Unauthorized Access Detection in Underlay Cognitive Satellite Networks

Francesco Benedetto, *IEEE Senior Member*, Gaetano Giunta, *IEEE Senior Member*, and Luca Pallotta, *IEEE Senior Member*

***Abstract*—This letter proposes a higher order moments-based spectrum sensing method for detecting unauthorized accesses in underlay cognitive satellite communication networks. Exploiting the second, fourth and sixth-order moments of the received signal, an estimate of the hidden signal power is evaluated. Then, the power estimation of the unauthorized user is used as decision variable to distinguish among the presence or absence of an unauthorized transmission within the satellite communication network. The effectiveness of the proposed algorithm is assessed by simulation. The analyses have shown that it overcomes some recently published techniques failing in detecting hidden users in underlay cognitive satellite communications.**

***Index Terms*—Cognitive satellite communication networks, spectrum sensing, underlay communications, high order moments, noise uncertainty.**

I. Introduction

COGNITIVE satellite communications are emerging as a promising solution to improve the spectrum utilization efficiency and provide high throughput with a ubiquitous coverage in future beyond 5G (B5G) and 6G communications [1]. Such communications scenarios impose significant threats, as compared to the previous generation of communication networks, and demanding requirements are further imposed on satellite communications [2]. To address such challenges, recent advances in wireless network security have been further explored in the context of cognitive satellite network [3].

Nonetheless security matters in conventional satellite networks have been effectively investigated so far, secure transmission issues in cognitive satellite communications are quite limited. Some efforts have been carried out in satellite-terrestrial networks: Lin et al. [4] studied the security issue of a cognitive satellite-terrestrial network, where a multi-antenna BS was employed as a source of green interference to improve the secrecy performance of primary satellite network. In [5], authors investigated the resource allocation schemes in a secure cognitive satellite-terrestrial network with the presence of a multi-antennas eavesdropper. Analogously in [6], the focus is on the designing of a hybrid satellite-terrestrial spectrum sharing system comprising several terrestrial secondary networks that cooperate with the primary satellite network. Similarly, [7] studied the performance of a multi-beam cognitive satellite terrestrial network where a mobile terrestrial network (secondary) gets some resources of the satellite network (primary) satisfying some constraints on the interference temperature. Then, paper [8] proposed a secure BF scheme in cognitive satellite-terrestrial network by minimizing the transmit power, while guaranteeing a range of outage constraints at both the satellite and terrestrial users. Other interesting developments can be also find in [9] where the authors propose a method aimed at designing cognitive overlay links within the framework of satellite communications to jointly allow the primary and the cognitive users to transmit efficiently using the available powers. Within the context of cognitive satellite terrestrial networks, [10] developed beamforming scheme for secure communications under rate-splitting multiple access (RSMA) assuming the systems operating in millimeter wave band. Moreover, [11] studied the possibility of having multicast communication comprising both satellite and aerial integrated network with RSMA, where both technologies operate in the same frequency band and are controlled by the same network. Finally, an overlay satellite-terrestrial network is also considered in [12], where beyond the primary satellite communications, there is a terrestrial internet-of-things network, opportunistically selected, that acts a power-domain multiplexing to both assists the primary network and also accesses to the spectrum.

However, to the best of our knowledge, no attention has been dedicated to the detection of unauthorized communications in cognitive satellite systems, where the scenario of frequency sharing is represented by the coexistence between the geostationary (GEO) and non-geostationary (NGEO) satellite networks. In particular, the NGEO system (i.e. the secondary user, SU) should not incur harmful interference to the GEO system (i.e. the primary user, PU) according to the policy of the Radio Regulations [13]. Recently, the authors in [14] utilize hypothesis testing and maximum posteriori to detect NGEO satellite signals which impact GEO system. In addition, they compare the performances of their method to the ones of the conventional spectrum sensing approach, namely the energy detector (ED) [15]. However, since both these two methods exploit the signal energy, they fail in detecting hidden communications where the SU (i.e. the unauthorized NGEO) masks itself under the noise floor with an even lower transmitting power.

