IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 18, 2020, accepted June 23, 2020, date of publication June 29, 2020, date of current version July 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005481

Optimal Cooperative Strategies for PHY Security Maximization Subject to SNR Constraints

KYRIAKOS FYTRAKIS[1], NICHOLAS KOLOKOTRONIS[2], (Member, IEEE), KONSTANTINOS KATSANOS[1], AND NICHOLAS KALOUPTSIDIS[1]

[1]Department of Informatics and Telecommunications, University of Athens, 15784 Athens, Greece
[2]Department of Informatics and Telecommunications, University of Peloponnese, 22131 Tripolis, Greece

Corresponding author: Kyriakos Fytrakis (kfitrakis@di.uoa.gr)

This work was supported in part by the Hellenic Foundation for Research and Innovation (HFRI) and in part by the General Secretariat for Research and Technology (GSRT), through the HFRI Ph.D. Fellowship Grant GA under Grant 1392.

ABSTRACT The cooperative jamming (CJ) and decode–and–forward (DF) protocols for physical layer security are studied in this paper. We propose a design that aims at maximizing the security gap, which is defined as the signal–to–noise ratio (SNR) difference between the destination and an eavesdropper, subject to security and reliability constraints defining the thresholds on the received signals' SNR values at the destination and the eavesdropper. A fractional quadratically constrained quadratic program (QCQP) is formulated, which is solved analytically and closed–form expressions are determined for both protocols. Numerical results demonstrate that the proposed designs achieve the same performance for the secrecy rate under both strategies compared with state–of–the–art approaches, for a proper choice of thresholds on SNR values. Additionally, for relaxed thresholds and at the cost of a slight decrease on the optimal secrecy rate value, the received SNR values at the eavesdropper are greatly decreased for the CJ protocol and even more for the DF protocol, while guaranteeing target SNR values at the destination, compared with previous state–of–the–art approaches.

INDEX TERMS Cooperative jamming, cooperative relaying, fractional programming, low–resource devices, physical layer security, wireless communications.

I. INTRODUCTION

Physical (PHY) layer security approaches have gained considerable attention over the past years as they can secure transmissions by exploiting the physical characteristics of the wireless medium against adversaries that intercept the transmitted messages or degrade the signals' strength received at the destination [2], [3], [31]. Wyner showed that the communication of a source–destination pair is perfectly secure provided that the source–eavesdropper channel is a degraded version of the main channel and rates are below the secrecy capacity of the channel [25], [28], [36]. The work of Wyner on the wiretap channel has been later extended to a variety of channel settings [6], [20], [21], [33].

The single–antenna systems' efficiency strongly depends on the channel conditions; secrecy capacity is zero if the channel between the source and eavesdropper is better than the channel between the source and destination [36]. On the other hand, multiple antenna systems [23], [33], [37, Ch. 6] seem to have no such limitations. However, due to cost and device limitations, network nodes may not have multiple antennas. Notable example of these simple systems is the Internet of Things (IoT), where many devices, e.g. sensors and embedded systems with limited capabilities need to communicate securely in the presence of an untrusted node/eavesdropper with similar capabilities. The IoT ecosystem will be facilitated by Fifth Generation (5G) wireless networks, and beyond, that aim to connect the surrounding devices of our everyday life through the network with much higher speed, low latency and ubiquitous connectivity [1], [15]. Under such scenarios, node cooperation is an effective way to enable single-antenna nodes to mimic multiple antenna systems and enjoy their benefits. In the latter case, communication between source and destination is aided by a set of helpers aiming at maximizing the secrecy capacity. Examples of cooperative transmission protocols are the decode–and–forward (DF), amplify–and–forward (AF) and cooperative jamming (CJ) [8]–[10], [16], [35]. Problems dealing with

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Fu Cheng.

secrecy capacity maximization typically lead to fractional quadratically constrained quadratic problems (QCQP). In the case of a single eavesdropper, closed–form optimal solutions have been derived subject to a transmit power constraint. When multiple eavesdroppers are considered [11], [22], suboptimal solutions are mainly sought. The global channel state information (CSI) is assumed to be known in the above works, though there have been proposals for similar schemes with partial CSI knowledge and statistical information about the eavesdroppers' CSI [27], [29]. Instead of utilizing jamming signals, artificial noise has also been proposed to confuse passive eavesdroppers [24], [26]. Recently, a mixture of cooperative beamforming and jamming strategies, combined with a helper selection scheme, has been proposed [5], [12], [14], [19], [30], [38].

In this paper, we consider a wireless network that consists of low–resource devices with limited capabilities, such as in the case of IoT paradigm. Multiple helpers (relays or jammers) assist a source to communicate securely with a destination in the presence of an untrusted node/eavesdropper. Perfect secrecy (i.e., perfectly zero information leakage to the untrusted node/eavesdropper) is not always needed to provide a perfectly secure service. In practical scenarios where services have different quality of service (QoS) requirements, if we ensure that the eavesdropper is operating below these requirements, then practical service-based secrecy can be guaranteed [15]. Instead of the achievable secrecy rate, we target at the use of the signal–to–noise ratio (SNR) to drive decisions. Measurement of the SNR at the receiver is efficiently done by using filtering techniques with a priori, or limited, knowledge of the signal even in complex communication environments [32]. Therefore, we focus on the maximization of the SNR difference between the destination and the eavesdropper, referred to as security gap. As demonstrated in our past work [17], [18], this approach can potentially lead to more efficient communication systems binding desired reliability and security constraints, in terms of SNR targets, along with the resources available at network nodes. We formulate a unified fractional QCQP problem with total transmit power, QoS constraints on the received SNR values at the destination and the eavesdropper that can be viewed as reliability and security constraints, allowing the joint investigation for optimal CJ and DF strategies under the presence of a single eavesdropper. Closed–form solutions are obtained in each case that are evaluated through extensive simulations and compared with direct transmission (no cooperation) and state–of–the–art algorithms, for the specific network, given in [11], [22]. We show that our proposed models, for proper choice of the thresholds on the SNR values, achieve the exact same performance as the analytical optimal solutions for the maximization of the secrecy rate subject to power constraints [11], [22]. On the other hand, if the SNR thresholds are relaxed, then we obtain significantly better performance for both protocols – specifically for the CJ protocol – for the security gap and the received SNR at the eavesdropper, while the received SNR at the destination is guaranteed, at the cost of a slight decrease on the secrecy rate. The main contributions of this paper are summarized as follows:

- The proposed approach ensures that different QoS requirements for security and reliability – modeled as constraints on the received SNR values at the destination and the eavesdropper – are guaranteed. This allows us to relax perfect secrecy requirements, whenever such a relaxation is tolerable [15], to achieve higher reliability at the destination or to slightly lower its attainable SNR accompanied by a considerable increase in the security. Instead of using the secrecy capacity, we maximize a tight bound of the secrecy rate, which is referred to as the security gap.
- We provide analytical solutions for the proposed scheme of DF and CJ protocols.
- We evaluate the proposed solutions by comparing them with low–complexity state–of–the–art algorithms [22] for solving the secrecy maximization problem subject to power constraints for network models Fig. 1. Our results shown that the proposed designs can achieve the exact same optimal secrecy rate as in [22]. Additionally, by properly choosing the SNR requirements of our model, at the cost of a negligible decrease of the optimal secrecy rate, we can further increase the perceived security (by decreasing the received SNR value at the eavesdropper) while guaranteeing the SNR value at the destination.

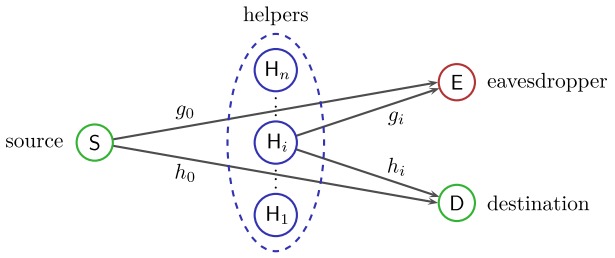

FIGURE 1. The source node S is assisted by helpers $H_1, \cdots, H_n$ to communicate with the destination D in the presence of an eavesdropper E.

The rest of the paper is organized as follows. In Section II we introduce the system model and the SNR based approach for the CJ and DF cooperative strategies. The theoretical results and closed–form solutions for the resulting fractional QCQP are provided in Section III. Simulation results and comparison with other proposed schemes are discussed in Section IV, while Section V provides the concluding remarks.

A. NOTATION

Boldface lowercase and uppercase letters denote column vectors and matrices, respectively; $\|\cdot\|$ is the Euclidean norm, and $\mathbb{E}[\cdot]$ denotes expectation. The conjugate of the complex number z is written as z^*. $\boldsymbol{I}_N$ denotes the order N identity matrix and $\mathbf{0}_N$ the $N \times N$ all-zero matrix (the index is omitted when the dimension is clear from the context). Conjugate and

conjugate transpose of the matrix $\boldsymbol{A}$ are written as $\boldsymbol{A}^*$ and $\boldsymbol{A}^\dagger$, respectively. $\boldsymbol{A} \succcurlyeq 0$ and $\boldsymbol{A} \succ 0$ mean that $\boldsymbol{A}$ is positive semidefinite and positive definite, respectively. The circularly symmetric complex Gaussian distribution with mean μ and variance σ^2 is denoted as $\mathcal{CN}(\mu, \sigma^2)$.

II. COOPERATIVE PHY SECURITY STRATEGIES

Consider the wireless network of Fig. 1 where the source S and destination D communicate securely in the presence of a passive eavesdropper E. We assume the presence of a fixed number of helping nodes $\mathsf{H}_1, \cdots, \mathsf{H}_n$ that assist S by either causing interference to E or by relaying the messages to D. The number n of helpers and the cooperative protocol (CJ or DF) used are assumed to be public information. All nodes are operating in half–duplex mode and are equipped with a single omni–directional antenna. Global CSI is assumed to be available at the trusted nodes to allow for efficient cooperation [11], [22]; consequently, not only are the baseband complex channel gains h_0^* and $\boldsymbol{h}^\dagger = (h_1^* \ \cdots \ h_n^*)$ between the source/destination and the helping nodes known, but also g_0^* and $\boldsymbol{g}^\dagger = (g_1^* \ \cdots \ g_m^*)$, that correspond to source/eavesdropper and relays/eavesdropper, respectively. In practice, this assumption is common and is used to model an honest–but–curious (e.g. untrusted) node [2]. Furthermore, all channels are assumed to experience Nakagami-m fading.

