Senigagliesi *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:276
https://doi.org/10.1186/s13638-019-1603-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Resource allocation for secure Gaussian parallel relay channels with finite-length coding and discrete constellations

Linda Senigagliesi[1*†], Marco Baldi[1†] and Stefano Tomasin[2†]

Abstract

We investigate the transmission of a secret message from Alice to Bob in the presence of an eavesdropper (Eve) and many of decode-and-forward relay nodes. Each link comprises a set of parallel channels, modeling for example an orthogonal frequency division multiplexing transmission. We consider the impact of efficient implementations, including discrete constellations and finite-length coding, defining an achievable secrecy rate under a constraint on the equivocation rate at Eve. Then, we propose a power and channel allocation algorithm that maximizes the achievable secrecy rate by resorting to two coupled Gale-Shapley algorithms for stable matching problem. We consider the scenarios of both full and partial channel state information at Alice. In the latter case, we only guarantee an *outage* secrecy rate, i.e., the rate of a message that remains secret with a given probability. Numerical results are provided for Rayleigh fading channels in terms of average outage secrecy rate, showing that practical schemes achieve a performance quite close to that of ideal ones.

Keywords: Channel state information, Decode-and-forward, Physical layer security, Relay channel, Resource allocation

1 Introduction

Adding secrecy features to the physical layer is an active and promising research area [1] that complements traditional computational security approaches. Indeed, a proper coding scheme can prevent an eavesdropper Eve from getting information on a message exchanged between the two legitimate users Alice and Bob [2].

In this paper we expand the results of [3] on resource allocation for confidential communications over the Gaussian parallel relay channels, as that work was limited to an ideal scenario, while we address a more realistic model by including the practical constraints of finite-length coding and discrete constellations. We first derive the achievable secrecy rate of this scheme under the assumption of full channel state information (CSI) by Alice and the relay nodes. Then, in order to consider the impact of discrete constellations and finite-length coding, we define an achievable secrecy rate under a constraint on the equivocation rate at Eve. Using an approximated formula of the achievable secrecy rate, we derive the optimal power allocation for point-to-point confidential transmission. By exploiting the power and rate adaptation algorithm for the parallel relay channels of [3], we obtain a resource allocation algorithm coupling two Gale and Shapley algorithms to allocate resources over the parallel relay channels. We also consider the partial CSI scenario, wherein Alice does not know the gains of her channels to Eve, while knowing their statistics. In this case, we only guarantee an *outage* secrecy rate, i.e., the rate of a message that remains secret with a given probability. We show that the algorithm derived for full CSI can be easily adapted to a partial CSI. Numerical results are provided, showing the merit of the proposed solution.

1.1 Related works

The physical layer security of messages transmitted over parallel channels with the assistance of trusted relays has already been addressed in the literature. Most works consider that relays can either forward the message or generate a noise signal to jam Eve. For links comprising a single channel, early works have addressed the relay

*Correspondence: l.senigagliesi@univpm.it
†Linda Senigagliesi, Marco Baldi, and Stefano Tomasin contributed equally to this work.
[1]Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Via Brecce Bianche 12, 60131 Ancona, Italy
Full list of author information is available at the end of the article

selection problem [4–6], while various combinations of message forwarding and jamming are considered in [7–10] with multiple antenna nodes. In [11], multiple relays either jam or forward noise, i.e., they transmit random codewords from a globally known codebook, that hurts more Eve than Bob.

We focus on links comprising parallel channels. For this scenario, in [12], rate-equivocation regions are derived by considering one relay only and assuming full CSI. In [13], orthogonal frequency division multiplexing (OFDM) is considered with a single relay, and Eve is equipped with multiple antennas under partial CSI: subcarriers, powers, and rates are optimized to maximize the average secrecy outage capacity. In [14], the downlink of a cellular system is considered, where the multi-antenna base station performs both beamforming and jamming against a single multi-antenna eavesdropper, and an outage problem is formulated under partial CSI. The scenario is extended in [15], where multiple relays operate in decode and forward (DF) mode and still an outage approach is considered. In [16], a single relay with parallel channels is considered, which performs cooperative jamming against Eve, under full CSI. When the single relay performs DF, resource optimization has been considered in [17]. More comprehensive results, considering also the direct transmission from Alice to Bob, are obtained in [18]. Resource allocation for transmission over parallel channels assisted by DF relays without secrecy features has also been widely studied. Bit loading [19] and power and rate allocation [20] have been investigated, while the availability of multiple relays transmitting on a single sub-carrier is studied in [21], with efficient greedy algorithms provided in [22]. The resource allocation for parallel channels with secrecy outage constraint has been considered in [23] and [24], without taking into account the conditions imposed by the presence of relay nodes in the system.

Recently, optimal resource allocation for security purposes under different conditions has gained the attention of several authors. In [25], an optimization framework for two-hop communications is proposed, jointly optimizing source and relay powers together, with the goal of maximizing the secrecy outage capacity in a massive multiple input multiple output (MIMO) scenario. In [26], optimal power allocation and pricing strategies are determined using a Stackelberg game model in order to maximize the players' utilities, under both perfect and imperfect CSI assumptions in the presence of multiple eavesdroppers. An optimal power strategy to maximize the achievable secrecy rate in wireless multi-hop DF relay networks with a power constraint is studied in [27], under the assumption of global CSI, and an iterative cooperative beamformer design is also proposed. The work is extended in [28] to the case of full-duplex relays, with cooperative beamforming to null out the signal at multiple eavesdroppers. In [29], a heuristic resource allocation iterative algorithm is presented, based on the proximal theory that maximizes the secure capacity of device-to-device communications in heterogeneous networks. Joint source-relay power optimization in a dual-hop communication using duality theory is performed in [30], with the aim of maximizing the overall secrecy rate, under individual power constraints and using a high signal to noise ratio (SNR) approximation. In [31], a robust resource allocation framework is proposed in the presence of an active eavesdropper, assuming that both the legitimate receiver and the eavesdropper are full-duplex: the receiver sends jamming signals against the eavesdropper, without the need for external helpers and having a partial CSI on the links between the eavesdropper and the legitimate receivers. Other works consider optimal power allocation for security purposes with the help of imperfect hardware analysis [32] and an external jammer [33]. Optimization algorithms for null-space beamforming with full CSI have been proposed in [34], while in [35], the authors propose a joint relay selection and optimal power allocation algorithm to maximize security in a cooperative network, considering the presence of untrusted relays and passive eavesdroppers, possibly colluding. These works do not take into consideration the impact of practical limitations in the system.

The impact of finite-constellation inputs on the achievable secrecy rate is analyzed in [36, 37]. However, the role of finite-length coding is not investigated, and neither parallel relay channels nor optimal power allocation are considered. The effect of finite-alphabet signaling on the secrecy performance achievable over the multiple-input single-output wiretap channel is instead studied in [38], where artificial noise is used to degrade the eavesdropper's performance. Still in [38], a power allocation scheme based on gradient search optimizes the ratio between the power of the information-bearing signal and the power of the artificial noise. In our setting, instead, we do not use artificial noise, i.e., we fix $\phi = 1$, and therefore, the optimization approach of [38] can not be applied to our case.

The rest of the paper is organized as follows. Section 2 outlines the system model for secret message transmission over parallel Gaussian relay channels. The achievable secrecy rates under full CSI are computed in Section 3, where we also compute the outage secrecy rate. In Section 4, an algorithm for resource allocation of a secure point-to-point transmission over parallel channels is obtained, which is used then in Section 5 for the resource allocation in a relay network. Numerical results of the proposed solution are presented in Section 6, before some conclusions are drawn in Section 7.

Notation: Vectors and matrices are written in bold letters. We denote the base-2 and natural-basis logarithm

by log and ln, respectively. We indicate the positive part of a real quantity x as $[x]^+ = \max\{x; 0\}$. $\mathbb{E}[X]$ denotes the expectation of the random variable X, $\mathbb{P}[\cdot]$ is the probability operator, and ^{T} denotes the matrix transpose operator. The entropy is denoted as $\mathbb{H}(\cdot)$, while the mutual information is denoted as $\mathbb{I}(\cdot;\cdot)$.

2 Methods and contribution

Next, we describe the setting we consider and the main contributions we provide.

2.1 System model

We consider a communication system to transmit a confidential message $\mathcal{M}$ from Alice to Bob through N trusted cooperating relays. Any link between a pair of devices is constituted by a set of K parallel additive white Gaussian noise (AWGN) channels. Eve is an eavesdropping device that overhears communications originated from both Alice and the relays. We assume that relay nodes decode and forward (DF) the messages they receive. This implies that each transmitting node in the system uses the same code and the same constellation to send a message. No direct link between Alice and Bob is available, and all devices operate in half-duplex mode. Therefore, the message transmission comprises two phases:

1) Alice transmits to the relays, and
2) The relays transmit to Bob.

We also assume that in phase 2 at most one relay transmits on channel k and that the two phases have the same duration.

The setting we consider is depicted in Fig. 1, where the link from Alice to relay n is represented by the K-size column vector $cH_n = [H_{n,1}, \ldots, H_{n,K}]^T$ containing the gains for each channel. The power of the signal received by relay n on channel k is therefore $H_{n,k}P_{n,k}$. Similarly, the vector $\bar{\boldsymbol{H}}_n$ denotes the power gains of the link between relay n and Bob, and $\bar{H}_{n,k}\bar{P}_{n,k}$ is the power of the signal received by Bob from relay n on channel k. Concerning Eve's channel, $\boldsymbol{G}$ is the vector of power gains of the signal coming from Alice, while $\bar{\boldsymbol{G}}_n$ is the power gain vector of the signal coming from relay n.

Let us denote with $\mathcal{X}_{n,k}$ and $\bar{\mathcal{X}}_{n,k}$ the signals transmitted by Alice and by relay n on channel k in the first and second phase, respectively. Similarly, $\mathcal{Y}_{n,k}$ and $\bar{\mathcal{Y}}_{n,k}$ denote the signals received by relay n and Bob on channel k in the first and second phase, respectively. Finally, $\mathcal{Z}_{n,k}$ and $\bar{\mathcal{Z}}_{n,k}$ denote the signals received by Eve from Alice and from relay n on channel k in the first and second phase, respectively.

We can therefore write the signal received by the n-th relay on channel k and the signal received by Bob respectively as

$$\mathcal{Y}_{n,k} = \boldsymbol{H}_n \mathcal{X}_{n,k} + w_n, \tag{1a}$$

$$\bar{\mathcal{Y}}_{n,k} = \bar{\boldsymbol{H}}_n \bar{\mathcal{X}}_{n,k} + \bar{w}_n. \tag{1b}$$

On Eve's side, we can write

$$\mathcal{Z}_{n,k} = \boldsymbol{G}_n \mathcal{X}_{n,k} + w_n, \tag{2a}$$

$$\bar{\mathcal{Z}}_{n,k} = \bar{\boldsymbol{G}}_n \bar{\mathcal{X}}_{n,k} + \bar{w}_n, \tag{2b}$$

where w_n and $\bar{w}_n$ represent the noise vectors in phase 1 and phase 2, which are assumed to be independent identically distributed (iid), with zero mean and unitary variance $\left(\sigma_n^2 = 1\right)$ for all channels.

Figure 1 also shows in brackets the power flow of the considered scenario. We indicate with $P_{n,k}$ the transmit power of Alice on channel k to relay n in phase 1, while $\bar{P}_{n,k}$ is the transmit power of relay n on channel k in phase

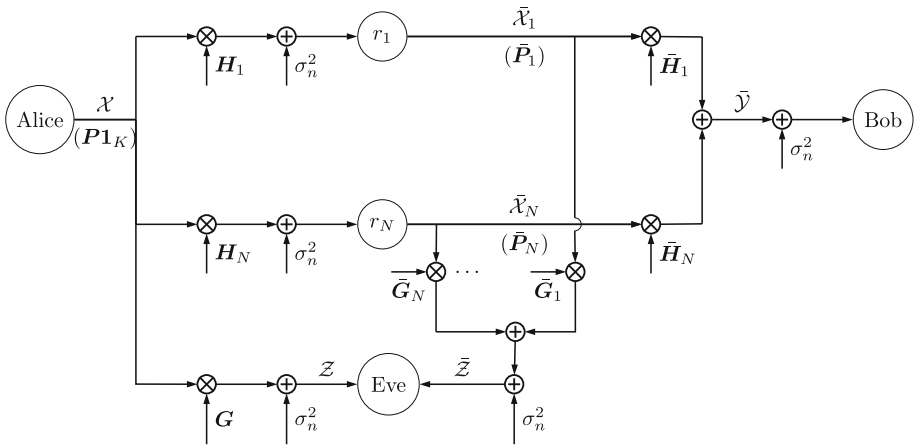

Fig. 1 System model of the relay parallel channels with N relays, $r_1, \ldots r_N$. Mixers $\otimes$ and adders $\uplus$ represent element-wise multiplication and addition of vectors, respectively.