To address such issues, we propose here a novel (and the first to the best of our knowledge) higher order moments-based spectrum sensing technique to detect low power unauthorized satellite communications in the presence of primary users, i.e. in underlay spectrum communications. The recently published IEEE 1900.1 std [16] defines spectrum underlay as *Dynamic spectrum access by secondary spectrum users*

F. Benedetto, G. Giunta and L. Pallotta are with the Signal Processing for Telecommunications and Economics Laboratory, University of Roma Tre, via Vito Volterra 62, 00146 Rome, Italy (e-mails: francesco.benedetto@uniroma3.it, gaetano.giunta@uniroma3.it, luca.pallotta@uniroma3.it).

that exploit spectral opportunities transmitting below an interference threshold, not causing harmful or even disruptive interference to the incumbent services. Even if the unauthorized users do not cause harmful interference, they must be effectively detected since they represent a system vulnerability. We consider here the problem of unauthorized user detection when the GEO satellite is working all the time since the case of unauthorized detection when the GEO is not working has been considered in [17] (i.e. overlay spectrum communications). The line of reasoning of the proposed technique consists in exploring the capabilities of the second-, fourth-, and sixth-order moments of the received (GEO plus Gaussian noise plus unauthorized NGEO) signal to obtain an effective estimate of the hidden signal power only. In fact, the above moments are the best suited candidates because they can be effectively estimated (estimation error increases with moment's order) and mathematically derived in a closed form. In particular, the unauthorized NGEO signal power is estimated by linearly combining both the second-, fourth-, and sixth-order moment of the received samples, that is then exploited as the decision variable to distinguish among the presence or absence of the hidden communication. Our computer simulations show that the devised method, in the presence of noise uncertainty, can effectively detect such unauthorized hidden signal, while the method in [14] and the conventional ED fail in such a detection. Therefore, we do not provide comparisons in our simulation tests, because of the lacks of other effective methods for detection of underlay satellite communications.

For the reader ease, herein we summarize the main novelties introduced in this letter:

- Study of the problem of detecting low-power underlay spectrum satellite communications when the primary GEO satellite is working all time;
- Development and analysis of a higher order moments-based spectrum sensing technique for the quoted application in scenarios of practical interest.

The structure of this letter can be summarized as in the following. Section II is devoted at formalizing the problem of non authorized transmission detection in satellite communications as well as to derive its solution. Section III provides a discussion of the results of numerical simulations conducted on the proposed algorithm on scenarios of practical interest. Finally, in Section IV some conclusions are drawn together with some hints for possible future developments.

II. System model and proposed solution

This section introduces the problem of the detection of a non-authorized user (NAU) in satellite cognitive communications despite the licensed primary user (PU) communication. More in details, the assumption herein made is that beyond a GEO satellite, which has the license to transmit over a specific frequency band, a non authorized NGEO system (i.e. NAU) transmits at the same time and on the same frequency bands. Since the aim of the NAU is to exploit the spectral resource without any impact on the licensed communications, it is characterized by a very low transmitting power (typically below the noise floor), aimed at hiding its presence. In fact, differently to jammer signals, the NAU does not provide any damage (or the damage can be neglected) to the guesting network because of its low power. Nevertheless, it is important to identify the presence of these non authorized transmissions because they can cause a vulnerability to the network directly impacting on the providers' costs as well as users security. Therefore, a sensing Earth station is devoted at revealing if a NAU is transmitting in spite of the licensed GEO system, as pictorially reported in Figure 1. The NAU can affect both the downlink and uplink transmissions, that can be studied separately; however, without loss of generality as well as to avoid redundancies in the exposition, the study is herein focused on the downlink phase only.

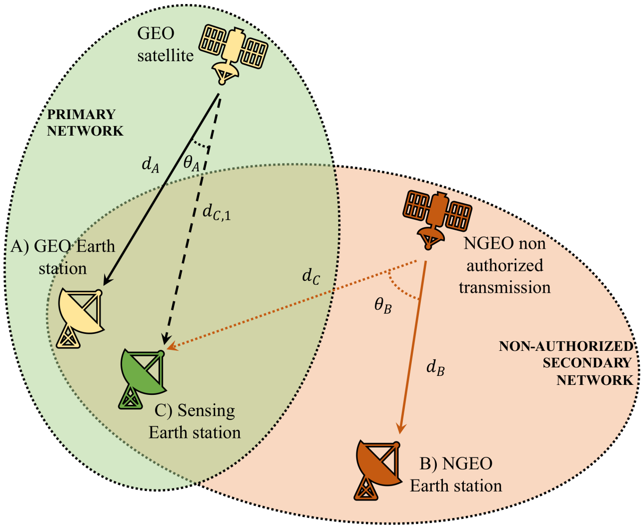

Figure 1. Descriptive scenario of the satellites configuration affected by the presence of an unauthorized user.

