Jamming Mitigation by Randomized Bandwidth Hopping

Marc Liechti
ETH Zurich
Zurich, Switzerland
marc@
liechti.one

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

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

ABSTRACT

We present bandwidth hopping spread spectrum (BHSS), a novel technique to improve the jamming resistance of wireless communications. In BHSS, the bandwidth of a signal is hopped rapidly in a manner that is unpredictable to the jammer. We show in this work that by combining bandwidth hopping at the transmitter with adaptive filtering at the receiver, 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. We have designed and implemented a BHSS transmitter and receiver system on off-the-shelf software-defined radios. Our experimental results with different hopping patterns show that BHSS is able to boost the power advantage of spread spectrum communication by 8 to 20 dB for jammers of fixed bandwidth. When both transmitter and jammer hop randomly, the average power advantage we achieve with our system is 11.4 dB.

CCS Concepts

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

Keywords

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

1. INTRODUCTION

Spread spectrum (SS) communication is a technique in which the bandwidth of the transmitted waveform is intentionally made wider than would be necessary to transmit the information over the channel. SS was originally developed to resist jamming attacks in military environments. However, nowadays, SS is also wide-spread in other civilian communications systems such as low-power sensor networks, WLAN, global navigation satellite systems, and unmanned aerial vehicle (UAV) control systems.

There exist two common spread spectrum techniques: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). To mitigate the interference 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. In FHSS, the transmitter randomly hops the carrier frequency of the modulated signal. 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*.

In theory, any level of jamming rejection can be achieved in DSSS or FHSS by using sufficient processing gain, i.e., by spreading the signal to an arbitrarily large bandwidth. For example, military communication systems may be using spreading factor up to 1000 [1, 2] to achieve processing gains in the order of 30 dB. However, the wireless spectrum is a scarce resource today and allocating that much spectrum for achieving jamming resistance is generally not desired or even impossible in non-military contexts, given the throughput requirements of current communication systems.

To overcome this fundamental challenge, *excision filtering* techniques have therefore been proposed in conjunction with the SS receiver in order to augment the processing gain without an increase in bandwidth. The main idea behind excision filters is to place an interference suppression filter prior to the despreading function in order to suppress a narrowband interferer without cancellation of the desired signal [3, 4, 5,

CoNEXT '15, December 01-04, 2015, Heidelberg, Germany
© 2015 ACM. ISBN 978-1-4503-3412-9/15/12…$15.00
DOI: http://dx.doi.org/10.1145/2716281.2836096

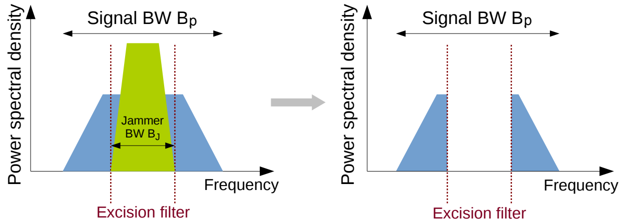

Figure 1: The jammer bandwidth is smaller than the signal bandwidth. Applying an excision filter removes the signal power of the jammer.

6, 7]. While highly effective at suppressing *unintentional* narrow-band interference, excision filters as such fail to resist against *malicious* jamming attacks. A malicious jammer can observe the signal bandwidth as being transmitted over the air and match his jamming waveform to the bandwidth of the signal rendering any excision filtering ineffective. The jamming resistance of SS in adversarial conditions has therefore been considered up to now as being equal to the processing gain of the system [1, 2, 8, 9].

In this paper, we show in contrast that it is possible to improve the jamming resistance in adversarial settings beyond the processing gain of traditional SS communication. The new concept we propose in this work is to *quickly hop the SS signal bandwidth according to a randomized hopping pattern that is known to the receiver, but unpredictable to the adversary*. In other terms, we explore the bandwidth as a new dimension that complements the chip and frequency domains for jamming-resilient communications. When the signal bandwidth is hopping fast enough such that the jammer cannot react quickly enough to the current bandwidth being transmitted, it is no longer possible for the jammer to match its bandwidth to the one of the transmitter.

Depending on the transmitter-jammer bandwidth offset, we can then differentiate three fundamental cases: (i) The signal width B_p is wider than the interfering jammer B_j (Figure 1). The jammer's interference appears as narrow-band and it can thus be suppressed at the receiver effectively with an excision filter prior despreading. (ii) The jammer signal is wider than the communication signal (Figure 2). The receiver can low-pass filter the received signal in baseband and hence remove the signal power of the jammer that is outside the signal spectrum. (iii) The interference has the same width as the signal (Figure 3). In the latter case, the receiver is left with the entire interference of the jammer when despreading the signal and the resistance is equal to the processing gain of traditional SS techniques. However, when the signal bandwidth is constantly hopping, the likelihood that the jammer bandwidth matches the one of the transmitter by chance is low and this case therefore rarely occurs.

While the idea of dynamically adapting the signal bandwidth in wireless communications has also been suggested recently in [10, 11], the hopping requirements for achieving jamming resistance impose new challenges that we address in this work:

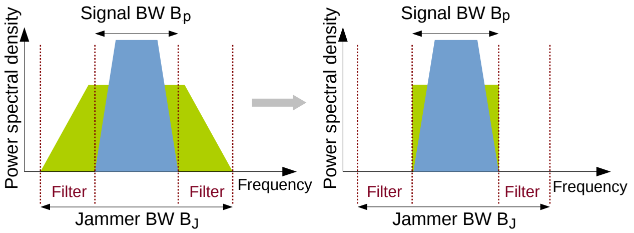

Figure 2: The jammer bandwidth is larger than the signal bandwidth. Applying a low-pass filter removes the power of the jammer that is outside the bandwidth of the communication signal.

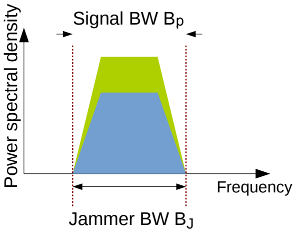

Figure 3: The signal and the jammer bandwidth are the same. The power of the jammer cannot be filtered out. When the signal bandwidth is constantly hopping, the likelihood that the jammer bandwidth matches the one of the transmitter by chance is low and this case therefore rarely occurs.

1. The signal bandwidth B_p must be adapted quickly when the radio is active during the transmission of individual packets. This is necessary to resist to modern reactive jammers [12] that are capable of following signals with reaction delays below packet transmission times. In contrast, existing communication schemes proposed in the literature operate at much coarser granularities and adapt the signal bandwidth between packet transmissions when the front-end radio is idle.
2. Previous works endorsed dynamic signal bandwidths having data throughput as primary objective. These works therefore do not address the issues of making the hopping pattern unpredictable and robust to jammers and to filter out interference at the receiver prior despreading in order to improve the jamming resistance beyond the processing gain of SS.

Our main contributions in this paper are:

- We propose bandwidth hopping spread spectrum (BHSS) as a technique to improve the jamming resistance beyond the processing gain of SS communication systems. In contrast to other jamming mitigation techniques [13, 14], BHSS improves the jamming resistance in communications systems that operate with a single omnidirectional antenna at the transmitter and receiver.
- We present the transmitter and receiver communication schemes to quickly hop the bandwidth of SS sig-

nals while actively transmitting, i.e. the bandwidth is hopped during the transmission of individual packets.

- We analytically derive the general SNR improvement of a BHSS receiver for different bandwidth offsets between transmitted and jamming signals. We evaluate the bit error rate and throughput of a BHSS receiver and compare those to the performance of conventional DSSS and FHSS receivers.
- We implement a bandwidth hopping transmitter and receiver on software defined radios and demonstrate the improved jamming resistance for different hopping patterns.

2. SYSTEM AND ATTACKER MODEL

We consider a scenario in which a transmitter wants to send data to a receiver over the wireless channel. This communication could be for example between a ground station and a UAV. The attacker is a jammer that wants to disrupt the wireless communication between the transmitter and the receiver.

