Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security

Nabil Romero-Zurita, Mounir Ghogho and Des McLernon

Abstract—In this letter we address physical layer security in MISO communications in the presence of passive eavesdroppers, i.e., the eavesdroppers’ channels are unknown to the transmitter. Spatial beamforming and artificial noise broadcasting are chosen as the strategy for secure transmission. With the aim of guaranteeing a given probability of secrecy, defined by quality of service constraints at the intended receiver and at the eavesdroppers, an optimum power allocation strategy between transmitted information and artificial noise is proposed. Both power constrained and power unconstrained systems are considered. Our proposed outage probability-based approach compares favourably to an existing second-order-statistic-based approach.

Index Terms—Beamforming, Artificial Noise, Physical Layer Security, Passive Eavesdropping, Secrecy.

I. INTRODUCTION

GIVEN the broadcast nature of wireless networks and the resulting security vulnerabilities such as eavesdropping, secure transmission techniques have received growing attention as a way to augment secrecy. One such approach is physical layer security which may prevent eavesdroppers’ attacks by exploiting the spatio-temporal variations of the wireless channel - a task that currently is partially performed by computationally demanding cryptographic algorithms.

Now, according to the fundamental concepts of information-theoretic security [1]–[3], the secrecy capacity for an AWGN channel is a function of the signal-to-noise ratios (SNRs) of the links between both transmitter to receiver and transmitter to eavesdropper. Indeed, secrecy capacity is greater than zero when the quality of the main channel is better than the eavesdropper’s counterpart. Thus, to calculate the secrecy capacity of the system and to guarantee a secure communication, the transmitter must know the channel state information (CSI) of both links. This description corresponds to the active eavesdropping scenario. Now, the passive eavesdropping case, where the eavesdropper’s CSI is not known at the transmitter, is indeed the most challenging problem and perfect secrecy cannot be guaranteed. One approach to deal with this situation is to use the concept of outage probability [4] which is defined as the probability that the instantaneous secrecy capacity falls below a predefined target secrecy rate. Another approach to define the secrecy of a system is to use quality-of-service (QoS) constraints on the SNRs of the legitimate and eavesdropper links based on statistics of the CSI [5], [6]. In [7] a probabilistic framework is presented to quantify the probability of secrecy in the presence of random network of eavesdroppers whose locations and channels are unknown.

Recently, a number of publications have highlighted the advantages of beamforming and artificial noise generation as a successful physical layer security strategies [5]–[9]. In [10], it was shown that beamforming is an optimal physical layer security transmission strategy for multiple-input-single-output (MISO) systems. In [5], beamforming and artificial noise generation were used to guarantee a given SNR at the intended receiver using only the minimum necessary power for information transmission while the remaining available power is allocated for noise broadcasting. This was also generalized to the case of a random network of eavesdroppers in [7] and to the case of frequency-selective channels in [9].

The QoS-based secure transmission approach in [6] is based on the first and second-order statistics of the CSIs, i.e., the QoS constraints are only enforced to be satisfied on average. In the case of a purely passive eavesdropper, the design [6] assumes that the first-order statistics of the CSI of the eavesdropper is zero and the covariance matrix is the identity matrix. In this letter, we take on outage probability approach, and we propose a transmission strategy that guarantees a minimum level of secrecy defined by the probability that the SNR at all eavesdroppers is below a maximum allowable value while satisfying a QoS requirement for the legitimate link. The proposed design provides better performance than [6] in the case of quasi-static channels.

II. SYSTEM AND SIGNAL MODELS

In this section, we formulate the power allocation problem with secrecy constraints for a MISO system using both beamforming as a transmit strategy and artificial noise to confuse unknown non-colluding eavesdroppers (i.e., eavesdroppers that do not work in a cooperative fashion). Following the well known cryptographic model, the legitimate transmitter and receiver are named Alice and Bob, and the eavesdroppers are collectively referred to as “the Eves.”