As to GEO system, the same system model as in [14], [17] is used, which considers the presence of a GEO satellite capable of transmitting with a possible power level chosen within a finite set, viz. $\sigma^2_{\text{geo},L} > \ldots > \sigma^2_{\text{geo},1} > 0$, and hence it uses a fixed power level during the transmission period [14]. As to the sensing Earth station, an isotropic radiating pattern is considered, since the direction of arrival of the non authorized transmission is not known. As a consequence, indicating with the r_k, $k = 1, \ldots, K$, the k-th signal acquired by the sensing GEO Earth station, the NAU detection problem can be formulated as the following binary hypothesis test

$$\begin{cases} H_0 : r_k = \sigma_{\text{geo}} \xi_{\text{geo}} e^{j\varphi} s_{\text{geo},k} + n_k \\ H_1 : r_k = \sigma_{\text{geo}} \xi_{\text{geo}} e^{j\varphi} s_{\text{geo},k} + n_k + \sigma_{\text{nau}} s_{\text{nau},k} \end{cases} \quad (1)$$

where $n_k \sim \mathcal{CN}(0, 2\sigma^2)$ is the noise term contribution which herein modeled as a zero-mean complex white Gaussian random variable, $\varphi \sim \mathcal{U}(0, 2\pi)$ is the random phase modeling the channel propagating effects uniformly distributed in $[0, 2\pi]$, and that can be neglecting within the sensing framework since the developed sensing system is essentially based on the energy exploitation. Furthermore, $s_{\text{geo},k}$ is the k-th symbol of the GEO satellite transmitted with power σ^2_{geo}, whereas $s_{\text{nau},k}$ represents the k-th transmitted symbol by the NAU with power

σ_{nau}^2 that is typically below the noise floor [18] and assumed also sharing an isotropic antenna. Additionally, ξ_{geo} is a scaling factor modeling the overall link budget from the satellite to the Earth station that is described by the following equation [14]

$$\xi_{\text{geo}}^2 = G_{C,\max} G_{\text{geo}}(\theta_A) \left(\frac{c}{4\pi f_0 d_{C,1}} \right)^2 A_g A_c, \tag{2}$$

where $G_{C,\max}$ indicates the maximum gain of the sensing GEO Earth station receiving antenna, $G_{\text{geo}}(\theta_A)$ represents the gain of the PU (i.e., the GEO satellite) antenna in the direction toward the sensing GEO Earth station θ_A, $c = 3 \times 10^8$ m/s is the speed of light, f_0 is the satellite operating central frequency, and $d_{C,1}$ is the distance between the GEO satellite and the sensing GEO Earth station. Finally, the two quantities A_g and A_c describe the gaseous and the cloud/fog absorption factors, respectively [19], [20].

A. Testing for the presence of a non authorized transmission

To take a decision about the presence or absence of the non authorized satellite signal in the band under test, problem (1) can be recast in a more compact matrix form, i.e.,

$$\begin{cases} H_0 : \boldsymbol{r} = \boldsymbol{s} + \boldsymbol{n} \\ H_1 : \boldsymbol{r} = \boldsymbol{s} + \boldsymbol{f} + \boldsymbol{n} \end{cases}, \tag{3}$$

where $\boldsymbol{n} \sim \mathcal{N}(\boldsymbol{0}, 2\sigma^2 \boldsymbol{I})$ is the noise contribution modeled as a K-dimensional white Gaussian column vector (with $\boldsymbol{I}$ indicating the identity matrix of size $K \times K$), $\boldsymbol{s} = \sigma_{\text{geo}} \xi_{\text{geo}} e^{j\varphi} [s_{\text{geo},1}, \ldots, s_{\text{geo},K}]^T$ is the K-dimensional column vector comprising the K samples of the GEO signal, while $\boldsymbol{f} = \sigma_{\text{nau}} [s_{\text{nau},1}, \ldots, s_{\text{nau},K}]^T$ is the K-dimensional column vector containing the samples of the non authorized transmission. Now, to solve problem (3), a test based on the power of the hidden transmitted signal σ_{nau}^2 is used. In particular, as better described in the following, the decision variable is an estimate of σ_{nau}^2 derived from the higher-order moments of the received data as in [21]. More precisely, since the unknown quantities involved in (3) are the three powers of the GEO signal, the non authorized transmitted signal, and the noise, we resort to the evaluation of the second-, fourth-, and sixth-order moments of the received signal, that are expressed in closed-form in terms of these unknown quantities (in fact, we should use at least three estimated moments to provide a unique solution). So, let indicate with μ_2 the second-order moment of the received signal, defined as

