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

Karel Pärlin, Taneli Riihonen, *Senior Member, IEEE*, Matias Turunen, Vincent Le Nir, and Marc Adrat

***Abstract*—Physical layer security is a sought-after concept to complement the established upper layer security techniques in wireless communications. An appealing approach to achieve physical layer security is to use cooperative jamming with interference that is known to and suppressible by the legitimate receiver but unknown to, and hence not suppressible by, the eavesdropper. 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 the feasibility of solving that challenge by cancelling the KI using the frequency offsets least mean squares (FO-LMS) algorithm. Results show that KI suppression directly improves processing the signal-of-interest and that cooperative jamming effectively provides security at the physical layer.**

***Index Terms*—Cooperative jamming, physical layer security.**

I. Introduction

WIRELESS communications are by nature broadcast, 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 the interference, such that only the eavesdropper is affected [2]. Targeting an eavesdropper this way requires the nodes to be positioned favorably, but also that the interference transmitter is capable of directing the interference and knows how the devices are positioned. This awareness, 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 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] somewhat negligently.

In this letter, we help bridge that gap between theory and practice by carrying out an extensive KI measurement campaign,[1] 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.

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 baseband complex form $x(n)$, is known to the receiver but not to the eavesdropper. Then, the discrete-time signal at the

Manuscript received 9 May 2023; accepted 4 June 2023. Date of publication 8 June 2023; date of current version 8 September 2023. This work was supported in part by the Academy of Finland and in part by the Finnish Scientific Advisory Board for Defence. The associate editor coordinating the review of this article and approving it for publication was L. Yang. *(Corresponding author: Karel Pärlin.)*

Karel Pärlin, Taneli Riihonen, and Matias Turunen are with the Faculty of Information Technology and Communication Sciences, Tampere University, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi).

Vincent Le Nir is with the Signal and Image Center, Royal Military Academy, 1000 Brussels, Belgium.

Marc Adrat is with the Fraunhofer Institute for Communication, Information Processing and Ergonomics, 53343 Wachtberg, Germany.

Digital Object Identifier 10.1109/LWC.2023.3284006

[1] Measurement dataset is available at https://dx.doi.org/10.21227/9mty-pf96.

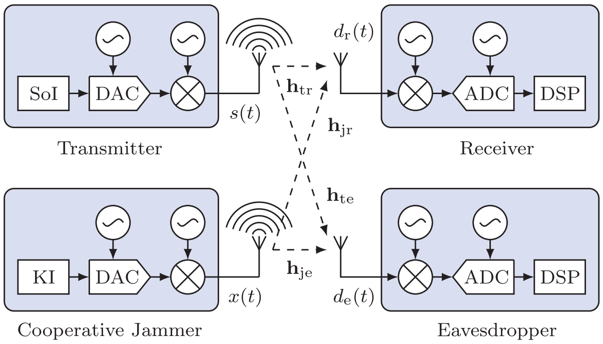


Fig. 1. System model of cooperatively jammed wireless communications.

receiver becomes a superposition of those two so that

$$d_\mathrm{r}(n) = \mathbf{h}_\mathrm{jr}^H \mathbf{y}_n e^{j\sum_{i=1}^{n} \epsilon(i)} + \mathbf{h}_\mathrm{tr}^H \mathbf{s}_n + v(n), \tag{1}$$

where $\mathbf{h}_\mathrm{tr}$ and $\mathbf{h}_\mathrm{jr}$ are the channel impulse responses from transmitter and jammer to the receiver respectively, $\{\cdot\}^H$ 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 $\eta(i)$ according to (2) in [10], 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

$$d_\mathrm{e}(n) = \mathbf{h}_\mathrm{je}^H \mathbf{x}_n + \mathbf{h}_\mathrm{te}^H \mathbf{s}_n + v(n), \tag{2}$$

where $\mathbf{h}_\mathrm{te}$ and $\mathbf{h}_\mathrm{je}$ are the channel impulse responses from transmitter and jammer to the eavesdropper respectively, and we can 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 $\mathbf{h}_\mathrm{tr}$, $\eta(n)$, and $\epsilon(n)$, resulting in

