

Secure Compute-and-Forward Transmission With Artificial Noise and Full-Duplex Devices

Stefano Tomasin

Department of Information Engineering
University of Padova, Italy

Abstract—We consider a wiretap channel with an eavesdropper (Eve) and an honest but curious relay (Ray). Ray and the destination (Bob) are full-duplex (FD) devices. Since we aim at not revealing information on the secret message to the relay, we consider the scaled compute-and-forward (SCF) where scaled lattice coding is used in the transmission by both the source (Alice) and Bob in order to allow Ray to decode only a linear combination of the two messages. At the same time Ray transmits artificial noise (AN) to confuse Eve. When Ray relays the decoded linear combination, Alice and Bob are transmitting AN against Eve. This can be a 5G cellular communication scenario where a mobile terminal (MT) aims at transmitting a secret message to a FD base station (BS), with the assistance of a network FD relay. With respect to existing literature the innovations of this paper are: a) Bob and Ray are FD devices; b) Alice, Ray and Bob transmit also AN; and c) the channel to Eve is not known to Alice, Bob and Ray. For this scenario we derive bounds on both the secrecy outage probability under Rayleigh fading conditions of the channels to Eve, and the achievable secrecy-outage rates.

Index Terms—Confidentiality; Full-Duplex; Physical layer security; Relays; Security.

I. INTRODUCTION

The next generation of mobile communication systems (5G) will most probably encompass various technological innovations, including among others, full-duplex (FD) devices [1] and multi-hop (relayed) transmissions. It has also been advocated [2] that security should be extended at the physical layer using, as a complement to traditional computational security, physical layer security (PLS) approaches.

In this paper we focus on PLS solutions for a relay-assisted communication, where both the relay and the destination are FD devices. It has already been shown the advantage of cooperation (relaying) for physical layer security [3], which motivates the focus on this approach. This scenario arises for example in a cellular 5G system, where a mobile terminal (MT) aims at transmitting a secret message to a FD base station (BS), with the assistance of a network FD relay. This scenario has been considered in the literature: for example, for FD relay see [4], [5] and references therein. In [6] an unauthenticated relay was considered (to be kept in the darkness of the secret message), and the destination sent artificial noise (AN) during the source's transmission, and both an upper bound on the secret rate and achievable rates were derived. When the relay is secure, linear precoding schemes can be applied on a decode and forward (DF) transmission with AN [7]. amplify and forward (AF) relaying and simultaneous

jamming by other nodes has been considered in [8] where selection of relay and jamming nodes has been addressed.

The case of FD destination without relaying is considered in [9] in the absence of channel-state information (CSI) on the eavesdropper channel, and in [10] under various CSI assumptions on the legitimate and eavesdropper channels. The case of a communication between single-antenna devices assisted by a multi-antenna FD relay is considered in [11], where joint information and jamming beamforming are designed to guarantee secrecy. A DF solution for FD relaying is also considered in [12] showing the advantages of FD over half-duplex (HD) network solutions. The multi-source multi-relay scenario has been considered in various papers (see [13] and references therein), with and without AF/DF and various knowledge of the CSI of the eavesdropper channel, and selection of sources and relays have been optimized. In [14] a modulo-and-forward is considered for a single relay without eavesdropper, and in the case of no CSI the outage probability is derived. In [15] a scaled compute-and-forward (SCF) was introduced, and the presence of an eavesdropper was also considered. However the source and destination nodes perfectly know the CSI to the eavesdropper, which is not always a realistic assumption.

In this paper we consider that both Ray and Bob are FD. Since we aim at not revealing information on the secret message to the relay, we consider the SCF. At the same time Ray transmits AN to confuse Eve. When Ray relays the decoded linear combination, Alice and Bob are transmitting AN against Eve. With respect to existing literature the innovations of this paper are: a) Bob and Ray are FD devices; b) Alice, Ray and Bob transmit also AN; and c) the channel to Eve is not known to Alice, Bob and Ray. For this scenario we derive a bound on the secrecy outage probability. In particular, for the case of Rayleigh fading conditions of the channels to Eve, we derive a close form expression of the secrecy outage probability bound.

II. SYSTEM MODEL

We consider a relay network with a device (Alice) willing to convey a message to another device (Bob), with the help of a relay (Ray). The message must remain secret to a potential passive eavesdropper (Eve), whose location (and even existence) is unknown to both Alice and Bob. Ray is always honest, thus he complies with the transmission protocol rules and aims at supporting Alice and Bob at best. However, he is curious, i.e., willing to know the secret message: thus the

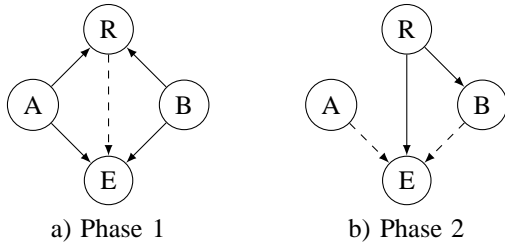


Figure 1. Transmissions in the two phases of the proposed scheme among Alice (A), Bob (B), Ray (R) and Eve (E). Solid lines represent transmission of messages, while dashed lines represent AN transmissions.

communication protocol ensures that the message remains secret also to him. In any case, Eve and Ray are not colluding to get information on the secret message.