The jammer is assumed to be in transmission range of both the transmitter and the receiver, so that he can overhear the signals from the transmitter as well as interfere with its own signals at the receiver. For this, the jammer may rely on half duplex or full duplex radios [15]. Regardless of the radio type, we assume that the jammer has reactive capabilities, i.e., the jammer can sense the channel and interfere with a signal based on the sensed channel information. Reactive jamming is a relatively strong attacker model, however it has been shown to be a realistic threat model as it is possible to implement such a jammer using commercial off-the-shelf (COTS) hardware only [12].

We assume the jammer reaction time to be lower-bounded. We denote the time difference between the arrival of the original signal and the jammer signal at the receiver as the jamming reaction time τ. The minimal reaction time τ_{min} is bounded by the sum of (i) the signal propagation delay between the sender and the jammer, (ii) the hardware and software reaction delay of the jammer to process the incoming signal and to make a jamming decision, and (iii) the signal propagation delay between the jammer and the receiver. It is therefore safe to assume that the minimum reaction time τ_{min} is greater than the duration of a couple of bits or symbols [12].

Both the legitimate transmitter and the jammer are assumed to have infinite energy but limited transmission power budget. The jammer can thus interfere with any signal waveform and an arbitrary signal bandwidth, as long as it does not exceed its power budget. In order to attack a SS system that is not hopping the bandwidth, the jammer may therefore sense the bandwidth of the signal sent by the transmitter and react with an additive white Gaussian noise (AWGN) signal that interferes at the receiver with the same bandwidth as the target signal. The mere application of excision filters without dynamically hopping the bandwidth of the signal is therefore ineffective at mitigating the impact of jamming under the considered reactive attacker model.

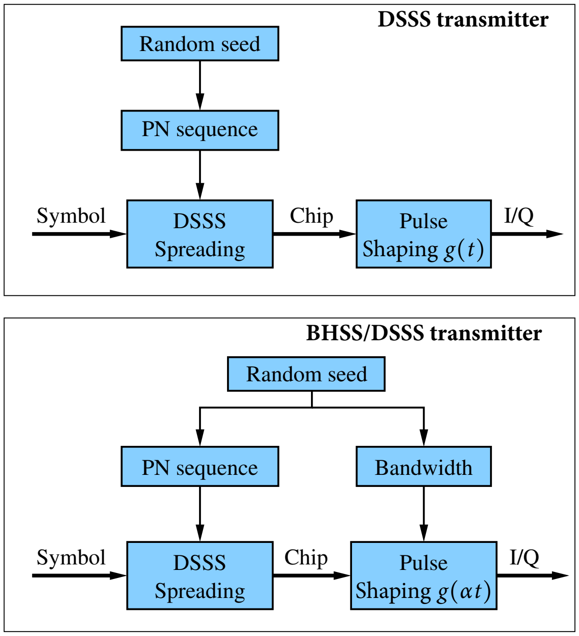

Figure 4: Comparison between conventional DSSS block scheme and block scheme of BHSS. In BHSS, the pulse shape is not constant but randomly changed to produce spread signals of different bandwidths. BHSS can analogously be applied to FHSS.

3. BANDWIDTH HOPPING TRANSMITTER

The novel concept we propose in this work is to hop randomly the bandwidth of the signal in a manner that is unpredictable to the jammer. Wireless communication systems have traditionally been designed with fixed signal bandwidths. Some more recent systems support adaptive signal bandwidths, but the bandwidths are not switched in the same way as proposed in this work. For example in [10], the authors propose SampleWidth, an algorithm that samples the channel conditions and dynamically switches between different bandwidths. However, the bandwidth is switched at the MAC layer when the experienced packet error rate or SNR drops below a certain value in order to move to more robust rates. Since the rate switching occurs at the MAC, the hopping between different bandwidths is too slow to protect against a reactive jammer that tries to match its bandwidth to the signal bandwidth of the signal. As shown in [12], reactive jammers are able to estimate signals over the air and generate matched jamming signals in the order of a couple of symbols. To thwart reactive jammers, it is therefore necessary to hop the bandwidth dynamically at the PHY layer by changing the bandwidth during the transmission of the signal.

Figure 4 illustrates how we propose to hop the bandwidth of a signal in a randomized manner. Our illustration refers to the application of bandwidth hopping to DSSS but it can be extended to FHSS in an analogous way as well. At the top of Figure 4, we see the block structure of a conventional DSSS transmitter. The bit stream of information is first

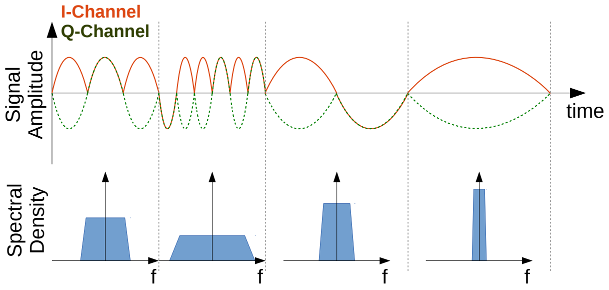

Figure 5: Signal waveform and bandwidth of a BHSS signal whose bandwidth is hopped dynamically during a transmission.

mapped to symbols and then chips by multiplying the symbols with a pseudo-noise (PN) sequence. This corresponds to the spreading operation of DSSS. The PN sequence is initialized with a random source to make the chip sequence unpredictable to the jammer. Each chip is then modulated with a pulse shape $g(t)$, whose shape is depending on the modulation scheme. The difference between the conventional DSSS transmitter and BHSS is visible at the bottom of Figure 4. Instead of using a constant pulse shape $g(t)$, we vary the shape of the pulse by scaling its duration with a factor α. The value of α is chosen randomly using a random seed and changed after a fixed number of symbols. By randomly varying the pulse shape duration, we produce modulated signals of different bandwidths that are unpredictable to the jammer. Stretching a signal in the time domain with α has the effect of reducing the signal width in the frequency domain by the same factor, and viceversa:

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

where $\mathcal{F}$ indicates the Fourier transform. Using this technique, the signal bandwidth can be adapted to any desired bandwidth without interrupting the signal transmission. An example of the signal waveform and bandwidth over four hops is shown in Figure 5. As we see in the top of the Figure, the pulse shape duration is first decreased and then increased twice. This produces a signal whose bandwidth in baseband is hopping as illustrated in the bottom of Figure 5. In the presence of jamming, the goal of the BHSS transmitter is therefore to hop according to a strategy that minimizes the bit error rate, while guaranteeing a sufficiently high communication rate.

4. BANDWIDTH HOPPING RECEIVER

The receiver has to face two main challenges to decode the data transmitted by the bandwidth hopping transmitter:

(i) It must acquire a signal whose bandwidth is hopping during a transmission with a random pattern.

(ii) The acquired signal will further include the superimposed interference generated by the jammer which needs to be estimated and filtered by the receiver.

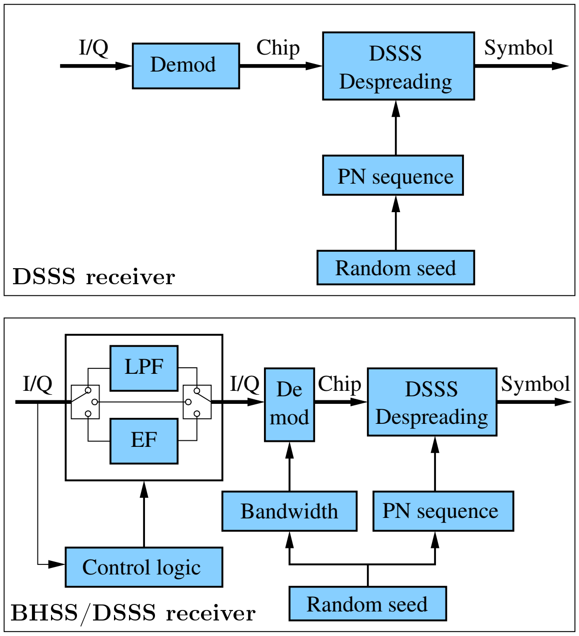

Figure 6: Comparison between conventional DSSS receiver and BHSS receiver. In BHSS, the demodulator is synchronized to the bandwidth of the signal and a control logic estimates and configures filters to suppress interference prior sending the I/Q samples to the demodulator. In the figure, LPF stands for low pass filter and EF for excision filter.