$$\begin{aligned} \mu_2 &= \mathbb{E}\left[\|\boldsymbol{s} + \boldsymbol{f} + \boldsymbol{n}\|^2 \right] \\ &= \mathbb{E}\left[\|\boldsymbol{s}\|^2 \right] + \mathbb{E}\left[\|\boldsymbol{f}\|^2 \right] + \mathbb{E}\left[\|\boldsymbol{n}\|^2 \right] \\ &+ 2\mathbb{E}\left[\Re\{\boldsymbol{s}^\dagger \boldsymbol{f}\} \right] + 2\mathbb{E}\left[\Re\{\boldsymbol{s}^\dagger \boldsymbol{n}\} \right] + 2\mathbb{E}\left[\Re\{\boldsymbol{f}^\dagger \boldsymbol{n}\} \right] \\ &= \mathbb{E}\left[\|\boldsymbol{s}\|^2 \right] + \mathbb{E}\left[\|\boldsymbol{f}\|^2 \right] + \mathbb{E}\left[\|\boldsymbol{n}\|^2 \right], \end{aligned} \tag{4}$$

having indicated with $\Re$ the real part of the argument; moreover, $\mathbb{E}$ denotes the statistical expectation with respect to a random variable that can be easily identified within the context, $\|\cdot\|$ is the Euclidean norm of its argument, and $(\cdot)^\dagger$ is the transpose conjugate operator.

Note that, the last equality in (4) is justified by the independence between the zero-means GEO signal, the non authorized transmission and the noise component, that is

$$\mathbb{E}\left[\Re\{\boldsymbol{s}^\dagger \boldsymbol{f}\} \right] = \mathbb{E}\left[\Re\{\boldsymbol{s}^\dagger \boldsymbol{n}\} \right] = \mathbb{E}\left[\Re\{\boldsymbol{f}^\dagger \boldsymbol{n}\} \right] = 0. \tag{5}$$

Therefore, (4) can be rewritten as

$$\mu_2 = \sigma_{\text{geo}}^2 + \sigma_{\text{nau}}^2 + \sigma^2, \tag{6}$$

whereas a possible estimate, say $\hat{\mu}_2$, is given by

$$\hat{\mu}_2 = \frac{1}{K} \boldsymbol{r}^\dagger \boldsymbol{r} = \frac{1}{K} \sum_{k=1}^{K} |r_k|^2, \tag{7}$$

with $|\cdot|$ indicating the modulus of the complex quantity argument. In a similar way, the fourth-order moment μ_4 of the received signal is formally defined as

$$\mu_4 = \mathbb{E}\left[\|\boldsymbol{s} + \boldsymbol{f} + \boldsymbol{n}\|^4 \right], \tag{8}$$

that can be demonstrated (see [18] to deepen into the mathematical details) to be also equal to

$$\begin{aligned} \mu_4 &= \mathbb{E}\left[\|\boldsymbol{s}\|^4 \right] + \mathbb{E}\left[\|\boldsymbol{f}\|^4 \right] + \mathbb{E}\left[\|\boldsymbol{n}\|^4 \right] \\ &+ 4\mathbb{E}\left[\|\boldsymbol{s}\|^2 \right] \mathbb{E}\left[\|\boldsymbol{n}\|^2 \right] + 4\mathbb{E}\left[\|\boldsymbol{f}\|^2 \right] \mathbb{E}\left[\|\boldsymbol{n}\|^2 \right] \\ &+ 4\mathbb{E}\left[\|\boldsymbol{s}\|^2 \right] \mathbb{E}\left[\|\boldsymbol{f}\|^2 \right] \\ &= \sigma_{\text{geo}}^4 + \sigma_{\text{nau}}^4 + 2\sigma^4 + 4\sigma_{\text{geo}}^2 \sigma_{\text{nau}}^2 + 4\sigma_{\text{geo}}^2 \sigma^2 + 4\sigma_{\text{nau}}^2 \sigma^2. \end{aligned} \tag{9}$$

