Wideband Cooperative Jamming with Band-Limited Known-Interference Cancellation

Karel Pärlin*, Vincent Le Nir†, Tommi Meriläinen‡, Aaron Byman‡, Marc Adrat§, and Taneli Riihonen*
*Tampere University, Finland
†Royal Military Academy, Belgium
‡Bittium, Finland
§Fraunhofer FKIE, Germany
e-mail: karel.parlin@tuni.fi

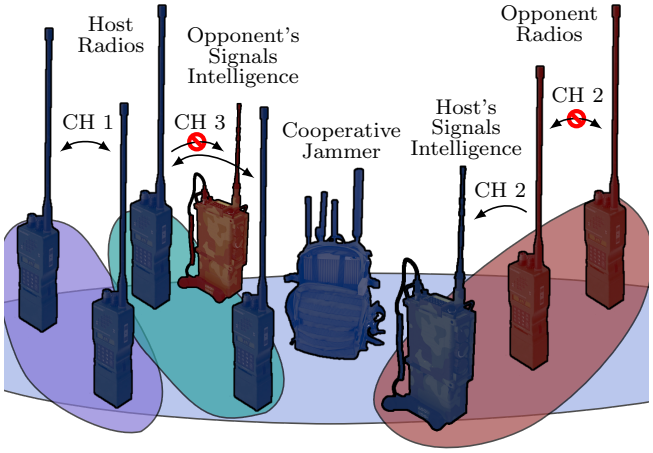
***Abstract*—Secure and reliable communications are vital to defense forces in achieving operational goals. Likewise, limiting the opponents' capabilities to communicate further advances the host forces' chances of operational success. In this work, we propose a method to fortify the host forces' wireless communications against adversarial attacks while at the same time restricting the opponents' capabilities to wirelessly communicate. That is, we propose a band-limited known-interference cancellation (KIC) method that enables the host forces to cover a large portion of the electromagnetic spectrum with wideband jamming, yet lets the host force communication nodes cancel that jamming signal upon reception even if the nodes only receive a narrowband portion of it. We study how the proposed KIC method works based on measurements with commercial off-the-shelf software-defined radios. The results demonstrate that the band-limited KIC method achieves performance that is comparable to non-band-limited methods and, in doing so, leads the way for practical applications of cooperative jamming in scenarios where narrowband communication links span over a wide bandwidth.**

I. Introduction

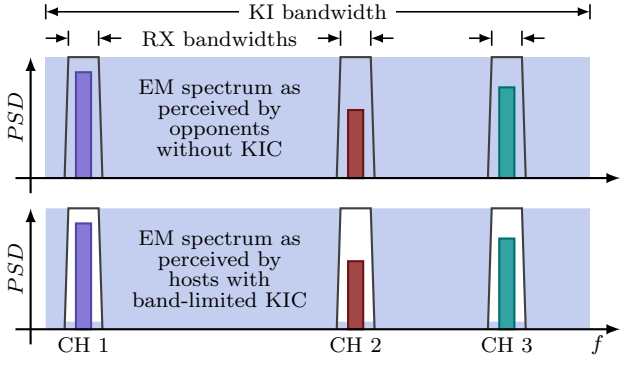
Jamming can provide physical layer security to authorized wireless communication nodes and limit unauthorized wireless nodes from communicating among themselves if the jamming signal can be canceled or avoided by the former but not by the latter [1]. It has been demonstrated that by using a cooperative jammer that transmits a jamming signal which is in advance known to the authorized nodes, both of these benefits can be achieved simultaneously by using known-interference cancellation (KIC) methods at the authorized receivers to suppress the effects of jamming therein [2], [3]. However, the existing KIC methods require the jamming signal bandwidth to not exceed the receiver bandwidth. When used with narrowband receivers that have their RF front-ends matched to a single channel, the existing KIC methods would also limit cooperative jamming to a single channel.

In practice it would be desirable to simultaneously secure and restrict authorized and unauthorized wireless communications respectively on multiple narrowband channels (as illustrated in Fig. 1). To that end, we extend in this work the same-bandwidth KIC method of [3], [4] to work in a band-limited configuration so that any received narrowband portion of a wideband jamming signal can be suppressed when knowledge about the wideband jamming signal is available. We analyze how the developed method performs when combined with a narrowband tactical communication system, how it performs when there is an adversarial narrowband interferer present, give insights into the method's applicability to frequency hopping systems, and finally demonstrate its potential benefits on the battlefield.

