

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/221905791>

Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance

Chapter · February 2011

DOI: 10.5772/15482 · Source: InTech

CITATIONS

17

READS

13,498

1 author:



[Naser Hossein Motlagh](#)

University of Helsinki

53 PUBLICATIONS 3,177 CITATIONS

[SEE PROFILE](#)

Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance

Naser Hossein Motlagh

*Department of Information Technology, Vaasa University of Applied Sciences
Finland*

1. Introduction

To improve the performance of short-range wireless communications, channel quality must be improved by avoiding interference and multi-path fading. Frequency hopping spread spectrum (FHSS) is a transmission technique where the carrier hops from frequency to frequency. For frequency hopping a mechanism must be designed so that the data can be transmitted in a clear channel and avoid congested channels. Adaptive frequency hopping is a system which is used to improve immunity toward frequency interference by avoiding using congested frequency channels in hopping sequence. Mathematical modelling is used to simulate and analyze the performance improvement by using frequency hopping spread spectrum with popular modulation schemes, and also the hopping channel situations are investigated.

In this chapter the focus is to improve wireless communication performance by adaptive frequency hopping which is implemented by selecting sets of communication channels and adaptively hopping sender's and receiver's frequency channels and determining the channel numbers with less interference. Also the work investigates whether the selected channels are congested or clear then a list of good channels can be generated and in practice to use detected frequency channels as hopping sequence to improve the performance of communication and finally the quality of service.

The Fourier transform mathematical modules are used to convert signals from time domain to frequency domain and vice versa. The mathematical modules are applied to represent the frequency and simulate them in MATLAB and as result the simulated spectrums are analysed. Then a simple two-state Gilbert-Elliott Channel Model (Gilbert, 1960; Elliott, 1963) in which a two-state Markov chain with states named "Good" and "Bad" is used to check if the channels are congested or clear in case of interference. Finally, a solution to improve the performance of wireless communications by choosing and using "Good" channels as the next frequency hopping sequence channel is proposed.

2. Review of related theories

2.1 Spread spectrum

Spread spectrum is a digital modulation technology and a technique based on principals of spreading a signal among many frequencies to prevent interference and signal detection. As

the name shows it is a technique to spread the transmitted spectrum over a wide range of frequencies. It started to be employed by military applications because of its Low Probability of Intercept (LPI) or demodulation, interference and anti-jamming (AJ) from enemy side. The idea of Spreading spectrum is to spread a signal over a large frequency band to use greater bandwidth than the Data bandwidth while the power remains the same. And as far as the spread signal looks like the noise signal in the same frequency band it will be difficult to recognize the signal which this feature of spreading provides security to the transmission.

Compared to a narrowband signal, spread spectrum spreads the signal power over a wideband and the overall SNR is improved because only a small part of spread spectrum signal will be affected by interference. In a communication system in sender and receiver sides' one spreading generator has located which based on the spreading technique they synchronize the received modulated spectrum.

2.2 Shannon capacity and theoretical justification for spread spectrum

Claude Shannon published the fundamental limits on communication over noisy channels in 1948 in the classic paper "A Mathematical Theory of Communication". Shannon showed that error-free communication is possible on a noisy channel provided that the data rate is less than the channel capacity. Shannon capacity (data rate) equation is the basis for spread spectrum systems, which typically operate at a very low SNR, but use a very large bandwidth in order to provide an acceptable data rate per user. Applying spread spectrum principles to the multiple access environments is a development occurring over the last decade (Bates & Gregory, 2001).

The Shannon equation states that the channel capacity " C " (error free bps) is directly proportional to the bandwidth " B " and is proportional to the log of SNR. Shannon capacity applies only to the additive white Gaussian noise (AWGN) channel. The channel capacity is a theoretical limit only; it describes the best that can possibly be done with any code and modulation method.

The basis for understanding the operation of spread spectrum technology begins with Shannon/Hartley channel capacity theorem:

$$C = B \times \log_2(1 + S/N) \quad (1)$$

In this equation, C is the channel capacity in bits per second (bps), which is the maximum data rate for a theoretical bit error rate (BER). B is the required bandwidth in Hz and S/N is the signal to noise ratio. Assume that C which represents the amount of information allowed by communication channel, also represent the desired performance. S/N ratio expresses the environmental conditions such as obstacles, presence of jammers, interferences, etc.

There is another explanation of this equation is applicable for difficult environments, for example when a low SNR caused by noise and interference. This approach says that one can maintain or even increase communication performance by allowing more bandwidth (high B), even when signal power is below the noise. In Shannon formula by changing the log base from 2 to e (the Napierian number) and noting that $\ln = \log_e$. Therefore:

$$C / B = (1 / \ln 2) \times \ln(1 + S/N) = 1.443 \times \ln(1 + S/N) \quad (2)$$

Applying the Maclaurin series development for

$$\ln(1+x) = x - x^2/2 + x^3/3 - x^4/4 + \dots + (-1)^{k+1} x^k/k + \dots \quad (3)$$

$$C/B = 1.443 \times (S/N - (S/N)^2/2 + (S/N)^3/3 - (S/N)^4/4 + \dots) \quad (4)$$

S/N is usually low for spread spectrum applications, considering that the signal power density can even be below the noise level. Assuming a noise level such that $S/N \ll 1$, Shannon's expression becomes simply:

$$C/B \approx 1.443 \times S/N \quad (5)$$

And very roughly:

$$C/B \approx S/N \text{ or } N/S \approx B/C \quad (6)$$

To send error free information for a given noise to signal ratio in the channel, therefore, one need only perform the fundamental spread spectrum signal spreading operation: increase the transmitted bandwidth.

2.3 Frequency hopping spread spectrum

Frequency hopping spread spectrum is a transmission technology used in wireless networks and a technique to generate spread spectrum by hopping the carrier frequency. FHSS uses narrow band signal which is less than 1 MHz, In this method data signal is modulated with a narrowband carrier signal that "hops" in random and hopping happens in pseudo-random "predictable" sequence in a regular time from frequency to frequency which is synchronized at both ends. Using FHSS technology improves privacy, it is a powerful solution to avoid interference and multi path fading (distortion), it decreases narrowband interference, increases signal capacity, improve the signal to noise ratio, efficiency of bandwidth is high and difficult to intercept also this transmission can share a frequency band with many types of conventional transmissions with minimal interference. For frequency hopping a mechanism must be defined to transmit data in a clear channel and to avoid the congested channels. Frequency hopping is the periodic change of transmission frequency and hopping happens over a frequency bandwidth which consists of numbers of channels. Channel which is used as a hopped channel is instantaneous bandwidth while the hopping spectrum is called total hopping bandwidth. Frequency hopping categorized into slow hopping and fast hopping which by slow hopping more than one data symbol is transmitted in same channel and by fast hopping frequency changes several times during one symbol. Hopping sequence means which next channel to hop; there are two types of hopping sequence: random hopping sequence and deterministic hopping sequence.

The focus of this work is on slow and deterministic frequency hopping sequence. In a frequency hopping network, there can be different number of receivers which one sender is designed as Base that is responsible to transmit the synchronization data to the receivers.

2.4 Adaptive frequency hopping

Adaptive frequency hopping (AFH) is a system in which devices constantly change their operating frequency to avoid interference from other devices and maintain security. AFH classifies channels as 'Good' or 'Bad' and adaptively selects from the pool of Good channels. 'Bad channels' means the channels with interference. The Idea of using AFH is to hop only

over Good and clear channels it means to choose the frequency channels that they have less interferences. For using AFH there must be a mechanism to choose 'Good' and 'Bad' channels. Using AFH has some advantages which they are:

- Active avoidance to narrowband interference and frequency fading
- Avoids crowded frequencies in hopping sequence
- Performance of BER is high
- Reduces transmission power
- Working with adaptive channel will further enhance system performance

RSSI (Received Signal Strength Indication) tells each channel quality to generate a list for 'bad channels'. As for using AFH there must be a mechanism to choose 'Good' and 'Bad' channels, this mechanism can be done by functionalizing one of the duplex channel as the feedback channel. The feedback information contains the channel numbers which are in use. In a duplex communication system as shown in Figure 1 there is a transmitter A and a receiver B to define as uplink and downlink from the sender to receiver and for the selection of frequency channel as the next hop to use the feedback from uplink. Also a system must be proposed to generate a hopping sequence number as the channel number which uplink "receiver" sends this number by the feedback to downlink "sender". Transmitter A baste on predefined frequency or control channel sends the data to receiver B, the RSSI value of downlink which is equivalent as SIR is measured at the end B. The receiver B analysis the data and sends a number to sender A over the uplink and if the measured data is below the criterion then LQA determines that channel needs to be switched. Sender A uses this number as a variable in a predefined algorithm which calculates the sequence of frequencies that must be used and sends a synchronization signal over downlink by the first frequency based on the calculated sequence to acknowledge the receiver side B that it has correctly calculated the sequence number. Finally communication starts between sender and receiver and both end receiver and sender change their frequencies based on the calculated order.

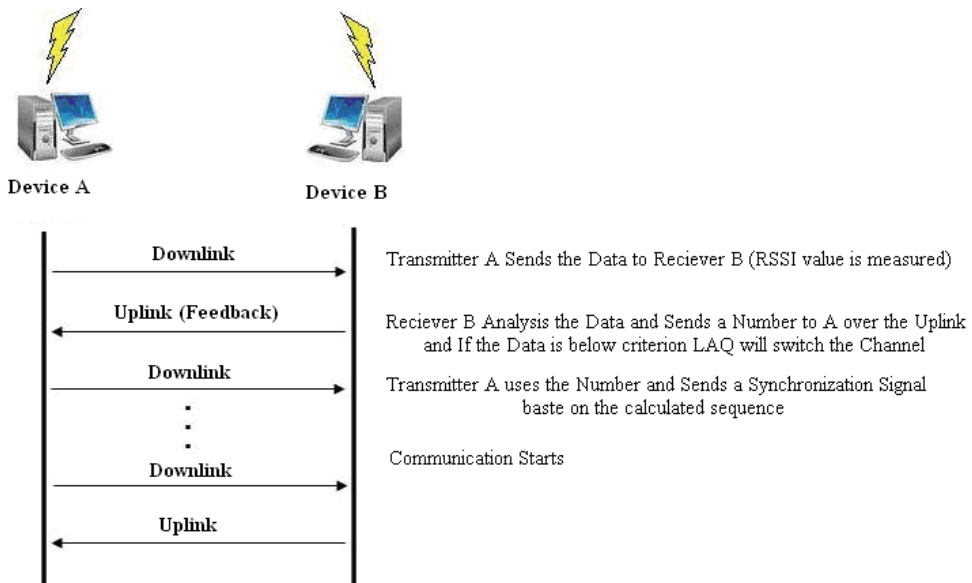


Fig. 1. Shows the communication scheme

To illustrate the system and principles of a proposed AFH scheme more, assume that there is a duplex transceiver system as shown in Figure 2. The system is an ordinary Frequency hopping system which uses a number of narrowband channels (Zander & Malmgren, 1995). As in Figure 2 HS is called Hope Sequence Generator, it generates pseudo-random symbols out of alphabet of size N_a . The generated sequence N_a is fed to the Mapping function that Maps incoming symbols onto a symbol alphabet of size N . And then these symbols are fed to the Frequency Hopper-Dehopper. The effect of these operations is that the system will use only N_a out of N available frequency at any time. The selection of which frequency to be used is made by LQA on the receiver side and since a duplex system is used the selected frequency is fed back to the transmitter side in the shape of a frequency map on the return channel.

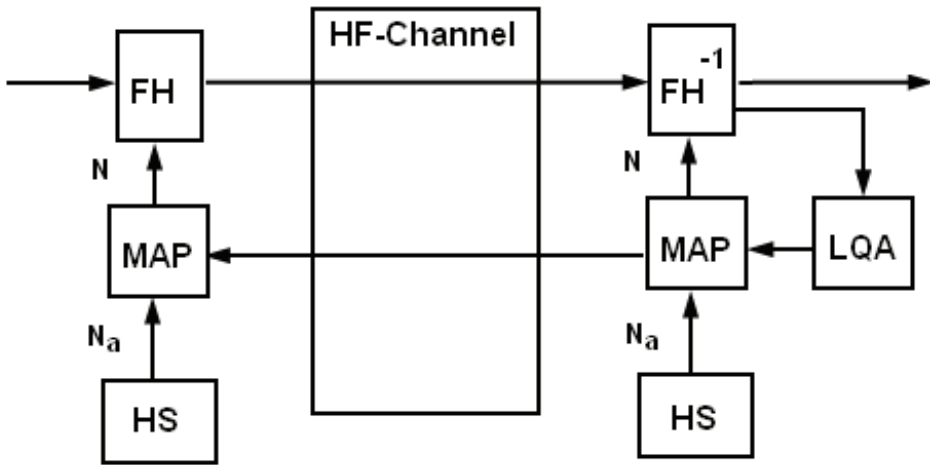


Fig. 2. Duplex transceiver system

To simplify the understanding of the AFH proposed system, assume a block-oriented transmission scheme is under use as shown in Figure 3.

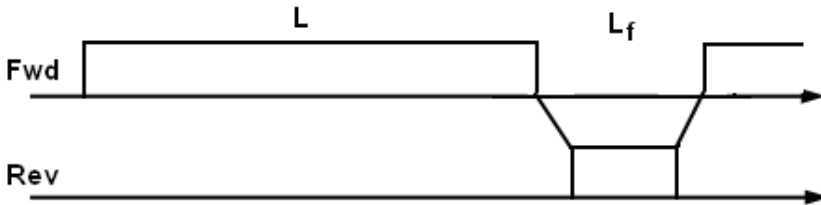


Fig. 3. Block-oriented transmission scheme

According to Figure 3, the transmitter transmits a frame of L chips which each contains one channel symbol. After the transmission of the block, the receiver performs its LQA and

replies by transmitting the new frequency map \mathbf{Lf} as a feedback block to be used in the subsequent (Forward) block transmission. It is important to mention that the proposed scheme the entire frequency map is transmitted at every updating instant and since the feedback channel is not perfectly reliable this procedure assures a high reliability. To generate a hopping sequence number as the channel number that uplink "receiver" sends this number by the feedback to downlink "sender" can be shown in a linear equation (Zander & Malmgren, 1995) and assuming binary transmission the size of the feedback block is:

$$\begin{aligned} C_f &= N_a \log_2 N + C_{OH} + R_x \\ N &= TotalAvailableChannels \\ N_a &= ActiveChannels \\ C_f &= ChipsOnFeedback \\ C_{OH} &= FeedbackOverhead \\ R &= ChipRate \\ \tau &= propagationTime + LOADelay \end{aligned}$$

LOH is feedback overhead which includes error detection symbols.

2.5 Channel and interference

Compared to the other kinds of wireless communications, high frequency (HF) communication is selectively fading because of the multipath propagation and abundance of interference from the others. Interference always exists in any wireless system. In the improved system bit error rate is highly important for the improvement of the communication systems. Every frequency channel due to interferences and fading shows different signal to noise ratio. In some of the frequency channels there are stronger SNR and these channels are more suitable for the transmission. Adaptive Frequency Hopping is a powerful solution and a technique that deals with different kind of interferences, noise sources and fading. For the simplicity of the work the focus will be only on the interference as the main disturbance in achieving a desired and suitable transmission quality and neglect all the other disturbance resources such as other noises and fading.

3. Markov chain

A Markov Chain process is a random process with the Markov property which means that given the present state the coming future states are independent from the past. Also the future states will be reached by probabilistic process and in every step the system may change its state from current state to another or remain in the same state, these changes in the states are called transitions and the probabilities are called transition probabilities.

Markov chain is formally presented as:

$$\Pr(X_{n+1} = x | X_n = x_n, \dots, X_1 = x_1) = \Pr(X_{n+1} = x | X_n = x_n) \quad (7)$$

A discrete time Markov Chains is a stochastic dynamical system in which the probability of arriving in a particular state at a particular time moment depends only on the state at the previous moment. That is:

1. States are discrete: $i = 0, 1, 2, \dots$
2. Time is discrete: $t = 1, 2, \dots$
3. Probabilities P_{ij} of transition from state i to state j in one time step are constant, i.e., they do not depend on time and do not depend on how the system got in state i "Markov property".

3.1 Gilbert-Elliott channel model

Bit error Models generate a sequence of noise bits (where 0's represent good bits and 1's represent bit errors) which to produce output bits modulo 2 to the input bits must be added. Models are grouped into two classes (Lemmon, 2002):

1. Memoryless Models
2. Models with Memories

In Memoryless Models the noise bits are produced by a sequence of independent trials that each trial has the same probability $P(0)$ of producing a correct bit and probability $P(1) = 1 - P(0)$ of producing a bit error.

The actual measurement from the communication channels indicate that these channels are with memories, for example the probability of 100's bit is erroneous is dependent on the 99's bit. For modelling of these kinds of probabilistic situations a commonly technique is used that is called Markov Chain. This technique helps to make the bit error probability depend on the states. The use of Markov Chain technique in bit error models was introduced by Gilbert-Elliott for the first time. Gilbert model based on Markov Chain has two states G (Good) and B (Bad or for Burst). In state G, transmission is error-free and in state B the link has probability h of transmitting a bit correctly. Figure 4 shows a transition diagram and bit error probabilities for Markov Chain. The situation of small p is where transition jumps from B to G and the capital P is where the probability of jumping from G to B. Also the states B and G tend to persist, and the model simulates bursts of errors.

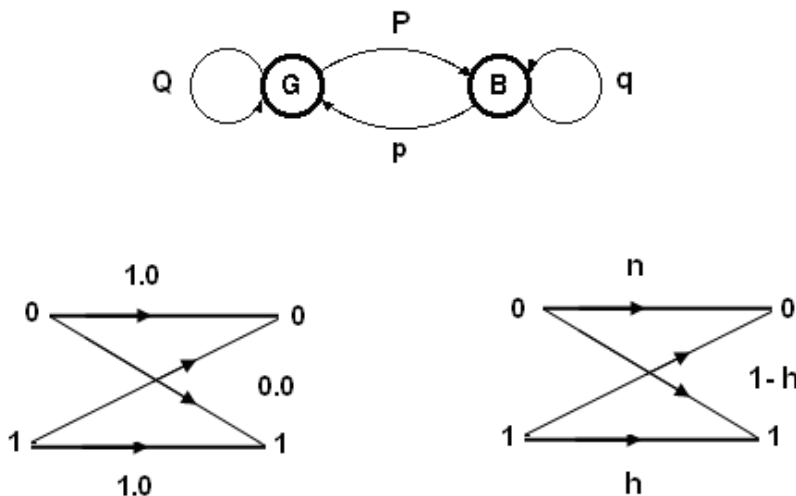


Fig. 4. Transition diagram and bit error probabilities model

The model has shown above is the transition diagram and bit error probability for Gilbert-Elliott Model and simply has three independent parameters (p , P and h) and also describes the error performance of wireless links.

The parameters p , P and h are not directly observable and must therefore be determined from statistic measurements of the error process and also important to note that Runs of G alternates with runs of B. The run length has geometric distributions, with mean $1/P$ for the G-runs and $1/p$ for the B-runs.

3.2 Geometric distribution

A Bernoulli process is a discrete time stochastic process consisting of sequence of independent random variables which take the values over two symbols, the general example for Bernoulli is coin tossing that's why it's said a Bernoulli process is coin flipping several times and also a variable in such a sequence called Bernoulli variable. Bernoulli distribution has two possible outcomes labeled by $n = 0$ and $n = 1$, in which $n = 1$ is 'Success' with probability p and $n = 0$ is 'Failure' occurs with probability $q = 1 - p$, where $1 < p < 1$. The performance of a fixed number of trials with fixed probability of success on each trial is known as a Bernoulli trial. The distribution of heads and tails in coin tossing is an example of Bernoulli distribution with $p = q = 1/2$.

Geometric distribution is number of Failures before the first success on sequence of independent Bernoulli trials. The geometric distribution is a district distribution for $n = 0, 1, 2 \dots$ having probability density function:

$$\Pr(X = x) = (1 - p)^{x-1} p \quad (8)$$

Also the mean value of x will be calculated as:

$$E[x] = \sum_{x=1}^{\infty} x \Pr(X = x) \quad (9)$$

Which is equal to $1/p$, also the Runs length of Good and Bad states can be expressed by geometric distribution in which for the Good runs, mean value of $1/P$ and for the Bad runs, the mean value of $1/p$ is used. Also the time fraction in both of Good and Bad states based on persistence in each state can be calculated for example the fraction of time spent in B state is:

$$P(B) = \frac{P}{P + p} \quad (10)$$

The sequence of states cannot be reconstructed from the sequence of bits in the error process, because both of 0's and 1's (The Good bits and bit errors) are produced in the B state and since bit errors happen only in state B with probability of $1-h$ then the probability of error is:

$$P(1) = P(1, B) = P(B)P(1 | B) = (1 - h) \frac{P}{P + p} \quad (11)$$

However the bits of the error process (Runs of 0's and 1's) and the distribution of run lengths of 0's (error Gaps) and 1's (error Bursts) are observable to determine model parameters.

