On Secrecy Performance of Multibeam Satellite System with Multiple Eavesdropped Users

Yeqiu Xiao[1], Jia Liu[2], Jiao Quan[1], Yulong Shen[1(✉)], and Xiaohong Jiang[3]

[1] School of Computer Science and Technology, Xidian University, Xi'an 710071, China
ylshen@mail.xidian.edu.cn
[2] Center for Cybersecurity Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan
[3] School of System Information Science, Future University Hakodate, Hakodate 041-8655, Japan

Abstract. Satellite communication system is expected to play an important role in wireless networks because of its appealing contributions to ubiquitous coverage, content multicast and caching, reducing user expenditure, and so on. However, due to the inherent broadcasting nature and serious channel conditions, satellite communication system is highly vulnerable to eavesdropping attacks. As an initial step towards this end, this paper focuses on the physical layer security technique and explores the secrecy performance of a multibeam satellite system, where multiple legitimate users are served and each user is exposed to an eavesdropper located in the same beam. With perfect channel state information at the satellite and adopting the complete zero-forcing approach for signal processing, we first derive the optimal beamforming vectors to maximize the achievable secrecy rate. Based on this, we further calculate the secrecy outage probabilities of an individual user and the whole system, respectively. Finally, simulation and numerical results are provided to show the secrecy performance of the multibeam satellite system.

Keywords: Multibeam satellite system · Physical layer security
Beamforming · Secrecy outage probability

1 Introduction

Due to the advantages of ubiquitous coverage, no limitation on user geographic position and low user expenditure, satellite communication (SATCOM) system is expected to play a significant role in facilitating the application and commercialization of wireless networks. However, compared with terrestrial communication systems, SATCOM system is much more vulnerable to eavesdropping and jamming attacks, caused by its inherent openness and bad communication conditions

L. Zhu and S. Zhong (Eds.): MSN 2017, CCIS 747, pp. 402–412, 2018.
https://doi.org/10.1007/978-981-10-8890-2_30

(i.e., precipitation attenuation, sky noise, gaseous absorption) [1]. As a result, improving the secrecy performance for SATCOM system is of great importance.

In the past, security in space missions mainly depends on upper layers by cryptographic encryption and decryption mechanisms [2]. However, the features of SATCOM networks, such as the high mobility and limited resources carried by satellites, lead to great difficulties in secret key distribution and management [3,4]. Hence, cryptographic methods cannot completely meet the security demands of satellite communication systems.

Conversely, physical layer (PHY) security based on information-theoretic security [5] has been commonly recognized as the strictest form of security by exploiting the inherent randomness of wireless channels. A basic framework of PHY security, the wiretap channel, was pioneered by Wyner [6] and extended to broadcast channels by Csiszár and Körner [7]. Later, there has been an increasing attraction on physical layer security to guarantee secure terrestrial wireless communication. The concept of secrecy rate is referred to as a rate at which the message can be reliably transmitted but eavesdroppers get no information about the message [3]. To guarantee positive secrecy rate, the legitimate users should have better signal-to-noise ratios (SNRs) than the unintended users. The techniques of multiple-input multiple-output (MIMO) antennas are helpful to improve the security of communication even when legitimate receivers have bad SNRs [3,8,9]. Different secrecy metrics are proposed to evaluate system security under various terrestrial communication scenarios, such as secrecy capacity and secrecy outage probability (SOP) [10–13].

However, there are few works focusing on the PHY security for satellite communication systems with multiple legitimate users. Some of the existed researches are interested in land mobile satellite communication systems or hybrid satellite-terrestrial networks based on Shadowed-Rician model [14–17], while others mainly pay attention to the secrecy transmission of multibeam SATCOM systems [2,18,19]. Multibeam satellite can enhance the channel qualities of intended receivers by generating beams through multiple antenna feeds. In this paper, for the first time, we explore the security performance for a multibeam satellite system with multiple receivers subjected to co-channel inference. A method originating from null-steering beamforming technique [20] is adopted to improve the secrecy rate of each intended user and then we also give out the corresponding derivation of beamforming vector. Finally, simulation and numerical results are carried out to show the secrecy performance of multiform SATCOM systems.

The remainder of this paper is structured as follows. The multibeam satellite system model and problem formulation are introduced in Sect. 2. The beamforming scheme as well as secrecy outage analysis is shown in Sect. 3. Section 4 presents the numerical results, and we conclude the paper in Sect. 5.

