This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2018.2853629, IEEE Communications Letters

Physical Layer Security in Cognitive Radio Networks Using Improper Gaussian Signaling

Guilherme Oliveira[1], Evelio Fernandez[1], Samuel Mafra[1], Samuel Montejo-Sánchez[2]

***Abstract*—We look into adopting Improper Gaussian Signaling (IGS) in order to enhance the secrecy performance of an underlay Cognitive Radio (CR) network, since in interference-limited networks asymmetric signals have been proven to achieve better performance than proper ones. In this letter, we analyze a scenario where a secondary user (SU) being eavesdropped transmit concurrently with a primary user. A closed-form expression for the Secrecy Outage Probability when only statistical channel state information is available at the secondary transmitter is derived. Results show that IGS can be beneficial for the SUs, especially when secondary transmit power is higher than primary transmit power.**

***Keywords* — Cognitive Radio Networks, Physical Layer Security, Improper Gaussian Signaling, Secrecy Outage Probability.**

I. Introduction

Cognitive Radio (CR) is a key-technology to promote a more efficient spectrum usage, since it is an intelligent system capable of learning from its external environment and adapting its operating parameters to the channel conditions. In the underlay paradigm, the unlicensed users, or Secondary Users (SUs) are allowed to share the same frequency band of licensed users, or Primary Users (PUs), provided that the interference caused to the PUs does not exceed a predefined threshold [1].

The opening of the licensed spectrum to underlay cognitive users, along with the broadcast nature of the wireless media, allows for eavesdropping and other malicious attacks [2]. In the last years, several works [2] have addressed the protection of information in CR networks through the use of Physical Layer Security (PLS) techniques, which are based on the concept of information-theoretic perfect secrecy, not excluding high-layer traditional encryption and keying security techniques. The goal of information-theoretic secrecy is to guarantee higher mutual information in the legitimate links, in comparison to that of the eavesdropper link.

Traditionally, diversity techniques such as cooperative diversity [3] and antenna diversity [4] have been employed to enhance the security of CR wireless systems. In [3], SUs communicate with the aid of relay nodes over Nakagami-m channels. In [4], SUs exploit the benefits of having multiple antennas to combine the received signals. In both works, the PLS is improved at the SU side. Additional techniques to improve CR networks secrecy performance can be found in [2] and in references therein, a comprehensive review regarding PLS in CR networks.

All techniques mentioned above attempt to improve the main channel quality in comparison to the eavesdropper channel. In other words, to achieve the PLS goal for CR networks, one must pursue better transmission rates between legitimate nodes and concurrently manage the interference caused to the PUs. Recent works [5]–[8] have shown that adopting Improper Gaussian Signaling (IGS) in interference-limited networks may be beneficial to the users experiencing and causing interference, since higher transmission rates can be achieved provided that some favorable conditions are assured.

Differently from traditional Proper Gaussian Signaling (PGS), IGS signals have the in-phase and quadrature components correlated or with uneven powers. Straightforwardly, using this technique in CR networks results in a less harmful interference at the PUs, allowing the SUs to transmit with higher power [5]. Therefore, the key idea of this work is to exploit this characteristic of improper signals in order to enhance the network secrecy performance, since it is directly related to the transmission rate and higher SUs rates can be obtained when employing IGS, as found in [5]–[8].

Hence, the objective of this letter is to analyze the secrecy performance of a CR network in which the SUs are subject to eavesdropping and transmit using IGS. To the best of the authors knowledge, this is the first work that addresses the network security issue employing IGS, concurrently with a primary transmission of PGS. The contribution of this letter is twofold. First, the SUs secrecy performance is analyzed adopting a signal design that employs IGS aiming at improving the SUs Secrecy Outage Probability (SOP) while maintaining an acceptable Quality of Service (QoS) at the PUs. Second, a closed-form expression for the SOP of SUs employing IGS is obtained when only statistical channel state information (SCSI) is available at the SU side.

II. System Model

We consider an underlay CR system in which secondary transmissions are subject to eavesdropping, as depicted in Fig. 1. The system encompasses two secondary nodes: a transmitter Alice (A) and a receiver Bob (B), two primary nodes: a Source (S) and a Destination (D), and an eavesdropper Eve (E). Main channels and interference channels coefficients between transmitter i and receiver j are denoted by h_{ij} and g_{ij}, respectively, where $i \in \{a, s\}$, $j \in \{b, d, e\}$, and $\{a, b, e, s, d\}$ denote Alice, Bob, Eve, Source and Destination, respectively.

