

Known-Interference Cancellation in Cooperative Jamming: Experimental Evaluation and Benchmark Algorithm Performance

Karel Pärlin, Taneli Riihonen, Matias Turunen, Vincent Le Nir, and Marc Adrat

Abstract—Physical layer security is sought-after in wireless communications to complement the established upper layer security techniques. An appealing approach is to use cooperative jamming with interference that is known to and suppressible by the legitimate receivers. Suppressing known interference (KI), however, is challenging due to the numerous unknowns, including carrier and sampling frequency offsets, that impact its reception. This letter presents a measurement campaign that captures this challenge and then demonstrates cancelling the KI using frequency offsets least mean squares (FO-LMS) algorithm. Results show that KI suppression directly improves processing the signal of interest.

Index Terms—Cooperative jamming, physical layer security, Internet of things, known-interference cancellation.

I. INTRODUCTION

WIRELESS communications are broadcast by nature, which on one hand means that multiple receivers can receive the same transmitted signal, but on the other hand it means that one receiver can receive the superposition of multiple transmitted signals. The former results in significant concern for the security of wirelessly transmitted information because of the susceptibility to eavesdropping, while the latter causes concern about robustness because of the vulnerability to interference. In order to secure wirelessly transmitted information, encryption is typically used on the upper layers of the communication model. In general, cryptographic systems can be implemented to provide reasonable security, but their functioning does rely on secure key exchange and limited adversarial computational capabilities. As such, there is significant interest in complementing the upper layer security at the physical layer [1] and the solution to achieving physical layer secrecy is often seen to be the other side of the broadcast transmission nature — the superposition of multiple signals.

Specifically, if an interference signal can be transmitted so that it superposes the signal of interest at the eavesdropper but not at the intended receiver, then that could secure the transmission. This could be achieved by either having the transmitter itself or a separate cooperative jammer produce

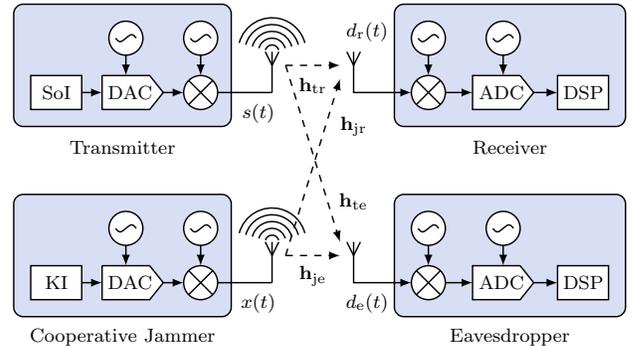


Fig. 1. System model of a cooperative jamming wireless network.

the interference, such that only the eavesdropper's channel is degraded [2]. Targeting a channel between specific devices assumes that the interference transmitter is equipped with multiple antennas and has knowledge about the channel states between the different devices. This, however, can be difficult to obtain in practice, especially if the adversary is passive.

An alternative, that does not rely on such knowledge, is to cover the whole area with interference but suppress it at the receiver. Instead, this relies on the receiver having the technological capability to cancel the interference from the total received signal and it knowing the transmitted interference signal. The latter is achieved if the receiver itself transmits the interference. This also results in self-interference (SI), but that can be suppressed using SI cancellation methods as in in-band full-duplex (IBFD) radios [3]. Such interference-transmitting receivers effectively block out near-by eavesdroppers [4]. However, they also block out near-by non-adversarial nodes, unless those nodes possess known-interference cancellation (KIC) capabilities and know the interference signal. Known interference (KI) from another radio is more complicated to cancel than SI due to oscillator inaccuracies [5] and methods to do so are scarce [6]. Still, information theoretical works often assume perfect KIC [7], [8].

In this work, we further bridge that gap by carrying out an extensive KI measurement campaign¹, demonstrating the practicality of KIC, and studying its impact on signal-of-interest processing. We consider a four-node network as in Fig. 1, where the jammer can be an IBFD node or not, but the focus is on how the interference affects the receiver and eavesdropper. The signal of interest is an IEEE 802.15.4 waveform, basis for many Internet-of-Things applications [9], and we use the waveform agnostic frequency offsets least mean squares (FO-LMS) algorithm [10] for KIC.

