electronics

MDPI

Article

A Cooperative Jamming Technique to Protect a Two-User Broadcast Channel with Confidential Messages and an External Eavesdropper

Gustavo Anjos [1,2,*], Daniel Castanheira [2], Adão Silva [1,2] and Atílio Gameiro [1,2]

1 Department of Electronics Telecommunications and Informatics, Universidade de Aveiro, 3810-193 Aveiro, Portugal; asilva@av.it.pt (A.S.); amg@ua.pt (A.G.)

2 Instituto de Telecomunicações, 3810-193 Aveiro, Portugal; dcastanheira@av.it.pt

* Correspondence: gustavoanjos@ua.pt

Received: 28 February 2020; Accepted: 16 March 2020; Published: 18 March 2020

Abstract: This work addresses the security of a two-user broadcast channel. The challenge of protecting a broadcast channel is associated with the necessity of securing the system, not only against eavesdropping attacks originating from external nodes, but also to ensure that the inside users do not eavesdrop on each other's information. To address this issue, the present work proposes a cooperative jamming scheme that provides protection against eavesdropping attacks carried out simultaneously by inside users and external eavesdroppers. To achieve this goal, the developed scheme combines real interference alignment with a blind cooperative jamming technique defined in the literature. An information theoretical analysis shows that positive secure degrees of freedom are achievable using the proposed solution.

Keywords: broadcast channel; physical layer security; cooperative jamming; real interference alignment; blind cooperative jamming

1. Introduction

In commercial wireless standards, protection against eavesdropping attacks has been provided by cryptographic protocols [1,2]. Despite the large-scale proliferation of these protocols, confidentiality is only achieved when the processing capabilities of the attacker are not sufficient to solve the mathematical problems underlying these protocols. However, with the recent progress in the field of quantum processing, some of these difficult mathematical problems will be solvable [3], making the current cryptographic techniques less secure. A research line that has been followed to address these new threats focuses on exploiting the random properties of the wireless channel with the aim of developing advanced security functionalities at the physical layer [4–6]. Contrary to what happens with commercial cryptosystems, in physical layer security, the secrecy performance is quantified from an information theoretical perspective, not relying on any type of technological limitation at the eavesdropper.

1.1. Motivation and Related Work

The exploitation of the wireless medium as a source of secrecy can be carried out in two different ways. In the first, the internal dynamics of the channel can be used as a source of entropy to extract secret keys [7,8]. A second approach involves the use of cooperative jamming to force the degradation of the eavesdropper channel. In relation to cooperative jamming, a typical approach considers artificial noise (AN) generation to impair the eavesdropper channel with continuous Gaussian signals. The work in [9] shows that a positive secrecy rate can be achieved by sending AN in the null space (NS) direction of the legitimate receiver. Although the solution in [9] does not require eavesdropper channel state information

(CSI) at the legitimate nodes, an advantage on the number of antennas is required at the transmitting side to create a null space. The impairment of the channel training phase with the execution of pilot contamination attacks carried out by active eavesdroppers can be used to increase the capacity of the wiretap channel. To address the secrecy capacity reduction caused by contaminated channel estimations, the work in [10] explores the additional degrees of freedom of a massive multiple-input-multiple-output (MIMO) system to impair the eavesdropper with AN. The authors of [10] analyzed the tradeoff between performance and complexity of NS-based precoding and random shaping precoding, concluding that the latter offers a good solution for AN generation. Considering a scenario where the cooperative jammer is also the information source of a second receiver, the authors of [11] designed an AN jamming solution to protect the first receiver, ensuring at the same time a specific quality-of-service at the second. The integration of wireless powered communications with cooperative jamming was proposed in [12]. Using first the base station as a power source and then as a cooperative jammer, a secrecy rate maximization was performed in [12], computing optimal parameters for the jamming and energy harvesting phases.

The development of cooperative secure communications to protect two-hop relay networks has also been one of the most active research topics in the field of physical layer security. The authors of [13] evaluated several precoding schemes to secure a MIMO relay network considering two cooperative jamming configurations. In the full cooperative jamming configuration, both inactive and active nodes transmit jamming signals; in the partial jamming configuration, only the inactive nodes are used as jammers. An optimal relay selection algorithm was designed in [14] to secure a two-hop wireless network in a scenario where an adaptive eavesdropper can also act as a malicious jammer. Similarly to [14], protection against passive eavesdropping attacks is provided in [15] by selecting a pair of nodes to perform the jamming and relaying functions. While [13–15] focus on decode-and-forward (DF) relaying techniques, the authors of [16,17] considered the use of amplify-and-forward (AF) relays.

Following the theoretical insights of the real interference alignment framework defined in [18,19], another important line of research was established with the results obtained in [20,21]. In real interference alignment, the rational dimensions available in single antenna systems are used to set alignment directions for data and interference. These directions are defined using rationally independent scalars as precoding coefficients. By making a proper selection of these coefficients, different alignment conditions between the jamming and information signals can be exploited to secure the system. According to the findings of [20,21], positive secure degrees of freedom (DoF) are obtained if the jamming process is designed with some structure. Through the alignment of discrete jamming signals with the information signals at the eavesdropper, the work in [20] showed that positive secure DoF are achievable if the eavesdropper CSI is available at the legitimate terminals. The same authors of [20] considered a more realistic scenario in [21] where eavesdropper CSI is not available. In this second scenario, the authors proposed a blind cooperative jamming solution, demonstrating that positive secure DoF can still be achieved by spreading the jamming components across the signal space of the eavesdropper.