In the proposed scenario all channels experience Rayleigh flat fading with average channel gain given by $\lambda_{ij} = d_{ij}^{-\alpha}$, where d_{ij} is the distance between nodes and α is the path-loss exponent. Note that h_{ij} and g_{ij} depend on d_{ij}, according to the

[1]Guilherme Oliveira, Evelio Fernandez and Samuel Mafra are with the Federal University of Paraná (UFPR), Curitiba-PR, Brazil. E-mails: gui.schunemann@gmail.com, evelio@ufpr.br, samuel.baraldi@ufpr.br

[2]Samuel Montejo-Sánchez is with Programa Institucional de Fomento a la I+D+i, Universidad Tecnológica Metropolitana, Santiago, Chile. E-mail: smontejo@utem.cl

This work was partially supported by CAPES (Brazil) and FONDECYT Postdoctoral Grant No. 3170021 (Chile).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2018.2853629, IEEE Communications Letters

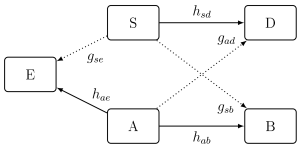

Fig. 1. System Model for a CR Network with Eavesdropper

path-loss model previously stated. In this scenario, the received signals at D, B and E at time t are denoted, respectively, by

$$y_d[t] = \sqrt{P_s}h_{sd}x_s[t] + \sqrt{P_a}g_{ad}x_a[t] + n_d[t], \quad (1)$$

$$y_b[t] = \sqrt{P_a}h_{ab}x_a[t] + \sqrt{P_s}g_{sb}x_s[t] + n_b[t], \quad (2)$$

$$y_e[t] = \sqrt{P_a}h_{ae}x_a[t] + \sqrt{P_s}g_{se}x_s[t] + n_e[t], \quad (3)$$

where P_s and P_a are the transmit powers of primary and secondary transmitters, respectively; $x_s[t]$ and $x_a[t]$ are the transmitted signals by S and A, respectively; whereas $n_d[t]$, $n_b[t]$ and $n_e[t]$ represent the noise at D, B and E, respectively, which is assumed to be Gaussian with variance N_0. Thus, the proper signal-to-interference-plus-noise ratio (SINR) for each link can be written as

$$\gamma_{ij} = \frac{P_i|h_{ij}|^2}{P_k|g_{kj}|^2 + N_0}, k \in \{a, s\} : k \neq i. \quad (4)$$

As usually in the underlay protocol, we consider that there is no cooperation between primary and secondary users. Then, a natural assumption is to consider that S transmits only using PGS, whereas A can employ either PGS or IGS, as in [6] and [7]. Since IGS signals may be statistically circularly asymmetric, the degree of impropriety of Alice's complex signal, $x_a[t]$, is measured by its circularity coefficient C_x, which is defined as [9], [10]:

$$C_x = |\tilde{\sigma}^2_{x_a}|/\sigma^2_{x_a}, \quad (5)$$

where $\sigma^2_{x_a} = \mathbb{E}[|x_a|^2]$ and $\tilde{\sigma}^2_{x_a} = \mathbb{E}[x_a^2]$ are the variance and pseudo-variance of Alice's signal, respectively, and $\mathbb{E}[\cdot]$ is the expected value operator. Knowing that $0 \leq C_x \leq 1$, the signal is called proper if $C_x = 0$, otherwise the signal is said to be improper. Note that $\sigma^2_{x_a} \triangleq P_a$. However, for ease of notation, hereinafter Alice's power is only denoted by P_a.

