Physical Layer Security in Multibeam Satellite Systems

Gan Zheng, Pantelis-Daniel Arapoglou, and Björn Ottersten

Abstract—Security threats introduced due to the vulnerability of the transmission medium may hinder the proliferation of Ka band multibeam satellite systems for civil and military data applications. This paper sets the analytical framework and then studies physical layer security techniques for fixed legitimate receivers dispersed throughout multiple beams, each possibly surrounded by multiple (passive) eavesdroppers. The design objective is to minimize via transmit beamforming the costly total transmit power on board the satellite, while satisfying individual intended users’ secrecy rate constraints. Assuming state-of-the-art satellite channel models, when perfect channel state information (CSI) about the eavesdroppers is available at the satellite, a partial zero-forcing approach is proposed for obtaining a low-complexity sub-optimal solution. For the optimal solution, an iterative algorithm combining semi-definite programming relaxation and the gradient-based method is devised by studying the convexity of the problem. Furthermore, the use of artificial noise as an additional degree-of-freedom for protection against eavesdroppers is explored. When only partial CSI about the eavesdroppers is available, we study the problem of minimizing the eavesdroppers’ received signal to interference-plus-noise ratios. Simulation results demonstrate substantial performance improvements over existing approaches.

Index Terms—Multibeam satellite, physical-layer security, semi-definite programming, artificial noise.

I. INTRODUCTION

Due to their inherent broadcasting nature and vast coverage area, satellite communications systems—whether civil or military—are particularly prone to security threats, a taxonomy of which is provided in [1]. To guarantee perfect security, one needs to prevent eavesdroppers from decoding any message intended to legitimate users. Security in space missions is achieved at various layers of the Consultative Committee of Space Data Systems (CCSDS) protocol stack. Typically, it is realized at upper layers by means of encryption schemes, like the Advanced Encryption Standard (AES) [2], which is relevant to both the telemetry/telecommand and the data channels.

In contrast to the upper layer techniques, security has also been addressed using an information-theoretic approach. The seminal works by Wyner [3] and shortly afterwards by Csiszár and Körner [4] demonstrated that for the wireline case, by exploring the random channel and coding, secure communication in the presence of an eavesdropper is possible without using key encryption, and can be carried out at the physical layer. Since then, there has been growing interest in ensuring secure terrestrial wireless communications at the physical layer to prevent malicious eavesdroppers from decoding the message [5], [6]. The key assumption to guarantee positive secrecy rate was that the legitimate users have better signal-to-noise ratios (SNRs) than the eavesdroppers, which is not always the case.

To improve the secrecy rate under unfavorable conditions where legitimate users have worst SNRs, one possible way to ensure positive secrecy rate is to use multiple-input multiple-output (MIMO) antennas at the transmitter and/or receivers. With perfect channel state information (CSI), secrecy capacity and optimization have been studied in [7]–[10]. When only partial CSI is available, such as channel mean and/or covariance matrix, the problem of finding the optimal input covariance has been addressed in [11].

Another promising approach is to embed artificial noise (AN) in the transmission of the information bearing signal for the purpose of degrading the channels to eavesdroppers. The concept was first proposed in [12] without knowing the eavesdroppers’ CSI where the AN is chosen to lie in the null space of the legitimate channel so that no interference is introduced to the legitimate receiver. Assuming a single legitimate user, it was shown in [13] that even with perfect CSI, the use of AN results in nearly optimal performance in the high SNR regime. In the case of single-antenna receivers, with perfect CSI about the legitimate user and mean CSI about the eavesdropper, beamforming and AN were studied in [14] for maximizing the ergodic capacity. In [15], assuming perfect CSI for both the legitimate user and the eavesdroppers, the beamforming weights and the covariance matrix of AN are jointly designed to minimize transmit power. In [16], with only information of eavesdroppers’ channel distribution at the transmitter, the optimal power allocation between signal and noise was studied and it was revealed that equal power allocation is near-optimal. Another direction to utilize AN is to separately optimize the legitimate receiver’s performance while confusing the eavesdroppers. For instance, [17] proposed to first satisfy the legitimate receiver’s signal to interference-plus-noise ratios (SINR) requirement using minimum power and then use the...
remaining power to transmit AN uniformly distributed in the null space of the desired signal. Most recently, [18] studied the optimization of beamforming and AN covariance matrix by providing SINR guarantee for the legitimate user with a maximum allowable SINR on the eavesdroppers where CSI is given in the form of correlation matrices. However, there are very few work dealing with multiple legitimate users with multiple eavesdroppers and directly considering the secrecy rate rather than separating the SINRs at legitimate users and eavesdroppers, especially in satellite communications.

Specific to multibeam satellite communications, beams generated via multiple antenna feeds could be used to enhance physical layer security. One of the few works along this direction is [19], which studies the joint optimization of power and beamforming with individual secrecy rate constraints. An iterative algorithm to optimize power was first proposed with fixed beamforming. Then the beamforming weights were achieved by using ZF constraints on co-channel interference among all legitimate users and useful signals received at eavesdroppers.

In this paper, the focus turns to fixed satellite communication systems employing multiple beams for increasing the spectrum reuse. Commonly occupying the Ka frequency band, configurations with multibeam coverage based on advanced antenna and beamforming concepts have great potential for providing broadband multimedia applications in both civil/commercial [20] and military satellite systems [21]. The aim of the analysis is to design an optimal transmit beamformer that realizes physical layer security. Focusing on the downlink, we assume that the transmitter (satellite) is aware of the existence of eavesdroppers as well as of their full or partial (in the form of covariance matrices) CSI. Note that the system and channel characteristics as well as their estimation are very different for the satellite scenario compared to the prior art for terrestrial systems. The beamforming scheme we arrive at is optimal in the sense that it minimizes the total on board transmit power while ensuring the individual secrecy rate constraints for each user. More specifically, the following contributions can be identified:

- We define a framework for physical layer security in broadband multibeam satellite systems serving fixed users with distinct system, antenna and channel characteristics; this framework is giving rise to new beamforming requirements.
- We consider a general eavesdropping case in a multituser system where each legitimate user can be surrounded by either their own multiple eavesdroppers or common multiple eavesdroppers which includes the system model in [19] as a special case where only a single and common eavesdroppers for all legitimate users is assumed. We aim at optimizing secrecy rate directly in contrast to the conventional approach [17] that separately considers the SINRs at legitimate users and eavesdroppers.
- With perfect CSI, we propose a partial ZF approach where the useful signal is orthogonal to the eavesdroppers’ channels, in contrast to the existing complete ZF method in [19] where no interference is received at the legitimate users and no useful signal is received at the eavesdroppers.
- We propose an iterative algorithm to find the approximated optimal transmit beamforming solution by showing the convexity of the problem using semi-definite programming (SDP) relaxation.
- We further explore the use of AN and prove its advantage over non-AN methods. We then propose an iterative algorithm to jointly optimize the transmit signals and AN covariance matrices.
- In addition, when only covariance matrices about eavesdroppers are available, we investigate the beamforming and AN design to minimize the maximum eavesdroppers’ SINR while guaranteeing the legitimate users’ SINR. An iterative algorithm based on bi-section search is devised to find the approximated optimal solution.