1.2. Contribution

The authors of [20,21] analyzed several network structures, including the wiretap channel, the interference channel and the multiple access channel. The broadcast channel was solely evaluated in [20] by considering a scenario where information leakage only occurs among legitimate users, i.e., not taking into account the presence of external eavesdroppers. In this type of channel, the interference generated by the information sent to the other users must always be decoded by the receiver in order to allow a correct acquisition of the intended data. Additionally, because this interference could represent valuable information, it should remain confidential even among the terminals registered as legitimate users inside the network. Please note that an eavesdropper could connect to the network as a fake legitimate user only for the purpose of tapping the information sent to the other users. Therefore, a robust secrecy solution should provide protection not only against attacks carried out by external eavesdroppers, but also against attacks executed by terminals registered in the network as legitimate

users. To the best of the authors' knowledge, securing a broadcast channel against eavesdropping attacks carried out simultaneously by internal users and external eavesdroppers is an open problem that remains untreated in the literature. To address this issue, the present work extends [20] by providing a cooperative jamming solution that also protects a two-user broadcast channel against passive eavesdropping attacks carried out by external terminals. To achieve this goal, the developed scheme combines real interference alignment with the concept of blind cooperative jamming defined in [21]. An information theoretical analysis shows that positive secure DoF are achievable with the proposed solution.

1.3. Organization

The remainder of this paper is organized as follows: Section 2 presents the system model, while Section 3 defines some preliminaries on real interference alignment. The cooperative jamming solution proposed in this manuscript is formulated in Section 4 and evaluated in Section 5. Some practical challenges are discussed in Section 6. The main conclusions are outlined in Section 7.

Notation: The discrete entropy of the random variable X is denoted by $H(X)$, and the continuous differential entropy by $h(X)$. The notation $I\,[X;Y]$ refers to the mutual information between X and Y, while the expected value of X is represented by $\mathrm{E}[X]$. A vector comprising n realizations of X is denoted by $\mathbf{X}^n$, and $o\,[f(x)]$ defines the little-o notation.

2. System Model

The communication model considered in this work is illustrated in Figure 1. Node "A" pretends to transmit two confidential messages to users "B_0" and "B_1". Additionally, a passive eavesdropper denoted by "E" tries to obtain the information sent to both users. This work also assumes that "B_0" and "B_1" are eavesdroppers of each other. To enhance the security level of the system, two jammers represented by "J_0" and "J_1" cooperate with "A", generating two independent jamming signals. All the terminals have a single antenna. The channel gains are real and remain static during the entire communication phase. Furthermore, this work also assumes that the channels of the different users are independently sampled from a continuous known distribution. Finally, this model assumes that the channel of the eavesdropper "E" is the only one that is not known by the remaining terminals.

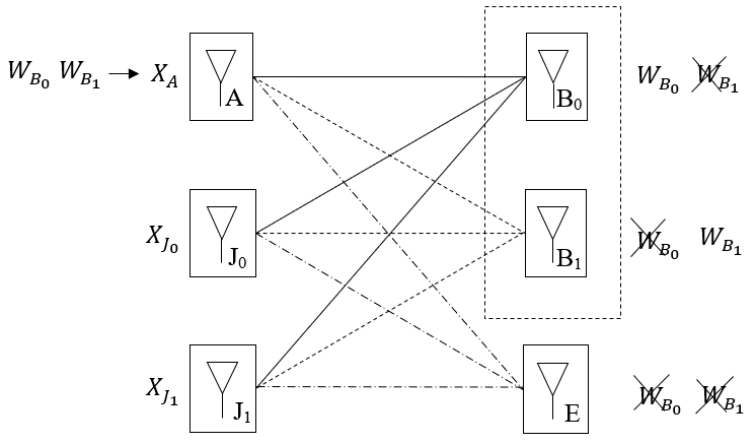

Figure 1. System model.

Defining X_T as the channel input of transmitter $T \in \{A, J_0, J_1\}$, and assuming an average power constraint $E\,[X_T^2] < P$, the signals observed at the receiving nodes $R \in \{B_0, B_1, E\}$ are formulated as

$$Y_{B_0} = h_{B_0A}X_A + h_{B_0J_0}X_{J_0} + h_{B_0J_1}X_{J_1} + N_{B_0} \tag{1}$$

$$Y_{B_1} = h_{B_1A}X_A + h_{B_1J_0}X_{J_0} + h_{B_1J_1}X_{J_1} + N_{B_1} \tag{2}$$

$$Y_E = h_{EA}X_A + h_{EJ_0}X_{J_0} + h_{EJ_1}X_{J_1} + N_E \tag{3}$$

The channel gain between terminal R and T is denoted by the coefficient h_{RT}, while noise at the receiving node R is defined by random variable N_R, which follows a zero-mean Gaussian distribution with variance $\sigma^2_{N_R}$. In this work, node "A" wants to transmit, in secrecy, message W_{B_0} to node "B_0", and message W_{B_1} to node "B_1". In the case of W_{B_0}, secrecy implies that the message is either protected against eavesdropping attacks carried out by "E" or "B_1". Similarly, the message W_{B_1} is secured if neither node "E" nor node "B_0" is capable of decoding the respective information. The messages are independent and chosen uniformly from the sets $\mathcal{W}_{B_0}$ and $\mathcal{W}_{B_1}$.