3.3 Parameter estimation

The determination of the three parameters p , P , and h from measurements of the error process requires that parameters be expressed as functions of three other parameters that are directly observable and for Markov Chain parameter estimation the functions which have been proved formerly (Lemmon, 2002), that those are:

$$\mu_{EB} = \frac{1}{1-q(1-h)} \quad (12)$$

$$\mu_{EG} = \frac{h(1-Q) + (1-q)}{(1-h)(1-Q)[1-q(1-h)]} \quad (13)$$

$$\sigma_{EB}^2 = \frac{\sqrt{q(1-h)}}{1-q(1-h)} \quad (14)$$

$$\sigma_{EG}^2 = \frac{(1-h)(qJ + p - Q)(J+1)}{[1-q(1-h)](J-L)(1-J)^3} + [J \leftrightarrow L] - \mu_{EG}^2 \quad (15)$$

In the equations μ_{EB} is the mean error burst length and μ_{EG} is the mean error gap length, σ_{EB}^2 is the variance of the error burst distribution and σ_{EG}^2 is the variance of error gap distribution. J and L are defined as:

$$2J = Q + hq + \sqrt{(Q + hq)^2 + 4h(p - Q)} \quad (16)$$

$$2L = Q + hq - \sqrt{(Q + hq)^2 + 4h(p - Q)} \quad (17)$$

4. Matlab modelling

4.1 Gilbert-Elliot modelling

Gilbert-Elliot channel model is used for modelling a telecommunication channel. For obtaining the parameters of this model, first a sequence of data bit is given to the transmitter and then from the receiver side the transmitted data is received as output data. With the input sequence and output sequence, bit error sequence can be calculated easily. By having this bit error sequence and the method of parameter estimation in Lemmon (2002) the model parameters can be calculated.

For this reason channel simulation is done with Simulink. To obtain the bit sequence of input and output, two variables with names "in" and "out" are used. With XORing the input and output bit sequences the bit error sequence is calculated. By setting bit error sequence at argument of function `marcov`, Markov parameters can be achieved from the output of function `marcov`. In function `marcov` by using the function `coef`, the sequence of error burst and error gap can be calculated. After calculation of statistical parameters of these two sequences, Markov parameters can be then calculated by function `fsolve` which solves nonlinear equations.

4.2 Defining Markov chain parameters

To obtain Markov parameters in Matlab, a function of `marcov` is created as follow.

```
error_seq= xor(in,out);
z=marcov(error_seq);
z=fsolve(@solv,[.1 .1],[],mcb,meg,veg);
```

In this function the error sequence is first inputted to the function of `coef` then the output of sequence is obtained as 0's and 1's.

For example assume there is a sequence of:

```
error_seq = [0 1 0 0 1 1 1 0 1 1 0 1 0 1 1 1 1 0 0 0]
```

Then at the output of function `coef` will obtain:

```
error_burst_seq = [1 3 2 1 4]
```

```
error_gap_seq = [1 3 1 1 1 3]
```

Now from the output `error_burst_seq` and `error_gap_seq` which is the sequence of error runs it can be seen that the length of the run of the errors has come in order of their happenings. Next step is to calculate the mean value and the variance of the sequence.

4.3 Channel performance evaluation

100 communication channels are evaluated and channel performances are categorized based on Gilbert-Elliot channel model. Gilbert-Elliot model is used for modelling a real communication channel and evaluating the performance of the channels, in which first a bit sequence is sent through a channel and then its bit error sequence is computed. Using bit error sequence helps to find out the parameters of the model. Markov parameters can be used to find following two functions: Fraction of time spent in state B (Bad) from equation (10) and probability of the error from equation (11).

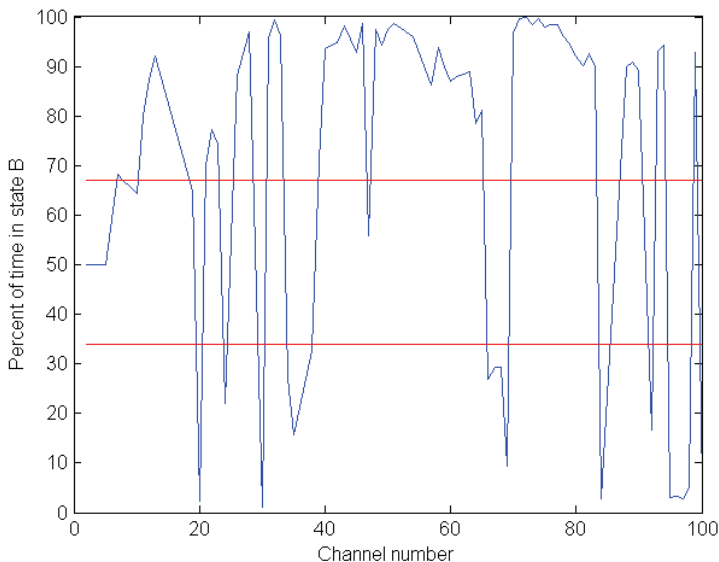


Fig. 5. Percent of time that each channel spends in state B

To evaluate the channel performance based on Gilbert-Elliot Markov chain model the information about bit error sequence is collected to simulate the channel model with Matlab. Additive white Gaussian noise (AWGN) channels with 100 random input powers are used in simulation.

First the percent of time is computed which each channel spends in state B or in the other word the probability of being in state B that multiplied by 100. Figure 5 shows the result of each channel being in Bad state.

The achieved result from Figure 2 helps to categorize the Channels based on three different groups as “Bad Channels”, “Good Channels” and “Very Good Channels” by identifying two threshold values and categorizing those decides to transmit data over “Very Good” and “Good” channels then by such transmission the performance of the communication system can be improved. Then the error probability in Bad state for each channel is computed. Figure 6 shows these probabilities for 100 different channels.

4.4 Testing

Gilbert-Elliot channel model is used to simulate the error process and correctly reproduce all of its statistical properties. To validate the model, the error process generated by the model must be compared to the measured error process. For testing, the program bit error sequence is generated using Markov chain model. Two programs are made as follow: `marcov_gen` is a bit error sequence generator for Markov parameters and `marcov_test` tests the bit error sequence and the output is displayed in workspace.

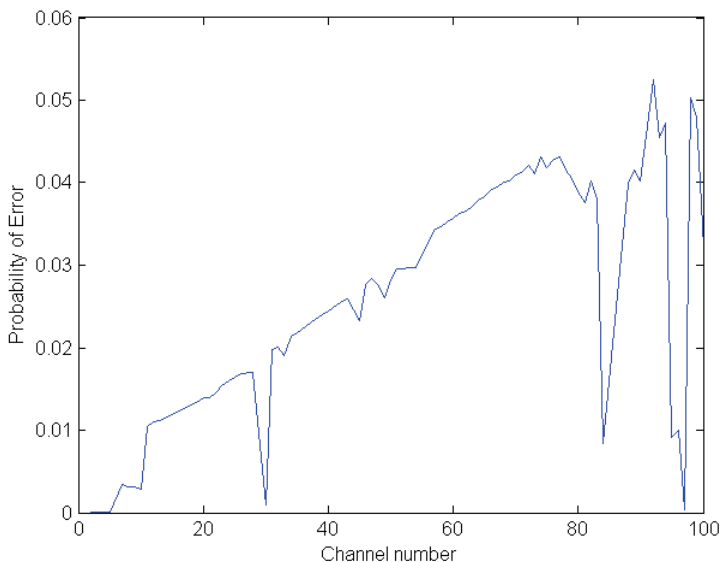


Fig. 6. Error probability being in Bad state for each channel

The objective of the parameter estimation is to choose values of the model parameters that generate error burst and error gap distributions that reassembles the corresponding

measured distributions as close as possible. Therefore for testing the mean and variance of error burst and error gap of regenerated error sequence are calculated and compared by statistical parameters of channel bit error sequence, where the result is shown in Table 1.

	error burst mean	error gap mean	error gap variance	
SNR = 3dB Input power = 1	1.0568	18.1134	319.4516	A
	1.0492	18.4713	319.3184	B
SNR = 3dB Input power = 2	1.1456	7.7868	48.9981	A
	1.1500	8.0421	55.0026	B
SNR = 3dB Input power = 3	1.2201	5.6570	25.5754	A
	1.2271	5.5166	24.5044	B

A: Statistical parameters channel error sequence.

B: Statistical parameters of regenerated error sequence.

Table 1. Statistical parameters of channel error and regenerated error sequence

For testing, first Markov model parameters of a channel error sequence are computed, then a sequence of the model is generated and statistical parameters are computed. The statistical parameters must be as equal as channel error sequence. It is important to mention that first state of the Markov model in function `marcov_gen` chooses the probability 0.5, so sometimes two different answers can be seen and that the nearest one to the error sequence statistic is the correct one.

5. Evaluation of frequency hopping

To design the frequency hopping (FH) model, MATLAB Simulink has been used. The spreader at transmitter section is an M-FSK modulation but the input of the modulator is hopping index. This section consists of a PN Sequence Generator, an Assemble Packets block and a Goto block as shown in Figure 7.

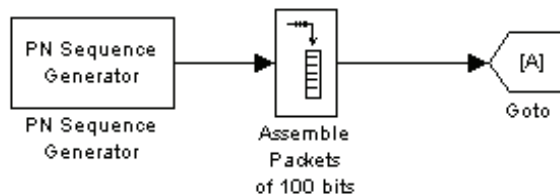


Fig. 7. Model of frequency hopping in Simulink

The design of frequency hopping spreader is shown in Figure 8. The spreader part consists of M-FSK modulator base (with M equal to 64), a From block (Hop index that is created in previous step), a To Frame block and a Multiplication block. The block parameter of FSK modulator is 64 in M-FSK number and it means that there are 64 hopping sections. These sub-bands are selected by the hop indexes.

The design of frequency hopping despreader, is the same as spreader section but the output of M-FSK modulator block is complex conjugated as shown Figure 9.

This frequency hopping model is used for evaluation of three different modulations: QAM, QPSK, GFSK, and compares the performance with the situation without frequency hopping. Performance evaluation is based on BER values under two situations (with and without FH) versus normalized signal-to-noise ratio (SNR) measured by E_b/N_0 values of the channel, as shown in Figure 10, 11, 12.

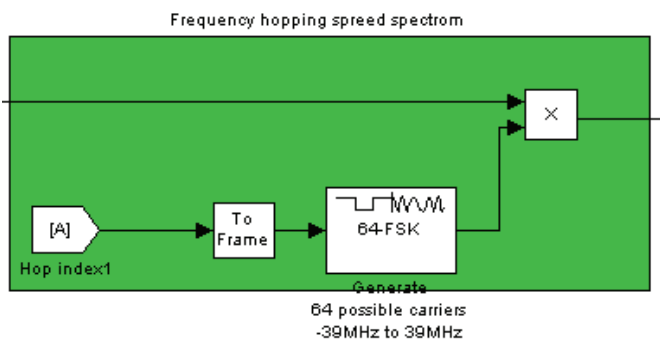


Fig. 8. Design of frequency hopping spreader

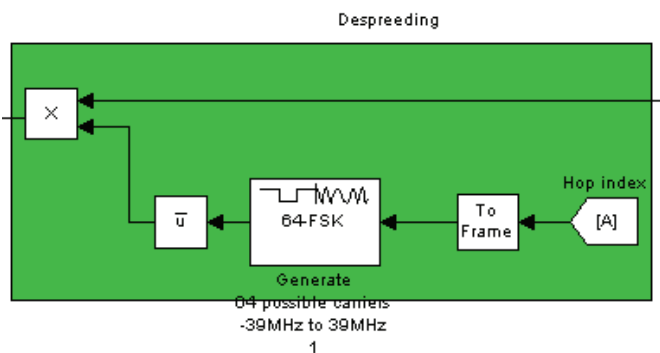


Fig. 9. Design of frequency hopping despreader

From Figure 10 it can be seen that applying FH with QAM modulation does not lead to a sensible improvement in performance or significant reduction of BER. From Figure 11 it can be seen that applying FH with QPSK modulation gives a good result and reduces

significantly BER compared to without FH at same level of SNR. From Figure 12 it can be seen that applying FH with GFSK modulation reduces dramatically BER compared to without FH at same level of SNR and lead to a much higher performance.

In overall, based on the evaluation results it can be concluded that applying the designed FH schemes with certain modulations can improve their communication performances, especially at weak SNR levels as most cases of short range wireless communications have.

6. Conclusion

As a result of the work it can be concluded that adaptive frequency hopping is a powerful technique to deal with interference and Gilbert-Elliot channel model is a good technique to analyze the situations of channels by categorizing the channel conditions based on their performance as Good or Bad, and then apply adaptive frequency hopping which hops frequencies adaptively by analyzing the state of the channel in case of environmental problems such as interferences and noises to improve the communication performance.

Frequency hopping spread spectrum is modelled with MATLAB and three different modulations i.e. QAM, QPSK and GFSK are studied to investigate which of these modulations are good to apply with FHSS model. The simulation results show that applying FHSS with QAM modulation dose not lead to a remarkable reduction of BER, but with QPSK modulation gives a good result and reduces BER at lower SNR, while in GFSK modulation shows a significant reduction of BER and lead to a high performance.

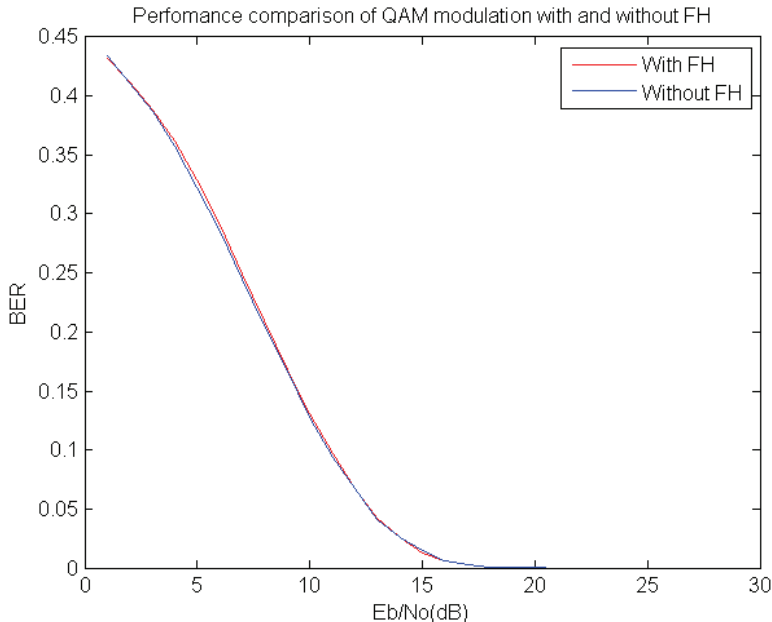


Fig. 10. QAM modulation

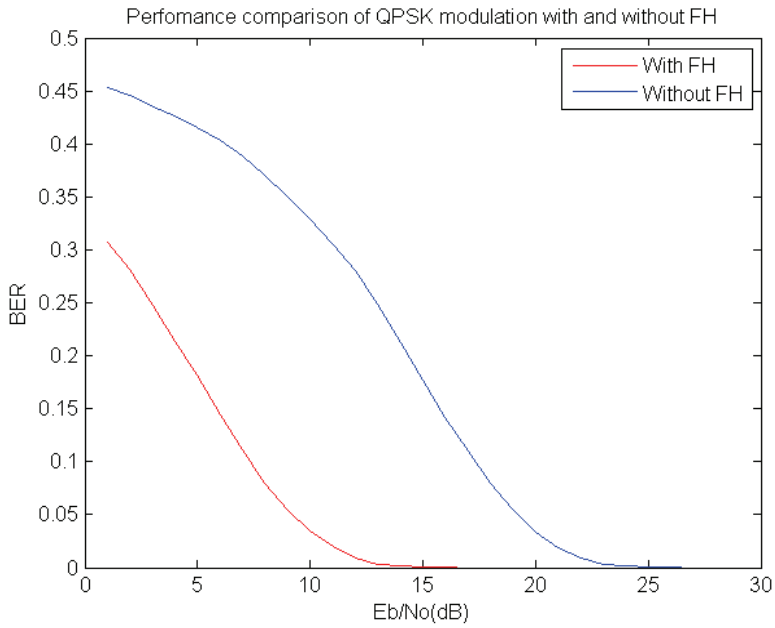


Fig. 11. QPSK modulation

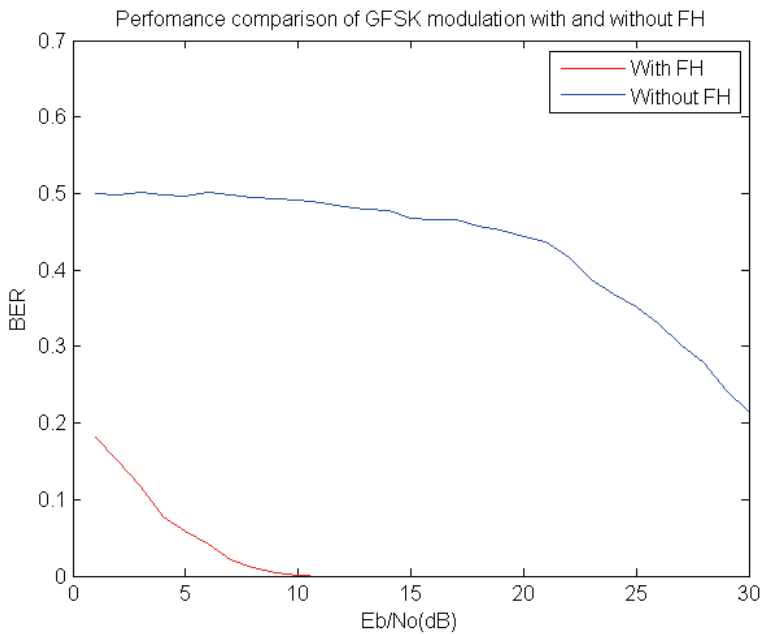


Fig. 12. GFSK modulation

7. Acknowledgement


The author gratefully acknowledges Dr. Yang Liu for his valuable support and guidance in this research work.

8. References

- Bates, R. J. & Gregory, D. W. (2001). *Voice & Data Communications Handbook*, McGraw-Hill Osborne Media
- Elliott, E. O. (1963). Estimates of error rates for codes on burst-noise channels, *Bell System Technical Journal*, Vol. 42, pp. 1977-1997
- Gilbert, E. N. (1960). Capacity of burst-noise channels, *Bell System Technical Journal*, Vol. 39, pp. 1253-1265
- Lemmon, J. J. (2002). Wireless link statistical bit error model, *Institute for Telecommunication Sciences*
- Zander, J. & Malmgren, G. (1995). Adaptive frequency hopping in HF communications, *IEE Proceedings Communications*, Vol. 142, pp. 99-105
- Ziener, R.; Peterson, E. R. L. & Borth, D. E. (1995). *Introduction to Spread Spectrum Communications*, Prentice Hall

introduction to frequency hopping spread spectrum, pseudo noise generator, slow and fast FHSS, uses of FHSS

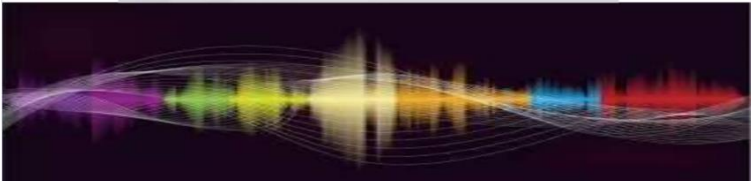
1 of 14 [Download Now](#)
Download to read offline




MUKESH PATEL SCHOOL OF
TECHNOLOGY MANAGEMENT
& ENGINEERING

[Save slide](#)


Frequency-hopping spread spectrum



Recommended



Frequency hopping spread spectrum
[Harshit Gupta](#)
25.1K views • 16 slides



5.2 ray propagation model part 1
[JAIGANESH SEKAR](#)
2.2K views • 8 slides

Diversity


25°C Sunny

FHSS- Frequency Hop Spread Sp... 2 of 14 [Download Now](#)


Introduction

- Frequency Hopping Spread Spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- The data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies.
- It is used as a multiple access method in the frequency-hopping code division multiple access (FH-CDMA) scheme.