$$e_\mathrm{r}(n) = d_\mathrm{r}(n) - \hat{\mathbf{h}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\sum_{i=1}^{n} \hat{\epsilon}(i-1)} \tag{3}$$

where $\hat{\mathbf{h}}_{n-1}$, $\hat{\epsilon}(n-1)$, and $\hat{\eta}(n-1)$ are respectively the estimates of the channel impulse response $\mathbf{h}_\mathrm{tr}$, 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 $e_\mathrm{r}(n) \approx \mathbf{h}_\mathrm{tr}^H \mathbf{s}_n + v(n)$, 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.

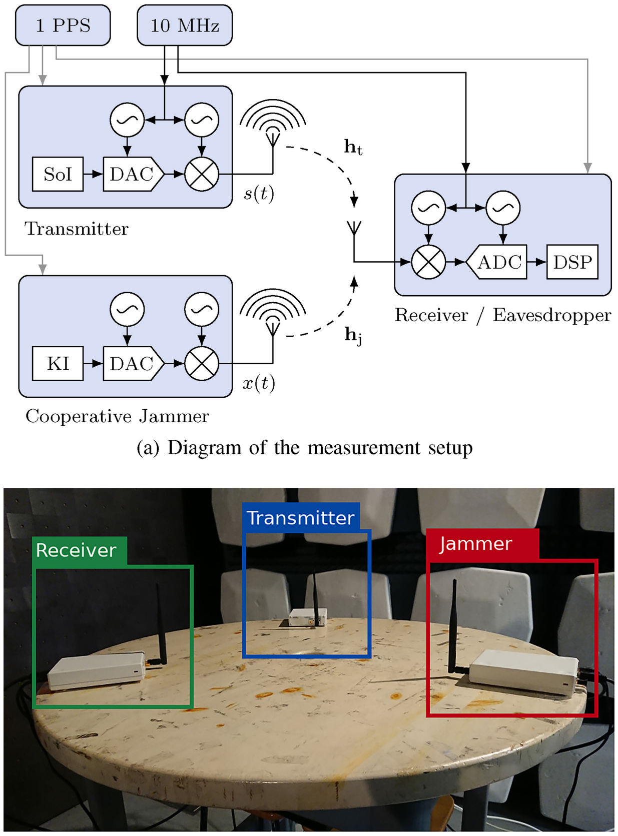
The signal-to-interference-plus-noise ratios (SINRs) with and without KIC are defined as

$$\gamma_\mathrm{r} = \frac{E\left[|\mathbf{h}_\mathrm{tr}^H \mathbf{s}_n|^2\right]}{E\left[|e_\mathrm{r}(n) - \mathbf{h}_\mathrm{tr}^H \mathbf{s}_n|^2\right]} \tag{4}$$

and

$$\gamma_\mathrm{e} = \frac{E\left[|\mathbf{h}_\mathrm{te}^H \mathbf{s}_n|^2\right]}{E\left[|d_\mathrm{e}(n) - \mathbf{h}_\mathrm{te}^H \mathbf{s}_n|^2\right]} = \frac{E\left[|\mathbf{h}_\mathrm{te}^H \mathbf{s}_n|^2\right]}{E\left[|\mathbf{h}_\mathrm{je}^H \mathbf{x}_n|^2\right] + \sigma_\mathrm{v}^2}, \tag{5}$$

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



(a) Diagram of the measurement setup

(b) Photograph of the measurement setup

Fig. 2. Setup for over-the-air experiments in an anechoic chamber.