Before the transmission, each message is mapped into a codeword of length n using the encoding functions $f_{B_0} : \mathcal{W}_{B_0} \to \mathbf{V}^n_{B_0}$ and $f_{B_1} : \mathcal{W}_{B_1} \to \mathbf{V}^n_{B_1}$. In each channel use, X_A is computed combining the codeword elements V_{B_0} and V_{B_1} with a jamming component U_A, resulting in the following transmitted signal

$$X_A = w_0V_{B_0} + w_1V_{B_1} + w_2U_A \tag{4}$$

At nodes "J0" and "J1", two jamming components U_{J_0} and U_{J_1} are also generated and transmitted using the signals

$$X_{J_0} = w_3U_{J_0} \tag{5}$$

$$X_{J_1} = w_4U_{J_1} \tag{6}$$

The coefficient w_i, $i \in \{0, 1, 2, 3, 4\}$ denotes a channel dependent precoder that is specified in Section 4. After the encoding phase, each message is transmitted across n channel uses at the following rates

$$R_{B_0} = \frac{1}{n}\log_2\left|\mathcal{W}_{B_0}\right| \tag{7}$$

$$R_{B_1} = \frac{1}{n}\log_2\left|\mathcal{W}_{B_1}\right| \tag{8}$$

where $\left|\mathcal{W}_{B_0}\right|$ and $\left|\mathcal{W}_{B_1}\right|$ define the cardinality of the sets $\mathcal{W}_{B_0}$ and $\mathcal{W}_{B_1}$, respectively. After sampling the channel output n times, "B_0" decodes $\mathbf{Y}^n_{B_0}$ and obtains an estimation of W_{B_0}, which is denoted by $\hat{W}_{B_0}$. In a similar way, "B_1" computes $\hat{W}_{B_1}$ after decoding $\mathbf{Y}^n_{B_1}$. The rate pair $\left(R_{B_0}, R_{B_1}\right)$ is achievable if for any $\epsilon > 0$ there exists an n-length code such that the probability of decoding error is given by

$$P_e\left[W_{B_0} \neq \hat{W}_{B_0}\right] \leq \epsilon \tag{9}$$

$$P_e\left[W_{B_1} \neq \hat{W}_{B_1}\right] \leq \epsilon \tag{10}$$

Furthermore, at the same time, W_{B_0} and W_{B_1} are transmitted in perfect secrecy if

$$\frac{1}{n}\min\left\{H(W_{B_0}|Y_{B_1}), H(W_{B_0}|Y_E)\right\} \geq \frac{1}{n}H(W_{B_0}) - \epsilon \tag{11}$$

$$\frac{1}{n}\min\left\{H(W_{B_1}|Y_{B_0}), H(W_{B_1}|Y_E)\right\} \geq \frac{1}{n}H(W_{B_1}) - \epsilon \tag{12}$$

The conditions in (9)–(12) can be mutually achieved if the rate pair $\left(R_{B_0}, R_{B_1}\right)$ belongs to the capacity region of the system. The proof of achievability can be performed using random code constructions featuring codeword lengths with $n \to \infty$. In the remainder of this work, it is assumed that the codebooks and encoding functions f_{B_0} and f_{B_1} at all terminals are known.

3. Preliminaries

This section presents a lemma that has been applied in the DoF analysis of different network structures. This lemma is a fundamental tool in the field of real interference alignment [18,19], being used to demonstrate that the fractional dimensions offered by single antenna systems can be exploited

to manage interference. In this work, this lemma is applied in the DoF analysis of the proposed cooperative jamming solution. The considered lemma was used in [20] to derive an upper bound on the probability of error of the following multi-layer constellation

$$X = \sum_{i=1}^{L_0} g_i c_i \tag{13}$$

where $\{g_i\}_{i=1}^{L_0}$ denotes a set composed by L_0 rationally independent real numbers, and $\{c_i\}_{i=1}^{L_0}$ defines L_0 information streams independently sampled from

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{14}$$

The ensemble $C(a, Q)$ represents a set of $2Q+1$ real numbers, where parameter a defines the distance between consecutive points. The probability of decoding error is derived for an additive noise channel

$$Y = X + N \tag{15}$$

where N denotes Gaussian noise with variance σ_N^2, and X defines a set of $(2Q+1)^{L_0}$ real points featuring an average power constraint $E\left[X^2\right] < P$. The considered lemma states the following:

Lemma 1. *For any small enough $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we select the parameters*

$$Q = P^{\frac{1-\delta}{2(L_1+\delta)}} \quad \text{and} \quad a = \gamma \frac{\sqrt{P}}{Q} \tag{16}$$

then the average power constraint $E\left[X^2\right] \leq P$ is satisfied, and for almost all $\{g_i\}_{i=1}^{L_0}$, except for a set of Lebesgue measure zero (probability of the event arbitrarily close to zero), the probability of error is upper bounded by

$$P_e \leq \exp\left(-\eta_\gamma P^{\xi}\right) \tag{17}$$

where η_γ is a positive constant independent of P, and the condition $\xi > 0$ is always verified for $L_1 \geq L_0$.