A. System Model

Alice is equipped with $N_t \geq 2$ antennas while Bob and each of the $K$ Eves have a single antenna. The channels between Alice and Bob (denoted by $\mathbf{h}_b$) is modelled as zero-mean complex Gaussian ($N_t \times 1$) vector whose elements are uncorrelated and have the same variance $\sigma^2_{h_b}$. The channel between Alice and the $k$th Eve ($\mathbf{h}_{ek}$) is similarly defined with elements’ variance $\sigma^2_{h_{ek}}$. Furthermore, the legitimate and eavesdropping channels are mutually independent. We also assume that $\mathbf{h}_b$ is perfectly known to Alice and considering pure passive eavesdropping, the $\mathbf{h}_{ek}$’s are unknown to Alice. So let $\mathbf{s}$ denote the beamformed signal vector transmitted by Alice and thus the scalar signals received by Bob and the $k$th Eve are respectively given by:

$$u = \mathbf{h}_b^H \mathbf{s} + n_b$$
$$v_k = \mathbf{h}_{ek}^H \mathbf{s} + n_{ek}$$

where $n_b$ and $n_{ek}$ are mutually independent, zero-mean, complex, Gaussian noise with variances $\sigma^2_n$ and $\sigma^2_{n_{ek}}$. Now $\mathbf{C}_s = \mathbb{E}\{\mathbf{s}\mathbf{s}^H\}$ denotes the covariance matrix of $\mathbf{s}$ and $P = \text{Tr}(\mathbf{C}_s)$ is the total transmitted power. We also introduce the scalar variables $a$ and $b$ that define the absolute power allocated for both information and artificial noise such that $P = a + b$. Thus the transmitted signal vector $\mathbf{s}$ can be modelled as follows:

$$\mathbf{s} = \sqrt{a} \mathbf{t} + \sqrt{b} \boldsymbol{\eta}$$
where \( t \) is the normalized \((N_t \times 1)\) beamforming vector s.t. \(|t| = 1\); \(d\) is the transmitted scalar complex information symbol with \(E\{\|d\|^2\} = 1\); and \( \eta \) is the \((N_t \times 1)\) artificial noise vector with covariance matrix \( C_\eta = E\{\eta \eta^H\} \) s.t. \( Tr(C_\eta) = 1 \).

The aim of this technique is to confuse the eavesdroppers by broadcasting noise in all the directions except towards Bob. So following [7], Alice chooses the beamforming vector \( t \) (in (3)) as the principal eigenvector \( (t_1) \) corresponding to the largest eigenvalue of \( h_b h_b^H \). The artificial noise vector \( \eta \) is then obtained by the linear combination of the remaining \( N_t - 1 \) eigenvectors (i.e., \( \eta \) will lie in the nullspace of \( h_b \)). In this way orthogonality between the artificial noise vector and the beamformer is preserved (i.e., \( t_1^H \eta = 0 \)). So with uniform power distribution among the remaining \( N_t - 1 \) eigenvectors \( \{t_i\}_{i=2}^{N_t} \), then \( \eta \) is generated as follows:

\[
\eta = \frac{1}{\sqrt{N_t - 1}} \sum_{i=2}^{N_t} t_i \eta_i
\]

where \( t_i \) is the \( i \)th eigenvector of \( h_b h_b^H \), and \( \eta_i \) is a random, complex scalar with unit magnitude and random phase uniformly distributed, (i.e., \( \eta_i = e^{j\phi_i} \) and \( \phi_i \in [0, 2\pi) \)). So we have:

\[
C_\eta = \frac{1}{N_t - 1} \sum_{i=2}^{N_t} t_i t_i^H.
\]

Finally, the received SNRs at both Bob and the \( k \)th Eve are easily derived as:

\[
\text{SNR}_b = \frac{a \|h_b\|^2}{\sigma_b^2}
\]

\[
\text{SNR}_{ek} = a t_1^H h_b e_k \left[ b h_b^H C_\eta h_b e_k + \sigma_e^2 \right]^{-1} h_b^H t_1.
\]

**B. Secrecy Constraints and Power Allocation Programming Problem**

Now, as we have already alluded to in the Introduction, one approach for obtaining a minimum level of secrecy when we do not have all the Eves’ CSIs at the transmitter, is to minimize the transmitted power \((P = a + b)\) while also enforcing a minimum SNR at Bob and ensuring (probabilistically) that the SNR at each eavesdropper is appropriately upper bounded.