2. The $N \times K$ matrix $\boldsymbol{P}$ ($\bar{\boldsymbol{P}}$) collects all transmit powers, having $P_{n,k}$ ($\bar{P}_{n,k}$) at entry n,k. In Fig. 1, $\boldsymbol{P}\mathbf{1}_K$ denotes the N-size column vector of transmit powers for each relay, with $\mathbf{1}_K$ being the K-size column vector of all ones. We consider power constraints for both Alice and the relays, i.e.,

$$\sum_{k=1}^{K} P_{n,k} \leq P_{\text{tot},1}, \quad n = 1, \ldots, N. \tag{3a}$$

$$\sum_{k=1}^{K} \bar{P}_{n,k} \leq P_{\text{tot},2}, \quad n = 1, \ldots, N. \tag{3b}$$

The power constraint per relay in phase (1) simplifies the power allocation in this phase and still provides an upper bound on the total transmit power from the source that cannot exceed $NP_{\text{tot},1}$.

Being the noise iid, the SNR at relay n for a transmission from Alice on channel k is $H_{n,k}P_{n,k}$, and similarly for a transmission from relay n on channel k, the SNR at Bob in phase 2 is $\bar{H}_{n,k}\bar{P}_{n,k}$.

2.2 Contribution

With respect to the previously described state of the art, the main contributions of this paper can be summarized as follows:

- To the best of our knowledge, there are no existing works on power allocation with a secrecy rate target under practical conditions, such as the use of finite-length codes and discrete constellations. Motivated by this, we provide a formulation of the secrecy rate under practical constraints and compare it with the achievable rate in ideal conditions. We consider both perfect and partial CSI under outage constraints.
- By proposing an approximated expression for the secrecy rate under practical conditions, we optimize the link-level parallel channel power allocation, generalizing the solution obtained for the ideal transmission scenario.
- Extending [3], we maximize the secrecy rate by resorting to an iterative algorithm based on the Gale and Shapley theory for the stable matching problem.
- Extending [24], we derive the optimal power allocation for the case of relayed transmission.
- Through numerical examples, we show that it is possible to achieve an acceptable secrecy rate, even using short codes and constellations with a small alphabet.

3 Achievable secrecy rate

We consider a per-channel encoding, i.e., Alice splits $\mathcal{M}$ into K messages $\mathcal{M}_k$, $k = 1, \ldots, K$, each of which is separately encoded and transmitted on a channel. In [24], an in-depth analysis of this coding strategy is provided, showing that it performs similarly to the scheme with joint coding across channels, while being simpler to design. Therefore, each relay in general receives only a subset of bits of the entire message. In the second phase, again, each relay splits the received secret bits into groups, which are separately encoded and transmitted on a different channel, among those assigned to the relay.

In both phases, secrecy is achieved through classical wiretap coding [1], based on adding random bits to the secret message and encoding the resulting block with capacity-achieving codes. The *weak* secrecy rate of a point-to-point transmission is the rate of a message $\mathcal{M}$ that [1]: (i) is correctly decoded by Bob and (ii) has a rate of mutual information with the signal received by Eve $\mathcal{Z}$ that is vanishing for infinite codewords, i.e.,

$$\lim_{l \to \infty} \frac{1}{l} \mathbb{I}(\mathcal{Z}; \mathcal{M}) = 0, \tag{4}$$

where l is the message length in bits. Due to the per-channel encoding, the achievable weak secrecy rate is the sum of the achievable secrecy rates on each used channel. Let $R_{n,k}$ be the secrecy rate on channel k, intended for relay n in phase 1, and $\bar{R}_{n,k}$ the secrecy rate on channel k transmitted by relay n in phase 2. Assuming that the added random bits at each transmission are independent, we immediately conclude that the achievable secrecy rate between Alice and Bob is the minimum between the secrecy rates in both phases, i.e.,

$$R_{\text{tot}}\left(\boldsymbol{P}, \bar{\boldsymbol{P}}\right) = \frac{1}{2} \sum_{n=1}^{N} \min \left\{ \sum_{k=1}^{K} R_{n,k}(P_{n,k}), \sum_{k=1}^{K} \bar{R}_{n,k}(P_{n,k}) \right\}, \tag{5}$$

where the factor $1/2$ is due to the two phases of the same duration, and we have highlighted the dependence of the achievable rates on the transmit powers. The minimum reflects the fact that either of the two phases can be a bottleneck for transmission, and the sum over the subcarriers k takes into account the fact that we decode and re-encode the data signal at the relays; thus, each relay demodulates all received signals and splits power and data among the subcarriers in its own way upon transmission in phase 2.

Since we assume that Alice is transmitting to a single relay per channel, we also have

$$R_{n^*,k}(P_{n^*,k}) > 0 \rightarrow R_{n,k}(P_{n,k}) = 0, \; n \neq n^*, \tag{6}$$

and since we assume that at most one relay is transmitting in any channel in phase 2, we also have

$$\bar{R}_{n^*,k}\left(\bar{P}_{n^*,k}\right) > 0 \rightarrow \bar{R}_{n,k}\left(\bar{P}_{n,k}\right) = 0, \; n \neq n^*. \tag{7}$$

In the following, we derive the achievable secrecy rates, when full CSI is available at Alice, taking into consideration infinite- and finite-length coding and continuous and

discrete modulation formats. Then with discuss the ϵ-outage achievable secrecy rate when Alice has only a partial CSI, i.e., she knows only the statistics of her channels to Eve.

3.1 Infinite-length coding with Gaussian signaling

When infinite-length coding and Gaussian signaling are used, perfect secrecy, i.e., no information leakage to Eve, can be achieved [1]. In this case, the achievable secrecy rate can be written as

$$R_{n,k}(P_{n,k}) = C(P_{n,k}H_{n,k}) - C(P_{n,k}G_{n,k}), \tag{8}$$

where $C(x) = \log(1+x)$. Similar expressions are obtained for $\bar{R}_{n,k}(\bar{P}_{n,k})$ where $P_{n,k}$, $H_{n,k}$, and $G_{n,k}$ are replaced by $\bar{P}_{n,k}$, $\bar{H}_{n,k}$, and $\bar{G}_{n,k}$, respectively.

3.2 Finite-length coding with Gaussian signaling

A first limitation to the achievable secrecy rates introduced by practical systems is related to the use of codes working on finite-length blocks of symbols. In such a setting, weak secrecy can not be guaranteed and Eve can get some information on the secret message[1]. Moreover, the decodability condition at Bob can not be guaranteed, and we must consider a non-zero codeword error rate (CER) κ.

Let $R_{n,k}$ and $\bar{R}_{n,k}$ be the message rates, for which we have a level of secrecy θ. In particular, in order to measure the information leakage to Eve, we resort to the equivocation rate, i.e., Eve's uncertainty about the message after observing the transmitted codeword (through her channel). For relay n transmitting on channel k and using codewords of m symbols, the equivocation rate per symbol is

$$\rho_{n,k}(P_{n,k}) = \frac{1}{2m}\mathbb{H}(\mathcal{M}_k|\mathcal{Z}_{n,k}), \tag{9}$$

$$\bar{\rho}_{n,k}\left(\bar{P}_{n,k}\right) = \frac{1}{2m}\mathbb{H}\left(\mathcal{M}_k|\bar{\mathcal{Z}}_{n,k}\right), \tag{10}$$

where the factor 2 comes from the fact that we have two phases of the same duration. We have that

$$0 \le \rho_{n,k}(P_{n,k}) \le R_{n,k}(P_{n,k}), \tag{11}$$

$$0 \le \bar{\rho}_{n,k}\left(\bar{P}_{n,k}\right) \le \bar{R}_{n,k}\left(\bar{P}_{n,k}\right), \tag{12}$$

where the upper bound is achieved with infinitely long codewords ($m \to \infty$). We consider that transmission is secure if

$$\frac{\rho_{n,k}(P_{n,k})}{R_{n,k}(P_{n,k})} \ge \theta, \quad \frac{\bar{\rho}_{n,k}\left(\bar{P}_{n,k}\right)}{\bar{R}_{n,k}\left(\bar{P}_{n,k}\right)} \ge \theta, \tag{13}$$

where $\theta \in (0,1]$ is a suitably defined parameter that limits the gap with respect to weak secrecy conditions with infinite-length coding. Let us indicate with $\hat{\mathcal{M}}_n$ the decoded version of message $\mathcal{M}_n$. The *achievable secrecy rates* for finite-length coding are therefore the maximum rates satisfying condition (13), i.e.,

$$R_{n,k}(P_{n,k}) = \max_r r \tag{14a}$$

s.t.

$$\frac{\rho_{n,k}(P_{n,k}, r)}{r} \ge \theta, \tag{14b}$$

$$\mathbb{P}\left[\mathcal{M}_n \ne \hat{\mathcal{M}}_n\right] \le \kappa, \tag{14c}$$

where (14b) comes directly from (13) and (14c) imposes a constraint on the decoding failure rate. A similar problem can be written for phase 2, for a given allocated power $\bar{P}_{n,k}$, i.e.,

$$\bar{R}_{n,k}\left(\bar{P}_{n,k}\right) = \max_r r \tag{15a}$$

s.t.

$$\frac{\bar{\rho}_{n,k}\left(\bar{P}_{n,k}, r\right)}{r} \ge \theta, \tag{15b}$$

$$\mathbb{P}\left[\mathcal{M}_n \ne \hat{\mathcal{M}}_n\right] \le \kappa. \tag{15c}$$

For the computation of the equivocation rate, we can resort to a lower bound. By the definition of entropy and mutual information, we have that Eve's equivocation rate can be rewritten as

$$\begin{aligned}\rho_{n,k}(P_{n,k}) = \frac{1}{m}\big[&\mathbb{H}(\mathcal{X}_{n,k}) - \mathbb{I}(\mathcal{X}_{n,k};\mathcal{Z}_{n,k}) + \\ &+\mathbb{H}(\mathcal{M}_n|\mathcal{Z}_{n,k},\mathcal{X}_{n,k}) - \mathbb{H}(\mathcal{X}_{n,k}|\mathcal{M}_n,\mathcal{Z}_{n,k})\big],\end{aligned} \tag{16}$$

where $\mathcal{X}_{n,k}$ and $\mathcal{Z}_{n,k}$ are the signals received by Bob and Eve in phase 1, respectively.

By the definition of spectral efficiency as upper bound to the mutual information, we have that

$$\mathbb{I}(\mathcal{X}_{n,k};\mathcal{Z}_{n,k}) < mC(P_{n,k}G_{n,k}), \tag{17}$$

and

$$\mathbb{H}(\mathcal{M}_n|\mathcal{Z}_{n,k},\mathcal{X}_{n,k}) \le \mathbb{H}(\mathcal{M}_n|\mathcal{X}_{n,k}) = 0. \tag{18}$$

On the other hand, the entropy of $\mathcal{X}_{n,k}$ is the code rate, which in turn determines the (non-null) CER at relay n, due to the use of finite-length coding. A bound on the code rate as a function of the CER for finite-length coding is provided by [39], that in this scenario can be written as

$$\begin{aligned}\mathbb{H}(\mathcal{X}_{n,k}) =& m\gamma(P_{n,k}H_{n,k}) = \\ =& m\left[C(P_{n,k}H_{n,k}) - \frac{\log e}{\sqrt{2m}}Q^{-1}(\kappa)\right]^+,\end{aligned} \tag{19}$$

where κ is the target CER at relay n and $[x]^+ = x$ for $x \ge 0$ and 0 otherwise, and $Q(\cdot)$ is the complementary cumulative distribution function of the standard Gaussian variable.