Throughout this paper, a number of notations will be adopted. Bold uppercase letters and bold lowercase letters denote matrices and vectors, respectively. $|\cdot|$ represents the modulus of a scalar. $||\cdot||$ is the Euclidean norm for a vector. The mean of a random variable is represented by $\mathbb{E}[\cdot]$. Hermitian transpose and

inverse are represented by $(\cdot)^{\dagger}$ and $(\cdot)^{-1}$, respectively. $\mathbf{A} \odot \mathbf{B}$ denotes Hadamard product of two matrices. $\mathbf{I}_N$ is an $N \times N$ identity matrix. $\mathcal{N}(\mu, \sigma^2)$ denotes the Gaussian distribution with mean μ and variance σ^2. J_k represents the first kind Bessel function of order k.

2 System Model

We consider the downlink of a multibeam satellite communication system with a geostationary satellite, which generates N co-channel beams on the ground via N corresponding antenna feeds (single-feed per beam) leading to a frequency reuse of one, as shown in Fig. 1. There are M ($M < N$) active fixed legitimate users receiving independent data streams from the satellite. The transmit power allocated to each beam is no more than P_0 and it is assumed that at any given time, each beam only serves one legitimate receiver at most. Moreover, we consider that there is a single eavesdropper located in the beam of each legitimate receiver. The overall channels of legitimate users and eavesdroppers can be expressed as

$$\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_M] \tag{1}$$

and

$$\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_M], \tag{2}$$

where $\mathbf{h}_k$ is an $N \times 1$ vector and presents the channel of legitimate user k, and $\mathbf{g}_k$ is an $N \times 1$ vector and presents the channel of the corresponding eavesdropper in the same beam k.

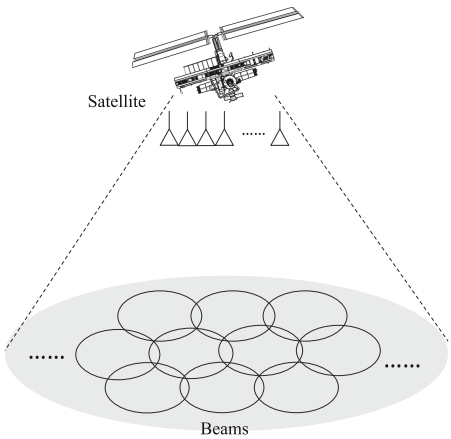


Fig. 1. Multibeam satellite communication scenario.

2.1 Channel Model

Unlike terrestrial communication systems, the satellite systems applying *Ka* band are subjected to various atmospheric fading mechanisms originating in the troposphere, which heavily affects system performance and availability [1]. Hence, it is essential to take the impact of the troposphere, especially, rain attenuation into consideration. Since rain attenuation is a long term effect, we assume that receivers will suffer from the same fading if located within the same beam but independent fading among different beams.

Rain Attenuation. To predict the rain attenuation effect, this paper employs the empirical model proposed in ITU-R Recommendation P.618-12 [21]. The final power gain in dB ($\xi_{dB} = 20\log_{10}(\xi)$) is modeled as a lognormal random $\ln(\xi_{dB}) \sim \mathcal{N}(\mu, \sigma)$, where μ and σ rely on the location of the receiver and the state of the satellite. The corresponding $N \times 1$ rain fading vector from all antenna feeds towards a single terminal antenna is given by [2,22]

$$\mathbf{a} = \xi^{-\frac{1}{2}} e^{-j\Phi}, \tag{3}$$

where Φ denotes an $N \times 1$ phase vector following uniform distribution over $[0, 2\pi)$.

Beam Gain. The beam gain matrix describes the average signal to interference-plus-noise ratios (SINR) at each user. It mainly relies on the satellite antenna beam pattern and the receiver position. We consider a radiation pattern given by [23]:

$$b_k(u) = B_k^{max} \cdot \left(\frac{J_1(u)}{2u} + 36\frac{J_3(u)}{u^3} \right)^2, \tag{4}$$

where $u = 2.07123 \sin\theta_k / \sin(\theta_{3dB})_k$, θ_k represents the angle between the receiver location and the k-th beam center as seen from the satellite and the coefficient, B_k^{max} is the maximum beam gain, J_1 and J_3 denote, respectively, the first kind Bessel functions of order 1 and 3.

Consequently, the overall channel for a certain user can be expressed as

$$\widetilde{\mathbf{h}} = \mathbf{a} \odot \mathbf{b}, \tag{5}$$

where $\mathbf{b}$ is an $N \times 1$ vector and represents the beam gain of the user collected from all transmit antennas.