Recommended



Frequency hopping spread spectrum
[Harshit Gupta](#)
25.1K views • 16 slides



5.2 ray propagation model part 1
[JAIGANESH SEKAR](#)
2.2K views • 8 slides

Diversity

25°C Sunny

FHSS- Frequency Hop Spread Sp... 3 of 14 [Download Now](#)

FHSS Block Diagram

```
graph LR; Input[Input data] --> CE[Channel encoder]; CE --> Mod[Modulator]; Mod --> Ch[Channel]; Ch --> DM[De-modulator]; DM --> CD[Channel decoder]; CD --> Output[Output data]; PG1[Pseudonoise generator] -- Spreading code --> Mod; PG2[Pseudonoise generator] -- Spreading code --> DM;
```

Recommended

- Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides
- 5.2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides
- Diversity

25°C Sunny

FHSS- Frequency Hop Spread Sp... 4 of 14 [Download Now](#)

Pseudo Noise Generator

```
graph LR; Clock --> FF1[FF 1]; FF1 --> FF2[FF 2]; FF2 --> FFm[FF m]; FFm --> Output[Output sequence]; Logic[Logic] --- FF1; Logic --- FF2; Logic --- FFm;
```

Figure 3 Pseudo random sequence generator

Used to spread the bandwidth of the modulated signal to

Recommended

- Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides
- 5.2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides
- Diversity


25°C Sunny

FHSS- Frequency Hop Spread Sp... 5 of 14 [Download Now](#)


Types of FHSS

- THERE ARE TWO TYPES OF FREQUENCY HOPPING:
 - SLOW FREQUENCY HOPPING SPREAD SPECTRUM
 - FAST FREQUENCY HOPPING SPREAD SPECTRUM

Recommended



Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides

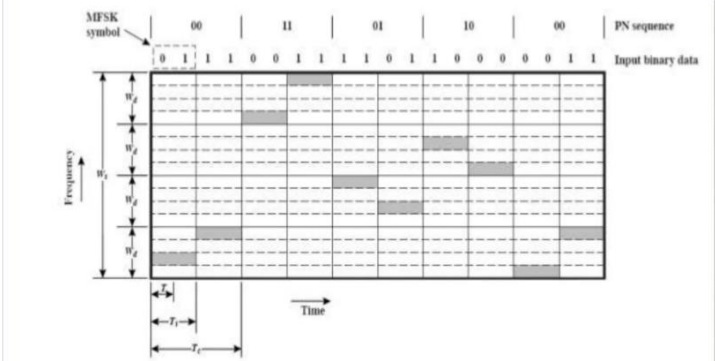


5. 2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides


25°C Sunny 12:42 PM 30/12/2023

FHSS- Frequency Hop Spread Sp... 6 of 14 [Download Now](#)


Slow FHSS



Recommended



Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides



5. 2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides

25°C Sunny 12:43 PM 30/12/2023

FHSS- Frequency Hop Spread Sp... 7 of 14 [Download Now](#)

Fast FHSS

MFSK symbol: 00 11 01 10 00 10 00 11 00 10 11 11 01 01 11 01 10
 PN sequence: 0 1 1 1 0 0 1 1 1 1 0 1 1 0 0 0 0 1 1
 Input binary data: 0 1 1 1 0 0 1 1 1 1 0 1 1 0 0 0 0 1 1

Frequency: W_1 to W_{10}
 Time: T_1 to T_{10}

25°C Sunny | Windows Taskbar | 12:43 PM 30/12/2023

Recommended

- Frequency hopping spread spectrum
 Harshit Gupta
 25.1K views • 16 slides
- 5.2 ray propagation model part 1
 JAIGANESH SEKAR
 2.2K views • 8 slides
- Diversity

FHSS- Frequency Hop Spread Sp... 8 of 14 [Download Now](#)

Uses of FSHH

- Military use
- Bluetooth
- Walkie-Talkies
- Other radios

25°C Sunny | Windows Taskbar | 12:43 PM 30/12/2023

Recommended

- Frequency hopping spread spectrum
 Harshit Gupta
 25.1K views • 16 slides
- 5.2 ray propagation model part 1
 JAIGANESH SEKAR
 2.2K views • 8 slides
- Diversity

FHSS- Frequency Hop Spread Sp... 9 of 14 [Download Now](#)

Military Use

- Spread-spectrum signals are highly resistant to deliberate jamming, unless the adversary has knowledge of the spreading characteristics.
- Military radios use cryptographic techniques to generate the channel sequence under the control of a secret Transmission Security Key (TRANSEC) that the sender and receiver share in advance.
- By itself, frequency hopping provides only limited protection against eavesdropping and jamming.

Recommended

- Frequency hopping spread spectrum Harshit Gupta 25.1K views • 16 slides
- 5. 2 ray propagation model part 1 JAIGANESH SEKAR 2.2K views • 8 slides
- Diversity

25°C Sunny

FHSS- Frequency Hop Spread Sp... 10 of 14 [Download Now](#)

- Most modern military frequency hopping radios also employ separate encryption devices such as the KY-100.

MILITARY USE:
Have-Quick KY 100
 UHF: 225-400 MHz frequency range
 2.4kbps or 12 or 16 kbps in wide band mode
 15-19 hopping frequencies per Net
 Time of Day, Word of Day, and Net Number
 -allows for multiple users
 -greater difficulty to jam

Recommended


- Frequency hopping spread spectrum Harshit Gupta 25.1K views • 16 slides
- 5. 2 ray propagation model part 1 JAIGANESH SEKAR 2.2K views • 8 slides
- Diversity

25°C Sunny

FHSS- Frequency Hop Spread Sp... 11 of 14 [Download Now](#)

Other radios

Other radios:



SINCGARS
(Single Channel Ground and Airborne Radio System)

VHF FM band, from 30 to 87.975 MHz
-2.5k channels totaling 2320 channels

Recommended

- Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides
- 5. 2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides
- Diversity


25°C Sunny

FHSS- Frequency Hop Spread Sp... 12 of 14 [Download Now](#)

Bluetooth

- Adaptive Frequency-hopping spread spectrum (AFH) (as used in Bluetooth) improves resistance to radio frequency interference by avoiding crowded frequencies in the hopping sequence. This sort of adaptive transmission is easier to implement with FHSS.

Bluetooth:



UHF: 2.4 Ghz
non licensed bw

79 1 MHz channels, 1600 hops a second
50% overhead from Hamming Code
Detects noisy channels and stops using them in specification ver 1.2


Recommended

- Frequency hopping spread spectrum
Harshit Gupta
25.1K views • 16 slides
- 5. 2 ray propagation model part 1
JAIGANESH SEKAR
2.2K views • 8 slides
- Diversity

25°C Sunny

FHSS- Frequency Hop Spread Sp... 13 of 14 [Download Now](#)

- Some walkie-talkies that employ frequency-hopping spread spectrum technology have been developed for unlicensed use on the 900 MHz band. Several such radios are marketed under the name eXtreme Radio Service (eXRS).
- Motorola has deployed a business-banded, license-free digital radio that uses FHSS technology: the DTR series, models 410, 550 and 650.

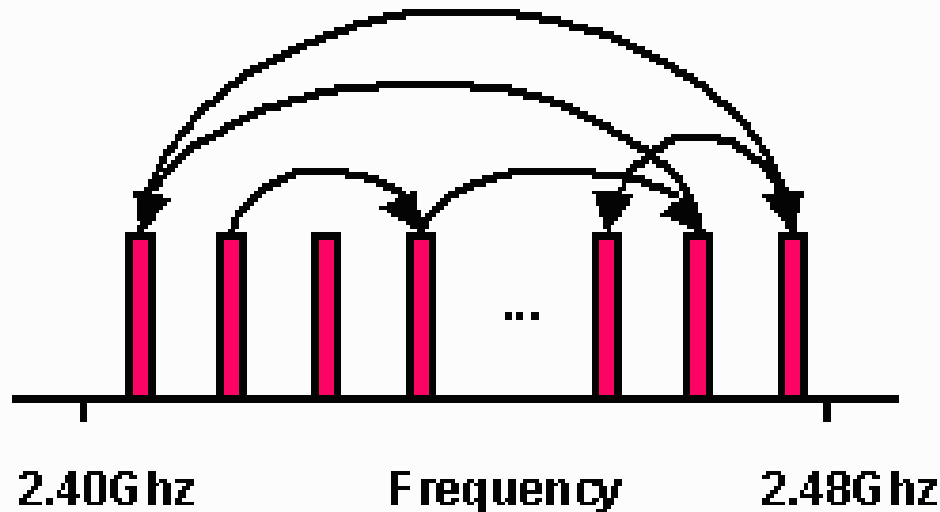


Recommended

- [Frequency hopping spread spectrum](#)
Harshit Gupta
25.1K views • 16 slides
- [5. 2 ray propagation model part 1](#)
JAIGANESH SEKAR
2.2K views • 8 slides
- [Diversity](#)

25°C Sunny | 12:44 PM 30/12/2023

FHSS



AJAL.A.J

Assistant Professor –Dept of ECE,

Federal Institute of Science And Technology (FISAT) TM

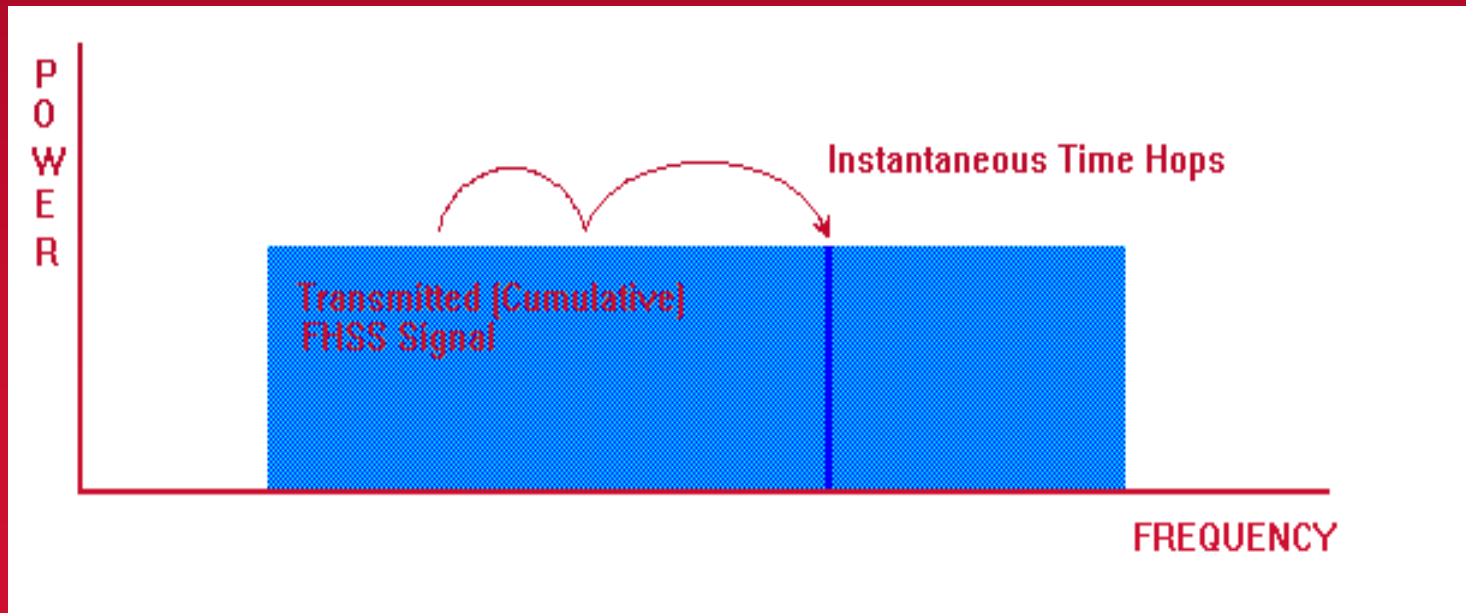
MAIL: ec2reach@gmail.com

Spread Spectrum Techniques

□ Frequency Hopped Spread Spectrum (FHSS)

Data carrier frequency is periodically modified (hopped) across a specific range of frequencies (spreading).

The shifting pattern is determined by the chosen code sequence (FSK – Frequency Shift Key).



Spread Spectrum



Frequency Hopping (FHSS)

(The radio carrier hops around the band.)

Direct Sequence (DSSS)

(The radio carrier signal is “spread out” on a specific channel)

DSSS VS FHSS

DSSS multiplies the data bits by a very fast pseudo-random bit pattern (PN sequence) that "spreads" the data into a large coded stream that takes the full bandwidth of the channel. DSSS is the basis for CDMA cellphones and 802.11 Wi-Fi wireless transmission.

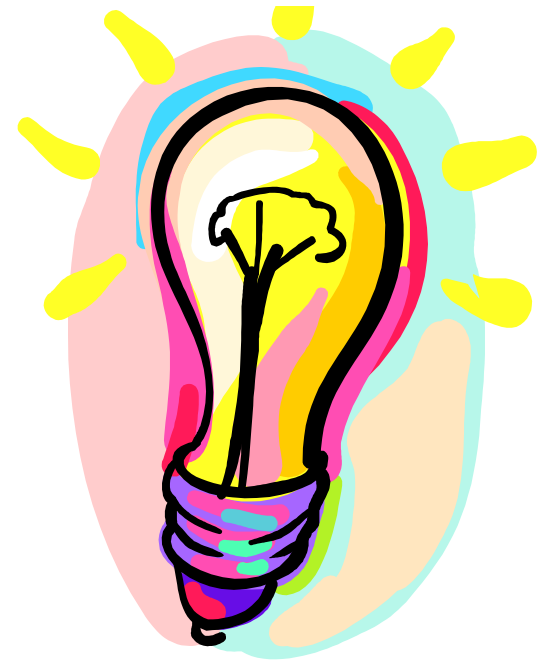
Frequency Hopping Spread Spectrum (FHSS)


FHSS continuously changes the center frequency of a conventional carrier several times per second according to a pseudo-random set of channels, while chirp spread spectrum changes the carrier frequency. Because a fixed frequency is not used, illegal monitoring of spread spectrum signals is extremely difficult

Frequency Hopping (FHSS)

What must the FHSS transmitting and receiving units know to communicate?

The hopping sequence.

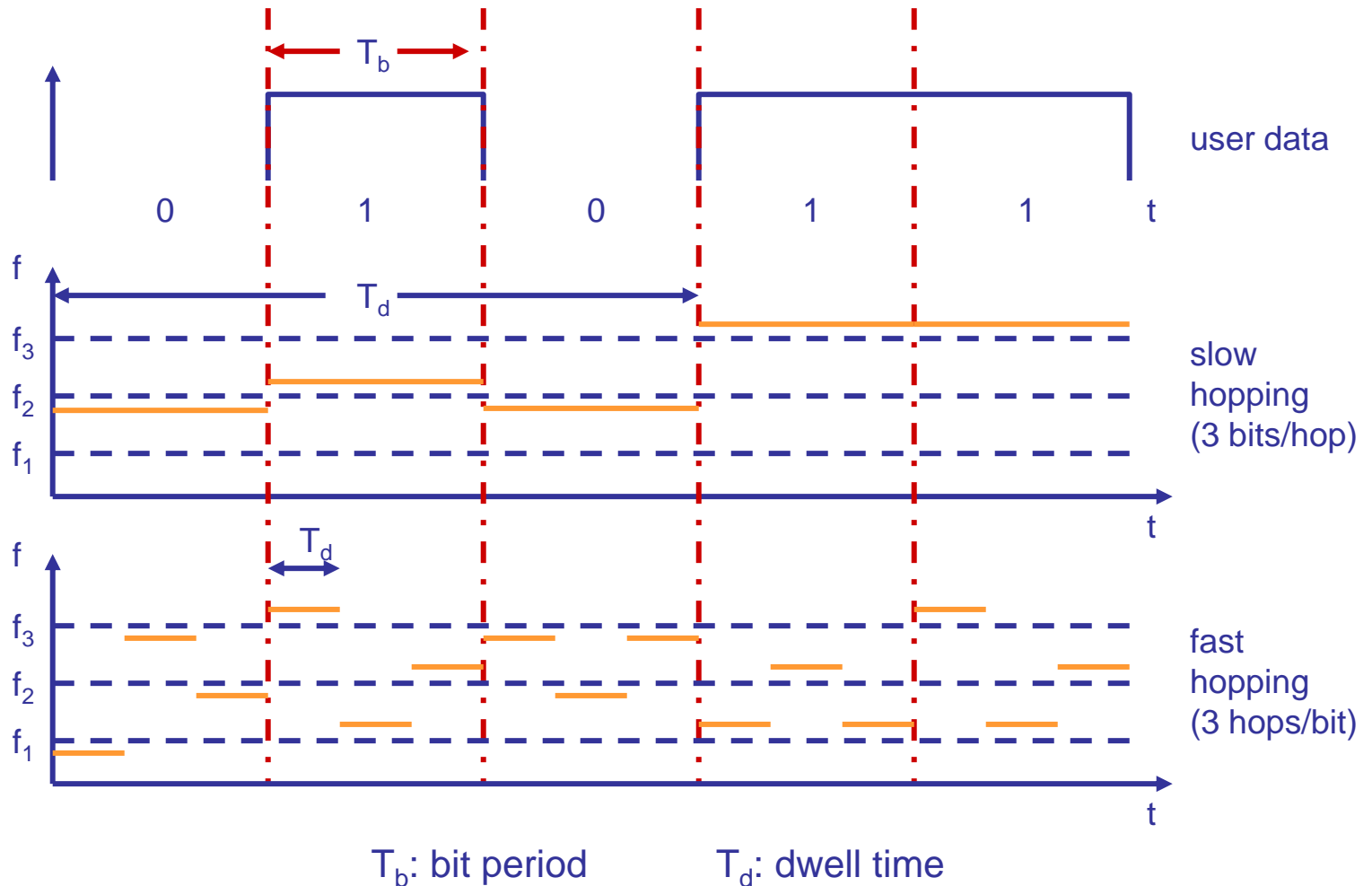


- 
- The data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies.
 - The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain.
 - This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same

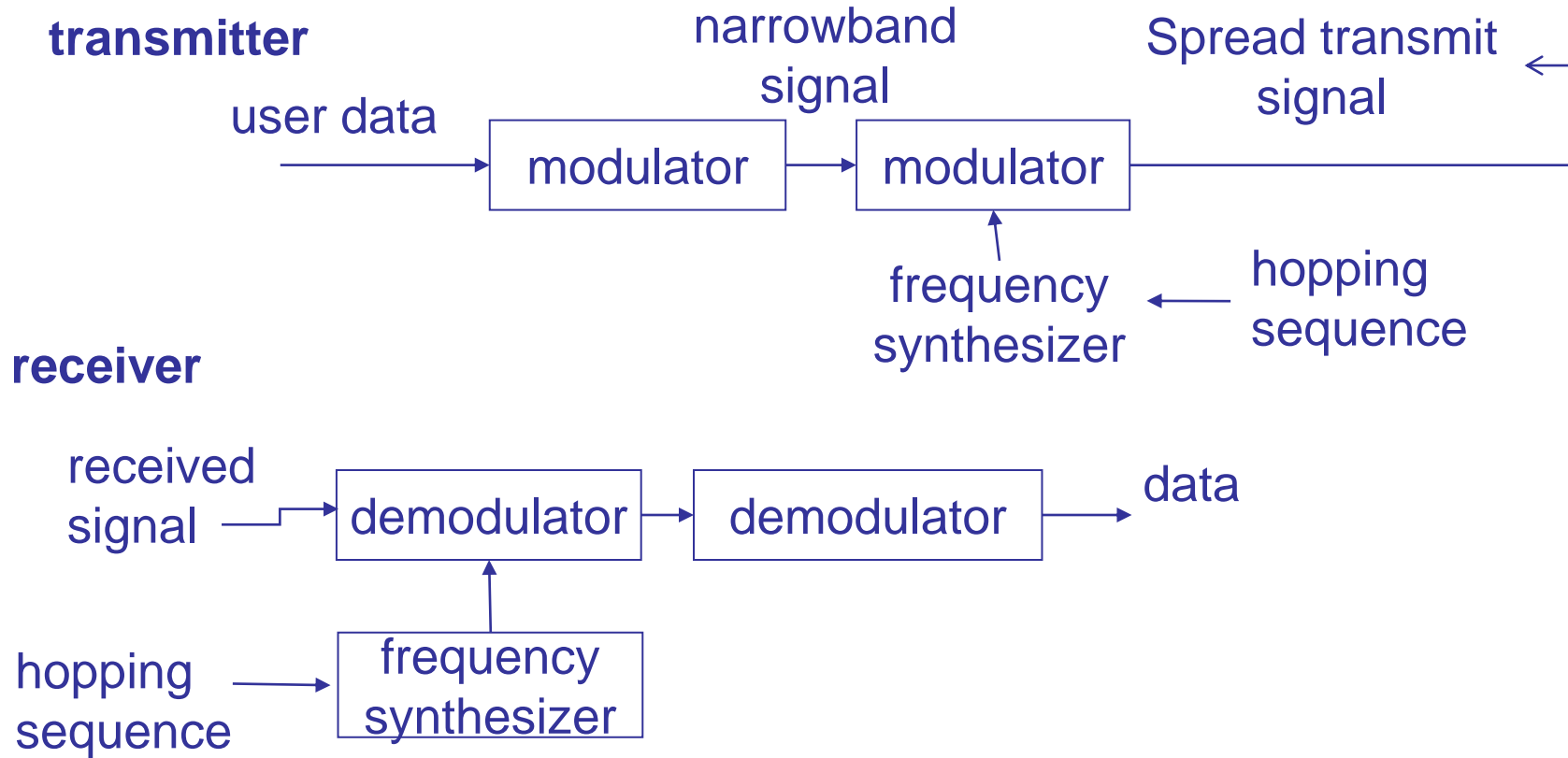
Frequency Hopping spread spectrum

- It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of "electronic warfare" - that is, the unauthorized interception or jamming of telecommunications.
- It also is known as frequency- hopping code division multiple access (FH-CDMA).