The remainder of this paper is organized as follows. In Section II, we introduce the multibeam satellite system model as well as the problem formulation. Section III describes the first proposed algorithm using partial ZF with perfect CSI. In Section IV, an iterative algorithm based on convex optimization is proposed to find the optimal transmit beamforming solution. Section V studies the use of AN and proposes an iterative algorithm to achieve the approximated optimal design of both useful signals and noise covariance matrices. Section VI extends the beamforming and AN optimization based on the covariance matrices about eavesdroppers. Simulation results are provided in Section VII and we conclude the paper in Section VIII.

Throughout this paper, the following notations will be adopted. Complex scalar is represented by a lowercase letter and $\| \cdot \|$ denotes its modulus. $\mathbb{E} [\cdot]$ denotes the mean of a random variable. Vectors and matrices are represented by bold lowercase and uppercase letters, respectively, and $\| \cdot \|$ is the Euclidean norm for a vector. The superscript $\dagger$ is used to denote the Hermitian transpose of a vector or matrix. $X \succeq 0$ means that matrix $X$ is positive semi-definite. $\text{trace}(X)$ denotes the trace of $X$. $A \odot B$ denotes Hadamard product of two matrices. Finally, $x \sim \mathcal{N}(m, \Theta)$ denotes a vector $x$ of Gaussian entries with a mean vector of $m$ and a covariance matrix of $\Theta$.

II. System Model And Problem Formulation

Consider the downlink of a satellite communication system employing a geostationary satellite and serving fixed users via multiple beams. Specifically, there are $N$ co-channel beams on ground that are formed by $N$ corresponding antenna feeds on board the satellite (single-feed per beam), resulting in a frequency reuse of one. Legitimate users are served in a time division multiplexed (TDM) fashion and, hence, at any given time, there is at most one legitimate receiver scheduled within each beam. Actually, taking into account the bursty nature of data communications, to avoid extreme interbeam interference and provide positive secrecy rate, it is assumed that there are $M < N$ active legitimate receivers (users) receiving independent data streams. This follows the trend of many practical techniques currently being investigated for multibeam satellite systems, where only a subset of beams is illuminated at each time slot [22]. The legitimate receiver $m$ is surrounded by $K_m$ eavesdroppers located within the same beam.
A. Channel Model

There are fundamental differences in terms of channel effects between $Ka$ band fixed satellite and terrestrial communication links. Thus, to realistically model this aspect is key in achieving physical layer security. Considering the satellite channel above 10 GHz operating under line-of-sight, it is subjected to various atmospheric fading mechanisms originating in the troposphere, which severely degrade system performance and availability [23]. When propagating through clouds, snow, hail, ice droplets and predominantly rain, radio waves suffer from attenuation. Out of these mechanisms, rain attenuation constitutes the dominant factor and will be taken into account in the course of our analysis. Since rain attenuation is a slow fading process that exhibits spatial correlation over tens of km, we will assume that both the legitimate users and the eavesdroppers undergo the same fading when located within the same beam, but independent fading between the different beams [24].

1) Rain Attenuation: To model the rain attenuation effect we employ the state-of-the-art empirical model proposed in the ITU-R $^2$ Recommendation P.618 [25]. The resulting distribution of the power gain in dB, $\xi_{db} = 20 \log_{10}(\xi)$, is commonly modeled as a lognormal random variable $\ln(\xi_{db}) \sim \mathcal{N}(\mu, \sigma)$, where $\mu$ and $\sigma$ depend on the location of the receiver, the frequency of operation, polarization and the elevation angle toward the satellite. The corresponding $N \times 1$ rain fading vector for all beams is given by

$$\mathbf{h} = \xi^{-\frac{1}{2}} e^{-j\phi}$$

(1)

where $\phi$ denotes an $N \times 1$ phase vector uniformly distributed over $[0, 2\pi]$.

2) Beam Gain: The beam gain defines the average SINR at each receiver and it mainly depends on the satellite antenna pattern and the receiver position. Typical multibeam satellite antennas are either direct radiating arrays or array-fed reflectors [20], both making use of a beamforming network. Define the $m$-th receiver’s position based on the angle $\theta_m$ between the beam center and the receiver location with respect to the satellite and $(\theta_{3db})_m$ as its 3-dB angle. Then the beam gain from the satellite antenna to the receiver $m$ is approximated by [26]:

$$b(m) = b_{max} \left( \frac{J_1(u_m)}{2u_m} + 36J_3(u_m) \right)^2$$

(2)

where $u_m = 2.07123 \sin \theta_m / \sin(\theta_{3db})_m$ and $J_1$ and $J_3$ are the first-kind Bessel function of order 1 and 3. The coefficient $b_{max}$ represents the gain at boresight.

Suppose $N \times 1$ vector $\mathbf{b}$ denotes the beam gain vector from all transmit antenna feeds to the receiver $m$, the overall channel for this user can be expressed as

$$\mathbf{h} = \tilde{\mathbf{h}} \odot \mathbf{b}^\frac{1}{2}$$

(3)

Since identical fading is justified amid the legitimate user and the eavesdroppers in the same beam, the only difference between their channels are the beam gains, which are determined by their different locations.