Let $\Gamma_\mathsf{d}, \Gamma_\mathsf{e}$ be equal to the values of $\gamma_\mathsf{d}, \gamma_\mathsf{e}$ in dB, which are the SNR at the destination and the eavesdropper, respectively. Instead of maximizing directly the secrecy rate, our objective is to determine $\max\,(\Gamma_\mathsf{d} - \Gamma_\mathsf{e})$, or equivalently $\max \gamma_\mathsf{d}/\gamma_\mathsf{e}$ subject to constraints pertaining to the total transmit power, reliability, and security. The expression $\Delta\Gamma = \Gamma_\mathsf{d} - \Gamma_\mathsf{e}$ represents the security gap and β_d (resp. β_e) is used below to denote the lower (resp. upper) bound on the received SNR at the destination (resp. eavesdropper). Specifically, our model is written mathematically as

$$\max \frac{\gamma_\mathsf{d}}{\gamma_\mathsf{e}} \quad \text{s.t. } \gamma_\mathsf{d} \geq \beta_\mathsf{d}, \ \gamma_\mathsf{e} \leq \beta_\mathsf{e} \tag{1}$$

where $\beta_\mathsf{d}, \beta_\mathsf{e}$ denote service requirements for reliability and security, respectively.

In the sequel we present several communication schemes between S and D when an E is in the vicinity of the former; specifically when there is no cooperation, i.e. direct transmission, and two cooperative transmission protocols, the CJ and DF protocol. When the source–eavesdroppers channel is better than the source–destination channel the secrecy rate is zero, or very low. Hence, for these cases cooperative transmission protocols, i.e., CJ and DF, can greatly improve the secrecy rate, especially for such scenarios where low–resource nodes are employed, e.g., IoT, with single antenna and restricted capabilities. That will be clear in the evaluation of the protocols in Section IV. For the cooperative transmission protocols we assume that all helpers are used. There are several works in the literature dealing with relay selection schemes [12], [19], but this is out of the scope of this work. Therefore, we assume that since the phase of relay selection has been completed, a trusted communication cluster has been formed among the source node S and all helpers H, and S decides how the total power budget is allocated among the nodes, e.g. it plays the role of a central coordination unit.

A. DIRECT TRANSMISSION

Let P be the total power budget available for transmitting a symbol x, with $\mathbb{E}\big[|x|^2\big] = 1$, from the source to the destination. If the source transmits x with maximum power P, the signal at the destination and the eavesdropper are given by $y_\mathsf{d} = \sqrt{P} h_0^* x + \eta_\mathsf{d}$ and $y_\mathsf{e} = \sqrt{P} g_0^* x + \eta_\mathsf{e}$, where $\eta_\mathsf{d}, \eta_\mathsf{e} \sim \mathcal{CN}(0, \sigma^2)$ represent the noise at the receivers. These expressions correspond to the direct transmission (DT) case, where the received SNR at the destination and the eavesdropper are $\gamma_\mathsf{d}^\mathsf{dt} = P|h_0|^2/\sigma^2$ and $\gamma_\mathsf{e}^\mathsf{dt} = P|g_0|^2/\sigma^2$, respectively.

B. COOPERATIVE JAMMING

Let the destination and the helping nodes share knowledge on a common jamming signal z to utilize, where $\mathbb{E}[|z|^2] = 1$. The source transmits x using a fraction of the power budget αP, whereas the ith helper transmits a weighted version of the jamming signal $w_i z$ with the remaining power $(1-\alpha)P$. The signals received at the destination and the eavesdroppers are $y_\mathsf{d} = \sqrt{(1-\alpha)P} h_0^* x + \sqrt{\alpha P}\boldsymbol{h}^\dagger \boldsymbol{w} z + \eta_\mathsf{d}$ and $y_\mathsf{e} = \sqrt{(1-\alpha)P} g_0^* x + \sqrt{\alpha P}\boldsymbol{g}^\dagger \boldsymbol{w} z + \eta_\mathsf{e}$, where $\boldsymbol{w}^\dagger = (w_1^* \ \cdots \ w_n^*)$ gathers the weights used by the helpers, with $\|\boldsymbol{w}\| = 1$. If $\boldsymbol{h}^\dagger \boldsymbol{w}$ and η_d (resp. $\boldsymbol{g}^\dagger \boldsymbol{w}$ and η_e) are independent random variables, the received SNR values at the destination and the eavesdropper are given by

$$\gamma_\mathsf{d}^\mathsf{cj} = \frac{(1-\alpha)P|h_0|^2}{\sigma^2 + \alpha P|\boldsymbol{h}^\dagger \boldsymbol{w}|^2} \tag{2}$$

$$\gamma_\mathsf{e}^\mathsf{cj} = \frac{(1-\alpha)P|g_0|^2}{\sigma^2 + \alpha P|\boldsymbol{g}^\dagger \boldsymbol{w}|^2} \tag{3}$$

where $\eta_\mathsf{d}, \eta_\mathsf{e} \sim \mathcal{CN}(0, \sigma^2)$. From (2) and (3) we have that $\gamma_\mathsf{d}^\mathsf{cj} \leq \gamma_\mathsf{d}^\mathsf{dt}$ and $\gamma_\mathsf{e}^\mathsf{cj} \leq \gamma_\mathsf{e}^\mathsf{dt}$ by non-negativity of all terms, and the bounds hold with equality when $\alpha = 0$.

C. DECODE–AND–FORWARD

The protocol is divided in two phases. During Phase–I, the source node transmits a signal x using a fraction of the power budget P that is received by the helping nodes. As in [11], [22], we assume that all helpers successfully decode the received signal. This happens if the rate at each helper is no less than the rate at the destination [11], and hence no less than the secrecy rate [22]. Hence,

$$\min_i \frac{1}{2} \log\left(1 + (1-\alpha)\frac{P|f_i|^2}{\sigma^2}\right) \geq R_\mathsf{s} \tag{4}$$

where $1 \leq i \leq n$, f_i the channel between source and the ith helper, and R_s is the secrecy rate. The transmitted signal is also received by the destination and the eavesdropper as $y_\mathsf{d}^{(1)} = \sqrt{(1-\alpha)P} h_0^* x + \eta_\mathsf{d}^{(1)}$ and

$y_{\mathsf{e}}^{(1)} = \sqrt{(1-\alpha)P}\, g_0^* x + \eta_{\mathsf{e}}^{(1)}$, respectively, where $\eta_{\mathsf{d}}^{(1)}, \eta_{\mathsf{e}}^{(1)} \sim \mathcal{CN}(0, \sigma^2)$. During Phase–II, cooperative transmission takes place, where the helpers transmit the re–encoded signal x with the remaining power; more precisely, the ith helper sends a weighted version $w_i x$ to the destination and the signals received are $y_{\mathsf{d}}^{(2)} = \sqrt{\alpha P}\boldsymbol{h}^\dagger \boldsymbol{w} x + \eta_{\mathsf{d}}^{(2)}$ and $y_{\mathsf{e}}^{(2)} = \sqrt{\alpha P}\boldsymbol{g}^\dagger \boldsymbol{w} x + \eta_{\mathsf{e}}^{(2)}$, where $\eta_{\mathsf{d}}^{(2)}, \eta_{\mathsf{e}}^{(2)}$ are independent from $\eta_{\mathsf{d}}^{(1)}, \eta_{\mathsf{e}}^{(1)}$ and identically distributed, and likewise $\|\boldsymbol{w}\| = 1$. By utilizing maximal ratio combining (MRC) [13], the destination and the eavesdropper achieve the following SNRs

$$\gamma_{\mathsf{d}}^{\mathsf{df}} = (1-\alpha)\gamma_{\mathsf{d}}^{\mathsf{dt}} + \alpha \frac{P|\boldsymbol{h}^\dagger \boldsymbol{w}|^2}{\sigma^2} \tag{5}$$

$$\gamma_{\mathsf{e}}^{\mathsf{df}} = (1-\alpha)\gamma_{\mathsf{e}}^{\mathsf{dt}} + \alpha \frac{P|\boldsymbol{g}^\dagger \boldsymbol{w}|^2}{\sigma^2} \tag{6}$$

equal to the SNRs of direct transmission by letting $\alpha = 0$.

D. ALGORITHMIC CONSIDERATIONS

Optimal solutions for the problem $\max \gamma_{\mathsf{d}}/\gamma_{\mathsf{e}}$, subject to constraints pertaining to the total transmit power, reliability, and security, are computed in this paper, for both the CJ and the DF cooperative protocols. These are computed in $\mathcal{O}(1)$ time for the CJ protocol by simply evaluating the closed-form expressions in Section III. This is roughly the case for the DF protocol as well, where the additional "correct decoding" constraint (4) adds a few more steps in the process; however, as added, this constraint is decoupled from the problem, and is thus efficiently solved using a similar bisection method like in [22, Sec. II]. More specifically, in each step we need to solve our maximization problem with $0 < \alpha \leq \hat{\alpha} < 1$, where $\hat{\alpha}$ is derived from the bisection procedure in each iteration. The procedure converges pretty fast, in just a few iterations, and finally solves the problem in the case of DF while taking into account the constraint (4).

III. THEORETICAL RESULTS ON SYSTEM DESIGN

In this paper we study the solvability of the problem (1) independently for CJ and DF protocols and evaluate their performance for each case. However, in this section we provide a unified approach in determining the optimal design for solving problem (1) for both the CJ and DF security strategies presented in Section II. In particular, let $\boldsymbol{B}, \boldsymbol{C} \succcurlyeq 0$ be matrices of rank one, with $\boldsymbol{B} = \boldsymbol{b}\boldsymbol{b}^\dagger$ and $\boldsymbol{C} = \boldsymbol{c}\boldsymbol{c}^\dagger$, for $\boldsymbol{b}, \boldsymbol{c} \in \mathbb{C}^N$. Both PHY security strategies lead to the following fractional QCQP problem

$$(\alpha^o, \boldsymbol{w}^o) = \arg \max_{\alpha, \boldsymbol{w} \neq \boldsymbol{0}} \frac{(1-\delta\alpha)r_1 + \alpha \boldsymbol{w}^\dagger \boldsymbol{B}\boldsymbol{w}}{(1-\delta\alpha)r_2 + \alpha \boldsymbol{w}^\dagger \boldsymbol{C}\boldsymbol{w}} \tag{7}$$

$$\text{s.t. } \alpha \in (0,1) \tag{7a}$$

$$\boldsymbol{w}^\dagger \boldsymbol{w} = 1 \tag{7b}$$

$$\boldsymbol{w}^\dagger \boldsymbol{B}\boldsymbol{w} \geq p_1(\alpha) \tag{7c}$$

$$\boldsymbol{w}^\dagger \boldsymbol{C}\boldsymbol{w} \leq p_2(\alpha) \tag{7d}$$

where $\delta \in \{0, 1\}$ is the parameter modeling the PHY security protocol —it is $\delta = 0$ for CJ and $\delta = 1$ for DF— and p_1, p_2 are functions directly related to the targeted SNR values, i.e. betas; moreover, we assume $0 < r_1 < \|\boldsymbol{b}\|^2$ and $0 < r_2 < \|\boldsymbol{c}\|^2$. The relation among the parameters of this subsection and those of the CJ and DF protocols is illustrated in Table 1.