Manuscript received November 24, 2022; date of current version November 24, 2022. The associate editor coordinating the review of this paper and approving it for publication was N. Name.

K. Pärlin, T. Riihonen, and M. Turunen are with Tampere University, Faculty of Information Technology and Communication Sciences, Korkeakoulunkatu 1, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi).

V. Le Nir is with Royal Military Academy, Signal and Image Center, Avenue de la Renaissance 30, B-1000 Brussels, Belgium (e-mail: vincent.lenir@rma.ac.be).

M. Adrat is with Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Fraunhofer Straße 20, 53343 Wachtberg, Germany (e-mail: marc.adrat@fkie.fraunhofer.de).

This research work was supported by the Academy of Finland and the Finnish Scientific Advisory Board for Defence.

Digital Object Identifier 10.1109/LWC.202X.XXXXXXX

¹The dataset is published at <https://doi.org/12.1234/XXXX.123.1234567>

II. KNOWN-INTERFERENCE CANCELLATION

The challenges of KIC follow from the system model in Fig. 1. The transmitter broadcasts a **signal** $s(t)$ that is of interest to the receiver and eavesdropper. The jammer, on the other hand, broadcasts a **signal** $x(t)$ that, in its discrete-time **complex** form $x(n)$, is known to the receiver but not to the eavesdropper. Then, the discrete-time signal at the receiver becomes a superposition of those two so that

$$d_r(n) = \mathbf{y}_n^* \mathbf{h}_{jr} e^{j \sum_{i=1}^n \epsilon(i)} + \mathbf{s}_n^* \mathbf{h}_{tr} + v(n), \quad (1)$$

where \mathbf{h}_{tr} and \mathbf{h}_{jr} are the channel impulse responses from transmitter and jammer to the receiver respectively, $\{\cdot\}^*$ denotes conjugate transpose, $v(n)$ is measurement noise with variance σ_v^2 , \mathbf{y}_n accounts for sampling $x(t)$ with **time-varying** sampling frequency offset $\eta(i)$, and the multiplicative term $e^{j \sum_{i=1}^n \epsilon(i)}$ accounts for the carrier frequency offset **and phase noise**. The received signal at the eavesdropper becomes

$$d_e(n) = \mathbf{x}_n^* \mathbf{h}_{je} + \mathbf{s}_n^* \mathbf{h}_{te} + v(n), \quad (2)$$

where \mathbf{h}_{te} and \mathbf{h}_{je} are the channel impulse responses from transmitter and jammer to the eavesdropper respectively, and we ignore the frequency offsets, since the signals are assumed to be unknown to the eavesdropper anyway.

Not knowing $x(n)$, the eavesdropper is stuck with the superposition of the received signals. The receiver, however, can subtract $x(n)$ from the received signal if it is able to estimate \mathbf{h}_{tr} , $\eta(n)$, and $\epsilon(n)$, resulting in

$$e_r(n) = d_r(n) - \hat{\mathbf{y}}_n^* \hat{\mathbf{h}}_{n-1} e^{j \sum_{i=1}^n \hat{\epsilon}(i-1)} \quad (3)$$

where $\hat{\mathbf{h}}_{n-1}$, $\hat{\epsilon}(n-1)$, and $\hat{\eta}(n-1)$ are respectively the estimates of the channel impulse response \mathbf{h}_{tr} , carrier frequency offset, and sampling frequency offset at iteration n , and $\hat{\mathbf{y}}_n$ is the result of resampling $x(n)$ with $\hat{\eta}(n-1)$. With very good parameter estimates, the error in (3) approximates to $e_r(n) \approx \mathbf{s}_n^* \mathbf{h}_{tr} + v(n)$, containing just the signal of interest and measurement noise. In practice, KIC is likely to result in some residual KI that degrades the signal-of-interest processing. The signal-to-interference-plus-noise ratios (SINRs) with and without KIC are defined as

$$\gamma_r = \frac{E[|\mathbf{s}_n^* \mathbf{h}_{tr}|^2]}{E[|e_r(n)|^2] - E[|\mathbf{s}_n^* \mathbf{h}_{tr}|^2]} \quad (4)$$

and

$$\gamma_e = \frac{E[|\mathbf{s}_n^* \mathbf{h}_{te}|^2]}{E[|\mathbf{x}_n^* \mathbf{h}_{je}|^2] + \sigma_v^2}, \quad (5)$$

where $E[\cdot]$ is the statistical expectation operator.