Hence, when Alice adopts IGS and interference is considered as Gaussian noise, the circularity coefficients of the received signal and of the interference-plus-noise signal at D can be expressed in terms of C_x, respectively, as [8], [11]:

$$C_{y_d} = \frac{P_a|g_{ad}|^2 C_x}{P_a|g_{ad}|^2 + P_s|h_{sd}|^2 + N_0}, \; C_{i_d} = \frac{P_a|g_{ad}|^2 C_x}{P_a|g_{ad}|^2 + N_0}. \quad (6)$$

Then, using (6), the mutual information of the S→D link, can be expressed as [8], [11]:

$$I_{sd} = \log_2\left[(1+\gamma_{sd})\sqrt{\frac{1-C^2_{y_d}}{1-C^2_{i_d}}}\right]. \quad (7)$$

For a more in-depth analysis of (6) and (7), please refer to [8, Eq. (23-30)]. Similarly, the mutual information of the A→B and A→E links can be expressed in terms of C_x. However, for these links, the improper interference-plus-noise signal vanishes, yielding:

$$I_{al} = \log_2\left[(1+\gamma_{al})\sqrt{1-C^2_{al}}\right], \quad (8)$$

where $l \in \{b, e\}$ and

$$C_{al} = \frac{P_a|h_{al}|C_x}{P_s|g_{sl}|^2 + P_a|h_{al}|^2 + N_0}. \quad (9)$$

To consider a fair comparison between Bob and Eve, both nodes are aware that Alice can transmit with PGS or IGS. Similar to [12], it was considered that only SCSI is available at the SU side. That is to say, Alice only knows other channel gains expected value ($\mathbb{E}[|h_{ij}|^2] \triangleq \lambda_{ij}$). The only channel which Alice knows the instantaneous gain is its direct link to Bob, h_{ab}. Hereinafter, all channel gains will be represented by their expected values (λ_{ij}), except for the instantaneous $|h_{ab}|^2$ gain. Since the perfect knowledge of other users CSI is difficult to obtain in practice [13], the knowledge of other channels SCSI can be done by estimating their location in the network or from indirect feedback from band manager [14].

Aiming not to interfere with the primary network, Alice power is limited with respect to a target primary transmission rate, R_s, in a scenario similar to the one adopted in [5]. Then, making $I_{sd} = R_s$ in (7) and solving it with respect to P_a, we obtain a feasible expression to limit Alice's transmit power as a function of R_s:

$$P^{\dagger}_{a,IGS}(C_x, R_s) = \frac{P_s\lambda_{sd} - N_0(2^{2R_s}-1)}{(1-C_x^2)(2^{2R_s}-1)\lambda_{ad}} + \sqrt{\theta_1}, \quad (10)$$

where:

$$\theta_1 = \frac{P_s^2\lambda_{sd}^2 2^{2R_s} + C_x^2(2^{2R_s}-1)(N_0^2 2^{2R_s} - (N_0+\lambda_{sd}P_s)^2)}{(1-C_x^2)^2(2^{2R_s}-1)^2\lambda_{ad}^2}. \quad (11)$$

Therefore, depending on the system parameters, Alice power is allocated according to

$$P_{a,IGS} = \max\{0, \min\{P_{a_{\max}}, P^{\dagger}_{a,IGS}(C_x, R_s)\}\}, \quad (12)$$

where $P_{a_{\max}}$ is the maximum allowable hardware power for Alice transmission, making Alice's power budget a function of C_x and R_s. Note that, numerically, $P^{\dagger}_a$ could achieve negative values when the primary link is not able to transmit with a predefined data rate. However, this would represent an unfeasible situation in the underlay protocol. Hence, it is assumed, in (12), that Alice remains silent when this happens, denoted by an unattainable R_s by the PU.

III. Secrecy Outage Performance Analysis

A secrecy outage event occurs when the mutual information of the A→B link is lower than or equal to that of the link between A→E. Then, using (8) and when only SCSI is available at Alice, the secrecy outage probability can be expressed as:

$$\begin{aligned}\mathcal{O}_{s,IGS} &= \Pr[I_{ab} - I_{ae} < R_a] \\ &= \Pr\left[\frac{(1+\gamma_{ab})^2(1-C^2_{ab})}{(1+\gamma_{ae})^2(1-C^2_{ae})} < 2^{2R_a}\right], \end{aligned} \quad (13)$$

where R_a is the target secrecy data rate, in bpcu.