This research work was supported by the Research Council of Finland, the Finnish Scientific Advisory Board for Defence, the Finnish Support Foundation for National Defence, and the Finnish Research Impact Foundation.



(a) Nodes' positioning and communication links



(b) EM spectrum without and with band-limited KIC

Fig. 1. Wideband cooperative jammer prevents an opponent from accessing the EM spectrum but requires band-limited KIC for narrowband host receivers to remain functional and achieve an EM advantage over the opponent.

II. Band-Limited KIC

Even when the receiver knows in advance the discrete-time baseband signal that a transmitter broadcasts, canceling the received version of that signal is not trivial because it will be significantly changed. This is caused by the radio-frequency (RF) front-end imperfections at the two devices, as well as the time-varying multipath propagation in between. In order to cancel the received version of the known signal, the aforementioned changes need to be estimated and compensated for at the receiver. Doing so has been studied extensively for carrying out self-interference cancellation (SIC) in full-duplex (FD) radios [5], [6]. However, compared to SIC, KIC methods require additionally to account for the carrier and sampling frequency offsets between the separate radios.

Several methods already exist that account for these frequency offsets and facilitate KIC [2], [3], [7]. However, the existing KIC methods only work when the known interference (KI) fits in the receiver bandwidth entirely. In this work, we build on an existing same-band KIC method [3] to develop a band-limited KIC method that can suppress a KI signal even when only a narrowband portion of the originally wideband KI signal is received. We consider the band-limited received signal to be

$$d(n) = \mathbf{w}^H \mathbf{r}_n, \tag{1}$$

where $\mathbf{w}$ is the impulse response with length K equivalent of the cascaded receiver filters and the received signal without filtering is $\mathbf{r}_n = [r(n), \ldots, r(n-K+1)]$. The individual elements of which are given by

$$r(n) = \mathbf{h}_{\text{jr}}^H \mathbf{y}_n e^{j\sum_{i=1}^{n}\epsilon(i)} + \mathbf{h}_{\text{tr}}^H \mathbf{s}_n + v(n) \tag{2}$$

where $\mathbf{h}_{\text{jr}}$ and $\mathbf{h}_{\text{tr}}$ are the respective channel impulse responses from jammer and transmitter to the receiver, $\mathbf{y}_n$ accounts for sampling the KI signal $x(t)$ with time-varying sampling frequency offset $\eta(i)$ according to [4, Eq. (2)], the term $e^{j\sum_{i=1}^{n}\epsilon_k(i)}$ accounts for the carrier frequency offset between the jammer and receiver, $\mathbf{s}_n$ is the signal of interest, and $v(n)$ is the measurement noise. We consider the band-limited clean received signal without KI to be

$$\tilde{d}(n) = \mathbf{w}^H \tilde{\mathbf{r}}_n, \tag{3}$$

where $\tilde{\mathbf{r}}_n = [\tilde{r}(n), \ldots, \tilde{r}(n-K+1)]$ and the individual vector elements are given by $\tilde{r}(n) = \mathbf{h}_{\text{tr}}^H \mathbf{s}_n + v(n)$.

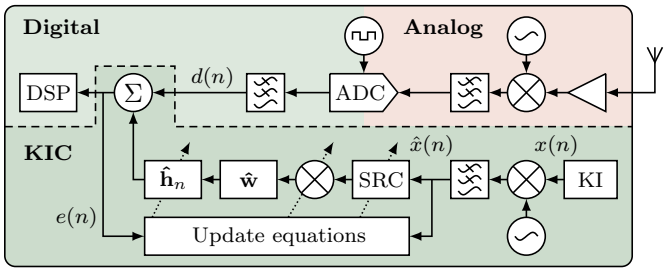


Fig. 2. The proposed band-limited KIC algorithm. The algorithm is implemented digitally and slots into the receiver path of any software-defined radio.