In this work, we use the adaptive FO-LMS algorithm [10] as the reference KIC method. At every iteration, **FO-LMS updates** the parameter estimates [10, Algorithm 1] by **minimizing the error in (3)** so that

$$\hat{\mathbf{h}}_n = \hat{\mathbf{h}}_{n-1} + \mu_w \left[\hat{\mathbf{y}}_n e^{j\phi(n)} \right]^* e_r(n), \quad (6a)$$

$$\hat{\epsilon}(n) = \hat{\epsilon}(n-1) + \mu_\epsilon \Im \left\{ \left[\hat{\mathbf{y}}_n^* \hat{\mathbf{h}}_{n-1} e^{j\phi(n)} \right]^* e_r(n) \right\}, \quad (6b)$$

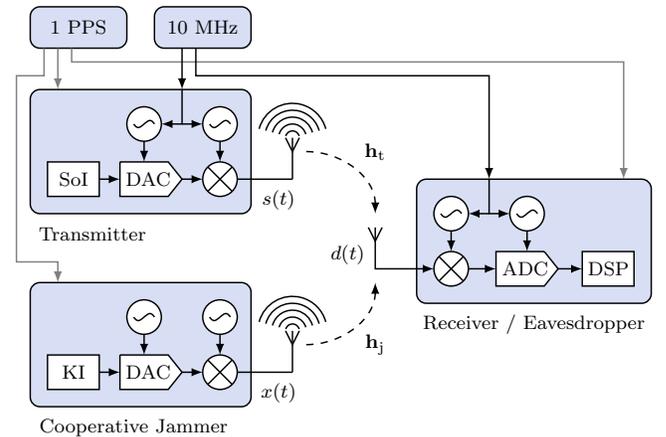
$$\hat{\eta}(n) = \hat{\eta}(n-1) + \mu_\eta \Re \left\{ \left[\hat{\mathbf{y}}_n^* \hat{\mathbf{h}}_{n-1} e^{j\phi(n)} \right]^* e_r(n) \right\}, \quad (6c)$$

where $\hat{\mathbf{y}}_n'$ is the derivative of $\hat{\mathbf{y}}_n^*$ and $\phi(n) = \sum_{i=1}^n \hat{\epsilon}(i-1)$.

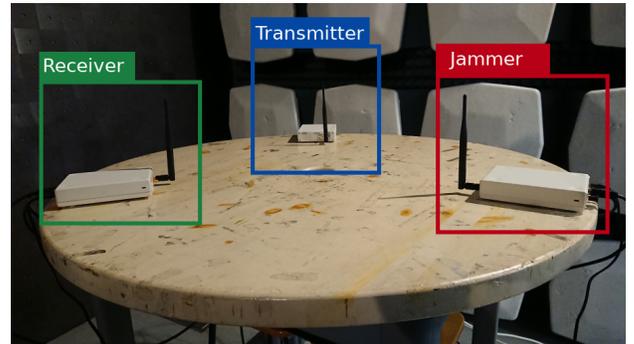
III. MEASUREMENT CAMPAIGN

In order to study the performance of the described KIC approach, we carried out an extensive experiment using the setup illustrated in Fig. 2a. The setup implements the system model with some simplifying modifications. Firstly, the receiver and eavesdropper were implemented using the same hardware, leaving the distinction to be made in software. Secondly, all three devices were connected to a reference timing generator, which provides the option to skip coarse time synchronization of the received signals. Finally, the transmitter and receiver were connected to a reference frequency generator, which makes processing the signal of interest more straightforward. Note that the jammer was not connected to the external frequency reference, meaning that KIC is not simplified.