B. Signal Model

Suppose the data intended for the legitimate user $m$ is $s_m$ with unit average power $E[|s_m|^2] = 1, \forall m$. Before transmission, it is weighted by the $N \times 1$ beamforming vector $\mathbf{w}_k$ and therefore the overall transmitted signal can be written in vector $\mathbf{x}$ as

$$\mathbf{x} = \sum_{n=1}^{M} \mathbf{w}_n s_n.$$

Denoting the $N \times 1$ channel vectors from the satellite to the legitimate receiver $m$ by $\mathbf{h}_m$, and from the satellite to the eavesdropper $k$ surrounding user $m$ by $\mathbf{g}_{m,k}$, the received signals at the legitimate user $m$ and at the eavesdropper $m$ surrounding it are, respectively,

$$y_m = \mathbf{h}_m^\dagger \sum_{n=1}^{M} \mathbf{w}_n s_n + n_m = \mathbf{h}_m^\dagger \mathbf{w}_m s_m + \sum_{n=1,n\neq m}^{M} \mathbf{h}_m^\dagger \mathbf{w}_n s_n + n_m.$$  

(4)

and

$$y_{m,k} = \mathbf{g}_{m,k}^\dagger \sum_{n=1}^{M} \mathbf{w}_n s_n + n_e = \mathbf{g}_{m,k}^\dagger \mathbf{w}_m s_m + \sum_{n=1,n\neq m}^{M} \mathbf{g}_{m,k}^\dagger \mathbf{w}_n s_n + n_e.$$  

(5)

where $n_m$ and $n_e$ are the noises at the legitimate receiver $m$ and the eavesdroppers surrounding it and they are independent and identically distributed (i.i.d.) zero-mean Gaussian random variables with respective variances $\sigma^2_n$ and $\sigma^2_e$.

The achievable secrecy rate for the legitimate user $m$ can be expressed as [27]

$$C_m = \log_2 \left( 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sum_{n=1,n\neq m}^{M} |\mathbf{h}_m^\dagger \mathbf{w}_n|^2 + \sigma^2_D} \right) - \max_{k \in \{1,2,\ldots,K_m\}} \log_2 \left( 1 + \frac{|\mathbf{g}_{m,k}^\dagger \mathbf{w}_m|^2}{\sum_{n=1,n\neq m}^{M} |\mathbf{g}_{m,k}^\dagger \mathbf{w}_n|^2 + \sigma^2_E} \right).$$  

(6)

C. Problem Formulation

The problem of interest is to minimize total transmit power subject to secrecy rate constraints $\{R_m\}$ by jointly optimizing transmit beamforming (power embedded). Mathematically, the problem can be written as

$$\min_{\mathbf{w}_m} \sum_{m=1}^{M} \|\mathbf{w}_m\|^2$$  

(7)

s.t. $C_m \geq R_m, \forall m.$

This problem is non-convex due to the presence of eavesdroppers and the optimal solution is not known in the literature.
D. Existing Solution – Complete Zero-Forcing

In [19], a simpler system and problem was considered where there is only one eavesdropper potentially detecting any intended user’s signal, which is a special case of the system considered in this paper. To make the problem tractable, [19] imposes complete ZF constraints to all receivers including both legitimate users and eavesdroppers, meaning that no interference is received at the intended users and no useful signal received at the eavesdroppers. Applying the principles to our system setting, the ZF constraints can be expressed as

\[ \mathbf{w}_m^\dagger \mathbf{h}_n = 0, \forall n \neq m \] and \[ \mathbf{w}_m^\dagger \mathbf{g}_{m,k} = 0, \forall m, k. \] (8)

With the interference among all users removed, the secrecy rate for the intended user \( m \) is simplified to

\[ C_m = \log_2 \left( 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sigma_D^2} \right). \]

In this way, the multiuser system is decoupled and each user’s performance can be optimized individually. However, this approach not only suppresses too much the system degrees-of-freedom due to unnecessary ZF constraints but also requires at least \( N \geq M + \max_m K_m \) transmit antenna feeds. This results in a performance degradation that will be illustrated by the simulation results in Section VII.

III. PROPOSED SOLUTION 1: PARTIAL ZERO-FORCING

To improve the performance of the complete ZF approach in [19], we first propose to only force to zero the useful signals received at the eavesdroppers while managing the interference among intended users efficiently. Namely, we consider the following ZF constraints

\[ \mathbf{w}_m^\dagger \mathbf{g}_{m,k} = 0, \forall m, k. \] (9)

Although it needs the same number of spatial degree-of-freedom \((M + \max_m K_m)\) in order to achieve reasonable performance, compared with the algorithm in [19], this approach, on the one hand, relaxes the interference constraints among intended users and on the other hand still removes the useful signal received at the eavesdroppers and simplifies the problem. Compare (8) with (9) from an optimization point of view, it is easily seen that partial ZF imposes less constraints than complete ZF, therefore leads to an improved solution. With the above constraints, the original problem (7) becomes

\[
\begin{align*}
\min_{\mathbf{w}_m} & \quad \sum_{m=1}^M \| \mathbf{w}_m \|^2 \\
\text{s.t.} & \quad 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^M |\mathbf{h}_n^\dagger \mathbf{w}_n|^2 + \sigma_D^2} \geq 2R_m \\
& \quad \mathbf{g}_{m,k}^\dagger \mathbf{w}_m = 0, \forall m, \forall k.
\end{align*}
\] (10)

The added ZF constraints do not increase difficulty of solving (10), and the well known algorithm in [28] can be applied to solve it straightforwardly.

IV. PROPOSED SOLUTION 2: THE OPTIMAL SOLUTION TO (7)

A. Equivalent Reformulation

Both algorithms mentioned previously rely on ZF constraints in order to make the problem (7) more tractable. In this section, we solve (7) optimally without any additional constraints. We start by reformulating (7) into

\[
\begin{align*}
\min_{\mathbf{w}_m} & \quad \sum_{m=1}^M \| \mathbf{w}_m \|^2 \\
\text{s.t.} & \quad 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^M |\mathbf{h}_n^\dagger \mathbf{w}_n|^2 + \sigma_D^2} \geq 2R_m \\
& \quad \max_{k \in \{1, \ldots, K_m\}} \left[ 1 + \frac{|\mathbf{g}_{m,k}^\dagger \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^M |\mathbf{g}_{m,k}^\dagger \mathbf{w}_n|^2 + \sigma_E^2} \right] \leq r_m, \quad (11)
\end{align*}
\]

and, by introducing a list of auxiliary variables \( r \triangleq \{r_1, r_2, \ldots, r_M\} \), further rewrite it as

\[
\begin{align*}
\min_{\mathbf{w}_m, r_m \geq 0} & \quad \sum_{m=1}^M \| \mathbf{w}_m \|^2 \\
\text{s.t.} & \quad 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^M |\mathbf{h}_n^\dagger \mathbf{w}_n|^2 + \sigma_D^2} \geq r_m 2R_m \\
& \quad 1 + \max_{k \in \{1, \ldots, K_m\}} \sum_{n=1, n \neq m}^M |\mathbf{g}_{m,k}^\dagger \mathbf{w}_n|^2 + \sigma_E^2 \leq r_m, \quad (12)
\end{align*}
\]

