Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 3, Number: 1, Pages: 15 - 19, Year: 2025

Systematic Study of Anti-Jamming Strategies Using Direct Sequence Spread Spectrum

Rizwan Ali, Muhammad Farooq, and Malaika Basit *

Electrical Engineering Department, Government College University, Lahore, 54000, Pakistan
Corresponding author: Maliaka Basit

Received: 10/03/2025, Revised: 12/05/2025, Accepted: 10/06/2025

***Abstract*—Interference has always been a problem for wireless communication, but deliberate jamming is a distinct kind of issue. In contrast to random noise, a jammer is something that intentionally works against you. In fact, if the system is not designed to manage it, even a low-power jammer can entirely shut down a link. This is precisely the reason Direct Sequence Spread Spectrum (DSSS) was created. The basic concept is straightforward, spread the signal over a much larger bandwidth to eliminate any narrowband interference and prevent serious harm. This study examines how DSSS accomplishes the strategies used to control bit errors even in difficult channel conditions, as well as the design choices that go into building a strong anti-jamming system around it. Different types of spread spectrum are studied, as well as processing gain, error correction coding, interleaving, and adaptive techniques that change the system's behavior based on what the channel is doing at that specific moment.**

***Index Terms*—Spread spectrum, DSSS, FHSS, processing gain.**

I. Introduction

Interference is a primary challenge in wireless communication. A person can easily understand the impact of interference on effective communication if they have ever tried to make a phone call in a crowded environment where several people are speaking at once. Suppose that the interference is intentional and someone is attempting to interfere with your transmission. It will impact the reliability of data transmission. Anti-jamming communication solutions are made to deal with such a fundamental situation [1-3].

A. Problem Statement

A jammer does not have to be very complicated to cause problems. The receiver's ability to make accurate bit judgments can be destroyed by a narrowband continuous transmitter and leads to a degraded signal quality. The power difference involved in this threat makes it extremely difficult to deal with the jammer may often achieve this with considerably less transmitted power than the designated system [4].

Spread spectrum techniques were first developed in the military to address such challenges, and DSSS in particular made its way into civilian uses as well, with GPS, Wi-Fi, and mobile networks. Due its robustness it became one of the most commonly utilized systems [5-8].

B. Objective

The main objectives of this study are to analyze DSSS as an anti-jamming technique, comprehend the working principle of DSSS in interference suppression, evaluate system's performance metric such as bit error rate BER, apprehend the supporting techniques like channel coding and interleaving and ascertain limitations, research gaps and improvements in DSSS-based systems.

II. Fundamentals of Spread Spectrum

Spread spectrum (SS) is a robust, high-gain and secure technology used in many applications.

A. Basic Principle

Spread spectrum purposefully makes the signal far wider than it has to be. This spread is especially accomplished in DSSS by multiplying the data signal by a high-rate pseudo-random sequence known as the spreading code, or PN sequence. Each bit of data, which has some duration Tb, gets divided into a much larger number of shorter intervals called chips, each of duration Tc. The ratio of these two rates chip rate to bit rate is the processing gain,

$$P_G = \frac{R_c}{R_b} = \frac{T_b}{T_c} \qquad (1)$$

Where P_G is the processing gain, R_c is the chip rate and R_b is the bit rate. For example, a processing gain of 10 says that the sent signal uses ten times as much bandwidth as the data rate would need. Although it may seem inefficient, that is precisely what makes DSSS strong. The desired data is sent coherently when the receiver correlates the incoming signal with the same PN sequence, whereas any narrowband interference spreads over the entire chip bandwidth and its power per unit bandwidth decreases by the same factor of processing gain (PG).

B. Jamming Margin

The jamming margin, which indicates how much stronger a

jammer may be than the intended signal before it begins to cause serious issues, is also closely related with processing gain.

$$J_m(dB) = P_G(dB) - \left[\frac{E_b}{N_o}(dB) - ImpLoss\ (dB)\right] \quad (2)$$

At P_G = 10 (dB) and a needed $\frac{E_b}{N_o}$ of 7 dB with minimum implementation loss, the system can tolerate a jammer that is approximately 3 dB above the signal. The bandwidth increases along with the jamming margin when the processing gain is increased as shown in Fig. 1. This is the primary trade-off that all DSSS designers must consider.