It would not suffice to filter out a portion of the wideband KI and use that band-limited portion of the KI with existing same-band KIC methods — the receiver does not know *a priori* which portion of the wideband KI it has received because of the two frequency offsets. The frequency offsets need to be compensated for before the bandwidth of the original KI is matched to that of the received KI. The proposed band-limited KIC method is illustrated in Fig. 2 and listed as Algorithm 1. In the algorithm listing, M denotes the number of filter taps used to model the channel $\mathbf{h}_{\text{jr}}$, N is the number of received samples, $\hat{x}$ holds a prepocessed version of the original KI signal x, d holds the received signal, μ_h, μ_ϵ, and μ_η are the respective step sizes controlling the rate of channel, carrier frequency offset, and sampling frequency offset estimation, $\hat{\mathbf{w}}$

Algorithm 1 band-limited extension of the FO-LMS algorithm

procedure BL-FO-LMS($M, N, \hat{x}, d, \mu_h, \mu_\epsilon, \mu_\eta, \hat{\mathbf{w}}, K, U$)
  $\hat{\mathbf{h}}_0 \leftarrow \mathbf{0}_{M\times 1}$, $\hat{\epsilon}(0) \leftarrow 0$, $\hat{\eta}(0) \leftarrow 0$ // Initializing parameter estimates
  $\hat{\mathbf{y}}_1 \leftarrow \mathbf{0}_{K\times 1}$, $\mathbf{z}_1 \leftarrow \mathbf{0}_{M\times 1}$, $\phi(1) \leftarrow 0$, $t(1) \leftarrow 0$ // Initializing internal variables
  for $n \leftarrow 1$ to N **do** // Iterating over received samples
    $\hat{\mathbf{y}}_n \leftarrow [\hat{x}(t(n))e^{j\phi(n)}, \hat{x}\left(t(n)-(U+\hat{\eta}(n-1))\right)e^{j\phi(n-1)}, \ldots,$ // Sampling rate conversion
      $\hat{x}\left(t(n)-(K+1)(U+\hat{\eta}(n-1))\right)e^{j\phi(n-K+1)}]$
    $\mathbf{z}_n \leftarrow [\hat{\mathbf{w}}^H\hat{\mathbf{y}}_n, \hat{\mathbf{w}}^H\hat{\mathbf{y}}_{n-1}, \ldots, \hat{\mathbf{w}}^H\hat{\mathbf{y}}_{n-M+1}]$ // Filtering
    $\hat{d}(n) \leftarrow \hat{\mathbf{h}}_{n-1}^H \mathbf{z}_n$
    $e(n) \leftarrow d(n) - \hat{d}(n)$ // Estimation error calculation
    $\hat{\mathbf{h}}_n \leftarrow \hat{\mathbf{h}}_{n-1} + \mu_h \mathbf{z}_n e^*(n)$ // Channel estimation
    $\hat{\epsilon}(n) \leftarrow \hat{\epsilon}(n-1) + \mu_\epsilon \Im\left\{\hat{d}(n)e^*(n)\right\}$ // Carrier frequency offset estimation
    $\hat{\eta}(n) \leftarrow \hat{\eta}(n-1) + \mu_\eta \Re\left\{\hat{\mathbf{h}}_{n-1}^H \mathbf{z}'_n e^*(n)\right\}$ // Sampling frequency offset estimation
    $\phi(n+1) \leftarrow \phi(n) + \hat{\epsilon}(n)$ // Updating internal variables
    $t(n+1) \leftarrow t(n) + (1+\hat{\eta}(n))$
  end for
end procedure

is the impulse response of the receiver filters modeled by K filter taps, and U is the undersampling factor of the received KI compared to the known KI.

As illustrated in Fig. 2, $x(n)$ is first frequency shifted so that the portion of wideband KI that is expected to be received (i.e., would be received without carrier frequency offset) is centered at baseband. Then, that frequency-shifted signal is low-pass filtered so that the sampling rate conversion within the algorithm does not introduce aliases in the final signal. After these preprocessing steps, the algorithm estimates the channel and frequency offsets in combination with applying the filter $\hat{\mathbf{w}}$. Comparable approaches have, for example, been applied in band-limited digital predistortion of wideband RF power amplifiers [8]. The algorithm provides an estimate of the received KI signal $\hat{d}(n)$ and, by subtracting that estimate from the actual received signal, an error signal

$$e(n) = d(n) - \hat{d}(n) \approx \mathbf{w}^H \tilde{\mathbf{r}}_n, \tag{4}$$

which with good estimates of the parameters will approximate to the filtered signal of interest and measurement noise.