Lemma 1 is supported by the Khintchine–Groshev theorem [18,19], which defines a lower bound on the minimal distance between consecutive points of (13). The theorem states that when the information streams $\{c_i\}_{i=1}^{L_0}$ are drawn from the set $C(a, Q)$, there exists a constant k_δ such that for any $\delta > 0$, the minimal distance between the $(2Q+1)^{L_0}$ points of X can be lower bounded by

$$d_{\min} \geq \frac{k_\delta a}{Q^{L_0 - 1 + \delta}} \tag{18}$$

The Khintchine–Groshev theorem can be extended to the case where the terms of $\{c_i\}_{i=1}^{L_0}$ are drawn from different sets $C_i(a, Q_i)$. In this case, the minimal distance between the $\prod_{i=1}^{L_0}(2Q_i+1)$ points of X is lower bounded in the following way:

$$d_{\min} \geq \frac{k_\delta a}{(\max_i Q_i)^{L_0 - 1 + \delta}} \tag{19}$$

The result formulated in Lemma 1 is applied in the DoF analysis of the cooperative jamming solution proposed in this work. In the real domain, a DoF pair is formulated as

$$\begin{cases} D_{B_0} = \lim\limits_{P \to \infty} \frac{R_{B_0}}{2\log_2(P)} \\ D_{B_1} = \lim\limits_{P \to \infty} \frac{R_{B_1}}{2\log_2(P)} \end{cases} \tag{20}$$

where P denotes a channel input power constraint, and the pair (R_{B_0}, R_{B_1}) comprises achievable secrecy rates for nodes "B_0" and "B_1".

4. Security Scheme

The cooperative jamming solution proposed in this work is developed in the context of the theoretical framework described in Section 3. Accordingly, in the following, we assume that the signals $\{V_{B_0}, V_{B_1}, U_A, U_{J_0}, U_{J_1}\}$ are mutually independent and are sampled from $C(a, Q)$ in (14), applying the parameters

$$Q = P^{\frac{1-\delta}{2(3+\delta)}} \quad \text{and} \quad a = \gamma \frac{\sqrt{P}}{Q} \tag{21}$$

After the encoding phase, the jamming and the information signals are linearly precoded and transmitted using the following signals:

$$X_A = \frac{1}{h_{B_1A}} V_{B_0} + \frac{h_{B_0J_0}}{h_{B_1J_0}h_{B_0A}} V_{B_1} + \frac{h_{B_0J_1}}{h_{B_1J_1}h_{B_0A}} U_A \tag{22}$$

$$X_{J_0} = \frac{1}{h_{B_1J_0}} U_{J_0} \tag{23}$$

$$X_{J_1} = \frac{1}{h_{B_1J_1}} U_{J_1} \tag{24}$$

Please note that in (22)–(24), the precoding coefficients w_i, $i \in \{0, 1, 2, 3, 4\}$ are designed without using the channel gains of the external eavesdropper "E", which complies with the passive condition defined for this terminal. For the channel model formulated in (1)–(3), the signals observed at the channel output are defined as

$$Y_{B_0} = \frac{h_{B_0A}}{h_{B_1A}} V_{B_0} + \frac{h_{B_0J_0}}{h_{B_1J_0}} \left[V_{B_1} + U_{J_0}\right] + \frac{h_{B_0J_1}}{h_{B_1J_1}} \left[U_A + U_{J_1}\right] + N_{B_0} \tag{25}$$

$$Y_{B_1} = \left[V_{B_0} + U_{J_0} + U_{J_1}\right] + \frac{h_{B_1A}h_{B_0J_0}}{h_{B_0A}h_{B_1J_0}} V_{B_1} + \frac{h_{B_1A}h_{B_0J_1}}{h_{B_0A}h_{B_1J_1}} U_A + N_{B_1} \tag{26}$$

$$Y_E = \frac{h_{EA}}{h_{B_1A}} V_{B_0} + \frac{h_{EA}h_{B_0J_0}}{h_{B_0A}h_{B_1J_0}} V_{B_1} + \frac{h_{EA}h_{B_0J_1}}{h_{B_0A}h_{B_1J_1}} U_A + \frac{h_{EJ_0}}{h_{B_1J_0}} U_{J_0} + \frac{h_{EJ_1}}{h_{B_1J_1}} U_{J_1} + N_E \tag{27}$$

The developed solution protects "B_0" from the eavesdropping attacks of "B_1", forcing the alignment of V_{B_0} with $U_{J_0} + U_{J_1}$ at the channel output of "B_1". At node "B_0", the information intended for "B_1" is also secured with the alignment of V_{B_1} with U_{J_0}. In the case of node "E", it is not possible to explicitly align V_{B_0} and V_{B_1} with any jamming signal. However, as demonstrated in [21], secrecy against node "E" is still achievable by filling the signal space of node "E" with enough jamming signals. As it is demonstrated in Section 5, positive secure DoF are achievable using the secrecy solution proposed in this work.