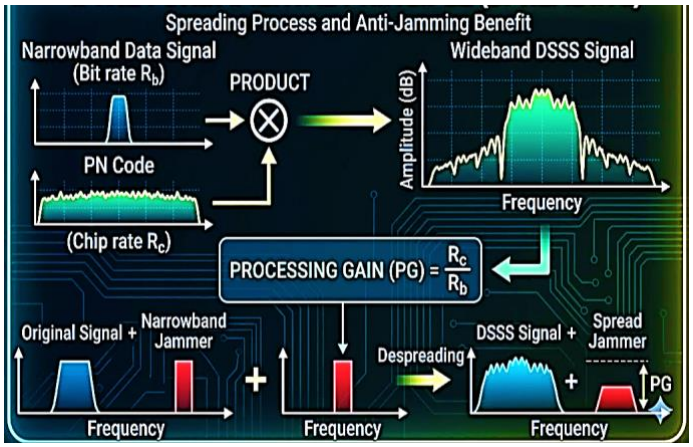

Figure 1: Overview of the fundamental technique of spreading of Signal

III. Spread Spectrum Variants

There are other ways to deploy spread spectrum besides DSSS, and learning about its alternatives helps identify DSSS's advantages and disadvantages.

A. *Direct Sequence Spread Spectrum (DSSS)*

DSSS works in the time domain. The data stream is directly multiplied by a PN code at chip rate to create a wideband baseband signal before any frequency up-conversion. The receiver recovers the signal with a correlator, which is typically an integrate-and-dump circuit that accumulates the product of the received chips and the local PN replica over one bit interval. A jammer without the PN sequence cannot take advantage of the correlator and sees its power spreading rather than centered because it is deterministic and only known to the targeted receiver.

DSSS works well in situations where narrowband interference is the primary threat and continuous transmission is necessary. Its main disadvantage is that the processing gain is set at design time unless an adaptive mechanism is added.

Figure 2:The Time Domain View of Spreading.

B. *Frequency Hopping Spread Spectrum (FHSS)*

In frequency hopping, the carrier frequency changes rapidly in along with a pseudo random hopping sequence. However, the signal only occupies a narrow frequency at any given time, it moves through a wide spectrum throughout time. If the hop rate is higher than the jammer's reaction time, a follower jammer which detects the frequency and tries to jam it is defeated. A jammer that fixes itself at a single frequency will only interfere with a small percentage of the hops. Military UHF radios and Bluetooth both use FHSS, although it is less effective against broadband noise jamming, it is especially effective against swept or fixed narrowband jammers.

C. *Hybrid FH/DSSS*

Some systems use both strategies. The signal spreads with a PN code at each frequency hop. This layered approach makes it more difficult to jam the system from multiple angles at the same time, hopping defeats follower jammers, while direct sequence spreading handles narrowband interference at each hop frequency. The cost is higher hardware complexity for both the transmitter and the receiver.

D. *Code Division Multiple Access (CDMA)*

In multi-user systems, CDMA is a direct application of DSSS. Every user on the network is given a unique spreading code, usually a Gold code, and they all use the same frequency band to transmit at the same time. While signals from other users show up as low-level noise at the receiver, correlation with a particular user's code extracts that user's data. This structure enables flexible capacity allocation and provides CDMA with inherent resistance to narrowband interference. This is the foundation of both IS-95 and WCDMA (3G) shown in Table I.

TABLE I
SCADA Applications by Industry

Technique	Spreading Method	Main Strength	Typical Use
DSSS	Time-domain PN multiply	Narrowband jam suppression	GPS, 802.11b, CDMA
FHSS	Frequency hopping	Follower jam avoidance	Bluetooth, military UHF
FH/DSSS	Both combined	Multi-threat resistance	Military secure links
CDMA	Orthogonal PN codes	Multi-user capacity	IS-95, WCDMA

IV. Significance of PC

The core of any DSSS system is the spreading code. It establishes whether the receiver can consistently recover the data, how well the signal is concealed, and how successfully interference is rejected. Selecting the appropriate type of code is more important than it might appear at first.

A. Efficient Spreading Code

A propagating code requires two characteristics. It must first have a sharp autocorrelation peak, meaning the sequence's correlation with itself yields a high value at zero delay, but the result abruptly declines at any other delay. This makes it possible for the receiver to neatly de-spread the signal. Second, in order to prevent signals from merging into one another when numerous codes are utilized in the same system, they must have low cross-correlation.