III. Measurement Setup

We evaluated the performance of the band-limited KIC method described in Section II when dealing with a combination of wideband KI and narrowband tactical communication signals using the measurement setup illustrated in Fig. 3. The three nodes were implemented using USRP-2900 software-defined radios that operated on $300\,\mathrm{MHz}$ center frequency and that were connected through coaxial cables. The connections included variable attenuators to control the signal-to-interference-plus-noise ratio (SINR) at the receiver.

The cooperative jammer transmitted a $12\,\mathrm{MHz}$ band-limited noise signal that was constructed with a pseudo-random number generator and digital filtering. This approach straightforwardly facilitates generating the same KI waveform in the cooperative jammer and authorized receivers, relying only on a pre-shared secret seed for the pseudo-random number generator. In practice, not knowing the seed would prevent opponents from canceling the received jamming signal even if they had KIC capabilities. The transmitter sent a signal of interest using the NATO narrowband waveform (NBWF) [9], which is a continuous phase-modulated waveform with different modes of either $25\,\mathrm{kHz}$ or $50\,\mathrm{kHz}$ bandwidth. In the measurements presented herein, the $25\,\mathrm{kHz}$ mode N1 was used.

The superposed signals were recorded for offline processing with wide and narrow bandwidths: $14.4\,\mathrm{MHz}$ and $300\,\mathrm{kHz}$, respectively. Same-band KIC was used on the recordings with wide bandwidth and band-limited KIC on the recordings with narrow bandwidth. To simplify the processing, all nodes were connected to a reference timing generator that provides coarse knowledge about where in the recordings the transmitted signals are positioned. Also, the transmitter and receiver, but not the cooperative jammer, were connected to a reference frequency generator that removed carrier and sampling frequency offsets between the two connected devices, simplifying the signal of interest processing but not simplifying the KIC.

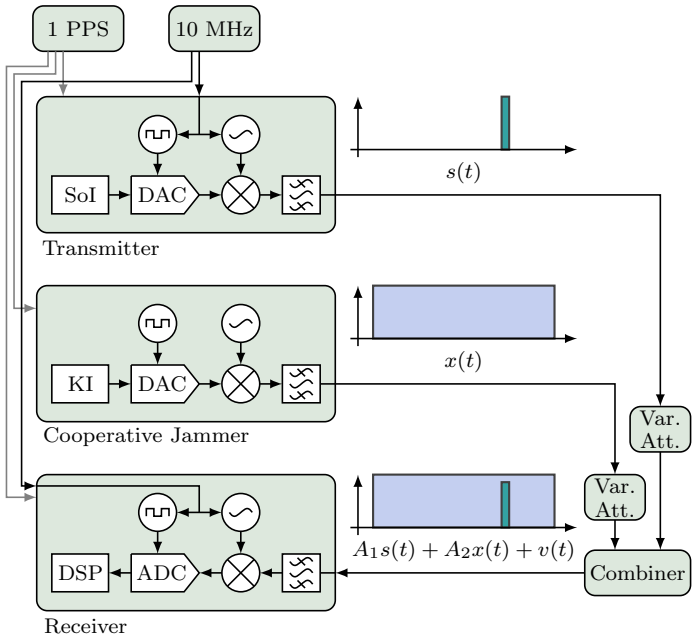


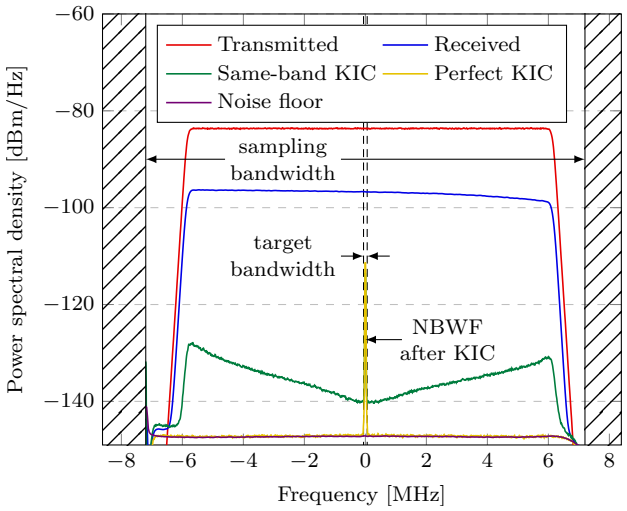
Fig. 3. Diagram of the measurement setup.