As shown in Fig. 2b, the measurements were carried out in an anechoic chamber. The three nodes were implemented using USRP-2900 software-defined radios that were positioned on the edges of a table in the middle of the chamber with approximately 0.5 m between any two devices. The radios were configured to 2.45 GHz center frequency with 8 MHz sampling rate. The USRPs provide approximately 90 dB transmit gain range and both transmitting node gains were varied over that range with 5 dB, and some additional 2.5 dB, steps. The entire resulting measurement grid was recorded on disk using the receiver. The receiver gain was kept fixed at a level that took full advantage of the DAC dynamic range when both transmitted signals were at their highest power.



(a) Diagram of the measurement setup.



(b) Photograph of the measurement setup.

Fig. 2. Measurement setup.

The signal of interest was taken to be IEEE 802.15.4, that specifies the physical layer and medium access control sub-layer for low data rate wireless connectivity with fixed, portable, and moving devices with no battery or limited energy consumption requirements [9]. It is the basis for several well-known high-level communication protocols such as Zigbee and 6LoWPAN amongst others. IEEE 802.15.4 specifies multiple physical layer implementation variants. In this work, we used the 2.4 GHz variant that is aligned with our chosen measurement carrier frequency, but is also the most common IEEE 802.15.4 physical layer variant, since it provides the maximum data rate and highest number of RF channels. This variant uses O-QPSK modulation and direct sequence spectrum spreading with about 9 dB of processing gain, offering 250 kbit/s data rate in a 2 MHz channel bandwidth.

For each gain configuration, we made ten separate recordings, each of which consisted of 512 signal-of-interest frames, whereas consecutive frames were separated by a pause in transmission equivalent in length to a frame itself. The KI was transmitted without a pause and covered all the frames. The KI was simple 4 MHz bandlimited Gaussian noise. Furthermore, except for a short burst in the beginning of the KI that optionally facilitates auto-correlation based KI start detection, the KI does not repeat making it difficult for an adversary to estimate the KI signal and sets this work apart from previous KIC experiments [6]. The following analysis takes advantage of the measurement simplifications. That is, the signal-of-interest demodulator knows where each transmitted frame starts in the received signal streams and the KI canceller knows where the KI starts in the received streams, but is then still affected by the carrier and sampling frequency offsets.

IV. RESULTS

The signal of interest and KI are illustrated in Fig. 3, which shows the power spectral density of the received superposed signals without KIC, with KIC, and with perfect KIC (i.e., the signal of interest received without the KI). In this case, we have chosen a point in the measurement grid where the received KI is much more powerful than the received signal of interest. The power spectral density plot already indicates that the reference KIC method suppresses the KI significantly, albeit not perfectly. For a more detailed analysis, Fig. 4 shows the residual KI power before and after cancellation, when there is no signal of interest received. This gives a baseline of how well the method can potentially perform. The results exhibit that FO-LMS is able to cancel the KI at most by about 39 dB before being limited by the nonlinearities and noise within the KI at high KI powers. The results also show that the method works already with very low interference-to-noise ratios.

Fig. 5 is the result of extending the analysis to include the signal of interest. In this case, the signal-of-interest gain is varied and the KI gain is set to 85 dB or 0 dB. The former allows us to get the results with and without KIC, while the latter acts as a reference case that would be achieved with perfect KIC. We look at the bit error rate at the receiver when demodulating the signal of interest. The bit error rate curve is significantly affected by the powerful jamming signal, as

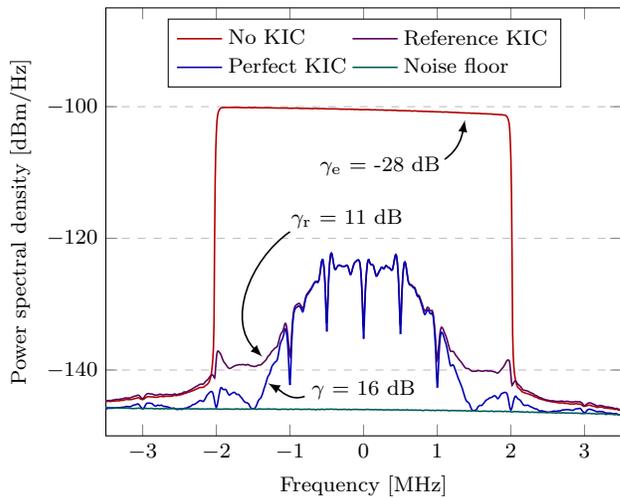


Fig. 3. Power spectral densities of the superposed KI and signal of interest without KIC, with proposed KIC, and with perfect KIC.