In order to address (i) and (ii), we introduce our receiver structure to synchronize to the signal bandwidth (Section 4.1) and suppress the interference of the jammer for different bandwidth offsets between the signal and the jammer (Section 4.2).

4.1 Bandwidth Synchronization

Conventional SS systems operate at fixed signal bandwidths. The DSSS and FHSS receivers therefore need only to synchronize to the PN sequence or the frequency hopping pattern for the despreading operation. For example, the receiver block structure for DSSS is shown at the top of Figure 6. The receiver first demodulates the chips from the received I/Q samples. Then, the symbols are despread by correlating the received chip sequence with a replica of the synchronized PN sequence. The PN sequence is synchronized to a random seed at the receiver. Random seed synchronization between transmitter and receiver can be done in different ways. The most common techniques rely on pre-shared keys [16] or through uncoordinated discovery schemes [17]. In this work, we assume that such a random source synchronization mechanism already exists since it is present in any SS system.

The block structure of the BHSS receiver is more complex. The bandwidth hopping further necessitates synchronization to the hopping pattern with the transmitter. Several synchronization schemes are conceivable. A receiver could in principle recover the instantaneous bandwidth of the signal by inspecting the spectrum of the acquired samples (e.g.

with FFT). However, this approach is not robust to jamming scenarios because the instantaneous bandwidth of the incoming signal may be dominated by the jammer for strong jamming powers. We therefore suggest instead to rely on the same random source as for the synchronization of the spreading operation in DSSS or FHSS. That is, we derive the instantaneous bandwidth at the receiver from the synchronized random source as shown at the bottom of Figure 6.

4.2 Jammer Estimation and Filtering

The main difference between a conventional SS receiver and our bandwidth hopping receiver is that we estimate and suppress the jammer prior despreading the signal. For this, the BHSS receiver includes a control logic that controls the configuration of a low-pass filter (LPF) and an excision filter (EF) prior demodulation as shown in Figure 6. This will result in an improvement of the jamming resistance beyond the processing gain of the despreading operation. In order to select an appropriate filter to suppress the jamming interference prior despreading, a control logic estimates the frequencies occupied by the jammer. A convenient way to do so is by means of spectral analysis. Since the spectrum of the PN sequences is relatively flat across the entire frequency band, jammers are easily recognizable. Narrow-band jammers will exhibit peaks at the frequencies occupied by the jammer within the spectrum of the signal bandwidth. Wide-band jammers will result in spectra that are significantly wider than the spectrum of the signal. Only jammers that have a power or bandwidth similar to the signal may not be estimated easily by means of spectrum analysis. However, estimation in this case is not necessary:

- In the case where the bandwidth of the jammer is close to the bandwidth of the signal, we cannot apply any pre-filtering anyway, since filtering requires a significant bandwidth offset between jammer and signal.
- In the case where the power of the jammer is in the same order of magnitude as the signal, pre-filtering is not needed either as the processing gain of the despreading operation should suffice to suppress the interference for successful decoding.

Therefore, the spectral analysis is well suited to estimate the jammer frequency occupancy across the entire power and bandwidth ranges that matters for the receiver.

The spectral estimate can be obtained by any one of the well-known spectral analysis techniques such as for example Bartlett's [18] or Welch's [19] method. Once the power spectral density of the received signal is estimated, the control logic can parametrize the interference suppression filter. A FIR filter is an appropriate filter structure to filter both narrow-band as well as wide-band jammers. The problem is to specify the K tab coefficients $h(n)$ or, equivalently, the DFT $H(k)$, defined as

$$H(k) = \sum_{n=0}^{K-1} h(n) e^{-j\frac{2\pi}{K}nk}, \quad k = 0,1,...,K-1. \tag{2}$$

When the jammer is narrow-band ($B_p > B_j$), an effective method for designing a FIR filter in the time domain for arbitrary jamming signals is to select an *excision filter* with its discrete Fourier transform (DFT) to be reciprocal to the square root of the power spectral density at equally spaced frequencies [7]. The DFT $H(k),\ k = 0,1,...K-1$ is therefore selected as

$$H(k) = \frac{1}{\sqrt{\hat{P}\left(\frac{k}{K}R_s\right)}} e^{-j\frac{\pi(K-1)}{K}k} \tag{3}$$

where $\hat{P}(f), 0 \le f \le R_s$, denotes the estimated power spectral density and R_s denotes the sampling rate. That is, the interference suppression filter attempts to whiten the spectrum of the incoming signal, and the excision filter will have large attenuation in the frequency range occupied by the jammer and a relatively small attenuation elsewhere.

When the jammer is wide-band ($B_p < B_j$), the FIR filter should suppress the frequencies outside the spectrum of the signal. The ideal filter is therefore a *low-pass filter* with a DFT $H(k), k = 0,1,...K-1$ as

$$H(k) = \begin{cases} 1 & \text{if } \frac{k}{K}R_s \le B_p, \\ 0 & \text{if } \frac{k}{K}R_s > B_p. \end{cases} \tag{4}$$

5. THEORETICAL RESULTS

This section compares the performance between a bandwidth hopping system and conventional SS with fixed bandwidth. In particular:

- We derive an upper bound on the improvement factor for different jammer-signal bandwidth offsets in terms of the SNR at the output of a correlation receiver.
- We compare the achievable bit error rate and throughput for an ideal QPSK receiver in the presence of different jamming bandwidths and power levels for BHSS, DSSS and FHSS.

5.1 SNR Improvement Factor

The SNR at the output of a correlation receiver is a convenient performance indicator to assess the improvement in performance obtained by interference suppression filters. We therefore derive the output SNR for bandwidth hopping and fixed bandwidth receivers, and define the SNR improvement factor as a measure to capture the performance gain of BHSS versus conventional spread spectrum.

In the correlation receiver, the received baseband signal, sampled at the chip rate, can be represented as

$$r(k) = p(k) + j(k) + n(k), k = 1,2,... \tag{5}$$

where the binary sequence $p(k)$ represents the PN chips with values ±1, $j(k)$ represents the sequences of samples of the jamming signal and $n(k)$ represents the sequence of noise samples. Let $h(k)$ represent the impulse response of the excision and low-pass FIR filters with K tabs, and let L represents the number of chips per information bit (also referred to as symbol) or the processing gain. We assume that the PN sequence $p(k)$ is white, the interference $j(k)$ has zero mean and autocorrelation function $\rho_j(k)$, and the additive noise $n(k)$ is white with variance σ_n^2.

As derived in the Appendix, the SNR at the output of the correlator can be expressed as:

$$\mathrm{SNR} = \frac{L}{\sum\limits_{l=1}^{K-1} h^2(l) + \sum\limits_{l=0}^{K-1}\sum\limits_{m=0}^{K-1} h(l)h(m)\rho_j(l-m) + \sigma_n^2 \sum\limits_{l=0}^{K-1} h^2(l)}. \quad (6)$$

If there is no suppression filter, $h(l) = 1$ for $l = 0$ and zero otherwise. Therefore the corresponding output SNR is

$$\mathrm{SNR}_{\mathrm{no}} = \frac{L}{\rho_j(0) + \sigma_n^2}, \quad (7)$$

where $\rho_j(0)$ represents the total power of the interference.

The ratio of the SNR in eq. (6) and eq. (7) represents the improvement in performance due to the bandwidth offsets. This ratio, denoted by γ, is

$$\gamma = \frac{\rho_j(0)+\sigma_n^2}{\sum\limits_{l=1}^{K-1} h^2(l) + \sum\limits_{l=0}^{K-1}\sum\limits_{m=0}^{K-1} h(l)h(m)\rho_j(l-m) + \sigma_n^2 \sum\limits_{l=0}^{K-1} h^2(l)}. \quad (8)$$

We observe that γ is independent of L. In other words, the SNR improvement of BHSS does not depend on the processing gain. As a consequence, the SNR improvement is a *universal result that applies to BHSS with an arbitrary processing gain.*

5.2 Upper Bound for SNR Improvement

In order to characterize the improvement that BHSS can provide over conventional spread spectrum, we derive an upper bound on the SNR improvement factor γ for different bandwidth offsets between transmitter and jammer. For the analysis, we assume ideal narrow-band and wide-band filters. An ideal narrow-band filter is an excision filter that filters out entirely all frequencies occupied by the narrow-band jammer without any distortion of the other remaining signal frequencies. An ideal wide-band filter is a low-pass filter that leaves the frequencies occupied by the transmitter unchanged while entirely suppressing the higher frequency range above the bandwidth of the transmitter as occupied by the wide-band jammer. In practice, it may not be feasible to implement such optimal filters with FIR filters but our idealized assumptions serve the purpose to understand the best achievable performance.