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

$$\hat{\mathbf{h}}_n = \hat{\mathbf{h}}_{n-1} + \mu_\mathrm{h} \hat{\mathbf{y}}_n e^{j\phi(n)} e_\mathrm{r}^*(n), \tag{6a}$$

$$\hat{\epsilon}(n) = \hat{\epsilon}(n-1) + \mu_\epsilon \Im\left\{\hat{\mathbf{h}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\phi(n)} e_\mathrm{r}^*(n)\right\}, \tag{6b}$$

$$\hat{\eta}(n) = \hat{\eta}(n-1) + \mu_\eta \Re\left\{\hat{\mathbf{h}}_{n-1}^H \hat{\mathbf{y}}'_n e^{j\phi(n)} e_\mathrm{r}^*(n)\right\}, \tag{6c}$$

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. 2(a). 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, a reference timing generator was used that *optionally* provides initial synchronization across the devices and emulates that step required in practical implementation. Finally, the transmitter and receiver were connected to a reference frequency generator, which makes processing the signal-of-interest more straightforward and allows us to focus the analysis on the KIC performance but in no way simplifies cancelling the KI.

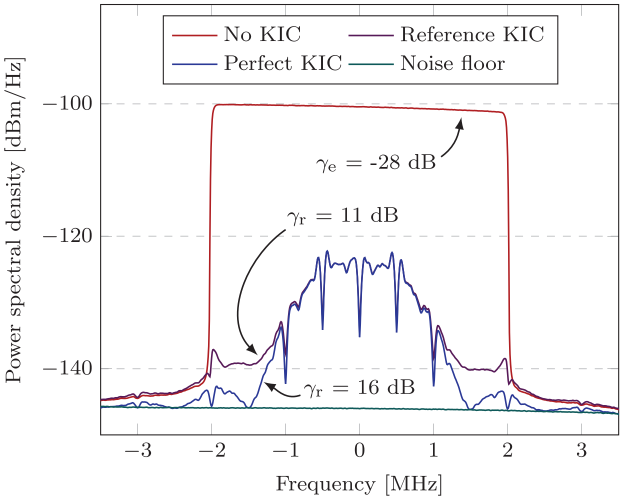


Fig. 3. Power spectral densities of the superposed KI and signal-of-interest without KIC, with proposed KIC, and with perfect KIC.

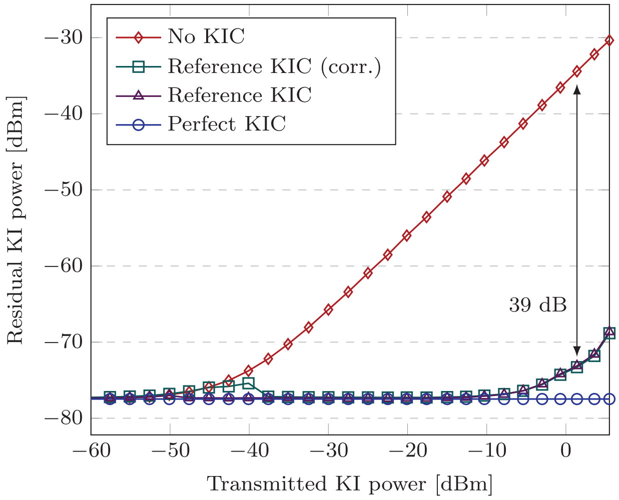


Fig. 4. Efficiency of the reference KIC method without the signal-of-interest and without or with existing coarse time synchronization.

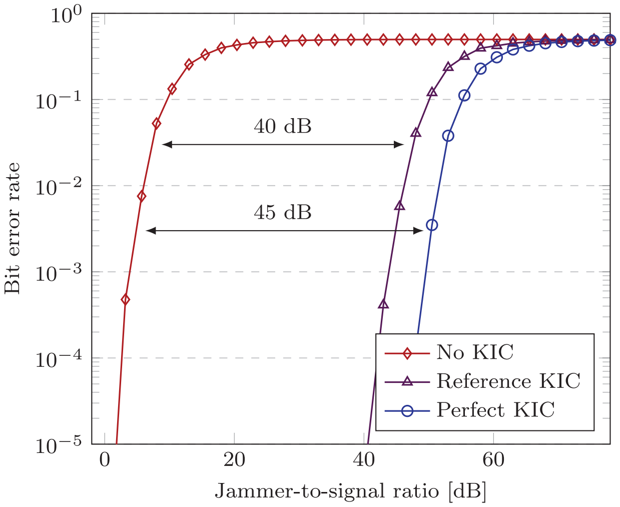


Fig. 5. Performance of the reference KIC when the known interference is received with a fixed power of −34 dBm, on top of which the signal-of-interest power is varied, resulting in the jammer-to-signal ratio on x-axis.