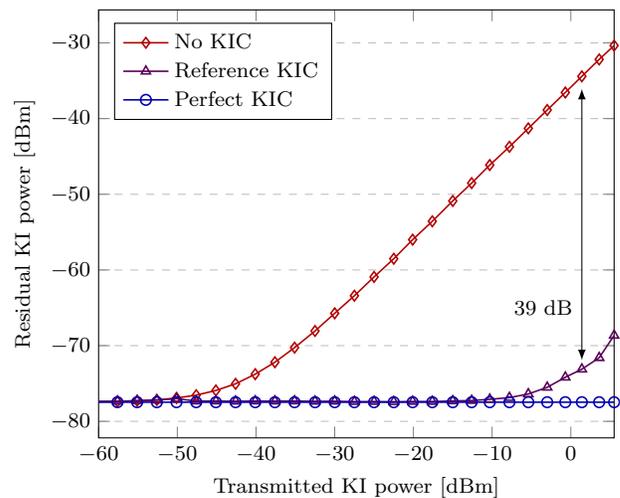


Fig. 4. Efficiency of the reference KIC method without the signal of interest.

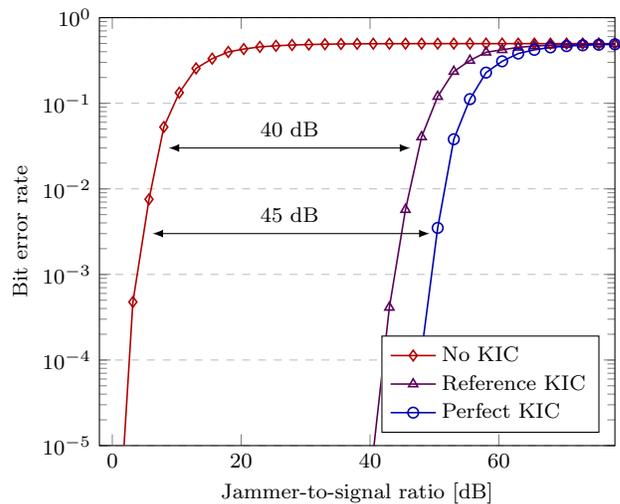


Fig. 5. Performance of the reference KIC when the known interference is received with a fixed power of -34 dBm, on top of which the signal-of-interest power is varied, resulting in the jammer-to-signal ratio on x-axis.

