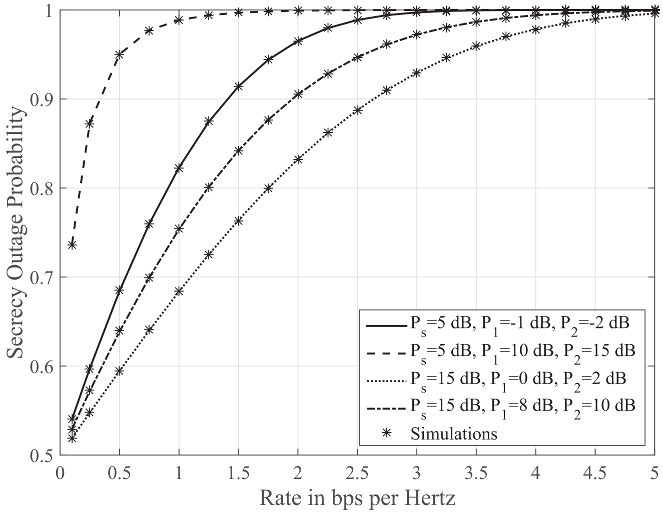


Fig. 4. P_{out}, as a function of the rate $\mathcal{R}$, in bps per Hz, for $N = 2$ cooperative jammers, $M = 1$ eavesdroppers, and various power levels.

and

$$I_{1,1}\left(\psi, \kappa_n, \lambda_n\right) = \frac{I_{1,0}\left(\psi, \kappa_n\right) - I_{1,0}\left(\psi, \lambda_n\right)}{\lambda_n - \kappa_n} \tag{32c}$$

$$I_{2,1}\left(\psi, \kappa_n, \lambda_n\right) = \frac{I_{1,0}\left(\psi, \lambda_n\right) - I_{1,0}\left(\psi, \kappa_n\right)}{\left(\kappa_n - \lambda_n\right)^2} - \frac{I_{2,0}\left(\psi, \kappa_n\right)}{\kappa_n - \lambda_n}. \tag{32d}$$

VII. NUMERICAL RESULTS AND DISCUSSIONS

In order to validate the performance of the proposed algorithms, we consider the secrecy network shown in Fig. 1, with a source–destination pair, three ($N = 3$) cooperative jammers and two ($M = 2$) eavesdroppers. In the following simulations, all the channel coefficients involved are generated using zero-mean circularly symmetric independent and identically distributed complex Gaussian RVs. In addition, the noise variances at the destination and the eavesdroppers are assumed to be 0.1.

To assess the convergence of the proposed secrecy rate maximization algorithm, the available maximum transmit powers at the source and relays have been set to, $P_s = 2$, $P_1 = 1$, $P_2 = 1$, and $P_3 = 3$. Fig. 2 depicts the convergence of the achievable secrecy rates for a set of different feasible channels. As evident from this figure, the proposed algorithm converges, while the achievable secrecy rates increase with the iteration number. In addition, it has been observed that the proposed Algorithm A converges to the same secrecy rate with different initialization of transmit powers at the jammers. However, we could not provide analytical results to prove this convergence. As we discussed in the convergence analysis of the algorithm, it can be observed that the achievable secrecy rate monotonically increases with the iteration number.

Next, we compare the performance of the proposed algorithm with the existing scheme in [19] and the best jammer selection scheme. The cooperative jamming scheme in [19] has been developed using both the convex optimization approach and the 1-D search scheme in the presence of a single eavesdropper, whereas the best jammer is selected from available cooperative jammers in the best jammer selection scheme. In order to evaluate this comparison, the same secrecy network in the previous simulation is considered with a single eavesdropper and with the same noise variance 0.1 at all the nodes. Fig. 3 depicts the achieved secrecy rates for different available transmit power at the source and the cooperative jammers for different sets of channels, where it is assumed that the maximum available transmit power at the source and the cooperative jammers is the same. As seen in Fig. 3, both the proposed algorithm and the scheme in [19] achieve the same secrecy rates for different sets of channels with the same transmit power constraints and better secrecy rates than the best jammer selection scheme. This confirms that the proposed algorithm shows the same performance as the optimal scheme in [19] and outperforms the best jammer selection scheme.

