

# Spread spectrum

From Wikipedia, the free encyclopedia

In telecommunication and radio communication, **spread-spectrum** techniques are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g., in satellite down links).

## Contents

- 1 Spread-spectrum telecommunications
- 2 Invention of frequency hopping
- 3 Spread-spectrum clock signal generation
- 4 See also
- 5 Notes
- 6 Sources
- 7 External links

## Spread-spectrum telecommunications

This is a technique in which a telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information. Frequency hopping is a basic modulation technique used in spread spectrum signal transmission.

Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called low probability of intercept (LPI) or low probability of detection (LPD). Although spread spectrum methods have been used for many years to establish LPD communication, the fundamental limits of covert communications were only recently studied<sup>[1]</sup> and extended for many scenarios, such as artificial noise generation.<sup>[2]</sup>

Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum. Each of these techniques employs pseudorandom number sequences—created using pseudorandom

number generators—to determine *and* control the spreading pattern of the signal across the allocated bandwidth. Wireless standard IEEE 802.11 uses either FHSS or DSSS in its radio interface.

- Techniques known since the 1940s and used in military communication systems since the 1950s "spread" a radio signal over a wide frequency range several magnitudes higher than minimum requirement. The core principle of spread spectrum is the use of noise-like carrier waves, and, as the name implies, bandwidths much wider than that required for simple point-to-point communication at the same data rate.
- Resistance to jamming (interference). DS (direct sequence) is good at resisting continuous-time narrowband jamming, while FH (frequency hopping) is better at resisting pulse jamming. In DS systems, narrowband jamming affects detection performance about as much as if the amount of jamming power is spread over the whole signal bandwidth, when it will often not be much stronger than background noise. By contrast, in narrowband systems where the signal bandwidth is low, the received signal quality will be severely lowered if the jamming power happens to be concentrated on the signal bandwidth.
- Resistance to eavesdropping. The spreading code (in DS systems) or the frequency-hopping pattern (in FH systems) is often unknown by anyone for whom the signal is unintended, in which case it obscures the signal and reduces the chance of an adversary's making sense of it. Moreover, for a given noise power spectral density (PSD), spread-spectrum systems require the same amount of energy per bit before spreading as narrowband systems and therefore the same amount of power if the bitrate before spreading is the same, but since the signal power is spread over a large bandwidth, the signal PSD is much lower — often significantly lower than the noise PSD — so that the adversary may be unable to determine whether the signal exists at all. However, for mission-critical applications, particularly those employing commercially available radios, spread-spectrum radios do not intrinsically provide adequate security; "...just using spread-spectrum radio itself is not sufficient for communications security".<sup>[3]</sup>
- Resistance to fading. The high bandwidth occupied by spread-spectrum signals offer some frequency diversity, i.e. it is unlikely that the signal will encounter severe multipath fading over its whole bandwidth, and in other cases the signal can be detected using e.g. a Rake receiver.
- Multiple access capability, known as code-division multiple access (CDMA) or code-division multiplexing (CDM). Multiple users can transmit simultaneously in the same frequency band as long as they use different  $k$  codes

## Invention of frequency hopping

Frequency-hopping may date back to radio pioneer Jonathan Zenneck's 1908 German book *Wireless Telegraphy* although he states that Telefunken was using it previously. It saw limited use by the German military in World War I,<sup>[4]</sup> was put forward by Polish engineer Leonard Danilewicz in 1929,<sup>[5]</sup> showed up in a patent in the 1930s by Willem Broertjes (U.S. Patent 1,869,659 (<https://www.google.com/patents/US1869659>), issued Aug. 2, 1932),<sup>[6]</sup> and in the top-secret US Army Signal Corps World War II communications system named SIGSALY.

During World War II, Golden Age of Hollywood actress Hedy Lamarr and avant-garde composer George Antheil developed an intended jamming-resistant radio guidance system for use in Allied torpedoes, patenting the device under US Patent 2,292,387 (<http://www.google.com/patents?vid=USPAT2292387>) on August 11, 1942. Their approach was unique in that frequency coordination was done with paper player piano rolls - a novel approach which was never put into practice.<sup>[7]</sup>