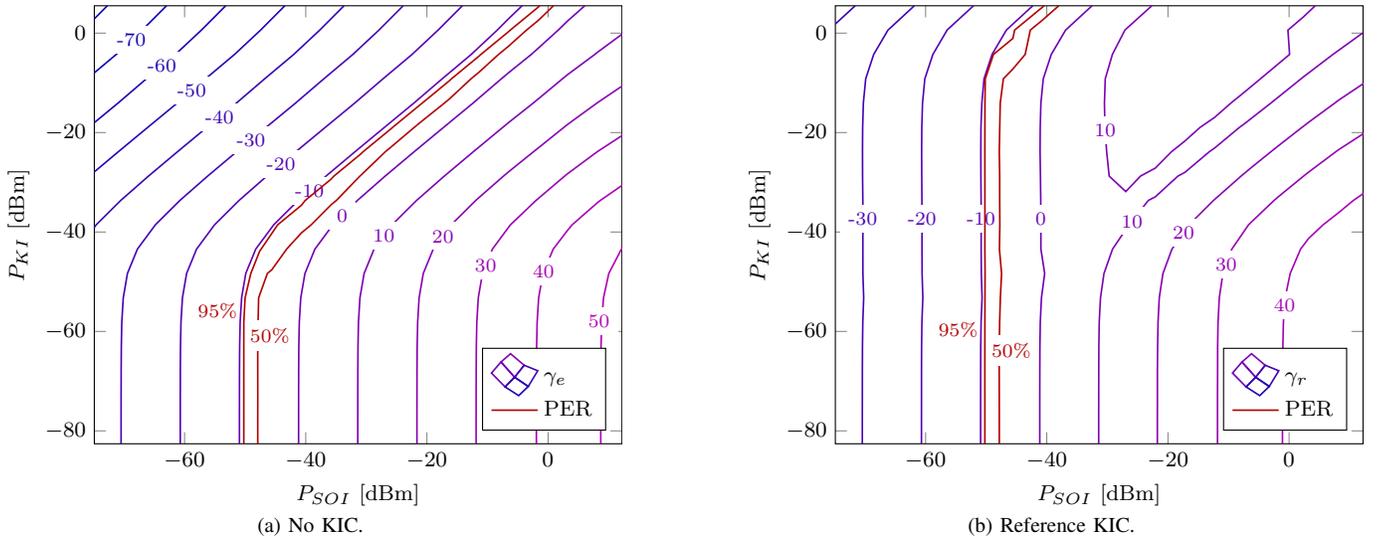


Fig. 6. SINRs at the eavesdropper, γ_e , and receiver, γ_r , (i.e., without and with KIC) along with the PERs. P_{KI} and P_{SOI} are the transmitted signal powers.

expected. The KIC directly translates to improved signal-of-interest demodulation, i.e., the results in Fig. 4 are consistent with those in Fig. 5, despite the added signal of interest. We also see that the residual KI, which remains after the reference KIC, prevents the demodulation performance from reaching that as after the perfect KIC.

Finally, the entire measurement grid is covered in Fig. 6 by plotting SINRs before and after the KIC together with the respective 95% and 50% packet error rate (PER) thresholds. The results characterize the reference KIC performance over a wide range that in practice may occur depending on the transmitted signal powers and node placements. There is a significant portion of the grid, where SINR without the KIC is too poor to successfully demodulate most of the packets, but KIC improves the SINR enough to facilitate successful demodulation. In alignment with the previous results, it is also clear that for high power KI, the reference KIC is unable to suppress the KI all the way to the noise floor, causing some SINR degradation. Similarly, the reference KIC is affected by a powerful signal of interest, which results in the flat SINR area in the upper right corner of Fig. 6b. Still, the reference KIC facilitates a significant shift in the SINR perspective that consequently improves physical layer security.

V. CONCLUSION

This letter studies the practicality of cooperative jamming with an arbitrary known interference (KI) waveform for the purpose of providing physical layer security in the presence of an eavesdropper. Specifically, we look at the capability of the frequency offsets least mean squares (FO-LMS) adaptive algorithm to suppress a KI signal that is received through an unknown channel with carrier and sampling frequency offsets. We also look at how the KI suppression affects the subsequent signal-of-interest processing. To facilitate the analysis in this work and to support further research into this topic, a comprehensive measurement dataset was collected and is released alongside this letter. The analysis results demonstrate that the

FO-LMS is well capable of suppressing a KI signal even when the KI is superposed with a signal of interest. Although, the algorithm is unable to deal with nonlinearities and phase noise in the received KI, which can result in some residual KI after the cancellation and therefore leaves room for improvement of the KI cancellation method. Still, despite these limitations, this approach is shown to be useful for providing physical layer security in the presence of an eavesdropper. Furthermore, this approach can also be used to prevent adversarial nodes from wirelessly communicating within an area while not overly hampering legitimate nodes therein.

REFERENCES

- [1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.
- [2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [3] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Tech.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.
- [4] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.
- [5] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, "Effect of frequency offset on cooperative jamming cancellation in physical layer security," in *Proc. IEEE Globecom Workshops*, Dec. 2018.
- [6] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 240–243, Feb. 2020.
- [7] R. H. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 764–777, Feb. 2010.
- [8] L. Sun, Y. Zhang, and A. L. Swindlehurst, "Alternate-jamming-aided wireless physical-layer surveillance: Protocol design and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1989–2003, Dec. 2020.
- [9] "IEEE standard for low-rate wireless networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020.
- [10] K. Pärilä, T. Riihonen, V. L. Nir, and M. Adrat, "Estimating and tracking wireless channels under carrier and sampling frequency offsets," *IEEE Trans. Signal Process.*, 2022, submitted for review.