TABLE 1. The relation between CJ, DF and the parameters of (7).

δ	$\boldsymbol{b}$	$\boldsymbol{c}$	r_1	r_2	q_1	q_2
0	$\boldsymbol{g}$	$\boldsymbol{h}$	σ^2/P	σ^2/P	$\lvert g_0\rvert^2/\beta_{\mathsf{E}}$	$\lvert h_0\rvert^2/\beta_{\mathsf{D}}$
1	$\boldsymbol{h}$	$\boldsymbol{g}$	$\lvert h_0\rvert^2$	$\lvert g_0\rvert^2$	$\beta_{\mathsf{D}}\sigma^2/P$	$\beta_{\mathsf{E}}\sigma^2/P$

Next, we assume that $\boldsymbol{b}, \boldsymbol{c}$ are not co-linear and that (7) has a nonempty feasibility set —i.e. $p_1(\alpha) \leq \|\boldsymbol{b}\|^2$ and $p_2(\alpha) \geq 0$. To solve (7), we reformulate the problem in accordance with an approach due to Dinkelbach [7]. Let $f(t, \alpha, \boldsymbol{w}) = (1 - \delta\alpha)(r_1 - tr_2) + \alpha \boldsymbol{w}^\dagger(\boldsymbol{B} - t\boldsymbol{C})\boldsymbol{w}$ and

$$F(t) = \max_{\alpha, \boldsymbol{w} \neq \boldsymbol{0}} f(t, \alpha, \boldsymbol{w}) \quad \text{, s.t. (7a)–(7d).} \tag{8}$$

Problems (7) and (8) are related via the following result.

Proposition 1: $F(t)$ is strictly decreasing and $F(t) = 0$ has a unique root t^o. Moreover, the optimal $(\alpha^o, \boldsymbol{w}^o)$ of the original problem (7) associated with t^o is also the solution of (8) and t^o is the optimal value taken by the objective function [22].

We proceed with the analysis of problem (8) by first defining the Lagrangian and then computing the Karush–Kuhn–Tucker (KKT) conditions that must be satisfied by an optimal solution [4]. The Lagrangian of (8) is given by

$$\begin{aligned}\mathcal{L}(t, \alpha, \boldsymbol{w}, \boldsymbol{\lambda}) = &-f(t, \alpha, \boldsymbol{w}) + \lambda_0 \left(\boldsymbol{w}^\dagger \boldsymbol{w} - 1\right) \\ &+\lambda_1 \left(p_1(\alpha) - \boldsymbol{w}^\dagger \boldsymbol{B}\boldsymbol{w}\right) + \lambda_2 \left(\boldsymbol{w}^\dagger \boldsymbol{C}\boldsymbol{w} - p_2(\alpha)\right)\end{aligned} \tag{9}$$

where $\boldsymbol{\lambda} = (\lambda_0\ \lambda_1\ \lambda_2)^T$ are the Lagrange multipliers corresponding to constraints (7b)–(7d).

Proposition 2: Let q_1, q_2 be such that $(1-\delta)r_1 < q_1 < \|\boldsymbol{b}\|^2$, $(1-\delta)r_2 < q_2 < \|\boldsymbol{c}\|^2$, and let p_1, p_2 be given by $p_i(\alpha) = (q_i - r_i)/\alpha - (-1)^\delta \eta_i$ for $i = 1, 2$, where $\eta_i = (1-\delta)q_i + \delta r_i$. Then, the optimal solution of (8) is such that either (7c) or (7d) hold with equality.

Proof: Let us first assume that $q_i \neq r_i$ for $i = 1, 2$. The partial derivatives of (9) are

$$\begin{aligned}\frac{\partial \mathcal{L}}{\partial \alpha} &= \delta(r_1 - tr_2) - \boldsymbol{w}^\dagger(\boldsymbol{B} - t\boldsymbol{C})\boldsymbol{w} \\ &\quad + \sum_{i=1}^{2} (-1)^i \lambda_i \frac{q_i - r_i}{\alpha^2}, \\ \frac{\partial \mathcal{L}}{\partial \boldsymbol{w}^\dagger} &= -\alpha(\boldsymbol{B} - t\boldsymbol{C})\boldsymbol{w} + \lambda_0 \boldsymbol{w} - \lambda_1 \boldsymbol{B}\boldsymbol{w} + \lambda_2 \boldsymbol{C}\boldsymbol{w}.\end{aligned}$$

At the optimal solution $(\alpha^o, \boldsymbol{w}^o)$ of problem (8) the KKT conditions must be satisfied. Specifically, from the partial derivatives of (9) evaluated at the optimal solution and the

complementarity conditions we have

$$\begin{aligned}\delta(r_1 - t^o r_2) - \boldsymbol{w}^{o\dagger}(\boldsymbol{B} - t^o\boldsymbol{C})\boldsymbol{w}^o + \sum_{i=1}^{2}(-1)^i\lambda_i\tfrac{q_i - r_i}{\alpha^2} &= 0\\ -\alpha^o(\boldsymbol{B} - t^o\boldsymbol{C})\boldsymbol{w}^o + \lambda_0^o\boldsymbol{w}^o - \lambda_1^o\boldsymbol{B}\boldsymbol{w}^o + \lambda_2^o\boldsymbol{C}\boldsymbol{w}^o &= 0\\ \lambda_1^o(p_1(\alpha^o) - \boldsymbol{w}^{o\dagger}\boldsymbol{B}\boldsymbol{w}^o) &= 0\\ \lambda_2^o(\boldsymbol{w}^{o\dagger}\boldsymbol{C}\boldsymbol{w}^o - p_2(\alpha^o)) &= 0\end{aligned}$$

After some manipulations we get the following expression

$$\delta\alpha^o(r_1 - t^o r_2) = \lambda_0^o + \sum_{i=1}^{2}(-1)^i\lambda_i^o\left(p_i(\alpha^o) - \frac{q_i - r_i}{\alpha^o}\right).$$

Due to Proposition 1, $F(t^o) = 0$. Therefore $\alpha^o(r_1 - t^o r_2) = \lambda_1^o(q_1 - r_1) - \lambda_2^o(q_2 - r_2)$ and thus $\lambda_0^o = (-1)^\delta\big(\lambda_2^o q_2 - \lambda_1^o q_1\big)$. Recall that $\lambda_1^o, \lambda_2^o \geq 0$ and $q_1, q_2 > 0$, thus if $\lambda_0^o \neq 0$ necessarily one of λ_1^o, λ_2^o is phstrictly positive. The same result would be obtained if $q_i = r_i$ for some $i = 1, 2$, but with η_i in place of q_i. Thus, the complementarity conditions

$$\begin{aligned}\lambda_1^o(p_1(\alpha^o) - \boldsymbol{w}^{o\dagger}\boldsymbol{B}\boldsymbol{w}^o) &= 0,\\ \lambda_2^o(\boldsymbol{w}^{o\dagger}\boldsymbol{C}\boldsymbol{w}^o - p_2(\alpha^o)) &= 0\end{aligned}$$

along with the above establish the claim. ∎

Next, we consider separately the cases where the constraints (7c), (7d) hold with equality, and determine the optimal solutions for the resulting problems.

A. EQUALITY IN (7d)

Let us assume that constraint (7d) holds with equality; then, we need also have $p_2(\alpha) \leq \|\boldsymbol{c}\|^2$, as (8) is assumed to have a nonempty feasibility set. Then

$$\alpha \in A = [a_1, a_2], \tag{7a′}$$

$$\boldsymbol{w}^\dagger\boldsymbol{C}\boldsymbol{w} = p_2(\alpha) \tag{7d′}$$

where $A \subset (0, 1)$, and the box constraint (7a′) is derived from the inequalities $p_1(\alpha) \leq \|\boldsymbol{b}\|^2$ and $0 \leq p_2(\alpha) \leq \|\boldsymbol{c}\|^2$, and $\alpha \leq \hat{\alpha}$ (only for $\delta = 1$). Hence, the objective function (8) becomes

$$F(t) = \max_{\alpha\in A}(1 - \delta\alpha)(r_1 - tr_2) + \alpha\left(\max_{\boldsymbol{w}\neq\boldsymbol{0}}\boldsymbol{w}^\dagger\boldsymbol{B}\boldsymbol{w}\right) - t\alpha p_2(\alpha).$$

The above optimization problem can be solved in two stages. First, we solve the inner QCQP to compute $\boldsymbol{w}^o = \arg\max_{\boldsymbol{w}\neq\boldsymbol{0}}\boldsymbol{w}^\dagger\boldsymbol{B}\boldsymbol{w}$, subject to constraints (7b)–(7c) by taking (7d) with equality. Next, the optimal value of α is determined for $\boldsymbol{w} = \boldsymbol{w}^o$ subject to (7a′).

Theorem 1: Let $\theta = \boldsymbol{b}\angle\boldsymbol{c}$ be the angle between $\boldsymbol{b}, \boldsymbol{c}$ and $\theta \neq 0 \pmod\pi$. Assuming that problem (7) has nonempty feasibility set, the optimal solution $\boldsymbol{w}^o := \boldsymbol{w}^o(\alpha)$ of

$$\max_{\boldsymbol{w}\neq\boldsymbol{0}}\boldsymbol{w}^\dagger\boldsymbol{B}\boldsymbol{w} \quad s.t.\ (7b), (7c), (7d') \tag{10}$$

is given by $\boldsymbol{w}^o = w_1(\alpha)\boldsymbol{b} + w_2(\alpha)\boldsymbol{c}$ with

$$w_1(\alpha) = \frac{1}{|\Omega|}\sqrt{\|\boldsymbol{c}\|^2 - p_2(\alpha)}\,e^{j(\phi+\theta-\omega)}, \tag{11a}$$

$$w_2(\alpha) = \frac{1}{\|\boldsymbol{c}\|^2}\left(|w_1||\boldsymbol{b}^\dagger\boldsymbol{c}| - \sqrt{p_2(\alpha)}\right)e^{j\phi} \tag{11b}$$

where $\Omega = \|\boldsymbol{b}\|\|\boldsymbol{c}\|\sin\theta$ and $\phi \in [0, 2\pi)$; $\omega = \pi/2$ if $p_2(\alpha) = \|\boldsymbol{c}\|^2\cos^2\theta$, and $\omega = \pi$ otherwise.