IV. Results

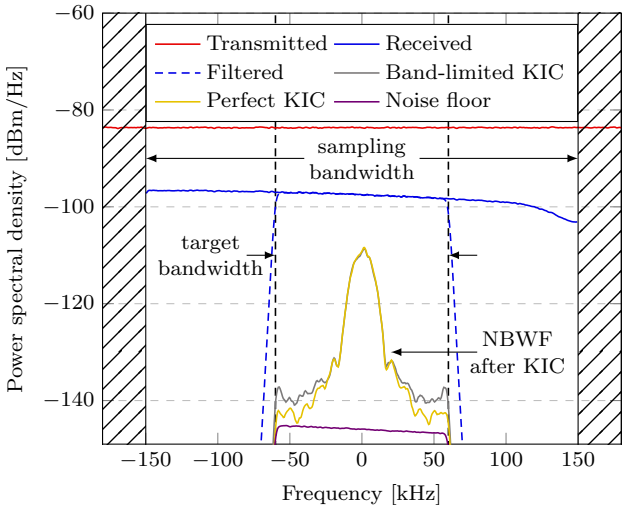
Fig. 4 illustrates the superposed measurement signals with wideband and narrowband reception. With wideband reception (Fig. 4a), the KI and signal of interest fit entirely within the $14.4\,\mathrm{MHz}$ receiver bandwidth, allowing same-band KIC methods to be used. With narrowband reception (Fig. 4b), only a portion of the KI signal fits within the $300\,\mathrm{kHz}$ receiver bandwidth while that bandwidth is sufficient for the signal of interest. The latter is in practice the preferable way to acquire the signal of interest as it lowers requirements on the receiver hardware and limits the effects of out-of-band interference. However, this approach requires a band-limited KIC method if wideband KI is used.

A. Same-Band vs Band-Limited KIC

Fig. 5 shows in detail the same-band and band-limited KIC performance depending on the received KI power when there is no signal of interest transmitted. This analysis provides a benchmark of how well the two KIC methods can potentially perform when the signal of interest is included. The results show that both methods achieve similar KIC performance, with around $48\,\mathrm{dB}$ of suppression at most. The methods' performance does drop significantly when the received KI is so powerful that the receiver front-end distorts the signal as neither method compensates for nonlinear distortions. Still, both KIC methods provide a considerable range of received KI power over which they achieve very good KI cancellation. The same-band KIC method has already been demonstrated effective when a KI superposes various signals of interest [3], [7] and, as such, the results in Fig. 5 are promising in terms of using band-limited KIC in narrowband tactical communication receivers for suppressing a portion of a wideband KI for subsequent signal-of-interest processing.



(a) Wideband reception of the measurement signals



(b) Narrowband reception of the measurement signals

Fig. 4. The measurement signals at different stages of the measurements. With narrowband reception, the out-of-band KI causes aliasing within the receiver bandwidth. To avoid the effects of these, the received 300 kHz signal is digitally filtered down to 120 kHz.

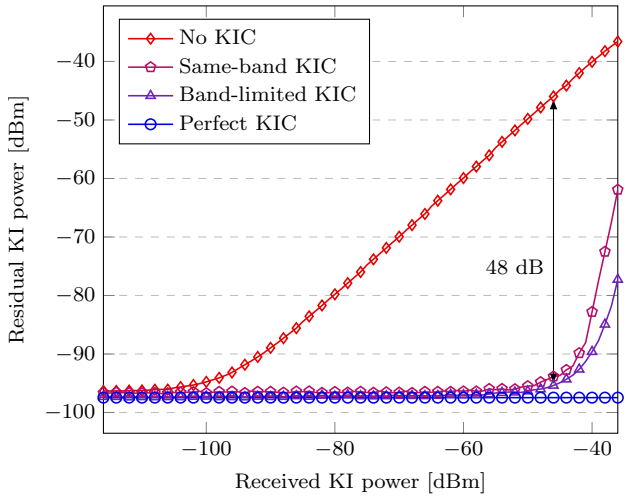


Fig. 5. Cancellation performance of the KIC methods without a signal of interest. Power of the signals was measured in the 120 kHz target band.