Both Alice and Eve¹ are assumed to be HD devices, while both Bob and Ray have FD capabilities. All users are equipped with a single antenna. The devices have a maximum unitary transmit power, and we assume that each receiver is subject to a zero-mean unitary-power additive white Gaussian noise (AWGN). Extension to the case of devices equipped with multiple antennas is left for future study.

We assume that there is no direct link between Alice and Bob, therefore the support of Ray is needed. Among antennas we have flat, reciprocal and AWGN channels. So that the complex channel between users are for the Alice/Bob-Ray channel G_x with $x = A$ or B , and for Alice/Bob-Ray-Eve channel Q_x with $x = A$ or B or R . Since we assume that the relay is curious but honest, we assume that he let Alice and Bob perfectly know the correct channel gains. On the other hand, Eve is not honest and we only assume to know the statistics of its channel to both Alice and Bob.

III. SECURE COMMUNICATION PROTOCOLS

The communication protocol is based on SCF. Starting from a lattice Λ , we construct two lattices $\Lambda_A, \Lambda_B \subset \Lambda$, having unitary second moment, being good in both quantizing and shaping sense of [16]. Let \mathcal{V}_A and \mathcal{V}_B be the fundamental Voronoi region of Λ_A and Λ_B , respectively. Let also $a_1, a_2 \in \mathbb{Z}$, and $\beta_A, \beta_B \in \mathbb{R}^+$.

The protocol comprises two phases, whose transmission activities are reported in Fig. 1. Solid lines represent transmission of messages, while dashed lines represent transmissions of AN. In both phases Eve listens to ongoing transmissions. The other devices operate as follows.

First phase:

- Alice encodes message \mathcal{M}_A of rate R_S by applying the random binning approach of [15] and selecting a lattice vector $S^A \in \Lambda \cap \mathcal{V}^A$. Then she transmits the lattice vector $X^A = [S^A/\beta_A + D^A] \pmod{\Lambda_A/\beta_A}$, where D^A is dither uniformly chosen from the scaled Voronoi region

¹Since we are considering Eve as a *passive* eavesdropper, nothing changes if we assume that she is FD.

\mathcal{V}_A/β_A . Let R_0 be the random signal rate and

$$R_A = R_0 + R_S \quad (1)$$

the rate of S^A .

- Bob encodes a random message with rate R_B $V^B \in \Lambda \cap \mathcal{V}^B$ chosen uniformly at random, and the transmitted vector is $X^B = [V^B/\beta_B + D^B] \pmod{\Lambda_B/\beta_B}$, where D^B is dither uniformly chosen from the scaled Voronoi region \mathcal{V}_B/β_B .
- Ray is receiving the signal from Alice and Bob and at the same time is transmitting zero-mean Gaussian AN.

Second phase:

- Alice transmits AN.
- Ray decodes

$$U = a_1 S^A + a_2 V^B \quad (2)$$

(conditions for successful decoding will be discussed in the following section), and computes $\tilde{U} = U/a_1 \pmod{\Lambda^A}$. Then he encodes \tilde{U} with a secrecy capacity achieving code using a random message with rate R_R , and transmits the encoded message X^R with rate $R_R + R_A$.

- Bob receives the message from Ray, and at the same time transmits zero-mean Gaussian AN.

We want Bob to decode the secret message at the end of the two phases, by letting at the same time Ray and Eve in the darkness of the secret message. The purpose of transmissions of message \mathcal{M}_B and ANs is to obtain secrecy. Ray, beyond operating according to the protocol, will also try to get information on the secret message. Note that the AN generated by Alice in the second phase does not affect Bob, since Bob does not receive signals from Alice.

This protocol is a generalization of the protocol described in [15] for the following reasons: a) Bob and Ray are FD devices; b) Alice, Ray and Bob transmit also AN; and c) the channel to Eve is not known to Alice, Bob and Ray.

In the following we assume that the achievable rate of the resulting Ray-Bob channel is higher than that of the Alice-Ray channel, in the absence of Bob transmissions².

A. Decodability Conditions

We first consider here the conditions on the various parameters (a_1, a_2, β_A and β_B) and rates (R_A and R_B) that ensure decodability of the secret message S^A at Bob. Let

$$\delta_A = |G_A|^2, \quad \delta_B = |G_B|^2, \quad (3)$$

be the signal to noise ratios (SNRs) of the Alice-Ray and Bob-Ray channel, respectively.