Analogously to the evaluation of the second-order moment, a possible estimate for μ_4 is given by

$$\hat{\mu}_4 = \frac{1}{K} \sum_{k=1}^{K} |r_k|^4. \tag{10}$$

Finally, following the same line of reasoning used for the previous moments, the six-order moment of the received signal identified by μ_6 can be expressed by

$$\begin{aligned} \mu_6 &= \mathbb{E}\left[\|\boldsymbol{s} + \boldsymbol{f} + \boldsymbol{n}\|^6 \right] \\ &= \sigma_{\text{geo}}^6 + \sigma_{\text{nau}}^6 + 6\sigma^6 + 9\sigma_{\text{geo}}^4 \sigma_{\text{nau}}^2 + 9\sigma_{\text{nau}}^4 \sigma_{\text{geo}}^2 + 9\sigma_{\text{geo}}^4 \sigma^2 \\ &+ 9\sigma_{\text{nau}}^4 \sigma^2 + 18\sigma_{\text{geo}}^2 \sigma^4 + 18\sigma_{\text{nau}}^2 \sigma^4 + 36\sigma_{\text{geo}}^2 \sigma_{\text{nau}}^2 \sigma^2, \end{aligned} \tag{11}$$

with an estimate for it that is given by

$$\hat{\mu}_6 = \frac{1}{K} \sum_{k=1}^{K} |r_k|^6. \tag{12}$$

Now, exploiting (6), (9), and (11), the powers of the three involved signals' contributions, viz. σ_{geo}^2, σ_{nau}^2, and σ^2, can be derived by solving the following non-linear system of equations

$$\begin{cases} \mu_2 &= \sigma^2_{\text{geo}} + \sigma^2_{\text{nau}} + \sigma^2 \\ \mu_4 &= \sigma^4_{\text{geo}} + \sigma^4_{\text{nau}} + 2\sigma^4 + 4\sigma^2_{\text{geo}}\sigma^2_{\text{nau}} + 4\sigma^2_{\text{geo}}\sigma^2 + 4\sigma^2_{\text{nau}} \\ \mu_6 &= \sigma^6_{\text{geo}} + \sigma^6_{\text{nau}} + 6\sigma^6 + 9\sigma^4_{\text{geo}}\sigma^2_{\text{nau}} + 9\sigma^4_{\text{nau}}\sigma^2_{\text{geo}} + 9\sigma^4_{\text{geo}}\sigma^2 \\ & \quad +9\sigma^4_{\text{nau}}\sigma^2 + 18\sigma^2_{\text{geo}}\sigma^4 + 18\sigma^2_{\text{nau}}\sigma^4 + 36\sigma^2_{\text{geo}}\sigma^2_{\text{nau}}\sigma^2 \end{cases} \tag{13}$$

with the sample estimates $\hat{\mu}_2$, $\hat{\mu}_4$, and $\hat{\mu}_6$, respectively derived in (7), (10), and (12), used in (13) in place of the unknown moments, μ_2, μ_4, and μ_6. More precisely, it can be shown that (13) has a unique possible solution [18], that is

$$\hat{\sigma}^2_{\text{geo}} = \sqrt{2\hat{\mu}_2^2 - \hat{\mu}_4}\cos\left(\frac{\gamma}{3}\right) + \sqrt{\frac{1}{2}\left(\hat{\mu}_4 - 2\hat{\mu}_2^2\right)\cos\left(2\frac{\gamma}{3}\right)}, \tag{14}$$

$$\hat{\sigma}^2_{\text{nau}} = \sqrt{2\hat{\mu}_2^2 - \hat{\mu}_4}\cos\left(\frac{\gamma}{3}\right) - \sqrt{\frac{1}{2}\left(\hat{\mu}_4 - 2\hat{\mu}_2^2\right)\cos\left(2\frac{\gamma}{3}\right)}, \tag{15}$$

and

$$\hat{\sigma}^2 = \hat{\mu}_2 - 2\sqrt{2\hat{\mu}_2^2 - \hat{\mu}_4}\cos\left(\frac{\gamma}{3}\right), \tag{16}$$

with

$$\gamma = \arctan\left(\frac{\sqrt{16(2\hat{\mu}_2^2 - \hat{\mu}_4)^3 - (12\hat{\mu}_2^3 - 9\hat{\mu}_2\hat{\mu}_4 + \hat{\mu}_6)^2}}{-12\hat{\mu}_2^3 + 9\hat{\mu}_2\hat{\mu}_4 - \hat{\mu}_6}\right) + \pi, \quad \text{for } 2\hat{\mu}_2^2 \neq \hat{\mu}_4. \tag{17}$$