[1] Indeed, the definition of weak secrecy (4) entails a limit to infinity of the message length that can not be used in finite-codewords schemes.

Let $\eta(R_{n,k}, P_{n,k}G_{n,k})$ be the CER experienced by a fictitious receiver at the wiretapper position trying to decode for $\mathcal{X}_{n,k}$ from observing $\mathcal{Z}_{n,k}$ and $\mathcal{M}$. By the Fano inequality, we have

$$\begin{aligned}&\mathbb{H}(\mathcal{X}_{n,k}|\mathcal{M}_n, \mathcal{Z}_{n,k}) \leq \\ &1 + m\left(\gamma(P_{n,k}H_{n,k}) - R_{n,k}\right)\eta(R_{n,k}, P_{n,k}G_{n,k})\,.\end{aligned} \tag{20}$$

Hence, from (16) and (20), we have the following lower bound on $\rho_{n,k}(P_{n,k})$:

$$\begin{aligned}\rho_{n,k}(P_{n,k}) \geq \sigma_{n,k}(P_{n,k}) &= \gamma(P_{n,k}H_{n,k}) - C(P_{n,k}G_{n,k}) \\ &- \left(\gamma(P_{n,k}H_{n,k}) - R_{n,k}\right)\eta(R_{n,k}, P_{n,k}G_{n,k}) - \frac{1}{m}\,.\end{aligned} \tag{21}$$

We pessimistically assume that Eve can exploit the channel to the maximum of its capacity, i.e., she can decode the received message without errors.

The above analysis can be simplified by considering that, for adherence to practical systems, deterministic coding instead of random coding can be used. In such a case, each l-bit block of data is univocally mapped into a codeword $\mathcal{C}_{n,k}$. This is opposed to either random or coset coding, which are often invoked in the literature for this kind of systems, but yield further issues (e.g., concerning the generation of randomness). In the case of deterministic coding, we no longer need to estimate the CER for the fictitious receiver, and we can write a simpler lower bound on the equivocation rate, that is

$$\rho_{n,k}(P_{n,k}) = \frac{1}{m}\left[\mathbb{H}(\mathcal{C}_{n,k}) - \mathbb{I}(\mathcal{C}_{n,k}; \mathcal{Z}_{n,k})\right]\,. \tag{22}$$

Resorting again to (17) and (19), we obtain the following approximation on Eve's equivocation rate

$$\begin{aligned}\rho_{n,k}(P_{n,k}) \simeq \xi_{n,k}(P_{n,k}) &\triangleq \\ &\left[C(H_{n,k}P_{n,k}) - \frac{\log e}{\sqrt{2m}}Q^{-1}(\kappa) - C(G_{n,k}P_{n,k})\right]^+\,,\end{aligned} \tag{23}$$

which does not depend on $R_{n,k}$.

By replacing $\rho_{n,k}(P_{n,k})$ with its approximated lower bound $\xi_{n,k}(P_{n,k})$ (and similarly for phase-2 equivocation rates) in problems (14) and (15) and removing the (already used) constraint on the error probability $\mathbb{P}[\mathcal{M}_n \neq \hat{\mathcal{M}}_n]$, we obtain the approximated achievable rates in the two phases; the solution can be easily obtained in a closed form as

$$R_{n,k}(P_{n,k}) = \frac{1}{\theta}\left[C(H_{n,k}P_{n,k}) - + \frac{\log e}{\sqrt{2m}}Q^{-1}(\kappa) - C(G_{n,k}P_{n,k})\right]^+ \tag{24}$$

Note that the obtained secrecy rate with finite-length coding is smaller than that obtained with infinite-length coding. In particular, $\frac{\log e}{\sqrt{2m}}Q^{-1}(\kappa)$ represents the secrecy rate loss due to finite-length coding, which decreases as either the code length m or the CER κ increase. Note that the choice of m is mostly dictated by implementation constraints as well as desired latency limitations, while κ is associated to the reliability of the transmission. In Fig. 2, we compare the results obtained for $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for codes of different length, choosing $H_{n,k}/G_{n,k}$ of 20 dB and $\theta = 1$.

We consider a fitting of $R_{n,k}(P_{n,k})$ solution of (14) by the linear combination of logarithms of the powers, in order to ease resource allocation, i.e.,

$$\begin{aligned}&R_{n,k}(P_{n,k}) \simeq \alpha_1 + \alpha_2\log(1+\alpha_3 H_{n,k}P_{n,k}) - \\ &\alpha_4\log(1+\alpha_5 H_{n,k}P_{n,k}) - \\ &-\left[\alpha_6\log(1+\alpha_7 G_{n,k}P_{n,k}) - \right. \\ &\left.-\alpha_8\log(1+\alpha_9 P_{n,k}G_{n,k})\right]\,.\end{aligned} \tag{25}$$

Note that (25) directly models the achievable secrecy rate rather than the equivocation rate, and the parameters α_i are chosen at solution of problem (14). By this formulation, the secrecy rates with ideal conditions can be seen as a sub-case of (25) with $\alpha_i = 1$ for $i = 2, 3, 6, 7$, and $\alpha_i = 0$ otherwise. The motivation behind the choice of this fitting will be better understood when using it in the resource optimization problem focus of this paper: indeed, it will turn out (see Section 4) that with this choice the optimization problem boils down to finding the roots of suitable polynomials.

Figure 3 shows $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for values of $H_{n,k}/G_{n,k}$ between 2 and 20 dB with a step of 1 dB, and results obtained by the fitting function (25) with $\kappa = 10^{-3}$, $m = 4096$, and $\theta = 0.9$. We observe a good agreement of the fitting function with $R_{n,k}(P_{n,k})$, especially at low rates, and high values of $G_{n,k}P_{n,k}$, with a slight overestimation of the rate for intermediate values of $G_{n,k}P_{n,k}$ for high $H_{n,k}/G_{n,k}$ ratios.

3.3 Infinite-length coding with discrete constellations

A second limitation of practical systems is the use of suboptimal constellations with discrete points taken from a finite alphabet. In this case, perfect secrecy can still be achieved, but we must consider the constellation-constrained spectral efficiency [40] $\hat{C}(\cdot)$ instead of $C(\cdot)$, i.e., (8) becomes

$$R_{n,k}(P_{n,k}) = \hat{C}(P_{n,k}H_{n,k}) - \hat{C}(P_{n,k}G_{n,k})\,. \tag{26}$$

In order to obtain simple resource allocation algorithms, we consider again (25) as a fitting of $R_{n,k}(P_{n,k})$. Figure 4 shows the secrecy rate as a function of the SNR for a 16-QAM constellation, and its comparison with the exact function. We observe a good agreement between the approximated and the exact curves, with slightly higher discrepancy for high values of $G_{n,k}P_{n,k}$. However, note that in a power optimization process, these high power values will not be used, since they provide a lower secrecy rate than lower power values. We still have a slight mismatch

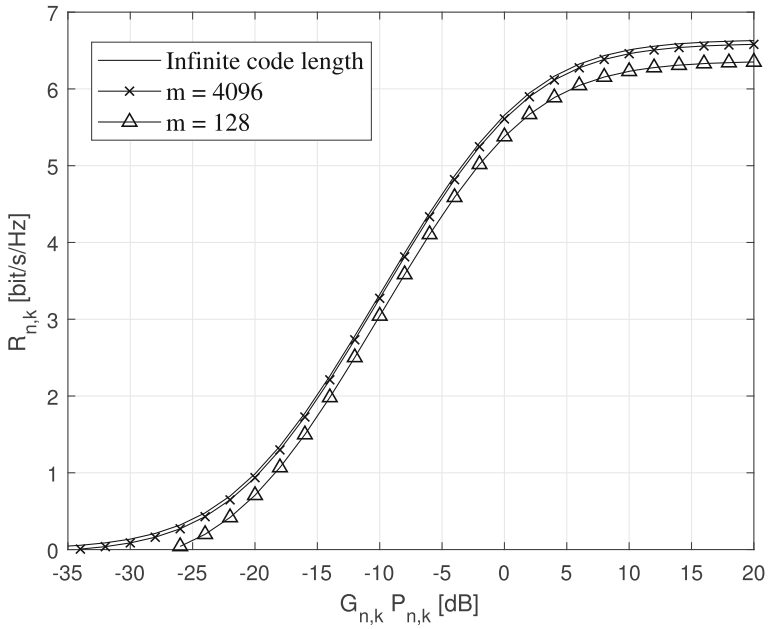

Fig. 2 $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for $H_{n,k}/G_{n,k}$ equals to 20 dB, for infinite-length codes and codes of length 4096 and 128, and $\theta = 1$

between the fitting and the analysis in correspondence of the maximum rate, which is however not so relevant (especially for increasing values of $H_{n,k}/G_{n,k}$).

3.4 Finite-length coding with discrete constellations

Let us consider the limitations introduced in Sections 3.2 and 3.3 jointly, i.e., both finite-length coding and discrete constellations, which describe a practical scenario. Also in this case, we resort to the equivocation rate for the definition of the achievable secrecy rate (see problems (14) and (15)), by replacing the spectral efficiency $C(P)$ with the constellation-constrained spectral efficiency $\hat{C}(P)$ in (23). On the other hand, since the approximation provided by [39] is valid for any input distribution, (19) still holds true.

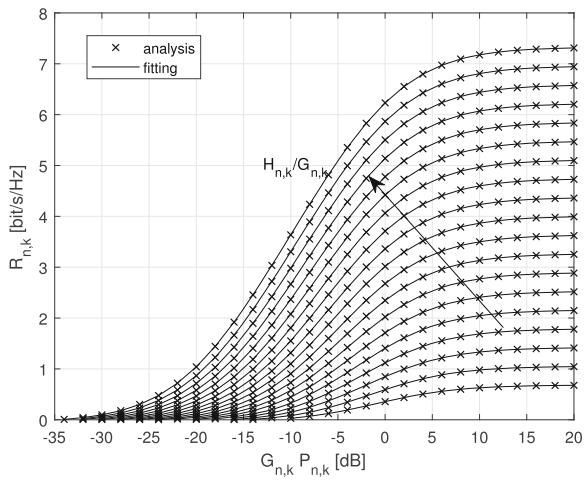

Fig. 3 $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for values of $H_{n,k}/G_{n,k}$ between 2 and 20 dB with a step of 1 dB, and results obtained with the fitting function (25), for codes of length 4096 and $\theta = 0.9$

As already done in the previous section, we propose to fit $R_{n,k}(P_{n,k})$ by the function (25). Figure 5 shows $R_{n,k}(P_{n,k})$ for values of $H_{n,k}/G_{n,k}$ between 2 and 20 dB with a step of 1 dB, and results obtained by the fitting function (25) with $\kappa = 10^{-3}$, 16-QAM constellation, and $m = 4096$. In this case, we observe a good agreement between the approximated and the exact curves for low values of $G_{n,k}P_{n,k}$, while the curves show a small difference at high values. As observed for the case of infinite-length coding, also in this case, the high power values will not be used in the optimization.

3.5 ϵ-Outage achievable secrecy rate

In many practical scenarios, Alice and the relays have only a partial CSI of their channels to Eve. This is mainly due to the fact that Eve may not have an advantage in revealing its channels, e.g., by transmitting, unless this could be useful to increase the rate of other messages exchanged between her and the legitimate nodes. Indeed, in the absence of full CSI, there is a non-zero probability (outage probability) that for any power allocation and choice of the secret message rate, Eve may get some information on $\mathcal{M}$.