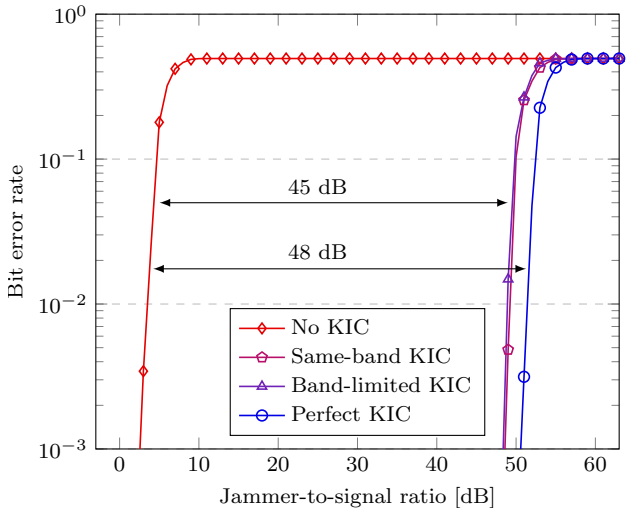


Fig. 6. Signal-of-interest demodulation performance without and with KIC.

B. NATO Narrowband Waveform

Fig. 6 demonstrates the KIC methods' performance as a measure of the NBWF bit error rate (BER), when that waveform is included in the measurements as the signal of interest. The measurements presented in Fig. 6 were carried out by varying the received signal-of-interest power while keeping that of the KI fixed, resulting in the varying jammer-to-signal ratio (JSR). Comparing Fig. 5 and Fig. 6, it is evident that the KI cancellation almost directly translates to improved signal-of-interest demodulation, i.e., the post-cancellation BER is improved comparably to the pure KI cancellation. This consistency does unfortunately also mean that the residual KI with these KIC methods prevents the demodulator from performing as it would with perfect KIC. Still, for a wide range of JSRs the results demonstrate a considerable benefit from cooperative jamming and its cancellation.

C. KIC under Blocker

Receiving a narrowband signal with a narrowband receiver, as opposed to with a wideband receiver, is fitting in practice so as not to overcomplicate the receiver architecture. Furthermore, narrowband-filtering in the analog domain allows to limit the negative effects of out-of-band interference on digitization [10]. Here, performance of the KIC methods is compared in the presence of such an interference which overlaps in frequency the wideband KI but not the target band. The measurements were carried by replacing the NBWF in the target band with a narrowband jamming signal just outside of that band. The received blocker power was varied while that of the KI was fixed. Fig. 7 shows that the blocker leads to significant residual KI in the target band when using the same-band KIC method. The band-limited KIC, however, continues performing as intended.

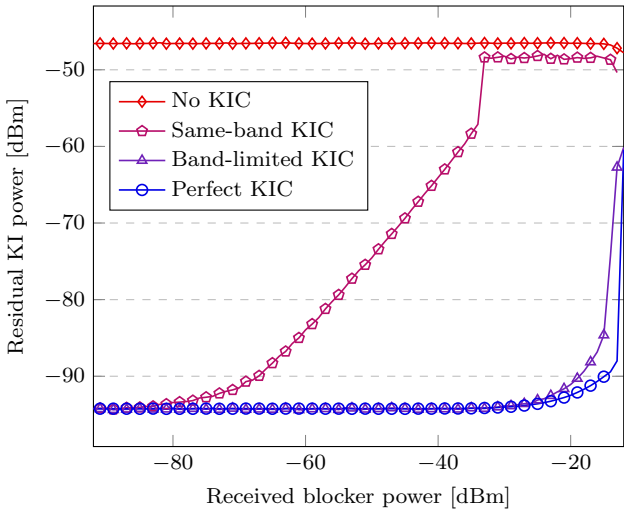


Fig. 7. Performance of the KIC methods with a blocker in the wide KI band but outside of the narrow target band. The blocker power was measured in the 14.4 MHz wide band and residual KI power in the 120 kHz target band.