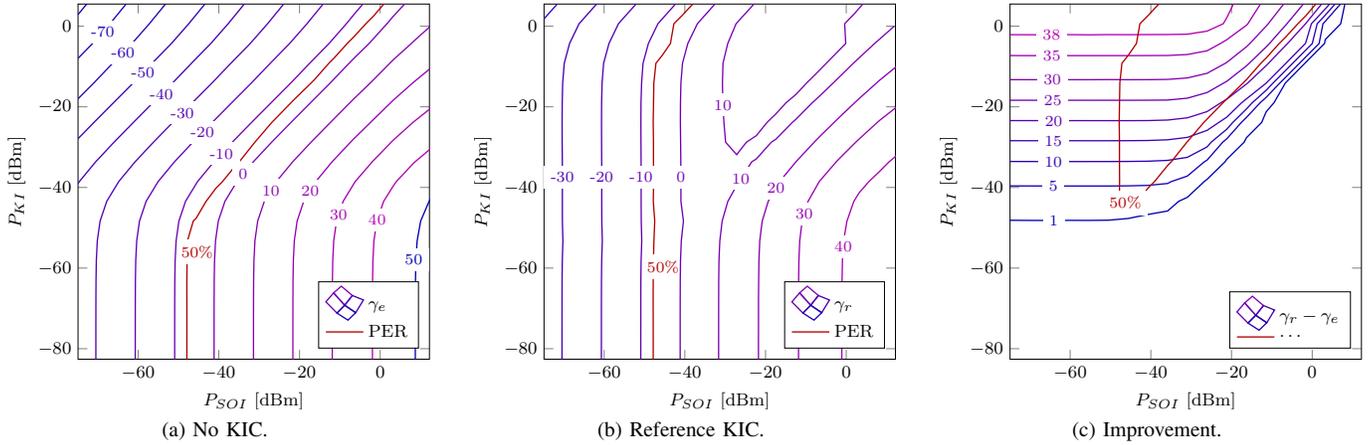


Fig. 7. SINR ratio and 50% packet error rate (PER) threshold at the eavesdropper and receiver (i.e., without and with KIC). The PER drops very quickly and only a single level is plotted for visual clarity. *Alternative for Fig. 6.*

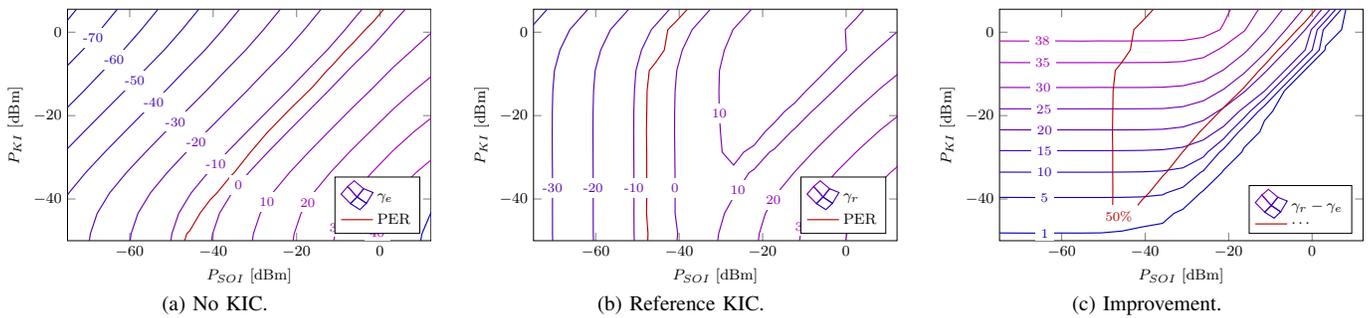


Fig. 8. SINR ratio and 50% packet error rate (PER) threshold at the eavesdropper and receiver (i.e., without and with KIC). The PER drops very quickly and only a single level is plotted for visual clarity. *Alternative for Fig. 6.*