which in turn can be re-organized as

\[
\begin{align*}
\min_{\mathbf{w}_m, r_m \geq 0} & \quad \sum_{m=1}^M \| \mathbf{w}_m \|^2 \\
\text{s.t.} & \quad |\mathbf{h}_m^\dagger \mathbf{w}_m|^2 - (r_m 2R_m - 1) \sum_{n=1, n \neq m}^M |\mathbf{h}_n^\dagger \mathbf{w}_n|^2 \geq (r_m 2R_m - 1) \sigma_D^2 \\
& \quad |\mathbf{g}_{m,k}^\dagger \mathbf{w}_m|^2 - (r_m - 1) \sum_{n=1, n \neq m}^M |\mathbf{g}_{m,k}^\dagger \mathbf{w}_n|^2 \leq (r_m - 1) \sigma_E^2, \forall k \in \{1, \ldots, K_m\}, \forall m.
\end{align*}
\] (13)

The equivalence of the problems (13) and (7) can be shown as follows. Let \( \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_M\} \) be a feasible solution to (7). If we set \( r_m \triangleq \left( 1 + \frac{|\mathbf{h}_m^\dagger \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^M |\mathbf{h}_n^\dagger \mathbf{w}_n|^2 + \sigma_D^2} \right) 2^{-R_m} \), then \( \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_M, r_1, r_2, \ldots, r_M\} \) is a feasible solution to (13). On the other hand, let \( \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_M, r_1, r_2, \ldots, r_M\} \) denote a feasible solution to (13). It is easy to see \( \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_M\} \) is also feasible for (7). Therefore (13) and (7) are equivalent.

Problem (13) is still difficult to solve because it is non-convex. In the following, we first solve it for fixed auxiliary variables \( r \) and then optimize \( r \) by studying its convexity and using an efficient gradient-based algorithm.

B. Optimization of \( \{\mathbf{w}_m\} \) for Fixed \( r \)

Before proceeding, we introduce a relaxation \( \mathbf{W}_m = \mathbf{w}_m \mathbf{w}_m^\dagger, \forall m \), and rewrite (13) for fixed \( r \) below by dropping
the non-convex constraint \( \text{rank}(\mathbf{W}_m) = 1 \),

\[
\begin{align*}
\min_{\mathbf{W}_m \succeq 0} & \quad \sum_{m=1}^{M} \text{trace}(\mathbf{W}_m) \\
\text{s.t.} & \quad \mathbf{h}_m^\dagger \mathbf{W}_m \mathbf{h}_m - (r_m 2^{R_m} - 1) \sum_{n=1, n \neq m}^{M} \mathbf{h}_m^\dagger \mathbf{W}_n \mathbf{h}_m \\
& \quad \geq (r_m 2^{R_m} - 1) \sigma_D^2, \forall m, \\
& \quad \mathbf{g}_{m,k}^\dagger \mathbf{W}_m \mathbf{g}_{m,k} - (r_m - 1) \sum_{n=1, n \neq m}^{M} \mathbf{g}_{m,k}^\dagger \mathbf{W}_n \mathbf{g}_{m,k} \\
& \quad \leq (r_m - 1) \sigma_E^2, \forall k \in \{1, 2, \ldots, K_m\}, \forall m.
\end{align*}
\] (14)

The main advantage of (14) is that for fixed \( \mathbf{r} \), it is a SDP problem and can be optimally solved [29]. Note that the obtained matrix \( \mathbf{W}_m \) might not be rank-1, therefore (14) is not equivalent to but a relaxation of (13) for fixed \( \mathbf{r} \). If a higher-rank solution \( \mathbf{W}_m \) is obtained, the randomization method [30] could be employed to find an approximated solution.

C. Optimization over \( \mathbf{r} \)

Denote the objective value of (14) as a function of \( \mathbf{r} \) by \( \mathcal{P}(\mathbf{r}) \). It can be seen that solving the original problem (11) is equivalent to minimizing \( \mathcal{P}(\mathbf{r}) \) with respect to \( \mathbf{r} \) where the optimization of \{ \( \mathbf{W}_m \) \} has been embedded in evaluating \( \mathcal{P}(\mathbf{r}) \). Next we focus on finding the optimal \( \mathbf{r} \) to minimize \( \mathcal{P}(\mathbf{r}) \).

Since \( \mathbf{r} \) are non-negative variables with lower bound 1 (due to the last constraint in (12)), the optimal solution can be found by global optimization algorithms like “Dividing RECTangles” (DIRECT [31]) with no prior knowledge about \( \mathcal{P}(\mathbf{r}) \). However, we will study the analytical property of \( \mathcal{P}(\mathbf{r}) \) to devise more efficient algorithms than DIRECT.

**Theorem 1:** \( \mathcal{P}(\mathbf{r}) \) is a convex function of \( \mathbf{r} \).

**Proof:** The Lagrangian of problem (14) as

\[
\begin{align*}
\mathcal{L}(\mathbf{W}_m, \Phi_m, \mathbf{r}, \mathbf{y}, \mathbf{z}) & = \sum_{m=1}^{M} \text{trace}(\mathbf{W}_m) - \sum_{m=1}^{M} \text{trace}(\mathbf{W}_m \Phi_m) \\
& \quad - \sum_{m=1}^{M} y_m (\mathbf{h}_m^\dagger \mathbf{W}_m \mathbf{h}_m - (r_m 2^{R_m} - 1)) \\
& \quad - (r_m 2^{R_m} - 1) \sum_{n=1, n \neq m}^{M} \mathbf{h}_m^\dagger \mathbf{W}_n \mathbf{h}_m \\
& \quad - \sum_{m=1}^{M} \sum_{n=1, n \neq m}^{M} z_{k,m} (\mathbf{g}_{m,k}^\dagger \mathbf{W}_m \mathbf{g}_{m,k} - (r_m - 1)) \\
& \quad - \sum_{m=1}^{M} \sum_{n=1, n \neq m}^{M} \mathbf{g}_{m,k}^\dagger \mathbf{W}_n \mathbf{g}_{m,k} - (r_m - 1) \sigma_E^2
\end{align*}
\]  

where \( \Phi_m \geq 0, \mathbf{y}, \mathbf{z} \geq 0 \) are dual variables associated with the constraints in (14).