Upper bound for narrow-band jamming: In case of a narrow-band jammer, the optimal excision filter is perfectly matched to the bandwidth of the jammer and the residual narrow-band interference (the term $\sum\limits_{l=0}^{K-1}\sum\limits_{m=0}^{K-1} h(l)h(m)\rho_j(l-m)$) in eq. (8)) becomes zero. The remaining noise after the filtering is then composed of the self-noise due to the time dispersion introduced by the interference suppression filter ($\sum\limits_{l=1}^{K-1} h^2(l)$) and the filtered white-band noise ($\sigma_n^2 \sum\limits_{l=0}^{K-1} h^2(l)$). Since the PN sequence and the noise are white, the power of both remaining terms are proportional to the bandwidth of the pass-band and the improvement factor is

$$\gamma = \frac{\rho_j(0) + \sigma_n^2}{\frac{B_p}{B_p - B_j}(1 + \sigma_n^2)}, B_j < B_p \quad (9)$$

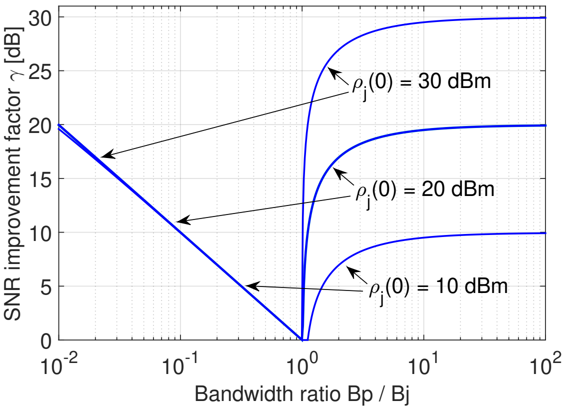

Figure 7: Upper bound on SNR improvement factor for ideal filtering and $\sigma_n^2 = 0.01$.

where B_p and B_j correspond to the bandwidths of the binary sequence $p(k)$ and the narrow-band interference $j(k)$ respectively. Note that this expression may become smaller than one when

$$B_j > \frac{\rho_j(0) - 1}{\rho_j(0) + \sigma_n^2} B_p. \quad (10)$$

This is the case when the bandwidth of the narrow-band jammer is close to the bandwidth of the PN sequence. In that case, applying an excision filter is worse than using no filter at all. Therefore, the excision filter should not be applied prior despreading when $B_j > \frac{\rho_j(0)-1}{\rho_j(0)+\sigma_n^2} B_p$. More precisely, the upper bound is therefore

$$\gamma = \begin{cases} \frac{\rho_j(0)+\sigma_n^2}{\frac{B_p}{B_p-B_j}(1+\sigma_n^2)} & \text{if } B_j \leq \frac{\rho_j(0)-1}{\rho_j(0)+\sigma_n^2} B_p, \\ 1 & \text{if } B_j > \frac{\rho_j(0)-1}{\rho_j(0)+\sigma_n^2} B_p. \end{cases} \quad (11)$$

Upper bound for wide-band jamming: In case of a wide-band jammer, the ideal filter is a low-pass filter that is perfectly matched to the bandwidth of the PN sequence. The PN sequence does hence not experience any self-noise. Assuming that the interference is white, we can also express the residual interference after filtering as a function of the bandwidth ratio between jammer and PN sequence as

$$\gamma = \frac{\rho_j(0) + \sigma_n^2}{\frac{B_p}{B_j}\rho_j(0) + \sigma_n^2}, B_j > B_p. \quad (12)$$

Discussion: An interesting observation is that the improvement factor is asymmetric. For illustrative purposes, we plot the bound of the SNR improvement factor versus the bandwidth ratio B_j/B_p in Figure 7. We use $\sigma_n^2 = 0.01$ and the improvement factor is plotted on a logarithmic scale

$$\gamma_{dB} = 10 \log \gamma. \quad (13)$$

For $0.01 < B_p/B_j < 1$, the SNR improvement improvement factor varies almost linearly from 0 dB up to approximately

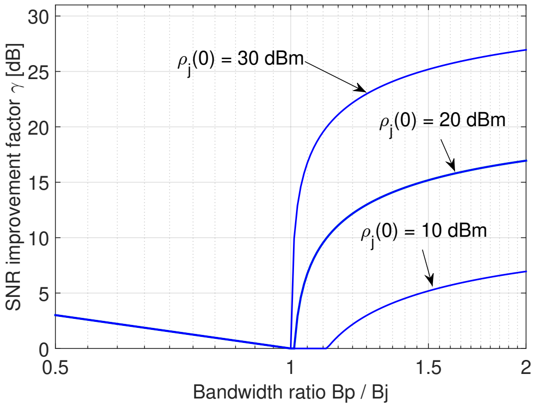

Figure 8: Zoomed version of the upper bound on SNR improvement factor shown in Figure 7.

20 dB according to eq. (12). We can see that for this bandwidth ratio range, the SNR improvement is almost independent of the jamming power and primarily determined by the bandwidth offset. For $B_p/B_j > 1$ and very small bandwidth offsets, the improvement factor remains one because the excision filter is not used as it would degrade the SNR more than without any filtering. For higher bandwidth offsets, the SNR improvement factor quickly converges to a value that is close to the power of the jammer, i.e., 10, 20 and 30 dBm in the Figure. Thus, the improvement is highest for strong jammers with a large bandwidth offset. Yet, a zoomed version is shown in Figure 8 and it indicates that significant gains can be achieved by BHSS for bandwidth ratios between 0.5 and 2.

5.3 Bit Error Performance

The results given above on SNR improvement indicate that significant performance gains can be achieved when the bandwidth of the signal and the bandwidth of the jammer have an offset. The analysis below compares the bit error rate of a BHSS signal against conventional DSSS and FHSS systems for jammers with fixed bandwidths as well as randomly hopping jammers.

In order to compute the bit error rate, we express the output of the demodulator, which is the decision variable for recovering the binary information, as

$$U = \sum_{k=1}^{L} y(k)p(k) \tag{14}$$

and we assume that the decision variable U has a Gaussian distribution. This is equivalent to assuming that the performance of this system is the same as that of QPSK signaling corrupted only by white Gaussian noise with variance equal to the total noise due to white noise, interference, and self-noise at the output of the demodulator. Under these assumptions, the bit error rate is given by

$$P_b = P(U < 0) = \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(U-\mu)^2}{2\sigma^2}} dU \tag{15}$$

where $\sigma^2 = var(U)$ and $\mu = E(U)$ are derived in the Appendix (eq. (19) and (20)). Thus,

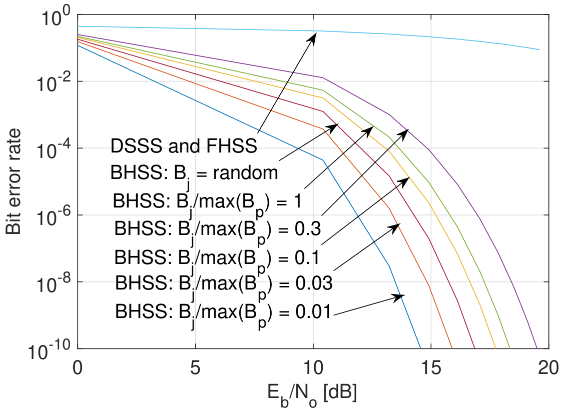

Figure 9: Bit error probability of BHSS compared to DSSS and FHSS. Signal-to-jamming ratio is −20 dB, processing gain is $L = 20$ dB and bandwidth hopping range is 100.

$$P_b = \frac{1}{2}\text{erfc}\Big(\sqrt{\frac{\mu^2}{2\sigma^2}}\Big) = \frac{1}{2}\text{erfc}\Big(\sqrt{\frac{\text{SNR}}{2}}\Big), \tag{16}$$

where the SNR for a bandwidth hopping and a conventional receiver are given in eq. (6) and (7).