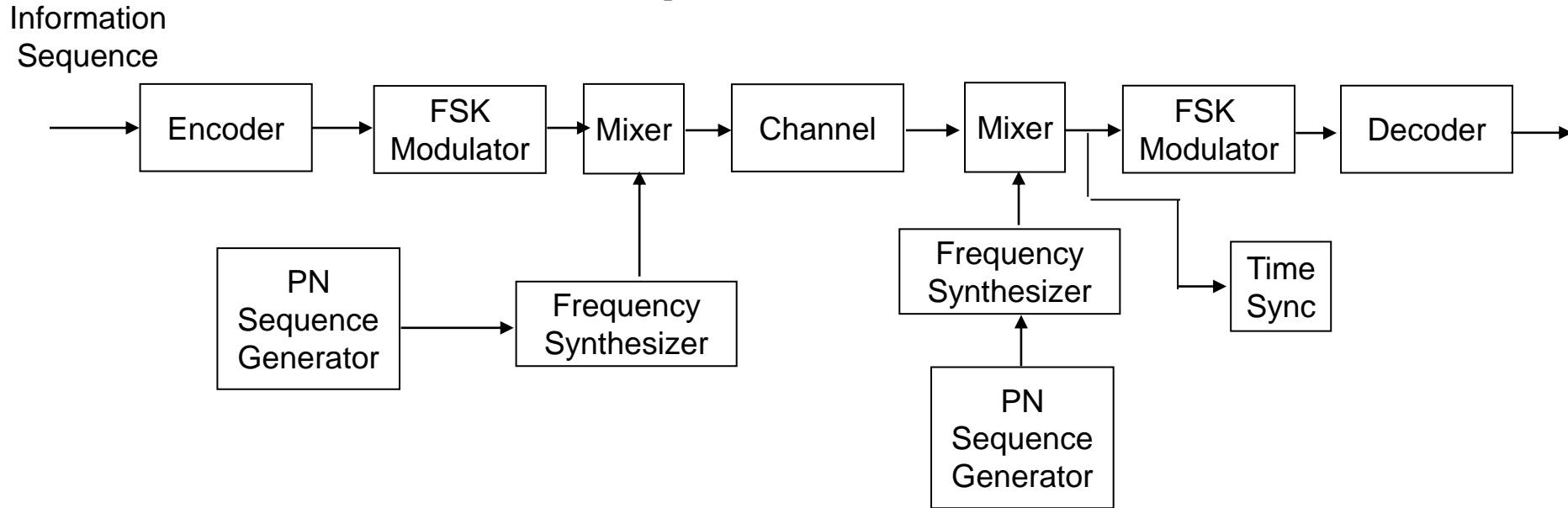
FHSS (Frequency Hopping Spread Spectrum) II



FHSS (Frequency Hopping Spread Spectrum)

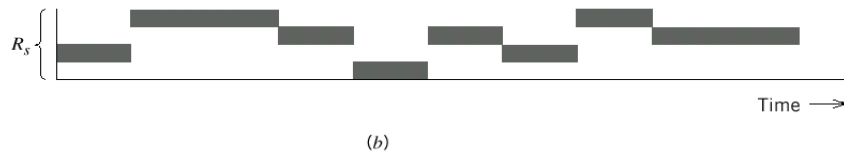
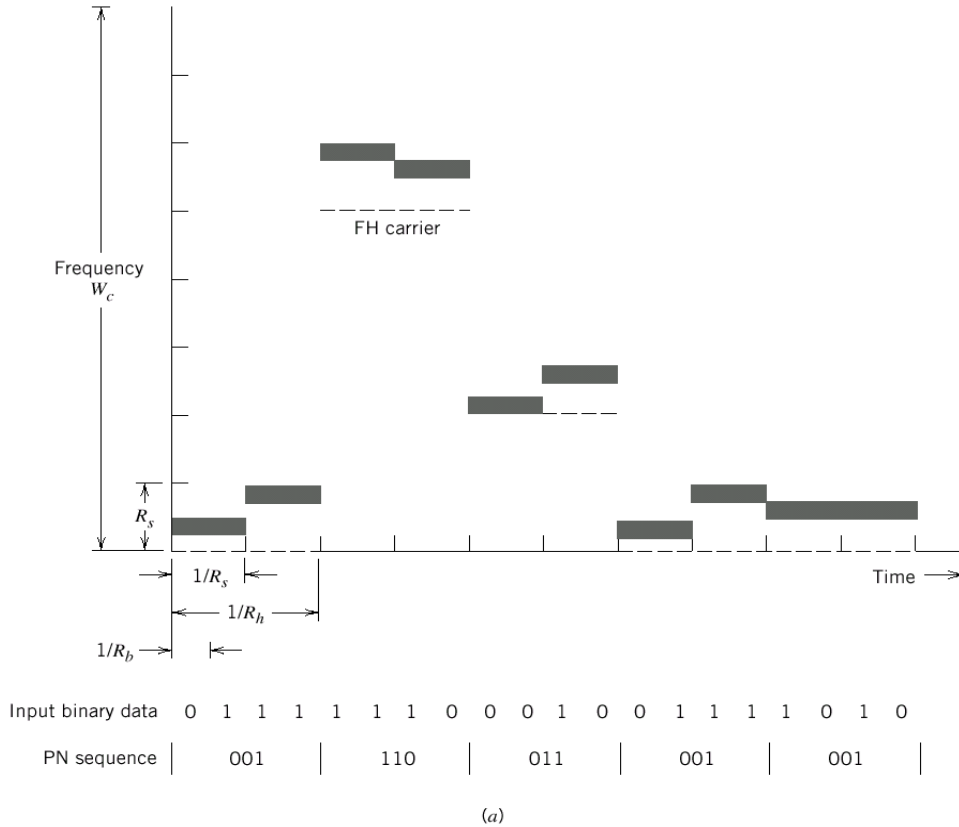


Frequency-Hopped (FH) Spread Spectrum



- FH/SS is usually used with Binary FSK or M-ary FSK
- The carrier frequency is determined by the output sequence from a PN generator
- Slow hopping system has a hopping rate that is lower than the information rate (symbol rate)
 - Several information symbols are transmitted by the same carrier frequency
- Fast hopping system has a hopping rate that is higher than the information rate
 - One information symbol is transmitted by different carrier frequencies.

Slow Frequency Hopping Example



Number of bits per MFSK symbol = 2 \rightarrow M = 4

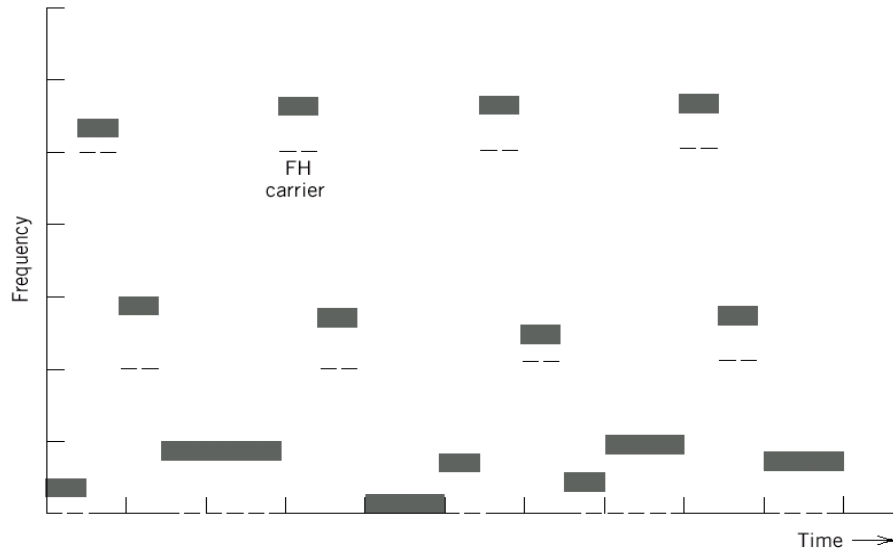
$$R_s = R_b/2$$

$$R_c = \max(R_h, R_s) = R_s$$

Length of PN segment per hop = 3

Total number of frequency hops = $2^3 = 8$

Fast Frequency Hopping Example



MFSK symbol: 0 1 1 1 1 1 1 0 0 0 1 0 0 1 1 1 1 0 1 0
 Input binary data
 PN sequence: 001110011001001001110011001001001110011001001001110011001001110011001001

(a)



(b)

Number of bits per MFSK symbol = 2 \rightarrow $M = 4$

$$R_s = R_b/2$$

$$R_c = \max(R_h, R_s) = R_h$$

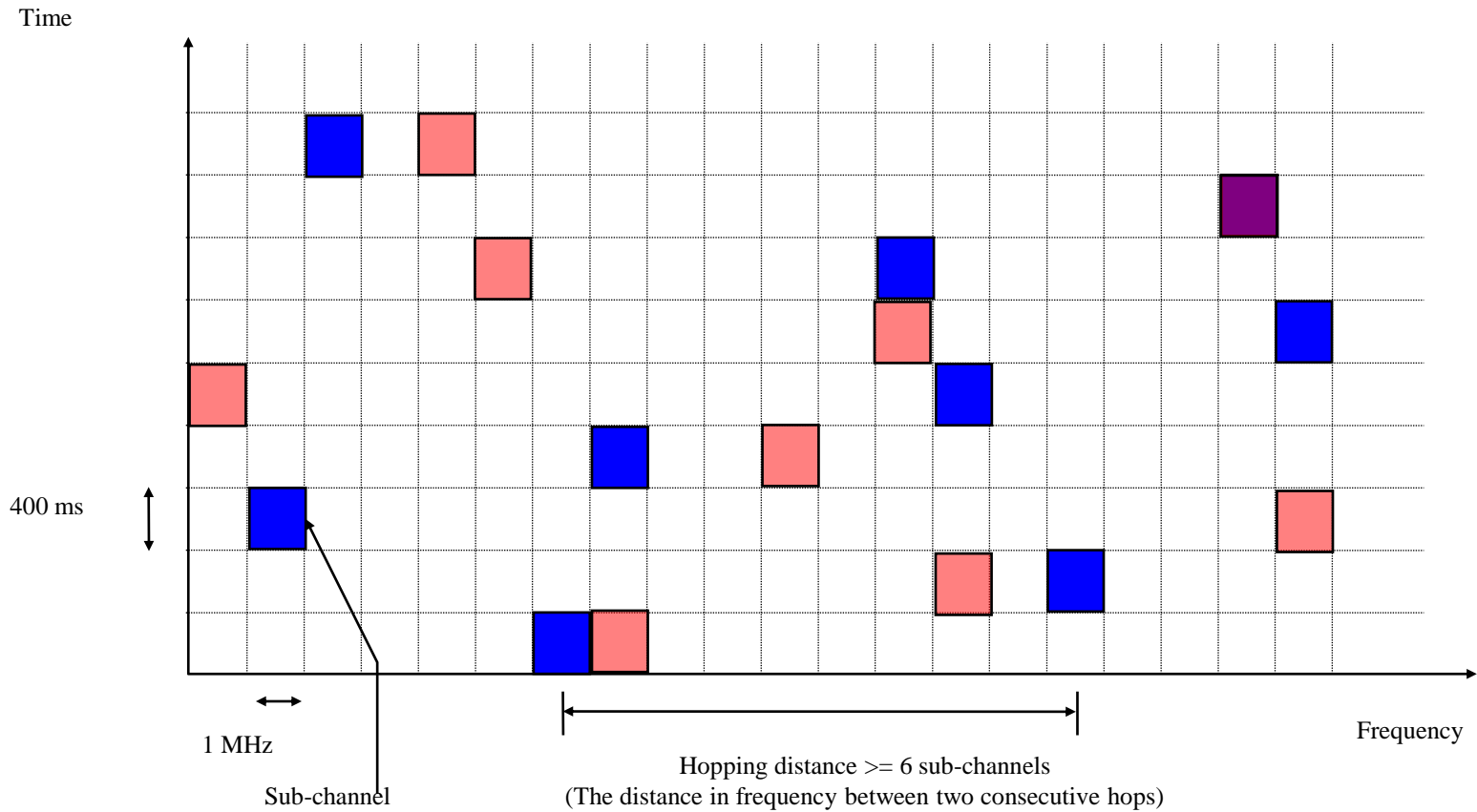
Length of PN segment per hop = 3

Total number of frequency hops = $2^3 = 8$

FHSS (only 1 and 2 Mbps)

- Band 2400-2483.5 MHz
- GFSK (Gaussian Frequency Shift Keying)
- Sub-channels of 1 MHz
- Only 79 channels of the 83 are used
- Slow hopping (2.5 hops per second)
- 3 main sets each with 26 different hopping sequences

FHSS (Cont.)

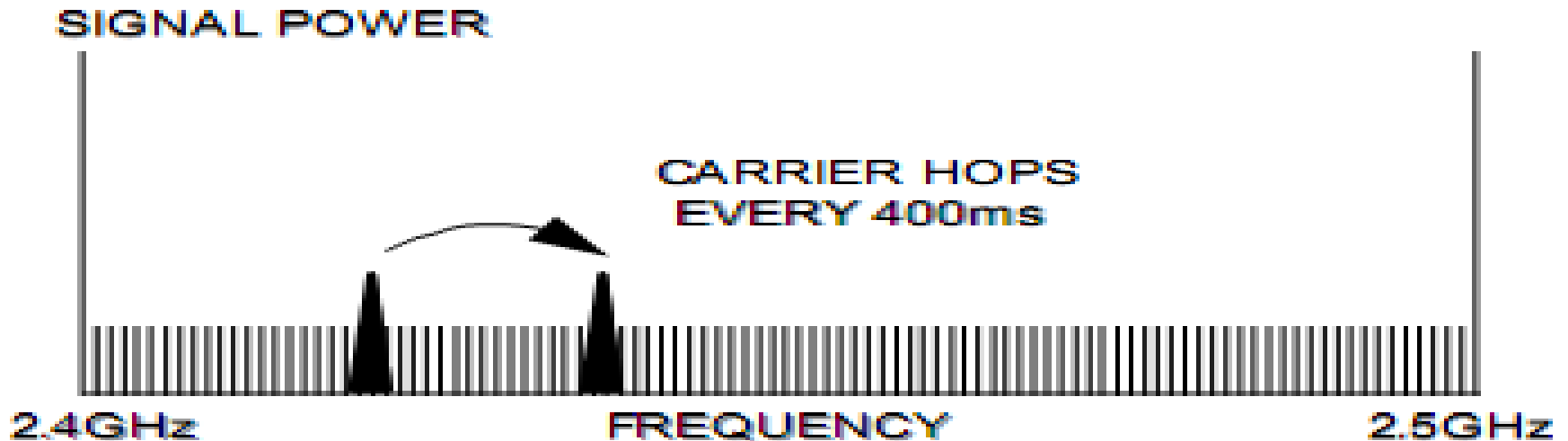


FHSS (Cont.)

- Sequences within same set collide at max. on 5 channels
- Min. hopping distance of 6 channels.
- No CDMA within same BSS
- Coexisting BSS in the same coverage area use different sequences from the same hopping set.

- Transmitting on one frequency for a certain time, then randomly jumping to another, and transmitting again.
- FH-CDMA devices use less power and are generally cheaper, but the performance of DS-CDMA systems is usually better and more reliable.
- The biggest **advantage** of frequency hopping lies in the coexistence of several access points in the same area, something not possible with direct sequence.

FH Modulation

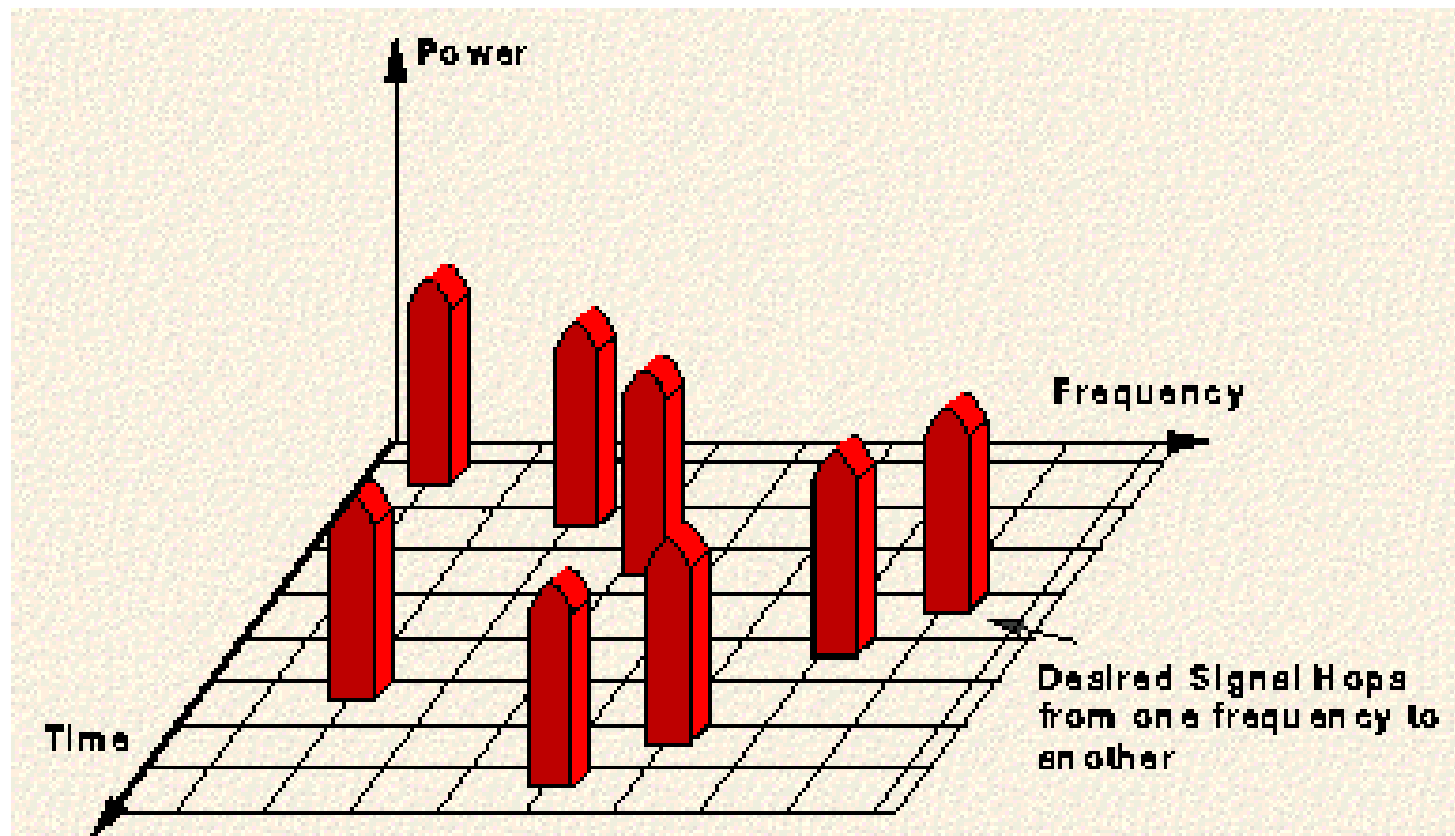


Frequency Hopping

- SIMPLE MODULATION (FSK)
- NARROWBAND, DISCONTINUOUS TRANSMISSION
- MORE NETWORK OVERHEAD
- HIGHER POWER DENSITY CAN GENERATE INTERFERENCE

- Frequency hopping has two benefits. Electrical *noise*—random electromagnetic signals which are not part of any communications signal—will only affect a small part of the signal. Also, the effects of any other forms of radio communications operating in narrow bands of the spectrum will be minimized. Any such interference that occurs will result in only a slightly reduced quality of voice transmission, or a small loss of data. Since data networks acknowledge successful receipt of data, any missing pieces will trigger a request to transmit the lost data.