Neither of these characteristics is guaranteed by a truly random sequence. Poor cross-correlation may exist between two distinct realizations of a random sequence. More significantly, the receiver cannot recreate an unknown random sequence without communicating it separately, which defeats the objective. A deterministic sequence that appears random but is produced from a compact description is required.

B. Maximum Length Sequence

A maximal-length sequence of period $L = 2^m - 1$ is produced by a Linear Feedback Shift Register of degree m with a basic feedback polynomial over GF(2). The processing gain defines the minimum register length required to cover each information bit for at least one complete period:

$$L_{PN} = 2^m - 1 \ , m = log_2 (P_G + 1) \quad (3)$$

This results in $m = 4$ and a series of period 15 chips for $P_G = 10$. An m-sequence's autocorrelation, which equals L_{PN} at zero shift and −1 at all other shifts, is as near to perfect as a binary sequence can go. Compared to storing and replaying a lengthy random sequence, the generator's hardware just needs m flip-flops and a few XOR gates.

C. Gold Codes for Systems with Multiple Users

Because distinct cyclic shifts of the same sequence do not have bounded cross-correlation, m-sequences from a single generator are insufficient when several simultaneous users are required. This is resolved with gold codes. They are created by XOR-ing two identical-length m-sequences derived from a chosen pair of primal polynomials. One favored pair can produce a set of $2^m + 1$ Gold codes, with a maximum cross-correlation magnitude of $2^{\left(\frac{m+2}{2}\right)} + 1$. CDMA functions because of this restricted cross-correlation, which allows each user's receiver to reject codes from other users with a known worst-case interference level as opposed to an unpredictable one.

V. DSSS Anti-Jamming Techniques

The SCADA landscape is undergoing a significant transformation driven by emerging technologies. These innovations promise to enhance capabilities while introducing new considerations for implementation.

A. Spreading as Primary Defense

The anti-jamming method is fundamentally the act of spreading. When a narrowband jammer transmits interference at some frequency within the chip bandwidth, the de-spreading correlator treats it the same way it treats any signal that does not match the PN sequence, it spreads it. The jammer's energy, which was previously concentrated in a small region, now dispersed across the entire chip bandwidth. Its effective power has decreased by a factor of PG by the time it gets to the bit choice point. That is a tenfold reduction at a processing gain of 10 dB.

B. Adaptive Processing Gain

A fixed processing gain represents a kind of compromise on bandwidth. An adaptive PG controller is used to address this. The idea is simple if the BER exceeds a certain threshold, the system increases the PG to improve jamming protection and If the BER is already very low, it lowers the PG to save bandwidth. In order to prevent the system from oscillating back and forth when the BER is close to the boundary, a tiny gap (hysteresis band) is maintained between these limits.

In real life, this can result in considerable bandwidth savings. In a quiet channel, a system that sets PG to 10 to handle a worst-case jammer will consume ten times more bandwidth than is required. When conditions are favorable, an adaptive system can reduce its PG to 2 or less, resulting in a fivefold reduction in bandwidth. This is especially useful in congested spectrum environments where unused bandwidth can be assigned to other users.

C. RAKE Receivers

In real wireless channels, signals need to pass through multiple pathways before they reach the receiver due to reflections from various surfaces each having slightly different delay, and these multipath components become resolvable at high chip rates when they arrive more than one chip period apart. A RAKE receiver takes advantage of this by operating a bank of correlators, each of which is locked to a different multipath delay. The outputs are then combined, either by selecting the strongest (selection combining) or by weighting them based on their signal strength (maximal ratio combining). The RAKE receiver treats multipath as extra energy to gather rather than as a source of interference. The wideband signal makes multipath components resolvable, and the RAKE receiver converts that into a diversity gain, which is one of the reasons DSSS was appealing for WCDMA

VI. Interleaving and Coding

Bit mistakes will still happen even with a well-thought-out DSSS spreading strategy. A jammer with sufficient strength or bandwidth will occasionally produce decision errors that the correlator is unable to stop on its own, and thermal noise is inevitable. This is where channel coding and interleaving come into action. They don't prevent faults from occurring, but they do provide the system with the means to identify and correct them later.