Proof: See Appendix A. ∎

Using the solution $\boldsymbol{w}^o$ provided by Theorem 1 we can find α^o by substituting $\boldsymbol{w}^o$ in $f(t, \alpha, \boldsymbol{w})$. After some manipulations, and a change of variables $x := x(t)$, we get the function

$$f(x, \alpha) = \begin{cases} r - x(1 - \alpha) + l\sqrt{s(\alpha)}, & \text{if } \delta = 0\\ x - r(1 - \alpha) + l\sqrt{s(\alpha)}, & \text{if } \delta = 1\end{cases} \tag{12}$$

where $l = 2|\Omega||\boldsymbol{b}^\dagger\boldsymbol{c}|/\|\boldsymbol{c}\|^4$ and

$$x = \frac{\Omega^2}{\|\boldsymbol{c}\|^2} + (-1)^\delta(t - k)q_2, \tag{13a}$$

$$r = \frac{\Omega^2}{\|\boldsymbol{c}\|^2} + (-1)^\delta(r_1 - k\,r_2) \tag{13b}$$

with $k = (|\boldsymbol{b}^\dagger\boldsymbol{c}|^2 - \Omega^2)/\|\boldsymbol{c}\|^4$. The function s in (12), which is non-negative by construction, equals the quadratic polynomial $s(\alpha) := p_2(\alpha)\big(\|\boldsymbol{c}\|^2 - p_2(\alpha)\big)\alpha^2 = -s_0 + s_1\alpha - (-1)^\delta s_2\alpha^2$, whose coefficients are given by $s_0 = (q_2 - r_2)^2$, $s_1 = (q_2 - r_2)\big(\|\boldsymbol{c}\|^2 + (-1)^\delta 2\eta_2\big)$, and $s_2 = \eta_2\big(\|\boldsymbol{c}\|^2 + (-1)^\delta\eta_2\big)$. From (7) and Proposition 2 we have that $0 < \eta_2 < \|\boldsymbol{c}\|^2$ and therefore $s_2 > 0$. If $l = 0$ (which holds if and only if $\boldsymbol{b}, \boldsymbol{c}$ are either co-linear or orthogonal) or $q_2 = r_2$ (for $\delta = 1$), f becomes a linear function of α; it is maximized at one of the endpoints of the interval A in (7a′). As this does not depend on x, α^o can be substituted in (11) to determine the optimal $\boldsymbol{w}^o$. Otherwise, α^o is provided by the following theorem.

Theorem 2: Let $u = \big((1-\delta)x + \delta r\big)/l$, and assume $q_2 \neq r_2$ and $\theta \neq 0 \pmod{\pi/2}$. The optimal solution $\alpha^o := \alpha^o(x)$ of $\max_{\alpha\in A} f(x, \alpha)$ is determined as follows.

1) *If $\delta = 1$ and $s_2 > u^2$ then $\alpha^o = a_2$.*
2) *If $\delta = 1$ and $s_2 = u^2$ then $\alpha^o = a_1$ (resp. $\alpha^o = a_2$) for $u < 0$ (resp. $u > 0$).*
3) *Otherwise, let $\Delta_s = s_1^2 - (-1)^\delta 4 s_0 s_2$ and*

$$\alpha^\star = (-1)^\delta\frac{1}{2s_2}\left(s_1 + u\sqrt{\frac{\Delta_s}{(u^2 + (-1)^\delta s_2)}}\right). \tag{14}$$

Then, $\alpha^o = \alpha^\star$ if $\alpha^\star \in A$, and $\alpha^o = a_1$ (resp. $\alpha^o = a_2$) if $\alpha^\star < a_1$ (resp. $\alpha^\star > a_2$).

Proof: See Appendix B. ∎

Finally, the optimal value of the original problem when (7d) holds with equality, and the actual values of $(\alpha^o, \boldsymbol{w}^o)$ are determined by computing the root of $F(x) = f(x, \alpha^o)$.

Theorem 3: The equation $F(x) = 0$ has a unique root x^o given by

$$x^o = \begin{cases}\dfrac{r(2s_2 - s_1) + \sqrt{\Delta_s(r^2 + l^2 z)}}{2z}, & \text{if } \delta = 0 \text{ and } \alpha^\star \in A\\ \dfrac{r(1 - \alpha^o)^\delta + (-1)^\delta l\sqrt{s(\alpha^o)}}{(1 - \alpha^o)^{1-\delta}}, & \text{otherwise}\end{cases}$$

where $z = r_2(\|\boldsymbol{c}\|^2 + r_2) > 0$; the optimal value of the original problem (7) is then

$$t^o = k + (-1)^\delta\frac{1}{q_2}\left(x^o - \frac{\Omega^2}{\|\boldsymbol{c}\|^2}\right). \tag{15}$$

Proof: See Appendix C. ∎

B. EQUALITY IN (7c)

Next, we assume that constraint (7c) holds with equality; in this case we also require $p_1(\alpha) \geq 0$, since (8) has a nonempty feasibility set. Likewise, we have

$$\alpha \in \tilde{A} = [\tilde{a}_1, \tilde{a}_2], \tag{7a''}$$

$$\boldsymbol{w}^\dagger \boldsymbol{B}\boldsymbol{w} = p_1(\alpha) \tag{7c'}$$

where $\tilde{A} \subset (0, 1)$, and the box constraint (7a'') is derived from the inequalities $0 \leq p_1(\alpha) \leq \|\boldsymbol{b}\|^2$ and $p_2(\alpha) \geq 0$, and $\alpha \leq \hat{\alpha}$ (only for $\delta = 1$). Hence, the objective function (8) becomes

$$F(t) = \max_{\alpha \in \tilde{A}} (1 - \delta\alpha)(r_1 - tr_2) + \alpha p_1(\alpha) - t\alpha \left(\min_{\boldsymbol{w} \neq \boldsymbol{0}} \boldsymbol{w}^\dagger \boldsymbol{C}\boldsymbol{w} \right).$$

Theorem 4: Let $\theta = \boldsymbol{b}\angle\boldsymbol{c}$ be the angle between $\boldsymbol{b}, \boldsymbol{c}$ and $\theta \neq 0 \pmod{\pi}$. Assuming that problem (7) has nonempty feasibility set, the optimal solution $\boldsymbol{w}^o := \boldsymbol{w}^o(\alpha)$ of

$$\min_{\boldsymbol{w} \neq \boldsymbol{0}} \boldsymbol{w}^\dagger \boldsymbol{C}\boldsymbol{w} \quad \textit{s.t. (7b), (7c'), (7d)} \tag{16}$$

is given by $\boldsymbol{w}^o = w_1(\alpha)\boldsymbol{b} + w_2(\alpha)\boldsymbol{c}$ with

$$w_1(\alpha) = \frac{1}{\|\boldsymbol{b}\|^2} \left(|w_2||\boldsymbol{b}^\dagger \boldsymbol{c}| + \sqrt{p_1(\alpha)} \right) e^{j\varphi}, \tag{17a}$$

$$w_2(\alpha) = \frac{1}{|\Omega|} \sqrt{\|\boldsymbol{b}\|^2 - p_1(\alpha)}\, e^{j(\varphi - \theta + \omega)} \tag{17b}$$

where $\Omega = \|\boldsymbol{b}\|\|\boldsymbol{c}\| \sin\theta$ and $\varphi \in [0, 2\pi)$; $\omega = \pi/2$ if $p_1(\alpha) = \|\boldsymbol{b}\|^2 \cos^2\theta$, and $\omega = \pi$ otherwise.

Proof: The proof is similar to that of Theorem 1 and is therefore omitted. The only difference is that we now have to deal with a minimization problem instead, which is solved by using Propositions 3, 4 that still hold in this case. ■

Substituting $\boldsymbol{w}^o$ found by Theorem 4 in $f(t, \alpha, \boldsymbol{w})$, and performing the change of variables $x := x(t)$, we obtain

$$f(x, \alpha) = \left(k - (-1)^\delta \frac{1}{q_1} \left(x + \frac{\Omega^2}{\|\boldsymbol{b}\|^2} \right) \right)^{-1} f'(x, \alpha)$$

where f' is given by (12) but with x, r, l defined as

$$x = -\frac{\Omega^2}{\|\boldsymbol{b}\|^2} + (-1)^\delta \left(k - \frac{1}{t} \right) q_1, \tag{18a}$$

$$r = -\frac{\Omega^2}{\|\boldsymbol{b}\|^2} + (-1)^\delta \left(k\, r_1 - r_2 \right) \tag{18b}$$

and $l = 2|\Omega||\boldsymbol{b}^\dagger \boldsymbol{c}|/\|\boldsymbol{b}\|^4$. In addition, $k = (|\boldsymbol{b}^\dagger \boldsymbol{c}|^2 - \Omega^2)/\|\boldsymbol{b}\|^4$ and the coefficients of $s(\alpha) := p_1(\alpha)\big(\|\boldsymbol{b}\|^2 - p_1(\alpha)\big)\alpha^2$, which retains the form given in the first case, are now defined as $s_0 = (q_1 - r_1)^2$, $s_1 = (q_1 - r_1)\big(\|\boldsymbol{b}\|^2 + (-1)^\delta 2\eta_1\big)$, and $s_2 = \eta_1\big(\|\boldsymbol{b}\|^2 + (-1)^\delta \eta_1\big)$. Likewise, if $l = 0$ or $q_1 = r_1$ (for $\delta = 1$), f becomes a linear function of α and is maximized at one of the endpoints of $\tilde{A}$ in (7a''). Note that $f(x, \alpha) = tf'(x, \alpha)$ due to (18a), with $t > 0$ by definition, and that only f' depends on α. Since the coefficients of f' share the same structure and properties with f in (12), we obtain the following when $q_1 \neq r_1$ (in which case it is $s_0, s_2 > 0$) and $\theta \neq 0 \pmod{\pi/2}$; this could be easily shown following the same steps as in the proof of Theorem 2.

Theorem 5: Let $u = \big((1-\delta)x + \delta r\big)/l$, and assume $q_1 \neq r_1$ and $\theta \neq 0 \pmod{\pi/2}$. The optimal solution $\alpha^o := \alpha^o(x)$ of $\max_{\alpha \in \tilde{A}} f(x, \alpha)$ is determined as follows.

1) *If $\delta = 1$ and $s_2 > u^2$ then $\alpha^o = \tilde{a}_2$.*
2) *If $\delta = 1$ and $s_2 = u^2$ then $\alpha^o = \tilde{a}_1$ (resp. $\alpha^o = \tilde{a}_2$) for $u < 0$ (resp. $u > 0$).*
3) *Otherwise, $\alpha^\star$ is defined as in (14). Then, $\alpha^o = \alpha^\star$ if $\alpha^\star \in \tilde{A}$, and $\alpha^o = \tilde{a}_1$ (resp. $\alpha^o = \tilde{a}_2$) if $\alpha^\star < \tilde{a}_1$ (resp. $\alpha^\star > \tilde{a}_2$).*

Finally the root of $F(x) = f(x, \alpha^o)$, allowing to determine the actual values of the optimal solution $(\alpha^o, \boldsymbol{w}^o)$, is computed by the following Theorem.

