Interference Suppression in Bandwidth Hopping Spread Spectrum Communications

Domenico Giustiniano
IMDEA Networks Institute
Madrid, Spain
domenico.giustiniano@imdea.org

Markus Schalch
ETH Zurich
Zurich, Switzerland
mschalch@gmx.ch

Marc Liechti
Trivo Systems GmbH
Berne, Switzerland
marc@liechti.one

Vincent Lenders
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

ABSTRACT

Bandwidth hopping spread spectrum (BHSS) has recently been proposed as a spectrum-efficient technique to combat jamming. In BHSS, the transmitter is randomly hopping the signal bandwidth in order to make it unpredictable to an attacker. When the signal bandwidth is unpredictable, the attacker cannot match its interference bandwidth to the signal bandwidth of the transmitter, and the receiver can filter out the interference power (or parts of it) prior demodulation, and thus increase decoding performance. The main challenge in BHSS is that the bandwidth must be hopping very rapidly at the symbol level in order to prevent a reactive jammer from following the hopping pattern by simple tracking techniques. Existing receiver filtering techniques as proposed in prior work require a long time to estimate the filter parameters and are thus unable to suppress the interference from the jammer when the bandwidth is hopping at the symbol level. In this paper, we propose a new filtering approach adapted for BHSS which is able to suppress arbitrary jamming interference even when the signal bandwidth is hopping after every symbol. Our approach is based on a filter bank which applies different filters in parallel and dynamically selects the best filter for every symbol according to the soft-state output of the demodulator. We evaluate the improvement of our method over classical filtering techniques in experiments using software-defined radios. Our results show a gain in interference suppression above 30 dB with respect to state-of-the-art solutions. We further implement frequency hopping for a BHSS system, and demonstrate the superiority of a system combining hopping in bandwidth, code and frequency against jamming attacks.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; • **Networks → Wireless access networks**;

WiSec '18, June 18–20, 2018, Stockholm, Sweden

ACM ISBN 978-1-4503-5731-9/18/06…$15.00
https://doi.org/10.1145/3212480.3212484

KEYWORDS

Wireless security, Jamming resistance, Bandwidth hopping, Interference filter, Spread spectrum, Software-Defined Radio

ACM Reference Format:
Domenico Giustiniano, Markus Schalch, Marc Liechti, and Vincent Lenders. 2018. Interference Suppression in Bandwidth Hopping Spread Spectrum Communications. In *WiSec '18: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, June 18–20, 2018, Stockholm, Sweden.* ACM, New York, NY, USA, 0 pages. https://doi.org/10.1145/3212480.3212484

1 INTRODUCTION

Jamming-resistant communication systems are typically based on two complementary spread spectrum techniques: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). In both techniques, the bandwidth of the waveform is intentionally made wider than necessary to transmit the information over the channel. A third complementary spread spectrum technique that has recently been proposed is bandwidth hopping spread spectrum (BHSS) [1]. The idea is that the transmitter hops the signal bandwidth with a random pattern that is unpredictable to the jammer.

The gain of BHSS arises when the *jammer bandwidth* cannot be matched to the *signal bandwidth*. It has been shown that BHSS is able to improve the jamming resistance of the communication beyond the processing gain of conventional spread spectrum techniques such as DSSS and FHSS without an increase in RF spectrum requirements [1]. This is achieved by combining bandwidth hopping at the transmitter and adaptive filtering prior to the demodulation at the receiver. A *band-pass filter* is used at the BHSS receiver to suppress the interference from the jammer when the communication bandwidth is smaller than the jammer bandwidth. An *excision filter* is instead used if the opposite holds.

This result implies that the throughput of a communication link can be improved without requiring in average more RF spectrum bandwidth. This is particularly important in future wireless networks with dynamic spectrum access (DSA) [2], because the spectrum utilization is getting very high over time and sacrificing RF spectrum for jamming resistance is often impossible and undesired under these conditions.

In order to be resistant against reactive jammers, the bandwidth of the signal must be hopped as quickly as possible, ideally in the

order of symbols, such that a jammer cannot learn and follow the signal bandwidth. When the signal bandwidth is hopped quickly, there are unique challenges that remained unaddressed in previous work:

- A filter needs to be selected on a per-symbol basis which is at odds with the long convergence time of existing filters that require several filter taps;
- The filter is often not tuned optimally leading to low performance figures.

Therefore, a fast-tuning filter that depends on the bandwidth offset between the communication signal and the jamming signal must be designed at the receiver to maximize the signal-to-interference (jamming) ratio of the filtered signal that is passed to the demodulator. The BHSS system proposed in [1] relies on common techniques from the literature for band-pass and excision filtering. In this work, we first show that these existing techniques are not well suited for BHSS, and they do not allow to exploit the full gain of BHSS that is theoretically possible. In addition, careful design of communication modules of BHSS is necessary in order to exploit its processing gain. Our contributions are as follows:

- We propose a novel approach to efficiently excise the jammer that is well suited for fast bandwidth hopping signals. Rather than estimating the jammer power as in state-of-the-art approaches, we let the signal pass through a filter bank and decode in parallel each signal. We present a metric to decide which filter performs best at suppressing the interference and we devise a symbol decoding quality estimator that hints about which filter is likely to produce correctly decoded bits at the demodulator;
- We introduce new components at the transmitter and the receiver in the BHSS system to achieve a successful decoding of BHSS data at the receiver under jamming attacks;
- We implement our approach on software-defined radio (SDR) platforms. Our extensive experiments show that a gain of up to 34 dB is reached compared to previous work. We further study frequency hopping for BHSS, combine the three spread spectrum technologies (BHSS, DSSS and FHSS) in one system and show through experiments that exploiting the three available dimensions (bandwidth, code and frequency) gives superior performance against jammers.

2 BACKGROUND AND RELATED WORK

In this section, we first review the spread spectrum techniques, including the recent BHSS. As BHSS requires an efficient filter before demodulation, we present known signal processing techniques in the literature for mitigating interference.

2.1 Spread spectrum techniques

In spread spectrum (SS) communication, an extra modulation is applied to the signal that expands the bandwidth beyond what is required by the underlying modulation of the data. This can be used for multiple-access, hidden communications, and higher resistance to interference [3], while our work focuses on the latter.