Thus we want to find the optimal power allocation strategy to guarantee a given probability of secrecy \( \beta \in [0, 1] \) satisfying the quality constraints \( \gamma_b \) and \( \gamma_e \). That is:

\[
\begin{align*}
\min_{a,b} & \quad a + b \\
\text{s.t.} & \quad \text{SNR}_b \geq \gamma_b \\
& \quad \mathbb{P}[\text{SNR}_{e_1} \leq \gamma_e, \cdots, \text{SNR}_{e_k} \leq \gamma_e] \geq \beta \\
& \quad a > 0, b \geq 0
\end{align*}
\]

where \( \mathbb{P}[\cdot] \) refers to an event probability.

For the power constrained system, we can define a maximum transmit power for Alice \((P_{\text{max}})\). In the case where the solution to the above is more than the maximum available power, (i.e., \( a + b > P_{\text{max}} \)), we will consider that the problem is infeasible. In this case, Alice does not transmit any information for that one particular channel realization and, as we will later observe, this reduces the overall throughput.

Since all \( h_{e_k} \) are mutually independent then, after dropping “\( k \)” for \( \text{SNR}_{e_k} \), (8c) simplifies to:

\[
(\mathbb{P}[\text{SNR}_e \leq \gamma_e])^K \geq \beta.
\]

Now using (6), (7) and (9), then (8) now becomes:

\[
\begin{align*}
\min_{a,b} & \quad a + b \\
\text{s.t.} & \quad a \|h_b\|^2 \left[ \sigma_b^2 \right]^{-1} \geq \gamma_b \\
& \quad \mathbb{P}\left[a t_1^H h_b \left[ b h_b^H C_\eta h_b + \sigma_e^2 \right]^{-1} h_b^H t_1 \leq \gamma_e\right] \geq \beta \\
& \quad a > 0, b \geq 0
\end{align*}
\]

**Lemma 1:** After re-arranging, (10c) can be written in terms of a random Hermitian quadratic form \( Y = h_b^H A h_b \), whose cumulative distribution function (CDF) for \( y \geq 0 \) is given by:

\[
F_Y(y) = 1 - \frac{1}{\left(1 + \frac{b}{\gamma_e} \pi \sqrt{\frac{\gamma_e}{\sigma_e^2}}\right)^{N_t - 1}} e^{-\frac{\gamma_e y}{\pi \sigma_e^2}} + \pi y, \quad y \geq 0.
\]

where

\[
A = \frac{a}{\gamma_e} t_1 t_1^H - b C_\eta.
\]

Note that we are not interested in the more complicated expression for \( F_Y(y) \) when \( y < 0 \).

**Proof:** See appendix A.

So (10) can now be re-written as:

\[
\begin{align*}
\min_{a,b} & \quad a + b \\
\text{s.t.} & \quad a \|h_b\|^2 \left[ \sigma_b^2 \right]^{-1} \geq \gamma_b \\
& \quad \mathbb{P} \left[ a t_1^H h_b \left[ b h_b^H C_\eta h_b + \sigma_e^2 \right]^{-1} h_b^H t_1 \leq \gamma_e \right] \geq \beta \\
& \quad a > 0, b \geq 0
\end{align*}
\]

where (13c) is simply \( F_Y(\sigma_e^2) \) in (11) (i.e., following the definition in (15)).

The above problem is now easily solved for the optimum \( a \) and \( b \) to give:

\[
\begin{align*}
\alpha = a^* = \frac{\gamma_b \sigma_e^2}{\|h_b\|^2} \\
\beta = b^* = \max \left\{0, \frac{\alpha^* (N_t - 1)}{\gamma_e} \right\}
\end{align*}
\]

***III. Simulation Results***

In this section we will present simulation results that measure the achieved secrecy probability, the secrecy throughput and the power distribution for two scenarios. The first one does not consider any constraint on the total power available (i.e., \( P \in [0, \infty) \)) while the second approach considers the practical case where the power available at the transmitter is limited (i.e., \( P \in [0, P_{\text{max}}] \)).