5. Secrecy Analysis

The secrecy analysis of the proposed scheme is presented in the following using the limits formulated in (20) as the evaluation metric. For the reliability and secrecy constraints defined in equations (9)–(12), the following secrecy rates

$$R_{B_0} \geq I\left[V_{B_0}; Y_{B_0}\right] - \max\left\{I\left[V_{B_0}; Y_{B_1} \middle| V_{B_1}\right]; I\left[V_{B_0}; Y_E \middle| V_{B_1}\right]\right\} \tag{28}$$

$$R_{B_1} \geq I\left[V_{B_1}; Y_{B_1}\right] - \max\left\{I\left[V_{B_1}; Y_{B_0} \middle| V_{B_0}\right]; I\left[V_{B_1}; Y_E \middle| V_{B_0}\right]\right\} \tag{29}$$

are achievable using the random encoding schemes defined in [22]. In order to derive an achievable DoF pair, all the mutual information terms in (28) and (29) are computed in this section. The main result of the theoretical analysis performed in this work is formalized in the following theorem:

Theorem 1. *The secure DoF pair* $(D_{B_0}, D_{B_1}) = (1/3, 1/3)$ *is achievable using the cooperative jamming scheme formulated in Section 4.*

Proof. See Sections 5.1 and 5.2. □

As stated above, in the asymptotical power regime of (20), fractional secure DoF can be reached by applying the cooperative jamming scheme developed in this work. The demonstration of Theorem 1 is provided in Sections 5.1 and 5.2.

5.1. DoF Characterization at "B_0"

The derivation of the achievable DoF at node "B_0" is presented in this subsection. To accomplish this, theoretical bounds on the mutual information terms of (28) are defined in Lemmas 2–4.

Introducing Lemma 2 first, a lower bound on the amount of legitimate information obtained by node "B_0" is formalized as follows:

Lemma 2. *For any* $\delta > 0$*, the amount of information* V_{B_0} *that node "*B_0*" obtains from the observation of* Y_{B_0} *is lower bounded by*

$$I\left[V_{B_0}; Y_{B_0}\right] \geq \left(\frac{1-\delta}{3+\delta}\right)\frac{1}{2}\log_2(P) - o\left[\log_2(P)\right] \tag{30}$$

Proof. The proof is provided in Appendix A. □

Lemma 2 was computed applying the theoretical tools provided by the real interference alignment framework described in Section 3, namely, Lemma 1. The amount of information intended for node "B_0" that is eavesdropped by "B_1" is quantified in Lemma 3.

Lemma 3. *The amount of information* V_{B_0} *that node "*B_1*" obtains from the observation of* Y_{B_1} *is given by*

$$I\left[V_{B_0}; Y_{B_1} \middle| V_{B_1}\right] = o\left[\log_2(P)\right] \tag{31}$$

Proof. Because V_{B_0} is aligned with $U_{J_0} + U_{J_1}$ in (26), "B_0" can only obtain information about V_{B_0} from the observation of $V_{B_0} + U_{J_0} + U_{J_1}$. Therefore, the following upper bound

$$\begin{aligned} I\left[V_{B_0}; Y_{B_1} \middle| V_{B_1}\right] &\leq I\left[V_{B_0}; V_{B_0} + U_{J_0} + U_{J_1}\right] \\ &\leq I\left[V_{B_0}; V_{B_0} + U_{J_0}\right] \\ &= o\left[\log_2(P)\right] \end{aligned} \tag{32}$$

can be computed assuming a noiseless and non-interference regime in (26). As demonstrated in [23], $I\left[V_{B_0}; V_{B_0} + U_{J_0}\right] < 1$ bits, leading to the result in (31). □

To complete the secure DoF characterization at "B_0", an upper bound on the amount of information V_{B_0} obtained by node "E" is formulated in Lemma 4. As in Lemma 2, the computation of Lemma 4 was performed using the theoretical framework defined in Section 3.

Lemma 4. *For any $\delta > 0$, the amount of information V_{B_0} that node "E" obtains from the observation of Y_E is defined by*

$$I\left[V_{B_0}; Y_E \middle| V_{B_1}\right] \leq \left[\frac{4\delta}{3+\delta}\right]\frac{1}{2}\log_2 P + o\left[\log_2(P)\right] \tag{33}$$

Proof. The proof is provided in Appendix B. □

According to Lemma 1, the value of δ in (30) and (33) can be made arbitrarily close to zero. Therefore, applying Lemmas 2–4 to (28) and (20), it is possible to conclude that $D_{B_0} = 1/3$ is achievable at node "B_0".