Next, we evaluate the optimality of the power allocation obtained through the proposed Algorithm A. In order to do this, we simulate Algorithm B for the same set of channels considered for Algorithm A. Table I presents the power allocation and the secrecy rates obtained through Algorithm B that is based on 1-D search and on Algorithm A. As we can conclude from this table, the power allocation and achieved secrecy rates are identical for different sets of channels in both algorithms. Note that there are small differences in the power allocation and achieved secrecy rates, due to the accuracy or precision of software used. However, these results provided in Table I confirm the optimality of the proposed secrecy rate maximization Algorithm A.

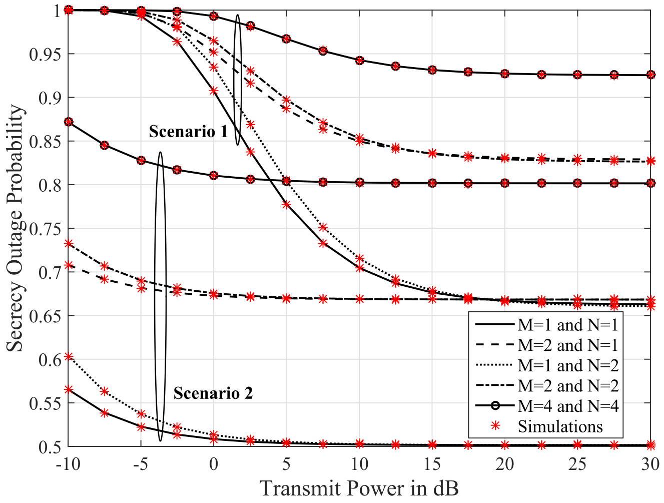


Fig. 5. SOP performance P_{out} as a function of source's transmit power P_s in decibels for both Scenarios 1 and 2, as well as various numbers of cooperative jammers and eavesdroppers.

By numerically evaluating (31), Fig. 4 depicts the SOP performance as a function of rate $\mathcal{R}$ in bps per Hertz for $N = 2$ cooperative jammers, $M = 1$ eavesdropper, and various power levels. It is shown in this figure that computer simulation results for SOP match perfectly with the equivalent numerical ones for all considered parameters. As expected, SOP degrades with increasing values for $\mathcal{R}$. In addition, as the transmit power of the source S increases and the transmit powers at the two cooperative jammers J_1 and J_2 decrease, SOP improves. The best SOP performance in this figure for all considered $\mathcal{R}$ values is achieved with $P_s = 15$ dB, $P_1 = 0$ dB, and $P_2 = 2$ dB, and the lower value for the SOP is 0.5.

The SOP performance as a function of source S's transmit power P_s is illustrated in Fig. 5. The following transmission scenarios have been considered: 1) Scenario 1: $\mathcal{R} = 1$, $P_1 = -4$ dB, and $P_i = P_1 + (i-1)$ dB with $i = 2, 3,$ and 4; and 2) Scenario 2: $\mathcal{R} = 0.01$, $P_1 = 1$ dB, and $P_i = P_1 + (i-1)$ dB with $i = 2, 3,$ and 4. For the SOP results, the single-integral expression given by (28) after substituting (29) and the closed-form expression given by (30) for arbitrary values of N and M as well as the closed-form expression given by (31) for $M = 2$ and $N = 1$ have been numerically evaluated. As clearly shown, computer simulation results for the SOP coincide with the numerical ones for all considered parameters. Furthermore, it is evident that, for the same values of N and M, the SOP performance of Scenario 2 is always better than that of Scenario 1. In both scenarios, the minimum SOP is accomplished with $N = M = 1$ and the maximum with $N = M = 4$. Also, as expected, the SOP improves with increasing values of P_s for all considered cases. In addition, it is shown in this figure that, as M increases while N is kept constant, the SOP degrades significantly. This performance degradation can be confronted for some range of P_s values by increasing N. However, increasing N introduces an SOP performance penalty, which needs to be taken under consideration when designing a cooperating jamming scheme.

VIII. Conclusion

In this paper, we studied the power allocation problem of secrecy rate maximization with cooperative jammers in the presence of multiple eavesdroppers. For this problem, a feasibility condition was first derived for power allocation in order to achieve the positive secrecy rate. Then, the original nonconvex secrecy rate maximization problem was solved to obtain the optimal power allocation at the jammers. The proposed optimal iterative approach was developed by approximating the secrecy rate function and formulating the corresponding problem into a geometric programming problem for a given set of power allocation at the jammers. In order to validate the optimality of the developed algorithm, we also developed a 1-D search algorithm based on bisection. In addition, the SOP analysis of the proposed cooperative jamming approach was derived for Rayleigh fading channels. Simulation results were provided to validate the optimality and convergence of the proposed algorithm as well as the theoretical derivation of SOP analysis. These results confirm that the proposed algorithm yields the optimal power allocation at the jammers, whereas the numerical simulation results demonstrate the correctness of theoretical derivations of the SOP analysis.