Theorem 6: With the above notation, the equation $F(x) = 0$ has a unique root x^o given by Theorem 3, with the difference that $\alpha^* \in \tilde{A}$, where $z = r_1(\|\boldsymbol{b}\|^2 + r_1) > 0$; the optimal value of the original problem (7) is then

$$t^o = \left(k - (-1)^\delta \frac{1}{q_1} \left(x^o + \frac{\Omega^2}{\|\boldsymbol{b}\|^2} \right) \right)^{-1}. \tag{19}$$

Proof: Let $F'(x) = f'(x, \alpha^o)$. Since $F(x) = tF'(x)$ due to $f(x, \alpha) = tf'(x, \alpha)$, and $t^o > 0$ by definition, $F(x^o) = 0$ if and only if $F'(x^o) = 0$. Analogous arguments with those used in the proof of Theorem 3, since F' admits the same structure and properties with the function F in the proof of Theorem 3, lead to x^o; the only difference is the particular value taken by $s(1) = -r_1(\|\boldsymbol{b}\|^2 + r_1) = -z$. The optimal value t^o is then can be computed from (18a). ■

IV. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of the proposed algorithms. In [22], the authors suggested low complexity, closed–form, optimal solutions for the maximization problem of the secrecy rate subject to power constraints only. Our proposed optimal strategies are of similar complexity as in [22] since we provide analytical optimal solutions for our optimization problems. Additionally, the security gap, our objective function, by definition, provides a lower bound on the secrecy rate. The introduction of the inequality constraints on the received SNR values at the destination and the eavesdropper further restricts the feasibility set defined by power constraints only. Therefore, the optimal secrecy rate achieved from the proposed optimal solutions in [22] defines the benchmark of our proposed solutions, i.e. evaluating the secrecy rate with our optimal strategies cannot be greater than its optimal value derived in [22]. Specifically, we compare our proposed CJ strategy with the optimal solution (CJ_{opt}) in [22, Sec. III-A.2], where the problem is recast as an one-dimensional optimization problem. In the case of DF, our protocol is compared with the optimal solution (DF_{opt}) in [22, Sec. III-A.1], where the problem is solved analytically but with the correct decoding constraint decoupled by using a bisection method.

We choose such a network configuration focusing on the distances and fading effects among the nodes, where the source, eavesdropper and destination are placed along a horizontal line as illustrated in Fig. 2. Furthermore, the helpers

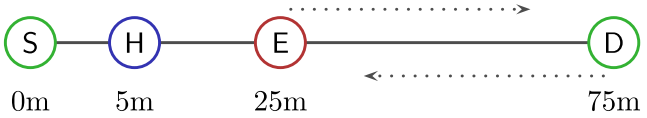

FIGURE 2. The simulation model; the source (S), helpers (H), eavesdropper (E), and destination (D) are placed along a line. The distances shown are measured from the source and E, D are allowed to move in the range [25m, 75m].

are assumed to be located randomly inside a two–dimensional grid. Despite the fact that the eavesdropper and destination can be at the same location, the different phases of their corresponding channels can result in differences at their received SNR values. The channels between any pair of nodes (k, l) are modeled as $f_{k,l} = \sqrt{d_{k,l}^{-c}}\ |f_{k,l}|\ e^{j\theta}$, where $d_{k,l}$ is the distance between the *kth* and *lth* node, $c = 3.5$ is the path loss exponent, $|f_{k,l}|$ denotes the fading coefficient of the channel, which is assumed to be distributed according to the Nakagami-m distribution, and θ is the phase uniformly distributed in $[0, 2\pi)$. The Nakagami-m distribution has the ability to model a wide class of fading channel conditions based on the value of the parameter m; for instance for $m = 1$, it becomes equivalent to the Rayleigh distribution. We assume $m = 3$, in order to indicate the existence of a strong LOS component which represents less-severe fading conditions. Specifically, for such small distances between the nodes, at most 75m (see also Fig. 2), $m = 3$ is an appropriate choice to model generic fading in the experimental setup. During the experiments, the source–destination distance is fixed at 50m (see also Fig. 2), and a number of $n = 10$ helpers are employed with random location inside a two–dimensional window of range 2m (at both horizontal and vertical axis), where the beginning of this area is fixed at 5m and extends towards destination's direction. In one case the SNR bounds β_{D} and β_{E} were adaptively chosen in each distance step as the optimum values in terms of the security gap, e.g. one decision could be the optimal SNR values derived from $\mathrm{CJ}_{\mathrm{opt}}$ and $\mathrm{DF}_{\mathrm{opt}}$, and the results for both protocols denoted by $\mathrm{CJ}_{\mathrm{gap\text{-}opt}}$ and $\mathrm{DF}_{\mathrm{gap\text{-}opt}}$. Additionally, as a second case, we relax the values of previous optimal betas and the results for both protocols in this case are denoted by $\mathrm{CJ}_{\mathrm{gap\text{-}rel}}$ and $\mathrm{DF}_{\mathrm{gap\text{-}rel}}$. The power budget and noise power are fixed at $P = 30$dBm and $\sigma^2 = -40$dBm, respectively. The experimental results for both the DF and CJ protocols are obtained after 1000 independent Monte Carlo simulations.

For the CJ protocol, in Fig. 3 it is observed that the secrecy rate for the $\mathrm{CJ}_{\mathrm{opt}}$ and $\mathrm{CJ}_{\mathrm{gap\text{-}opt}}$ is exact the same for every position of the eavesdropper from $25 - 75$m. Hence, by solving our proposed alternate physical layer security scheme $\mathrm{CJ}_{\mathrm{gap\text{-}opt}}$ we achieve exact the same performance for the secrecy rate with the optimal solution of the information–theoretic approach. The same behavior holds for the security gap, the received SNR at the destination and eavesdropper illustrated in Fig. 4, Fig. 5 and Fig. 6, respectively. When we relax the choice of betas, i.e. $\mathrm{CJ}_{\mathrm{gap\text{-}rel}}$, it is seen in Fig. 3 that the secrecy rate is slightly decreased, as expected since the optimal value is the upper bound on

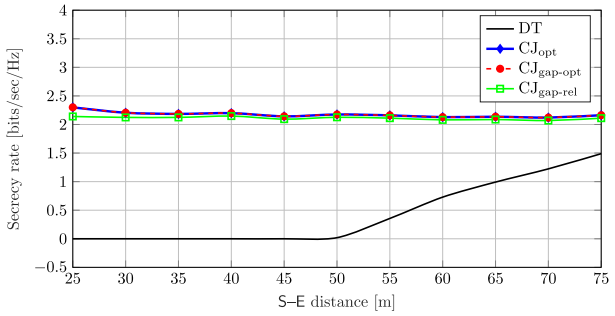

FIGURE 3. Secrecy rate versus source–eavesdropper distance for the CJ protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

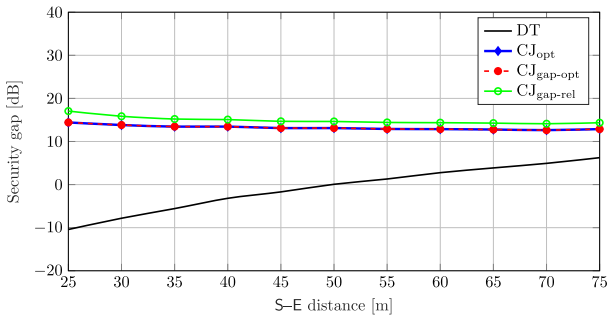

FIGURE 4. Security gap versus source–eavesdropper distance for the CJ protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

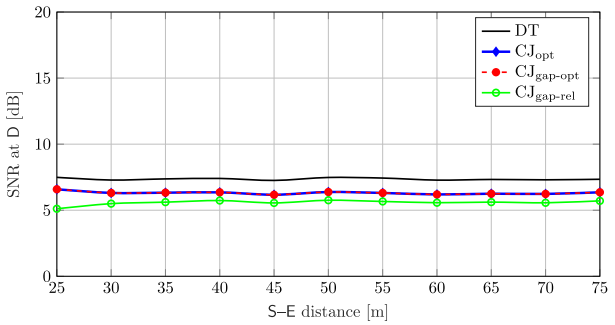

FIGURE 5. Received SNR value at the destination versus source–eavesdropper distance for the CJ protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

our proposed scheme, by 2% on average and the received SNR at the destination Fig. 5 is decreased by 14% on average (pure number) compared with their optimal values. However, the received SNR at the eavesdropper is greatly decreased by 40% on average (pure number) compared with its optimal value Fig. 6. Consequently, the security gap is further improved compared with its optimal value by 45% on average (pure number) Fig. 4. Hence, by letting a small decrease on the received SNR at the destination $\mathrm{CJ}_{\mathrm{gap\text{-}rel}}$ compared with its value at the optimal solution $\mathrm{CJ}_{\mathrm{opt}}$, we can achieve a great decrease on the received SNR at the eavesdropper.