5.2. DoF Characterization at "B_1"

The DoF characterization at node "B_1" is presented in the following. As demonstrated in Section 5.1, all the mutual information terms of (29) are analyzed in this subsection. Again using the framework described in Section 3, a lower bound on the amount of information V_{B_1} obtained by node "B1" is defined in Lemma 5.

Lemma 5. *For any $\delta > 0$, the amount of information V_{B_1} that node "B_1" obtains from the observation of Y_{B_1} is lower bounded by*

$$I\left[V_{B_1}; Y_{B_1}\right] \geq \left(\frac{1-\delta}{3+\delta}\right)\frac{1}{2}\log_2(P) - o\left[\log_2(P)\right] \tag{34}$$

Proof. Similar to the proof of Lemma 2 in Section 5.1, only the equivalent channel gains are different. □

Lemma 6 quantifies an upper bound on the total information V_{B_1} acquired by "B_0" when the channel output in (25) is observed.

Lemma 6. *The amount of information V_{B_1} that node "B_0" obtains from the observation of Y_{B_0} is given by*

$$I\left[V_{B_1}; Y_{B_0} \middle| V_{B_0}\right] = o\left[\log_2(P)\right] \tag{35}$$

Proof. Because V_{B_1} is aligned with U_{J_0} in (25), "B_0" only obtains information about V_{B_1} from the observation of $V_{B_1} + U_{J_0}$. Therefore, the following upper bound

$$\begin{aligned} I\left[V_{B_1}; Y_{B_0} \middle| V_{B_0}\right] &\leq I\left[V_{B_1}; V_{B_1} + U_{J_0}\right] \\ &= o\left[\log_2(P)\right] \end{aligned} \tag{36}$$

can be computed assuming a noiseless and non-interference regime in (25). As demonstrated in [23], $I\left[V_{B_0}; V_{B_0} + U_{J_0}\right] < 1$ bits, leading to the result in (35). □

The leakage of information V_{B_1} at node "E" is upper bounded in Lemma 7. As shown in Lemma 4, the theoretical framework defined in Section 3 was again applied to build Lemma 7.

Lemma 7. *For any $\delta > 0$, the amount of information V_{B_1} that node "E" obtains from the observation of Y_E is upper bounded by*

$$I\left[V_{B_1}; Y_E \middle| V_{B_0}\right] \leq \left[\frac{4\delta}{3+\delta}\right]\frac{1}{2}\log_2 P + o\left[\log_2(P)\right] \tag{37}$$

Proof. Similar to the proof of Lemma 4 in Section 5.1. □

The achievability of $D_{B_1} = 1/3$ follows from Lemmas 5–7, (29) and (20). After this final step, the proof of Theorem 1 is completed.

6. Discussion

Although this work considers a static channel environment, in a real scenario, the channel is always dynamic and therefore must be measured periodically. In a dynamic channel context, a practical execution of the proposed scheme would require the implementation of a channel training phase for each new realization of the channel. This channel training phase would comprise an initial stage for pilot transmission, which would be carried out by all the terminals with the exception of node "E". Then, a channel feedback stage would be performed in order to provide each node with the necessary information to set the alignment conditions and to allow the decoding process at "B_0" and "B_1". Due to the large number of channel gains that must be known at each terminal, one of the main challenges associated with the practical implementation of the proposed scheme is related to the complexity and overhead associated with the channel training phase. These requirements stem from the alignment conditions that need to be met to ensure the security requirements. We should point out that this issue is not specific to the proposed scheme, being widely recognized as a general problem in the field of real interference alignment, particularly when these types of techniques are applied to large multiuser networks. To address the practical constraints mentioned above, efficient channel training methods must be designed to enable the practical implementation of such technology.

7. Conclusions

A physical layer security solution employing two cooperative jammers was developed in this work by combining the concepts of real interference alignment and blind cooperative jamming. The proposed scheme complements the related literature by protecting a two-user broadcast channel against simultaneous internal and external eavesdropping attacks. An information theoretical analysis of the developed solution showed that in a high signal to noise ratio (SNR) regime, a secure DoF of $1/3$ is achieved at each user.

Author Contributions: Investigation, G.A.; Supervision, D.C. and A.S.; Validation, D.C., A.S. and A.G.; Writing—original draft, G.A.; Writing—review and editing, D.C. and A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the project MASSIVE5G (PTDC/EEI-TEL/30588/2017); the project UIDB/50008/2020-UIDP/50008/2020; the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Program (COMPETE 2020), Regional Operational Program of Lisbon, Fundação para a Ciência e Tecnologia; PES3N: Soluções Energeticamente Eficientes para Redes de Sensores Seguras—POCI-01-0145-FEDER- 030629; and an FCT grant for the first author (SFRH/BD/136787/2018).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The proof of Lemma 2 is derived in the following. For convenience, Lemma 2 is repeated here.