Appendix A
Proof of Lemma 1

Function $g(\mathbf{x})$ can be written as

$$g(\mathbf{x}) = \sum_{k=1}^{K} a_k \left[\frac{w_k(\mathbf{x})}{a_k}\right] \geq \prod_{k=1}^{K} \left[\frac{w_k(\mathbf{x})}{a_k}\right]^{a_k} = \hat{g}(\hat{\mathbf{x}}) \quad \text{(A.1)}$$

where the inequality in (A1) is obtained from the arithmetic–geometric mean inequality. This inequality holds with equality when $a_k = \frac{w_k(\hat{\mathbf{x}})}{g(\hat{\mathbf{x}})}$ as follows:

$$\begin{aligned}\hat{g}(\hat{\mathbf{x}}) &= \prod_{k=1}^{K} \left[\frac{w_k(\hat{\mathbf{x}})}{\bar{a}_k}\right]^{\bar{a}_k} \\ &= \prod_{k=1}^{K} g(\hat{\mathbf{x}})^{\sum_{k=1}^{K} \frac{w_k(\hat{\mathbf{x}})}{g(\hat{\mathbf{x}})}} = g(\hat{\mathbf{x}})\end{aligned}$$

where

$$\bar{a}_k = \frac{w_k(\hat{\mathbf{x}})}{g(\hat{\mathbf{x}})} \text{ and } \sum_{k=1}^{K} \frac{w_k(\hat{\mathbf{x}})}{g(\hat{\mathbf{x}})} = 1. \quad \text{(A.2)}$$

This completes the proof of Lemma 1.

Appendix B
Derivation of (23)

Starting from (22) and using the definition of conditional probability results in

$$\begin{aligned}P_{\mathrm{out}} &= 1 + \Pr\left[\frac{\gamma_D}{\mu} + \nu < \gamma_{E_{\max}} < \gamma_D\right] - \Pr\left[\gamma_{E_{\max}} < \gamma_D\right] \\ &= 1 - \int_0^{\infty} F_{\gamma_{E_{\max}}}\left(\frac{y}{\mu} + \nu\right) f_{\gamma_D}(y) dy. \quad \text{(B.1)}\end{aligned}$$

Using the change of variables $x \to y/\mu + \nu$ and the fact that $\nu < 0$ yields (23).

Appendix C
Closed-Form Solution for (29)

To solve integral Y given by (29) that appears in the SOP expression given by (28), we first make use of the multinomial expansion [32, eq. (23)] for the M-factor product, yielding

$$\begin{aligned}&\prod_{i=1}^{M}\left[1 - P_s \exp\left(-\frac{\sigma_{E_i}^2 x}{P_s}\right)\sum_{n=1}^{N}\frac{\mathcal{A}_n}{x+\lambda_n}\right]\\ &= 1 + \sum_{\{\alpha_i\}_{i=1}^{M}} P_s^i \exp\left(-\frac{x}{P_s}\sum_{j=1}^{i}\sigma_{E_{\alpha_j}}^2\right)\left(\sum_{n=1}^{N}\frac{\mathcal{A}_n}{x+\lambda_n}\right)^i.\end{aligned} \tag{C.1}$$

Then, in the latter expression, we utilize the multinomial theorem to expand the ith power of the N-term sum as follows:

$$\begin{aligned}\left(\sum_{n=1}^{N}\frac{\mathcal{A}_n}{x+\lambda_n}\right)^i &= \sum_{k_1+k_2+\cdots+k_N=i}\frac{i!}{\prod_{n=1}^{N}k_n!}\\ &\quad\times\prod_{t=1}^{N}\frac{\mathcal{A}_t^{k_t}}{(x+\lambda_t)^{k_t}}.\end{aligned} \tag{C.2}$$