For decodability with vanishing error probability at Ray of U with infinite codeword length we must have [15]

$$R_A \leq \log_2 \left(\frac{\beta_A^2 \delta_A}{M_N} \right), \quad R_B \leq \log_2 \left(\frac{\beta_B^2 \delta_B}{M_N} \right) \quad (4)$$

²Generalization to any ratio of power is possible, with more elaborate expressions.

where

$$M_N = \frac{\delta_A \delta_B (a_1 \beta_A - a_2 \beta_B)^2 + (a_1 \beta_A)^2 \delta_A^2 + (a_2 \beta_B)^2 \delta_B^2}{\delta_A + \delta_B + 1}. \quad (5)$$

For decodability of the secret message sent by Ray in the second phase we must ensure

$$\log_2(1 + \delta_B^2) \geq R_R + R_A. \quad (6)$$

IV. ACHIEVABLE SECRECY RATE

We now consider the secrecy conditions for the proposed protocol. We will first consider the case without Eve, where we only want to let Ray not to get any information on \mathcal{M}_A , and then consider the case in which Eve is also present and we want to let her too in the darkness of the secret message.

A. Achievable Secrecy Rate Without Eve

We assume now that Eve is not present. Then, the protocol must ensure perfect secrecy only with respect to Ray.

The resulting system corresponds to the scenario of [15] for which the achievable secrecy rate is bounded as

$$R_S \leq \log_2 \frac{1 + \delta_A + \delta_B}{[\sqrt{(1 + \delta_A)(1 + \delta_B)} - \sqrt{\delta_A \delta_B}]^2} - 2, \quad (7)$$

with the maximum achieved with $a_1 = a_2 = 1$ and

$$\frac{\beta_1}{\beta_2} = \sqrt{\frac{\delta_B(1 + \delta_A)}{\delta_A(1 + \delta_B)}}. \quad (8)$$

B. Achievable Secrecy Rate With Eve

Since here we assume that legitimate users only have a statistical description of the channel to Eve, we cannot employ the approach of [15] that imposed that a linear combination of messages \mathcal{M}_A and \mathcal{M}_B was also decodable by Eve. Moreover, we should also take into account the fact that Eve receives the message sent by Ray.

About Eve, we only aim at preventing her from getting information on the secret message, not caring if she decode some liner combination of \mathcal{M}_A and \mathcal{M}_B . Therefore two actions will be taken:

- in the first phase Ray transmits AN that will lower the decoding capabilities of Eve, and
- in the second phase Ray encodes with a random binning approach his message.

These two actions will not be enough to guarantee that Eve does not get any information on the secret message. There will be in any case an outage event, i.e., the event in which Eve gets some information on \mathcal{M}_A . We can upper-bound this outage probability by computing the probability that either Eve is able to get some information from either the first phase or the second phase. Let \mathcal{O}_i be the outage event in phase $i = 1, 2$. We will derive a superset of the outage event in the first phase, i.e., $\mathcal{O}_1 \subseteq \bar{\mathcal{O}}_1$, and we will upper-bound the outage probability as

$$P_{\text{out}} = 1 - \mathbb{P}[\mathcal{O}_1^C, \mathcal{O}_2^C] \leq 1 - \mathbb{P}[(\bar{\mathcal{O}}_1)^C, \mathcal{O}_2^C], \quad (9)$$

where \mathcal{A}^C represents the complementary event to event \mathcal{A} .

Remark: We will ensure that in the second phase Eve does not get information on both \mathcal{M}_A and \mathcal{M}_B , since a leakage on \mathcal{M}_B could help her in extracting information on \mathcal{M}_A from what she received in the first phase.

Remark: We still need to ensure that Ray does not get any information on the secret message, hence (7) must still hold.

We now detail the actions and the corresponding secrecy outage probabilities.

First Phase: Let Y^E be the signal received by Eve in the first phase. The information leakage rate on \mathcal{M}_A to Eve is

$$\begin{aligned} R_L &= \frac{1}{N} I(\mathcal{M}_A; Y^E) \\ &= \frac{1}{N} [H(\mathcal{M}_A) - H(X^A, X^B | Y^E) \\ &\quad - H(\mathcal{M}_A | Y^E, X^A, X^B) + H(X^A, X^B | Y^E, \mathcal{M}_A)] \quad (10) \\ &= \frac{1}{N} [H(\mathcal{M}_A) - H(X^A, X^B) + I(X^A, X^B; Y^E) \\ &\quad + H(X^B) - I(X^B; Y^{E'})] \end{aligned}$$

where $H(\cdot)$ and $I(\cdot; \cdot)$ are the entropy and the mutual information, and in the second line we observe that if Eve knows \mathcal{M}_A she can subtract X^A from Y^E (to obtain $Y^{E'}$), and $H(X^A, X^B | Y^E, \mathcal{M}_A) = H(X^B | Y^E)$ (since by knowing \mathcal{M}_A she also knows X^A). We thus obtain the upper bound