As a matter of fact, the situation for which $2\hat{\mu}_2^2 = \hat{\mu}_4$ is related to the case of no-transmission, viz. $\hat{\sigma}^2_{\text{geo}} = \hat{\sigma}^2_{\text{nau}}$, that is of no interest for the specific work. After all these premises, indicating with η a suitable detection threshold, the final test for revealing the presence of a non authorized transmission exploits as decision variable the estimates of σ^2_{nau} given in (15), that is

$$\hat{\sigma}^2_{\text{nau}} \underset{H_0}{\overset{H_1}{\gtrless}} \eta, \tag{18}$$

namely if $\hat{\sigma}^2_{\text{nau}} > \eta$, we assume the presence of the NAU, otherwise we decide for its absence.

It is worth to observe that the estimated second, forth, and sixth moments are asymptotically (i.e., $K \to +\infty$) Gaussian for the Khintchine's Strong Law of Large Numbers [22] and that the variable $\hat{\sigma}^2_{\text{nau}}$ is a non-linear but differentiable function of such random variables. As a consequence, if we limit Taylor's polynomial expansion of that function (in the neighborhood of moments' true values) to first order terms, while all the estimation errors of the moments go to zero, then even the testing variable $\hat{\sigma}^2_{\text{nau}}$ tends to be asymptotically Gaussian with mean equal to σ^2_{nau} under both hypotheses. This leads to conclude that the performance in terms of detection and false alarm probabilities P_{D} and P_{FA} could be approximately computed, for very large K, from a theoretical point of view. Their respective expressions can be found in [23] and are omitted herein for sake of brevity.

III. Numerical simulation studies

This section discusses results of computer simulations aimed at assessing the performance of the proposed methodology in terms of non authorized transmission detection in satellite communication systems. To do this, the analyses have been conducted following the Monte Carlo paradigm to evaluate the detection probability (P_{D}) of the non authorized user under several transmitting power conditions. More precisely, a total of 10^4 independent trials have been done to evaluate P_{D}, whereas the detection threshold has been set through the rule of performing $100/P_{\text{FA}}$ independent runs in order to ensure a nominal false alarm probability equal to $P_{\text{FA}} = 10^{-2}$. Additionally, the simulation parameters set-up comprises the availability of 10^6 independent and identically distributed (i.i.d.) samples at the sensing Earth station having the antenna with a gain of 50 dBi, and assuming the overall system working at a central operating frequency in the downlink phase equal to 18.48 GHz. Additionally, the PU is located at an elevation of 35678 km, whereas the gaseous and cloud absorption factors are set to 2 dB and 1 dB, respectively.

Figure 2 shows P_{D} versus the SNR at the receiver side parametrized to different values of non authorized transmission power below the noise level, viz. $\sigma^2_{\text{nau}} = [-11, -9, -7, -5]$ dB and nominally $\sigma^2_{\text{geo}} = 0$ dB. More precisely, the considered simulation settings assume that the actual disturbance variance varies within a specific interval, namely it is assumed $\sigma^2_a \sim \mathcal{U}\left(\sigma^2/\rho, \rho\sigma^2\right)$, with the parameter ρ, which rules the amount of uncertainty [24], set equal to 1 dB. In the above illustrated situation both the method of [14] and the classic energy detector (ED) [15] fail in detecting the NAU user as a consequence of the fact that they are based on the evaluation of the signal's energy. In fact, their curves show very low detection values, i.e. $P_{\text{D}} \approx P_{\text{FA}} = 10^{-2}$. As to the proposed method, the P_{D} curves derived applying the threshold in the asymptotic Gaussian approximation regime are also displayed. Now, from a first visual inspection of the curves of Figure 2, it is evident the capability of the proposed moment-based method in revealing the undesired transmission for low SNR values. Nevertheless, as expected the P_{D}s tend to reduce more and more as the GEO satellite power increases with respect to the thermal noise floor. In fact, for high SNR values, the algorithm is not yet capable of correctly detecting the NAU. In addition, the curves of Figure 2 emphasize the difficulties of the devised methodology in detecting the NAU when it transmits with a very low power.