Substituting (C2) into (C1) and then into (29), integral Y can be rewritten as

$$\begin{aligned}Y &= \sum_{n=1}^{N}\frac{\mathcal{A}_n}{\mu}\left[\sigma_D^2 I_{1,0}\left(\xi,\kappa_n,0\right)\frac{P_s}{\mu} + I_{2,0}\left(\xi,\kappa_n,0\right)\right]\\ &\quad + \sum_{\{\alpha_i\}_{i=1}^{M}} P_s^i \sum_{k_1+k_2+\cdots+k_N=i}\frac{i!\prod_{t=1}^{N}\mathcal{A}_t^{k_t}}{\prod_{n=1}^{N}k_n!}\\ &\quad\times\sum_{n=1}^{N}\frac{\mathcal{A}_n}{\mu}\left[\sigma_D^2 I_{1,\{k_n\}_{n=1}^{N}}\left(\psi_i,\kappa_n,\{\lambda_n\}_{n=1}^{N}\right)\right.\\ &\quad\left.+\frac{P_s}{\mu}I_{2,\{k_n\}_{n=1}^{N}}\left(\psi_i,\kappa_n,\{\lambda_n\}_{n=1}^{N}\right)\right]\end{aligned} \tag{C.3}$$

where $\psi_i \triangleq \xi + P_s^{-1}\sum_{j=1}^{i}\sigma_{E_{\alpha_j}}^2$. In addition, $I_{\ell,\{k_n\}_{n=1}^{N}}(\alpha_1, \alpha_2, \{\alpha_{3,n}\}_{n=1}^{N})$ for $\ell = 1, 2$, as well as for k_n being positive integer and α_1, α_2, and $\alpha_{3,n} \in \mathbb{R}_+^* \ \forall\, n = 1, 2, \ldots, N$, is defined as

$$\begin{aligned}&I_{\ell,\{k_n\}_{n=1}^{N}}\left(\alpha_1,\alpha_2,\{\alpha_{3,n}\}_{n=1}^{N}\right)\\ &= \int_0^\infty \frac{\exp\left(-\alpha_1 x\right)}{\left(x+\alpha_2\right)^{\ell}\prod_{n=1}^{N}\left(x+\alpha_{3,n}\right)^{k_n}}dx.\end{aligned} \tag{C.4}$$

By using [23, Sec. 2.1] for the rational function integrand in (C5) in order to rewrite the integral as summations of integrals, it can be shown that

$$\begin{aligned}&I_{\ell,\{k_n\}_{n=1}^{N}}\left(\alpha_1,\alpha_2,\{\alpha_{3,n}\}_{n=1}^{N}\right) = \sum_{i=1}^{\ell} Z_i \int_0^\infty \frac{\exp\left(-\alpha_1 x\right)}{\left(x+\alpha_2\right)^i}dx\\ &+\sum_{j=1}^{N}\sum_{i=1}^{k_j}\Theta_i^{(k_j)}\int_0^\infty\frac{\exp\left(-\alpha_1 x\right)}{\left(x+\alpha_{3,j}\right)^i}dx\end{aligned} \tag{C.5}$$

where the real-valued parameter Z_i is given by

$$Z_{\ell-k+1} = \frac{1}{(k-1)!}\frac{d^{k-1}}{dx^{k-1}}\zeta(x)\Big|_{x=-\alpha_2} \tag{C.6}$$

for $k \le \ell$ with $\zeta(x) = \prod_{n=1}^{N}\left(x+\lambda_n\right)^{-k_n}$, and the real-valued parameter $\Theta_i^{(k_j)}$ by

$$\Theta_{k_j-k+1}^{(k_j)} = \frac{1}{(k-1)!}\frac{d^{k-1}}{dx^{k-1}}\theta_j(x)\Big|_{x=-\lambda_j} \tag{C.7}$$

for $k \le k_j$ with $\theta_j(x) = \left(x+\alpha_2\right)^{-1}\prod_{n\neq j}^{N}\left(x+\lambda_n\right)^{-k_n}$. Using [23, eq. (3.353/2)] for the integrals appearing in (C5) yields

$$\begin{aligned}&I_{\ell,\{k_n\}_{n=1}^{N}}\left(\alpha_1,\alpha_2,\{\alpha_{3,n}\}_{n=1}^{N}\right) = \sum_{i=1}^{\ell}\frac{Z_i}{(i-1)!}\sum_{r=1}^{i-1}(r-1)!\\ &\times\left(-\alpha_1\right)^{i-r-1}\alpha_2^{-r} - \frac{\left(-\alpha_1\right)^{i-1}}{(i-1)!}\exp\left(\alpha_1\alpha_2\right)\mathrm{Ei}\left(-\alpha_1\alpha_2\right)\\ &+\sum_{j=1}^{N}\sum_{i=1}^{k_j}\frac{\Theta_i^{(k_j)}}{(i-1)!}\sum_{r=1}^{i-1}(r-1)!\left(-\alpha_1\right)^{i-r-1}\alpha_{3,j}^{-r} - \frac{\left(-\alpha_1\right)^{i-1}}{(i-1)!}\\ &\times\exp\left(\alpha_1\alpha_{3,j}\right)\mathrm{Ei}\left(-\alpha_1\alpha_{3,j}\right).\end{aligned} \tag{C.8}$$