In order to compare the performance of a BHSS receiver to the DSSS and FHSS receivers, we plot the bit error rate against the SNR without interference, i.e., the signal-to-white Gaussian noise ratio per bit E_b/N_o, where E_b is the energy per bit and N_0 the single-sided spectral density of the Gaussian noise. Figure 9 illustrates the error rate performance for a BHSS transmitter that hops randomly among a bandwidth range of 100, i.e., $\frac{\max(B_p)}{\min(B_p)} = 100$. For BHSS, DSSS, and FHSS, the signal-to-interference ratio per chip is left constant at −20 dB, the noise is $\sigma_n^2 = 0.01$ and the processing gain is $L = 20$ dB. In the case of DSSS, the jammer bandwidth B_j is matched to the same bandwidth as the spreaded signal. Since we restrict our communication systems to the same available bandwidth, FHSS achieves the same jamming resistance as DSSS by using narrower sub-channels in the frequency band. For BHSS, the jammer cannot match its bandwidth to the signal since the bandwidth is changed faster than the reaction time of the jammer and we therefore consider jamming strategies which employ fixed jamming bandwidths between the minimum and maximum bandwidth used by BHSS, as well as a random bandwidth hopping jammer analogous to the BHSS signal.

As we can see in Figure 9, the bit error rate for the DSSS and FHSS receivers remain close to 0.5 even when E_b/N_o is as high as 15 dB. These receivers are thus not able to suppress the interference despite the inherent processing gain of $L = 20$ dB provided by the signal spreading. In contrast, the BHSS receiver outperforms the DSSS and FHSS receivers and significantly improves the performance for any jammer bandwidth. When the bandwidth of the jammer is fixed, the bit error may drop down to rates well below 10^{-10} depending on the bandwidth of the jammer. When the jammer is

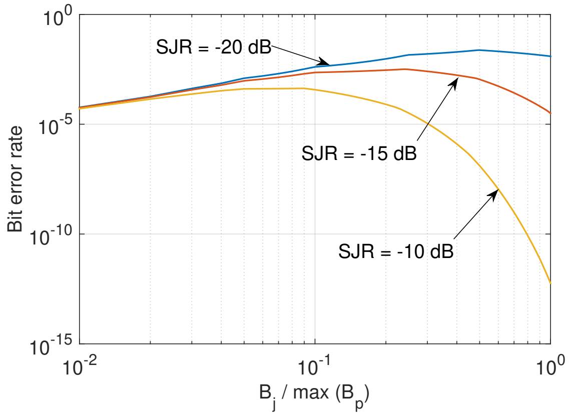

Figure 10: Bit error probability of BHSS versus different jamming bandwidths. Bandwidth hopping range is 100 **and processing gain is** $L = 20$ **dB.**

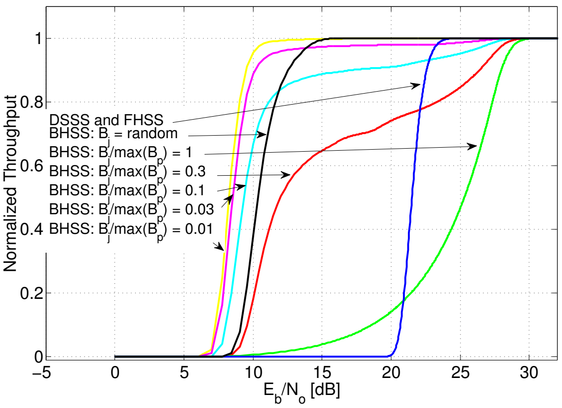

Figure 11: Throughput of BHSS compared to DSSS and FHSS. Signal-to-jamming ratio is -20 **dB and bandwidth hopping range is** 100**.**

also hopping its bandwidth randomly, the bit error rate for $E_b/N_o = 15$ dB drops to about 10^{-7} which is better than when the jammer fixes its bandwidth to values $B_j/\max(B_p) > 0.1$, but worse than for values below 0.1. This suggests that a jammer may be better off by jamming with a fixed bandwidth than by hopping its bandwidth randomly. However, a BHSS system may also respond to jammers of fixed bandwidth by stopping to hop and selecting a bandwidth that achieves the lowest bit error rate given the bandwidth of the jammer. Therefore, a jammer is forced to also employ a random hopping strategy to counterfeit adaptive BHSS systems.

In Figure 10, we further plot the bit error rate of BHSS versus the bandwidth of the jammer B_j for different signal-to-jamming ratios (SJR). The processing gain is again $L = 20$ dB and the bandwidth hopping range of BHSS is 100. As we can see, the bit error curves for the different SJR values all exhibit a maximum at different jammer bandwidths. A jammer will hence maximize the bit error rate by selecting a jamming bandwidth which is matched to the SJR. However, it may be challenging for the jammer to estimate the exact SJR at the receiver, specially when the transmitter or receiver are mobile. When the jammer is not able to estimate the SJR, he may again be better off by randomly hopping across all bandwidths that are used by BHSS.

5.4 Throughput Comparison

The previous results have shown that BHSS outperforms DSSS and FHSS in terms of bit error rate. However, since BHSS sacrifices transmission rate when hopping to smaller bandwidths, an interesting question is whether the overall throughput of BHSS can still be higher or at least equal to DSSS and FHSS despite the hopping to smaller bandwidths for jamming mitigation.

To answer this question, we compare the throughput of all three systems using a packet-based communication model. If P_p is the packet error probability, the throughput can be expressed as

$$T = R(1 - P_p), \tag{17}$$

where R corresponds to the packet transmission data rate in bits per second. In absence of channel coding, a packet is declared incorrect if at least one bit is erroneous. Assuming that the bit errors are i.i.d., from digital communication theory [20], the expectation value of the packet error probability for a data packet length of N bits is then

$$P_p = 1 - (1 - P_b)^N. \tag{18}$$

To compare the throughput in a fair manner, we fix the rate R and the spectral occupancy of each system to identical values. In other words, we compare the throughput of each system for equal capacity with the signal bandwidth of each system computed as previously in Section 5.3. To do so, we use a processing gain and bandwidth hopping range for BHSS of $L_{BHSS} = 20$ dB and $\frac{\max(B_p)}{\min(B_p)} = 100$ respectively, and configure the processing gain of DSSS and FHSS to achieve the same data transmission rate R as BHSS. This configuration results in processing gains for DSSS and FHSS of $L_{DSSS} = L_{FHSS} = 25.4$ dB.

We plot the throughput against E_b/N_o in Figure 11 for packets of size $N = 500$ bytes, a signal-to-jamming ratio of -20 dB and a noise of $\sigma_n^2 = 0.01$. The throughput is normalized to a maximum value of 1. As expected, the throughput of BHSS depends on the jammer bandwidth. We notice that when the jamming bandwidth is relatively small, the throughput quickly improves as E_b/N_o increases. Except for very large values of E_b/N_o, BHSS significantly outperforms DSSS and FHSS in terms of throughput. On the other end, when the jammer bandwidth is relatively large, the throughput does not improve that quickly as E_b/N_o increases. For example, when the jammer bandwidth is $\max(B_p)$, BHSS achieves only a throughput of 0.3 while DSSS and FHSS have already reached the maximum throughput of one. Nevertheless, BHSS can generally be considered as superior in terms of throughput because it is not a good strategy for the jammer to use a fixed bandwidth for his jamming signals, since a BHSS system may also stop hopping when the jammer is not dynamically adapting his bandwidth. As we can see, the throughput of BHSS against random hopping jammers is strictly better for any E_b/N_o. The throughput curves are separated by roughly 12 dB, meaning that a DSSS or FHSS system would need to increase its processing gain by that amount in order to achieve the same jamming resistance as BHSS. In other words, this means that a DSSS or FHSS system requires sixteen times more radio-frequency bandwidth than a BHSS system to achieve the same throughput under jamming.