DSSS and FHSS. In DSSS, the transmitter spreads a low bit-rate information signal to a wider spectrum of fixed width by multiplying the signal with a higher bit-rate pseudorandom spreading chip sequence. Because of the higher bit-rate of the chip sequence, this results in a wider bandwidth [4]. In FHSS, the transmitter randomly hops the carrier frequency of the modulated signal after some time t. The available bandwidth is divided into channels. Each channel has the same bandwidth as the signal to transmit. This has the effect of spreading the signal bandwidth over a wider band than actually occupied by the information bandwidth.

The demodulation operation in SS has the effect of mitigating the amount of interference power to a fraction that is proportional to the ratio between the spreading chip band (DSSS)/hopping band (FHSS) to the actual signal bandwidth, which is the so-called *processing gain*.

BHSS. BHSS was proposed in [1], and it relies on unpredictable hopping of the signal bandwidth B_s providing the protection against an attacker of bandwidth B_j that tries to disturb the communication. We distinguish three different cases:

- $B_s < B_j$: If the signal is smaller than the jammer bandwidth, we can band-pass filter the signal and therefore cut out some of the jammer energy that lies outside the band of the communication. This filtering does not attenuate the legitimate signal but a portion of the jamming power remains after filtering;
- $B_s = B_j$: If the jammer matches the signal bandwidth, we cannot filter out any power of the jamming signal;
- $B_s > B_j$: In the case of a narrowband jammer, a band reject filter can be applied. This filter will entirely excise the jammer energy. Obviously, some part of the signal energy is filtered as well. However, when the remaining overall signal energy is large enough, the signal can still be decoded.

For $B_s < B_j$ and $B_s > B_j$, BHSS can cut out some of the jammer energy at the receiver and get a power advantage over the jammer. When the hopping is sufficiently fast among a large set of different bandwidths, the probability $Pr\{B_s = B_j\}$ is low. Therefore, an advantage in BHSS is achieved if the jammer cannot detect and jam the full signal bandwidth B_s within the hopping time t.

In the BHSS transmitter, half sine pulse shaping $g(t)$ is applied to control the signal bandwidth B_s. In fact, stretching a signal $g(t)$ in the time domain of a factor α reduces the bandwidth by the same factor, and viceversa:

$$g(t) \xrightarrow{\mathcal{F}} G(\omega) \Longrightarrow g(\alpha t) \xrightarrow{\mathcal{F}} \frac{1}{|\alpha|} G(\frac{\omega}{\alpha}) \tag{1}$$

where $\mathcal{F}$ indicates the Fourier transform.

As in [1], our work refers to the application of bandwidth hopping to DSSS. There are two parameters to specify how bandwidth hopping is applied:

Hopping time: This interval specifies for how long (how many symbols) a certain bandwidth is chosen.

Samples per chip: Each chip is modulated with a pulse shape $g(t)$. The duration of the pulse shape is changed with the number of samples per chip. The transmission starts with a pseudo-randomly selected bandwidth and then changes to the next bandwidth pseudo-randomly for the same amount of symbols.

For interference suppression in BHSS, the receiver needs to estimate B_j and to control a filter logic selecting the appropriate filter parameters for the band-pass and excision filters. In the following

section we present the main filtering techniques proposed in the literature for interference rejection.

2.2 Filtering interference

We introduce representative works in each area, sorted by the domain in which they are applied.

Time domain. The general idea of interference rejection in the time domain is to include a Finite Impulse Response (FIR) filter before the received input signal is fed into the correlation receiver. Assuming that the autocorrelation function of the interference is known, [5] calculated the filter weights by minimizing the mean-square error between the interference and its estimation. [6] modeled the interference as white noise passed through an all-pole filter. The idea proposed was to estimate the pole positions by linear prediction using the received signal. The suppression filter is then a FIR filter with zero positions at the estimated poles. To generate such a model, the autocorrelation of the interference needs to be estimated. [7] introduced a filter bank with different excision filters. Their approach targeted periodic jammers and it converged slowly (2-5 seconds) in presence of a reactive attacker model as considered in this work (see next Section).

Transform domain. Jamming mitigation techniques that operate in transform domains use a frequency domain (Discrete Fourier Transform, DFT) or the Wavelet transformation, process the signal in the new domain and then transform back the signal in the time domain. In [5], a threshold was applied to the signal and bins exceeding the threshold were set to zero. In [6], a FIR filter was designed to whiten the DFT spectrum and cancel peaks from narrowband jammers. In [8], the signal was transformed into Wavelet domain, where the high energy bins are excised. The Wavelet approach performed better that the DFT for non-stationary interference.

Time-frequency domain. In [9, 10], a filter approach based on a time-frequency distribution (TFD) was proposed. The goal was to filter out highly non-stationary interference. The idea was to apply a TFD such as Wigner distribution to get a time-varying spectral analysis on the signal and to attenuate the signal in the regions where there is a strong interference.

Spatial domain. In receivers with more than a single antenna, more properties of a signal can be extracted. Assuming that the signal of the jammer is not sent from the same place as the real signal, [5] described how to use the angle of arrival to distinguish a jamming signal from a useful signal.

3 ATTACKER MODEL AND CHALLENGE

We first present the jammer model and then the challenge with such attackers in BHSS systems.

3.1 Attacker model

The goal of the jammer is to block the communication between the transmitter and the receiver by emitting radio signals into the shared medium. The signals might vary in waveform, transmission time or follow a certain strategy, which result in constant, periodic, random or reactive jammers. In this work, we assume that the jammer has a finite maximal transmission power and a finite bandwidth. Further, all keys to pseudo-random functions are secret and unknown to the jammer [11]. Therefore, the hopping pattern for the different bandwidths in BHSS is secret, similarly to patterns for DSSS and FHSS. We also assume that the threat comes from a reactive jammer that first senses the channel and based on the observations, it reacts with transmitting a matched jamming waveform [12]. The reaction time of the reactive jammer is r, which is the superposition of the channel sensing, waveform generation and propagation delays.