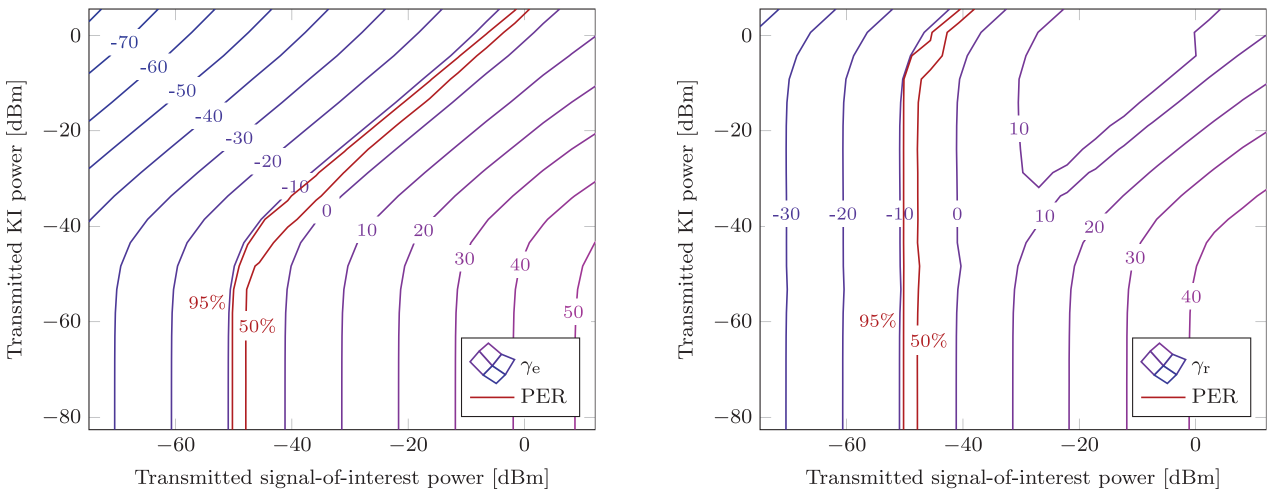
As shown in Fig. 2(b), the measurements were carried out in an anechoic chamber. The three nodes were implemented using USRP-2900 software-defined radios that were positioned on the edges of a table in the middle of the chamber with approximately 0.5 m between any two devices. The radios were configured 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[1] was recorded on a drive 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.

The signal-of-interest was taken to be IEEE 802.15.4 that specifies the physical layer and medium access control sublayer 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 letter, we used the 2.4 GHz option 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. The KI was 4 MHz bandlimited noise created with a pseudorandom number generator and filtering. This approach would also straightforwardly facilitate generating the same signal across legitimate nodes in practice, relying only on a pre-shared secret seed to avoid transferring and storing the complex-valued baseband jamming waveform into each device. Furthermore, except for a short burst (2048 samples in length) 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 letter apart from previous KIC experiments [6]. The following analysis takes advantage of the measurement simplifications but also demonstrates the use of the repeated start sequence. That is, the signal-of-interest demodulator always knows where each transmitted frame starts in the received signal streams since the aim is to focus on KIC performance. The KI canceller, however, either knows where the KI starts in the received streams or detects its start through auto-correlation. In either case, the KI canceller is then still affected by the carrier and sampling frequency offsets.

IV. Experimental 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.,



(a) No KIC

(b) Reference KIC

Fig. 6. SINRs at the eavesdropper, γ_e, and receiver, γ_r, (i.e., without and with KIC) along with the PERs with regards to the transmitted signal powers.

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. This view 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 without and with cancellation when there is no signal-of-interest received. Either auto-correlation is used to detect the start of the KI or the coarse time synchronization from the shared timing generator is relied on. The latter results in a more robust cancellation at low received interference powers as the correlation-based signal detector can in that range misjudge the start of the signal beyond the extent that the FO-LMS algorithm can handle (i.e., the offset is larger than the estimated channel impulse response length).