6. EXPERIMENTAL RESULTS

This section presents experimental results we obtained with a prototype BHSS system implemented on software-defined radios (SDR). The goal of these experimental results is to assess the power advantage of BHSS over classical SS under more realistic system assumptions than in the theoretical analysis from the previous section which assumed an ideal receiver with ideal filters. With real hardware components, the receiver must deal with frequency, timing, phase, and sampling noise which will impact the receiver performance under jamming. In addition, the excision and low-pass filters may no longer entirely remove the undesired frequencies from the jammer without distorting the signal from the transmitter.

6.1 Implementation on SDR

Our implementation relies on the GnuRadio framework for software-defined radios from Ettus Research. We have implemented a BHSS transmitter and receiver for the QPSK modulation. The system relies on a 16-ary DSSS modulation similar to the one used in IEEE 802.15.4 [21]. The DSSS system spreads 4-bit symbols to 32 chips, corresponding to a spreading factor of 8, or a processing gain of 9 dB. In analogy to IEEE 802.15.4 frames, the frame structure we implement is based on a preamble, start of frame delimiter (SFD), data and a cyclic redundancy check (CRC). The preamble and SFD serve for frame, frequency, time, and phase synchronization at the receiver. The CRC is used to check whether frames are correctly received.

We rely for our experiments on the USRP N210 which offers a maximum bandwidth of 50 MHz. However, because of the limited resources of our system setup, the maximum number of samples we are able to process in real-time on the receiver computer is 20 MS/s, limiting the bandwidth of our signals to a maximum of 10 MHz. Our implementation therefore supports a configurable signal bandwidth of $B_p = \frac{10}{n}$ MHz, with $n \geq 1$. All signal bandwidths are sampled at the same, maximum sampling rate R_s of 20 MS/s in order to avoid processing delays when the sampling rate would be switched while hopping.

For the modulation of the chips, we rely on a half-sine pulse shape $g(t)$. The duration of the half-sine pulse shape is changed after a configurable number of symbols. In principle, it would be possible to change the pulse shape after the transmission of each chip. However, sub-symbol bandwidth hopping is not necessary as it is safe to assume that the jammer will need at least a couple of symbols to estimate the signal bandwidth in order to react with the matched jamming signal [12]. For the purpose of our experiments, transmitter and receiver have a pre-shared random bandwidth hopping sequence.

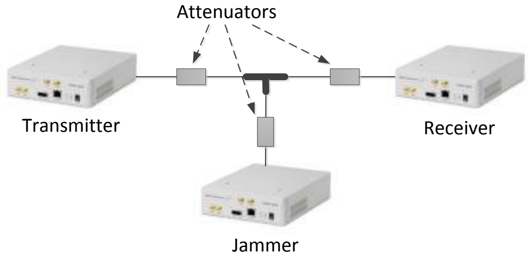

Figure 12: Experimental setup with BHSS transmitter, BHSS receiver and jammer.

The receiver estimates the power spectral density of the interference using an FFT. Upon estimation of the spectral density, a control logic applies an appropriate FIR filter configuration to suppress the jammer prior demodulating the signal. In order to minimize the processing delays, we pre-compute the taps of all possible low-pass filters in advance with the GnuRadio filter design tool. The tabs of the excision filters are set in order to be reciprocal to the square root of the power spectral density of the jammer, as shown in eq. (3). We use the maximum number of taps supported by our receiver hardware resources to process the incoming samples in real-time. This results in a maximum filter order of 3181 for a transition width of 10 kHz and stop-band attenuation of 70 dB.

Real receivers need to be able to tolerate frequency, phase and timing errors which occur due to clock, sampling, and channel noise. The mechanisms to correct these offsets are all implemented after the FIR filter. Otherwise, the jammer may disturb the error correction and the gain of the filter may not be fully exploited. Phase and frequency are corrected with the help of a Costas loop [22] while timing synchronization is achieved with the Gardner timing recovery [23]. After frequency, time and phase correction, the signal is demodulated with a filter matched to the half sine pulse shape currently being employed by the transmitter. After chip demodulation, the receiver then correlates each sequence of 32 chips (a symbol) with the 16 different symbols and selects the one with the highest correlation.

6.2 Experimental Setup

We evaluate experimentally the gain of our implementation with a test setup including a BHSS transmitter, a BHSS receiver and a jammer. All three nodes are running on URSP N210 from Ettus Research which are attached each to a computer running GnuRadio. The jammer emits a constant white Gaussian noise signal with different bandwidths. We generate a white Gaussian noise signal by using a random Gaussian source from GnuRadio and applying a low pass filter on the signal. As we are not interested in any environmental multipath noise on the communication, we connect transmitter, receiver and jammer with SMA coaxial cables, attenuators and T-connector as shown in Figure 12. Despite performing the experiments over coaxial cables, our results

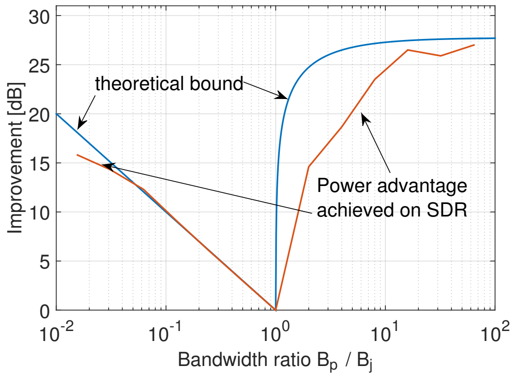

Figure 13: Power advantage achieved with our SDR-based implementation.

are representative of real-world scenarios in which the radios communicate to each other with antennas over line-of-sight because both channels can be modeled as additive white Gaussian noise (AWGN) channels. Another realistic setup of our experiments is that we do not synchronize the clocks of the SDRs and all of them use their own internal oscillator. Different power levels for the transmitter and jammer are produced by adding different attenuators at the cable ends and by varying the transmit gain of the SDRs. In all experiments, we hop between a set of seven pre-defined bandwidths: 10, 5, 2.5, 1.25, 0.625, 0.312, and 0.156 MHz. The bandwidth hopping range is therefore 64. All the results reported in this Section are derived by averaging the performance over 10, 000 transmitted packets for all data points.

6.3 Power Advantage for Fixed Bandwidth Offsets

In order to compare the performance of our SDR-based implementation to the theoretical bound from Section 5.1, we first determine the minimal SNR required to achieve a particular error performance with and without interference filtering for fixed bandwidth offsets between jammer and signal, i.e., when the bandwidth is not hopping. In analogy to the SNR improvement factor in eq. (8), we define the *power advantage* as the ratio of the SNRs to achieve an error performance below 50 percent packet losses without and with filter. A packet loss is defined as a packet for which the CRC does not match the content of the packet. The power advantage is directly comparable to the SNR improvement factor as both indicate how much stronger the power of the signal must be when no interference is suppressed before the despreading operation.

We have measured the power advantage for 49 bandwidth offset constellations between the seven pre-defined signal bandwidths and the same seven bandwidths for the jammer. For all constellations having identical bandwidth ratio, B_p/B_j, we average the power advantage and plot the result in Figure 13. As a reference, we also show the theoretical bound for the SNR improvement factor γ as derived in the Section 5.1. We observe that for offsets $B_p/B_j < 1$, the achieved power advantage as measured with our implementation follows very closely the theoretical bound. In this regime, the bandwidth of the jammer is wide-band and the low-pass filter is active. It shows that the low-pass filter as implemented using the FIR filter is quite optimal at suppressing the frequencies of the jammer without distortion of the original signal. In contrast, for $B_p/B_j > 1$, our implementation is not able to the exploit the full theoretical gain. Specially, for $10 > B_p/B_j > 1$, the implementation sacrifices roughly half of the possibly achievable SNR improvement. This is the result from factors such as the non-ideal excision filters, or the fact that the jammer and the chip sequences are not entirely white given the limited processing gain of 9 dB we have with a spreading factor of 8. Yet, for $B_p/B_j > 10$, we observe significant gains of more than 25 dB as expected.

Bandwidth [MHz]	10	5	2.5	1.25	0.625	0.313	0.156
Linear [%]	14.3	14.3	14.3	14.3	14.3	14.3	14.3
Exponential [%]	50.4	25.2	12.6	6.3	3.1	1.6	0.8
Parabolic [%]	27.1	15.8	6.3	0.1	1.3	22.0	27.4

Table 1: Random distributions for the different hopping patterns.