A. BCH Forward Error Correction

Cyclic block codes based on Galois field algebra are known as BCH codes. The parameters for a code with polynomial degree m and error correcting capability t are derived directly from the algebraic structure:

$N = 2^m - 1$ (length of code word)

$K = N - m \cdot t$ (bits of information per code word)

$R = \frac{K}{N}$ (Code Rate)

This results in BCH (15, 11), a code word of 15 bits with 11 information bits that solves one error per word at a code rate of 0.733 when m = 4 and t = 1. The Berlekamp-Massey method is used by the BCH decoder to identify received error bits and flip those bits. BCH is appealing for this application because it grows cleanly: moving to t = 2 offers BCH (15, 7) with stronger security, and moving to t = 3 gets BCH (15, 5) all from the same underlying structure, without changing the codec. The noise model at the channel level is impacted by the BCH coding rate. The effective SNR per information bit must be modified thus adding redundancy in the transmission of information bit:

$$SNR_{Adj} = \frac{E_b}{N_0} + 10log_{10}(R) \quad (4)$$

With R = 0.733 and Eb/N0 = 7 dB, the channel's adapted SNR is about 5.65 dB. If this change is left out into the noise model, the system's calibration will be unreliable.

B. Scrambling Convolution

After BCH encoding, extended sequences of identical bits are still possible, which causes two issues. They first produce spectral lines in the broadcast signal, which can facilitate the signal's detection. Secondly, is the synchronization problem. By XOR-ing the bit stream with the output of a LFSR, a convolutional scrambler eliminates this. The receiver's descrambler uses the same polynomial and initial state to reverse the operation, making the bit pattern pseudo-random without adding any redundancy.

C. Matrix Interleaving

BCH and other block codes are made to deal with isolated faults. When a powerful interferer briefly disrupts the channel it causes burst mistakes. Even if the rest of the message is clean, a single burst could overload the BCH decoder and erase an entire code word. The common solution is interleaving. Before being sent, bits are read out row by row and written into a matrix column by column. The inverse procedure rearranges them at the receiver. As a result, after de-interleaving, a burst of successive channel faults that occur in a succession spreads over numerous code words. The anticipated worst-case burst length is used to determine the inter-leaver's depth:

$$D = 4 \times expected\_burst\_length \quad (5)$$

For example, a depth of D = 20 means that after de-interleaving, a burst of up to 20 adjacent bit errors maps for just one error per code word. This is exactly the situation for which BCH (15, 11) was developed.

D. Soft decision Decoding

Hard-decision decoding discards important information when the receiver commits to a 0 or 1 before sending the bit to the decoder. While Soft-decision decoding allows the decoder to weigh uncertain bits differently from confident ones after receiving the reliability information. According to coding theory, this usually results in an extra 2 dB of coding gain over hard-decision decoding for the same code.

VII. System Performance

A. BER In Jamming

The performance of bit error rate as a function of SNR under jamming conditions is the most common indicator of anti-jamming efficiency. The theoretical BER in AWGN for un-spread BPSK is:

$$BER = Q(\sqrt{(2 \cdot Eb/No)}) \quad (6)$$

The BER curve shifts to the right when a narrowband jammer with jammer-to-signal ratio JSR is added because the effective noise at the receiver increases by JSR. The jammer's contribution at the correlator output is decreased by PG for DSSS with PG and the BER curve has an effective shift of only (JSR - PG) dB. The jammer has little effect on the BER curve when PG is higher than JSR in decibels; the system functions nearly as if there were no jamming.

In a system with PG = 10 and Eb/N0 = 7 dB, even with a jammer of identical power to the signal, the BER remains near 0.002% – a few errors occur over two hundred thousand bits. At the same power level, the same jammer causes un-spread BPSK to have error rates with respect to various percent, which is far beyond the point where any practical error correction can recover the data.

B. Bandwidth Compromise and Shannon Capacity

Expanding the signal doesn't increase capacity as $C = B \cdot \log_2(1 + SNR)$ according to Shannon's channel capacity theorem. The product remains constant because the SNR per unit bandwidth decreases by the same factor when spreading increases, the bandwidth by PG:

$C\_DSSS = (PG \cdot B) \cdot \log_2(1 + SNR/PG) \approx C\_BPSK$ for large PG

In reality, DSSS exchanges durability for bandwidth. It is much more difficult to interfere with narrowband interference because the same information propagates over a much wider channel.