In particular, we focus on the secrecy outage probability in each transmission phase and for each channel. Let $\pi_{n,k}$ and $\bar{\pi}_{n,k}$ be the secrecy outage probabilities on channel k with respect to relay n in the first and the second phase, when messages are transmitted at rates $R_{n,k}(P_{n,k})$ and $\bar{R}_{n,k}(\bar{P}_{n,k})$, respectively. We consider as design criterion

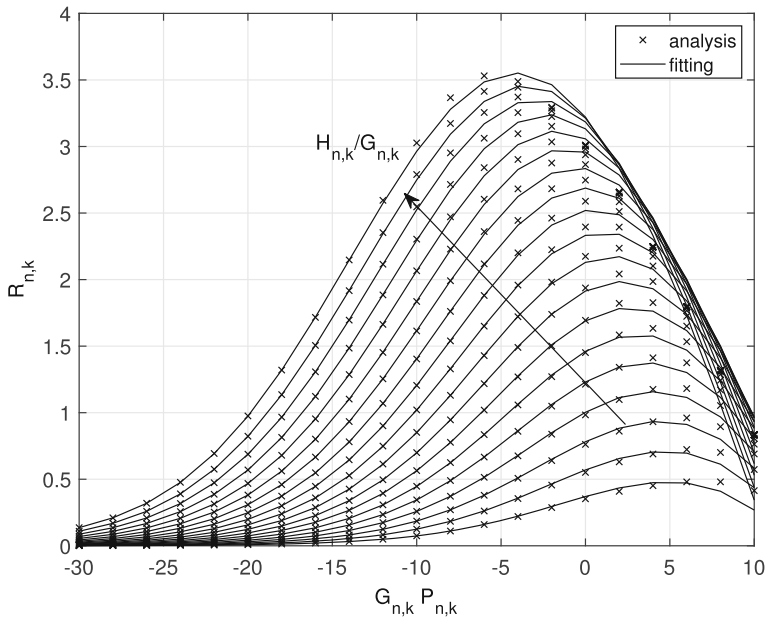

Fig. 4 $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for values of $H_{n,k}/G_{n,k}$ between 2 and 20 dB with a step of 1 dB, and results obtained with the fitting function (25), considering a 16-QAM constellation

the limitation of the secrecy outage probability on each channel, i.e.,

$$\pi_{n,k} \leq \epsilon\,, \quad \bar{\pi}_{n,k} \leq \epsilon\,, \tag{27}$$

where ϵ is the target secrecy outage probability.

In the following, we assume that the legitimate nodes know the statistics of both $G_{n,k}$ and $\bar{G}_{n,k}$, thus having a partial CSI. If $R_{n,k}(P_{n,k})$ is the achievable secrecy rate for Alice-Eve channel realization $G^*_{n,k}$, then the secrecy outage probability can be written as

$$\pi_{n,k} = \mathbb{P}\left[G_{n,k} > G^*_{n,k}\right]. \tag{28}$$

Similar expressions are obtained for the second phase. From (27), we define F_ϵ as the *outage gain*, i.e., the channel gain for which

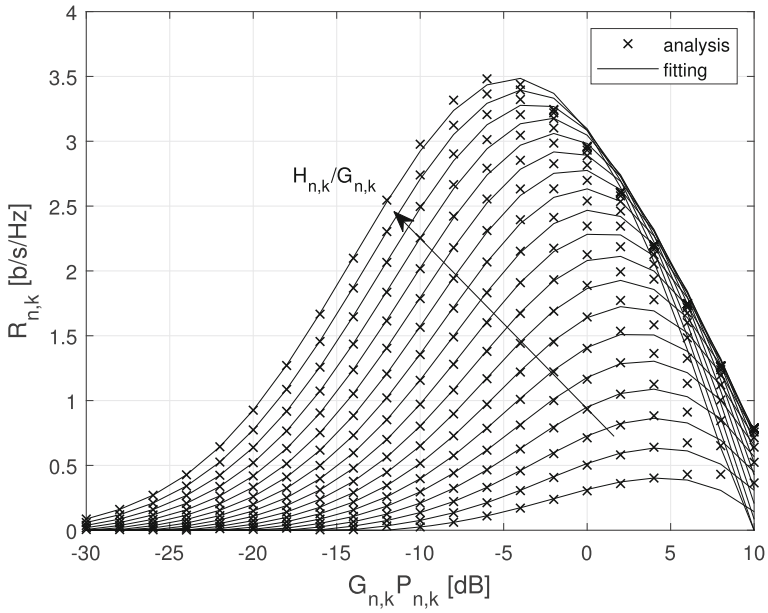

Fig. 5 $R_{n,k}(P_{n,k})$ as a function of $G_{n,k}P_{n,k}$ for values of $H_{n,k}/G_{n,k}$ between 2 and 20 dB with a step of 1 dB, and results obtained with the fitting function (25), considering a 16-QAM constellation and $m = 4096$

$$\pi_{n,k} = \mathbb{P}\left[G_{n,k} > F_\epsilon\right] = \epsilon. \tag{29}$$

Then, the ϵ-outage achievable secrecy rate can be obtained from the previous sections by considering $G_{n,k} = \bar{G}_{n,k} = F_\epsilon$.

Note that this approach works with any kind of fading (e.g., Rayleigh Rician, Nakagami fading). For example, for Rayleigh fading

$$\mathbb{P}\left[G_{n,k} \le F_\epsilon\right] = \exp\left[-F_\epsilon / \left(d_{\mathrm{E}}^{-\zeta}\right)\right], \tag{30}$$

where ζ is the path-loss exponent, therefore

$$F_\epsilon = -d_{\mathrm{E}}^{-\zeta} \ln \epsilon\,. \tag{31}$$

For Nakagami fading, $G_{n,k}$ is gamma distributed, i.e., $\mathbb{P}\left[G_{n,k} \le F_\epsilon\right] = \frac{1}{\Gamma(\sigma)}\gamma(\sigma, \kappa F_\epsilon)$, where σ is the shape parameter, κ is the rate parameter, and $\Gamma(\cdot)$ and $\gamma(\cdot)$ are the Gamma and lower-incomplete Gamma functions, respectively. Therefore, we have

$$F_\epsilon = \frac{1}{\kappa}\gamma^{-1}(\sigma, \Gamma(\sigma)\epsilon)\,, \tag{32}$$

where $\gamma^{-1}(\sigma, x)$ represents the inverse lower-incomplete Gamma function.

4 Single link power optimization

We first consider the single-link power optimization, where we allocate powers that maximize the secrecy sum rate between two nodes, using parallel channels. This problem must be solved in both transmission phases, and here, we focus on the first phase, i.e., the optimization of the communication from Alice to a specific relay n, assuming that all power $P_{\mathrm{tot},1}$ can be used on that link. In this situation, we have $P_{n',k} = 0$ for $n' \neq n$, $n = 1, \ldots, N$, $k = 1, \ldots, K$, and we must solve

$$R_{\max} = \max_{\{P_{n,k}\}} \sum_{k=1}^{K} R_{n,k}(P_{n,k})\,, \quad \text{s.t. (3)}. \tag{33}$$

The four cases of previous section are considered, i.e., (a) infinite-length coding with Gaussian constellation, (b) finite-length coding with Gaussian constellation, (c) infinite-length coding with discrete constellations, and (d) finite-length coding with discrete constellations. Moreover, we consider here the case of ϵ-outage rates discussed in Section 3.5, thus considering gain F_ϵ for all channels to Eve.

4.1 Infinite-length coding with Gaussian signaling

For infinite-length coding with Gaussian signaling, the optimization problem (33) has been proven to be convex and solved in [41, Th. 1]. In particular, we immediately see that all channels for which $H_{n,k} < F_\epsilon$ must be switched off ($P_{n,k} = 0$), since they do not provide any secrecy rate. Let the set of used channels be

$$\mathcal{F} = \{k : H_{n,k} > F_\epsilon\}\,. \tag{34}$$

Then, we have

$$\begin{aligned} P_{n,k} &= \left[-\frac{\lambda(H_{n,k}+F_\epsilon)}{2\lambda F_\epsilon H_{n,k}} + \right. \\ &\quad \left. \frac{\sqrt{[\,\lambda(H_{n,k}+F_\epsilon)]^2 - 4\lambda F_\epsilon H_{n,k}(\lambda - H_{n,k} + F_\epsilon)}}{2\lambda F_\epsilon H_{n,k}}\right]^+ \\ &= \left[-\frac{H_{n,k}+F_\epsilon}{2F_\epsilon H_k} + \right. \\ &\quad \left. \frac{\sqrt{(H_{n,k}+F_\epsilon)^2 - 4FH_{n,k}(1-(H_k-F_\epsilon)/\lambda)}}{2F_\epsilon H_k}\right]^+ \\ &= \left[-\frac{H_{n,k}+F_\epsilon}{2F_\epsilon H_k} + \right. \\ &\quad \left. \frac{\sqrt{(H_{n,k}-F_\epsilon)^2 + 4FH_{n,k}(H_{n,k}-F_\epsilon)/\lambda)}}{2F_\epsilon H_{n,k}}\right]^+, \end{aligned} \tag{35}$$

where $\lambda \ge 0$ is the Lagrange multiplier to be optimized in order to satisfy the power constraint, which can be computed by a dichotomic search to find the unique optimal solution.

4.2 Finite-length coding with Gaussian signaling

For finite-length coding with Gaussian signaling, we exploit the fitting (25) and the optimization problem (33) becomes

$$\begin{aligned} R_{\max} = \max_{\{P_{n,k}\}} & \sum_{k=1}^{K} \alpha_1 + \alpha_2 \log(1+\alpha_3 H_{n,k} P_{n,k}) \\ & - \alpha_4 \log(1+\alpha_5 H_{n,k} P_{n,k}) - \alpha_6 \log(1+\alpha_7 F_\epsilon P_{n,k}) \\ & + \alpha_8 \log(1+\alpha_9 F_\epsilon P_{n,k})\,, \end{aligned} \tag{36a}$$

$$\text{subject to (3)}. \tag{36b}$$

We observe that (36) is a maximization problem of continuously differentiable objective functions with inequality constraints of continuously differentiable functions, thus satisfying the necessary conditions for the application of the Lagrange multipliers method, which provides the constrained maxima as one or more solutions of

$$\begin{aligned} & \frac{\alpha_2\alpha_3 H_{n,k}}{1+\alpha_3 H_{n,k} P_{n,k}} + \frac{\alpha_4\alpha_5 H_{n,k}}{1+\alpha_5 H_{n,k} P_{n,k}} + \\ & + \frac{\alpha_6\alpha_7 F_\epsilon}{1+\alpha_7 F_\epsilon P_{n,k}} + \frac{\alpha_8\alpha_9 F_\epsilon}{1+\alpha_9 F_\epsilon P_{n,k}} - \lambda = 0\,, \end{aligned} \tag{37}$$

where $\lambda \ge 0$ is the Lagrange multiplier to be chosen in order to satisfy the power constraint.