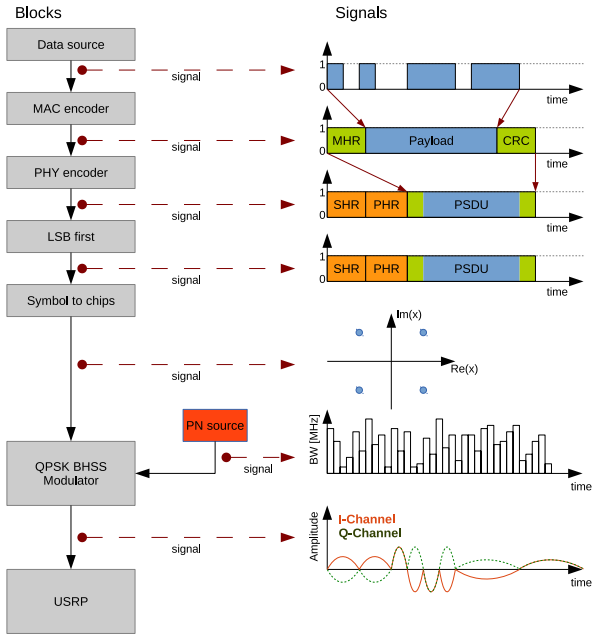


Figure 1: BHSS transmitter.

3.2 Challenge in BHSS systems

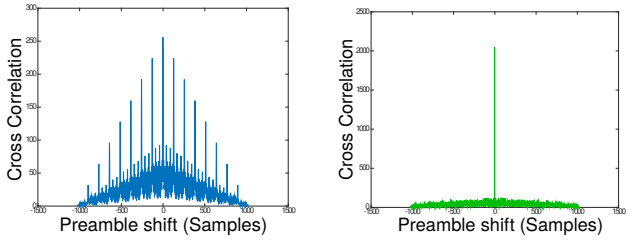
In this work, we target a hopping time t smaller than the reaction time r of the jammer ($t < r$). A reaction time of 20 μs was reached in [12] on an FPGA-based implementation of a reactive jammer. For typical packet-based communication systems such as IEEE 802.15.4, the symbol duration is in the order of a few microseconds. This implies that hopping at the symbol level is a necessary condition to counter-attack *reactive jamming attacks*. However, the practicality of a transmission scheme based on BHSS that is hopping at the symbol level was not addressed in previous works [1] which only hop the bandwidth between packet transmissions. The challenges addressed in this work are then *how to guarantee an efficient decoding of a signal that is hopping the bandwidth at the symbol level, and how to prove its practicality by means of experiments.*

4 TRANSMITTER

We first present the design of the original BHSS transmitter from [1] and then our proposed modifications.

4.1 Existing BHSS transmitter

Figure 1 gives an overview of the original BHSS transmitter structure which resembles the IEEE 802.15.4 architecture. First, in the packet encoder block, the MAC and the PHY headers are prepended



(a) Cross-correlation with current preamble.

(b) Cross-correlation with proposed preamble.

Figure 2: On the left: a preamble that consists of 8 zero symbols peaks if the symbol is shifted by x symbols, where $0 \leq x < 8$. On the right: for a Gold sequence preamble, there is only one peak for the unshifted signal.

to the data to transmit. A CRC-16 checksum is appended to allow an integrity check for the packet at the receiver. After changing the bit order in the least significant bit (LSB) block, DSSS modulation is applied with the input bits mapped to chips in the symbol to chips block. 4 input bits are mapped to 16 complex samples according to the chip table.

For pulse shaping, to avoid the usage of a resampler, the number of available bandwidths is limited by choosing the following number of samples per chip: 2, 4, 8, 16, 32, 64, 128. This results in the bandwidths presented in Table 1.

4.2 Proposed new transmitter design

In what follows, we introduce our new communication blocks for BHSS, and explain why they are needed.

The existing BHSS implementation in [1] is loosely based on the IEEE 802.15.4 standard. The preamble is specified as 8 consecutive zero symbols. In general, a repeating symbol pattern is well suited to estimate the carrier frequency offset. With such a pattern, a receiver can correlate the preamble to estimate the frequency offset. However, a repeating preamble structure is not beneficial when it comes to communicate in the presence of a jammer, since it leads to multiple peaks after correlation in the preamble detection at the receiver. Figure 2(a) illustrates the problem. If we correlate one zero symbol with the whole 8 zero symbol preamble sequence, we already get a clear peak. With every additional symbol, the peak increases, until the maximum is reached with 8 zero symbols.

Samples per chip	Signal bandwidth
2	10 MHz
4	5 MHz
8	2.5 MHz
16	1.25 MHz
32	0.625 MHz
64	0.3125 MHz
128	0.15625 MHz

Table 1: The corresponding bandwidths for the samples per chips at a sampling rate of 10 MHz.

To mitigate this problem, a cyclic function in the cross correlation is not desirable. We then use Gold codes, pseudo-random numbers that provide a bounded cross correlation value between two sequences or shifted versions of the sequence [13]. Gold codes are used, e.g., in the Global Positioning System (GPS) and in the preamble of the random access in cellular Code Division Multiple Access (CDMA) systems [14, 15]. In Fig. 2(b) we show the cross correlation peak of shifted versions of the preamble. As desired, there is a single strong peak correlating with the original signal.

As in [1], our BHSS implementation spreads the signal in spectrum according to Eq. (1). In the BHSS modulator block, we additionally implement the support for FHSS. Choosing the next frequency is performed together with the next bandwidth. Thus, the hopping time is valid for frequency and bandwidth change. We shift a complex signal $C = a + ib$ in frequency by multiplying it with $e^{i*2\pi fk/S}$, where f is the frequency shift, k the current sample and S the sampling rate.

5 RECEIVER

As for the receiver, we first present the original design of BHSS and then our proposed modifications.

5.1 Existing BHSS receiver

In the existing BHSS receiver, an Automatic Gain Controler (AGC) adjusts the magnitude of the signal to get a constant input level. Once the signal is in the preferred range, the preamble is detected. Phase guess is calculated and fed into a PID controller according to Gardener's timing recovery to compensate for frequency and phase offset [16]. The detection is done implementing a matched filter that processes the last two symbols of the preamble (zero symbols). Next, the receiver implements the actual decoding and filtering of the packet. The DFT of the samples of one symbol is computed. Two options are possible:

- in case $B_s < B_j$ (wideband jammer), the bins outsides the signal bandwidth are set to zero [5];
- in case $B_s > B_j$ (narrowband jammer), the excision filter attempts to whiten the spectrum of the incoming signal with its DFT to be reciprocal to the square root of the estimated power spectral density [6].

An inverse DFT is then taken and the samples are further decoded, with the signal being decoded chip by chip. One chip is matched against its half sine pulse shape in a matched filter. If 16 chips are decoded, a symbol is declared complete. Finally, the CRC-16 checksum is used to verify if the packet is correct.