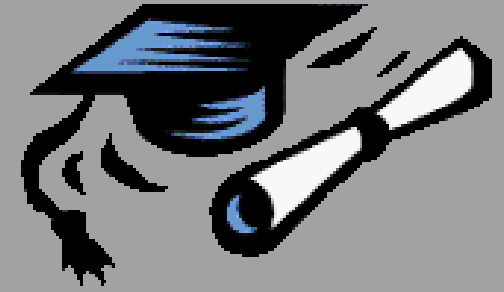
Frequency Hopping



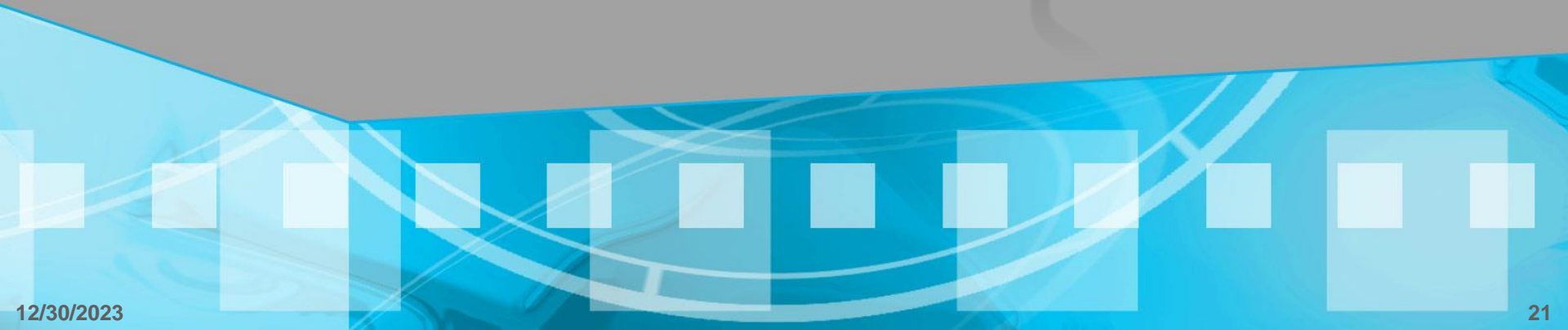
Disadvantage:

- a high processing-gain is hard. There is need for a frequency-synthesizer able perform fast-hopping over the carrier-frequencies.

THANKS



ANY



See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/329572298>

Random Paths to Frequency Hopping

Article in *American Scientist* · December 2018

DOI: 10.1511/2019.107.1.46

CITATIONS

10

READS

2,051

1 author:



[Tony Rothman](#)

New York University

70 PUBLICATIONS 589 CITATIONS

[SEE PROFILE](#)

A reprint from

American Scientist

the magazine of Sigma Xi, The Scientific Research Honor Society

This reprint is provided for personal and noncommercial use. For any other use, please send a request to Permissions, American Scientist, P.O. Box 13975, Research Triangle Park, NC, 27709, U.S.A., or by electronic mail to perms@amsci.org. ©Sigma Xi, The Scientific Research Honor Society and other rightsholders

Random Paths to Frequency Hopping

Actress Hedy Lamarr famously co-patented a widely used secure-communication technology, but popular accounts ignore her many predecessors.

Tony Rothman

In an age when we ought to know better, the public perception of the evolution of science and technology retains the flavor of old just-so stories. In these tales, great discoveries or inventions are typically made by a single person. The hero, often an outsider working in splendid isolation, experiences a cinematic eureka moment when everything becomes blindingly clear. History is forever altered, and on we go until the next pivotal genius appears.

The truth is generally the opposite: Those who work in science and technology see that ideas are not unique; every conceivable approach to an outstanding problem is attempted by the community; contributions flow from every quarter; progress takes place incrementally; and multiple researchers inevitably hit on the same idea, producing discoveries that are simultaneous or nearly so. Assignment of credit is rarely clear-cut or generously inclusive. The old adage that “every discovery is named for the last person who discovered it” strikes closer to the mark than we might like to admit. Who receives acclaim depends, too, on whose story serves political interests, fits a convenient cultural narrative, or simply registers as sufficiently sensational.

An archetypal case is the invention of radio. To American—and Italian—schoolchildren, Guglielmo Marconi was the responsible party. In England, Oliver Lodge is accorded precedence; in Russia, Alexander Stepanovich Popov; in India, Jagdish Chandra Bose.

*Tony Rothman is a cosmologist in the department of applied physics at New York University Tandon School of Engineering. He is a coadjutor of *Les Amis de George Antheil*. He once wrote a play about Hedy Lamarr and George Antheil, but he attempts to distinguish fantasy from reality. Email: tonyrothman@gmail.com*

In New Zealand, credit mostly goes to Ernest Rutherford. None of these answers is wrong, exactly, but neither is any one of them exclusively right. All of these inventors created comparable devices within about a year of 1894.

Recently, attempts to address historical slights have lapsed instead into another kind of just-so story. Over the past two decades it has become standard, even fashionable, to credit the invention of Wi-Fi, Bluetooth, and even cell phones to 1940s movie star Hedy Lamarr. The story is appealing and exotic: Lamarr, an intelligent woman and amateur inventor, was shoehorned into a Hollywood culture that valued her as a screen siren and nothing more. Since a Google doodle was devoted to the actress in 2015 and *Bombshell*, a documentary about her, was released in 2017, the popular history has become chiseled in marble—well, let us say, arrayed in bits.

It is true that Lamarr and her unlikely partner, the radical modernist composer George Antheil, hold a patent for an important radio-transmission method that finds its way into several modern communications technologies, including Bluetooth. But it is equally true that their patent was hardly the first in this area. It is further true that the earliest operational systems employing this technique were created after World War II independently of their patent, and the essential idea can be traced back nearly to the birth of radio itself. If Lamarr and Antheil’s attorneys had performed a more diligent patent search, different doodles might well have graced Google.

The Actress and the Composer

The tale of Hedy and George might have been written by Arthur Conan Doyle, or even Graham Greene. Briefly: At an early age Hedy Lamarr, born Hedwig Kiesler in Austria, married Fritz Mandl,

a Nazi sympathizer and Austria’s leading munitions manufacturer, on the eve of World War II. Lamarr escaped this unhappy union (as she tells it, disguised as a maid whom she had drugged) and soon after ended up in Hollywood. Through a mutual interest in the obscure field of applied endocrinology, she met George Antheil. Revealing that she possessed a flair for inventing weapons, Hedy shared with him an idea for a secure torpedo guidance system that employed a novel technique known as *frequency hopping*.

Frequency hopping is the simplest version of a radio transmission technique today known as *spread-spectrum technique*, which refers to any method that widens the frequency band of a signal. Normally, radio stations broadcast on a single carrier frequency, which makes eavesdropping deliberately easy: You tune your radio to the correct frequency and receive the programming. By contrast, frequency hopping prevents the interception and decipherment of a transmission by shifting the carrier frequency in a predetermined, usually pseudorandom fashion—in other words, in a way that appears random but is produced by a deterministic algorithm. A receiver hopping around in synchrony with the transmitter can pick up the message, but an eavesdropper tuned to a single frequency will hear only a blip as that bit of message flashes by. Frequency hopping is largely jam-proof as well. If the frequencies are spaced widely enough, any jam-

Actress Hedy Lamarr (bottom) and composer George Antheil (top left) patented a form of frequency hopping for secure communication. Popular articles have spread awareness of their efforts but have tended to overlook many other important contributors, from cryptographer Gilbert Vernam (top) to Bluetooth inventor Jaap Haartsen (middle right).

illustration: Barbara Aulicino; Images: ahistoryblog.com/Bruce Ware Allen; © Union européenne 2012/EC Service Audiovisuel/Christoph Boeckheler; U.S. Patent Office; Pictorial Press Ltd/Alamy

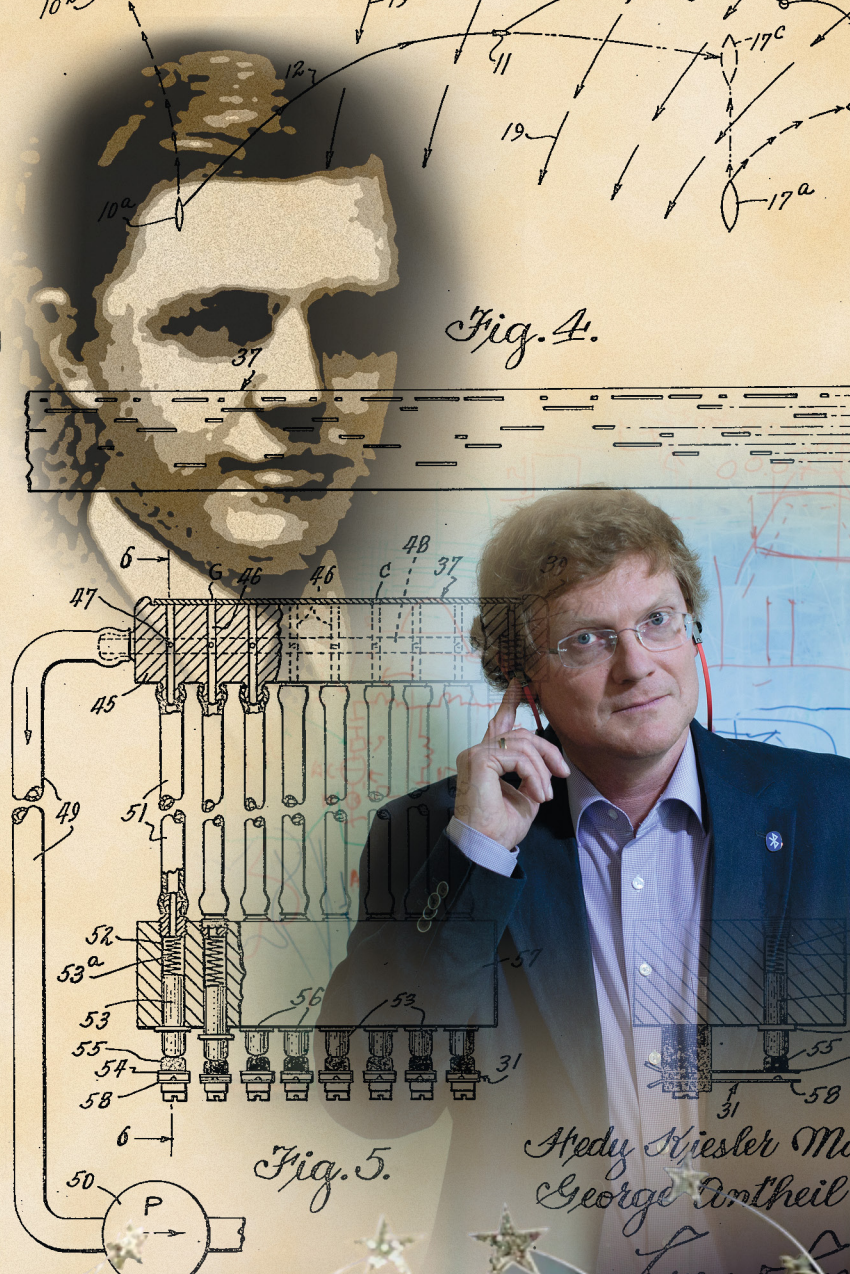
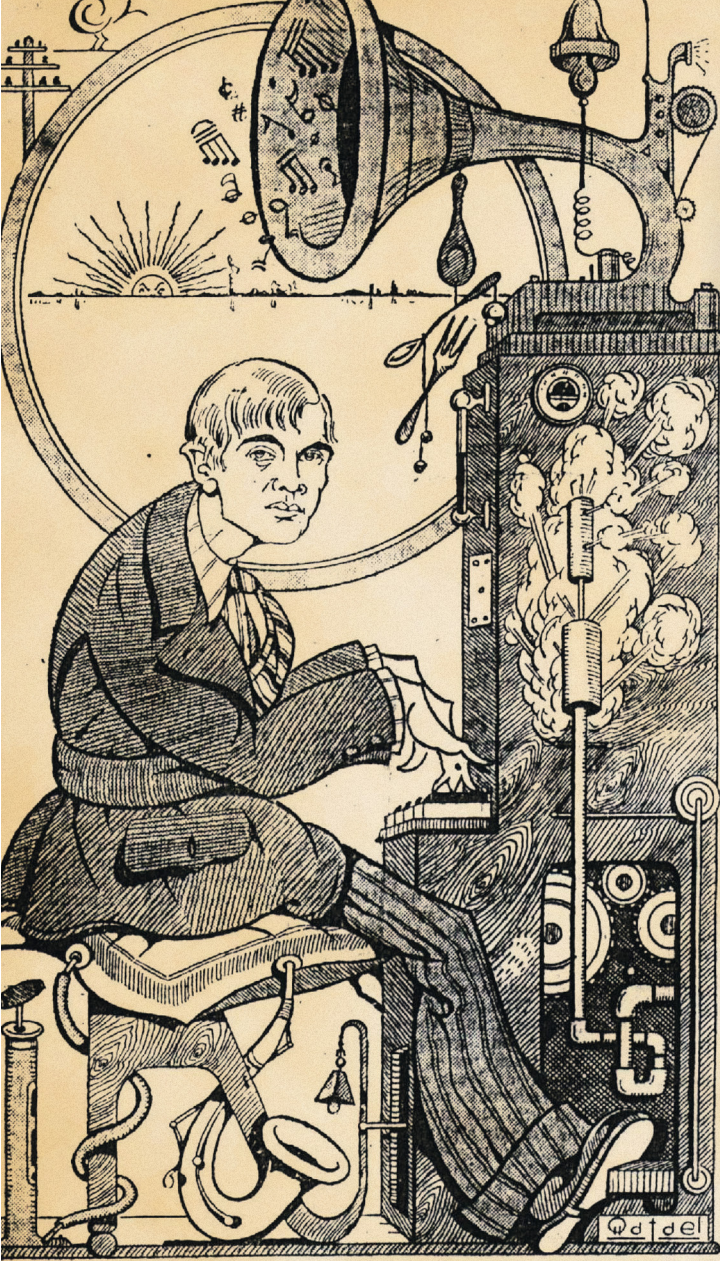


Fig. 4.



Fig. 5.

*Hedy Kiesler M...
George Antheil
Lyon...*

WESTERN EUROPE EDITION
THE STARS AND STRIPES
 Unofficial Newspaper of U.S. Forces in the European Theater
 Vol. 2—No. 128 1 Fr. Monday

Hedy Adds New Twist



Actress Invents Control Device With Torpedo Idea, Has Patent

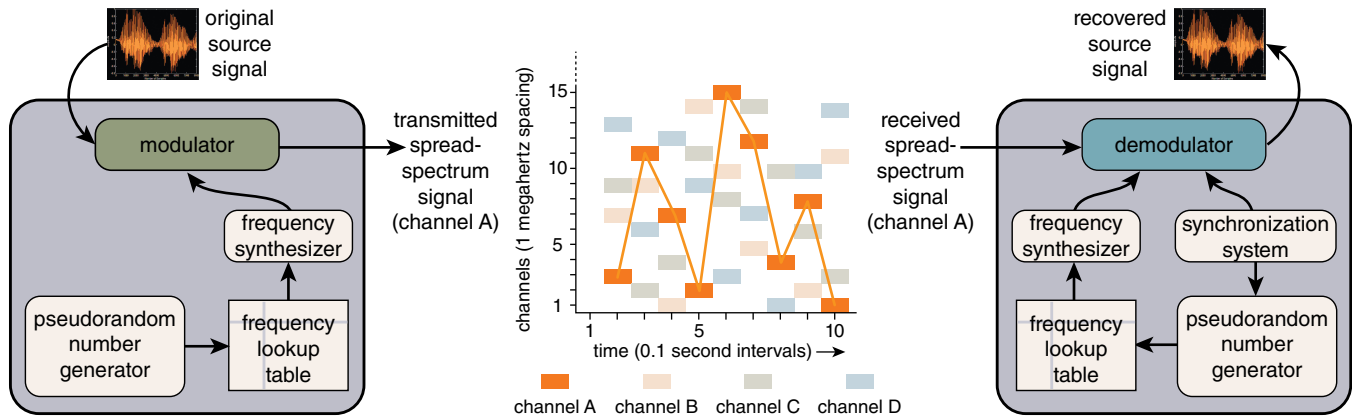
HOLLYWOOD, Nov. 18 (AP).—It could not have been a press agent's stunt, because the timing was too perfect, but the report from London that film actress Hedy Lamarr had patented a radio steering device for torpedoes at least had a patent to back it up.

In an interview, Hedy modestly admitted she did only "creative work" on the device. She said she and composer George Antheil "did the really important chemical part."

...ter...
 CHASER...
 over...
 way...
 my...
 of some way to get the balance for the British. A radio controlled torpedo. I thought would do it."
 Hedy asserted that the "control" device works on aerial as well as submarine torpedoes.

She said it works on anything...
 She said it works on anything...
 planning the invention and watching them pick, sort and put together all the little hinged pieces...





In frequency hopping, a source signal is sampled at short time intervals; each interval is modulated with a different frequency that is selected using a pseudorandom number generator (left). The unpredictable hops in frequency (center) make the message difficult to intercept and allow the transmission of overlapping channels. The receiver (right) reverses the randomly generated frequency shifts, using synchronization signals exchanged with the transmitter, and retrieves the original signal. (Information provided by Glenn Babecki.)

ming signal will interfere with only a small part of the message.

Trained as an actress, Hedy lacked the technical expertise to put her idea into practice. George was likewise no engineer, but two decades earlier he had written a concert piece, the notorious *Ballet Mécanique*, which included parts for synchronized player pianos. That background instantly triggered a thought: He would place a player-piano roll punched with 88 rows of randomly placed perforations in the transmitter to control the hopping among 88 radio frequencies; he would place an identical roll in the receiver; and then he would synchronize the two. Why 88? That's the number of keys on a piano.

An invention notebook in George's handwriting reveals that he was influenced by Philco's 1939 Mystery Control, the first commercially available radio remote controller. With the help of Samuel Mackowen, a California Institute of Technology engineer, George ironed out the bugs in their invention, and he and Hedy applied for a patent in June 1941. Considering the familiarity with patent conventions and technical radio concepts on display, it seems likely that Mackowen wrote the patent itself. On August 11, 1942, Lamarr and Antheil received U.S. Patent 2,292,387 (issued to Lamarr under her married name, Hedy Markey) for a "secret communication system."

Despite the novelty of their approach, the pneumatic player-piano mechanism made their system unwieldy—and certainly unworkable in battle. Antheil made strenuous lobbying efforts to get the invention adopted by the Navy, but

it was shelved. According to George, the Navy brass thought he wanted to put a player piano in a torpedo. Nevertheless, one frequently encounters claims (for instance, in Richard Rhodes's 2011 book *Hedy's Folly*) that because of its military potential, the Lamarr-Antheil patent was classified by the Navy. Although it adds to the story's drama, that detail does not appear to be true.

The authors of the *Spread Spectrum Communications Handbook* state that the patent was processed routinely with no imposition of secrecy. A tiny *New York Times* notice dated October 1, 1941, did report that the National Inventors Council "classed Miss Lamarr's invention in the 'red-hot' category," but two days later Lamarr and Antheil's patent attorneys, Lyon and Lyon, wrote a letter (provided to me by Antheil scholar Mauro Piccinini) to their clients making a contrary claim:

We noticed considerable publicity to the papers recently resulting from statements of Col. Lent of the National Inventors Council. This publicity is rather puzzling in view of the fact that the Patent Office has not issued a Secrecy Order. It is also difficult to understand why the Secrecy Order has not been issued in view of the fact that the Examiner has found nothing antedating the invention.

George himself apparently didn't believe the invention was classified: He gives the patent number in his 1945 autobiography *Bad Boy of Music* and is under the impression that anybody can get a copy of the thing by mailing

10 cents to the Patent Office. In addition, in their letter Lyon and Lyon also expressed surprise that "the Patent Office did not discover more pertinent patents than those cited." That surprise turned out to be well-founded.

Claims and counterclaims have been made as to whether Lamarr originated the frequency-hopping scheme or learned of it in meetings at Fritz Mandl's firm, the Hirtenberger Patronenfabrik. In *Bad Boy*, George affirms that she got her education at those meetings, and although he is not exactly the world's most reliable memoirist, he could hardly have received the information from anyone but Hedy. Robert Price, an engineer at Massachusetts Institute of Technology's Lincoln Laboratory and a pioneer of spread-spectrum technology, interviewed Lamarr. He told me that he came away convinced that she had heard the idea in her husband's boardroom, and with tongue somewhat planted in cheek, Price called her "the Mata Hari of World War II." Still, one must be mindful of historical gender roles—of how Lamarr might have presented herself as well as how her statements might have been received.