The dual problem can be written as

\[
\begin{align*}
\max_{\mathbf{y}, \mathbf{z}} \quad & \sum_{m=1}^{M} y_m (r_m 2^{R_m} - 1) \sigma_D^2 - \sum_{m=1}^{M} \sum_{k=1}^{K_m} z_{k,m} (r_m - 1) \sigma_E^2 \\
\text{s.t.} \quad & \mathbf{I} - y_m \mathbf{h}_m \mathbf{h}_m^\dagger + (r_m 2^{R_m} - 1) \sum_{n=1, n \neq m}^{M} \mathbf{y}_n \mathbf{h}_n \mathbf{h}_n^\dagger + \\
& \sum_{k=1}^{K_m} z_{k,m} \mathbf{g}_{m,k} \mathbf{g}_{m,k}^\dagger - \sum_{k=1}^{K_m} (r_m - 1) z_{k,m} \sum_{n=1, n \neq m}^{M} \mathbf{g}_{m,k} \mathbf{g}_{n,k}^\dagger \\
& \geq 0, \forall m.
\end{align*}
\]  (16)

Due to the strong duality between the primary problem (14) and the dual problem (16), the objective value of (16) is also \( \mathcal{P}(\mathbf{r}) \). Observe that for given \( \mathbf{y}, \mathbf{z} \), the objective function of (16) is linear and convex about \( \mathbf{r} \), therefore its maximum over \{ \( \mathbf{y}, \mathbf{z} \) \}, \( \mathcal{P}(\mathbf{r}) \), is convex about \( \mathbf{r} \) [29, p80]. This completes the proof.

**Theorem 1** shows that any local search algorithm can find the global optimum of \( \mathcal{P}(\mathbf{r}) \) therefore greatly reduces the complexity. We have the following straightforward result to facilitate the design of gradient-based algorithms [32].

**Corollary 1:** The derivative of \( \mathcal{P}(\mathbf{r}) \) is given by

\[
\frac{\partial \mathcal{L}}{\partial r_m} = y_m 2^{R_m} \left( \sum_{n=1, n \neq m}^{M} \mathbf{h}_m^\dagger \mathbf{W}_n \mathbf{h}_m + \sigma_D^2 \right) \\
- \sum_{k=1}^{K_m} z_{k,m} \left( \sum_{n=1, n \neq m}^{M} \mathbf{g}_{m,k}^\dagger \mathbf{W}_n \mathbf{g}_{m,k} + \sigma_E^2 \right).
\]  (17)

The main iterative algorithm can be summarized as follows. For given \( \mathbf{r} \), solve both the primary problem (14) and the dual problem (16) to obtain the primary variables \{ \( \mathbf{W}_m \) \} and dual variables \( \mathbf{y}, \mathbf{z} \); then update \( \mathbf{r} \) using the gradient-based algorithm and the gradient result in (17). The overall iterative algorithm to solve (13) is given in Algorithm 1.

The major computational complexity comes from solving the primary problem (14). The dual problem (16) is normally solved as a by-product using the interior-point methods such as primal-dual path-following algorithms. (14) has \( (M + \sum_{m=1}^{M} K_m) \) constraints and the dimension of \( \mathbf{W}_m \) is \( N \times N \), \( \forall m \), so the complexity to solve the it is \( \mathcal{O}((M + \sum_{m=1}^{M} K_m)^4 N^4 \log(\frac{1}{\epsilon})) \) where \( \epsilon \) is the given accuracy [30].

V. PROPOSED SOLUTION 3: OPTIMAL SOLUTION WITH ARTIFICIAL NOISE

A. Signal Model With Artificial Noise

Note that there are two objectives for the transmitter optimization: one is to ensure the transmission quality of legitimate users and the other is to degrade the channel of eavesdroppers. Hitherto, it has been assumed that only the useful signals are optimized which satisfies only the first purpose. In this section, we propose to jointly transmit the intended signal together with AN over the multiple beams; this serves the second purpose, i.e., to weaken the signals received at the eavesdroppers. The idea was originally proposed in [12] concentrating on the case where no CSI about eavesdroppers...
where all symbols bear the same meaning as before and can be written in vector form as

\[ \mathbf{x} = \sum_{m=1}^{M} \mathbf{w}_m \mathbf{s}_m + \mathbf{n}, \]

where \( \mathbf{s}_m \) is the AN vector whose elements are zero-mean complex Gaussian random variables with covariance matrix \( \mathbf{R} = \mathbb{E}(\mathbf{n} \mathbf{n}^H) \).

With the additional AN vector to the signal model (4-5) in Section II-B, the secracy rate for user \( m \) can be expressed as

\[
C_m^{AN} = \log \left( 1 + \frac{\mathbf{h}_m^H \mathbf{w}_m}{\sum_{n=1, n \neq m}^{M} |\mathbf{h}_m^H \mathbf{w}_n|^2 + \mathbf{h}_m^H \mathbf{R} \mathbf{s}_m + \sigma_D^2} \right) - \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{w}_m|^2}{\sum_{n=1, n \neq m}^{M} |\mathbf{g}_{m,k}^H \mathbf{w}_n|^2 + \mathbf{g}_{m,k}^H \mathbf{R} \mathbf{g}_{m,k} + \sigma_E^2} \right). \quad (19)
\]

Note that most existing works assume that \( \mathbf{n} \) is random but orthogonal to the intended users’ channels [12]. This assumption, although simplifies the signal model (e.g., \( \mathbf{h}_m^H \mathbf{n} = 0 \)), introduces unnecessary performance loss. Here we do not impose any special structure on the covariance of AN, \( \mathbf{R} \).

### B. Problem Formulation

The problem of interest is to minimize total transmit power subject to secracy rate constraints \( \{R_m\} \), which is the same as before except for the additional degree of freedom: design of AN. The mathematical problem can be written as

\[
\min_{\mathbf{w}_m, \mathbf{R} \succeq 0} \sum_{m=1}^{M} \|\mathbf{w}_m\|^2 + \text{trace}(\mathbf{R}) \quad (20)
\]

s.t. \( C_m^{AN} \geq R_m, \forall m \).

Before solving problem (20), we first emphasize and quantify the benefits due to the use of artificial noise.

C. Advantage of Using Artificial Noise

As shown in [19], in order to decouple multiple users using ZF constraints, the satellite should employ at least \( N = M + 1 \) antenna feeds (beams), which corresponds to the case of a single eavesdropper. If multiple eavesdroppers are present for each user in our formulation (7), the number of required antenna feeds would be \( M + \max_m K_m \); otherwise, the system will be secrecy rate limited, meaning not all positive secrecy rate can be supported, even with unlimited power. The main advantage of using AN is to satisfy secrecy rate requirements with less transmit antenna feeds and is summarized in the theorem below.