5.2 Proposed new receiver design

The structure of the receiver has been adjusted to cope with the additional challenges in BHSS communication (cf. Section 3.2).

5.2.1 Preamble detection. In the previous design, the matched filter for the preamble was matched on the last two symbols of the preamble. The decision to match only two symbols was based on performance considerations. For the smallest bandwidth (128 samples per chip, see Table 1), the length of the filter would be 16384 taps, if we match on all 8 preamble symbols. In addition, this implementation would lead to many false positives in the preamble

detection (cf. Section 4.2). In the new receiver, we match on a Gold sequence of length 1023. Therefore, the length of the filter is not critical anymore and our matched filter is matched on the whole preamble.

5.2.2 Decoding. Instead of decoding each chip, we directly decode the whole symbol by using matched filters. The matched filter is an ideal filter, if the signal to match is known. In our case, we do not know the signal in advance. However, we know the preamble signal and the length of one symbol. After the preamble is detected, we therefore know how many samples correspond to the next symbol. In addition, we know that the symbol is one out of 16 possibilities. In order to learn which symbol is the correct one, we run 16 matched filters, each one matching to a different symbol. This is implemented by setting the taps of a FIR filter to the complex conjugates of the chips in reverse order. We choose the symbol with the highest output of the matched filter as the output symbol.

5.2.3 Excision filters. The problem we face in a real system is that *we do not know if there is a jammer, and if there is one, what is its bandwidth.* There are different adaptive solutions in the literature (c.f. Section 2.2), but only a few solutions work with variable signal bandwidth. We propose and implement the following two different concepts.

Jammer estimation. In the first approach, we dynamically estimate the jammer and excise the jammer bandwidth if a jammer is detected. We implement two types of filters in the DFT domain: i) excise large frequency bins filter [5], and ii) whiten large frequency bins, which attenuates large frequency bins instead of completely excise them.

Parallel filtering. For the second approach, we do *not* estimate the jammer. The idea is to decode different filtered versions of the same signal that are optimized for a specific jammer scenario and to choose the best result. Our approach runs the filters in parallel and decodes each resulting signal. In what follows, we describe the decision logic and the implementation details of this second approach.

5.2.4 Decision logic with parallel filtering. The decision of which decoded signal to select is made by comparing the cross correlation *cc* values. Decisions are taken per symbol. Throughout the decoding step, we get one cross correlation value *cc* for each possible symbol (out of 16) and the symbol with the highest value is chosen. In order to compare different decoding schemes, we use the following normalization cross correlation function $n\_cc(s)$:

$$n\_cc(s) = \frac{\max_{i=0..15} cc(S_i, s)}{\sum_{i=0}^{15} cc(S_i, s)}, \tag{2}$$

where S_i corresponds to the symbol i and s is the decoding of the symbol to compare against. The normalized cross correlation $n\_cc(s)$ for a decoding indicates how certain we are that the decision on one out of the 16 symbols is correct. Therefore, $n\_cc(s)$ is an indicator for the quality of the received signal. A higher $n\_cc(s)$ means that the quality is better while a lower $n\_cc(s)$ indicates inferior quality.

5.2.5 Implementation details of parallel filtering. In our implementation, we decide among four different versions of the signal:

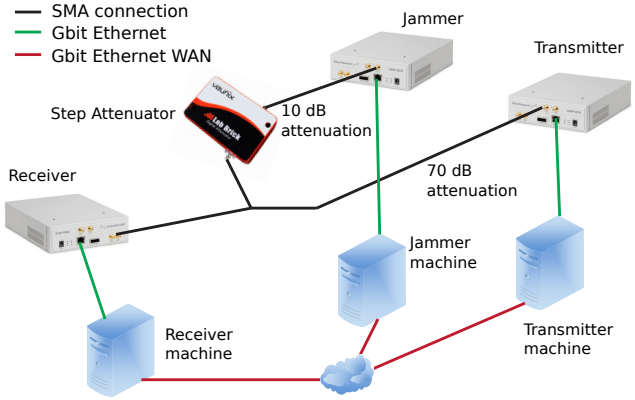


Figure 3: Testbed.

- Unfiltered: No excision filter is applied and the signal is decoded unfiltered;
- Excision of $\frac{B_s}{8}$: A band-pass filter with a stop band of $\frac{B_s}{16}$ and a transition band of $\frac{B_s}{16}$ is applied before the decoding. This filter removes narrowband jammers within $\frac{B_s}{8}$;
- Excision of $\frac{B_s}{4}$: It removes narrowband jammers within $\frac{B_s}{4}$. The band-pass filter has both a stop band and a transition band of $\frac{B_s}{8}$ respectively;
- Excision of $\frac{B_s}{2}$: The largest excision filter has a stop band of $\frac{B_s}{4}$ and a transition band of $\frac{B_s}{8}$. This filter therefore excises jammers within $\frac{B_s}{2}$.

The filters for all bandwidths are designed in equiripple design mode as high pass FIR filters. They have a stop band attenuation of 80 dB, are stable, have linear phase and a constant group delay. The filter taps are quantized as floats.

The presented filtering approach is not restricted to the use of FIR filters. Our implementation allows to choose between FIR filters and DFT excision, as shown in our evaluation (cf. Sec. 7).

6 TESTBED AND METHODOLOGY

We first describe the testbed used throughout the evaluation, then the measurements we conduct and finally present the jammer implementation.

6.1 Testbed

The testbed is illustrated in Fig. 3. We use three SDRs for the evaluation process, with one board as transmitter, one as receiver and the last one as jammer. For both the transmitter and the receiver, we use Ettus Research USRP N210 SDRs. These devices can sample at 25 complex megasamples per second, resulting in a maximum bandwidth of 25 MHz, and are equipped with SBX daughterboards, that can transmit and receive at frequencies from 400 MHz to 4.4 GHz. The jamming device is an Ettus Research USRP2 SDR equipped with a XCVR2450 daughterboard. This board is capable to receive and transmit within the unlicensed ISM-band at 2.4 GHz and 5 GHz. We operate at a center frequency of 2.45 GHz with all devices throughout the evaluation. The sampling rate is fixed to

10 complex megasamples per second resulting in a signal bandwidth of up to 10 MHz.