$$R_L < \frac{1}{N} [I(X^A, X^B; Y^E) - I(X^B; Y^{E'})]. \quad (11)$$

Now, from the definition of the capacity of the multiple access channel (MAC) from Alice and Bob to Eve $C_{MAC}(X^A, X^B; Y^E)$ (considering also the AN transmitted by Ray) we have

$$R_L < C_{MAC}(X^A, X^B; Y^E) - \frac{1}{N} I(X^B; Y^{E'}). \quad (12)$$

Unfortunately, it is hard to lower bound $I(X^B; Y^{E'})$. We can consider two cases, either Eve is able to decode \mathcal{M}^B from $Y^{E'}$, or not. Considering the lattice coding, from [17] the first case occurs if $R_B \leq C(X^B; Y^{E'})$ where $C(X^B; Y^{E'}) = \max I(X^B; Y^{E'})$ and we have

$$R_L \leq C_{MAC}(X^A, X^B; Y^E) - R_B. \quad (13)$$

On the other hand, if Eve is not able to decode \mathcal{M}_B we can only upper bound R_L as follows

$$R_L \leq C_{MAC}(X^A, X^B; Y^E). \quad (14)$$

Since Alice applies random binning, a subset $(\bar{\mathcal{O}}_1)^C \subset \bar{\mathcal{O}}_1^C$ of the *non secrecy-outage* event is given by

$$\begin{aligned} (\bar{\mathcal{O}}_1)^C &= \mathcal{S}_1 \cup \mathcal{S}_2 = \\ &\quad \{C_{MAC}(X^A, X^B; Y^E) - R_B \leq R_0, \\ &\quad C(X^B; Y^{E'}) \geq R_B\} \cup \\ &\quad \{C_{MAC}(X^A, X^B; Y^E) \leq R_0, C(X^B; Y^{E'}) \leq R_B\}. \end{aligned} \quad (15)$$

Therefore (9) becomes

$$P_{\text{out}} \leq 1 - (P[\mathcal{S}_1, \mathcal{O}_2^C] + P[\mathcal{S}_2, \mathcal{O}_2^C]). \quad (16)$$

Second Phase: In the second phase we aim at preventing Eve from getting any information on both \mathcal{M}_A and \mathcal{M}_B . Alice and Bob transmit AN and Ray will employ random binning. Note that we cannot utilize the randomness of the first phase for secrecy purposes, since Eve may have decoded the randomness of the first phase (while not being able of getting any information on the secret message) and can exploit this knowledge in the second phase. This is why we need a second random binning process. Therefore we have a secrecy outage event when

$$C(X^R; \bar{Y}) \geq R_R, \quad (17)$$

where \bar{Y} is the signal received by Eve in the second phase.

C. Rayleigh Fading Scenario

We now derive the close form expression of the secrecy outage probability bound for the case in which all links with Eve are characterized by Rayleigh fading. In particular, let $1/\lambda_A$, $1/\lambda_B$, and $1/\lambda_R$ be the average SNR of the links between Eve and Alice, Bob and Ray, respectively.

Denoting the scalars $q_A = |Q_A|^2$, $q_B = |Q_B|^2$, $q_R = |Q_R|^2$, we have $C_{MAC}(X^A, X^B; Y^E) = \log_2 \left(1 + \frac{q_A + q_B}{1 + q_R} \right)$ and

$$\begin{aligned} \mathcal{S}_1 = & \left\{ \log_2 \left(1 + \frac{q_A + q_B}{1 + q_R} \right) \leq R_0 + R_B, \right. \\ & \left. \log_2 \left(1 + \frac{q_B}{1 + q_R} \right) \geq R_B \right\} = \\ & \{q_A + q_B \leq \mu(1 + q_R), q_B \geq \nu(1 + q_R)\}, \end{aligned} \quad (18)$$

with $\mu = 2^{R_0 + R_B} - 1$ and $\nu = 2^{R_B} - 1$, and analogously

$$\begin{aligned} \mathcal{S}_2 = & \{q_A + q_B - \mu'q_R \leq \mu', q_B - \nu q_R \leq \nu\} \\ = & \left\{ q_R \geq \max \left(\frac{q_A + q_B - \mu'}{\mu'}, \frac{q_B - \nu}{\nu} \right) \right\}, \end{aligned} \quad (19)$$

with $\mu' = 2^{R_0} - 1$.