Theorem 2: With AN transmitted, the minimum number of antenna feeds required to guarantee any positive secrecy rate is \( N = M + 1 \), regardless of the number of eavesdroppers for each user, given \( \mathbf{H} \triangleq [\mathbf{h}_1, \ldots, \mathbf{h}_M] \) is full column rank and \( \mathbf{g}_{m,k} \) is not in the column space of \( \mathbf{H}, \forall m, k \).

Proof: It suffices to give explicit solutions to guarantee positive secrecy rate when \( N \geq M + 1 \).

We first choose the noise design to be \( \mathbf{w}_m = 0, \forall m, \|\mathbf{u}\| = 1 \). Then (19) becomes

\[
C_m^{AN} = \log \left( 1 + \frac{|\mathbf{h}_m^H \mathbf{v}_m|^2}{\sum_{n=1, n \neq m}^{M} |\mathbf{h}_m^H \mathbf{v}_n|^2 + \sigma_D^2} \right) - \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{v}_m|^2}{|\mathbf{g}_{m,k}^H \mathbf{u}|^2 + \sigma_E^2} \right) \geq \log \left( 1 + \frac{|\mathbf{h}_m^H \mathbf{v}_m|^2}{\sum_{n=1, n \neq m}^{M} |\mathbf{h}_m^H \mathbf{v}_n|^2 + \sigma_D^2} \right) - \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{v}_m|^2}{P_m |\mathbf{g}_{m,k}^H \mathbf{u}|^2} \right). \quad (21)
\]

We then choose the beamforming vector to be \( \mathbf{v}_m = \sqrt{P_m} \mathbf{v}_m \) where \( \mathbf{v}_m^H \mathbf{h}_m = 0, \forall n \neq m, \|\mathbf{v}_m\| = 1, \forall m \). Then (21) reduces to

\[
C_m^{AN} \geq \log \left( 1 + \frac{|\mathbf{h}_m^H \mathbf{v}_m|^2}{\sigma_D^2} \right) - \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{v}_m|^2}{\sigma_D^2} \right) = \log \left( 1 + \frac{|\mathbf{h}_m^H \mathbf{v}_m|^2}{\sigma_D^2} \right) - \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{v}_m|^2}{|\mathbf{g}_{m,k}^H \mathbf{u}|^2} \right). \quad (22)
\]

where the second term \( \max_{k \in \{1, 2, \ldots, K_m\}} \log \left( 1 + \frac{|\mathbf{g}_{m,k}^H \mathbf{v}_m|^2}{|\mathbf{g}_{m,k}^H \mathbf{u}|^2} \right) \) is a constant, therefore \( C_m \) increases monotonically with transmit power \( P \) and any secrecy rate is achievable if there is no limit on \( P \). This completes the proof. 

Next we focus on the optimal solution to (20) following the same philosophy as in Section IV.
By first introducing the auxiliary variables \( r \) and using the same relaxation \( W_m = w_m w_m^\dagger \), and rewrite (20) as

\[
\begin{align*}
\min_{W_m \geq 0, R \geq r} & \sum_{m=1}^{M} \text{trace}(W_m) + \text{trace}(R) \\
\text{s.t.} & \quad h_m^\dagger W_m h_m - (r_m 2^{R_m} - 1) \\
& \quad \left( \sum_{n=1, n \neq m}^{M} h_m^\dagger W_n h_m + h_m^\dagger R h_m \right) \geq (r_m 2^{R_m} - 1)\sigma_D^2, \\
& \quad \left( \sum_{n=1, n \neq m}^{M} g_{m,k}^\dagger W_n g_{m,k} + g_{m,k}^\dagger R g_{m,k} \right) \leq (r_m - 1)\sigma_E^2, \\
& \quad k = 1, 2, \cdots, K_m, \forall m. \tag{23}
\end{align*}
\]

We then optimize \( \{w_m, R\} \) for fixed \( r \) and optimize \( r \) which will be addressed subsequently.

D. Optimization of \( \{w_m, R\} \) for Fixed \( r \)

As before, we give the derivative result of \( \mathbb{P}(r) \) in the following corollary.

\[
\frac{\partial L}{\partial r_m} = y_m 2^{R_m} \left( \sum_{n=1, n \neq m}^{M} h_m^\dagger W_n h_m + h_m^\dagger R h_m + \sigma_D^2 \right) - \sum_{k=1}^{K_m} z_{k,m} \left( \sum_{n=1, n \neq m}^{M} g_{m,k}^\dagger W_n g_{m,k} + g_{m,k}^\dagger R g_{m,k} + \sigma_E^2 \right). \tag{25}
\]

Corollary 2: The derivative of \( \mathbb{P}(r) \) is given by

\[
\frac{\partial L}{\partial L} = y_m 2^{R_m} \left( \sum_{n=1, n \neq m}^{M} h_m^\dagger W_n h_m + h_m^\dagger R h_m + \sigma_D^2 \right) - \sum_{k=1}^{K_m} z_{k,m} \left( \sum_{n=1, n \neq m}^{M} g_{m,k}^\dagger W_n g_{m,k} + g_{m,k}^\dagger R g_{m,k} + \sigma_E^2 \right).
\]

With the convexity of \( \mathbb{P}(r) \) established and the derivative information available, the gradient based algorithms could be applied to find its optimal \( r \). Algorithm 1 can be modified by incorporating the optimization of \( R \) to solve (20).

VI. Optimization Based on Eavesdroppers’ Channel Covariance Matrices

In previous sections, we have assumed that full CSI about the eavesdroppers is available at the transmitter, which is difficult to obtain in practice due to the random rain fading. Instead, in this section, we assume that only the location information of the eavesdroppers is available, hence a statistical estimation of the CSI can be carried out in the form of the covariance matrix. Indeed, according to the model in [25], if the location of the earth station along with the link characteristics are known, the attenuation due to rain can be estimated in statistical terms. Denote the channel of one eavesdropper by

\[
g = \bar{g} \circ b = \xi^\dagger e^{-j\Phi} \circ b. \tag{26}
\]

where \( \xi \) and \( b \) are the channel gain due to rain attenuation and the beam gain matrix, respectively, which for a given location is deterministic. \( \Phi \) denotes random phases. The covariance can be obtained as \( G = E_{\Phi} [gg^\dagger] \).