## Spread-spectrum clock signal generation

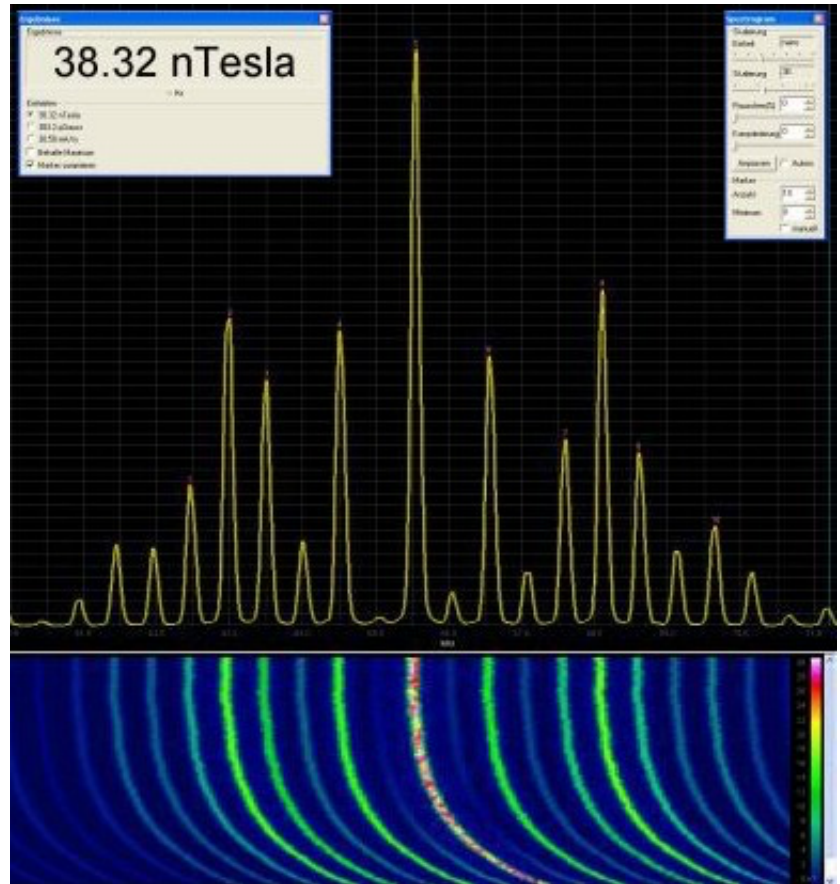
Spread-spectrum clock generation (SSCG) is used in some synchronous digital systems, especially those containing microprocessors, to reduce the spectral density of the electromagnetic interference (EMI) that these systems generate. A synchronous digital system is one that is driven by a clock signal and, because of its periodic nature, has an unavoidably narrow frequency spectrum. In fact, a perfect clock signal would have all its energy concentrated at a single frequency (the desired clock frequency) and its harmonics. Practical synchronous digital systems radiate electromagnetic energy on a number of narrow bands spread on the clock frequency and its harmonics, resulting in a frequency spectrum that, at certain frequencies, can exceed the regulatory limits for electromagnetic interference (e.g. those of the FCC in the United States, JEITA in Japan and the IEC in Europe).

Spread-spectrum clocking avoids this problem by using one of the methods previously described to reduce the peak radiated energy and, therefore, its electromagnetic emissions and so comply with electromagnetic compatibility (EMC) regulations.

It has become a popular technique to gain regulatory approval because it requires only simple equipment modification. It is even more popular in portable electronics devices because of faster clock speeds and increasing integration of high-resolution LCD displays into ever smaller devices. Since these devices are designed to be lightweight and inexpensive, traditional passive, electronic measures to reduce EMI, such as capacitors or metal shielding, are not viable. Active EMI reduction techniques such as spread-spectrum clocking are needed in these cases.

However, spread-spectrum clocking, like other kinds of dynamic frequency change, can also create challenges for designers. Principal among these is clock/data misalignment, or clock skew.

Note that this method does not reduce total radiated energy, and therefore systems are not necessarily less likely to cause interference. Spreading energy over a larger bandwidth effectively reduces electrical and magnetic readings within narrow bandwidths. Typical measuring receivers used by EMC testing laboratories divide the electromagnetic spectrum into frequency bands approximately 120 kHz wide.<sup>[8]</sup> If the system under test were to radiate all its energy in a narrow bandwidth, it would register a large peak. Distributing this same energy into a larger bandwidth prevents systems from putting enough energy into any one narrowband to exceed the statutory



Spread spectrum of a modern switching power supply (heating up period) incl. waterfall diagram over a few minutes. Recorded with a NF-5030 EMC-Analyzer

limits. The usefulness of this method as a means to reduce real-life interference problems is often debated, since it is perceived that spread-spectrum clocking hides rather than resolves higher radiated energy issues by simple exploitation of loopholes in EMC legislation or certification procedures. This situation results in electronic equipment sensitive to narrow bandwidth(s) experiencing much less interference, while those with broadband sensitivity, or even operated at other higher frequencies (such as a radio receiver tuned to a different station), will experience more interference.


FCC certification testing is often completed with the spread-spectrum function enabled in order to reduce the measured emissions to within acceptable legal limits. However, the spread-spectrum functionality may be disabled by the user in some cases. As an example, in the area of personal computers, some BIOS writers include the ability to disable spread-spectrum clock generation as a user setting, thereby defeating the object of the EMI regulations. This might be considered a loophole, but is generally overlooked as long as spread-spectrum is enabled by default.


An ability to disable spread-spectrum clocking in computer systems is considered useful for overclocking, as spread spectrum can lower maximum clock speed achievable due to clock skew.