2.2 Signal Model

Let s_k be the data for user k with unit average power $\mathbb{E}\left[s_k^2\right] = 1, \forall k$. Before transmission, the satellite employs transmit beamforming to communicate with legitimate receivers, and the corresponding beamforming vector is denoted by $\mathbf{w}_k \in \mathbb{C}^{N \times 1}$. Hence, the on board transmitted signal can be expressed as

$$\mathbf{x} = \sum_{k=1}^{M} \mathbf{w}_k s_k. \tag{6}$$

The received signal at the m-th legitimate receiver is given by

$$y_m = \mathbf{h}_m^\dagger \mathbf{w}_m s_m + \mathbf{h}_m^\dagger \sum_{k=1,k\neq m}^{M} \mathbf{w}_k s_k + n_m, \tag{7}$$

and the signal received by its corresponding eavesdropper is determined as

$$y_m^e = \mathbf{g}_m^\dagger \mathbf{w}_m s_m + \mathbf{g}_m^\dagger \sum_{k=1,k\neq m}^{M} \mathbf{w}_k s_k + n_e, \tag{8}$$

where n_k and n_e are the additive Gaussian noises at the m-th legitimate user and the eavesdropper surrounding it, which respectively satisfy $n_m \sim \mathcal{N}(0, \sigma_D^2)$ and $n_e \sim \mathcal{N}(0, \sigma_E^2)$. The term $h_m^\dagger \mathbf{w}_m s_m$ is the desired signal at the m-th legitimate user, while $h_m^\dagger \sum_{k=1,k\neq m}^{M} \mathbf{w}_k s_k$ is the co-channel interference.

Hence, the achievable secrecy rate [24] of the legitimate receiver m can be calculated as

$$C_m^s = \log_2 \left(1 + \frac{\left|\mathbf{h}_m^\dagger \mathbf{w}_m\right|^2}{\sum_{k=1,k\neq m}^{M} \left|\mathbf{h}_k^\dagger \mathbf{w}_k\right|^2 + \sigma_D^2} \right) - \log_2 \left(1 + \frac{\left|\mathbf{g}_m^\dagger \mathbf{w}_m\right|^2}{\sum_{k=1,k\neq m}^{M} \left|\mathbf{g}_k^\dagger \mathbf{w}_k\right|^2 + \sigma_D^2} \right). \tag{9}$$

2.3 Problem Formulation

In this paper, we are interested in maximizing the achievable secrecy rate for each intended user, while subjecting to the transmit power constraint P_0 for each individual transmit signal, which can be formally formulated as the following optimization problem:

$$\begin{aligned} &\arg\max_{\mathbf{w}} \quad C_m^s \\ &s.t. \qquad \|\mathbf{w}_m\| < P_0. \end{aligned} \tag{10}$$

3 Beamforming Vectors and Secrecy Outage Analysis

3.1 Complete Zero-Forcing

In this section, we consider a beamforming design in [18], named complete zero-forcing, to maximize the achievable secrecy rate C_m^s. By use of complete ZF, not only signals at all eavesdroppers are nulled out, but co-channel interference among all users is also completely eliminated. Then we have

$$\mathbf{w}_m^\dagger \mathbf{h}_k = 0, \forall k \neq m \quad \text{and} \quad \mathbf{w}_m^\dagger \mathbf{g}_m = 0, \forall m, \tag{11}$$

which makes the achievable secrecy rate of the legitimate receiver m simplified to

$$C_m^s = \log_2\left(1 + \frac{\left|\mathbf{h}_m^\dagger \mathbf{w}_m\right|^2}{\sigma_D^2}\right). \tag{12}$$

3.2 Problem Solution

The optimization problem in (10) can be reformulated as

$$\begin{aligned} \arg\max_{\mathbf{w}} \quad & C_m^s \\ s.t. \quad & \mathbf{w}_m^\dagger \mathbf{h}_k = 0, \quad \forall k \neq m \\ & \mathbf{w}_m^\dagger \mathbf{g}_m = 0 \\ & \mathbf{w}_m^\dagger \mathbf{w}_m = P_0 \end{aligned} \tag{13}$$

and further formulated as

$$\begin{aligned} \arg\max_{\mathbf{w}} \quad & C_m^s \\ s.t. \quad & \mathbf{\Delta}^\dagger \mathbf{w}_m = \mathbf{0}_{1\times M}, \\ & \mathbf{w}_m^\dagger \mathbf{w}_m = P_0 \end{aligned} \tag{14}$$

where

$$[\mathbf{\Delta}]_{ij} = \begin{cases} [\mathbf{H}]_{ij} & j \neq m \\ [\mathbf{G}]_{ij} & j = m \end{cases}. \tag{15}$$

Here, $\mathbf{H}$ and $\mathbf{G}$ describes the overall channel of all legitimate users and all eavesdroppers mentioned in Sect. 2, respectively.