6.4 Power Advantage with Bandwidth Hopping

Next, we analyze the power advantage of BHSS versus the spread spectrum receiver with fixed bandwidth. To have comparable results, we use for the latter the same code base as BHSS but disable bandwidth hopping. First, we introduce the three different hopping patterns we have implemented for our tests. Then, we evaluate the performance of these hopping patterns for jammers of fixed bandwidth and for jammers that hop according to the same patterns.

6.4.1 Hopping Patterns

We have implemented the following three hopping patterns:

Linear hopping: With this pattern, the transmitter hops according to a uniform random distribution within the set of possible bandwidths. In our experiments with 7 bandwidths from 0.15625 to 10 MHz, this results in an average bandwidth utilization of 2.83 MHz and an average throughput of 354 kb/s.

Exponential hopping: The exponential hopping pattern is chosen such that on average each bandwidth is used for the same amount of time. It compensates for the unequal transmit time of the different bandwidths by drawing randomly from the set of available bandwidths according to an exponential distribution. This results in an average bandwidth of 6.72 MHz and a throughput of 840 kb/s.

Parabolic hopping: In this pattern, we hop randomly between different bandwidths according to a parabolic distribution. The intuition for this strategy is that most jamming power can filtered out when $B_p \ll B_j$ or $B_p \gg B_j$. Thus, using the smallest and largest bandwidths more often is likely to result in good filtering. Using Monte Carlo simulations, we compute a parabolic distribution that provides the maximum minimal power advantage for all possible jammer bandwidths. Maximizing the minimum power advan-

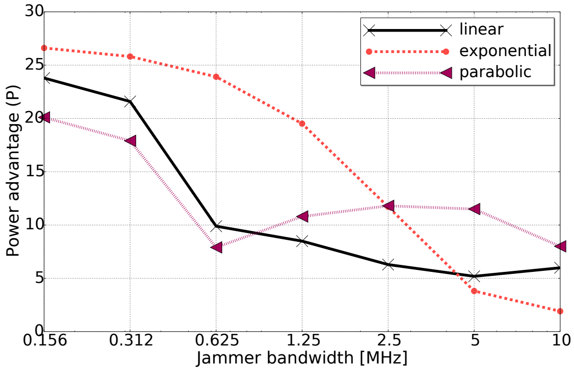

Figure 14: Power advantage versus jamming bandwidth for linear, exponential and parabolic hopping patterns.

tage over all possible bandwidths is the best option against an attacker which matches its bandwidth to the one with lowest power advantage. It results in an average bandwidth of 3.77 MHz and an average throughput of 471 kb/s. The exact distributions of all three strategies are given in Table 1.

6.4.2 *Fixed Jammer Bandwidth*

Figure 14 shows the power advantage of BHSS for the different hopping patterns and jammers of fixed bandwidths. The power advantage is defined for this plot as the ratio of the minimum SNRs to achieve an error performance below 50 percent packet losses for BHSS and the fixed-bandwidth receiver. For the fixed-bandwidth receiver, we use the maximum bandwidth of BHSS, i.e., 10 MHz for the signal and the jammer. The power advantage therefore corresponds to the SNR improvement of BHSS over conventional DSSS for equal RF spectrum requirements. As we can see, BHSS is able to achieve considerable improvements. Depending on the hopping pattern and jamming bandwidth, power advantages between 2 dB and 26 dB are achieved. The empirical results further confirm that the power advantage considerably depends on the bandwidth of the jammer. Interestingly, the jamming bandwidth that minimizes the power advantage of BHSS is different for the different hopping patterns. The minimum power advantage for the linear hopping pattern is at 5 MHz jamming bandwidth, while it is at 0.625 MHz for the parabolic and at 10 MHz for the exponential hopping patterns. In contrast, the highest power advantage is achieved for a jamming bandwidth of 0.156 MHz for all hopping patterns. This can be explained by the bandwidth hopping range of 64 we are using in our experiments. For this limited range, the power advantage for large bandwidth ratios B_p/B_j is larger than for small bandwidth ratios because of the asymmetry of the SNR improvement factor for low-pass and excision filtering (see Figure 13). Narrow-band jammers are therefore on average filtered more effectively than wide-band jammers. By using larger bandwidth hopping ranges, the highest power advantage might be therefore at different jamming bandwidths for different hopping patterns.

Considering this result, a jammer might be tempted to jam using a fixed bandwidth that achieves the lowest power advantage. However, as mentioned earlier, relying on a fixed jamming bandwidth as a jammer might be not be the best strategy as after detection that the jammer is using a fixed bandwidth, the transmitter could also switch to a fixed bandwidth having the largest offset to the jammer and therefore maximizing the power advantage for the receiver. In order to avoid this situation, the jammer should also hop its bandwidth randomly. The performance against bandwidth hopping jammers is the focus of the following sub-section.

		Hopping pattern jammer		
		linear	exponential	parabolic
Hopping pattern signal	linear	9.6	6.5	12.5
	exponential	15.7	3.3	15.2
	parabolic	12.2	11.4	13.7

Table 2: Power advantage in dB for different bandwidth hopping patterns for BHSS and the jammer.

6.4.3 *Bandwidth Hopping Jammer*

In a next step, we analyze the power advantage for random hopping jammers. We consider the same hopping patterns for the jammer as for BHSS. Table 2 summarizes the power advantage for all nine combinations of hopping patterns between signal and jammer. As we observe, the hopping pattern greatly affects the power advantage. The highest power advantage of 15.7 dB is achieved when the signal is hopping according to the exponential pattern and the jammer follows the linear hopping pattern. However, the exponential hopping pattern is worst (3.3 dB) when the jammer is also hopping its bandwidth according to the exponential hopping pattern. From this perspective, BHSS should not rely on this pattern as it is not the most robust one against any of the three types of jammer. The most robust pattern is the parabolic pattern. If the signal follows this pattern, the worst power advantage is 11.4 dB, when the jammer is hopping according to the exponential pattern.

7. RELATED WORK

Spread spectrum communication techniques such as DSSS and FHSS have been around for decades to mitigate the impact of jamming [24]. 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 pseudo-random spreading chip sequence. The receiver then despreads the signal by correlating the received signal with a replica of the pseudo-random sequence. The correlation operation at the receiver reduces the level of the interference by spreading it across the entire frequency band occupied by the pseudo-random sequence. Thus, the interference is rendered equivalent to a lower level noise with a relatively flat spectrum. At the same time, the cross-correlation operation collapses the desired information signal back to the bandwidth occupied by the information signal prior to spreading. This operation has the effect of reducing the amount of interference power to a fraction that is approximately equal to the ratio of the information bandwidth to the spreading bandwidth. In FHSS, the transmitter randomly hops the carrier frequency of the modulated signal. This has the effect of spreading the signal bandwidth over a wider band than actually occupied by the information bandwidth. The jammer interference can then be suppressed at the receiver by bandpass filtering the received signal according to the instantaneous carrier frequency used by the transmitter. Similar to DSSS, the demodulation operation of FHSS has the effect of mitigating the amount of interference power to a fraction that is proportional to the ratio between the hopping band to the actual signal bandwidth. In theory, any level of jamming suppression can be achieved with DSSS or FHSS by using a sufficient processing gain [8, 9]. However, high processing gains require large spreading of the signal bandwidths. Since the RF spectrum is a scarce resource today, achieving jamming resistance using arbitrary large bandwidths is generally not always possible.

Excision filters have been proposed in conjunction to the spread spectrum receivers in order to augment the processing gain without an increase in signal bandwidth [4, 5, 6, 7]. However, excision filters alone are not effective at suppressing interference from jammers since the interference can be matched by the jammer to the bandwidth of the signal which makes excision filtering ineffective. In this work, we also rely on excision filters to suppress narrow-band jammers, however by making use of bandwidth hopping, we are able to improve the processing gain in the presence of intentional interference from jamming.

DeBruhl and Tague [25] proposed using adaptive filters to mitigate the impact of jamming in spread spectrum systems. Their approach targeted however only periodic jammers which are not able to quickly match desired waveforms while sensing the channel. In contrast, BHSS provides improvements against also reactive jammers.