The three SDRs are connected to each other over SMA cables and a T-connector. This removes multipath effects and uncontrollable disturbances, that we do not account for in this work, and allows to make controllable and repeatable experiments. To control the signal power, we add static attenuators, as well as a digital step attenuator. In our setting, we include a static 70 dB attenuation from the transmitter device to the T-connector. The jammer device is connected to the digital step attenuator. Before the attenuator, a static 10 dB attenuation is included to guarantee that the allowed input power of the receiver is never exceeded. The digital step attenuator is a Vaunix LDA-602E. It has a dynamic range of 120 dB. The attenuation can be controlled by a host computer that is connected to the step attenuator by USB. Each SDR is connected to a separate host machine with communication through Gigabit Ethernet interface. We use GNU Radio 3.7.5.1 release [17], with new blocks implemented in C++.

6.2 Measurements

Power measurements. The power of the signal and the interference need to be determined at the receiver. To do so, we accumulate the received power over time as follows: $P_{tot} = \frac{\sum_{t=-n}^{n} |u(t)|^2}{2n}$. In order to get the noise power at the receiver for a certain signal bandwidth, we measure P_{tot}, after applying a band-pass filter on the signal bandwidth when the transmitter is not active. In a second measurement, the transmitter is active and we measure the power of the signal plus the noise at the receiver. By subtracting the noise power from the signal and noise power, we get the signal power:

$$S = P_{S+N} - P_N$$

In the same way, we measure the interference power in tests where the interference signal is the only one present:

$$I = P'_{I+N} - P'_N$$

The Signal-to-Interference Ratio (SIR) can then be expressed in dB as follows:

$$SIR_{dB} = 10 * log(\frac{S}{I}) = 10 * log(\frac{P_{S+N} - P_N}{P'_{I+N} - P'_N})$$

Gain computation. In order to compare different receiver approaches R_i to a reference case R_{ref}, we calculate the gain at an error rate of 50% for different B_s and B_j:

$$Gain(R_i, R_{ref}) = SIR_{dB}^{R_{ref}}(PER = 50\%) - SIR_{dB}^{R_i}(PER = 50\%) \quad (3)$$

The Packet Error Rate (PER) can be exchanged with the Symbol Error Rate (SER). A positive gain in Eq. (3) means that R_i outperforms the reference case R_{ref}.

6.3 Jammer implementation

We consider a jammer which transmits white Gaussian noise. Our implementation uses a fast noise source that generates a pool of 8192 samples from the distribution. The samples are chosen uniformly random from this pool. For evaluation purposes, we fix the jammer bandwidth in each test since we assume that a reactive jammer will not be able to react quickly enough to match its bandwidth to the hopping pattern of the transmitter. However, as the signal bandwidth is changed every few symbols in the tests, there is a continuous change in the offset between the signal and the jammer that allows to understand how different bandwidth offsets affect the performance. The bandwidth of the jammer is determined by a low pass FIR filter with the specified bandwidth using a Hamming window. The transition width is set to 10 kHz and the stop band attenuation is 70 dB. Finally, as mentioned in Section 3.1, the jammer has a finite maximal transmission power and a finite bandwidth. Therefore, a jammer covering a very large bandwidth has limited power allocated to each frequency band, and viceversa.

7 EVALUATION IN BASIC SETTINGS

We present and discuss the results obtained from different experimental evaluations.

7.1 Comparison to state-of-the-art BHSS

As reference receiver R_{ref}, we consider the one in [1]. In this first study, we consider that both our system and the reference one do not hop and do not apply excision filters (cf. Section 5.2.3). We then compute the gain of the new receiver with respect to R_{ref} using the metric presented in Eq. (3) with 50% PER both in our receiver and in R_{ref}. The results are summarized in Table 2, where we can observe that the proposed receiver design on preamble detection and decoding presented in Section 5.2 improves the jamming resistance in all the scenarios with different bandwidth offsets between signal and jammer.

7.2 Analysis of normalized cross correlation

Narrowband jammer. We study $n\_cc(s)$ considering a 10 MHz signal and jamming bandwidth of 0.15625 MHz (narrowband jammer). The results are shown in Fig. 4, with the *solid line that indicates the average n_cc(s), while the filled area represents the standard deviation.* In the absence of an excision filter, $n\_cc(s)$ decreases at a SIR of around -10 dB, which corresponds to the SIR at which symbol errors occur for the smallest jamming bandwidth (0.15625 MHz). In Fig. 4, we also show $n\_cc(s)$ for two filtered signals. As desired, $n\_cc(s)$ of the unfiltered signal drops below the filtered one around -10 dB SIR, while the filter with $B_s/8$ provides the most robust performance.

Signal bandwidth (MHz) \ Jammer bandwidth (MHz)	0.15625	0.3125	0.625	1.25	2.5	5	10
0.15625	-	-	6.75	5.02	6.99	4.8	6.37
0.3125	2.89	7.16	5.45	3.44	7.23	2.12	7.53
0.625	3.72	1.12	4.37	5	5.28	1.25	3.9
1.25	7.05	4.28	4.97	4.58	7.63	2.92	3.49
2.5	2.92	2.74	3.28	5.54	4.7	3.59	3.61
5	4.93	3.98	3.78	3.88	4.63	3.89	1.77
10	10.06	6.75	4.46	4.05	5.13	5.88	4.75

Table 2: Gain in dB for new receiver compared to [1] at a PER of 50%.

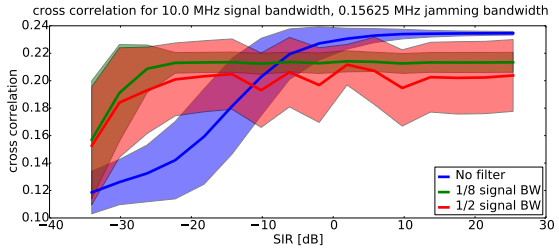


Figure 4: The normalized cross correlation $n\_cc(s)$ without filter decreases below the values with filter for increasing SIR and a narrowband jammer.

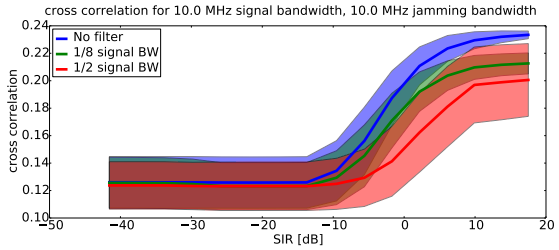


Figure 5: For $B_j = B_s$, the normalized cross correlation $n\_cc(s)$ without filter is higher than with filter.