For the DF protocol, the secrecy rate and the security gap, in Fig. 7 and Fig. 8 respectively, show the advantage of using the proposed DF protocol over the DT, since for the

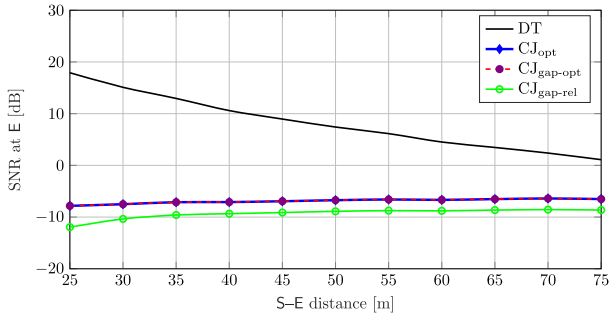

FIGURE 6. Received SNR value at the eavesdropper versus source–eavesdropper distance for the CJ protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

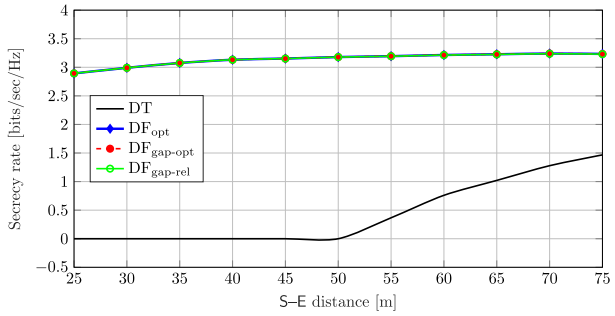

FIGURE 7. Secrecy rate versus source–eavesdropper distance for the DF protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

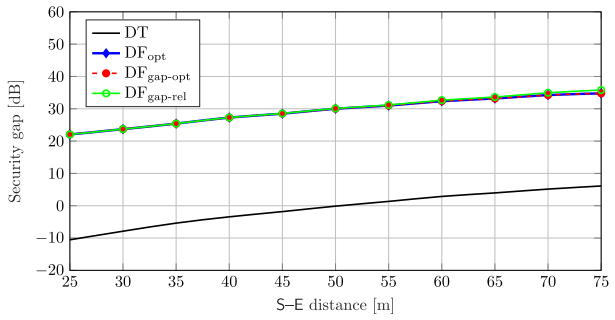

FIGURE 8. Security gap versus source–eavesdropper distance for the DF protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

particular setup the secrecy rate of the latter is almost zero. In addition, we see that $\mathrm{DF}_{\mathrm{opt}}$ and $\mathrm{DF}_{\mathrm{gap\text{-}opt}}$ achieve exact the same secrecy rate and security gap, as in the CJ protocol. Consequently, the same holds for the received SNR values at the destination and eavesdropper depicted in Fig. 9 and 10, respectively. Hence, our proposed solution of the alternate physical layer security approach $\mathrm{DF}_{\mathrm{gap\text{-}opt}}$, provides exact the same performance compared with the optimal solution $\mathrm{DF}_{\mathrm{opt}}$ of the information–theoretic approach, which is our scheme's benchmark. Finally, by a relaxation on the SNR thresholds $\mathrm{DF}_{\mathrm{gap\text{-}rel}}$ it is observed that the SNR at the eavesdropper is decreased for about 7% to 22% (pure numbers) as depicted in Fig. 10 at the interval $60 - 75$m, which further results to an increasing of security gap for about 7% to 27% (pure numbers) at this range of distances. This improvement comes

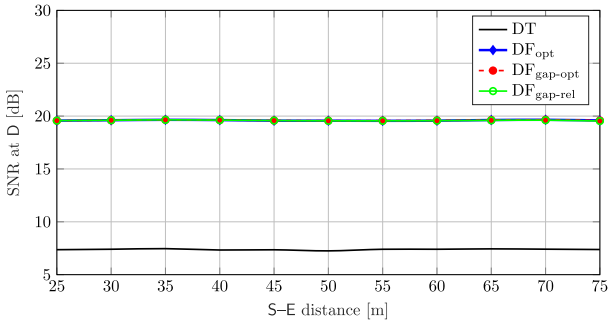

FIGURE 9. Received SNR value at the destination versus source–eavesdropper distance for the DF protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

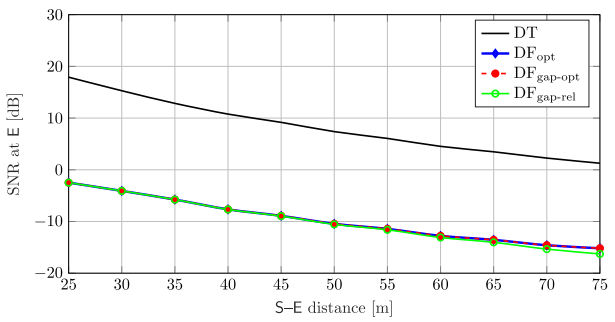

FIGURE 10. Received SNR value at the eavesdropper versus source–eavesdropper distance for the DF protocol. Results are shown for $n = 10$ helpers with the destination fixed at 50m from the source.

with a negligible cost to the received SNR at the destination and the secrecy rate.

V. CONCLUSION

Two cooperative PHY security protocols, CJ and DF, were studied in this paper aiming at maximizing effectively the SNR difference between the destination and an eavesdropper. QoS constraints that allow one to explicitly define a target reliability and security level were also included, so as to avoid situations where the resulting SNR at the destination is undesirably low (likewise high at the eavesdroppers) although the secrecy rate is maximized. Closed–form expressions were provided for both strategies for optimal problems whose performance was evaluated by extensive numerical analysis and comparisons with the state–of–the–art designs. It was shown that our approach achieves the same performance with the state–of–the–art algorithms for both protocols while it improves the performance —in terms of the security gap and received SNR at the eavesdropper— while ensuring reliability and security levels. That comes with a negligible cost for secrecy rate and the received SNR at the destination, compared to previous approaches. Ongoing research work focuses on improving our results to multiple eavesdroppers where our techniques are expected to allow overcoming the limitation on the number of helpers whenever nulling constraints should be imposed. In these cases, the proposed solutions for the DF protocol (see e.g. [11]) work only if the number of helpers is larger than that of the eavesdroppers. Additionally, we want

to study our approach in different and more complex wireless networks where the capabilities of nodes are not necessarily so limited, i.e. multiple antennas systems, multiple eavesdroppers, smart eavesdroppers, etc.

APPENDIX A
PROOF OF THEOREM 1

For simplicity, the functions p_1 and p_2 will be treated as positive constants since the optimization problem is solved with respect to $\boldsymbol{w}$, assuming α to be fixed. This is also the case for other quantities, e.g. w_1, w_2, depending on α. As a result, we write p_1, p_2 instead of $p_1(\alpha), p_2(\alpha)$, etc.

A. INTERMEDIATE RESULTS

Since (10) has a nonempty feasibility set, its optimal solution is found by solving

$$\max_{\boldsymbol{w}\neq\boldsymbol{0}} \boldsymbol{w}^\dagger \boldsymbol{B}\boldsymbol{w} \quad \text{s.t. (7b),(7d}') \,. \tag{20}$$

To prove the theorem, we need two intermediate results, stated in Propositions 3 and 4 below.

Proposition 3: Let $\theta = \boldsymbol{b}\angle\boldsymbol{c}$, $\theta \neq 0 \pmod{\pi}$, and $\boldsymbol{D} = (\boldsymbol{b}\ \boldsymbol{c})$. The problem (20) is equivalent to

$$\max_{z\neq\boldsymbol{0}} z^\dagger \tilde{\boldsymbol{B}} z \quad s.t. \quad z^\dagger \tilde{\boldsymbol{I}} z \leq 1\,,\ z^\dagger \tilde{\boldsymbol{C}} z = p_2 \tag{21}$$

where $\tilde{\boldsymbol{I}} = \boldsymbol{D}^\dagger\boldsymbol{D}$, $\tilde{\boldsymbol{B}} = \boldsymbol{D}^\dagger\boldsymbol{B}\boldsymbol{D}$ and $\tilde{\boldsymbol{C}} = \boldsymbol{D}^\dagger\boldsymbol{C}\boldsymbol{D}$.

Proof: The Moore-Penrose pseudoinverse is defined as $\boldsymbol{D}^\# = (\boldsymbol{D}^\dagger\boldsymbol{D})^{-1}\boldsymbol{D}^\dagger$. Let $\boldsymbol{P} = \boldsymbol{D}\boldsymbol{D}^\#$ and $\boldsymbol{P}^\perp = \boldsymbol{I}_N - \boldsymbol{P}$ be the orthogonal projection operators on the range and the null space of $\boldsymbol{D}$, respectively. By writing $\boldsymbol{w} = \boldsymbol{P}\boldsymbol{w} + \boldsymbol{P}^\perp\boldsymbol{w} = \boldsymbol{u} + \boldsymbol{v}$, note that the objective function and the equality constraint do not depend on $\boldsymbol{v}$; the power constraint becomes $\boldsymbol{u}^\dagger\boldsymbol{u} + \boldsymbol{v}^\dagger\boldsymbol{v} = 1$ due to $\boldsymbol{u} \perp \boldsymbol{v}$ (i.e. $\boldsymbol{u}^\dagger\boldsymbol{v} = 0$). The optimal value of (20) is obtained at $\boldsymbol{w}^o = (\boldsymbol{u}^o, \boldsymbol{v})$ for any $\boldsymbol{v}$ in the null space of $\boldsymbol{D}$ satisfying $\|\boldsymbol{u}\|^2 + \|\boldsymbol{v}\|^2 = 1$ and $\|\boldsymbol{v}\| \geq 0$, which implies $\|\boldsymbol{u}\|^2 \leq 1$. The proof is concluded by noting that $\boldsymbol{w} = \boldsymbol{D}\boldsymbol{z}$ for some $\boldsymbol{z} \in \mathbb{C}^2$, as it holds $\boldsymbol{P}\boldsymbol{D} = \boldsymbol{D}$ and $\boldsymbol{P}^\perp\boldsymbol{D} = \boldsymbol{0}$. ∎

Proposition 4: With the above notation, (21) is equivalent to

$$\max_{z\neq\boldsymbol{0}} z^\dagger \tilde{\boldsymbol{B}} z \quad s.t.\ z^\dagger \tilde{\boldsymbol{I}} z = 1\,,\ z^\dagger \tilde{\boldsymbol{C}} z = p_2\,. \tag{22}$$

Proof: The Lagrangian of the problem (21) is given by

$$\mathcal{L}(z, \boldsymbol{\zeta}) = -z^\dagger \tilde{\boldsymbol{B}} z + \zeta_0(z^\dagger z - 1) + \zeta_2(z^\dagger \tilde{\boldsymbol{C}} z - p_2) \tag{23}$$

where $\boldsymbol{\zeta} = (\zeta_0\ \zeta_2)^T$ are the Lagrange multipliers. From the KKT conditions (omitted due to space limitations), we get $\tilde{\boldsymbol{B}} z^o = \zeta_0^o z^o + \zeta_2^o \tilde{\boldsymbol{C}} z^o$, where $\zeta_0^o \geq 0$ and $\zeta_2^o \neq 0$. Let us first assume that $\zeta_0^o = 0$; then $(\tilde{\boldsymbol{B}} - \zeta_2^o\tilde{\boldsymbol{C}})z^o = 0$. Due to $z^o \neq \boldsymbol{0}$, we necessarily have that $\text{rank}(\tilde{\boldsymbol{B}} - \zeta_2^o\tilde{\boldsymbol{C}}) < 2$. After straightforward manipulations, the determinant $\det(\tilde{\boldsymbol{B}} - \zeta_2^o\tilde{\boldsymbol{C}})$ is computed as $-\zeta_2^o\Omega^4$, where Ω is defined in Theorem 1. Thus, it must be $\Omega = 0$ since $\zeta_2^o \neq 0$ by definition. But $\Omega = 0$ if and only if $\theta = 0, \pm\pi$, which leads to a contradiction (note that $\boldsymbol{b}, \boldsymbol{c} \neq \boldsymbol{0}$). As a result, $\zeta_0^o > 0$ and by the complementarity condition we have that the optimal solution z^o satisfies $z^{o\dagger}\tilde{\boldsymbol{I}} z^o = 1$. ∎