The problem in (14) could be obtained by the knowledge of null-steering beamformer and its optimal solution is given by as [25]

$$\mathbf{w}_m = \frac{\sqrt{P_0}}{\|(\mathbf{I}_N - \mathbf{F})\,\mathbf{h}_m\|}(\mathbf{I}_N - \mathbf{F})\,\mathbf{h}_m, \tag{16}$$

where $\mathbf{F} = \Delta\left(\Delta^\dagger \Delta\right)^{-1}\Delta^\dagger$ and $\mathbf{I}_N$ is an $N\times N$ identity matrix.

3.3 Secrecy Outage Analysis

In order to evaluate the secrecy performance of the satellite system in this paper, secrecy outage probability is introduced. It expresses the probability that secrecy outage event occurs. Secrecy outage event of an intended user m will occur in the case that its achievable secrecy rate falls below a predefined confidential information rate ε_m. The secrecy outage probability is expressed as

$$P_m^{out} = Pr\left(C_m^s < \varepsilon_m\right). \tag{17}$$

Substituting achievable secrecy rate C_m^s from (12) into (17), the secrecy outage probability (SOP) of the legitimate user m can be rewritten as

$$P_m^{out} = Pr\left(\left|\mathbf{h}_m^{\dagger}\mathbf{w}_m\right|^2 < \sigma_D^2\left(2^{\varepsilon_m} - 1\right)\right). \tag{18}$$

For the whole multibeam satellite system, we introduce two secrecy performance metric measurements in this paper. The first one is a statistic value based on the average SOP of all legitimate receivers

$$P_{average}^{out} = \frac{1}{M}\sum_{k=1}^{M} P_m^{out}, \tag{19}$$

and the second one describes the probability that the system will be secrecy outaged once an intended user cannot keep secure communication with the satellite,

$$P_{strict}^{out} = 1 - \prod_{k=1}^{M}(1 - P_m^{out}), \tag{20}$$

which is a much strict standard.

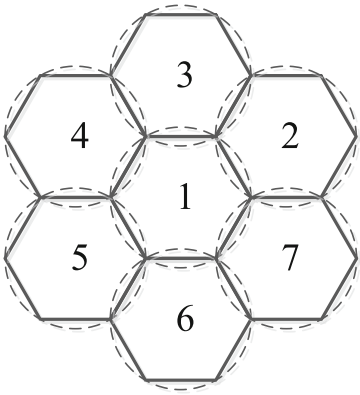
4 Simulation Results Analysis

In this section, we investigate the secrecy outage probability (SOP) of the multibeam satellite communication (SATCOM) system with complete zero-forcing technique. For simplicity, we consider a system with $M = 3$ active beams and assume that all receivers set the same secrecy rate constraint $\varepsilon_m = \varepsilon_0, \forall m$. Each legitimate user is supposed to be located in the beam center while the distance between an unintended receiver and the corresponding legitimate receiver is randomly ranging from $[0.15R, R)$, where R is the beam radius, as shown in Fig. 2. Some significant parameters of the multibeam SATCOM system in this paper are given in Table 1. We will present the secrecy performance of all legitimate users and the whole system, respectively and explore the factors that affect the secrecy performance. Note that aiming at evaluating the secrecy outage probability, this paper performs Monte Carlo experiments consisting of 10000 independent trials to obtain the average results.

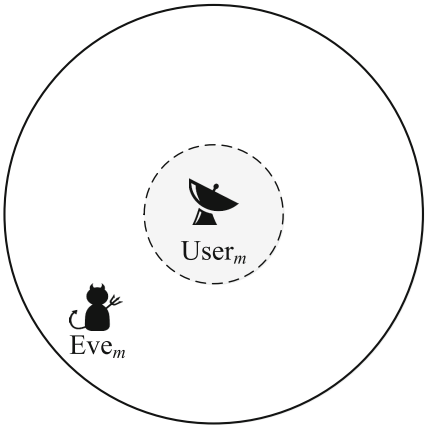
Figure 3 depicts the results for the SOP of each user and the whole system against the secrecy rate constraint in the case that satellite only generates 4 beams. In Figs. 3 and 4, SOP_a and SOP_s correspond to $P_{average}^{out}$ and P_{strict}^{out} mentioned in Sect. 3. It is observed that user 2 (the legitimate receiver in the 2nd beam) would be less likely secrecy outaged compared with others. Taking note that the distance between the legitimate receiver in the 2nd beam and the 4th beam center is larger, communication of user 2 suffers less co-channel interference from the 4th beam. Otherwise, we illustrate that in the view of P_{strict}^{out}, the performance of system secrecy is mainly affected by those users with the worst performance.