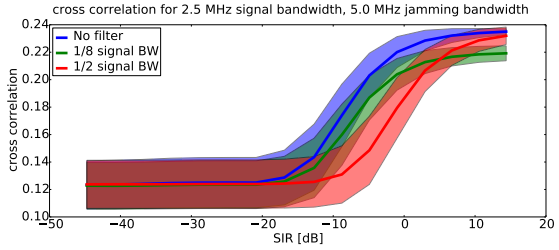


Figure 6: For a wideband jammer, $n\_cc(s)$ without filter is higher than with filter.

Jammer of bandwidth equal to the signal and wideband jammer. In Section 5.2.3 we discussed that an excision filter is beneficial only in case of a narrowband jammer. As decision metric to choose the correct filter, we expect that $n\_cc(s)$ should indicate this. We plot $n\_cc(s)$ in Fig. 5 in a scenario where $B_j = B_s$. We observe that $n\_cc(s)$ behaves as desired. The value for the case without filtering is the highest and we therefore do not apply a filter. The same behavior can be observed in Fig. 6 for a wideband jammer $B_j > B_s$. As before, no filter is applied.

7.3 Comparison among interference suppression methods

We evaluate the performance of our receiver with the different filtering techniques presented in Sec. 5.2.3. The transmitted signal has a constant B_s, which allows us to compare different B_s individually.

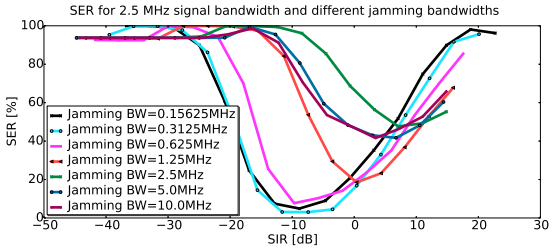


Figure 7: SER for 2.5 MHz signal and different B_j with filtering approach that excises large frequency bins.

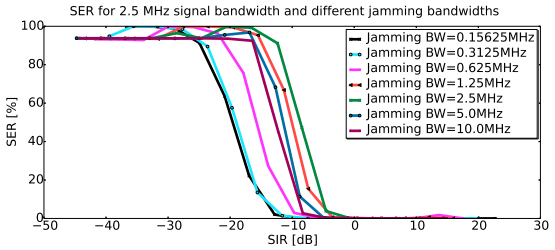


Figure 8: SER for 2.5 MHz signal and different B_j with filtering approach that whitens large frequency bins.

7.3.1 Jammer estimation. We first evaluate the two types of excision filters operating in the DFT domain.

Excise large frequency bins filter. In Fig. 7, the SER for the implementation that excises the large frequency bins is shown. We see that this excision technique helps to excise a narrowband jammer, if the SIR is around -10 dB. However, the performance of the approach degrades both if the jammer gets stronger and also if it gets weaker. This behavior is not desirable. The problem with this approach is that, *in case of a very weak jammer or no jammer, too many frequency bins are excised and the signal gets corrupted.*

Whiten large frequency bins. The results whitening only the largest frequency bins are shown in Fig. 8. *If the largest frequency bins are not completely excised, but only slightly modified, the performance for weak jammers is better, since the signal is not distorted as much as with excising all the energy.* Not shown here for reasons of limited space, we have also tested a version that whitens the entire spectrum, as proposed in [6]. However, the results are slightly worse than the proposed filter.

7.3.2 Parallel filtering. We evaluate our proposed parallel filtering approach (c.f. Section 5.2.3). In Fig. 9, we depict the SER for a 5 MHz signal and a 1.25 MHz jammer for all different combinations of the excision filters. The filter that excises $\frac{1}{8}$ of B_s is represented as "PF 1/8" in Fig. 9. We observe that it is too small and the performance degrades. The filter that removes $\frac{B_s}{4}$ matches the jamming bandwidth exactly ($\frac{1}{4} * 5\,\text{MHz} = 1.25\,\text{MHz}$) in this scenario. Therefore a good performance is expected. However, we see that the performance with the filter that removes $\frac{B_s}{4}$ is worse than expected. The performance degradation is due to our jammer implementation (c.f. Section 6.3). The low pass filter that filters the jamming signal to the desired bandwidth is not ideal. Due to the

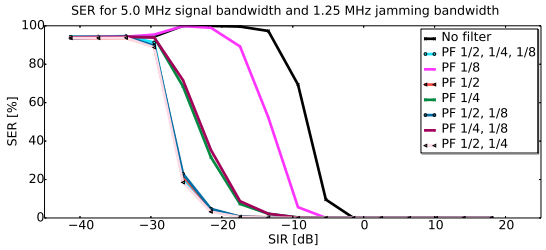


Figure 9: SER for 5 MHz signal and 1.25 MHz jamming bandwidth for different excision filters.

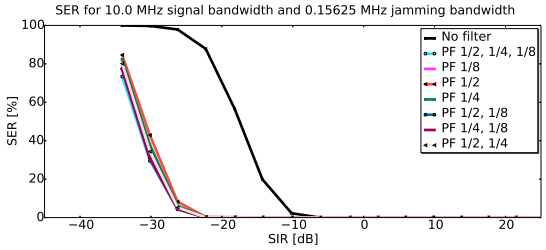


Figure 10: SER for 10 MHz signal and 0.15625 MHz jamming bandwidth for different excision filters.

Signal bandwidth (MHz) \ Jammer bandwidth (MHz)	0.15625	0.3125	0.625	1.25	2.5	5	10
0.15625	0	0.03	0	0	0	0	0.02
0.3125	-0.08	-0.14	-0.12	-0.25	-0.17	-0.14	-0.08
0.625	0.07	0.13	-0.2	-0.34	-0.15	-0.47	-0.1
1.25	0.03	0.03	0.12	-0.23	-0.16	-0.19	-0.12
2.5	-0.03	0	0.1	0.1	-0.16	-0.17	-0.15
5	-0.12	0.01	0	0.1	0.08	-0.14	-0.16
10	-0.49	-0.24	0.02	-0.01	-0.29	0	-0.16

Table 3: Gain in dB for two filters in parallel that remove $\frac{B_s}{2}$ and $\frac{B_s}{4}$.