Moreover, one can show that a closed-form expression for the system SOP may be derived by finding the Cumulative Distribution Function (CDF) of the random variable $|h_{ab}|^2$, which is exponentially distributed due to the Rayleigh fading assumption, as in [12]:

$$\mathcal{O}_{s,IGS} = \int_0^{\psi_1} \frac{\exp(-\frac{|h_{ab}|^2}{\lambda_{ab}})}{\lambda_{ab}}\, d|h_{ab}|^2 = 1 - \exp\left(-\frac{\psi_1}{\lambda_{ab}}\right). \quad (14)$$

The upper limit of the integral in (14) is obtained by solving the inequality in (13) with respect to h_{ab}, and is found to be

$$\psi_1 = \frac{\frac{P_s\lambda_{sb}+N_0}{P_s\lambda_{se}+N_0}\sqrt{\theta_2} - P_s\lambda_{sb} - N_0}{(1-C_x^2)P_{a,IGS}}, \quad (15)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2018.2853629, IEEE Communications Letters

where

$$\theta_2 = C_x^2(N_0 + P_s\lambda_{se})^2 - 2^{2R_a}(1 - C_x^2) \times [(C_x P_{a,IGS}\lambda_{ae})^2 - (P_{a,IGS}\lambda_{ae} + P_s\lambda_{se} + N_0)^2]. \quad (16)$$

One can note that I_{al}, in (8), decreases with the increment of C_x. Nonetheless, since the interference caused at the PU is less harmful than a proper one, Alice can increase its transmission power. Then, it is possible for the SU to increase their achievable rate and, consequently, achieve lower SOP values. This behavior is due to the fact that IGS has lower differential entropy compared to PGS, since its real and imaginary parts are correlated. Thus, when interference is treated as noise, an improper interference increases the achievable rates in scenarios with interference constraints. Consequently, achieving lower SOP values depends on a trade-off between how much improper will the signal be and with how much power will it be transmitted, i.e., a trade-off between C_x and $P_{a,IGS}$, without forgetting to meet the R_s constraint.

Finally, since the SOP is related to the ratio between I_{ab} and I_{ae}, there is a high dependency of the SOP on the average channel gains and on the distance between nodes.

IV. Practical Considerations

In practical implementations, Alice and Bob can always decide to transmit with PGS if better results can be achieved regarding some performance metric (SOP or power consumption). In terms of the SOP, it is only necessary to verify the inequality $\mathcal{O}_{s,IGS} < \mathcal{O}_{s,PGS}$: if true, use IGS, else, use PGS. Although, solving the inequality for C_x is a very complicated task, meanwhile its numerical solution is trivial. Note that the demanded power for a PGS scheme is known [1]:

$$P_{a,PGS} = \frac{\lambda_{sd}P_s - N_0(2^{R_s} - 1)}{\lambda_{ad}(2^{R_s} - 1)}, \quad (17)$$

as well as the SOP [2]:

$$\mathcal{O}_{s,PGS} = 1 - \exp\left(\frac{\psi_2}{\lambda_{ab}}\right), \quad (18)$$

where

$$\psi_2 = \frac{(N_0 + \lambda_{sb}P_s)(N_0 + \lambda_{se}P_s - 2^{R_a}(N_0 + \lambda_{se}P_s + \lambda_{ae}P_{a,PGS}))}{P_{a,PGS}}. \quad (19)$$

Note that (17) and (18) are particular cases of (10) and (14) when $C_x = 0$. In a scenario where it is only mandatory to respect a SOP threshold, one could even test what scheme meets the condition and, in case both PGS and IGS are below the SOP threshold, SUs could pick the one whose power consumption or computational cost is lower.

V. Numerical Results

In this section, numerical results are provided to illustrate the findings presented previously. For the results showed here, a unitary noise variance ($N_0 = 1$) was considered and the path loss exponent was set to $\alpha = 4$. The secrecy rate R_a and the PU target rate R_s were both set equal to 1 bpcu. Assumed S transmit power was $P_s = 10$ dB. In the figures, Monte Carlo simulations are represented by red circles.