For the second phase we have $C(X^R; \bar{Y}) = \log_2 \left(1 + \frac{q_R}{1 + q_A + q_B} \right)$, and

$$\begin{aligned} \mathcal{O}_2^C = & \left\{ \log_2 \left(1 + \frac{q_R}{1 + q_A + q_B} \right) \leq R_R \right\} = \\ & \{q_R - \phi(q_A + q_B) \leq \phi\} \\ & \left\{ q_A + q_B \geq \frac{q_R}{\phi} - 1 \right\}, \end{aligned} \quad (20)$$

with $\phi = 2^{R_R} - 1$. Hence we have

$$P[\mathcal{O}_1^C, \mathcal{O}_2^C] = P[\mathcal{S}_1, \mathcal{O}_2^C] + P[\mathcal{S}_2, \mathcal{O}_2^C]. \quad (21)$$

We observe that $\mathcal{S}_1 \mathcal{O}_2^C \neq \emptyset$ if

$$\frac{q_R}{\phi} - 1 \leq \mu q_R + \mu, \quad (22)$$

which always occurs if $\mu\phi \geq 1$, while it requires

$$q_R \leq \frac{\phi + \mu\phi}{1 - \mu\phi} = \gamma \quad \text{if } \mu\phi < 1. \quad (23)$$

Moreover, condition \mathcal{O}_2^C has no effect if

$$\frac{q_R}{\phi} - 1 \leq \nu q_R + \nu, \quad (24)$$

which always occurs if $\nu\phi \geq 1$, and which occurs when

$$q_R \leq \frac{\phi + \nu\phi}{1 - \phi\nu} = \delta, \quad \text{if } \nu\phi < 1. \quad (25)$$

Considering the definition of $Z(A, B, C, D, C', D', E, F, F)$ in (26)-(36) reported in the next page, Therefore we have the following cases

- 1) **Case** $\mu\phi \geq 1$ **and** $\phi\nu < 1$. This will lead to $P[\mathcal{S}_1, \mathcal{O}_2^C] = Z(0, \delta, \mu, \mu, \nu, \nu, 0, \mu) + Z(\delta, \infty, 1/\phi, -1, \nu, \nu, 1, \mu) + Z(\delta, \infty, \mu, \mu, 1/\phi, -1, 0, \mu)$.
- 2) **Case** $\mu\phi \geq 1$ **and** $\phi\nu \geq 1$. This will lead to $P[\mathcal{S}_1, \mathcal{O}_2^C] = Z(0, \infty, \mu, \mu, \nu, \nu, 0, \mu)$.
- 3) **Case** $\mu\phi < 1$. This will imply $\phi\nu < 1$ and will lead to $P[\mathcal{S}_1, \mathcal{O}_2^C] = Z(0, \delta, \mu, \mu, \nu, \nu, 0, \mu) + Z(\delta, \gamma, 1/\phi, -1, \nu, \nu, 1, \mu) + Z(\delta, \gamma, \mu, \mu, 1/\phi, -1, 0, \mu)$.

We observe that $\mathcal{S}_2 \mathcal{O}_2^C \neq \emptyset$ if either $\mu'\phi \geq 1$ and $\nu\phi \geq 1$, or $\mu'\phi < 1$, $\nu\phi \geq 1$ and

$$q_R \leq \frac{\phi + \mu'\phi}{1 - \mu'\phi} = \gamma', \quad (37)$$

or $\mu'\phi \geq 1$, $\nu\phi < 1$ and $q_R \leq \delta$, or $\mu'\phi < 1$, $\nu\phi < 1$ and $q_R \leq \min\{\delta, \gamma'\}$.

Moreover, condition \mathcal{O}_2^C has no effect if $q_R < \phi$. Lastly, if $\mu' \leq \nu$, \mathcal{S}_2 reduces to $\mathcal{S}_2 = \{q_A + q_B - \mu'q_R \leq \mu'\}$ (the other bound has no effect). Therefore we have the following cases

- 1) **Case** $\mu'\phi \geq 1$, $\mu' > \nu$ **and** $\phi\nu \geq 1$. This will lead to $P[\mathcal{S}_2, \mathcal{O}_2^C] = Z(0, \phi, \nu, \nu, 0, 0, 0, \mu') + Z(\phi, \infty, 1/\phi, -1, 0, 0, 1, \mu') + Z(\phi, \infty, \nu, \nu, 1/\phi, -1, 0, \mu')$.
- 2) **Case** $\mu'\phi \geq 1$, $\mu' > \nu$ **and** $\phi\nu < 1$. This will lead to $P[\mathcal{S}_2, \mathcal{O}_2^C] = Z(0, \phi, \nu, \nu, 0, 0, 0, \mu') + Z(\phi, \delta, 1/\phi, -1, 0, 0, 1, \mu') + Z(\phi, \delta, \nu, \nu, 1/\phi, -1, 0, \mu')$.
- 3) **Case** $\mu'\phi \geq 1$ **and** $\mu' \leq \nu$. This will lead to $P[\mathcal{S}_2, \mathcal{O}_2^C] = Z(0, \phi, \mu', \mu', 0, 0, 0, \mu') + Z(\phi, \infty, 1/\phi, -1, 0, 0, 1, \mu') + Z(\phi, \infty, \mu', \mu', 1/\phi, -1, 0, \mu')$.
- 4) **Case** $\mu'\phi < 1$ **and** $\mu' > \nu$. This will lead to $P[\mathcal{S}_2, \mathcal{O}_2^C] = Z(0, \phi, \nu, \nu, 0, 0, 0, \mu') + Z(\phi, \min\{\gamma', \delta\}, 1/\phi, -1, 0, 0, 1, \mu') + Z(\phi, \min\{\gamma', \delta\}, \nu, \nu, 1/\phi, -1, 0, \mu')$.
- 5) **Case** $\mu'\phi < 1$ **and** $\mu' \leq \nu$. This will lead to $P[\mathcal{S}_2, \mathcal{O}_2^C] = Z(0, \phi, \mu', \mu', 0, 0, 0, \mu') + Z(\phi, \gamma', 1/\phi, -1, 0, 0, 1, \mu') + Z(\phi, \gamma', \mu', \mu', 1/\phi, -1, 0, \mu')$.