Now, in order to evaluate the performance of our proposed power allocation method, we need to compare with a technique that is also using similar QoS constraints to define the secrecy of the system. One such technique appears in [6], but unlike our approach, all the Eves’ CSIs’s in (8c) are now available at the transmitter and the artificial noise is transmitted towards the Eves’ directions rather that in an isotropic fashion.

So, in order to compare “like with like” under the same passive eavesdropping case, [6] includes the option to use only knowledge of the eavesdroppers’ correlation matrix at Alice (which we also assume in this paper, i.e., \( E\{h_b h_b^H\} = \sigma_e^2 I \)) and the instantaneous value of \( h_b \).
Now for the simulations, three eavesdroppers are considered ($K = 3$) with the same channel and noise conditions, so eavesdroppers’ indexes can again be omitted. We set channel variances to $\sigma_{h_b}^2 = \sigma_{h_e}^2 = 1$. The noise power is the same for Bob and all the Eves, i.e., $\sigma_{e}^2 = \sigma_{e'}^2 = 1$ in (1) and (2). For the power constrained system we set $P_{\text{max}} = 6$ and 200,000 Monte Carlo runs are considered. The SeDuMi solver [11] and the YALMIP modelling tool [12] are also used to implement the reference technique’s algorithm [6]. Finally, in all the simulations our proposed method and the reference technique are referred to as “Prop:” and “Ref:” respectively.

In Fig. 1 the achieved probability of secrecy resulting from the proposed power allocation technique in (14) is shown when the target probability of secrecy $\beta$ in (8c) varies from 0.05 to 0.95. From the graphs it is clear that our approach guarantees the intended probability of secrecy $\beta$ while the reference technique can only offer a fixed (constant) probability of secrecy that does not depend on the power available at the transmitter. Indeed, the reference technique has a maximum achieved probability of secrecy even for the unconstrained power scenario. For the above simulated conditions this value is 0.24 approximately.

In the power constrained case, as explained in subsection II-B, transmission only takes place when (i): (8b) and (8c) are both satisfied and (ii): the solution in (14) requires $P = a + b \leq P_{\text{max}}$. So there is a trade off between guaranteeing a high probability of secrecy ($\beta$) and secrecy throughput. This behavior is observed in Fig. 2 where the normalized secrecy throughput is plotted. We define the normalized secrecy throughput as the ratio between the number of channel realizations whose information is “securely transmitted” (i.e., it satisfies (8c)) and the total number of channel realizations in our simulation times the achieved probability of secrecy. So from Fig. 2, our technique generally offers a higher throughput than the reference approach. Indeed, for the power unconstrained system, the target probability of secrecy is always guaranteed and we also achieve the maximum possible secrecy throughput. On the other hand, for the power constrained case, as the target probability of secrecy approaches 1 (i.e., as the security conditions become more demanding), the throughput decreases due to the fact that we only transmit information for fewer channel realizations.

It is worth pointing out that as a result of our efficient power allocation technique, in the case of the power constrained system, the secrecy throughput of our scheme (unlike the reference technique) can be improved by incrementing the power available at the transmitter. This is clearly shown in Fig. 3 where the effect of increasing $P_{\text{max}}$ is analyzed for two target probability of secrecy, $\beta = 0.8$ and 0.9. Here, when using larger values of $P_{\text{max}}$, our scheme is perfectly capable of guaranteeing the maximum secrecy throughput rates while the reference method is constrained to a fixed value of secrecy throughput, irrespective of $P_{\text{max}}$.

In Fig. 4 the power distribution for the power unconstrained case is illustrated for different values of the target probability of secrecy ($\beta$). Here, the average power requested for the strategy in (14) is observed (where “average power” is the mean value of $P$ over those Monte Carlo runs which transmission takes place (i.e., $P \leq P_{\text{max}}$)).

Note that in general our scheme is capable of guaranteeing a given probability of secrecy for a higher number of eavesdroppers ($K$), but then (from (14) it is necessary to provide more power at the
transmitter.

Finally, it is important to remark upon the simplicity of our proposed power allocation scheme which relies on simple mathematical calculations and does not require solving an optimization problem using highly complex computational algorithms as in [6].