In order to suitably select the circularity coefficient C_x, two different settings regarding the relative distance between nodes were assessed, since channels gains are directly dependent of the distance between nodes. In both settings the distances between nodes were normalized with respect to the distance between S and B ($d_{sb} = 1$). Hence, the following values for the remaining distances between nodes for the first and second settings were considered, respectively, (I) $d_{ab} = d_{ad} = 0.5$, $d_{sd} = d_{ae} = 0.7$ and $d_{se} = 0.3$; (II) $d_{ab} = d_{se} = 0.3$ and $d_{ad} = d_{sd} = d_{ae} = 0.7$. Setting I illustrates a scenario where it is most likely that $\lambda_{ab} = \lambda_{ad}$, while Setting II depicts a scenario in which $\lambda_{ab} > \lambda_{ad}$. In this connection, it is worth noting that increasing I_{al} is related to the A→D channel gain, and IGS will achieve better performance than PGS only if $\lambda_{ad} > \lambda_{ab}$, as pointed out in [6].

In Fig. 2 the system SOP was analyzed as a function of C_x, assessing whether IGS is beneficial to the SOP. It is shown that employing PGS is a better strategy for the SU when $P_{a_{\max}} < P_s$ in both settings. When $P_{a_{\max}} = P_s = 10$ dB, there is a clear behavior change among the two distance settings. For distance Setting I, IGS can be beneficial to the system performance, as noticeable from the dashed blue lines.

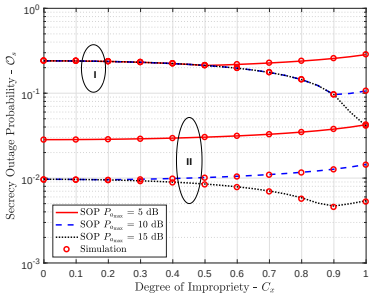

Fig. 2. System SOP *vs* C_x. $P_s = 10$ dB, $R_s = R_a = 1$ bpcu.

In addition, when $P_{a_{\max}} > P_s$, employing IGS is always a better strategy for the SU. Moreover, there is a turning point when $C_x = 0.9$, due to the fact that Alice would be able to transmit with more power without violating the PU acceptable interference threshold when employing IGS. However, Settings I and II differ with respect to the optimal degree of impropriety to be employed. Hence, due to the analysis presented in Fig. 2 the results hereinafter are obtained adopting $C_x = 1$ for distance Setting I and $C_x = 0.9$ for distance Setting II.

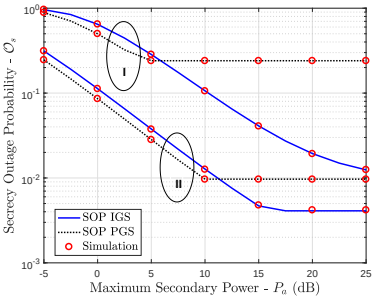

Fig. 3. System SOP *vs* $P_{a_{max}}$. $P_s = 10$ dB, $R_s = R_a = 1$ bpcu.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2018.2853629, IEEE Communications Letters

Now, in order to analyze the system secrecy performance when Alice employs PGS or IGS, in Fig. 3 the SOP is plotted as a function of $P_{a_{\max}}$. It is noticeable that IGS can be beneficial to the secrecy performance of the system if Alice's power is high enough.

At some point, the SOP when Alice employs PGS remains constant, indicating that no more benefits could be obtained even when $P_{a_{\max}}$ increases. The saturation of the SOP in Fig. 3 denotes that increasing $P_{a_{\max}}$ would surpass the R_s interference limit at the PU. As a consequence, Alice must choose another value for P_a, which does not improve the SOP. Thus, when adopting an optimal C_x, it is possible to attain better system performance without affecting the PU performance for both distance settings.

Fig. 4 shows the SOP as a function of P_s and considering $P_{a_{\max}} = 15$ dB. It can be noticed that, as S increases its transmit power, employing IGS is not the best strategy for the SU in terms of the SOP for both distance settings. However, when $P_s < P_{a_{\max}}$ there is a larger performance gain region for IGS over PGS in distance Setting I.

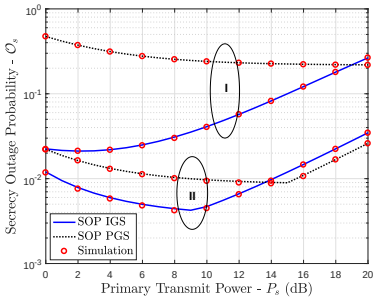

Fig. 4. System SOP *vs* P_s. $P_{a_{\max}} = 15$ dB, $R_s = R_a = 1$ bpcu.