$$Z(A, B, C, D, C', D', E, F) = \lambda_A \lambda_B \lambda_R \int_{q_R=A}^B \int_{q_B=Dq_R+C'}^{Cq_R+C'} \int_{q_A=E(q_R/\phi-1-q_B)}^{Fq_R+F-q_B} e^{-\lambda_B q_B} e^{-\lambda_A q_A} e^{-\lambda_R q_R} dq_A dq_B dq_R =$$

$$- \lambda_B \lambda_R \int_{q_R=A}^B e^{-\lambda_R q_R} \int_{q_B=Dq_R+C'}^{Cq_R+C'} e^{-\lambda_B q_B} \left[e^{-\lambda_A [Fq_R+F-q_B]} - e^{-\lambda_A E(q_R/\phi-1-q_B)} \right] dq_B dq_R \quad (26)$$

$$Z_{x,1}(A, B, C, D, C', D', E, F) = \frac{\lambda_B \lambda_R e^{-\lambda_A F}}{\lambda_A - \lambda_B} \left\{ \frac{e^{(\lambda_A - \lambda_B)x'}}{(\lambda_A - \lambda_B)x - \lambda_R - \lambda_A F} \left[e^{((\lambda_A - \lambda_B)x - \lambda_R - \lambda_A F)B} - e^{((\lambda_A - \lambda_B)x - \lambda_R - \lambda_A F)A} \right] \right\} \quad (27)$$

$$X_{x,1}(A, B, C, D, C', D', E, F) = \frac{\lambda_B \lambda_R e^{\lambda_A E}}{\lambda_A E - \lambda_B} \left\{ \frac{e^{(\lambda_A E - \lambda_B)x'}}{(\lambda_A E - \lambda_B)x - \lambda_R - \frac{\lambda_A E}{\phi}} \left[e^{((\lambda_A E - \lambda_B)x - \lambda_R - \frac{\lambda_A E}{\phi})B} - e^{((\lambda_A E - \lambda_B)x - \lambda_R - \frac{\lambda_A E}{\phi})A} \right] \right\} \quad (28)$$

$$Z_2(A, B, C, D, C', D', E, F) = \frac{\lambda_B \lambda_R e^{-\lambda_A F} (C - D)}{-(\lambda_R + \lambda_A F)^2} \{ e^{-(\lambda_R + \lambda_A F)B} [(\lambda_R + \lambda_A F)(B + \frac{C' - D'}{C - D}) + 1] - e^{-(\lambda_R + \lambda_A F)A} [(\lambda_R + \lambda_A F)(A + \frac{C' - D'}{C - D}) + 1] \} \quad (29)$$

$$X_2(A, B, C, D, E, F) = \frac{\lambda_B \lambda_R e^{\lambda_A E} (C - D)}{-(\lambda_R + \lambda_A E/\phi)^2} \{ e^{-(\lambda_R + \lambda_A E/\phi)B} [(\lambda_R + \lambda_A E/\phi)(B + \frac{C' - D'}{C - D}) + 1] - e^{-(\lambda_R + \lambda_A E/\phi)A} [(\lambda_R + \lambda_A E/\phi)(A + \frac{C' - D'}{C - D}) + 1] \} \quad (30)$$

$$Z_{x,2}(A, B, C, D, C', D', E, F) = \frac{\lambda_B \lambda_R e^{-\lambda_A F} e^{(\lambda_A - \lambda_B)x}}{\lambda_A - \lambda_B} (B - A), \quad X_{x,2}(A, B, C, D, C', D', E, F) = \frac{\lambda_B \lambda_R e^{\lambda_A E} e^{(\lambda_A E - \lambda_B)x}}{\lambda_A E - \lambda_B} (B - A), \quad (31)$$