IV. CONCLUSION

In this letter we investigate a probabilistic approach for achieving secrecy over MISO systems by using beamforming as a transmit strategy and broadcasting artificial noise to confuse eavesdroppers. An effective power distribution between information and artificial noise is introduced. This approach guarantees a given probability of secrecy defined by the QoS constraints both at the intended receiver and at the eavesdroppers. The power allocations are given by simple closed-form expressions. Simulation results show that this strategy is energy consumption efficient (i.e., it allocates the minimum power to achieve a given probability of secrecy) for both unconstrained and constrained transmitted power. For the constrained power case, there is a trade-off between secrecy throughput and achieving a high probability of secrecy that can be improved by augmenting the total amount of power available at the transmitter.

APPENDIX A

PROOF OF LEMMA 1

The left hand side of (10c) can easily be re-written as follows:

\[ \mathbb{P} \left[ h_k^H A h_e \leq \sigma_e^2 \right] \]  

(15)

where

\[ A = \frac{a}{\gamma_e} t_1 t_1^H - b C_h. \]  

(16)

Hence, (15) corresponds to the CDF of an indefinite Hermitian quadratic form \( Y = h_k^H A h_e \) in a random vector \( h \), where \( \mathbb{E} \{ h_k h_k^H \} = \sigma_e^2 I \). Now \( Y \) can be written as \( Y = \bar{h}_e^H \overline{A} h_e \), where \( \bar{h}_e = \frac{h_e}{\sigma_e} \) and so \( \mathbb{E} \{ \bar{h}_e \bar{h}_e^H \} = I \). Then \( \overline{A} = \sigma_e^2 A \) and the eigenvalues of \( \overline{A} \) are \( \sigma_e^2 \lambda_i (A) \). Considering the definition of \( C_h \) and \( t_1 \) we set:

\[ \overline{A} = \sigma_e^2 \left[ \frac{a}{\gamma_e} t_1 t_1^H - \frac{b}{\gamma_e} \frac{t_1 t_2^H}{N_e - 1} - \cdots - \frac{b}{\gamma_e} \frac{t_{N_e} t_{N_e}^H}{N_e - 1} \right]. \]  

(17)

From this effective eigendecomposition the \( N_e \) eigenvalues of \( \overline{A} \) are \( \lambda_1 \) and \( \lambda_2 \) (with multiplicity orders equal to one and \( N_e - 1 \) respectively) such that:

\[
\begin{bmatrix}
\frac{a}{\gamma_e} t_1^H & \frac{b}{\gamma_e} \frac{t_2^H}{N_e - 1} & \cdots & \frac{b}{\gamma_e} \frac{t_{N_e}^H}{N_e - 1}
\end{bmatrix}
\]  

(18)

Following the procedure detailed in [13] and bearing in mind the multiplicity order of the eigenvalues of \( \overline{A} \), then the CDF of \( Y \) is:

\[
F_Y (y) = u (y) + \alpha_1 \frac{\lambda_1}{\lambda_1} e^{-\frac{y}{\lambda_1}} u \left( \frac{y}{\lambda_1} \right) + \sum_{k=1}^{N_e-1} \alpha_{k+1} e^{-\frac{y}{\lambda_2}} u \left( \frac{y}{\lambda_2} \right)
\]  

(19)

where \( u (x) \) is the unit step function.

Since in our problem \( \lambda_1 > 0 \) and \( \lambda_2 < 0 \), and as we are only interested in \( F_Y (y) \) for positive values of \( y \), since \( y = \sigma_e^2 \geq 0 \) (see (15)), then \( \{ \alpha_{k+1} \}_{k=1}^{N_e-1} \) in (19) can be neglected while \( \alpha_1 \) is given by:

\[
\alpha_1 = \frac{\lambda_1}{\lambda_1} e^{-\frac{y}{\lambda_1}} u \left( \frac{y}{\lambda_1} \right).
\]

(20)

Finally, from (18), (19) and (20) we get an expression for \( F_Y (y) \) for \( y \geq 0 \), as in (11).

REFERENCES