Signal bandwidth (MHz) \ Jammer bandwidth (MHz)	0.15625	0.3125	0.625	1.25	2.5	5	10
0.15625	0.22	0.16	0.15	0.07	-0.01	0.16	0.14
0.3125	-1.7	-0.12	-0.01	0.03	-0.05	0.01	0.13
0.625	-21.36	-11.96	-0.15	0	-0.06	-0.08	0.02
1.25	-22.4	-19.12	-11.01	-0.16	-0.05	0.06	0.01
2.5	-23.4	-21.57	-18.06	-7.21	-0.08	-0.01	0.03
5	-20.87	-20.39	-18.15	-14.95	-4.22	-0.04	0
10	-14.6	-16.78	-17.57	-15.89	-8.54	-2.28	-0.03

Table 4: Gain in dB for two DFT excision filters that remove $\frac{B_s}{2}$ and $\frac{B_s}{4}$.

transition width and frequency offsets of the devices there is some amount of the jammer energy outside of the desired bandwidth.

Signal bandwidth (MHz) \ Jammer bandwidth (MHz)	0.15625	0.3125	0.625	1.25	2.5	5	10
0.15625	13.69	11.6	11.38	10.91	9.9	9.94	9.03
0.3125	11.89	10.65	9.47	9.04	9.04	7.36	5.01
0.625	33.77	18.16	8.04	6.04	6.63	6.06	5.89
1.25	29.28	28.03	18.02	6.18	6.76	5.92	5.96
2.5	30.16	29.13	24.49	9.47	2.36	3.45	1.96
5	23.61	26.63	25.18	15.79	8.17	3.66	2.61
10	13.72	18.6	25.84	26.99	8.23	3.93	1.43

Table 5: Gain in dB for our approach compared to [1].

In case of a very narrowband jammer, the use of smaller filters is more beneficial than larger filters. In Fig. 10 we depict this case for a 10 MHz signal and a 0.15625 MHz jammer. However, the difference between the filter that removes $\frac{1}{2}$ of the signal bandwidth and the smaller filters is minor. The performance of the smaller filters is degraded due to the jammer implementation as outlined in the previous experiment, since the jammer is effectively larger. In addition, the energy distribution of the half sine pulse shape is not flat. For instance, the energy within the inner 2.5 MHz of a 5 MHz signal gives 64.7% of the total energy. The amount of energy that is filtered is therefore not linear with the bandwidth that is cut out. Moreover, our BHSS implementation spreads the signal in spectrum. This introduces some jamming resistance against narrowband jammers. The unfiltered signal therefore already provides limited jamming resistance against narrowband jammers.

7.4 Gain of Parallel Filter approach

From the study in the previous section, we choose the approach that runs three excision filters ($B_s/2$, $B_s/4$ and $B_s/8$) in parallel *as reference case*, and compute the gain of the other approaches compared to the reference. First, we compute the SIR at a SER of 50% for the reference case. Then, we compute the gain by subtracting this SIR to the one achieved with the approach to compare (see Eq. (3)). In Table 3, we present the gain for running the two larger filters ($B_s/2$ and $B_s/4$) in parallel. We observe that the positive as well as the negative gain stays below 0.5 dB. The use of the two largest excision filters provide the best trade-off between jamming resistance and computational efficiency. Other selections of filters are not shown here and as they have performance drops.

Finally, we present the result of the parallel filtering approach which runs with DFT excision (c.f. Section 5.2.3). In Table 4, we show the gain of running two DFT excision filters that whiten $B_s/2$ and $B_s/4$ of the signal compared to the reference case. The performance of the DFT filters do not reach the FIR filters, as we measure a negative gain. We do not show our other parallel filters that operate in the DFT domain as they show worse results.

7.5 Comparison to state-of-the art BHSS receiver

Table 5 shows the gain of our approach compared to the receiver in [1]. We achieve a positive gain throughout all signal and jamming bandwidths. The gain for wideband jamming scenarios results from our new receiver design (c.f. Section 5). The gain for narrowband

BHSS pattern	2,4,8,16,32,64,128	2,4,32,32	2,4,64,8,2
Transmission time	$2.268T_r$	$1.094T_r$	T_r

Table 6: Transmission times of BHSS patterns used in the experiment compared to the reference case 1.25 MHz.

	DSSS no filter	DSSS filter	BHSS no filter
SIR at 50% SER (dB)	-10.6761465	-10.5679408	-13.44447269
Gain (dB)	0	-0.11	2.77
	BHSS filter	BHSS 2,4,32,32 filter	BHSS 2,4,64,8,2 filter
SIR at 50% SER (dB)	-19.70478857	-28.71706466	-29.88480471
Gain (dB)	9.03	18.04	19.21

Table 7: Gain table for different BHSS patterns compared to DSSS with fixed bandwidth of 1.25 MHz.

jammers is achieved through the proposed filtering approach. Our approach achieves a gain of up to 33.77 dB.

8 EVALUATION WITH BANDWIDTH HOPPING AT THE SYMBOL LEVEL

We now study the performance of our implementation of BHSS considering bandwidth hopping at the symbol level.

8.1 BHSS vs DSSS

In this section, we compare BHSS with DSSS. We use a fixed bandwidth of 1.25 MHz for DSSS. Three larger and three smaller bandwidths are available for hopping (c.f. Table 1). A constant jammer with B_j equal to 1.25 MHz is used.

We evaluate different hopping patterns for BHSS. The hopping time is set to three symbols. The standard pattern (BHSS) uses all available bandwidths once. Furthermore we use two patterns that use only a subset of the available bandwidths. The first pattern (BHSS 2, 4, 32, 32) uses 10 MHz, 5 MHz and twice 0.625 MHz. The second pattern (BHSS 2, 4, 64, 8, 2) chooses among 10 MHz, 5 MHz, 0.3125 MHz, 2.5 MHz and 10 MHz again. We select these patterns based on throughput considerations. For fairness in the evaluation, we choose the transmission time T_r of the 1.25 MHz signal bandwidth as reference value. We then calculate the average T_r for one symbol for a given BHSS pattern, and summarize the transmission time ratios for the patterns we use in the experiment in Table 6. We observe that, for the last pattern, the average T_r for a symbol is the same as in the reference case. Therefore the throughput of the system is the same as well. The first two patterns have slightly longer T_r and therefore a lower throughput.

In Table 7, we calculate the gain for the hopping patterns. In our measurement, we achieve a gain of 9.03 dB for BHSS. For the patterns that have approximately the same T_r, a gain of 18.04 dB and 19.21 dB respectively is achieved. The additional gain results mainly from the large bandwidths that are used more often in these patterns, i.e. they have a larger bandwidth offset with respect to B_j.