Lemma 2. *For any $\delta > 0$, the amount of information V_{B_0} that node "B_0" obtains from the observation of Y_{B_0} is defined by*

$$I\left[V_{B_0}; Y_{B_0}\right] \geq \left(\frac{1-\delta}{3+\delta}\right)\frac{1}{2}\log_2(P) - o\left[\log_2(P)\right] \tag{A1}$$

Proof. Applying the theoretical framework described in Section 3, a lower bound on the amount of information V_{B_0} obtained by "B_0" can be derived as follows

$$\begin{aligned} I\left[V_{B_0};Y_{B_0}\right] &= H\left(V_{B_0}\right) - H\left(V_{B_0}\middle|Y_{B_0}\right) \\ &\overset{(a)}{\geq} \log_2(2Q+1) - \left[1 + P_e \log_2(2Q+1)\right] \\ &\overset{(b)}{\geq} \log_2\left(P^{\frac{1-\delta}{2(3+\delta)}}\right) - \exp\left(-\eta_\gamma P^{\xi}\right)\log_2\left(P^{\frac{1-\delta}{2(3+\delta)}}\right) - 1 \\ &\overset{(c)}{=} \left(\tfrac{1-\delta}{3+\delta}\right)\tfrac{1}{2}\log_2(P) - o\left[\log_2(P)\right] \end{aligned} \tag{A2}$$

The Fano inequality in [24] is applied to step (a), while Lemma 1 is used in (b). Note that the equivalent channel coefficients in (25) are rationally independent. Therefore, according to Lemma 1, for $L_1 = 3$ the upper bound on the probability of error defined in (17) can be applied to the channel output of "B_0", which validates (b). Additionally, since the last two terms of (b) do not scale with $\log_2 P$, the final result in (c) holds. □

Appendix B

The proof of Lemma 4 is derived in this section. For simplification purposes, in the following let us assume that

$$\mathbf{U} = \begin{bmatrix} U_A & U_{J_0} & U_{J_1} \end{bmatrix} \tag{A3}$$

denotes a vector containing all the jamming signals used by the proposed scheme. Additionally, variable Y'_E is also defined as

$$Y'_E = \frac{h_{EA}}{h_{B_1A}}V_{B_0} + \frac{h_{EA}h_{B_0J_1}}{h_{B_0A}h_{B_1J_1}}U_A + \frac{h_{EJ_0}}{h_{B_1J_0}}U_{J_0} + \frac{h_{EJ_1}}{h_{B_1J_1}}U_{J_1} + N_E \tag{A4}$$

For convenience, Lemma 4 is repeated here.

Lemma 4. *For any $\delta > 0$, the amount of information V_{B_0} that node "E" obtains from the observation of Y_E is defined by*

$$I\left[V_{B_0};Y_E\middle|V_{B_1}\right] \leq \left[\frac{4\delta}{3+\delta}\right]\frac{1}{2}\log_2 P + o\left[\log_2(P)\right] \tag{A5}$$

Proof. Again using the framework defined in Section 3, an upper bound on the amount of information V_{B_0} obtained by "E" is derived as follows:

$$\begin{aligned} I\left[V_{B_0};Y_E\middle|V_{B_1}\right] &= I\left[V_{B_0},\mathbf{U};Y_E\middle|V_{B_1}\right] - I\left[\mathbf{U};Y_E\middle|V_{B_0},V_{B_1}\right] \\ &\overset{(d)}{=} I\left[V_{B_0},\mathbf{U};Y_E\middle|V_{B_1}\right] - \left[H\left(\mathbf{U}\middle|V_{B_0},V_{B_1}\right) - H\left(\mathbf{U}\middle|Y_E,V_{B_0},V_{B_1}\right)\right] \\ &\overset{(e)}{\leq} I\left[V_{B_0},\mathbf{U};Y_E\middle|V_{B_1}\right] - H\left(\mathbf{U}\middle|V_{B_0},V_{B_1}\right) + o\left(\log_2 P\right) \\ &= h\left(Y_E\middle|V_{B_1}\right) - h\left(Y_E\middle|V_{B_0},V_{B_1},\mathbf{U}\right) - H(\mathbf{U}) + o\left(\log_2 P\right) \\ &= h\left(Y'_E\right) - h(N_E) - H(\mathbf{U}) + o\left(\log_2 P\right) \\ &\overset{(f)}{\leq} h\left(Y'_E\right) - H(\mathbf{U}) + o\left(\log_2 P\right) \\ &= h\left(Y'_E\right) - \log_2(2Q+1)^3 + o\left(\log_2 P\right) \\ &\leq h\left(Y'_E\right) - \log_2 Q^3 + o\left(\log_2 P\right) \\ &\overset{(g)}{\leq} \tfrac{1}{2}\log_2\left(2\pi e\sigma^2\right) - \log_2 Q^3 + o\left(\log_2 P\right) \\ &\overset{(h)}{\leq} \tfrac{1}{2}\log_2 P - \log_2 Q^3 + o\left(\log_2 P\right) \\ &\overset{(i)}{\leq} \tfrac{1}{2}\log_2 P - \log_2 P^{\frac{3}{2}\left[\frac{1-\delta}{3+\delta}\right]} + o\left(\log_2 P\right) \\ &= \tfrac{1}{2}\log_2 P - \left[\tfrac{3(1-\delta)}{3+\delta}\right]\tfrac{1}{2}\log_2 P + o\left(\log_2 P\right) \\ &= \left[\tfrac{4\delta}{3+\delta}\right]\tfrac{1}{2}\log_2 P + o\left(\log_2 P\right) \end{aligned} \tag{A6}$$