$$Z_x(A, B, C, D, C', D', E, F) = \begin{cases} Z_{x,1}(A, B, C, D, C', D', E, F) & \text{if } (\lambda_A - \lambda_B)x - \lambda_R - \lambda_A F \neq 0 \\ Z_{x,2}(A, B, C, D, C', D', E, F) & \text{if } (\lambda_A - \lambda_B)x - \lambda_R - \lambda_A F = 0 \end{cases}, \quad x = C, D \quad (32)$$

$$X_x(A, B, C, D, C', D', E, F) = \begin{cases} X_{x,1}(A, B, C, D, C', D', E, F) & \text{if } (\lambda_A E - \lambda_B)x - \lambda_R - \frac{\lambda_A E}{\phi} \neq 0 \\ X_{x,2}(A, B, C, D, C', D', E, F) & \text{if } (\lambda_A E - \lambda_B)x - \lambda_R - \frac{\lambda_A E}{\phi} = 0 \end{cases}, \quad x = C, D \quad (33)$$

$$T_1(A, B, C, D, E, F) = \begin{cases} Z_C(A, B, C, D, C', D', E, F) - Z_D(A, B, C, D, C', D', E, F) & \text{if } \lambda_A - \lambda_B \neq 0, \\ Z_2(A, B, C, D, C', D', E, F) & \text{if } \lambda_A - \lambda_B = 0 \end{cases} \quad (34)$$

$$T_2(A, B, C, D, C', D', E, F) = \begin{cases} X_C(A, B, C, D, C', D', E, F) - X_D(A, B, C, D, C', D', E, F) & \text{if } \lambda_A E - \lambda_B \neq 0, \\ X_2(A, B, C, D, C', D', E, F) & \text{if } \lambda_A E - \lambda_B = 0 \end{cases} \quad (35)$$

$$Z(A, B, C, D, C', D', E, F) = T_2(A, B, C, D, C', D', E, F) - T_1(A, B, C, D, C', D', E, F). \quad (36)$$

V. NUMERICAL RESULTS

In order to show an example of performance of the considered system, we consider $\delta_A = 20$ dB, $\delta_B = 10$ dB. We first have spanned the value of β_A/β_B and found the achievable region of (R_A, R_B) couples, as shown in Fig. 2.

Then we set $\lambda_A = \lambda_R = 1$, and $\lambda_B = 2$, and $R_S = 0.1$ bit/s/Hz, and $R_R = 7$ bit/s/Hz. Fig. 3 shows the bound on the secrecy outage probability (in a log scale) as a function of R_A and R_B . Note that we have only shown the values of \bar{P}_{out} in correspondence of valid couples R_A and R_B that ensure the decodability conditions for the secret message at Bob, while not leaking any information to Ray. We also identify the couple (R_A, R_B) providing the minimum \bar{P}_{out} , which is about 10^{-5} .

In general, we observe that increasing R_A reduces the chances of leaking information to Eve in the first phase (since we can increase R_0). On the other hand, since Ray

transmits the secret message at rate R_A , we potentially have an information leakage in the second phase since the rate of the random message $R_R - R_A$ is decreased.

Fig. 4 shows the secrecy probability outage bound \bar{P}_{out} vs R_S for three values of R_R . R_A and R_B have been optimized to minimize \bar{P}_{out} . We observe that as R_S increases, the outage bound increases too, since the random message rates R_0 and $(R_R - R_A)$ in the two phases are reduced. Also, increasing R_R provides a lower \bar{P}_{out} since it allows to better protect the second phase, increasing the random message rate.

VI. CONCLUSIONS

We have considered a secure communication scenario where a secret message must be kept unknown both to a curious but honest device that relays the message to the destination, and to an eavesdropper. While the channel to the relay is known to the legitimate devices, the channel to the eavesdropper

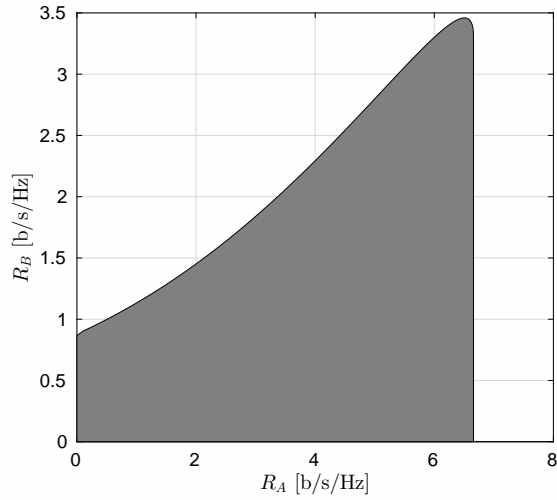


Figure 2. Achievable region of (R_A, R_B) pairs.