By using the common denominator of the four fractions in (37), by simple algebraic steps, we separate the terms of different order and we define

$$A_{n,k} = \lambda \ln(2)\alpha_3\alpha_5\alpha_7\alpha_9 H_{n,k}^2 F_\epsilon^2, \tag{38a}$$

$$\begin{aligned} B_{n,k} = {} & \alpha_3\alpha_5\alpha_6\alpha_7\alpha_9 H_{n,k}^2 F_\epsilon^2 - \alpha_3\alpha_5\alpha_7\alpha_8\alpha_9 H_{n,k}^2 F_\epsilon^2 \\ & - \alpha_2\alpha_3\alpha_5\alpha_7\alpha_9 H_{n,k}^2 F_\epsilon^2 + \alpha_3\alpha_4\alpha_5\alpha_7\alpha_9 H_{n,k}^2 F_\epsilon^2 \\ & + \lambda \ln(2)\alpha_5\alpha_7\alpha_9 H_{n,k} F_\epsilon^2 + \lambda \ln(2)\alpha_3\alpha_7\alpha_9 H_{n,k} F_\epsilon^2 \\ & + \lambda \ln(2)\alpha_3\alpha_5\alpha_9 H_{n,k}^2 F_\epsilon + \lambda \ln(2)\alpha_3\alpha_5\alpha_7 H_{n,k}^2 F_\epsilon, \end{aligned} \tag{38b}$$

$$\begin{aligned} C_{n,k} = {} & \lambda \ln(2)\alpha_3\alpha_5 H_{n,k}^2 - \alpha_2\alpha_3\alpha_5\alpha_9 H_{n,k}^2 F_\epsilon \\ & + \lambda \ln(2)\alpha_7\alpha_9 F_\epsilon^2 + \lambda \ln(2)\alpha_5\alpha_7 H_{n,k} F_\epsilon \\ & - \alpha_2\alpha_3\alpha_5\alpha_7 H_{n,k}^2 F_\epsilon + \alpha_4\alpha_5\alpha_7\alpha_9 H_{n,k} F_\epsilon^2 \\ & + \alpha_3\alpha_4\alpha_5\alpha_9 H_{n,k}^2 F_\epsilon + \lambda \ln(2)\alpha_3\alpha_9 H_{n,k} F_\epsilon \\ & + \lambda \ln(2)\alpha_3\alpha_7 H_{n,k} F_\epsilon + \alpha_3\alpha_6\alpha_7\alpha_9 H_{n,k} F_\epsilon^2 \\ & + \alpha_3\alpha_5\alpha_6\alpha_7 H_{n,k}^2 F_\epsilon - \alpha_5\alpha_7\alpha_8\alpha_9 H_{n,k} F_\epsilon^2 \\ & - \alpha_3\alpha_7\alpha_8\alpha_9 H_{n,k} F_\epsilon^2 - \alpha_3\alpha_5\alpha_8\alpha_9 H_{n,k}^2 F_\epsilon \\ & + \lambda \ln(2)\alpha_5\alpha_9 H_{n,k} F_\epsilon - \alpha_2\alpha_3\alpha_7\alpha_9 H_{n,k} F_\epsilon^2 \\ & + \alpha_3\alpha_4\alpha_5\alpha_7 H_{n,k}^2 F_\epsilon + \alpha_5\alpha_6\alpha_7\alpha_9 H_{n,k} F_\epsilon^2, \end{aligned} \tag{38c}$$

$$\begin{aligned} D_{n,k} = {} & \alpha_4\alpha_5\alpha_7 H_{n,k} F_\epsilon - \alpha_2\alpha_3\alpha_9 H_{n,k} F_\epsilon \\ & - \alpha_5\alpha_8\alpha_9 H_{n,k} F_\epsilon - \alpha_3\alpha_8\alpha_9 H_{n,k} F_\epsilon \\ & + \alpha_5\alpha_6\alpha_7 H_{n,k} F_\epsilon - \alpha_2\alpha_3\alpha_7 H_{n,k} F_\epsilon \\ & + \alpha_4\alpha_5\alpha_9 H_{n,k} F_\epsilon - \alpha_2\alpha_3\alpha_5 H_{n,k}^2 \\ & + \alpha_3\alpha_6\alpha_7 H_{n,k} F_\epsilon + \alpha_6\alpha_7\alpha_9 F_\epsilon^2 \\ & - \alpha_7\alpha_8\alpha_9 F_\epsilon^2 + \lambda \ln(2)\alpha_9 F_\epsilon + \lambda \ln(2)\alpha_7 F_\epsilon \\ & + \lambda \ln(2)\alpha_5 H_{n,k} \\ & + \alpha_3\alpha_4\alpha_5 H_{n,k}^2 + \lambda \ln(2)\alpha_3 H_{n,k}, \end{aligned} \tag{38d}$$

$$\begin{aligned} E_{n,k} = {} & \lambda \ln(2) - \alpha_2\alpha_3 H_{n,k} - \alpha_8\alpha_9 F_\epsilon \\ & + \alpha_6\alpha_7 F_\epsilon + \alpha_4\alpha_5 H_{n,k}. \end{aligned} \tag{38e}$$

Then, the Lagrangian (37) becomes

$$\begin{aligned} & A_{n,k} P_{n,k}^4 + B_{n,k} P_{n,k}^3 + C_{n,k} P_{n,k}^2 \\ & \quad + D_{n,k} P_{n,k} + E_{n,k} = 0\,. \end{aligned} \tag{39}$$

For a given $\lambda \geq 0$, for all real positive roots of the polynomial, we compute (26) and select the root yielding the highest secrecy rate. When no real roots are found, it means that the secrecy rate is strictly decreasing for $P_{n,k} > 0$; thus, $P_{n,k} = 0$ and a null secrecy rate is achieved.

We can now appreciate the value of the fitting (25), which provides the simple polynomial (39), whose roots can be obtained using well-established algorithms. Note that the algorithm must include a dichotomic search over $\lambda \geq 0$ in order to satisfy the power constraints. Again, note that the solution to problem (36) is a generalization of the solution (35) for ideal transmission conditions.

4.3 Discrete constellations

For infinite-length coding with discrete constellations, the optimization problem (33) using the fitting (25) becomes (36); hence, by applying also in this case the Lagrange multiplier method, we obtain again (39).

For finite-length coding with discrete constellations, the optimization problem (33) using the fitting (25) becomes (36) and the Lagrange multiplier methods lead to (39).

5 Maximum rate power allocation

We now consider the power allocation problem at Alice and Bob with the aim of maximizing the secrecy rate, i.e.,

$$R_{\max} = \max_{\boldsymbol{P},\bar{\boldsymbol{P}}} R_{\text{tot}}(\boldsymbol{P}, \bar{\boldsymbol{P}})\,, \tag{40a}$$

$$\text{subject to power constraints (3)}, \tag{40b}$$

$$\text{and rate constraints (6) and (7)}. \tag{40c}$$

As observed in [3], this is a mixed-integer programming problem, and for its solution, we resort to the iterative approach of [3], based on the game-theoretic Gale and Shapley algorithm for the stable matching problem [42]. In the following, we report the algorithm developed in [3] with its detailed description.

The stable matching problem aims at matching dames to cavaliers, preventing any dame and any cavalier belonging to two different couples both preferring to be matched. In our scenario, dames and cavaliers are channels and relay, respectively, and the preference of matching is the achievable secrecy rate when using the channel for that relay. We have actually two coupled stable matching problems for the two phases. We use an iterative algorithm, where at each iteration, one step of the Gale and Shapley algorithm is performed for both problems.

We start computing the overall rates obtained by assigning all channels to each relay in phase 2 (finding the best power allocation for both phases and the best channel assignment in phase 1), and then, we exclude the relay-channel couple in phase 2 that provides the lowest rate. At the second iteration, we compute the overall rates obtained by assigning all channels (except the couple excluded in the first iteration) to each relay in phase 2 (again optimizing powers and phase-1 channel allocation), before excluding another relay-channel couple in phase 2 that provides the lowest rate. The process is iterated excluding a couple at each iteration until for each channel we have at most one associated relay in phase 2. Within each iteration, the channel allocation for phase 1 is obtained by applying the Gale and Shapley algorithm to the matching of channels and relays in phase 1 (for a given allocation in phase 2).

Algorithm 1 shows the general solution of the algorithm that iteratively computes the rates offered by relays to Bob

for each channel, and Bob discards the proposal providing the lowest rate for all channels where at least two proposals have been received. The process is iterated until Bob receives at most one proposal of non-zero rate for each channel. The outputs of the algorithm are the allocated power matrices $\boldsymbol{P}$ and $\bar{\boldsymbol{P}}$, having as (n,k) entry $P_{n,k}$ and $\bar{P}_{n,k}$, respectively. Matrices $\boldsymbol{R}$ and $\bar{\boldsymbol{R}}$ collect the rates in the two phases and are defined analogously. The set $\bar{\mathcal{Q}}_k$, $k=1,\ldots,$ is iteratively updated and at each iteration collects the indices of relays that are not allowed to transmit on channel k in phase 2. Set $\bar{\mathcal{S}}_n = \{k : n \notin \bar{\mathcal{Q}}_k\}$ instead collects all channels available for transmission to relay n in phase 2.

Algorithm 1: General Resource Allocation Algorithm

output: $\boldsymbol{P}, \bar{\boldsymbol{P}}$
1.1 Set $\bar{\mathcal{Q}}_k = \emptyset$;
1.2 **while** $(\exists k : |\bar{\mathcal{Q}}_k| < N-1)$ **do**
1.3 $(\boldsymbol{P}, \bar{\boldsymbol{P}}, \bar{\boldsymbol{R}})$ = `Rate_Offer_Phase_2` $(\{\bar{\mathcal{Q}}_k\})$;
1.4 Find relay channel indices (n', k') from (41);
1.5 $\bar{\mathcal{Q}}_{k'} = \bar{\mathcal{Q}}_{k'} \cup \{n'\}$
1.6 **end**
1.7 **return**

Initially, all these sets are empty as all relays are potentially free to transmit on any channel in phase 2. Note that the constraint of having at most one relay transmitting in each channel is not taken into account initially. However, at each iteration, a competing relay for one channel is prevented from transmitting and the process stops exactly when there is at most one relay transmitting on each channel. At each iteration, the routine `Rate_Offer_Phase_2` is run, which provides the power allocation that maximizes the total rate under the power constraints and the channel availability in phase 2 (i.e., sets $\bar{\mathcal{Q}}_k$). Then, we remove the relay that provides the minimum rate on one channel, i.e., we select the relay/channel index

$$(n', k') = \text{argmin}_{(n,k):|\bar{\mathcal{Q}}_k|<(N-1) \text{ and } n\notin\bar{\mathcal{Q}}_k} \bar{R}_{n,k} \tag{41}$$

and insert its index in $\bar{\mathcal{Q}}_k$.

The `Rate_Offer_Phase_2` algorithm (shown in Algorithm 2) computes the rate offers for phase 2, given channel availability $\bar{\mathcal{S}}_n$ for each relay $n=1,\ldots,N$. In formulas, this is problem (40a)-(40b) subject to the additional constraint

$$\sum_{k=1}^{K} R_{n,k}(P_{n,k}) = \sum_{k\in\bar{\mathcal{S}}_n} \bar{R}_{n,k}(\bar{P}_{n,k}), \quad n=1,\ldots,N. \tag{42}$$

In Algorithm 2 $\bar{\boldsymbol{R}}_{n,\cdot}$ ($\bar{\boldsymbol{P}}_{n,\cdot}$) denotes the nth row of $\bar{\boldsymbol{R}}$ ($\bar{\boldsymbol{P}}_{n,\cdot}$). Matrix $\bar{\boldsymbol{H}}_{n,\bar{\mathcal{S}}_n}$ collects the columns of matrix $\bar{\boldsymbol{H}}$ with indices in $\bar{\mathcal{S}}_n$.

Algorithm 2: `Rate_Offer_Phase_2`

Input : $\{\bar{\mathcal{Q}}_k\}$
Output: $\boldsymbol{P}, \bar{\boldsymbol{P}}, \bar{\boldsymbol{R}}$
Data: $\epsilon, \bar{\boldsymbol{H}}$
2.1 $\mathcal{S}_n = \{k : n \notin \bar{\mathcal{Q}}_k\}$
2.2 **for** $n=1$ **to** N **do**
2.3 $(\bar{\boldsymbol{P}}_{n,\cdot}, \bar{\boldsymbol{R}}_{n,\cdot})$ = `MACalPowRate` $(\bar{\boldsymbol{H}}_{\bar{\mathcal{S}}_n,n}, P_{tot}, \infty)$;
2.4 **end**
2.5 $(\boldsymbol{P}, \boldsymbol{R})$ = `Rate_Offer_Phase_1` $(\bar{\boldsymbol{R}})$;
2.6 **for** $n=1$ **to** N **do**
2.7 $(\bar{\boldsymbol{P}}_{n,\cdot}, \bar{\boldsymbol{R}}_{n,\cdot})$ = `MACalPowRate` $(\bar{\boldsymbol{H}}_{\bar{\mathcal{S}}_n,n}, P_{tot}, \sum_{k=1}^{K} R_{n,k})$;
2.8 **end**
2.9 **return**

The solution is achieved by computing the rates achieved in phase 2 through function `MACalPowRate`, which takes into account channel availability. Let $\bar{R}(\bar{P}_{n,k})$ be obtained solution. Then, we compute the maximum rates achievable in phase 1 under the rate matching constraint (40c), by invoking the function `Rate_Offer_Phase_1`. Lastly, we consider the rates obtained in phase 1 as a constraint to re-compute the optimal power allocation in phase 2, under the channel availability constraint. This is achieved by calling `MACalPowRate` for each relay, with the additional constraint that the rate in phase 2 can not exceed that in phase 1, i.e., $\sum_{k=1}^{K} R_{n,k}$.