The notion that Lamarr's patent might have begun with an idea she heard from her former husband's colleagues is dismissed in the documentary *Bombshell*, where the filmmakers claim that German engineers at the time were unaware of the technology. However, Hans-Joachim Braun, whose 1997 article in *American Heritage of Invention and Technology* spurred the original interest in Lamarr's role as an inventor, informed me that documentary evidence in the Bundesarchiv-Militärarchiv in Freiburg shows that German engineers before World War II were aware of frequency hopping, although they lacked the means to put it into practice.

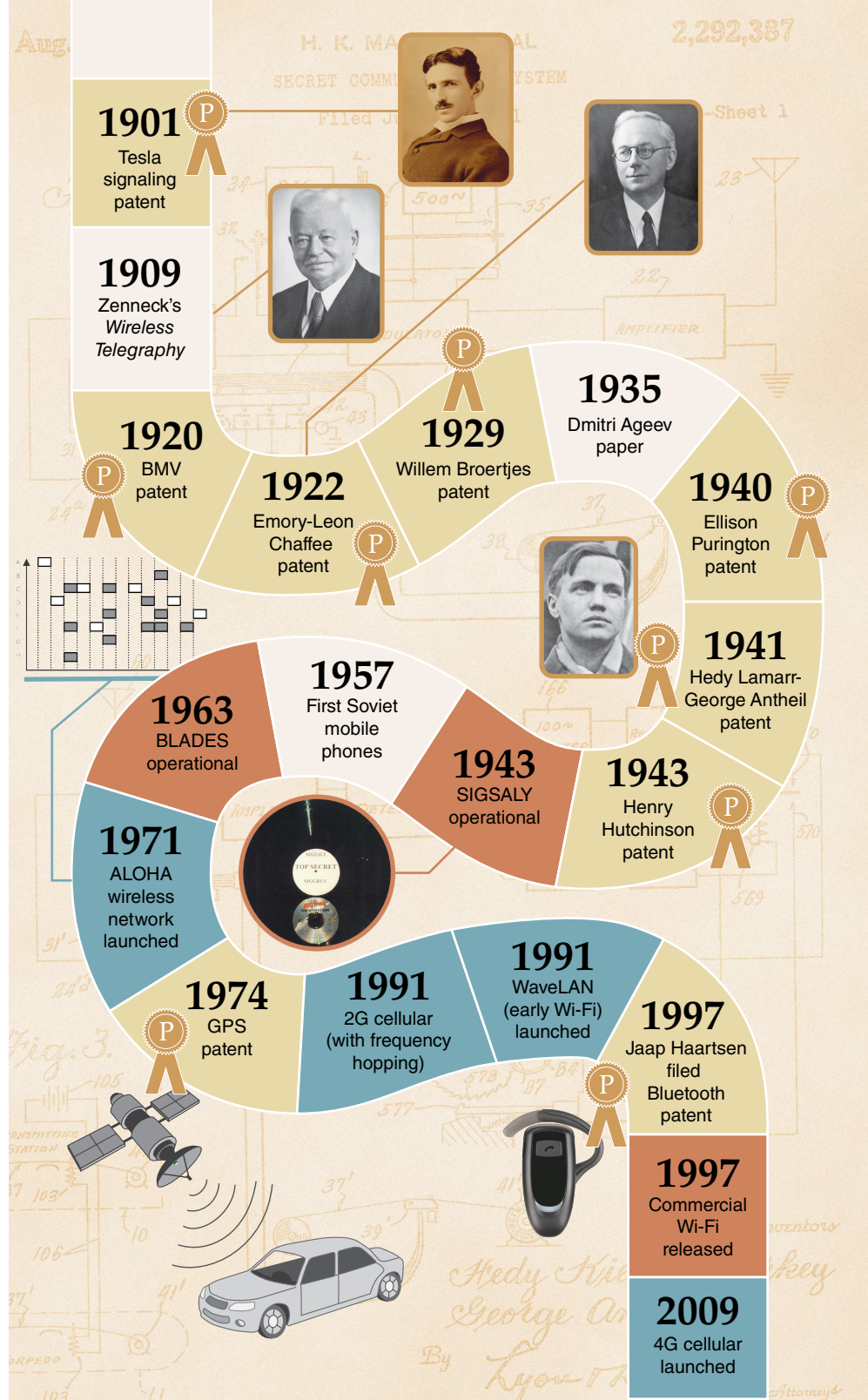
Great Minds Think Alike

At any rate, Hedy and George were hardly alone. In September 1940—a year before Lamarr and Antheil filed their patent application—Ellison Purington, who had done graduate work in physics at Harvard University and had worked on torpedo guidance systems at the Hammond Laboratory during World War I, filed an application for a “System for Reducing Interference.” In this patent (U.S. Patent 2,294,129), granted in 1942, Purington proposes “wobbling” the carrier frequency to reduce the ability of other transmitters to interfere with the signal. There seems to be no substantial difference between Purington’s frequency wobbling and Lamarr’s frequency hopping, except that frequency-hopping systems hop over a much wider bandwidth than Purington envisioned.

Purington’s eureka wasn’t the only one. In January 1943, five months after Lamarr and Antheil received their patent, U.S. Army Signal Corps officer Henry Hutchinson applied for a “speech privacy apparatus” relating to a “means of maintaining secrecy in communication, particularly in telephone circuits.” Like the Lamarr-Antheil patent, Hutchinson’s employed frequency hopping; instead of player-piano rolls, his scheme utilized cryptographic machines to produce a pseudorandom hopping sequence on demand. In this case, the application *was* held under a secrecy order until 1950, when Hutchinson was awarded U.S. Patent 2,495,727.

In an unusually noble act for the time, Hutchinson listed a dozen previous patents for secret communication systems dating back to the 1920s. Virtually all of them had emerged from Western Electric, the American Telephone and Telegraph Company (AT&T), or Bell Labs—the third having been formed in 1925 as a result of the consolidation of the first two. A number of the authors, including well-known pioneers of communications Harry Nyquist and Ralph Hartley, later participated in the top-secret Project X during World War II. Declassified patents from Project X also reveal a few additional pieces of prior art from the 1920s and 1930s. Glenn Babecki, an electrical engineer, and I have examined these early patents.

Every one of them proposes ensuring the secrecy of a message by hopping unpredictably among a group of low-frequency audio channels. In the majority of patents, the scrambled message



More than a century separates Nikola Tesla’s frequency-based “method of signaling” from today’s widely used spread-spectrum data transmissions. The researchers and inventions listed here are just highlights of a story that defies simple narratives. Even well-formed concepts often follow convoluted paths to implementation: Roger Easton’s key patent for GPS (“Navigation system using satellites and passive ranging techniques”) was granted a full 45 years ago.

is then transmitted by telephone line or radio along a single high-frequency carrier wave, making the system secure but not jam proof. Because the carrier wave is held at a constant frequency, we would probably not refer to this group

of patents as frequency-hopping patents in the modern sense. On the other hand, Hutchinson’s list reveals that in 1940 Purington had already received a patent (U.S. Patent 2,204,050) for a secrecy scheme that incorporates the frequency-

wobbling concept and so could be called frequency hopping. An even earlier Purlington patent (U.S. Patent 1,992,441, from 1935, overlooked by Hutchinson) also utilizes frequency wobbling.

Despite his honorable intentions, Hutchinson missed the proposal of Dutch inventor Willem Broertjes, who on October 11, 1929, submitted a patent application in Germany for a “Method of Maintaining Secrecy in the Transmission of Wireless Telegraph Messages.” A month later Broertjes filed an application in America, and in 1932 he was awarded U.S. Patent 1,869,659. In it, he writes that

The known methods of maintaining secrecy operate, in most cases, with codes or cryptograms and with a periodically modified transmission frequency, which is received by means of a receiving apparatus, the tuning of which is modified in synchronism.

According to Broertjes, then, the idea of changing transmission frequencies is already commonplace, but he argues that this approach does not prevent the interception and decipherment of the message, because a broadband receiver could pick up all the frequencies. As Lamarr and Antheil did later, Broertjes then proposes a system in which a number of “working frequencies,” known to the sender and receiver alone, can be varied in a “random or variable manner,” or even left out. “In a method of this kind,” he writes,

secrecy is ensured by reason of the fact that an unauthorized receiver which at first, is tuned in to only a single frequency length,

picks up only disconnected portions of the message.

The Broertjes patent can be faulted in that the operation of the receiving mechanism is left largely as an exercise for the reader. The transmitter includes a “code wheel” that selects a new frequency each time a telegraph key is depressed. One can only assume that the receiver contains a duplicate wheel, but Broertjes prefers manual operation, so it remains unclear how he intends synchronization to be effected. Despite its flaws, Broertjes’s invention proves that the frequency-hopping concept was available in Germany well before the war.

But the fundamental law of invention and discovery is the “infinite chain of priority,” which ensures that someone else always did it first. In this case, the chain included Emory-Leon Chaffee, a Harvard University physicist who had worked with Purlington at Hammond Laboratory. In an application filed in 1922 but granted only in 1927 (U.S. Patent 1,642,663), Chaffee describes a “System of Radiocommunication” that proposes wobbling the carrier frequency in an “erratic manner” in order to provide secrecy.

Nor do the antecedents end here. Chaffee was beaten to the punch by another AT&T team, consisting of Otto B. Blackwell, De Loss K. Martin, and Gilbert S. Vernam, whose proposal not only predates all those on Hutchinson’s list, but also anticipates many features of the Broertjes and the Lamarr-Antheil inventions as well. On December 18, 1920, the team filed an application for a “Secrecy Communication System,” which was

finally granted U.S. Patent 1,598,673 on September 7, 1926. The authors write:

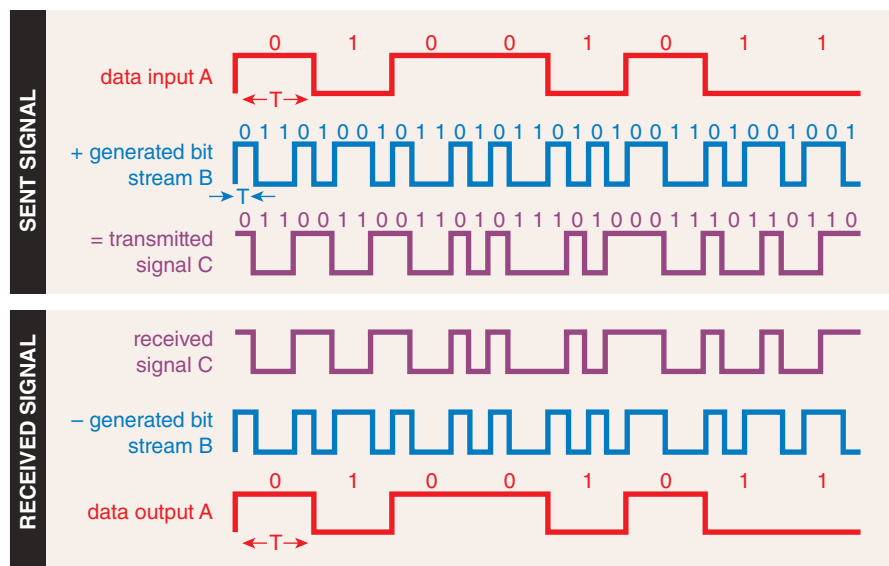
Heretofore in certain types of signaling systems, in which a high frequency wave is utilized as the agency of transmitting the signals, the signals have been transmitted by electromagnetic waves of a definite high frequency or wave length and any station tuned to said wave length might be capable of receiving said signals. In the present invention secrecy is obtained by the transmission of signals on a plurality of waves of different frequencies, successive portions of a message being transmitted on waves of different frequencies whereby a station tuned to one of said waves receives only a partial and therefore unintelligible disclosure of the communication.

The authors go on to say that the frequency shifting is “not accomplished in a cyclic order but rather in a random and variable manner.” Anticipating Antheil’s player-piano rolls, the team members employ perforated telegraph tape with randomly punched holes to control the frequency hopping. From a technical standpoint, their electronic implementation is superior to the Lamarr-Antheil version in all respects, and is superior to the other Bell Labs patents as well.

Infinite Regression

At first glance, the patent of Blackwell, Martin, and Vernam appears to nail down the origin of frequency hopping, but the devil lies in the details. Like most of the later Bell Labs inventors, the authors evidently intended to transmit the message across a telephone line after randomly scrambling the audio frequencies to unspecified “higher” carrier frequencies. That approach implies a narrow transmission band. They do state that radio transmission would work equally well, but they do not make clear whether that additional carrier would also hop frequencies. Their patent therefore seems to repre-

Direct-sequencing is another form of frequency hopping, used in modern cordless phones, Wi-Fi, and the Global Positioning System (GPS). For transmission (top), it merges a sent-data input (A) with a high data-rate bitstream (B) to produce a new signal (C) that is highly resistant to both jamming and interference. At the receiving end, the bitstream is removed, or demodulated, to recover the original data input (bottom).



sent audio frequency hopping, but not radio frequency hopping. Interestingly, none of the later patents cite this one or Chaffee's; whether this was the result of a simple oversight or some weightier consideration remains a mystery.

The relative sophistication of the Blackwell, Martin, and Vernam patent

is unclear whether any aspects of the Blackwell, Martin, and Vernam patent

The interception of messages by stations other than those called, can be prevented to some extent by telegraphing so rapidly that such relays as are customarily used will not respond and only specially trained operators will be able to read the messages in the telephone. Furthermore, the apparatus can be so arranged that the wave-length is easily and rapidly changed and then vary the wave-length in accordance with a prearranged program, perhaps automatically. This method makes it very difficult for an uncalled listener to tune his receiver to the rapid variations, but it is of no avail against untuned, highly sensitive receivers.

The fundamental law of invention is the infinite chain of priority: Someone else always did it first.

compared with its successors demonstrates that technology does not always progress smoothly. It also illuminates the difference between a patent produced by amateurs and one produced by professionals. In 1919, Vernam had patented what has become known as the Vernam Cipher, in which a plaintext message is mixed with a random stream of characters to provide a coded message. It was the electronic implementation of the "one-time pad" (a message key used once and destroyed), which renowned information theorist Claude Shannon of Bell Labs later proved to be unbreakable.

Vernam's 1919 patent (U.S. Patent 1,310,719) is widely considered to be one of the most important in the history of cryptography, so it comes as no sur-

prised that within a year he participated in the invention of a secure transmission system. Later, in one of the most secret projects of World War II, the U.S. military developed Project X, the first uncrackable communications system.

It is unclear whether any aspects of the Blackwell, Martin, and Vernam patent ideas on cryptography certainly did. In the Blackwell, Martin, and Vernam patent we see the concept of frequency hopping partly realized, but the endless chain of priority ensures that, yes, the germ of the idea had appeared earlier still. Jonathan Zenneck was an early German radio pioneer who was held during World War I as an enemy alien in the United States, which he happened to be visiting at the war's outbreak. His *Wireless Telegraphy*, the standard textbook on the subject for many years, appeared in Germany in 1909 and in English translation in 1915. In a chapter on receivers, Zenneck discusses varying the wavelength of messages:

Zenneck does not mention that for full secrecy the wavelengths should be shifted in an unpredictable manner, but otherwise the proposal is for frequency hopping in the modern sense. He adds in a footnote that "This method was adapted by the Telefunken Co. at one time," showing that the core principle was applied as early as the opening of the 20th century.

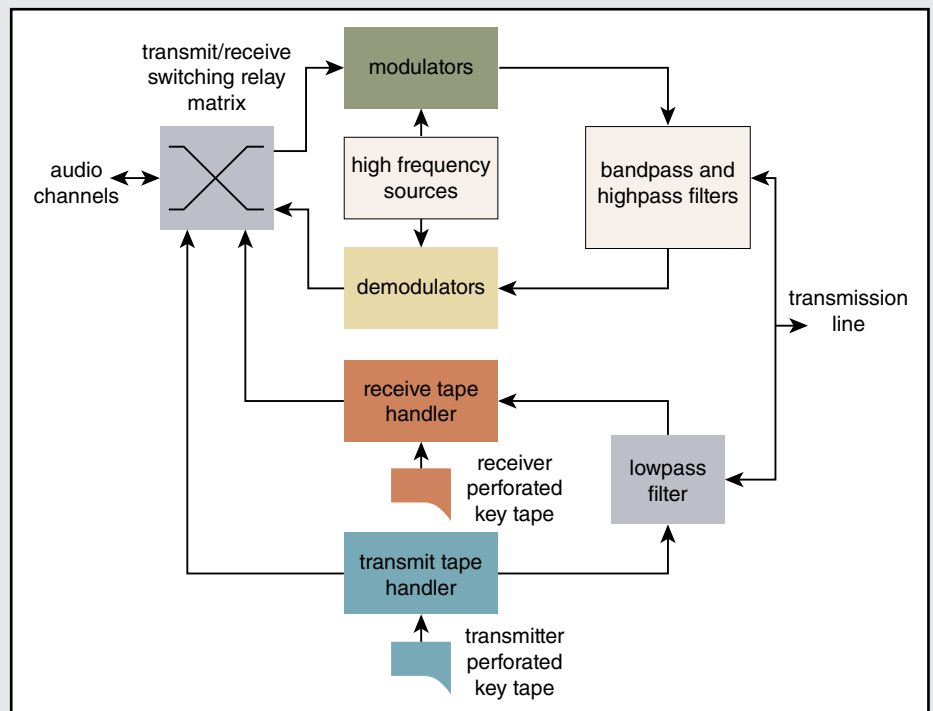
Yet even Zenneck's book is not the technology's *urtext*. Given that Nikola Tesla's obsessive fans have credited him with inventing the radio, the laser, the electron microscope, and the atomic bomb, it would be almost surprising if he hadn't invented frequency hopping,

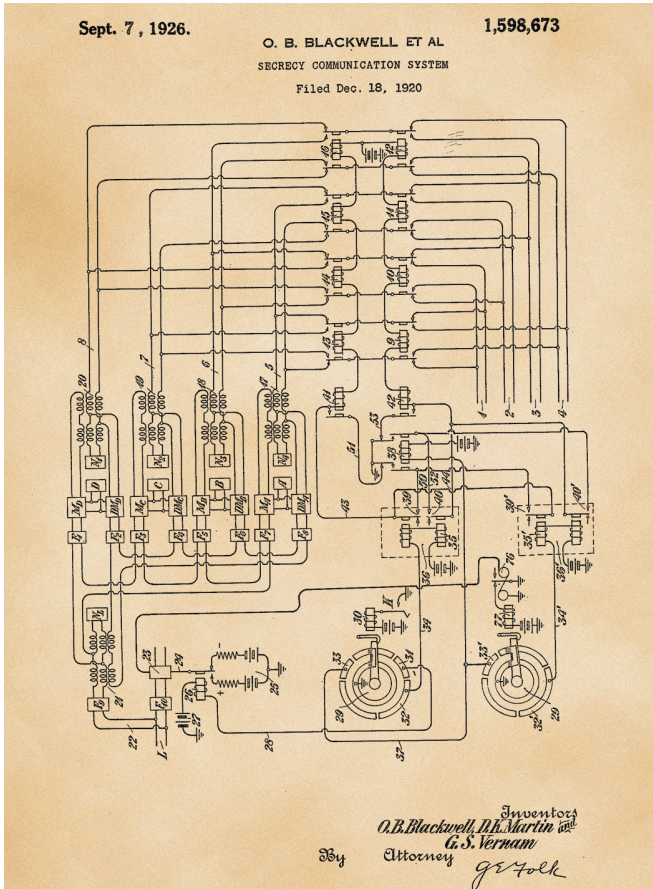
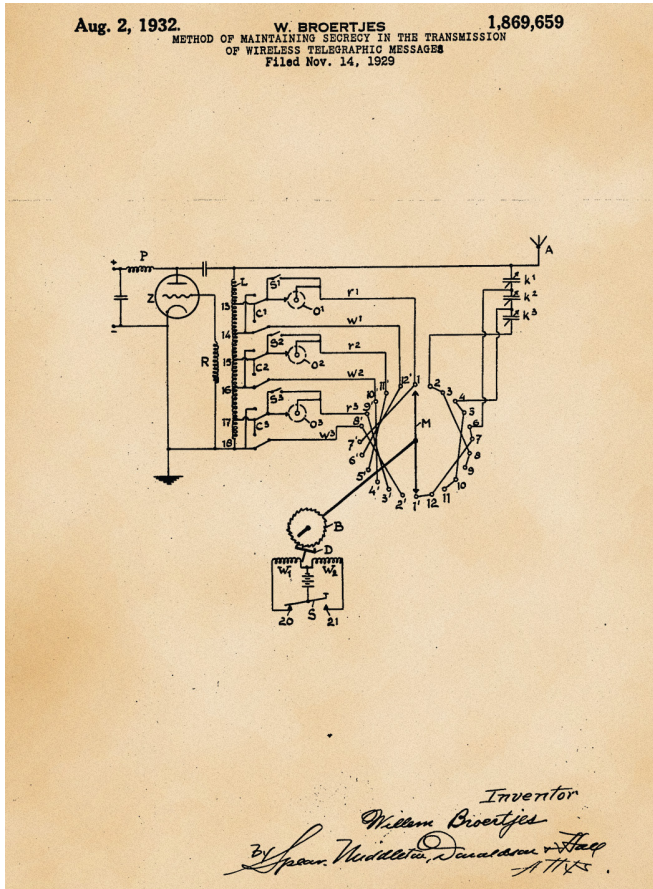
Barbara Aulicino

First Frequency Hopper?