Finally, substituting (C8) into (C3) yields a closed-form expression for integral Y.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

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

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

[5] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[6] L. Wang, M. Elkashlan, J. Huang, N. Tran, and T. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.

[7] F. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[8] J. Zhu, Y. Zou, G. Wang, Y. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna selection aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.

[9] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Jun. 2015.

[10] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[11] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and Y. S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[12] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimizations for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.

[13] W. Xiang, S. L. Goff, M. Johnston, and K. Cumanan, "Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications," *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 249–252, Jun. 2015.

[14] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[15] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

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

[17] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 29, no. 10, pp. 2067–2076, Jun. 2011.

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

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

[20] Y. Zou, J. Zhu, G. Wang, and H. Shao, "Secrecy outage probability analysis of multi-user multi-eavesdropper wireless systems," in *Proc. IEEE Int. Conf. Commun. China*, Shanghai, China, Oct. 2014, pp. 309–313.

[21] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *Proc. IEEE Statist. Signal Process. Workshop*, Ann Arbor, MI, USA, Aug. 2012, pp. 389–392.

[22] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[23] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.

[24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[25] Y. Ye, *Interior Point Algorithms. Theory and Analysis.* New York, NY, USA: Wiley, 1997.

[26] M. Chiang, C. W. Tan, D. P. Palomar, D. O'Neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.

[27] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, 1978.

[28] A. Wiesel, C. Y. Eldar, and A. Beck, "Maximum likelihood estimation in linear models with a Gaussian model matrix," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 292–295, May 2006.

[29] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 14–18, 2006, pp. 356–360.

[30] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. New York, NY, USA: Wiley, 2005.

[31] D. Hammarwall, M. Bengtsson, and B. Ottersten, "Acquiring partial CSI for spatially selective transmission by instantaneous channel norm feedback," *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1188–1204, Mar. 2008.

[32] G. C. Alexandropoulos, A. Papadogiannis, and P. C. Sofotasios, "A comparative study of relaying schemes with decode and forward over Nakagami-m fading channels," *J. Comput. Netw. Commun.*, vol. 2011, 2011, Art. no. 560528.

Kanapathippillai Cumanan (M'10) received the B.Sc. (Hons.) degree in electrical and electronic engineering from the University of Peradeniya, Peradeniya, Sri Lanka, in 2006 and the Ph.D. degree in signal processing for wireless communications from Loughborough University, Loughborough, U.K., in 2009.

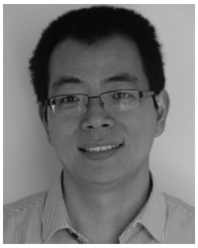
He is currently a Lecturer with the Department of Electronics, University of York, York, U.K. He was with the School of Electronic, Electrical and System Engineering, Loughborough University. He was a Teaching Assistant with the Department of Electrical and Electronic Engineering, University of Peradeniya, in 2006. In 2011, he was an Academic Visitor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. He was a Research Associate with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon Tyne, U.K., from 2012 to 2014. His research interests include physical layer security, cognitive radio networks, relay networks, convex optimization techniques, and resource allocation techniques.

Dr. Cumanan received an Overseas Research Student Award Scheme from Cardiff University, Cardiff, U.K., where he was a Research Student from 2006 to 2007.

George C. Alexandropoulos (S'07–M'10–SM'15) was born in Athens, Greece, in 1980. He received the Diploma degree in computer engineering and informatics, the M.A.Sc. degree (with distinction) in signal processing and communications, and the Ph.D. degree in wireless communications from the University of Patras (UoP), Patras, Greece, in 2003, 2005, and 2010, respectively.