Wireless communication systems have generally been designed to operate at fixed bandwidths. Some more recent systems support adaptive signal bandwidths, but the bandwidths are not switched in the same way. For example in [10], the authors propose SampleWidth, an algorithm that samples the channel conditions and dynamically switches between different bandwidths. Pejovic and Belding proposed WhiteRate in [11], a context-aware approach to wireless rate adaptation. While also adapting the signal width, the goal of SampleWidth and WhiteRate is entirely different from BHSS. These works try to improve the throughput in an non-adversarial setting while BHSS aims at mitigating the impact of adversarial interference. Therefore, our design relies on fast and unpredictable bandwidth hopping patterns providing the protection against an attacker that tries to disturb the communication.

Extensions of DSSS and FHSS have been proposed such as UDSSS [17] and UFH [26]. However, the basic spreading principles of these extensions remain the same, whereas BHSS spreads the signal by hopping it across different bandwidths, a hopping dimension that has been not exploited so far by any other spread spectrum techniques.

Several anti-jamming techniques have been proposed which do not rely on spread spectrum methods. For example, directional antennas [13] offer a higher degree of protection by restricting the direction from which an attacker may emit interference, at the cost of restricting also the direction of the communication. Multiple antenna systems and beamforming can also be used to alleviate this problem [14]. By spacing the multiple antennas at least half of the wavelength from each other, the jammer signal can be isolated from the regular communication and subtracted at the receiver. Unlike multiple antenna systems, BHSS is able to mitigate the impact of adversarial interference using a single antenna.

8. CONCLUSION

Spread spectrum communication inherently provides interference resistance against jamming, however the processing gain is bounded by the spreading factor. Conventional spread spectrum systems therefore require to increase the frequency band occupation of the signal in order to achieve a desirable jamming resistence. In this work, we have proposed bandwidth hopping as a technique to increase the jamming resistence of spread spectrum communications without the need to increase the occupied frequency band of the signal. We have derived a theoretical bound for the SNR and bit error rate improvement of BHSS over conventional DSSS and FHSS. We have designed and implemented transmitter and receiver structures on software-defined radios to hop the bandwidth during the transmission of the signal which allow us to hop the bandwidth fast enough to protect against reactive jamming. Our experimental results on software-defined radios confirm that significant improvements can be achieved on real systems. In our experiments, we were able to achieve power advantages from 8 to 20 dB against fixed-bandwidth jammers for a bandwidth hopping range of 64. When both the signal and the jammers are hopping randomly their bandwidths, we achieved an average power advantage of 11.4 dB for BHSS. These results demonstrate that the processing gain of spread spectrum systems can be improved beyond the spreading factor, even against a strong attacker model such as reactive jamming.

Acknowledgments

We thank our shepherd Shyamnath Gollakota for the constructive feedbacks. This work has been funded in part by the European Commission in the framework of the H2020-ICT-2014-2 project Flex5Gware (Grant agreement no. 671563) and in part by Ministerio de Economía y Competitividad grant TEC2014-55713-R.

9. REFERENCES

[1] R. A. Poisel, *Modern communications jamming principles and techniques*. Artech House Publishers, 2004.

[2] D. L. Adamy, *EW 102: A Second Course in Electronic Warfare*. Artech House, 2004.

[3] F. M. Hsu and A. A. Giordano, "Digital Whitening Techniques for Improving Spread Spectrum Communications Performance in the Presence of Narrow-band Jamming and Interference," *IEEE Transactions on Communications*, vol. 26, February 1978.

[4] M. G. Amin, "Interference Mitigation in Spread Spectrum Communication Systems Using Time-Frequency Distributions," *IEEE Transactions on Signal Processing*, vol. 45, no. 1, January 1997.

[5] M. G. Amin, C. Wang, and A. R. Lindsey, "Optimum Interference Excision in Spread Spectrum Communications Using Open-Loop Adaptive Filters," *IEEE Transactions on Signal Processing*, vol. 47, no. 7, July 1999.

[6] L. B. Milstein and R. A. Iltis, "Signal Processing for Interference Rejection in Spread Spectrum Communications," *IEEE ASSP Magazine*, April 1986.

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

[8] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2004.

[9] J. Proakis, *Digital Communications*, 3rd ed. McGraw Hill, 2001.

[10] R. Chandra, R. Mahajan, T. Moscibroda, R. Raghavendra, and P. Bahl, "A case for adapting channel width in wireless networks," in *ACM SIGCOMM '08*, 2008, pp. 135–146.

[11] V. Pejovic and E. M. Belding, "Whiterate: A context-aware approach to wireless rate adaptation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 4, April 2014.

[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] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. E. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[14] T. D. Vo-Huu, E.-O. Blass, and G. Noubir, "Counter-jamming using mixed mechanical and software interference cancellation," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '13, New York, NY, USA, 2013, pp. 31–42.

[15] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *ACM SIGCOMM*, August 2013.

[16] M. K. Simon, K. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 2002.

[17] C. Pöpper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, 2010.

[18] M. S. Batlett, "Smoothing Periodograms from Time-Series with Continuous Spectra," *Nature*, vol. 161, May 1948.

[19] P. D. Welch, "The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms," *IEEE Transactions on Audio and Electroacoustics*, vol. 15, no. 2, June 1967.

[20] J. Proakis and M. Salehi, *Digital Communications*, ser. McGraw-Hill higher education. McGraw-Hill Education, 2007. [Online]. Available: http://books.google.ch/books?id=HroiQAAACAAJ

[21] "IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.

[22] K. Mueller and M. Muller, "Timing recovery in digital synchronous data receivers," *Communications, IEEE Transactions on*, vol. 24, no. 5, pp. 516–531, May 1976.

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

[24] R. L. Pickholtz, D. L. Schilling, Laurence, B. Milstein, and S. Member, "Theory of spread spectrum communications: a tutorial," *IEEE Transactions on Communications*, vol. 30, pp. 855–884, 1982.

[25] 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.

[26] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated fhss anti-jamming communication," in *Proceedings of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '09, 2009, pp. 207–218.

Appendix

In order to demonstrate the effectiveness of the narrow-band and wide-band interference suppression techniques, we shall compare the performance of the receiver with and without the suppression filters for different jamming-signal bandwidth offsets. The received signal $r(k)$ is first fed as input to the filter and the output is

$$\begin{aligned} y(k) &= \sum_{l=0}^{K-1} h(l) r(k-l), k = 1, 2, \ldots \\ &= \sum_{l=0}^{K-1} h(l)[p(k-l) + j(k-l) + n(k-l)]. \end{aligned}$$

The signal is then fed to the PN correlator. The output of the PN correlator, which is the decision variable for recovering the binary information, is expressed as

$$U = \sum_{k=1}^{L} y(k) p(k)$$

where L represents the number of chips per information bit (also referred to as symbol) or the processing gain. To determine the SNR, we must compute the mean and variance of U [7]. We assume that the PN sequence $p(k)$ is white, the interference $j(k)$ has zero mean and autocorrelation function $\rho_j(k)$, and the additive noise $n(k)$ is white with variance σ_n^2. Then, the mean of U is

$$E(U) = L \tag{19}$$

and the variance is

$$\begin{aligned} \text{var}(U) &= L \sum_{l=1}^{K-1} h^2(l) + L \sum_{l=0}^{K-1} \sum_{m=0}^{K-1} h(l) h(m) \rho_j(l-m) \\ &+ L\sigma_n^2 \sum_{l=0}^{K-1} h^2(l). \end{aligned} \tag{20}$$

The first term on the right-hand side of the expression for the variance represents the mean square value of the self-noise due to the time dispersion introduced by the interference suppression filter. The second term is the mean square value of the residual interference. The last term is the mean square value of the wide-band noise.

The SNR at the output of the correlator is defined as the ratio of the square of the mean to the variance [7], and it is then computed as:

$$\text{SNR} = \frac{L}{\sum_{l=1}^{K-1} h^2(l) + \sum_{l=0}^{K-1} \sum_{m=0}^{K-1} h(l) h(m) \rho_j(l-m) + \sigma_n^2 \sum_{l=0}^{K-1} h^2(l)}.$$