Altogether this gives a baseline understanding of how well the method can potentially perform. The results exhibit that FO-LMS is able cancel the KI at most by about 39 dB before being limited by the nonlinearities and noise within the KI at high KI powers. Given that the estimated carrier and sampling frequency offsets were on the order of kilohertz and hertz respectively, the performance is nonetheless very good. In Fig. 5, the analysis is extended 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. Firstly, the bit error rate curve is significantly affected by the powerful jamming signal, as expected. Secondly, 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. Unfortunately this also means that the residual KI remaining after the reference KIC prevents the demodulation performance from reaching that as after the perfect KIC.

The entire measurement grid is presented in Fig. 6 by plotting SINRs before and after the KIC together with the 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. We see that 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 above 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. 6(b). Still, the reference KIC facilitates a significant shift in the SINR.

That shift in the SINR consequently provides security at the physical layer. This is evident by contrasting the results from Fig. 6 with that of the perfect KIC and calculating the secrecy capacity that the legitimate receiver has over the eavesdropper given either reference or perfect KIC at the receiver. The secrecy capacity, $C_s = \max\{\log_2(1+\gamma_r) - \log_2(1+\gamma_e), 0\}$, is plotted in Fig. 7 with regards to the received KI and signal-of-interest powers. It is clear that the reference KIC does not always allow to achieve quite the same secrecy capacity as perfect KIC would. At high KI and low signal-of-interest powers (i.e., upper left corner), this is due to the reference method's inability to deal with nonlinearities in the KI. When the signal-of-interest power is relatively high compared to the KI power (i.e., lower right corner), this is because the signal-of-interest hampers the KIC. However, the physical layer security provided by the reference KIC is still significant, especially considering that without KIC the secrecy capacity is zero since then $\gamma_r = \gamma_e$ in the experiments.

V. Conclusion

In this letter, we studied the practicality of cooperative jamming with an arbitrary known interference (KI) waveform for the purpose of providing physical layer security in the presence

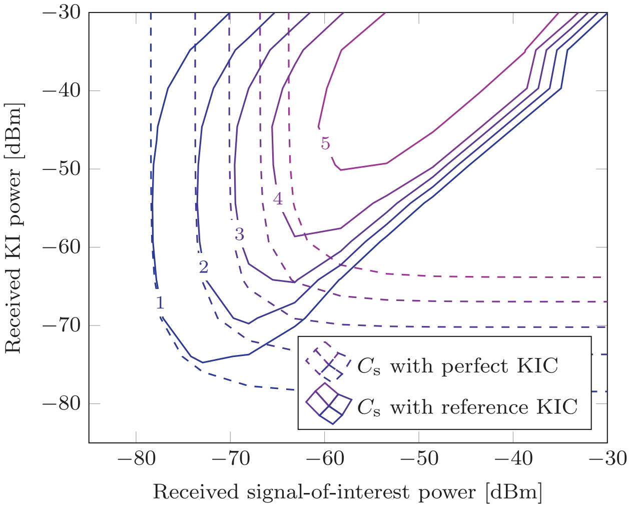


Fig. 7. Secrecy capacity, C_s, in bps/Hz with perfect and reference KIC.

of an eavesdropper. Specifically, we looked 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 analyzed how the KI suppression affects the subsequent signal-of-interest processing. To facilitate the analysis in this letter, and to support further research into this topic, a comprehensive measurement dataset was collected and is released alongside this letter.[1] The experimental results demonstrated that the FO-LMS is well capable of suppressing a KI signal even when the KI is superposed with a signal-of-interest. The algorithm is, though, 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, the results showed that this approach is useful for providing physical layer security in the presence of an eavesdropper. Furthermore, this approach could 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, 3rd Quart., 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 Techn.*, 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, pp. 1–5.

[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, 2020.

[9] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Standard 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), 2020.

[10] K. Pärlin, T. Riihonen, V. Le Nir, and M. Adrat, “Estimating and tracking wireless channels under carrier and sampling frequency offsets,” *IEEE Trans. Signal Process.*, vol. 71, pp. 1053–1066, Mar. 2023.