Table 1. Main parameters of the multibeam satellite system.

Parameter	Value
Satellite orbit	Geostationary
Number of active beams	$M = 3$
Beam radius	$R = 250$ km
3 dB angle	$\theta_{3dB} = 0.4^\circ$
Rain fading statistics	$\{\mu; \sigma\} = \{-3.125; 1.591\}$
Transmit power constraint	$P_0 = 1\,\mathrm{dB}$



(a) Geographic distribution of beams.



(b) Eavesdropping scenario in a beam.

Fig. 2. A specific multibeam SATCOM scenario.

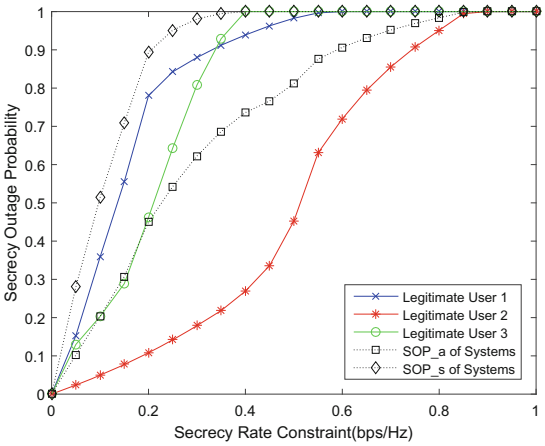


Fig. 3. Secrecy outage probability vs. secrecy rate constraint.

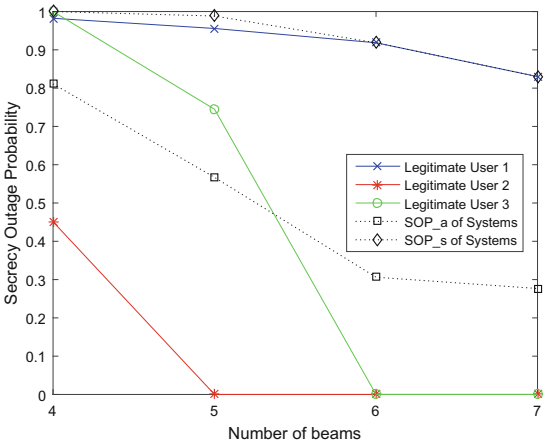


Fig. 4. Secrecy outage probability vs. number of beams.

Figure 4 shows the secrecy outage probability of the system according to the number of beams generated by the satellite. The secrecy rate constraints are randomly selected as $[0.10\ 0.34\ 0.39]^T$. We can notice that two kinds of system SOP both decrease as the number of beams increases. And P_{strict}^{out} of the system is mainly dependent upon the user performing badly.

5 Conclusion

In this paper, we investigated the secrecy performance of a multibeam satellite communication system subject to transmit power constraint. Complete zero-forming technique, a kind of null-steering beamforming method, was adopted to

eliminate co-channel interference. By analyzing the secrecy outage performance of both individual user and the whole system, we found that the secrecy outage probability will decrease as the active beam number increases but the secrecy rate constraint decreases. Simulation results have also shown the fact that the strict standard of system SOP is mainly affected by users with low channel quality.

Acknowledgments. This work was supported in part by the Natural Science Foundation of China (NSFC) under Grant U1536202, Grant 61373173, and Grant 61571352; in part by the Project of Cyber Security Establishment with Inter-University Cooperation; and in part by the Secom Science and Technology Foundation.