The `MACalPowRate` algorithm is reported in Algorithm 3, where $\boldsymbol{h}$ denotes the channel matrix (possibly being a sub-matrix of $\boldsymbol{H}$ or $\bar{\boldsymbol{H}}$). The `MACalPowRate` algorithm aims at maximizing the total secret rate over channel set $\mathcal{S}_n$, in point to point transmission, under (a) a power constraint and (b) a total rate constraint. Note that the point to point solution of Section 4 is indicated by function `MACAllocation` and that the algorithm performs a dichotomic search between zero allocated power and P_{tot} in order to find the intermediate power constraint that yields a rate satisfying the rate constraint. Further details on the algorithm can be found in [23].

The `Rate_Offer_Phase_1` algorithm reported in Algorithm 4 aims providing the offers for rates in phase 1, given the maximum rates that can be supported in phase 2, $\bar{\boldsymbol{R}}$. Solution is achieved by applying again the Gale Shapley approach, where now at each iteration relays offer rates for phase 1 and Alice discards the worst proposal. In particular, the rate proposal to relay n in phase 1 is obtained by power allocation that maximizes the

Algorithm 3: `MACalPowRate`

Input : $\boldsymbol{h}$, P_{tot}, $\rho_{\max}$
Output: $\boldsymbol{\pi}$, $\boldsymbol{\rho}$
Data: ϵ

$w_{\min} = 0$, $w_{\max} = 1$, $w = 1$.
$(\boldsymbol{\pi}, \boldsymbol{\rho})$ = `MACAllocation` $(\boldsymbol{h}, P_{tot})$;
if $\sum_k \rho_k > \rho_{\max}$ **then**
  while $|\sum_k \rho_k - \rho_{\max}| > \epsilon$ **do**
    if $\sum_k \rho_k > \rho_{\max}$ **then**
      $w_{\max} = w$
    else
      $w_{\min} = w$
    end
    $w = (w_{\max} + w_{\min})/2$;
    $(\boldsymbol{\pi}, \boldsymbol{\rho})$ = `MACAllocation` $(\boldsymbol{h}, wP_{tot})$;
  end
end
return

secrecy rate to relay n, assuming that all power is available to transmit to relay n. This is achieved by calling N times `MACAllocation`, one time for each Alice-relay link, obtaining power allocations $P^*_{n,k}$. Among all proposals to all relay, we select the worst one, corresponding to the channel-relay couple $(n', k') = \text{argmin}_{(n,k)} R_{n,k}\left(P^*_{n,k}\right)$, and we discard it, by preventing relay n' from allocating power on channel k'. The process is iterated by updating the power allocation for user n'. In order to take into account the power constraint of phase 1 that operates across the relays, the maximum power available to relay n' is reduced, since channel k' is used by another relay. As we do not know which relay at the end will use the channel, the total power available for user n' is reduced by the minimum among all power allocations, i.e., $P_{\text{tot}} - \min_{n \neq n'} P_{n,k^*}$. The process is iterated until for each channel Alice transmits at most one relay. At a generic iteration, let $\mathcal{Q}_k$ be the set of relays to which Alice transmits on channel k, and $\mathcal{S}_n$ the set of channels that can be used for relay n. Then, the discarded proposal is that of relay/channel couple

$$(n', k') = \min_{k, n \in \mathcal{Q}_k} R_{n,k}(P^*_{n,k}), \tag{43}$$

and the maximum power to be used for transmission to relay n is

$$P_n^{(\text{tot})} = P_{\text{tot}} - \sum_{k \neq \mathcal{S}_n} \min_{n \in \mathcal{Q}_k} P_{n,k}. \tag{44}$$

Algorithm 4: `Rate_Offer_Phase_1`

input : $\bar{\boldsymbol{R}}$
output: $\boldsymbol{P}$, $\boldsymbol{R}$

Set $\mathcal{Q}_k = \emptyset$, $\mathcal{S}_n = \{1, \ldots, K\}$, $P_n^{(\text{tot})} = P_{\text{tot}}$;
while $(\exists k : |\mathcal{Q}_k| < N - 1)$ **do**
  for $n = 1$ **to** N **do**
    $(\boldsymbol{P}_{\cdot,n}, \boldsymbol{R}_{\cdot,n})$ = `MACalPowRate` $(\boldsymbol{H}_{\mathcal{S}_n,n}, P_n^{(tot)}, \sum_{k=1}^{K} \bar{R}_{n,k})$;
  end
  Compute (n', k^*) using (43);
  $\mathcal{Q}_{k^*} = \mathcal{Q}_k \cup \{n^*\}$;
  $\mathcal{S}_n = \{k : n \notin \mathcal{Q}_k\}$;
  for $n = 1$ **to** N **do**
    Compute $P_n^{(\text{tot})}$ from (44);
  end
end
return

5.1 Complexity

The complexity $\mathcal{C}$ of Algorithm 1 can be measured as a function of the number of relays N as follows

$$\mathcal{C} = \mathcal{O}\left\{2N^2\mathcal{I}_5\left(1 + \mathcal{I}_3\right) + N^3\left[\mathcal{C}_5(1 + \mathcal{I}_3) + 1\right]\right\}, \tag{45}$$

where $\mathcal{I}_3$ and $\mathcal{I}_5$ represent the number of iterations performed within the `while` cycle of the Algorithms `MACalPowRate` and `MACAllocation`, respectively. Therefore, we can say that the proposed resource allocation algorithm asymptotic complexity corresponds to $\mathcal{O}(N^3)$. In order to evaluate the impact of $\mathcal{I}_3$ and $\mathcal{I}_5$ in terms of average and maximum value, in Fig. 6, we report their cumulative density function (c.d.f.) for different values of N. Note that both $\mathcal{I}_3$ and $\mathcal{I}_5$ do not depend on N, and they do not depend either on the configuration setting, i.e., on choice of code and modulation. $\mathcal{I}_3$ and $\mathcal{I}_5$ show an average value of about 4 and 13.5 iterations, respectively, independently of N.

6 Results and discussion

Let us consider the scenario reported in Fig. 7, where the relay nodes are positioned along a line that is orthogonal to the segment between Alice to Bob, intersecting it at a distance d_{I} and d_{II} from Alice and Bob, respectively. Moreover, relays are equispaced with a distance Δ between any two adjacent relays. We further assume that the eavesdropper is at least at a distance d_{E} from any transmitting node, i.e., it is outside of the dashed circles surrounding Alice and the relays.

The $K = 16$ channels between any couple of nodes are assumed independent Rayleigh fading. We also consider $P_{\text{tot},1} = P_{\text{tot},2} = 1$. The average SNR at unitary distance is of 0 dB, and the path loss coefficient is 3.5; thus, the average SNR at distance d is $d^{-3.5}$. About the eavesdropper, since it is assumed to be at a minimum distance d_{E} from any transmitting node, the outage gain is obtained from (29). For finite-length coding, we assume a CER at Bob $\kappa = 10^{-3}$, and $m = 128$ or 4096.

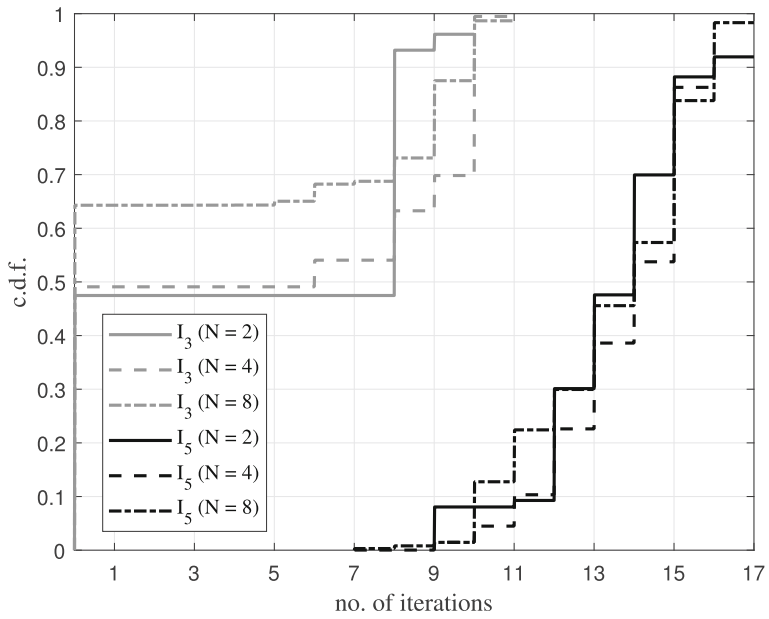

Fig. 6 Cumulative density function (c.d.f.) of $\mathcal{I}_3$ and $\mathcal{I}_5$

6.1 Impact of eve's distance

We first consider a scenario wherein each relay has the same distance from Alice and Bob, i.e., $d_{\mathrm{I}} = d_{\mathrm{II}} = 0.8$, the separation between relays is $\Delta = 0.05$, and the number of relays is $N = 2$, 4, or 8.

Figures 8 and 9 show the average maximum outage secrecy rate $\mathbb{E}[R_{\max}]$, averaged over channel realizations, as a function of d_{E}, for a target secrecy outage probability $\epsilon = 10^{-4}$, and comparing different coding and constellations settings. We first investigate the impact of discrete constellations with respect to Gaussian signaling, and Fig. 8 shows the average maximum outage secrecy rate obtained when using infinite-length coding with both the aforementioned signalling schemes. We observe that the use of 16-QAM does not yield any significant performance loss with respect to Gaussian signaling, since the maximum rate of 16 channels with 16-QAM is 256 b/s/Hz, which is well above the average secrecy rate of 25 b/s/Hz achievable in the considered setting with ideal Gaussian signaling. Therefore, constellations with small alphabet already provide close-to-optimal performance. Moreover, by increasing the number of relays, the average maximum outage secrecy rate increases, as a diversity gain is available on the links among legitimate nodes. Figure 9 shows results for finite-length coding and both Gaussian signaling and discrete constellations. As regards the Gaussian signaling, comparing Figs. 8 and 9, we note a negligible performance degradation for a codeword length $m = 4096$ with respect to infinite-length coding, since $Q^{-1}(\kappa) = 3.1$, and from (23), the loss is of the order of $K \cdot 10^{-3} \approx 10^{-2}$. About Fig. 9, we observe that finite-length coding further increases the gap with respect to Gaussian signaling: this is due to the fact that proper matching in the two phases of relaying must be found to achieve an end-to-end secrecy rate and adding constraints further limits this performance, in a non-linear fashion. Lastly, as $d_{\mathrm{E}} \to \infty$, we note that the rate curves flatten in correspondence of the insecure rate of the relay parallel channels, as in this case, security conditions are always met and the performance is limited only by the legitimate channel conditions.