Step (e) results from the joint application of the Fano inequality [24] and Lemma 1 to the last term of step (d). Because the variance of N_E is finite and independent of P, the differential entropy of N_E does not scale with $\log_2 P$, which validates (f). Moreover, defining σ^2 as the variance of Y'_E in (A4), an upper bound on $h\left(Y'_E\right)$ is derived in (g) by applying the closed form solution for the differential entropy of a normal distribution with variance σ^2. The upper bound in (h) is valid since σ^2 only scales with the average power at the channel input, which is constrained to P according to Lemma 1. Finally, step (i) is obtained by setting Q with the value defined in (21). □

References

1. Schneier, B. Cryptographic design vulnerabilities. *IEEE Comput.* **1998**, *31*, 29–33. [CrossRef]
2. Sandirigama, M.; Idamekorala, R. Security Weaknesses of WEP Protocol IEEE 802.11b and Enhancing the Security with Dynamic Keys. In Proceedings of the Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference, Toronto, ON, Canada, 26–27 September 2009; pp. 433–438.
3. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994.
4. Mukherjee, A.; Fakoorian, S.; Ali, A.; Huang, J.; Swindlehurst, A. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [CrossRef]
5. Yener, A.; Ulukus, S. Wireless physical-layer security: Lessons learned from information theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [CrossRef]
6. Makarfi, A.U.; Rabie, K.M.; Kaiwartya, O.; Li, X.; Kharel, R. Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces. Available online: https://arxiv.org/abs/1912.12183 (accessed on 7 February 2020).
7. Ren, K.; Su, H.; Wang, Q. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wirel. Commun.* **2011**, *18*, 6–12. [CrossRef]
8. Wang, Q.; Xu, K.; Ren, K. Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 1666–1674. [CrossRef]
9. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2018**, *7*, 2180–2189. [CrossRef]
10. Zhu, J.; Schober, R.; Bhargava, V.K. Secure transmission in multicell massive MIMO systems. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 4766–4781. [CrossRef]
11. Hu, L.; Wen, H.; Wu, B.; Tang, J.; Pan, F. Adaptive Secure Transmission for Physical Layer Security in Cooperative Wireless Networks. *IEEE Commun. Lett.* **2017**, *21*, 524–527. [CrossRef]
12. Tang, L.; Li, Q. Wireless Power Transfer and Cooperative Jamming for Secrecy Throughput Maximization. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 556–559. [CrossRef]
13. Huang, J.; Swindlehurst, A.L. Cooperative Jamming for Secure Communications in MIMO Relay Networks. *IEEE Trans. Signal Process.* **2011**, *59*, 4871–4884. [CrossRef]
14. Yang, L.; Chen, J.; Jiang, H.; Vorobyov, S.A.; Zhang, H. Optimal Relay Selection for Secure Cooperative Communications with an Adaptive Eavesdropper. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 26–42. [CrossRef]
15. Hoang, T.M.; Duong, T.Q.; Vo, N.S.; Kundu, C. Physical Layer Security in Cooperative Energy Harvesting Networks with a Friendly Jammer. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 174–177. [CrossRef]
16. Alotaibi, E.R.; Hamdi, K.A. Optimal Cooperative Relaying and Jamming for Secure Communication. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 689–692. [CrossRef]
17. Salem, A.; Hamdi, K.; Rabie, K. Physical Layer Security with RF Energy Harvesting in AF Multi-Antenna Relaying Networks. *IEEE Trans. Commun.* **2016**, *64*, 3025–3038. [CrossRef]
18. Motahari, A.S.; Oveis-Gharan, S.; Khandani, A.K. Real Interference Alignment with Real Numbers. Available online: https://arxiv.org/abs/0908.1208 (accessed on 14 October 2016).
19. Motahari, A.S.; Oveis-Gharan, S.; Maddah-Ali, M.; Khandani, A.K. Real Interference Alignment: Exploiting the Potential of Single Antenna Systems. *IEEE Trans. Inf. Theory* **2014**, *60*, 4799–4810. [CrossRef]
20. Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks. *IEEE Trans. Inf. Theory* **2014**, *60*, 3359–3378. [CrossRef]

21. Mukherjee, P.; Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks with No Eavesdropper CSIT. *IEEE Trans. Inf. Theory* **2017**, *63*, 1898–1922. [CrossRef]
22. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R.D. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory* **2008**, *54*, 2493–2507. [CrossRef]
23. Anjos, G.; Castanheira, D.; Silva, A.; Gameiro, A.; Gomes, M.; Vilela, J.P. Exploiting the Reciprocal Channel for Discrete Jamming to Secure Wireless Communications Against Multiple-Antenna Eavesdropper. *IEEE Access* **2018**, *6*, 33410–33420. [CrossRef]
24. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2006.