B. PROOF OF THEOREM 1

Since $\boldsymbol{w} = \boldsymbol{D}\boldsymbol{z}$ (see the proof of Proposition 3), by letting $\boldsymbol{z} = (w_1\ w_2)^T \in \mathbb{C}^2$ we obtain that $\boldsymbol{w} = w_1\boldsymbol{b} + w_2\boldsymbol{c}$. From Proposition 4, the problem (22) becomes

$$\max_{z\in\mathbb{C}^2} \|\boldsymbol{b}\|^2 - |w_2|^2\Big(\|\boldsymbol{b}\|^2\|\boldsymbol{c}\|^2 - |\boldsymbol{b}^\dagger\boldsymbol{c}|^2\Big) \tag{24}$$

$$\text{s.t. } |w_1|^2\|\boldsymbol{b}\|^2 + |w_2|^2\|\boldsymbol{c}\|^2 + 2\Re\big(w_1^* w_2 \boldsymbol{b}^\dagger\boldsymbol{c}\big) = 1 \tag{24a}$$

$$|w_1|^2 = \frac{\|\boldsymbol{c}\|^2 - p_2}{\|\boldsymbol{b}\|^2\|\boldsymbol{c}\|^2 - |\boldsymbol{b}^\dagger\boldsymbol{c}|^2}\,. \tag{24b}$$

Note that if $p_2 = \|\boldsymbol{c}\|^2$ or $\theta = \pm\pi/2$ (i.e. $\boldsymbol{b} \perp \boldsymbol{c}$), the problem becomes trivial and $\boldsymbol{z} = (w_1\ w_2)^T$ is easily found to be given by (11). Indeed, in the first case (24a), (24b) immediately lead to $|w_1| = 0$ and $|w_2| = 1/\|\boldsymbol{c}\|$; the second case yields $|w_1| = \sqrt{\|\boldsymbol{c}\|^2 - p_2}/\|\boldsymbol{b}\|\|\boldsymbol{c}\|$ and $|w_2| = \sqrt{p_2}/\|\boldsymbol{c}\|^2$.

In the rest of the proof we therefore assume that $p_2 < \|\boldsymbol{c}\|^2$ and $\theta \neq 0 \pmod{\pi/2}$ that gives $0 < |\boldsymbol{b}^\dagger\boldsymbol{c}|^2 < \|\boldsymbol{b}\|^2\|\boldsymbol{c}\|^2$. The optimization problem (24) is then simplified to $\min_{z\in\mathbb{C}^2} |w_2|^2$ subject to (24a)–(24b). Let $w_1 = |w_1|e^{j\varphi}$, $w_2 = |w_2|e^{j\phi}$ and $\boldsymbol{b}^\dagger\boldsymbol{c} = |\boldsymbol{b}^\dagger\boldsymbol{c}|e^{j\theta}$. Substitution into (24a) leads to the following quadratic equation with indeterminate $|w_2|$

$$\|\boldsymbol{c}\|^2|w_2|^2 + \big(2|w_1||\boldsymbol{b}^\dagger\boldsymbol{c}|\cos\omega\big)|w_2| + \big(|w_1|^2\|\boldsymbol{b}\|^2 - 1\big) = 0$$

where $\omega = \phi + \theta - \varphi$. The above equation has real solutions if and only if $\Delta \geq 0$, where

$$\begin{aligned}\Delta &= 4|w_1|^2|\boldsymbol{b}^\dagger\boldsymbol{c}|^2\cos\omega^2 - 4\|\boldsymbol{c}\|^2\big(|w_1|^2\|\boldsymbol{b}\|^2 - 1\big)\\ &= 4|w_1|^2|\boldsymbol{b}^\dagger\boldsymbol{c}|^2\big(\tilde{p}_2 - \sin^2\omega\big)\end{aligned} \tag{25}$$

and $\tilde{p}_2 = p_2/|w_1|^2|\boldsymbol{b}^\dagger\boldsymbol{c}|^2$. By hypothesis, (24) has a nonempty feasibility set, and hence we necessarily have $\Delta \geq 0$, where equality holds if and only if $\tilde{p}_2 = \sin^2\omega$. The root(s) of the quadratic equation are given by

$$|w_2| = |w_1|\frac{|\boldsymbol{b}^\dagger\boldsymbol{c}|}{\|\boldsymbol{c}\|^2}\,g_i(\omega), \quad i = 0, 1 \tag{26}$$

where $g_i(\omega) = -\cos\omega + (-1)^i\sqrt{\tilde{p}_2 - \sin^2\omega}$ must satisfy $g_i(\omega) \geq 0$. Therefore, in order to minimize $|w_2|$, we have to minimize the value of g_i. If $\Delta = 0$, then $g_i(\omega) = -\cos\omega$ and therefore the optimal ω^o minimizing g_i is clearly its root $g_i(\omega^o) = 0$, which is equal to $\omega^o = \pm\pi/2 \Leftrightarrow \varphi = \phi + \theta \mp \pi/2$. This, combined with $\Delta = 0$ yields $\tilde{p}_2 = 1$. On the other hand, for $\Delta > 0$, we have $g_i(\omega) = 0$ if and only if $(-1)^i\cos\omega \geq 0$ and $\tilde{p}_2 = 1$. In both of the above cases, from (24a) and (24b) we get $|w_2| = 0$ and $|w_1| = 1/\|\boldsymbol{b}\|$, which are special cases of (11), and may be obtained by substituting $p_2 = |w_1|^2|\boldsymbol{b}^\dagger\boldsymbol{c}|^2$ or $p_2 = \|\boldsymbol{c}\|^2\cos^2\theta$ due to (24b).

In the sequel, we confine ourselves to $\Delta > 0$ and $\tilde{p}_2 \neq 1$; this implies that both g_i and $|w_2|$ are positive. The first- and second-order derivatives of g_i are given by

$$\frac{dg_i(\omega)}{d\omega} = \frac{g_i(\omega)\sin\omega}{g_i(\omega) + \cos\omega}\,,$$

$$\frac{d^2g_i(\omega)}{d\omega^2} = \frac{\frac{dg_i}{d\omega}(\omega)\sin\omega\cos\omega + g_i(\omega)(1 + g_i(\omega)\cos\omega)}{(g_i(\omega) + \cos\omega)^2}\,.$$

The angle(s) ω^o minimizing g_i necessarily satisfy $dg_i(\omega^o)/d\omega = 0$ or equivalently $\sin\omega^o = 0$ therefore giving $\omega^o \in \{0, \pi\}$ as the candidate values for each root. In this case

$$\frac{d^2 g_i(\omega^o)}{d\omega^2} = g_i(\omega^o)\frac{1 + g_i(\omega^o)\cos\omega^o}{(g_i(\omega^o) + \cos\omega^o)^2} > 0$$
$$\Leftrightarrow 1 + g_i(\omega^o)\cos\omega^o > 0 \Leftrightarrow (-1)^i \cos\omega^o > 0$$

and the ith root in (26) attains its minimal value at $\omega^o = i\pi$, with $g_i(\omega^o) = -(-1)^i(1 - \sqrt{\tilde{p}_2}) = (1 - \sqrt{\tilde{p}_2})e^{j(\omega^o - \pi)}$. As a result of the above, we can write

$$|w_2| = |w_1|\frac{|\boldsymbol{b}^\dagger \boldsymbol{c}|}{\|\boldsymbol{c}\|^2}\left(1 - \sqrt{\tilde{p}_2}\right) \tag{27}$$

according to (26), and incorporate the extra term $e^{j(\omega^o - \pi)}$ in the exponential representation of w_2; this implies that we have the equation $\omega^o = (\phi + (\omega^o - \pi)) + \theta - \varphi$ from which we get $\varphi = \phi + \theta - \pi$ and ϕ is a free variable.

APPENDIX B
PROOF OF THEOREM 2

Let $u = \big((1 - \delta)x + \delta r\big)/l$. Setting the first-order partial derivative of $f(x, \alpha)$ equal to zero, and squaring both sides of the resulting equation, we have that

$$\frac{\partial f(x,\alpha)}{\partial \alpha} = lu + l\big(s_1 - (-1)^\delta 2s_2\alpha\big)\frac{\sqrt{s(\alpha)}}{2} = 0$$
$$\Leftrightarrow 2u\sqrt{s(\alpha)} = (-1)^\delta 2s_2\alpha - s_1$$
$$\Rightarrow \big(s_1^2 + 4u^2 s_0\big) - 4vs_1\alpha + (-1)^\delta 4vs_2\alpha^2 = 0 \tag{28}$$

where $v = u^2 + (-1)^\delta s_2$. Note that if $v \le 0$, which can only happen if $\delta = 1$, the above polynomial either degenerates to a constant term ($v = 0$) or its discriminant is negative ($v < 0$). In these cases, $\partial f/\partial\alpha$ has no root and its sign determines the optimal value α^o; it will be one of the endpoints of the interval A in (7a′). In particular, by taking the second-order derivative of f we get (after some manipulations) the expression

$$\frac{\partial^2 f(x,\alpha)}{\partial\alpha^2} = -\frac{l}{\sqrt{s(\alpha)}}\left(\left(u - \frac{1}{l}\frac{\partial f(x,\alpha)}{\partial\alpha}\right)^2 + (-1)^\delta s_2\right)$$

and therefore the extreme points of $\partial f/\partial\alpha$, for $\delta = 1$, satisfy $\big(u - \frac{1}{l}\frac{\partial f(x,\alpha)}{\partial\alpha}\big)^2 + (-1)^\delta s_2 = 0$. If $v = 0$, the extreme point is such that $\partial f/\partial\alpha = 2ul$, leading to $\mathrm{sgn}(\partial f/\partial\alpha) = \mathrm{sgn}(u)$, with $\mathrm{sgn}(\cdot)$ denoting the signum function. Likewise, if $v < 0$, we have $\partial f/\partial\alpha > 0$ and thus $\alpha^o = a_2$. Let us next assume $v > 0$. Then, the roots of the quadratic polynomial derived from (28) by squaring both sides are

$$\alpha_i = (-1)^\delta \frac{1}{2s_2}\left(s_1 + (-1)^i|u|\sqrt{\frac{\Delta_s}{v}}\right), \quad i = 0, 1$$

where $\Delta_s = s_1^2 - (-1)^\delta 4s_0 s_2$ equals the discriminant of s and hence $\Delta_s > 0$ due to $q_2 \neq r_2$. Substitution of α_i in (28), only one of which is a root of $\partial f/\partial\alpha$, leads to the conclusion that it must be $(-1)^i = \mathrm{sgn}(u)$. Thus, the only root of $\partial f/\partial\alpha$ is

$$\alpha^\star = (-1)^\delta \frac{1}{2s_2}\left(s_1 + u\sqrt{\frac{\Delta_s}{v}}\right). \tag{29}$$

What remains to be shown is that $\alpha^\star$ is indeed the point where f attains its maximum. From the second-order derivative of f we get, using $\partial f(x,\alpha^\star)/\partial\alpha = 0$, that $\partial^2 f(x,\alpha^\star)/\partial\alpha^2 = -lv/\sqrt{s(\alpha^\star)} < 0$. Hence, $\alpha^o = \alpha^\star$ if $\alpha^\star \in A$; otherwise, $\alpha^o = a_1$ (resp. $\alpha^o = a_2$) if $\alpha^\star < a_1$ (resp. $\alpha^\star > a_2$).