Now, to corroborate further with the results shown in Figure 2, the next plot of Figure 3 depicts the P_{D} as a function of the NAU power, σ^2_{nau}. The graph shows the curves for different SNRs, viz. SNR $= [8, 14, 20, 26, 30]$ dB. As expected, the trend of growth of the P_{D} with respect to the NAU power is clearly observed. Moreover, the curves associated with low SNRs reach higher and higher P_{D} values for lower and lower σ^2_{nau}. This behavior, from one hand underlines the effectiveness of the proposed method in detecting the NAU, but on the other hand, it shows its limits when the NAU is capable of masking itself in the noise floor with an even lower transmitting power.

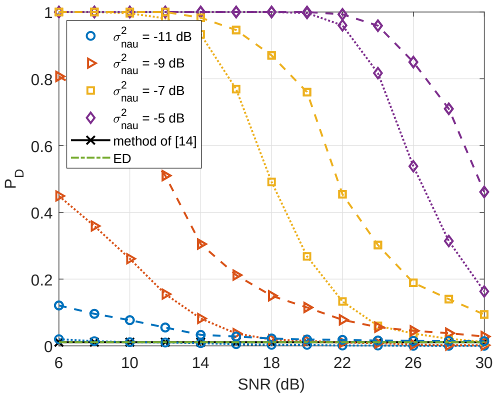

Figure 2. Detection probability versus SNR for $\sigma^2 = 0$ dB and $\sigma^2_{\text{nau}} = [-11, -9, -7, -5]$ dB. Thresholds are set to have a nominal $P_{\text{FA}} = 10^{-2}$ with both the Monte Carlo simulation method (dashed curves) and the asymptotic Gaussian approximation (dotted curves).

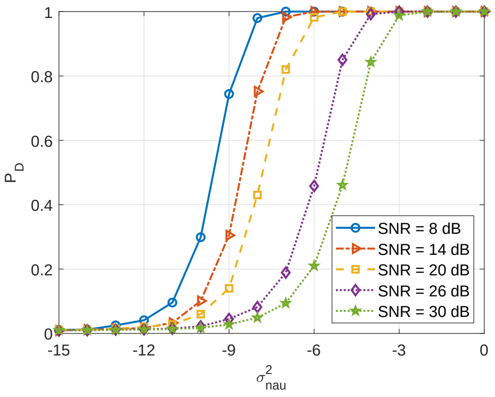

Figure 3. Detection probability versus σ^2_{nau} for $\sigma^2 = 0$ dB and SNR $= [8, 14, 20, 26, 30]$ dB. Thresholds are set to have a nominal $P_{\text{FA}} = 10^{-2}$.

IV. Conclusions

This letter has introduced a novel (and the first to the best of the authors' knowledge) spectrum sensing technique based on high order moments for detecting hidden unauthorized users in underlay cognitive satellite communication networks. The power of the unauthorized SU (i.e. the NGEO) signal is first estimated as a linear combination of both the second-, fourth-, and sixth-order moments of the received noisy signal, and then used as the metric for performing an effective detection. Numerical simulations have shown that conventional detectors fail in performing such a detection while the proposed method can effectively detect hidden unauthorized signals in underlay cognitive satellite communications.

References

[1] X. Wen, Y. Ruan, Y. Li, and R. Zhang, "Cognitive Region Design for Overlay Cognitive Satellite Terrestrial Networks," *IEEE Communications Letters*, vol. 25, no. 1, pp. 244–248, 2020.

[2] N. Panwar and S. Sharma, "Security and Privacy Aspects in 5G Networks," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2020, pp. 1–5.

[3] W. Lu, T. Liang, K. An, and H. Yang, "Secure Beamforming and Artificial Noise Algorithms in Cognitive Satellite-Terrestrial Networks with Multiple Eavesdroppers," *IEEE Access*, vol. 6, pp. 65760–65771, 2018.