With only channel covariance information, it is difficult to realize perfect secrecy directly. Instead, our design objective here is to minimize the received SINRs at the eavesdroppers while satisfying the legitimate users’ SINR constraints. Mathematically, the problem formulations with AN3 is written as,

\[
\min_{w_m, R \geq 0} \max_{m \in \{1, 2, \cdots, K_m\}} \max_{k \in \{1, 2, \cdots, M\}} \left( w_m \right) \geq \Gamma_m, \forall m,
\]

\[
\sum_{m=1}^{M} \left| h_m^\dagger w_m \right|^2 + \sum_{m=1}^{M} \left| h_m^\dagger R h_m + \sigma_D^2 \right| \geq \Gamma_m, \forall m,
\]

\[
\sum_{m=1}^{M} \left\| w_m \right\|^2 + \sum_{m=1}^{M} \text{trace}(R) \leq P_T. \tag{27}
\]

In order to make it tractable, we introduce an auxiliary variable \( \gamma \) and apply rank relaxation \( W_m = w_m w_m^\dagger \) to obtain the
following problem
\[
\begin{align*}
\min \quad & \mathbf{w}_m^* \mathbf{r}_m \\
\text{s.t.} \quad & \sum_{n=1, n \neq m}^M \mathbf{h}_m^* \mathbf{w}_n \mathbf{h}_m + \mathbf{h}_m^* \mathbf{R} \mathbf{h}_m + \sigma_D^2 \geq \gamma_m, \\
& \sum_{n=1, n \neq m}^M \text{trace}(\mathbf{W}_n^* \mathbf{G}_{m,k}) + \text{trace}(\mathbf{R} \mathbf{G}_{m,k}) + \sigma_E^2 \leq \gamma, \\
& \sum_{m=1}^M \text{trace}(\mathbf{W}_m) + \text{trace}(\mathbf{R}) \leq P_T,
\end{align*}
\] (28)

which is a SDP problem and can be optimally solved when \( \gamma \) is fixed. Then we can use the bi-section method [29] to find the optimal \( \mathbf{w}_m \). The approximated optimal \( \gamma \) and \( \mathbf{w}_m \) can then be extracted from \( \mathbf{W}_m \) using the randomization method in [30].

The main computational complexity is due to the feasibility check of problem (28). Following the same analysis of (14), the associated complexity of solving (28) is \( O((1 + M + \sum_{m=1}^M K_m)^2 N^\frac{3}{2} \log(\frac{1}{\epsilon})) \) where \( \epsilon \) is the given accuracy.

VII. SIMULATION RESULTS

Computer simulations are performed to evaluate the performance of the proposed algorithms employing as a performance metric the total transmit RF power available on board the satellite, namely the sum of power transmitted by all beams. Unless otherwise specified, we consider a system with \( M = 3 \) active beams (users) and each user is overheard by a single eavesdropper, i.e., \( K_m = 1, \forall m \). Table I lists the channel and system parameters adopted for the simulations. We assume that the legitimate receivers – e.g. military camps – are located in the beam centers while the distance between the eavesdropper and a legitimate receiver within a beam is random and at least 0.15\( D \) where \( D \) is the beam diameter. The rain attenuation within each beam is random approximated by the lognormal distribution with the the statistical parameters of Table I. These values correspond to a typically mid-European temperate climate and the corresponding rain attenuation exceeded for specific percentages of time is shown in Fig. 1.

For simplicity, we further assume the secrecy rate requirements for all users are the same and \( R = R_m, \forall m \) measured in bps/Hz. In the numerical results, the ranges selected for \( R \) conform with the typical rates achieved in practical fixed satellite systems, e.g. based on the DVB-S2 (digital video broadcasting via satellite 2) standard [34]. The algorithm using complete ZF approach in [19] is used as the benchmark and labeled as “C-ZF” while the proposed partial ZF approach is labeled as “Proposed P-ZF Scheme.”

Fig. 2 depicts the typical convergence behavior of the proposed Algorithm 1. The secrecy rate constraints are [2.4763 0.2449 3.2038]\( T \). The intended users’ channel is

\[
\mathbf{h}_1 = \begin{bmatrix} -0.2906 - 0.3953i & -0.1874 + 0.1744i & 0.1404 + 0.1263i \\
-0.1190 + 1.4668i & 0.1946 + 0.0097i & 0.9749 - 0.5734i \\
0.0842 - 0.0916i & 0.1944 - 0.0156i & -0.0801 + 0.3065i \\
0.1933 + 0.0765i & -0.0062 - 0.1360i & 0.3114 + 0.6967i \end{bmatrix}
\]

while the eavesdroppers’ channel is given by

\[
\mathbf{g}_1 = \begin{bmatrix} -0.2377 + 0.4092i & -0.0892 - 1.0110i & 0.4395 - 0.4339i \\
0.2948 - 0.4132i & 0.3600 + 0.1622i & 0.3836 + 0.2849i \\
0.4309 - 0.0068i & -0.2520 - 0.6658i & 0.6953 + 0.1182i \\
-0.5477 - 0.0539i & 0.4349 + 0.8919i & 0.3603 - 0.4968i \end{bmatrix}
\]

The initial value of \( r \) is set to 1.5. It is observed that as

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Climatic conditions</td>
<td>Central Europe</td>
</tr>
<tr>
<td>Frequency band</td>
<td>Ka (20 GHz)</td>
</tr>
<tr>
<td>Satellite orbit</td>
<td>Geostationary</td>
</tr>
<tr>
<td>Polarization</td>
<td>Circular</td>
</tr>
<tr>
<td>Elevation angle</td>
<td>30°</td>
</tr>
<tr>
<td>Number of active beams</td>
<td>( M = 3 )</td>
</tr>
<tr>
<td>Beam diameter</td>
<td>( D = 500 ) km</td>
</tr>
<tr>
<td>3 dB angle</td>
<td>( \theta_{MB} = 0.4° )</td>
</tr>
<tr>
<td>Rain fading statistics</td>
<td>{ \mu; \sigma } = {-3.125; 1.591}</td>
</tr>
</tbody>
</table>

**TABLE I**
PARAMETERS OF THE MULTIBEAM SATELLITE SYSTEM.
iteration goes, the transmit power drops fast to the minimum. Fig. 3 shows the results for the transmit power against the required secrecy rate for $N = 4$ beams. It is observed that the proposed P-ZF approach saves more than 10 dBW and 5 dBW power compared with the C-ZF approach in the low and high rate regions, respectively. Note that on board power is the major driver for the cost of the satellite platform. The performance gain achieved is due to the more intelligent interference management than ZF for legitimate users. While the proposed optimal solution both with and without AN outperforms the existing C-ZF approach significantly for over 20 dBW in all tested secrecy regions thanks to the optimized transmission.