A block diagram illustrates the primary components of the "Secrecy Communication System"—a direct predecessor to frequency hopping—patented by Otto Blackwell, De Loss Martin, and Gilbert Vernam. Audio channels (the original message) are shifted in a pseudorandom sequence to higher frequencies by a switching matrix according to a pattern encoded in a perforated telegraph tape and sent via a tape transmitter. The higher frequencies are combined with carrier frequencies in the modulators; the modulated signals are separated by band-pass filters, then transmitted.

The receiver is basically a mirror image of the transmitter: It demodulates the incoming signals, down-converting them to their original frequencies according to the switching pattern in the telegraph tape, to recover the message.





Dutch inventor Willem Broertjes described a form of frequency hopping for secure communication in a patent (left) filed in 1929, a dozen years before Hedy Lamarr and George Antheil filed. In 1920 American Telephone and Telegraph researchers Otto Blackwell, De Loss Martin, and Gilbert Vernam patented a system (right) that anticipated pivotal aspects of later frequency-hopping schemes, including changing frequencies by punching random holes in a telegraph tape.

too. Here, Tesla might even have a legitimate claim. In U.S. Patent 723,188 (applied for in 1901, granted in 1903), he considers a “Method of Signaling” that consists of two or more transmitters operating on different frequencies. The receiver is designed to respond only when both signals are received.

Tesla’s language is obscure, but his essential idea is the familiar one that by varying the frequencies in a predetermined pattern, only the desired receiver will be able to detect the transmitted message. Here the chain of priority at last fades out, for if one goes much earlier, the concept of radio itself had yet to be born.

The Randomness of History

No history of invention will ever be complete. In a seminal 1982 article on the history of spread-spectrum communications, electrical engineer Robert Scholtz of the University of Southern California cites several hundred contributions to the technology’s development. Never-

theless he overlooked some, including the Lamarr-Antheil patent and the other early patents discussed here. The 1994 *Spread Spectrum Communications Handbook*, by Marvin Simon, Jim Omura, Robert Scholtz, and Barry Levitt, awards Lamarr and Antheil their due prominence but still misses others. At the other extreme, *Bombshell* fails to mention any of Lamarr and Antheil’s predecessors.

Any approach to the history of science and technology that aggrandizes lone inventors is largely static: Beyond the snapshots of inspirational eureka moments, nothing much happens. Borrowing a metaphor from biology, we might call this view “extreme punctuated equilibrium.” Between disruptive interventions of genius, scientific progress grinds to a halt.

Yet surely in science and technology the protagonists should be the ideas themselves. The essential lessons—and excitement—from the history of science derive from observing the evolution of an idea, from its nebulous

birth to the time at which it condenses into recognizable form. Ideas, in a real sense, have a life of their own. In science, if you don’t think of something, someone else will, and in nearly the same words, as the frequency-hopping patents amply demonstrate.

If ideas are born of necessity, then the mother of secret communications has been war. Most of the research into spread-spectrum transmission took place in anticipation of war, or during war itself. By some estimates, during World War II as many as 90 percent of German electronics engineers were involved in the country’s (ultimately unsuccessful) anti-jamming campaign. Under such circumstances, the invention of frequency hopping was not just probable, it was inevitable.

Tracing the development of a technology such as frequency hopping in an evolutionary fashion is not easy. History begins to vanish the moment a blackboard is erased. In this case, not only were numerous patents overlooked, but much of the work was classified, leaving gaps in the historical record and resulting in repeated, near-duplicate inventions. At about the time Lamarr and Antheil were finalizing their ideas, the U.S. Army Signal Corps

commissioned Bell Labs engineers to begin work on Project X, also known by its code name, SIGSALY. Based on the labs' earlier vocoder (voice encoder) system, SIGSALY went online in 1943, ultimately carrying encrypted voice communications between U.S. President Franklin D. Roosevelt and British Prime Minister Winston Churchill.

SIGSALY became the first completely uncrackable secret communications system. It digitized the voices of the interlocutors and then scrambled their

hopping systems put into practice after World War II all derived from the Lamarr-Antheil patent. Reality is neither so simple nor so linear. The handful of available patents that provide the basis for BLADES's operation make no mention of the Lamarr-Antheil patent. The ideas prevailed, not the individuals.

Shadows of Invention

Although the spread-spectrum approach is now ubiquitous in commercial communications, tracking its

of the Soviet Union, Western researchers had little idea of what was going on there, but that hardly means that Soviet scientists were idle. In 1935, a Russian communications engineer named Dmitri Vasilievich Ageev published a paper titled "Principles of the Theory of Linear Selection," which lays down the mathematical basics of spread-spectrum techniques. There may well be other Soviet contributions that have not yet come to light, but we do know that as early as 1957, prototype mobile phones, evidently based on Ageev's ideas, were operational in Moscow.

So long as large swaths of technological research take place under secrecy, redundancy and inefficiency will remain facts of life. As a former National Security Agency employee once remarked to me, "The military usually develops an idea 10 years before the civilian sector." To the extent that the comment was not an idle boast, it does suggest considerable hidden and wasted intellectual resources. Private corporations, too, guard their secrets, fueling duplication of effort, even as cutthroat competition engenders horse-trading that allegedly keeps consumer prices down.

As a rule, scientists engaged in fundamental research would rather do something novel themselves than try to duplicate someone else's results, which only adds to the noise. In that regard, the overwhelming concentration of talent at the old Bell Labs had its advantages. It may be too much to hope that a new system can be devised to streamline the chaos. Failing that, one can at least take solace from knowing that recognition for one's accomplishments depends largely on the diligence of the patent search, and that the march of ideas will continue regardless of who gets the credit.

If ideas are born of necessity, then the mother of secret communication has been war.

amplitudes according to one-time pads, which in this case were vinyl recordings that sampled the randomly fluctuating brightness of mercury-vapor lamps. These vinyls—cousins of Antheil's player-piano rolls—were shipped to Washington and London, where turntables tuned to the National Bureau of Standards timing signal started up at the same instant. After a single use, the vinyls were destroyed.

Because SIGSALY scrambled voice amplitudes rather than frequencies, it was not *de jure* frequency hopping. Then again, because transmission of the radio signals involved frequency modulation, the random amplitudes got scrambled to random frequencies, making it a *de facto* frequency-hopping scheme. To this day SIGSALY is little known to the public, surely because many of its innovations remained classified until 1976.

During the postwar era, another major effort at developing a secure, jam-proof system was put forth by Sylvania with its Buffalo Laboratories Application of Digitally Exact Spectra, or BLADES, which began in 1955 as system for communicating with Polaris submarines. It was tested by 1957 and in 1963 it was installed on the flagship U.S.S. Mount McKinley, where it successfully thwarted intentional jamming efforts. Evidently it was the earliest frequency-hopping system put into action. The details of BLADES are still murky, because it was (and perhaps remains) classified.

The secrecy surrounding BLADES and other military research has bolstered the story that early frequency-

provenance is no easy task. Bluetooth technology does employ frequency hopping, but its inventor, Jaap Haartsen, tells me that he was unaware of the Lamarr-Antheil patent when he was working on the system at Ericsson in the 1990s. Frequency hopping was merely the standard that the U.S. Federal Communications Commission (FCC) required on the frequency band he intended to use for an interference-proof local communication system.

Many recent articles cite Lamarr-Antheil's invention as having been vital to the development of modern Wi-Fi, but Haartsen also points out that Wi-Fi abandoned frequency hopping early on, because it provided insufficient bandwidth. For a time, Wi-Fi used a spread-spectrum technique known as *direct sequencing*, but since a change in FCC rules, it employs yet another type of spread-spectrum technology, *orthogonal frequency division multiplexing*. The Global Positioning System (GPS), another alleged part of Lamarr's legacy, has always used direct sequencing. Although the early 2G cellular network did use a form of frequency hopping, later networks have employed direct sequencing and orthogonal frequency division multiplexing. Any link to player pianos and torpedoes has yet to be demonstrated.

As with the history of radio, an unofficial form of classification has left its distorting stamp on the history of frequency hopping: nationalism. All of the patents discussed here are German or American, but surely that cannot represent the full reality. During the lifetime

Bibliography

- Scholtz, R. A. 1982. The origins of spread spectrum communications. *IEEE Communications Transactions* 30:822–854.
- Simon, M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt. 1994. *The Spread Spectrum Communications Handbook*. New York: McGraw-Hill.
- Rothman, T. 2003. *Everything's Relative and Other Fables from Science and Technology*. Hoboken, NJ: John Wiley and Sons.

For relevant Web links, consult this issue of *American Scientist Online*:

www.amsci.org/magazine/issues/2018/january-february



AHEAD OF WHAT'S POSSIBLE™

SEARCH

Company ▾ myAnalog ▾ Products ▾ Applications ▾ Design Center ▾ Education ▾ Support ▾

An Introduction to Spread-Spectrum Communications

Abstract

This application note is a tutorial overview of spread-spectrum principles. The discussion covers both direct-sequence and fast-hopping methods. Theoretical equations are given to allow performance estimates. Relation to CDMA and TDMA is provided. A schematic of a code sequence generator is shown. Spectral plots illustrate direct-sequence spread-spectrum (DSSS) and frequency-hopping spread-spectrum (FHSS) methods.

Introduction

As spread-spectrum techniques become increasingly popular, electrical engineers outside the field are eager for understandable explanations of the technology. There are books and websites on the subject, but many are hard to understand or describe some aspects while ignoring others (e.g., the DSSS technique with extensive focus on PRN-code generation).

The following discussion covers the full spectrum (pun intended).

A Short History

Spread-spectrum communications technology was first described on paper by an actress and a musician! In 1941 Hollywood actress Hedy Lamarr and pianist George Antheil described a secure radio link to control torpedoes. They received U.S. Patent #2.292.387. The technology was not taken seriously at that time by the U.S. Army and was forgotten until the 1980s, when it became active. Since then the technology has become increasingly popular for applications that involve radio links in hostile environments.

Typical applications for the resulting short-range data transceivers include satellite-positioning systems (GPS), 3G mobile telecommunications, W-LAN (IEEE® 802.11a, IEEE 802.11b, IEEE 802.11g), and Bluetooth®. Spread-spectrum techniques also aid in the endless race between communication needs and radio-frequency availability—situations where the radio spectrum is limited and is, therefore, an expensive resource.

Theoretical Justification for Spread Spectrum

Spread-spectrum is apparent in the Shannon and Hartley channel-capacity theorem:

$$C = B \times \log_2 (1 + S/N)$$

In this equation, C is the channel capacity in bits per second (bps), which is the maximum data rate for a theoretical bit-error rate (BER). B is the required channel bandwidth in Hz, and S/N is the signal-to-noise power ratio. To be more explicit, one assumes that C , which represents the amount of information allowed by the communication channel, also represents the desired performance. Bandwidth (B) is the price to be paid, because frequency is a limited resource. The S/N ratio expresses the environmental conditions or the physical characteristics (i.e., obstacles, presence of jammers, interferences, etc.).

There is an elegant interpretation of this equation, applicable for difficult environments, for example, when a low S/N ratio is caused by noise and interference. This approach says that one can maintain or even increase communication performance (high C) by allowing or injecting more bandwidth (high B), even when signal power is below the noise floor. (The equation does not forbid that condition!)

Modify Equation 1 by changing the log base from 2 to e (the Napierian number) and by noting that $\ln = \log_e$. Therefore:

$$C/B = (1/\ln 2) \times \ln(1 + S/N) = 1.443 \times \ln(1 + S/N)$$

Applying the MacLaurin series development for

$$\ln(1 + x) = x - x^2/2 + x^3/3 - x^4/4 + \dots + (-1)^{k+1}x^k/k + \dots$$

$$C/B = 1.443 \times (S/N - 1/2 \times (S/N)^2 + 1/3 \times (S/N)^3 - \dots)$$

S/N is usually low for spread-spectrum applications. (As just mentioned, the signal power density can even be below the noise level.) Assuming a noise level such that $S/N \ll 1$, Shannon's expression becomes simply:

$$C/B \approx 1.433 \times S/N$$

Very roughly:

$$C/B \approx S/N$$

Or:

$$N/S \approx B/C$$

To send error-free information for a given noise-to-signal ratio in the channel, therefore, one need only perform the fundamental spread-spectrum signal-spreading operation: increase the transmitted bandwidth. That principle seems simple and evident. Nonetheless, implementation is complex, mainly because spreading the baseband (by a factor that can be several orders of magnitude) forces the electronics to act and react accordingly, which, in turn, makes the spreading and despreading operations necessary.

Definitions

Different spread-spectrum techniques are available, but all have one idea in common: the key (also called the code or sequence) attached to the communication channel. The manner of inserting this code defines precisely the spread-spectrum technique. The term "spread spectrum" refers to the expansion of signal bandwidth, by several orders of magnitude in some cases, which occurs when a key is attached to the communication channel.

The formal definition of spread spectrum is more precise: an RF communications system in which the baseband signal bandwidth is intentionally spread over a larger bandwidth by injecting a higher frequency signal (Figure 1). As a direct consequence, energy used in transmitting the signal is spread over a wider

bandwidth, and appears as noise. The ratio (in dB) between the spread baseband and the original signal is called processing gain. Typical spread-spectrum processing gains run from 10dB to 60dB.

To apply a spread-spectrum technique, simply inject the corresponding spread-spectrum code somewhere in the transmitting chain before the antenna (receiver). (That injection is called the spreading operation.) The effect is to diffuse the information in a larger bandwidth. Conversely, you can remove the spread-spectrum code (called a despreading operation) at a point in the receive chain before data retrieval. A despreading operation reconstitutes the information into its original bandwidth. Obviously, the same code must be known in advance at both ends of the transmission channel. (In some circumstances, the code should be known only by those two parties.)

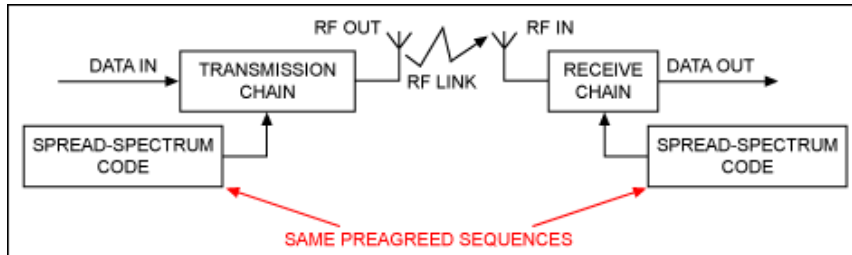


Figure 1. Spread-spectrum communication system.

Bandwidth Effects of the Spreading Operation

Figure 2 illustrates the evaluation of signal bandwidths in a communication link.

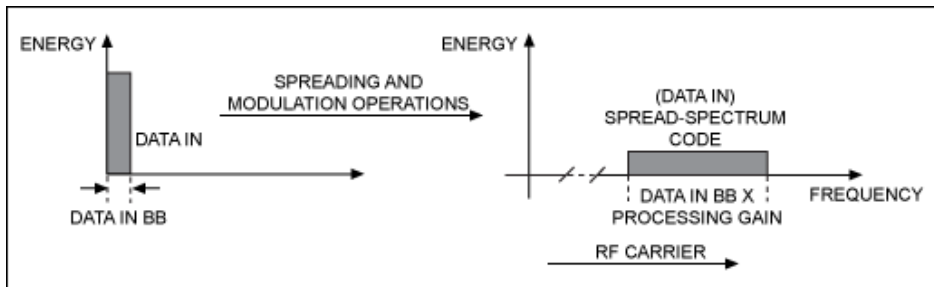


Figure 2. Spreading operation spreads the signal energy over a wider frequency bandwidth.

Spread-spectrum modulation is applied on top of a conventional modulation such as BPSK or direct conversion. One can demonstrate that all other signals not receiving the spread-spectrum code will remain as they are, that is, unspread.

Bandwidth Effects of the Despreading Operation

Similarly, despreading can be seen in Figure 3.

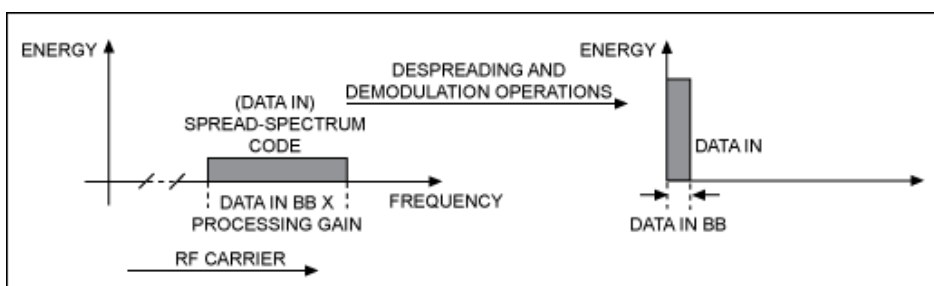


Figure 3. The despreading operation recovers the original signal.

Here a spread-spectrum demodulation has been made on top of the normal demodulation operations. One can also demonstrate that signals such as an interferer or jammer added during the transmission will be spread during the despreading operation!

Waste of Bandwidth Due to Spreading Is Offset by Multiple Users

Spreading results directly in the use of a wider frequency band by a factor that corresponds exactly to the "processing gain" mentioned earlier. Therefore spreading does not spare the limited frequency resource. That overuse is well compensated, however, by the possibility that many users will share the enlarged frequency band (Figure 4).

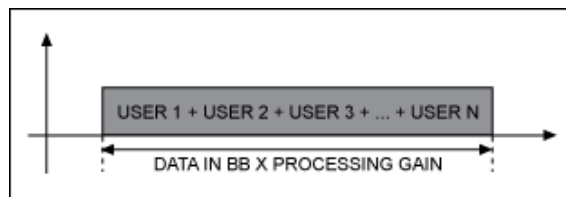


Figure 4. The same frequency band can be shared by multiple users with spread-spectrum techniques.

Spread Spectrum Is a Wideband Technology

In contrast to regular narrowband technology, the spread-spectrum process is a wideband technology. W-CDMA and UMTS, for example, are wideband technologies that require a relatively large frequency bandwidth, compared to narrowband radio.

Benefits of Spread Spectrum

Resistance to Interference and Antijamming Effects

There are many benefits to spread-spectrum technology. Resistance to interference is the most important advantage. Intentional or unintentional interference and jamming signals are rejected because they do not contain the spread-spectrum key. Only the desired signal, which has the key, will be seen at the receiver when the despreading operation is exercised. See Figure 5.

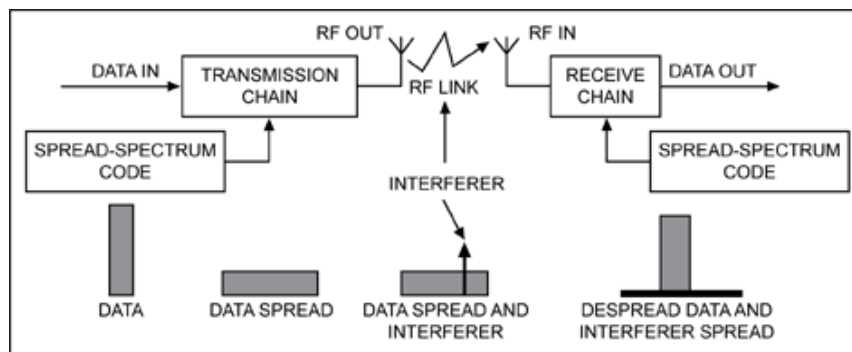


Figure 5. A spread-spectrum communication system. Note that the interferer's energy is spread while the data signal is despread in the receive chain

You can practically ignore the interference, narrowband or wideband, if it does not include the key used in the despreading operation. That rejection also applies to other spread-spectrum signals that do not have the right key. Thus different spread-spectrum communications can be active simultaneously in the same band, such as CDMA. Note that spread spectrum is a wideband technology, but the reverse is not true: wideband techniques need not involve spread-spectrum technology.

Resistance to Interception

Resistance to interception is the second advantage provided by spread-spectrum techniques. Because nonauthorized listeners do not have the key used to spread the original signal, those listeners cannot decode it. Without the right key, the spread-spectrum signal appears as noise or as an interferer. (Scanning methods can break the code, however, if the key is short.) Even better, signal levels can be below the noise floor, because the spreading operation reduces the spectral density. See Figure 6. (Total energy is the same, but it is widely spread in frequency.) The message is thus made invisible, an effect that is particularly strong with the direct-sequence spread-spectrum (DSSS) technique. (DSSS is discussed in greater detail below.) Other receivers cannot "see" the transmission; they only register a slight increase in the overall noise level!