Table II. BER performance comparison across operating conditions (Eb/N0 = 7 dB, PG = 10).

Scenario	Eb/N0 (dB)	BER	Observation
DSSS, PG=10, with jammer	7	0.002%	Near error-free; full PG suppression
DSSS, PG=10, no jammer	7	< 0.001%	Baseline — AWGN only
Unspread BPSK, with jammer	7	5–40%	Catastrophic; no spreading protection
Adaptive PG, high SNR	15+	< 0.001%	Converged to PG=2; bandwidth saved

VIII. Research Gaps

Despite the the robustness of the DSSS systems there are several research gaps which includes the limitation of adaptive PG in practical applications, there vulnerability to jammers and intelligent systems that can learn the system behavior, high spreading factor leads to inefficient bandwidth utilization, synchronization complexity especially for dynamic environment and lack of security that makes them open to spoofing attacks

IX. Conclusion

Anti-jamming communication is fundamentally about making it more difficult for an attacker to interrupt your connection than it is beneficial for them to attempt. DSSS is a long-lasting technology because it deals with this issue from various angles at once.

The hard work is done by the spreading itself, which reduces narrowband interference by the processing gain factor and changes a targeted attack into background noise. In addition to spreading, interleaving splits burst errors into distinct variations that the code can manage, scrambling maintains a clean visual appearance, and BCH coding corrects any remaining errors that manage to pass through.

Adaptive processing gain organizes these elements into something that responds to what the channel is doing rather than being optimized for a fixed worst scenario. Additionally, strategies like power control and RAKE combining expand the system's adaptability into multipath and multi-user scenarios that are not controlled by the simple single-link model.

X. Future Directions

A. Where DSSS Has Been Used

GPS is the most obvious example of DSSS in daily life. The L1 C/A code is a 1.023 Mcps Gold code that allows GPS receivers to function even when signal levels are extremely low, the signal arriving from a satellite after traveling tens of thousands of kilometers is weaker than the receiver's thermal noise floor, but the correlator accurately pulls it out. The same spreading mechanism that eliminates noise also provides the precise timing required for positioning. DSSS was introduced to mobile telephony by IS-95 and the next generation. Every voice call shared the same frequency band at the same time and utilized a unique spreading code. CDMA's natural interference rejection allowed more users to coexist per unit of spectrum than previous frequency division schemes. IEEE 802.11b Wi-Fi used an 11-chip Barker sequence for spreading, allowing early Wi-Fi networks to effectively reject interference in crowded 2.4 GHz environments.

B. Improvements and Future of Technology

Development of adaptive DSSS system that adjust the PG dynamically based on channel conditions, jammer detection by integration of machine learning algorithms are the major improvements. One of the interesting trend is to make a hybrid of DSSS and FHSS for enhancing the anti-jamming performance. A use of cryptographically secured spreading code to prevent unauthorized access. Implementation of cognitive radio techniques for improved efficiency.

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, R.A.,M.F., and M.B.; methodology, R.A., M.F.; software, R.A., M.F., and M.B.; validation, M.B., R.A., M.F.; writing—original draft preparation, R.A.; writing—review and editing, M.F. and M.B.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

References

[1] J. G. Proakis and M. Salehi, Digital Communications, 5th ed. New York: McGraw-Hill, 2008.

[2] R. E. Ziemer and R. L. Peterson, Introduction to Spread-Spectrum Communications. Prentice Hall, 1995.

[3] A. J. Viterbi, CDMA: Principles of Spread Spectrum Communication. Addison-Wesley, 1995.

[4] R. C. Dixon, Spread Spectrum Systems with Commercial Applications, 3rd ed. Wiley, 1994.

[5] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications Handbook, rev. ed. McGraw-Hill, 1994.

[6] S. B. Wicker, Error Control Systems for Digital Communication and Storage. Prentice Hall, 1995.

[7] B. Sklar, Digital Communications: Fundamentals and Applications, 2nd ed. Prentice Hall, 2001.

[8] D. Torrieri, Principles of Spread-Spectrum Communication Systems, 4th ed. Springer, 2018.