8.2 BHSS and FHSS in wideband jamming

We then compare the performance of BHSS and FHSS in a wideband jamming scenario. A constant 10 MHz jammer is applied. FHSS operates at a constant bandwidth of 2.5 MHz and uses three channels: one at center frequency, one at +2.5 MHz and one at −2.5 MHz. BHSS uses all available bandwidths and hops every three symbols

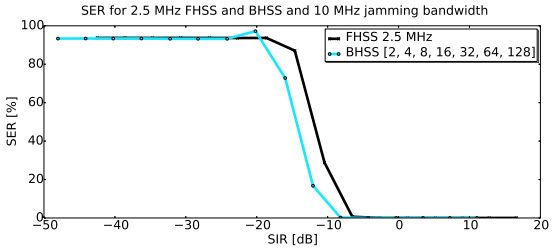


Figure 11: SER for 2.5 MHz FHSS and BHSS with 10 MHz jamming bandwidth.

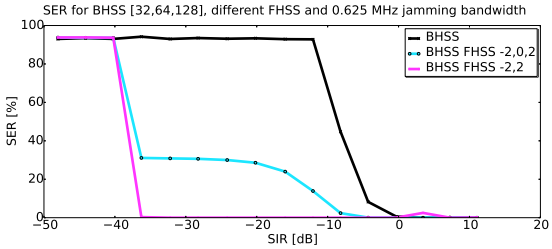


Figure 12: SER for 0.625 MHz jammer at center frequency and different BHSS patterns with frequency hopping.

(cf. Table 1). The results of the SER are depicted in Fig. 11, showing that we achieve a gain of 2.43 dB. However, the average transmission time of one symbol for the BHSS approach is $4.54 \cdot T_{2.5MHz}$, where $T_{2.5MHz}$ corresponds to the transmission time for a constant 2.5 MHz bandwidth. The throughput of the BHSS approach is therefore lower than the throughput of FHSS.

8.3 BHSS with frequency hopping

We combine the three SS technologies BHSS, DSSS and FHSS, by enhancing BHSS with frequency hopping. For BHSS, we use the three smallest available bandwidths (0.15625, 0.3125, 0.625 MHz). We introduce a constant jammer with 0.625 MHz jamming bandwidth at center frequency. In Fig. 12 we show the SER for such a scenario and different frequency hopping patterns for BHSS. BHSS without frequency hopping is strongly affected by the jammer at center frequency. In the second pattern a channel at -2.5 MHz, one at center frequency and one at +2.5 MHz are used. The channel at center frequency will be affected by the jammer, while the others are not. We therefore expect a SER of 33%, which is what we observe in Fig. 12. The last pattern completely avoids the center frequency by using only the two channels at -2.5 Mhz and +2.5 MHz respectively. With this pattern, there is no performance degradation due to the jammer.

9 CONCLUSION

In this work, we have proposed a novel filtering technique as well as new communication modules at the transmitter and the receiver to allow signal bandwidth hopping every few symbols, and boost the performance of BHSS against jamming attacks. We showed that the use of as few as two filters is sufficient for good jamming mitigation

and that our approach learns effectively about the best excision filters to apply in case of narrowband jammers. We showed that FIR filters in BHSS outperform filters that process the signal in the frequency domain. Finally, we showed that the three spread spectrum technologies DSSS, BHSS and FHSS can coexist and work together in a complementary way to enhance the overall performance of wireless communications under jamming attacks.

REFERENCES

[1] M. Liechti, V. Lenders, and D. Giustiniano, "Jamming mitigation by randomized bandwidth hopping," in *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '15. ACM, 2015, pp. 11:1–11:13.

[2] M. Song, C. Xin, Y. Zhao, and X. Cheng, "Dynamic spectrum access: from cognitive radio to network radio," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 23–29, February 2012.

[3] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*. Springer US, 2006.

[4] R. Beerends, *Fourier and Laplace Transforms*, ser. Fourier and Laplace Transforms. Cambridge University Press, 2003.

[5] L. B. Milstein and R. A. Iltis, "Signal processing for interference rejection in spread spectrum communications," *ASSP Magazine, IEEE*, vol. 3, no. 2, pp. 18–31, 1986.

[6] J. W. Ketchum and J. G. Proakis, "Adaptive Algorithms for Estimating and Supressing Narrow-Band Interference in PN Spread Spectrum Systems," *IEEE Trans. on Comm.*, vol. 30, no. 5, May 1982.

[7] B. DeBruhl and P. Tague, "Mitigation of Periodic Jamming in a Spread Spectrum System by Adaptive Filter Selection," in *International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS)*, February 2012.

[8] M. J. Medley, G. J. Saulnier, and P. K. Das, "Applications of the wavelet transform in spread spectrum communications systems," in *SPIE's International Symposium on Optical Engineering and Photonics in Aerospace Sensing*. International Society for Optics and Photonics, 1994, pp. 54–68.

[9] M. G. Amin, "Interference mitigation in spread spectrum communication systems using time-frequency distributions," *Signal Processing, IEEE Transactions on*, vol. 45, no. 1, pp. 90–101, 1997.

[10] M. G. Amin, C. Wang, and A. R. Lindsey, "Optimum interference excision in spread spectrum communications using open-loop adaptive filters," *Signal Processing, IEEE Transactions on*, vol. 47, no. 7, pp. 1966–1976, 1999.

[11] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications handbook*. McGraw-Hill New York, 2002.

[12] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proceedings ACM Conference on Wireless Network Security (WiSec)*, 2011, pp. 47–52.

[13] R. Gold, "Optimal binary sequences for spread spectrum multiplexing (corresp.)," *Information Theory, IEEE Transactions on*, vol. 13, no. 4, pp. 619–621, 1967.

[14] S. G. Glisic, *Adaptive WCDMA: theory and practice*. John Wiley & Sons, 2003.

[15] B. W. Parkinson, J. J. Spilker Jr *et al.*, "Global positioning system: Theory and applications volume 1 & ii, aiaa," 1996.

[16] F. Gardner, "A bpsk/qpsk timing-error detector for sampled receivers," *IEEE Transactions on Communications*, vol. 34, no. 5, pp. 423–429, May 1986.

[17] E. Blossom, "Gnu radio: Tools for exploring the radio frequency spectrum," *Linux J.*, vol. 2004, no. 122, pp. 4–, Jun. 2004.