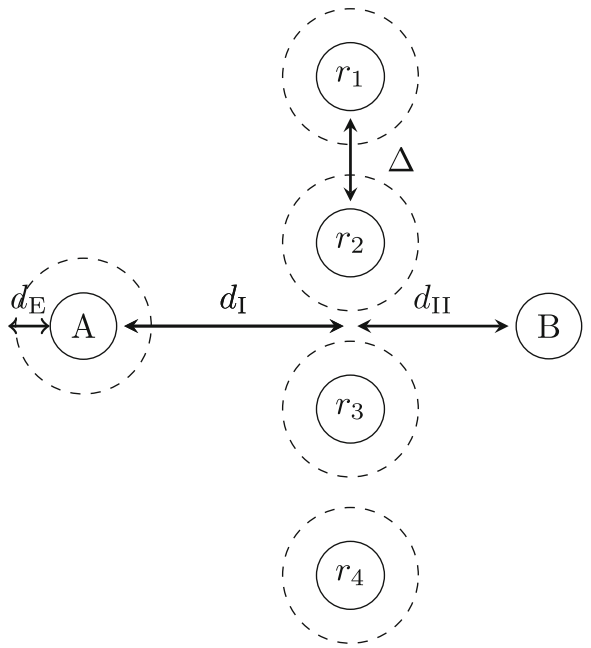

Fig. 7 Node position diagram. (A) Alice, (B) Bob, r_n: relay n

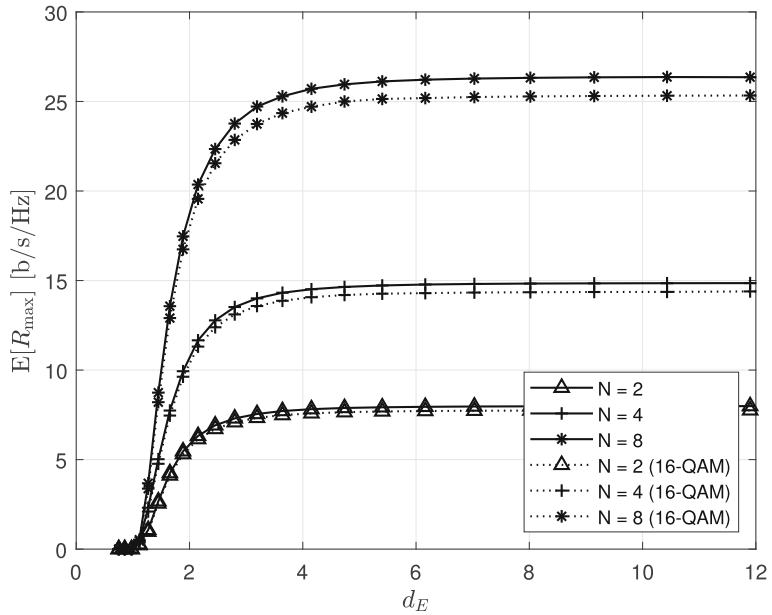

Fig. 8 Average maximum secrecy rate as a function of d_{E} with infinite-length coding, both Gaussian signaling and discrete (16-QAM) constellations and various values of *N*

6.2 Impact of codeword length

In Fig. 10, the impact of the codeword length for finite-length coding with Gaussian signaling is investigated. Note that the performance of codes with long codewords ($m = 4096$) is comparable to that of infinite-length coding. Considering a 16-QAM, differences between infinite-length coding and 4096-length coding are negligible as the average maximum outage secrecy rates coincide for all numbers of relay nodes. Similar results are obtained with discrete constellations, not reported here for the sake of conciseness, where, as seen before, the impact of finite-length coding is stronger than for the Gaussian signaling.

6.3 Impact of relative node distances

We now study the impact of the relative distances among legitimate nodes. In particular, we fix the Alice-Bob distance to $d_{\mathrm{I}} + d_{\mathrm{II}} = 2$, and we let both the ratio between

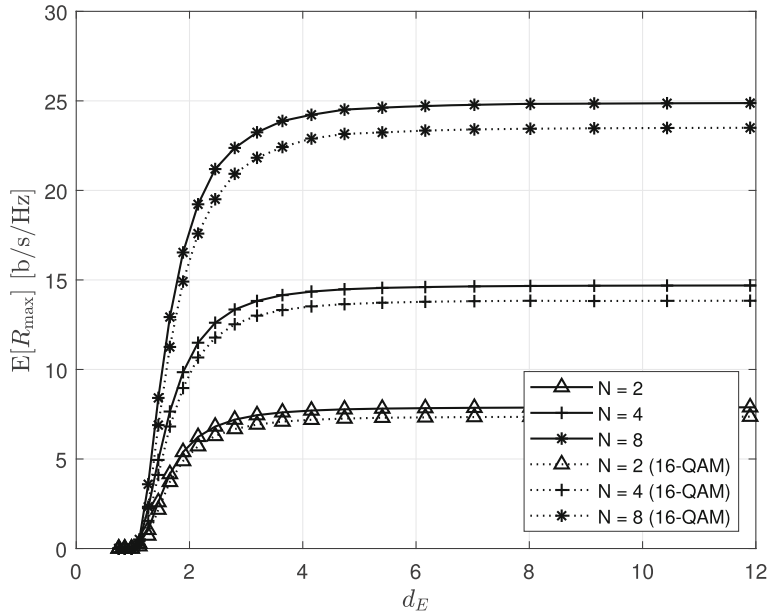

Fig. 9 Average maximum outage secrecy rate as a function of d_{E} with finite-length coding ($m = 4096$), both Gaussian and discrete (16-QAM) constellations, and various values of *N*

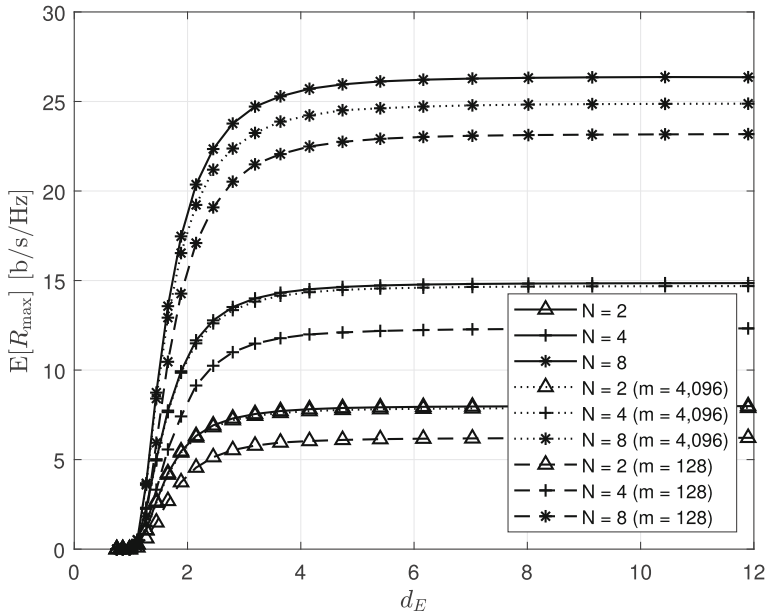

Fig. 10 Average maximum outage secrecy rate as a function of d_{E} with Gaussian constellation, both infinite- and finite-length ($m = 128$ and $m = 4096$) coding, and various values of N

the two distances ($d_{\mathrm{I}}/d_{\mathrm{II}}$) and the distance among the relays vary, i.e., $\Delta = \{0.05, 0.1, 0.5\}$, for $d_{\mathrm{E}} = 10$, $\epsilon = 10^{-4}$, and $N = 4$ relays.

Figure 11 shows the average maximum outage secrecy rate as a function of $d_{\mathrm{I}}/d_{\mathrm{II}}$, and finite-length coding ($m = 4096$) with Gaussian signaling. We observe that for decreasing values of Δ, the curves tend asymptotically to a maximum average secrecy rate of 2 b/s/Hz. On the other hand, as $d_{\mathrm{I}}/d_{\mathrm{II}}$ tends to infinity, the average maximum outage secrecy rate tends to zero, as the Alice-relay links will provide vanishing data rates. When the distance Δ tends to zero, all the relay nodes are squeezed in the same point between Alice and Bob, which represents the optimal relaying configuration.

6.4 Comparison with other solutions

Figures 12 and 13 provide a comparison between our resource allocation (denoted as Gale-Shapley, or GS)

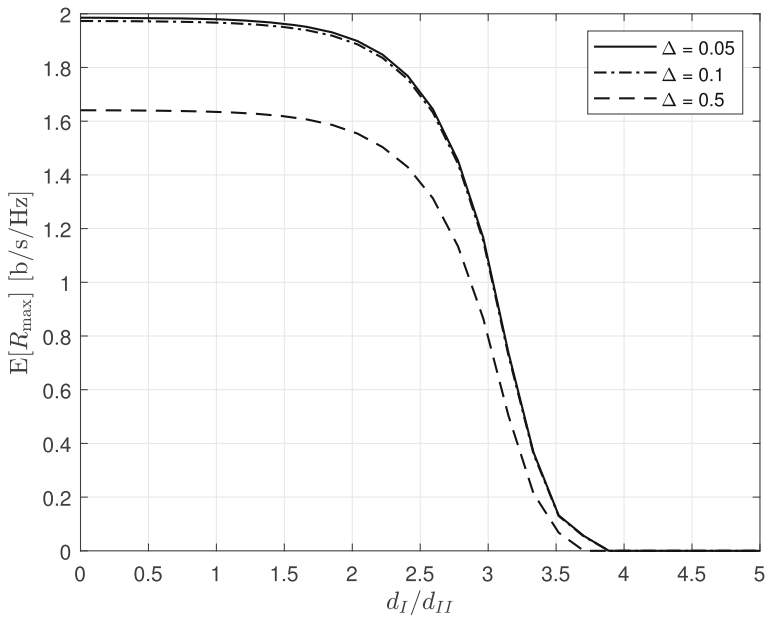

Fig. 11 Average maximum outage secrecy rate as a function of $d_{\mathrm{I}}/d_{\mathrm{II}}$, various values of Δ, and finite-length coding ($m = 4096$) with discrete (16-QAM) constellations, for $d_{\mathrm{E}} = 10$, $\epsilon = 10^{-4}$, and $N = 4$ relays

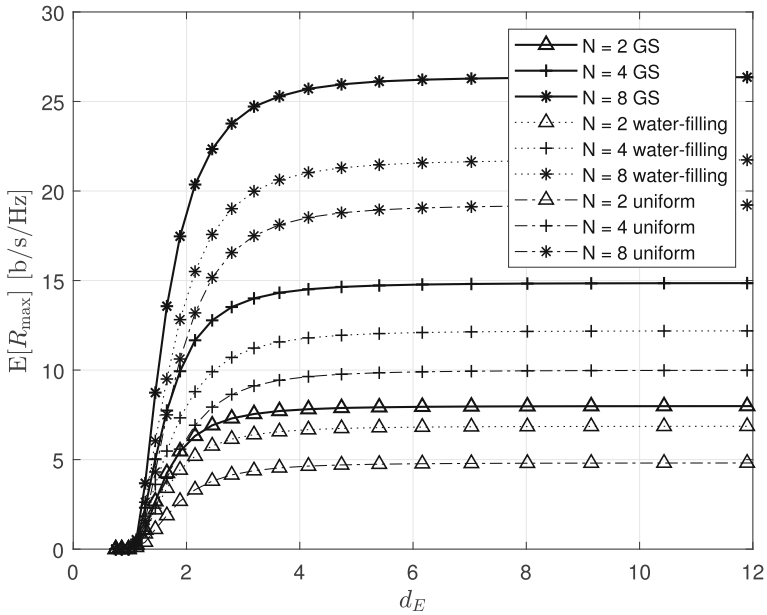

Fig. 12 Average maximum outage secrecy rate as a function of d_E, with infinite-length coding ($m = 4096$) and Gaussian constellation, obtained using GS power allocation, water-filling, and uniform power allocation

strategy and two suboptimal solutions, respectively uniform power allocation over the K channels and water-filling allocation. Various scenarios are considered, i.e., infinite-length codes with Gaussian signaling and finite-length coding with discrete constellations. We also consider that each relay has the same distance from Alice and Bob, i.e., $d_{\mathrm{I}} = d_{\mathrm{II}} = 0.8$, the separation between relays is $\Delta = 0.05$, and the number of relays is $N = 2$, 4, or 8. Water-filling provides the best possible power allocation in Eve's absence, since it assigns more power to the channels presenting better gains. However, this solution is not convenient from a security standpoint, since channels that are good for the legitimate receiver could also be good for the attacker, thus degrading the secrecy performance. As predicted, uniform allocation leads to the worst average secrecy rate for all the considered cases.