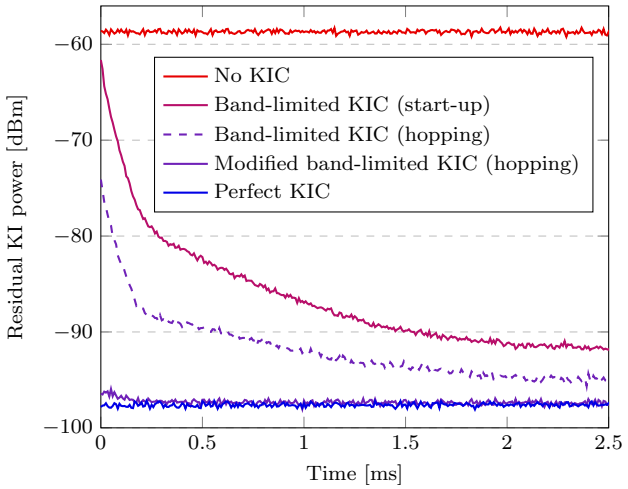


Fig. 8. Convergence of the band-limited KIC method in the start-up phase and after frequency hops, averaged over one thousand measurement runs.

D. Frequency-Hopped KIC

Tactical communications often rely on rapid frequency hopping to evade an opponent's electronic countermeasures [11]. And, for KIC to be practically suitable for such frequency-hopped systems, the KIC needs to be able to react quickly to the changes caused by the frequency hopping so as to not create significant overhead in the system. The RF front-end of the USRP-2900s used in the measurements herein introduce a random phase shift every time that the center frequency is changed. This causes the receiver to perceive the channel differently and the proposed band-limited KIC method to take some time to re-converge after a frequency hop. However, the latter can be largely avoided if the phase offset is compensated for explicitly after a frequency hop as a one-time operation. For example, by calculating the phase difference between the received signal and the estimate of the received signal for the first received sample after a frequency hop so that

$$\theta = \arg\{d(n)\hat{d}(n)^*\} \tag{5}$$

and then including that phase offset in the channel estimate

$$\hat{\mathbf{h}}_{n-1} = \hat{\mathbf{h}}_{n-1}e^{j\theta}. \tag{6}$$

Fig. 8 shows the band-limited KIC method's convergence rate during the initial start-up phase and during subsequent frequency hops to different channels. The proposed band-limited KIC takes on the order of tens of milliseconds to converge during the start-up phase (only partially shown). Even though the channel and frequency offsets remain almost the same during subsequent frequency hops, the proposed method converges only slightly faster because of the random phase offset (dashed purple line). However, with the explicit phase offset compensation, the KI is suppressed relatively seamlessly even after frequency hops (solid purple line).

E. Battlefield Performance

We used the results from subsection IV-B to simulate the impact of cooperative jamming on a pair of narrowband communication nodes belonging either to host or opponent forces (i.e., both either have or do not have KIC). The position of one communication node and the cooperative jammer was fixed, while the position of the second communication node was varied across the simulated battlefield. Path losses between all the nodes were obtained using the Egli model [12], with the nodes' antennas at a height of 1 m, antennas having unit absolute gain, and carrier frequency being 300 MHz. Jamming transmit power was taken to be 25 W within the narrowband target bandwidth of 120 kHz, tactical radios' transmit power to be 2 W, and noise floor to be equivalent to that seen in the measurements, i.e. −97 dBm. Fig. 9 shows, for any position of the second communication node, the higher of the BERs at the two communication nodes. Distances in the results are modest due to the above parameter selection yet still demonstrate that a considerable advantage for the host can be achieved.