APPENDIX C
PROOF OF THEOREM 3

Note that for $\delta = 1$, we get $u = r/l$ and therefore the value of $\alpha^\star$ in (14) is independent of x. We can directly compute the root of $F(x) = f(x, \alpha^o)$ from (12) since it is then a linear function. The same holds if $\delta = 0$ and $\alpha^\star \notin A$, where α^o is set in Theorem 2 to be one of the endpoints of A. Next we assume $\delta = 0$ and $\alpha^\star \in A$; by Theorem 2 and (28) we get

$$\begin{aligned} F(x) &= r - x(1 - \alpha^o) + l\sqrt{s(\alpha^o)} \\ &= r - x\left(1 - \frac{1}{2s_2}\left(s_1 + \frac{x}{l}\sqrt{\frac{\Delta_s}{v}}\right)\right) + \frac{l}{2}\sqrt{\frac{\Delta_s}{v}} \\ &= r - x\left(1 - \frac{s_1}{2s_2}\right) + \frac{l}{2s_2}\sqrt{\Delta_s v} \end{aligned}$$

where $v := v(x) = (x/l)^2 + s_2$. To find the optimal value of the original problem, we have to determine the root of F.

$$F(x) = 0 \Leftrightarrow x\big(2s_2 - s_1\big) - 2rs_2 = l\sqrt{\Delta_s v}$$
$$\Rightarrow \big(x\big(2s_2 - s_1\big) - 2rs_2\big)^2 = \Delta_s\big(x^2 + l^2 s_2\big)$$
$$\Leftrightarrow d(x) = d_0 - d_1 x + d_2 x^2 = 0 \tag{30}$$

where the coefficients of d are given by $d_0 = 4r^2 s_2 - l^2\Delta_s$, $d_1 = 4r(2s_2 - s_1)$ and $d_2 = 4(s_0 - s_1 + s_2) = -4s(1)$. Only one of d's roots, which are given by

$$x_i = \frac{d_1 + (-1)^i\sqrt{d_1^2 - 4d_0 d_2}}{2d_2}, \quad i = 0, 1 \tag{31}$$

is also a root of F. Note that the discriminant of d is equal to $16\Delta_s(r^2 - l^2 s(1))$, which is positive since from the definition of s we find that $s(1) = -r_2(\|\boldsymbol{c}\|^2 + r_2) < 0$ and $\Delta_s > 0$. In particular, from (30), (31) we see that x_i should satisfy

$$x_i\big(2s_2 - s_1\big) - 2rs_2 > 0 \Leftrightarrow \mathrm{sgn}(r)\xi_0 + (-1)^i\xi_1 > 0 \tag{32}$$

where $\xi_0 = |r|\sqrt{\Delta_s}$ and $\xi_1 = (2s_2 - s_1)\sqrt{r^2 - l^2 s(1)}$ in the above relation are both positive. It may be further shown that $\xi_0 < \xi_1$ since for all $\theta \neq 0 \pmod\pi$ we have $\xi_0 < \xi_1 \Leftrightarrow -s(1)\big(4r^2 s_2 + l^2(2s_2 - s_1)^2\big) > 0$. From the above analysis we derive that x_0 is the unique root of F, as otherwise we would get $\mathrm{sgn}(r)\xi_0 > \xi_1$ from (32) for $i = 1$, which does not hold. Finally, the value of the optimal t^o is directly computed from (13a).

ACKNOWLEDGMENT

The authors would like to thank Asst. Prof. G. C. Alexandropoulos (the Department of Informatics and Telecommunications, University of Athens, Greece) for several insightful discussions related to this work.

REFERENCES

[1] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019, doi: 10.1109/COMST.2019.2916180.

[2] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013, doi: 10.1109/msp.2013.2260875.

[3] M. Bloch and J. Barros, *Physical–Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

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

[5] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012, doi: 10.1109/TIFS.2011.2166386.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978, doi: 10.1109/tit.1978.1055892.

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

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1132–1138, doi: 10.1109/allerton.2008.4797687.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2009, pp. 2613–2616, doi: 10.1109/icassp.2009.4960158.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP 15th Workshop Stat. Signal Process.*, Aug. 2009, pp. 417–420, doi: 10.1109/ssp.2009.5278549.

[11] 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, doi: 10.1109/tsp.2009.2038412.

[12] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "User and relay selection with artificial noise to enhance physical layer security," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10906–10920, Nov. 2018, doi: 10.1109/tvt.2018.2870280.

[13] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005, doi: 10.1017/CBO9780511841224.

[14] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180–2193, May 2017, doi: 10.1109/tcomm.2017.2651066.

[15] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019, doi: 10.1109/comst.2018.2878035.

[16] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018, doi: 10.1109/twc.2018.2831217.

[17] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "Cooperation for secure wireless communications with resource-bounded eavesdroppers," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 1379–1384, doi: 10.1109/glocomw.2014.7063626.

[18] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "A cooperative jamming protocol for physical layer security in wireless networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 5803–5807, doi: 10.1109/icassp.2015.7179084.

[19] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009, doi: 10.1109/twc.2009.090323.

[20] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008, doi: 10.1109/tit.2008.928272.

[21] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978, doi: 10.1109/tit.1978.1055917.

[22] 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, doi: 10.1109/tsp.2011.2159598.

[23] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Mar. 2007, pp. 905–910, doi: 10.1109/ciss.2007.4298439.

[24] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015, doi: 10.1109/tsp.2014.2369001.

[25] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009, doi: 10.1561/0100000036.

[26] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized Artificial-Noise-Aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011, doi: 10.1109/tsp.2010.2094610.

[27] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013, doi: 10.1109/tifs.2013.2248730.

[28] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Boston, MA, USA: Springer, 2010, doi: 10.1007/978-1-4419-1385-2.

[29] 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, doi: 10.1109/tifs.2013.2261060.

[30] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019, doi: 10.1109/tifs.2018.2859593.

[31] 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, 3rd Quart., 2014, doi: 10.1109/surv.2014.012314.00178.

[32] T. Rappaport, *Wireless Communications, Principles and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

[33] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470, doi: 10.1109/isit.2007.4557589.

[34] F. J. Solis and R. J.-B. Wets, "Minimization by random search techniques," *Math. Oper. Res.*, vol. 6, no. 1, pp. 19–30, Feb. 1981, doi: 10.1287/moor.6.1.19.

[35] L. Tang, X. Gong, J. Wu, and J. Zhang, "Secure wireless communications via cooperative relaying and jamming," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 849–853, doi: 10.1109/glocomw.2011.6162575.

[36] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[37] X. Zhou, L. Song, and Y. Zhang Eds., *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2014.

[38] Y. Zou, X. Wang, and W. Shen, "Primal relay selection for physical–layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013, doi: 10.1109/JSAC.2013.131011.

KYRIAKOS FYTRAKIS received the B.Sc. degree in physics and the M.Sc. degree in electronics and radioelectrology from the University of Athens, Greece, in 2009 and 2012, respectively, where he is currently pursuing the Ph.D. degree with the Department of Informatics and Telecommunications. His research interests span the areas of signal processing, resource allocation, physical layer security, and mathematical optimization for wireless networks.

NICHOLAS KOLOKOTRONIS (Member, IEEE) received the B.Sc. degree in mathematics from the Aristotle University of Thessaloniki, Greece, in 1995, and the M.Sc. degree (Hons.) in highly efficient algorithms and the Ph.D. degree in cryptography from the National and Kapodistrian University of Athens, in 1998 and 2003, respectively. From 2002 to 2004, he was with the European Dynamics S.A., Greece, as a Security Consultant involved in managing research projects and tenders. Since 2004, he has held visiting positions at the University of Piraeus, the University of Peloponnese, the National and Kapodistrian University of Athens, and the Open University of Cyprus. He has been a member of working groups for the provisioning of professional cyber–security training to large organizations, including the Hellenic Telecommunications and Posts Commission (EETT). He is currently an Associate Professor and the Head of the Cryptography and Security Group, Department of Informatics and Telecommunications, University of Peloponnese. He has published more than 75 articles in international scientific journals, conferences, and books and has participated in more than 20 EU–funded and national research and innovation projects. His research interests span the broad areas of security, cryptography, and coding theory. He has been a TPC Member in numerous international conferences, and a Co-Chair of workshops and conferences in IoT security. He was an Associate Editor of the *EURASIP Journal on Wireless Communications and Networking* from 2009 to 2017 and a Regular Reviewer of a number of prestigious journals, including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS) and the IEEE TRANSACTIONS ON INFORMATION THEORY (TIT).

KONSTANTINOS KATSANOS received the B.Sc. degree in electrical engineering from the Department of Electrical and Computer Engineering, University of Patras, in 2014, and the M.Sc. degree from the Department of Informatics and Telecommunications, University of Athens, Greece, in 2016. He is currently pursuing the Ph.D. degree with the Department of Informatics and Telecommunications. His research interests span the areas of signal processing, physical-layer security and optimization for wireless networks. He has received in 2017 the Hellenic Foundation for Research and Innovation (HFRI) and the General Secretariat for Research and Technology (GSRT) Fellowship.

NICHOLAS KALOUPTSIDIS received the B.Sc. degree (Hons.) in mathematics from the University of Athens, Greece, in 1973, and the M.Sc. and Ph.D. degrees in systems science and mathematics from Washington University in St. Louis, St. Louis, MO, USA, in 1975 and 1976, respectively. He has held visiting positions at Washington University, the University of Utah, Harvard University, and Stanford University. He is currently a Professor with the Department of Informatics and Telecommunications, University of Athens. He is the author of the textbook *Signal Processing Systems: Theory and Design* (Wiley, 1997) and co-editor of the book *Adaptive System Identification and Signal Processing Algorithms* (Prentice-Hall, 1993).