[4] Z. Lin, M. Lin, J.-B. Wang, Y. Huang, and W.-P. Zhu, "Robust Secure Beamforming for 5G Cellular Networks Coexisting with Satellite Networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 932–945, 2018.

[5] B. Li, Z. Fei, X. Xu, and Z. Chu, "Resource Allocations for Secure Cognitive Satellite-Terrestrial Networks," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 78–81, 2017.

[6] P. K. Sharma, P. K. Upadhyay, D. B. da Costa, P. S. Bithas, and A. G. Kanatas, "Performance Analysis of Overlay Spectrum Sharing in Hybrid Satellite-Terrestrial Systems With Secondary Network Selection," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6586–6601, 2017.

[7] O. Y. Kolawole, S. Vuppala, M. Sellathurai, and T. Ratnarajah, "On the Performance of Cognitive Satellite-Terrestrial Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 668–683, 2017.

[8] B. Li, Z. Fei, Z. Chu, F. Zhou, K.-K. Wong, and P. Xiao, "Robust Chance-Constrained Secure Transmission for Cognitive Satellite–Terrestrial Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4208–4219, 2018.

[9] L. B. C. d. Silva, T. Benaddi, and L. Franck, "A Design Method of Cognitive Overlay Links for Satellite Communications," in *2018 9th Advanced Satellite Multimedia Systems Conference and the 15th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, 2018, pp. 1–6.

[10] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure and Energy Efficient Transmission for RSMA-based Cognitive Satellite-Terrestrial Networks," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 251–255, 2020.

[11] Z. Lin, M. Lin, T. de Cola, J.-B. Wang, W.-P. Zhu, and J. Cheng, "Supporting IoT with Rate-Splitting Multiple Access in Satellite and Aerial Integrated Networks," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11123–11134, 2021.

[12] P. K. Sharma, B. Yogesh, D. Gupta, and D. I. Kim, "Performance Analysis of IoT-based Overlay Satellite-Terrestrial Networks under the Interference," *IEEE Transactions on Cognitive Communications and Networking*, 2021.

[13] International Telecommunication Union, *Radio Regulations*, 2012.

[14] C. Zhang, C. Jiang, J. Jin, S. Wu, L. Kuang, and S. Guo, "Spectrum Sensing and Recognition in Satellite Systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2502–2516, 2019.

[15] P. De and Y.-C. Liang, "Blind Spectrum Sensing Algorithms for Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 5, pp. 2834–2842, 2008.

[16] "IEEE Standard for Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management - Redline," *IEEE Std 1900.1-2019 (Revision of IEEE Std 1900.1-2008) - Redline*, pp. 1–144, 2019.

[17] F. Benedetto, G. Giunta, and L. Pallotta, "Cognitive Satellite Communications Spectrum Sensing Based on Higher Order Moments," *IEEE Communications Letters*, vol. 25, no. 2, pp. 574–578, 2021.

[18] F. Benedetto, G. Giunta, E. Guzzon, and M. Renfors, "Effective Monitoring of Freeloading User in the Presence of Active User in Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2443–2450, 2013.

[19] A. Dissanayake, J. Allnutt, and F. Haidara, "A Prediction Model that Combines Rain Attenuation and other Propagation Impairments Along Earth-Satellite Paths," *IEEE Transactions on Antennas and Propagation*, vol. 45, no. 10, pp. 1546–1558, 1997.

[20] A. Dissanayake, "Ka-Band Propagation Modeling for Fixed Satellite Applications," *Online Journal of Space Communication*, vol. 2, pp. 1–5, 2002.

[21] F. Benedetto, G. Giunta, E. Guzzon, and M. Renfors, "Detection of Hidden Users in Cognitive Radio Networks," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2013, pp. 2296–2300.

[22] P. K. Sen and J. M. Singer, *Large Sample Methods in Statistics: An Introduction with Applications*, Springer US, 1993.

[23] F. Benedetto and G. Giunta, "A Fast Time-Delay Estimator of PN Signals," *IEEE Transactions on Communications*, vol. 59, no. 8, pp. 2057–2062, 2011.

[24] R. Tandra and A. Sahai, "SNR Walls for Signal Detection," *IEEE Journal of selected topics in Signal Processing*, vol. 2, no. 1, pp. 4–17, 2008.