References

1. Arapoglou, P.D., Liolis, K., Bertinelli, M., Panagopoulos, A., Cottis, P., De Gaudenzi, R.: MIMO over satellite: a review. IEEE Commun. Surv. Tutor. **13**(1), 27–51 (2011)
2. Zheng, G., Arapoglou, P.D., Ottersten, B.: Physical layer security in multibeam satellite systems. IEEE Trans. Wirel. Commun. **11**(2), 852–863 (2012)
3. Hong, Y.W.P., Lan, P.C., Kuo, C.C.J.: Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. IEEE Signal Process. Mag. **30**(5), 29–40 (2013)
4. Schneier, B.: Cryptographic design vulnerabilities. Computer **31**(9), 29–33 (1998)
5. Shannon, C.E.: Communication theory of secrecy systems. Bell Labs Tech. J. **28**(4), 656–715 (1949)
6. Wyner, A.D.: The wiretap channel. Bell Labs Tech. J. **54**(8), 1355–1387 (1975)
7. Csiszár, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theor. **24**(3), 339–348 (1978)
8. Zou, Y., Zhu, J., Wang, X., Leung, V.C.: Improving physical-layer security in wireless communications using diversity techniques. IEEE Netw. **29**(1), 42–48 (2015)
9. Foschini, G.J., Gans, M.J.: On limits of wireless communications in a fading environment when using multiple antennas. Wirel. Pers. Commun. **6**(3), 311–335 (1998)
10. Barros, J., Rodrigues, M.R.: Secrecy capacity of wireless channels. In: 2006 IEEE International Symposium on Information Theory, pp. 356–360. IEEE (2006)
11. Koyluoglu, O.O., Koksal, C.E., El Gamal, H.: On secrecy capacity scaling in wireless networks. IEEE Trans. Inf. Theor. **58**(5), 3000–3015 (2012)
12. Romero-Zurita, N., Ghogho, M., McLernon, D.: Outage probability based power distribution between data and artificial noise for physical layer security. IEEE Signal Process. Lett. **19**(2), 71–74 (2012)
13. Zou, Y., Zhu, J., Wang, G., Shao, H.: Secrecy outage probability analysis of multiuser multi-eavesdropper wireless systems. In: IEEE/CIC International Conference on Communications in China (ICCC), pp. 309–313. IEEE (2014)
14. An, K., Lin, M., Liang, T., Ouyang, J., Chen, H.: Average secrecy capacity of land mobile satellite wiretap channels. In: 8th International Conference on Wireless Communications & Signal Processing (WCSP), pp. 1–5. IEEE (2016)
15. An, K., Lin, M., Liang, T., Ouyang, J., Yuan, C., Lu, W.: Secrecy performance analysis of land mobile satellite communication systems over Shadowed-Rician fading channels. In: 25th Wireless and Optical Communication Conference (WOCC), pp. 1–4. IEEE (2016)

16. Yan, Y., Zhang, B., Guo, D., Li, S., Niu, H., Wang, X.: Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network. In: 25th Wireless and Optical Communication Conference (WOCC), pp. 1–5. IEEE (2016)
17. An, K., Lin, M., Liang, T., Ouyang, J., Yuan, C., Li, Y.: Secure transmission in multi-antenna hybrid satellite-terrestrial relay networks in the presence of eavesdropper. In: International Conference on Wireless Communications & Signal Processing (WCSP), pp. 1–5. IEEE (2015)
18. Lei, J., Han, Z., Vazquez-Castro, M.Á., Hjorungnes, A.: Secure satellite communication systems design with individual secrecy rate constraints. IEEE Trans. Inf. Forensics Secur. **6**(3), 661–671 (2011)
19. Yuan, C., Lin, M., Ouyang, J., Bu, Y.: Joint security beamforming in cognitive hybrid satellite-terrestrial networks. In: IEEE 83rd Vehicular Technology Conference (VTC Spring), pp. 1–5. IEEE (2016)
20. Friedlander, B., Porat, B.: Performance analysis of a null-steering algorithm based on direction-of-arrival estimation. IEEE Trans. Acoust. Speech Signal Process. **37**(4), 461–466 (1989)
21. Series, P.: Propagation data and prediction methods required for the design of earth-space telecommunication systems. Recommendation ITU-R, 618-12 (2015)
22. Zheng, G., Chatzinotas, S., Ottersten, B.: Generic optimization of linear precoding in multibeam satellite systems. IEEE Trans. Wirel. Commun. **11**(6), 2308–2320 (2012)
23. Díaz, M.A., Courville, N., Mosquera, C., Liva, G., Corazza, G.E.: Non-linear interference mitigation for broadband multimedia satellite systems. In: International Workshop on Satellite and Space Communications (IWSSC 2007), pp. 61–65. IEEE (2007)
24. Liang, Y., Kramer, G., Poor, H.V., Shamai, S.: Compound wiretap channels. EURASIP J. Wirel. Commun. Netw. **2009**, 5 (2009)
25. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)