A last interesting analysis is to observe the performance of the system when Eve is no longer at a fixed position. In this scenario, S, D, A and B are located at coordinates $[1, 1]$, $[0.5, 0.5]$, $[1, 0]$ and $[1.5, 0]$ on a bi-dimensional Cartesian plane, respectively. Eve coordinates on this plane are denoted by $[x, y]$, where $x = y = \rho$. Through Monte Carlo simulations, Fig. 5 shows the SOP *versus* ρ while Eve moves from $[0, 0]$ to $[1, 1]$, with increments of 0.1 in both axis simultaneously.

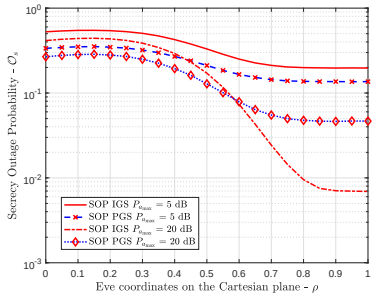

Fig. 5. SOP for moving eavesdropper topology. $P_s = 10$ dB, $P_{a_{\max}} = 15$ dB, $R_s = R_a = 1$ bpcu , IGS: $C_x = 1$, PGS: $C_x = 0$

As Eve moves farther from D, the value of the system SOP decreases for both PGS and IGS signaling. However, when $\rho > 0.6$, IGS attains better performance than PGS, since it can reach lower values of SOP when $P_{a_{\max}} = 20$ dB. This result confirms the potential gain that can be attained using IGS for security interests, indicating that the initial idea of this work is feasible in practice.

VI. Conclusion

This letter analyzed the secrecy performance of the unlicensed users in a CR network when IGS is adopted. A closed-form expression for the SOP when SUs are only aware of SCSI was derived. Later, comparisons between the PGS and IGS cases were made. The results showed that IGS can be beneficial to the system secrecy performance. These results are the first regarding the use of IGS to enhance the PLS of CR networks, a major issue for the development of the future wireless networks. Possible unfolding of this research includes finding an optimal combination of C_x and P_a which minimizes the SOP while maintaining an acceptable QoS at the PU.

References

[1] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 609–612, 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[3] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M. S. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over nakagami- m fading channels," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 614–627, 2017.

[4] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure Transmission in Cognitive MIMO Relaying Networks With Outdated Channel State Information," *IEEE Access*, vol. 4, pp. 8212 – 8224, 2016.

[5] C. Lameiro, I. Santamaria, and P. J. Schreier, "Rate Region Boundary of the SISO Z-Interference Channel With Improper Signaling," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1022–1034, 2017.

[6] ——, "Benefits of Improper Signaling for Underlay Cognitive Radio Christian," *IEEE ICC 2015*, pp. 1398–1403, 2015.

[7] O. Amin, W. Abediseid, and M. S. Alouini, "Underlay cognitive radio systems with improper gaussian signaling: Outage performance analysis," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4875–4887, 2016.

[8] Y. Zeng, C. M. Yetis, E. Gunawan, Y. L. Guan, and R. Zhang, "Transmit optimization with improper gaussian signaling for interference channels," *IEEE Trans. Signal Process.*, vol. 61, no. 11, pp. 2899–2913, 2013.

[9] F. D. Neeser and J. L. Massey, "Proper complex random processes with applications to information theory," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1293–1302, 1993.

[10] P. J. Schreier and L. L. Scharf, "Second-order analysis of improper complex random vectors and processes," *IEEE Trans. Signal Process.*, vol. 51, no. 3, pp. 714–725, 2003.

[11] Y. Zeng, R. Zhang, E. Gunawan, and Y. L. Guan, "Optimized transmission with improper gaussian signaling in the K-user MISO interference channel," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6303–6313, 2013.

[12] M. Gaafar, O. Amin, W. Abediseid, and M. S. Alouini, "Underlay spectrum sharing techniques with in-band full-duplex systems using improper gaussian signaling," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 235–249, 2017.

[13] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On Secrecy Performance of Multiantenna-Jammer-Aided Secure Communications With Imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8014–8024, 2016.

[14] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, 2016.