## See also


- Defeat device
- Direct-sequence spread spectrum
- Electromagnetic compatibility (EMC)
- Electromagnetic interference (EMI)
- Frequency allocation
- Frequency-hopping spread spectrum
- George Antheil
- HAVE QUICK military frequency-hopping UHF radio voice communication system
- Hedy Lamarr
- Open spectrum
- Orthogonal variable spreading factor (OVSF)
- Process gain
- Spread-spectrum time-domain reflectometry
- Time-hopping spread spectrum
- Ultra-wideband

## Notes

1. Bash, Boulat A.; Goeckel, Dennis; Towsley, Don (September 2013). "Limits of Reliable Communication with Low Probability of Detection on AWGN Channels". *IEEE Journal on Selected Areas in Communications*. **31** (9): 1921–1930. arXiv:1202.6423 (<https://arxiv.org/abs/1202.6423>). doi:10.1109/JSAC.2013.130923 (<https://doi.org/10.1109%2FJSAC.2013.130923>). ISSN 0733-8716 (<https://www.worldcat.org/issn/0733-8716>).
2. Soltani, Ramin; Bash, Boulat; Goeckel, Dennis; Guha, Saikat; Towsley, Don (September 2014). "Covert single-hop communication in a wireless network with distributed artificial noise generation". *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. pp. 1078–1085.

- arXiv:1610.00384 (<https://arxiv.org/abs/1610.00384>). doi:10.1109/ALLERTON.2014.7028575 (<https://doi.org/10.1109%2FALLERTON.2014.7028575>). ISBN 978-1-4799-8009-3.
3. Shaw, William T. (2006). *Cyber Security for SCADA Systems*. PennWell Books. p. 76. ISBN 9781593700683.
  4. Denis Winter, *Haig's Command - A Reassessment*
  5. Danilewicz later recalled: "In 1929 we proposed to the **General Staff** a device of my design for secret radio telegraphy which fortunately did not win acceptance, as it was a truly barbaric idea consisting in constant changes of transmitter frequency. The commission did, however, see fit to grant me 5,000 *złotych* for executing a model and as encouragement to further work." Cited in Władysław Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War II*, 1984, p. 27.
  6. "Random Matrix Theory for Wireless Communications" ([http://www.idc.int.de/fileadmin/user\\_upload/rmt.pdf](http://www.idc.int.de/fileadmin/user_upload/rmt.pdf)) (PDF).
  7. Ari Ben-Menahem, Historical Encyclopedia of Natural and Mathematical Sciences, Volume 1, Springer Science & Business Media - 2009, pages 4527-4530
  8. American National Standard for Electromagnetic Noise and Field Strength Instrumentation, 10 Hz to 40 GHz—Specifications, ANSI C63.2-1996, Section 8.2 Overall Bandwidth

## Sources

-  This article incorporates public domain material from the General Services Administration document "Federal Standard 1037C" (<http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm>) (in support of MIL-STD-188).
- NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management
- National Information Systems Security Glossary
- History on spread spectrum, as given in "Smart Mobs, The Next Social Revolution", Howard Rheingold, ISBN 0-7382-0608-3
- Władysław Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, edited and translated by Christopher Kasperek, Frederick, MD, University Publications of America, 1984, ISBN 0-89093-547-5.
- Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, Fifth Edition.

## External links

- HF Frequency Hopping ([http://hf-ssb-transceiver.at-communication.com/en/qmac/frequency\\_hopping.html](http://hf-ssb-transceiver.at-communication.com/en/qmac/frequency_hopping.html))
- A short history of spread spectrum (<http://www.eetimes.com/design/microwave-rf-design/4235369/A-short-history-of-spread-spectrum?Ecosystem=microwave-rf-design>)
- HF VHF UHF Spread Spectrum Radio (<http://hf-military-tactical-radio.at-communication.com/en/rsi/rsi8100.html>)
- CDMA and spread spectrum (<http://www.telecomspace.com/cdma.html>)
- Information about the use of spread spectrum for reduced AGP EMI (<http://www.rojakpot.com/showFreeBOG.aspx?Lang=0&bogno=114>)
- Spread Spectrum Scene newsletter (<http://sss-mag.com/index.html>)
- Presentations at 4/08 George Mason University conference on unlicensed spread spectrum history (<http://iep.gmu.edu/UnlicensedWireless>)

- Interview for the Indian press with Hedy Lamarr's (the inventor of spread spectrum) son, Anthony Ioder, on the impact of her invention ([http://www.hedylamarr.org/deccan\\_article.html](http://www.hedylamarr.org/deccan_article.html))

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Spread\\_spectrum&oldid=810715025](https://en.wikipedia.org/w/index.php?title=Spread_spectrum&oldid=810715025)"

---

This page was last edited on 17 November 2017, at 00:18.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

- [Contact Wikipedia](#)
- [Developers](#)
- [Cookie statement](#)