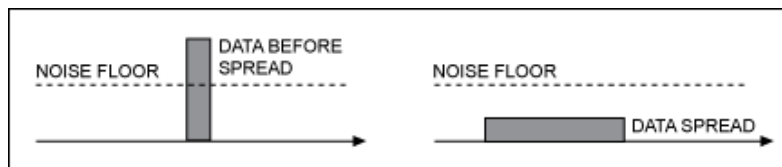


Figure 6. Spread-spectrum signal is buried under the noise level. The receiver cannot "see" the transmission without the right spread-spectrum keys.

Resistance to Fading (Multipath Effects)

Wireless channels often include multiple-path propagation in which the signal has more than one path from the transmitter to the receiver (Figure 7). Such multipaths can be caused by atmospheric reflection or refraction, and by reflection from the ground or from objects such as buildings.

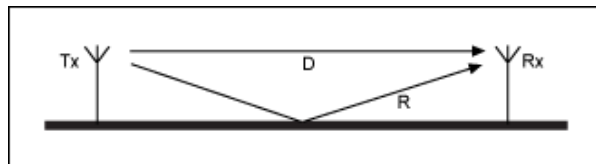


Figure 7. Illustration of how the signal can reach the receiver over multiple paths.

The reflected path (R) can interfere with the direct path (D) in a phenomenon called fading. Because the despreading process synchronizes to signal D, signal R is rejected even though it contains the same key. Methods are available to use the reflected-path signals by despreading them and adding the extracted results to the main one.

Spread Spectrum Allows CDMA

Note that spread spectrum is not a modulation scheme, and should not be confused with other types of modulation. One can, for example, use spread-spectrum techniques to transmit a signal modulated by FSK or BPSK. Thanks to the coding basis, spread spectrum can also be used as another method for implementing multiple access (i.e., the real or apparent coexistence of multiple and simultaneous communication links on the same physical media). So far, three main methods are available.

FDMA—Frequency Division Multiple Access

FDMA allocates a specific carrier frequency to a communication channel. The number of different users is limited to the number of "slices" in the frequency spectrum (Figure 8). Of the three methods for enabling multiple access, FDMA is the least efficient in term of frequency-band usage. Methods of FDMA access include radio broadcasting, TV, AMPS, and TETRAPOLE.

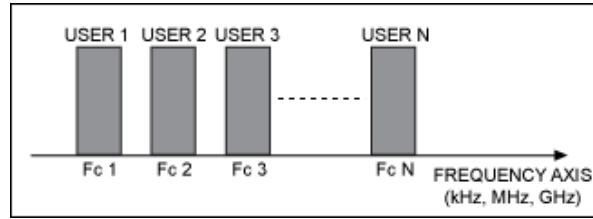


Figure 8. Carrier-frequency allocations among different users in a FDMA system.

TDMA—Time Division Multiple Access

With TDMA the different users speak and listen to each other according to a defined allocation of time slots (Figure 9). Different communication channels can then be established for a unique carrier frequency. Examples of TDMA are GSM, DECT, TETRA, and IS-136.

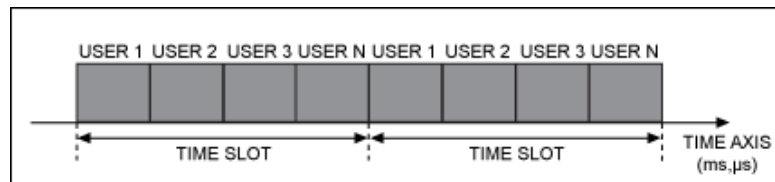


Figure 9. Time-slot allocations among different users in a TDMA system.

CDMA—Code Division Multiple Access

CDMA access to the air is determined by a key or code (Figure 10). In that sense, spread spectrum is a CDMA access. The key must be defined and known in advance at the transmitter and receiver ends. Growing examples are IS-95 (DS), IS-98, Bluetooth, and WLAN.

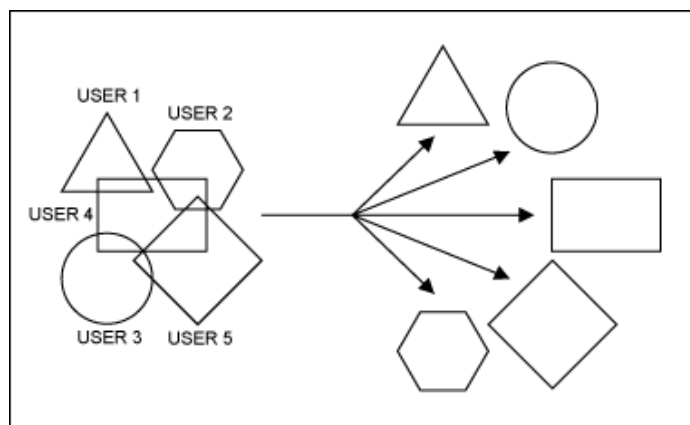


Figure 10. CDMA systems access the same frequency band with unique keys or codes.

One can, of course, combine the above access methods. GSM, for instance, combines TDMA and FDMA. GSM defines the topological areas (cells) with different carrier frequencies, and sets time slots within each cell.

Spread Spectrum and (De)coding "Keys"

At this point, it is worth restating that the main characteristic of spread spectrum is the presence of a code or key, which must be known in advance by the transmitter and receiver(s). In modern communications the codes are digital sequences that must be as long and as random as possible to appear as "noise-like" as possible. But in any case, the codes must remain reproducible, or the receiver cannot extract the message that has been sent. Thus, the sequence is "nearly random." Such a code is called a pseudo-random number (PRN) or sequence. The method most frequently used to generate pseudo-random codes is based on a feedback shift register.

One example of a PRN is shown in Figure 11. The shift register contains eight data flip-flops (FF). At the rising edge of the clock, the contents of the shift register are shifted one bit to the left. The data clocked in by FF1 depends on the contents fed back from FF8 and FF7. The PRN is read out from FF8. The contents of the FFs are reset at the beginning of each sequence length.

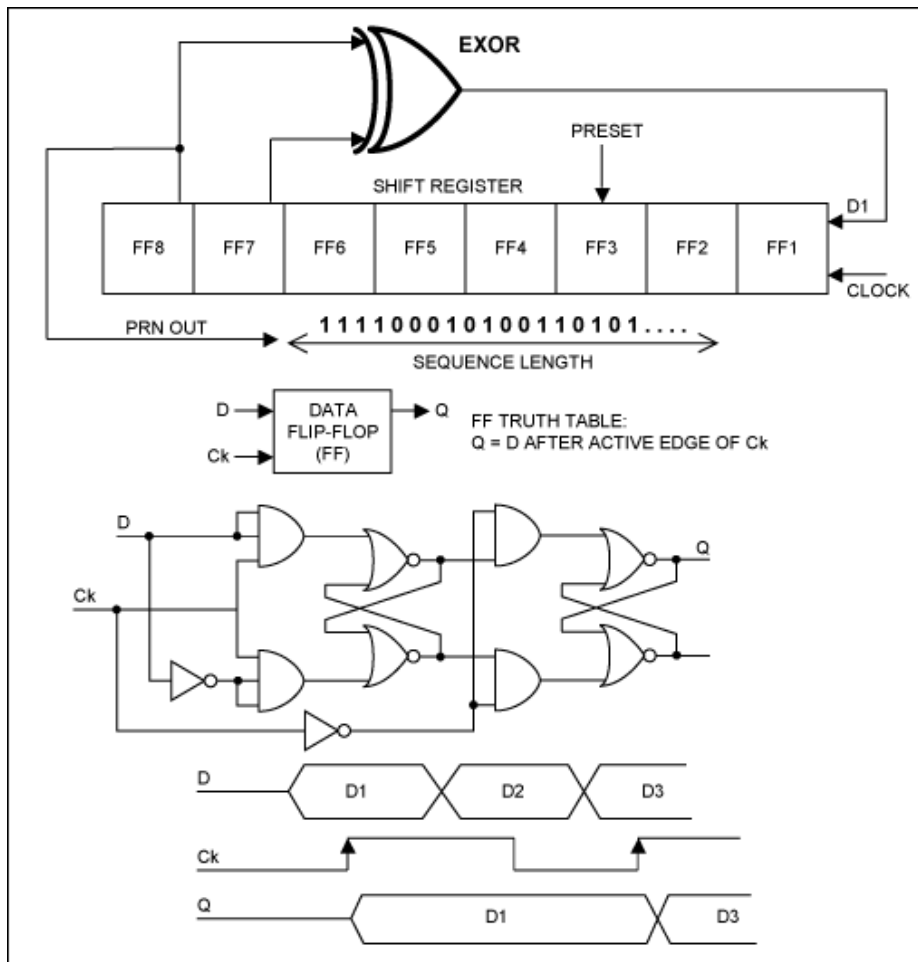


Figure 11. Block diagram of a sample PRN generator.

Many books are available on the generation of PRNs and their characteristics, but that development is outside the scope of this basic tutorial. Simply note that the construction or selection of proper sequences, or sets of sequences, is not trivial. To guarantee efficient spread-spectrum communications, the PRN sequences must respect certain rules, such as length, autocorrelation, cross-correlation, orthogonality, and bits balancing. The more popular PRN sequences have names: Barker, M-Sequence, Gold, Hadamard-Walsh, etc. Keep in mind that a more complex sequence set provides a more robust spread-spectrum link.

But there is a cost to this: more complex electronics both in speed and behavior, mainly for the spread-spectrum despreading operations. Purely digital spread-spectrum despreading chips can contain more than several million equivalent 2-input NAND gates, switching at several tens of megahertz.

Different Modulation Spreading Techniques for Spread Spectrum

Different spread-spectrum techniques are distinguished according to the point in the system at which a PRN is inserted in the communication channel. This is very basically illustrated in the RF front-end schematic in Figure 12.

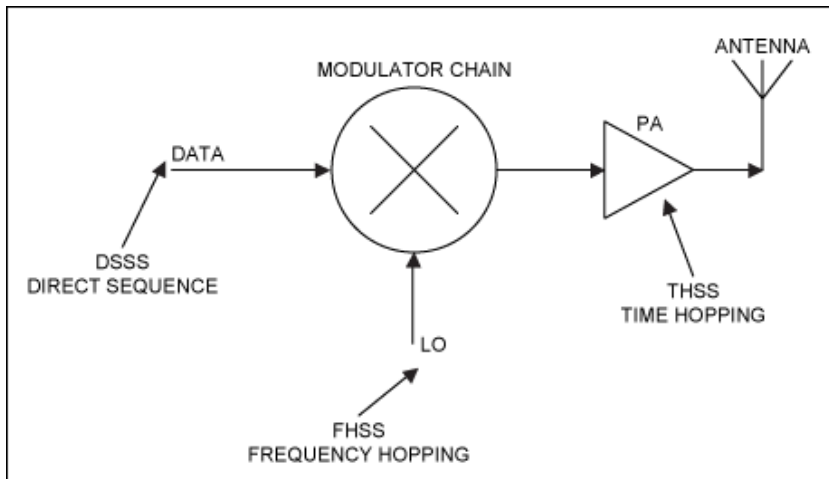


Figure 12. Several spreading techniques are applied at different stages of the transmit chain.

If the PRN is inserted at the data level, this is the direct-sequence form of spread spectrum (DSSS). (In practice, the pseudo-random sequence is mixed or multiplied with the information signal, giving an impression that the original data flow was "hashed" by the PRN.) If the PRN acts at the carrier-frequency level, this is the frequency-hopping form of spread spectrum (FHSS). Applied at the LO stage, FHSS PRN codes force the carrier to change or "hop" according to the pseudo-random sequence. If the PRN acts as an on/off gate to the transmitted signal, this is a time-hopping spread-spectrum technique (THSS). There is also the "chirp" technique, which linearly sweeps the carrier frequency in time.

One can mix all the above techniques to form a hybrid spread-spectrum technique, such as DSSS + FHSS. DSSS and FHSS are the two techniques most in use today.

Direct-Sequence Spread Spectrum (DSSS)

With the DSSS technique, the PRN is applied directly to data entering the carrier modulator. The modulator, therefore, sees a much larger bit rate, which corresponds to the chip rate of the PRN sequence. Modulating an RF carrier with such a code sequence produces a direct-sequence-modulated spread spectrum with $(\sin x)/x$ ² frequency spectrum, centered at the carrier frequency.

The main lobe of this spectrum (null to null) has a bandwidth twice the clock rate of the modulating code, and the side lobes have null-to-null bandwidths equal to the code's clock rate. Illustrated in Figure 13 is the most common type of direct-sequence-modulated spread-spectrum signal. Direct-sequence spectra vary somewhat in spectral shape, depending on the actual carrier and data modulation used. Below is a binary phase shift keyed (BPSK) signal, which is the most common modulation type used in direct-sequence systems.

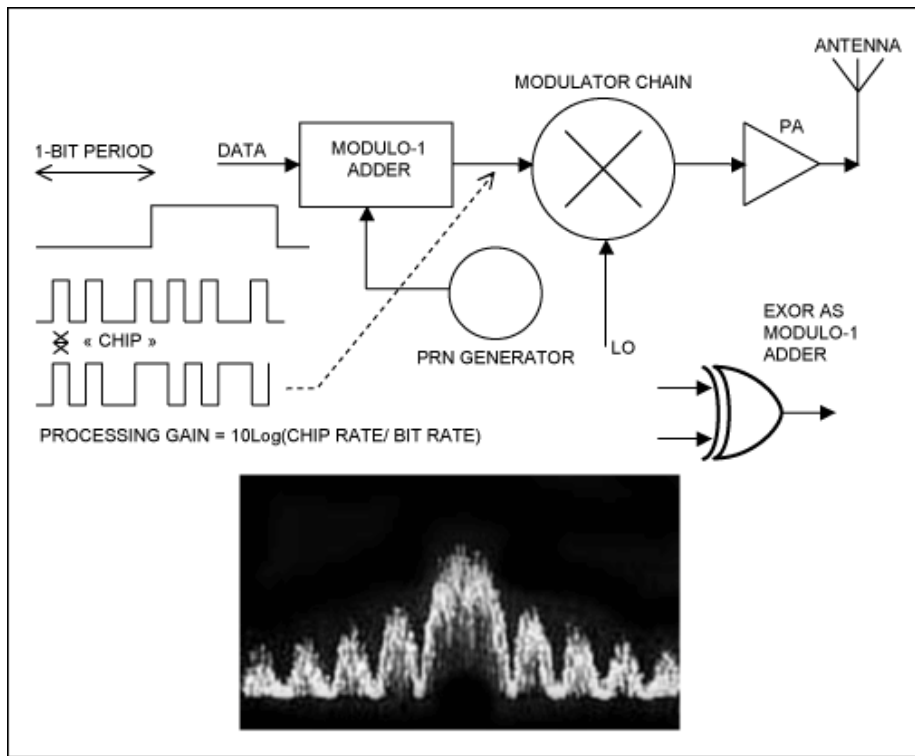


Figure 13. Spectrum-analyzer photo of a DSSS signal. Note the original signal (nonspread) would only occupy half of the central lobe.

Frequency-Hopping Spread Spectrum (FHSS)

The FHSS method does exactly what its name implies—it causes the carrier to hop from frequency to frequency over a wide band according to a sequence defined by the PRN. The speed at which the hops are executed depends on the data rate of the original information. One can, however, distinguish between fast frequency hopping (FFHSS) and low frequency hopping (LFHSS). The latter method, the most common, allows several consecutive data bits to modulate the same frequency. FFHSS is characterized by several hops within each data bit.

The transmitted spectrum of a frequency-hopping signal is quite different from that of a direct-sequence system. Instead of a $((\sin x)/x)^2$ -shaped envelope, the frequency hopper's output is flat over the band of frequencies used (see Figure 14). The bandwidth of a frequency-hopping signal is simply N times the number of frequency slots available, where N is the bandwidth of each hop channel.

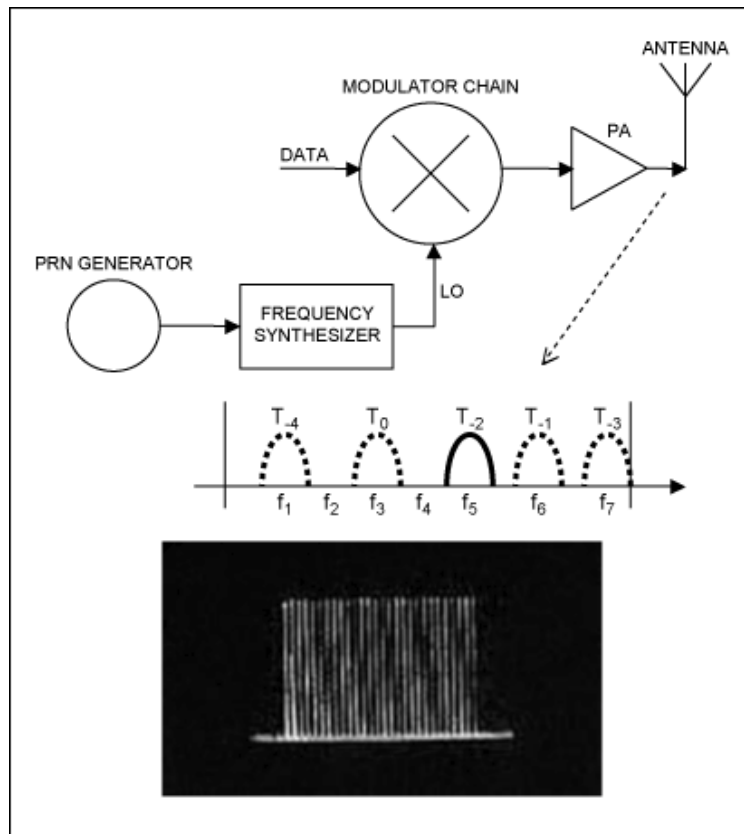


Figure 14. Spectrum-analyzer photo of a FHSS signal.

Time-Hopping Spread Spectrum (THSS)

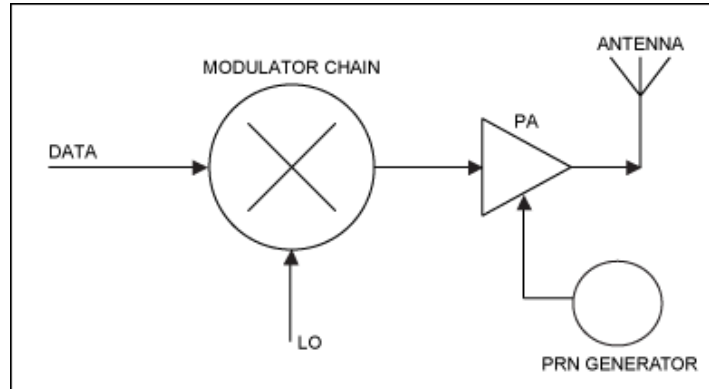


Figure 15. THSS block diagram.

Figure 15 illustrates THSS, a method not well developed today. Here the on and off sequences applied to the PA are dictated according to the PRN sequence.

Implementations and Conclusions

A complete spread-spectrum communication link requires various advanced and up-to-date technologies and disciplines: an RF antenna, a powerful and efficient PA, a low-noise and highly linear LNA, compact transceivers, high-resolution ADCs and DACs, rapid low-power digital signal processing (DSP), etc. Though designers and manufacturers compete, they are also joining in their effort to implement spread-spectrum systems.

The most difficult area is the receiver path, especially at the despread level for DSSS, because the receiver must be able to recognize the message and synchronize with it in real time. The operation of code recognition is also called correlation. Because correlation is performed at the digital-format level, the tasks are mainly complex arithmetic calculations including fast, highly parallel, binary additions and multiplications.

The most difficult aspect of today's receiver design is synchronization. More time, effort, research, and money have gone toward developing and improving synchronization techniques than toward any other aspect of spread-spectrum communications. Several methods can solve the synchronization problem, and many of them require a large number of discrete components to implement. Perhaps the biggest breakthroughs have occurred in DSP and in application-specific integrated circuits (ASICs). DSP provides high-speed mathematical functions that analyze, synchronize, and decorrelate a spread-spectrum signal after slicing it in many small parts. ASIC chips drive down costs with VLSI technology and by the creation of generic building blocks suitable for any type of application.

SOCIAL



QUICK LINKS

- About ADI
- ADI Signals+
- Analog Dialogue
- Careers
- Contact us
- Investor Relations
- News Room
- Quality & Reliability
- Sales & Distribution
- Incubators

LANGUAGES

- English
- 简体中文
- 日本語

MYANALOG

Interested in the latest news and articles about ADI products, design tools, training and events?

[Go to myAnalog](#)