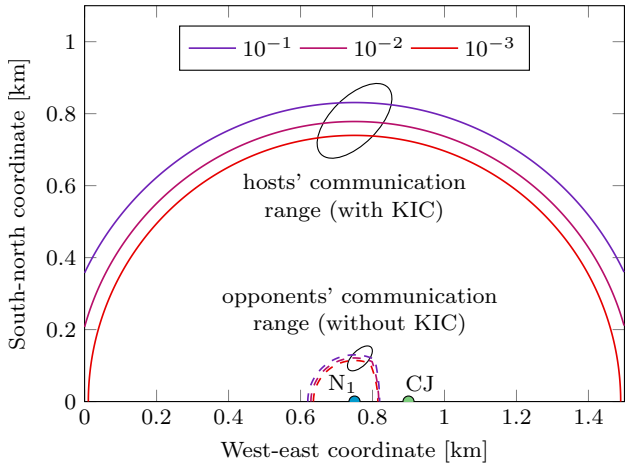


Fig. 9. Simulated two-way NBWF communication performance under cooperative jamming. The contour lines show the higher BER of the BERs at the two communication nodes.

V. Conclusion

We presented a band-limited known-interference cancellation (KIC) algorithm, which allows to estimate and compensate for an unknown wireless channel as well as carrier and sampling frequency offsets between a transmitter-receiver pair when receiving a band-limited portion of a transmitted wideband known interference (KI) signal. The proposed algorithm aims to facilitate wideband cooperative jamming for preventing unauthorized users from accessing the electromagnetic (EM) spectrum while not affecting authorized users with narrowband receivers. That is, the host forces could simultaneously secure multiple of their own narrowband tactical communication links and disrupt those of the adversary, plus prevent the adversary from carrying out various electronic support and attack operations.

We studied the algorithm's performance with software-defined radios and the NATO narrowband waveform (NBWF). Measurement results demonstrated that the band-limited algorithm achieves KI cancellation comparable to that of same-band KIC all the while receiving only a narrow portion of the KI. Furthermore, the band-limited KIC showed a direct positive impact on the NBWF processing when received superposed with a KI over a wide range of jammer-to-signal ratios (JSRs). Owing to the fundamental characteristic of narrowband reception, the band-limited KIC method demonstrated improved performance compared to same-band KIC in canceling KI when confronted by a narrowband blocker signal. And, with a few additional steps, the algorithm also showed good performance in a frequency-hopped configuration. Finally, by using the measurement results as basis for simulations, we demonstrated the potential impact of cooperative jamming and KIC on tactical communications in a battlefield.

References

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, Oct. 2018.

[2] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 240–243, Feb. 2020.

[3] K. Pärlin, T. Riihonen, M. Turunen, V. Le Nir, and M. Adrat, "Known-interference cancellation in cooperative jamming: Experimental evaluation and benchmark algorithm performance," *IEEE Wireless Communications Letters*, vol. 12, pp. 1598–1602, Sep. 2023.

[4] K. Pärlin, T. Riihonen, V. Le Nir, and M. Adrat, "Estimating and tracking wireless channels under carrier and sampling frequency offsets," *IEEE Transactions on Signal Processing*, vol. 71, pp. 1053–1066, Mar. 2023.

[5] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[6] B. Smida, R. Wichman, K. E. Kolodziej, H. A. Suraweera, T. Riihonen, and A. Sabharwal, "In-band full-duplex: The physical layer," *Proceedings of the IEEE*, Mar. 2024.

[7] K. Pärlin, T. Riihonen, M. Turunen, V. Le Nir, and M. Adrat, "Distributed cooperative jamming with multi-reference known-interference cancellation," in *Proc. International Conference on Military Communications and Information Systems*, Apr. 2024.

[8] C. Yu, L. Guan, E. Zhu, and A. Zhu, "Band-limited Volterra series-based digital predistortion for wideband RF power amplifiers," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 12, pp. 4198–4208, Dec. 2012.

[9] V. Le Nir and B. Scheers, "Low complexity generic receiver for the NATO narrow band waveform," in *Proc. International Conference on Military Communications and Information Systems*, May 2017.

[10] A. Rasekh and M. S. Bakhtiar, "Effect of out-of-band blockers on the required linearity, phase noise, and harmonic rejection of SDR receivers without input SAW filter," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 11, pp. 4913–4926, Aug. 2018.

[11] E. B. Felstead, "Follower jammer considerations for frequency hopped spread spectrum," in *Proc. IEEE Military Communications Conference*, vol. 2, Oct. 1998, pp. 474–478.

[12] J. J. Egli, "Radio propagation above 40 MC over irregular terrain," *Proceedings of the IRE*, vol. 45, no. 10, pp. 1383–1391, Oct. 1957.