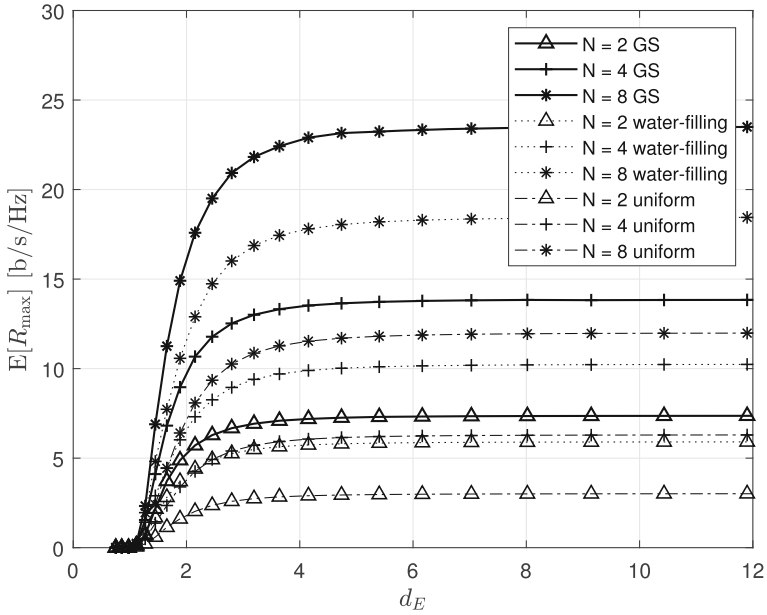

Fig. 13 Average maximum outage secrecy rate as a function of d_E, with finite-length coding ($m = 4096$) and discrete (16-QAM) constellations, obtained using optimal power allocation, water-filling, and uniform power allocation

7 Conclusions

In this paper, we have derived the secrecy rate of the Gaussian relay parallel channel under finite-length coding and discrete constellation constraints, defined as the maximum rate for which a minimum equivocation rate is achieved at Eve. Moreover, we have applied a coupled version of the Gale and Shapley algorithm to allocate power within each channel in order to maximize the secrecy rate. Numerical results show the effectiveness of our resource allocation approach and show that moderate sizes of both the constellation alphabet and the codeword length are sufficient to achieve close-to-optimal secrecy rates for typical wireless transmission scenarios.

Abbreviations

AWGN: Additive white Gaussian noise; CER: Codeword error rate; CSI: Channel state information; DF: Decode and forward; iid: Independent identically distributed; MIMO: Multiple input multiple output; OFDM: Orthogonal frequency division multiplexing; SNR: Signal to noise ratio

Acknowledgements

The material in this paper was presented in part at the IEEE Conference on Communications and Network Security (CNS 2015) – Workshop on Physical-layer Methods for Wireless Security, Florence, Italy, Sep. 2015.

Authors' contributions

All the authors participated in writing the article and revising the manuscript. All authors read and approved the final manuscript.

Availability of data and materials

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Via Brecce Bianche 12, 60131 Ancona, Italy. [2]Department of Information Engineering, University of Padova, Via Gradenigo 6, 35131 Padova, Italy.

Received: 22 May 2019 Accepted: 15 November 2019
Published online: 17 December 2019

References

1. M. Bloch, J. Barros, *Physical-Layer Security. From Information Theory to Security Engineering*. (Cambridge University Press, Cambridge, 2011), p. 357
2. W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, J. Barros, Coding for secrecy: an overview of error-control coding techniques for physical-layer security. IEEE Signal Process. Mag. **30**(5), 41–50 (2013)
3. S. Tomasin, in *Proc. IEEE Conference on Communications and Network Security (CNS)*. A Gale-Shapley algorithm for allocation of relayed parallel wiretap coding channels, (2015), pp. 119–124. https://doi.org/10.1109/CNS.2015.7346819
4. C.-L. Wang, T.-N. Cho, K.-J. Yang, in *Proc. 75th IEEE Vehicular Technology Conference (VTC Spring)*. A new cooperative transmission strategy for physical-layer security with multiple eavesdroppers, (2012), pp. 1–5. https://doi.org/10.1109/VETECS.2012.6240269
5. Y. Shen, X. Jiang, J. Ma, W. Shi, in *Information Technology Convergence*, ed. by J. J. J. H. Park, L. Barolli, F. Xhafa, and H.-Y. Jeong. Secure and reliable transmission with cooperative relays in two-hop wireless networks (Springer, Dordrecht, 2013), pp. 397–406
6. S. Luo, H. Godrich, A. Petropulu, H. V. Poor, in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*. A knapsack problem formulation for relay selection in secure cooperative wireless communication, (2011), pp. 2512–2515. https://doi.org/10.1109/ICASSP.2011.5946995
7. Z. Ding, M. Xu, J. Lu, F. Liu, Improving wireless security for bidirectional communication scenarios. IEEE Trans. Veh. Technol. **61**(6), 2842–2848 (2012). https://doi.org/10.1109/TVT.2012.2197032
8. L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010). https://doi.org/10.1109/TSP.2009.2038412
9. J. Li, A. P. Petropulu, S. Weber, On cooperative relaying schemes for wireless physical layer security. IEEE Trans. Signal Process. **59**(10), 4985–4997 (2011). https://doi.org/10.1109/TSP.2011.2159598
10. X. Chen, D. W. K. Ng, W. H. Gerstacker, H. Chen, A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutor. **19**(2), 1027–1053 (2017). https://doi.org/10.1109/COMST.2016.2633387
11. R. Bassily, S. Ulukus, Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. IEEE Trans. Signal Process. **61**(6), 1544–1554 (2013). https://doi.org/10.1109/TSP.2012.2235433
12. Z. H. Awan, A. Zaidi, L. Vandendorpe, Secure communication over parallel relay channel. IEEE Trans. Inf. Forensic. Secur. **7**(2), 359–371 (2012). https://doi.org/10.1109/TIFS.2012.2185493
13. D. W. K. Ng, E. S. Lo, R. Schober, Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks. IEEE Trans. Wirel. Commun. **10**(10), 3528–3540 (2011). https://doi.org/10.1109/TWC.2011.082011.110538
14. D. W. K. Ng, E. S. Lo, R. Schober, in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*. Resource allocation for secure OFDMA networks with imperfect csit, (2011), pp. 1–6. https://doi.org/10.1109/GLOCOM.2011.6133580
15. D. W. K. Ng, R. Schober, in *Proc. 12th Canadian Workshop on Information Theory (CWIT)*. Resource allocation for secure OFDMA decode-and-forward relay networks, (2011), pp. 202–205. https://doi.org/10.1109/CWIT.2011.5872157
16. Z. Yu, Y. Ma, B. Wang, J. Zhao, in *Proc. Int. Conf. on Wireless Communications Signal Processing (WCSP)*. Optimal resource allocation for OFDM wiretap channel with cooperative jammer, (2012), pp. 1–4. https://doi.org/10.1109/WCSP.2012.6542965
17. C. Jeong, I.-M. Kim, in *Proc. 8th Int. Workshop on Multi-Carrier Systems Solutions (MC-SS)*. Optimal power allocation for secure multi-carrier relay systems, (2011), pp. 1–4. https://doi.org/10.1109/MC-SS.2011.5910728
18. C. Jeong, I.-M. Kim, Optimal power allocation for secure multicarrier relay systems. IEEE Trans. Signal Process. **59**(11), 5428–5442 (2011). https://doi.org/10.1109/TSP.2011.2162956
19. B. Gui, L. J. Cimini, Bit loading algorithms for cooperative OFDM systems. EURASIP J. Wirel. Commun. Netw. **2008**(1), 476797 (2008)
20. L. Vandendorpe, J. Louveaux, O. Oguz, A. Zaidi, Rate-optimized power allocation for DF-relayed OFDM transmission under sum and individual power constraints. EURASIP J. Wirel. Commun. Netw. **2009**(1), 814278 (2009). https://doi.org/10.1155/2009/814278
21. T. Wang, L. Vandendorpe, Sum rate maximized resource allocation in multiple DF relays aided OFDM transmission. IEEE J. Sel. Areas Commun. **29**(8), 1559–1571 (2011)
22. K. Bakanoglu, S. Tomasin, E. Erkip, Resource allocation for the parallel relay channel with multiple relays. IEEE Trans. Wirel. Commun. **10**(3), 792–802 (2011)
23. N. Laurenti, S. Tomasin, F. Renna, in *Proc. IEEE Int. Conf. Commun. (ICC)*. Resource allocation for secret transmissions on parallel Rayleigh channels, (2014). https://doi.org/10.1109/icc.2014.6883651
24. M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, F. Renna, Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans. Inf. Forensic. Secur. **9**(11), 1765–1779 (2014). https://doi.org/10.1109/TIFS.2014.2348915
25. J. Chen, X. Chen, W. H. Gerstacker, D. W. K. Ng, Resource allocation for a massive MIMO relay aided secure communication. IEEE Trans. Inf. Forensic. Secur. **11**(8), 1700–1711 (2016)
26. H. Fang, L. Xu, K.-K. R. Choo, Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks. Appl. Math. Comput. **296**, 153–167 (2017)
27. J. H. Lee, Optimal power allocation for physical layer security in multi-hop DF relay networks. IEEE Trans. Wirel. Commun. **15**(1), 28–38 (2016). https://doi.org/10.1109/TWC.2015.2466091
28. J.-H. Lee, I. Sohn, Y.-H. Kim, Transmit power allocation for physical layer security in cooperative multi-hop full-duplex relay networks. Sensors. **16**(10), 1726 (2016)

29. K. Zhang, M. Peng, P. Zhang, X. Li, Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks. IEEE Trans. Veh. Technol. **66**(2), 1822–1834 (2017). https://doi.org/10.1109/TVT.2016.2566298
30. W. Aman, G. A. S. Sidhu, H. M. Furqan, Z. Ali, Enhancing physical layer security in AF relay-assisted multicarrier wireless transmission. Trans. Emerg. Telecommun. Technol. **29**(6), 1–14 (2018). https://doi.org/10.1002/ett.3289
31. M. R. Abedi, N. Mokari, H. Saeedi, H. Yanikomeroglu, Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: active adversary. IEEE Trans. Wirel. Commun. **16**(2), 885–899 (2017). https://doi.org/10.1109/TWC.2016.2633336
32. A. Kuhestani, A. Mohammadi, K. Wong, P. L. Yeoh, M. Moradikia, M. R. A. Khandaker, Optimal power allocation by imperfect hardware analysis in untrusted relaying networks. IEEE Trans. Wirel. Commun. **17**(7), 4302–4314 (2018)
33. A. Kuhestani, A. Mohammadi, P. L. Yeoh, Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer. IEEE Trans. Commun. **66**(6), 2671–2684 (2018)
34. M. Obeed, W. Mesbah, Efficient algorithms for physical layer security in two-way relay systems. Phys. Commun. **28**, 78–88 (2018). https://doi.org/10.1016/j.phycom.2018.03.007
35. A. Kuhestani, A. Mohammadi, M. Mohammadi, Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers. IEEE Trans. Inf. Forensic. Secur. **13**(2), 341–355 (2018)
36. S. Bashar, Z. Ding, C. Xiao, On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input. IEEE Trans. Commun. **60**(12), 3816–3825 (2012). https://doi.org/10.1109/TCOMM.2012.091212.110199
37. Z. Mheich, F. Alberge, P. Duhamel, Achievable secrecy rates for the broadcast channel with confidential message and finite constellation inputs. IEEE Trans. Commun. **63**(1), 195–205 (2015)
38. X. Liu, D. Ma, J. Xiong, W. Li, L. Cheng, in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. Power allocation for an-aided beamforming design in MISO wiretap channels with finite-alphabet signaling, (2016), pp. 1–6. https://doi.org/10.1109/vtcfall.2016.7881170
39. Y. Polyanskiy, Saddle point in the minimax converse for channel coding. IEEE Trans. Inf. Theory. **59**(5), 2576–2595 (2013)
40. N. Varnica, X. Ma, A. Kavcic, in *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*. Capacity of power constrained memoryless AWGN channels with fixed input constellations, vol. 2, (2002), pp. 1339–13432. https://doi.org/10.1109/GLOCOM.2002.1188416
41. E. A. Jorswieck, A. Wolf, in *Proc. of Int. Workshop on Multiple Access Communications (MACOM)*. Resource allocation for the wire-tap multi-carrier broadcast channel, (Saint Petersburg, 2008). https://doi.org/10.1109/ictel.2008.4652697
42. D. Gale, L. S. Shapley, College admissions and the stability of marriage. Am. Math. Mon. **69**, 9–15 (1962)

Publisher's Note