From 2001 to 2010, he was a Research Fellow with the Signal Processing and Communications Laboratory, Department of Computer Engineering and Informatics, School of Engineering, UoP. From 2006 to 2010, he was with the Wireless Communications Laboratory, Institute of Informatics and Telecommunications, National Center for Scientific Research "Demokritos," Athens, Greece, as a Ph.D. Scholar. From 2007 to 2011, he collaborated with the Institute for Astronomy, Astrophysics, Space Applications, and Remote Sensing, National Observatory of Athens, where he participated in one national and two European projects. In 2011, he also worked with the Telecommunication Systems Research Institute, Technical University of Crete, Chania, Greece, in the framework of one European project. In the summer semester of 2011, he was an Adjunct Lecturer with the Department of Telecommunications Science and Technology, University of Peloponnese, Tripoli, Greece. From 2011 to 2014, he was a Senior Researcher with the Athens Information Technology Center for Research and Education, where he has been involved with the technical management of four European projects and lectured several mathematics courses. Since 2014, he has been a Senior Researcher with the Mathematical and Algorithmic Sciences Laboratory, France Research Center, Huawei Technologies France, Boulogne-Billancourt, France. His research interests include the general areas of performance analysis and signal processing for wireless networks, with an emphasis on multiantenna systems, interference management, high-frequency communication, cooperative networking, and cognitive radios.

Dr. Alexandropoulos is a Senior Member of the IEEE Communications Society and the IEEE Signal Processing Society and a Professional Engineer of the Technical Chamber of Greece. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS and as an Associate Editor for *IET Electronics Letters*. He received a Postgraduate Scholarship from the Operational Program for Education and Initial Vocational Training II, Ministry of Education, Lifelong Learning, and Religious Affairs, Republic of Greece; a student travel grant for the 2010 IEEE Global Telecommunications Conference in Miami, FL, USA; and the Best Ph.D. Thesis Award by a Greek University in the field of informatics and telecommunications from the Informatics and Telematics Institute, Thessaloniki, Greece, in 2010.



Zhiguo Ding (S'03–M'05–SM'15) received the B.Eng. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2000 and the Ph.D. degree from Imperial College London, London, U.K., in 2005, both in electrical engineering.

From July 2005 to August 2014, he was with Queen's University Belfast, Imperial College London, and Newcastle University. Since September 2014, he has been a Chair Professor with Lancaster University, Lancashire, U.K. From October 2012 to September 2016, he was an academic visitor with Princeton University, Princeton, NJ, USA. His research interests include 5G networks, game theory, cooperative and energy-harvesting networks, and statistical signal processing.

Dr. Ding is an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE WIRELESS COMMUNICATION LETTERS, IEEE COMMUNICATION LETTERS, and the *Journal of Wireless Communications and Mobile Computing*. He received the Best Paper Award at the 2009 IET Communication Conference on Wireless, Mobile, and Computing; IEEE COMMUNICATIONS LETTER Exemplary Reviewer in 2012; and the EU Marie Curie Fellowship during 2012–2014.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (five years) and Ph.D. degrees in electrical and computer engineering from the University of Patras, Patras, Greece, in 1987 and 1999, respectively.

From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Thessaloniki, Greece, where he is currently a Professor with the Department of Electrical and Computer Engineering and the Director of Digital Telecommunications Systems and Networks Laboratory. He is also an Honorary Professor at South West Jiaotong University, Chengdu, China. He has authored or coauthored more than 400 technical papers published in scientific journals and presented at international conferences. He is also the author of the Greek edition of a book on telecommunications systems and the coauthor of the book entitled *Advanced Optical Wireless Communications Systems* (Cambridge, U.K.: Cambridge Univ. Press, 2012). His research interests include the broad area of digital communications systems and signal processing, with an emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, molecular communications, communications and robotics, and wireless security.

Dr. Karagiannidis is involved as a General Chair, Technical Program Chair, and member of Technical Program Committees in several IEEE and non-IEEE conferences. He was an Editor in the IEEE TRANSACTIONS ON COMMUNICATIONS, a Senior Editor of IEEE COMMUNICATIONS LETTERS, an Editor of the *EURASIP Journal of Wireless Communications and Networks*, and a several-times Guest Editor of the IEEE SELECTED AREAS IN COMMUNICATIONS. From 2012 to 2015, he was the Editor-in Chief of IEEE COMMUNICATIONS LETTERS. He is one of the highly cited authors across all areas of electrical engineering and was recognized in 2015 and 2016 as a Thomson Reuters highly cited researcher.