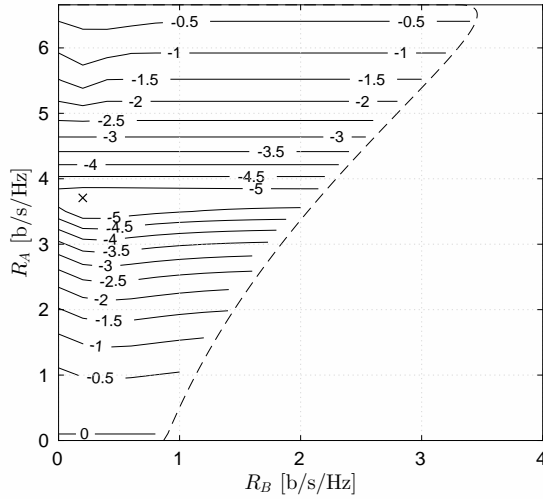


Figure 3. Contour plot of $\log_{10} \bar{P}_{\text{out}}$ as a function of R_A and R_B . Only values of R_A and R_B allows decodability conditions at Bob and secrecy at Ray are considered. The couple of (R_A, R_B) providing the minimum value of \bar{P}_{out} is shown with a cross

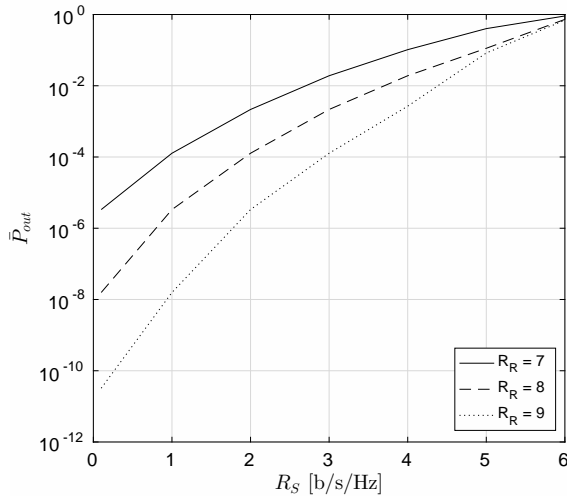


Figure 4. Secrecy probability outage bound \bar{P}_{out} vs R_S for three values of R_R . R_A and R_B have been optimized to minimize \bar{P}_{out} .

is not known, hence a secrecy outage event is possible. Considering FD devices and letting Ray transmit AN, we have described the protocol that mixes a SCF approach and a random binning approach to provide secrecy. Then the secrecy outage probability for a Rayleigh fading scenario has been computed in a close form. Lastly, some numerical results have provided an insight into the main features of the considered system.

REFERENCES

- [1] Zhongshan Zhang, Xiaomeng Chai, Keping Long, A. V. Vasilakos and L. Hanzo, "Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128-137, May 2015.
- [2] Nan Yang, Lifeng Wang, G. Geraci, M. Elkashlan, Jinhong Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, April 2015.
- [3] Hui-Ming Wang and Xiang-Gen Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47-53, Dec. 2015.
- [4] Xiaoming Chen, Caijun Zhong, Chau Yuen and Hsiao-Hwa Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40-46, Dec. 2015.
- [5] L. Jimenez Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32-39, Dec. 2015.
- [6] X. He and A. Yener, "Two-Hop secure communication using an untrusted relay: a Case for cooperative jamming," in *Proc. IEEE Global Telecomm. Conf. (GLOBECOM)*, New Orleans, LO, pp. 1-5, 2008.
- [7] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Proc.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.
- [8] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.
- [9] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Commun. Letters*, vol. 16, no. 10, pp. 1628-1631, Oct. 2012.
- [10] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Proc.*, vol. 61, no. 20, pp. 4962-4974, Oct. 15, 2013.
- [11] F. Zhu, F. Gao, M. Yao and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Proc.*, vol. 62, no. 24, pp. 6391-6401, Dec. 15, 2014.
- [12] G. Chen, Y. Gong, P. Xiao and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 3, pp. 574-583, March 2015.
- [13] L. Fan, N. Yang, T. Duong, M. Elkashlan, and G. Karagiannidis, "Exploiting direct links for physical layer security in multi-user multi-relay networks," *IEEE Trans. Wireless Commun.*, to appear, doi: 10.1109/TWC.2016.2530068.
- [14] Shengli Zhang, Lisheng Fan, Mugen Peng and H. Vincent Poor, "Near-optimal modulo-and-forward scheme for the untrusted relay channel", available online <http://arxiv.org/abs/1503.08928>.
- [15] Zhijie Ren, Jasper Goseling, Jos H. Weber and Michael Gastpar, "Secure transmission on the two-hop relay channel with scaled compute-and-forward," available online <http://arxiv.org/abs/1509.04075>.
- [16] U. Erez and R. Zamir, "Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, pp. 2293-2314, vol. 50, 2004.
- [17] Jingge Zhu and Michael Gastpar, "Asymmetric compute-and-forward with CSIT," in *Proc. Int. Zurich Seminar on Commun.* 2014, <http://dx.doi.org/10.3929/ethz-a-101095320>.