Linking the results reported in Fig. 1 and Fig. 3, Fig. 4 examines the impact of rain attenuation under a secrecy rate constraint of $R = 1 \text{ bps/Hz}$ and $N = 4$ beams. It is observed that a large amount of power is necessary to compensate the high rain fade margins at availability percentages exceeding 99.99%, which however are not typical in practice. Even more substantial transmit power savings of 20-30 dBW over the C-ZF approach are observed than that in Fig. 3 for all three proposed schemes. The optimal solutions proposed are quite robust when the availability is less than 99.9%.

In Fig. 5, results are provided for the total transmit power versus number of transmit antenna feeds on the satellite with the secrecy rate constraint $R = 1 \text{ bps/Hz}$. As can be seen, more transmit antenna feeds indeed save substantial power for both the C-ZF and the proposed P-ZF approach. When the number of feeds $N$ changes from 4 to 7, more than 15 dBW and 10 dBW power savings are observed for the C-ZF and the proposed P-ZF approach, respectively. This is because for both ZF schemes, the primary use of antenna feeds is to null out interference among different receivers either completely or partially. Hence, when there are not many antenna feeds, there is little room to degrade the eavesdroppers’ channels and minimize the transmit power. When $N = 7$, the gap between two ZF schemes becomes smaller and this is because the increased spatial degree-of-freedom helps null out the interference among all receivers completely. While for the proposed optimal solutions, they are not sensitive to the number of the feeds as it can be seen that the variation of transmit power is within 5 dBW for $N = 4 \sim 7$.

An interesting observation from Fig. 3–5 is that, the difference between the proposed optimal solutions with and without AN is hardly seen. This is because as shown in Theorem 2, the main advantage of using AN is the reduced number of required antenna feeds when there are more than one eavesdroppers. While in all previously simulated scenarios, there is only one eavesdropper for each intended user and the rate constraints are not very demanding, therefore AN is not quite necessary in general. In the following, the benefits of using AN will be shown when there are not enough antenna feeds and perfect CSI is not available.

In Fig. 6, we illustrate the feasibility probability against the number of eavesdroppers in each beam. We assume there are $N = 4$ beams and the secrecy rate constraints are $R = 3 \text{ bps/Hz}$. The feasibility probability for the C-ZF approach is trivial, i.e., one when the number of eavesdropper is 1 and

4Feasibility refers to the existence of a feasible solution to (7) or (21) using a specific scheme.
Fig. 6. Probability of feasibility vs. number of eavesdroppers in each beam.

zero otherwise, therefore not shown. First note that when there is only one eavesdropper in each beam, since there are enough antenna feeds $N = M + 1$, all three proposed methods can satisfy the rate constraints. As the number eavesdroppers increases, the feasibility probability drops quickly for the proposed P-ZF and the optimal solution without AN, but not immediately zero, which shows improvement over C-ZF. The advantage of the proposed approach with AN can be clearly seen that it can always satisfy the rate constraints.

Finally, in Fig. 7 we provide the eavesdropper SINR (linear) values when only the channel covariance matrices about the eavesdroppers are known. We assume that each eavesdropper is randomly located on the circle centered at the legitimate user with radius $0.25D$. For the legitimate receivers, a SINR requirement of 10 dB is set. We choose the approach using ZF beamforming to guarantee no interference among legitimate receivers as a benchmark and label it as “ZF Beamforming.” As our objective is to minimize the maximum of received SINRs at eavesdroppers, the received SINRs are balanced which is expected. Fig. 7(a) shows the result when there is a transmit power limit of 40 dBW. The proposed optimal solution without AN can suppress $1/3$ received SINR compared with the ZF approach. Fig. 7(b) shows the result when there is no transmit power limit. With AN, the proposed solution can almost completely block the reception of eavesdroppers and this result is also expected from Theorem 2. The average power for the ZF approach, the proposed optimal solution without AN and the proposed optimal solution with AN are 48.7, 84.5 and 69.8 dBW, respectively.

VIII. CONCLUSIONS

This paper has investigated the transmit beamforming optimization for providing physical-layer security in multibeam satellite systems aiming at setting the ground of this new research direction and enabling the widespread application of secure civil and military data communications via satellite. Taking into account a rain fading channel along with a multifeed satellite antenna and assuming perfect CSI about the eavesdroppers, the problem of minimizing the total transmit power while satisfying individual intended users’ secrecy rate constraints has been studied. A partial ZF approach has been first proposed as an enhancement of existing approaches. By analyzing its convexity, an iterative algorithm combining SDP relaxation and gradient-based method has been proposed to find the approximated optimal solution. We have also studied the use of artificial noise and proved its advantage of guaranteeing secrecy rate. We extended the design to cope with the case when only channel covariance matrices about eavesdroppers are available. Simulation results have shown a substantial performance improvement over the existing complete ZF beamforming without AN, gaining more than 10 dB of power in some cases for typical link availability specifications.

ACKNOWLEDGMENT

The authors would like to thank Société Européenne des Satellites (SES) for the support through SnT-SES partnership.
Björn Ottersten (F’04) (S’87-M’89-SM’99-F’04) was born in Stockholm, Sweden, in 1961. He received the M.S. degree in electrical engineering and applied physics from Linkping University, Linkping, Sweden, in 1986 and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1989.

He has held research positions at the Department of Electrical Engineering, Linkping University; the Information Systems Laboratory, Stanford University, Stanford, CA; and the Katholieke Universiteit Leuven, Leuven, Belgium. In 1991, he was appointed Professor of signal processing at the Royal Institute of Technology (KTH), Stockholm, where he was head of the Department for Signals, Sensors, and Systems from 1992 to 2004 and Dean of the School of Electrical Engineering from 2004 to 2008. Since 2009, he has been Director of securityandtrust.lu at the University of Luxembourg. During 1996-1997, he was Director of Research at ArrayComm Inc, San Jose, CA, a start-up company based on Ottersten’s patented technology. His research interests include wireless communications, stochastic signal processing, sensor array processing, and time-series analysis.

Dr. Ottersten has coauthored papers that received an IEEE Signal Processing Society Best Paper Award in 1993, 2001, and 2006. He has served as Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and on the Editorial Board of the EURASIP Signal Processing Journal and a member of the Editorial Board of the EURASIP Journal of Advances in Signal Processing. Dr. Ottersten is a Fellow of EURASIP. He is a first recipient of the European Research Council advanced research grant.