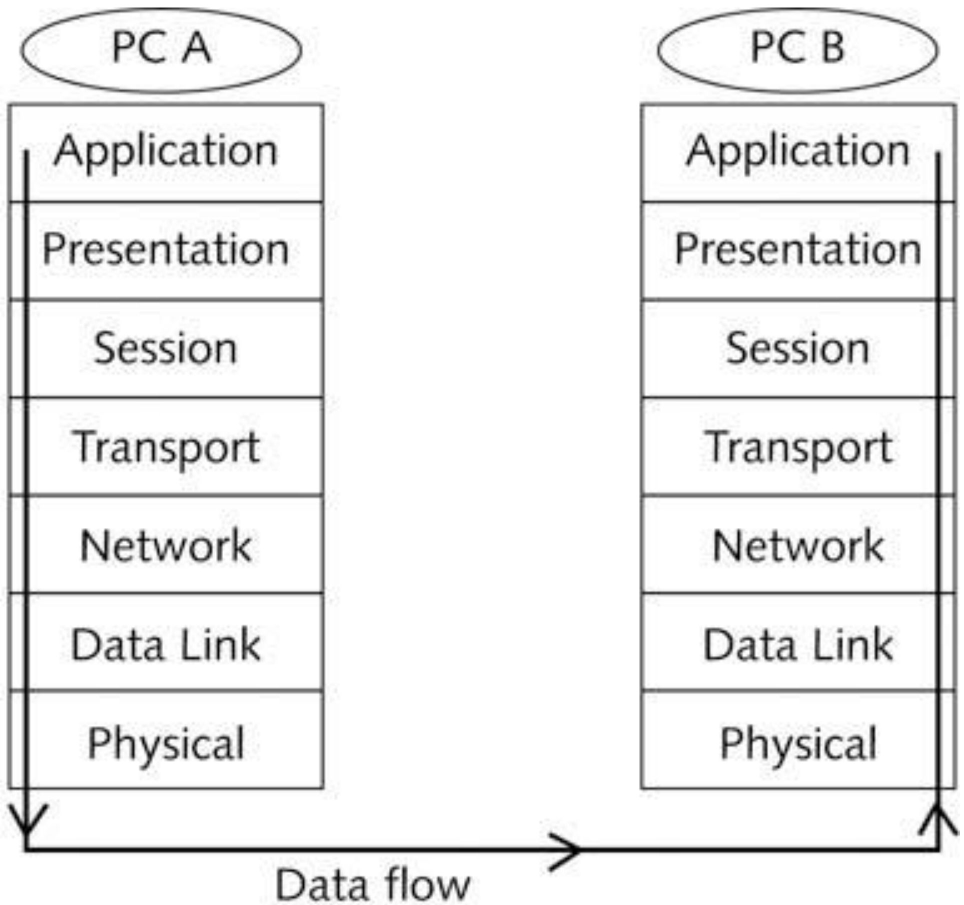
ICA0008
Fundamentals of Wireless LANS

Tauseef ahmed, PhD

Spread Spectrum Technologies

Introduction



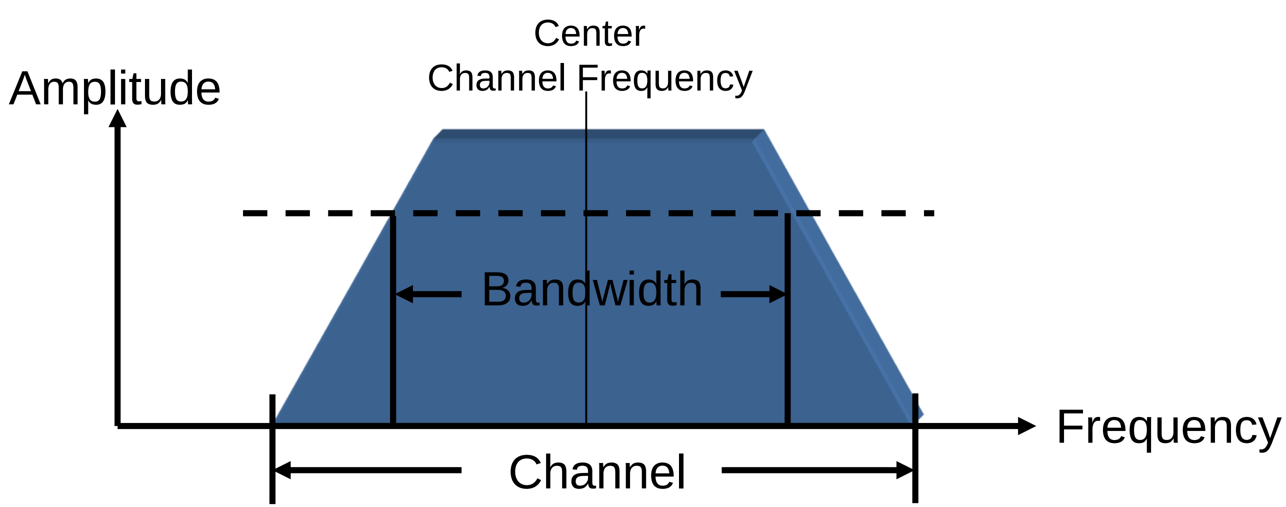
OSI data flow

OSI Model

OSI Layer	Layer Name	Functionality	Technology Examples
Layer 7	Application	Defines the provision of services to applications, such as checking for resource availability and authenticating users.	Most firewalls, FTP, POP3, HTTP, etc.
Layer 6	Presentation	The Presentation layer has the primary responsibility of interpreting and presenting data to or from the Application layer.	Many encryption technologies, compression technologies, protocol conversion, etc.
Layer 5	Session	The responsibility for managing sessions (connections) between two networked Application layers rests on the Session layer.	Remote Procedure Call, TCP also resides here (the TCP/IP stack does not match perfectly to the OSI model), etc.
Layer 4	Transport	The Transport layer is the area where packet delivery confirmation and packet rebuilding occur.	TCP, UDP, etc.
Layer 3	Network	The Network layer is responsible for management of routing, relaying, and terminating connections between network nodes.	Internet Protocol (IP), routers, stateless inspection firewalls or packet filters, etc.
Layer 2	Data Link	The Data Link layer is responsible for detecting and correcting errors in the Physical layer and for transmitting data from one place to another. The Data Link layer may be divided into the Logical Link Control (LLC) and Medium Access Control (MAC) sublayers.	Bridges, switches, MAC addresses, IEEE 802.11 framing, etc.
Layer 1	Physical	The Physical layer includes the standards that control the transmission of the data streams on the specific medium.	Frequency-hopping spread spectrum, direct-sequence spread spectrum, OFDM, Ethernet hubs, etc.

Telecommunication Channel

- Channel - a path along which information in the form of an electrical signal passes. Usually a range of contiguous frequencies involved in supporting information transmission.



RF Bands for Wireless Networks

- ISM- Industrial Scientific and Medical – Three Bands
  - 900 MHz band
  - 2.4 GHz band
  - 5 GHz Band
- UNII- Unlicensed National Information Infrastructure
  - These bands are located between 5 GHz and 6 GHz and are defined by the FCC for use by unlicensed RF transmitters.
  - UNII-1 (Lower)
  - UNII-2 (middle)
  - UNII2 Extended
  - UNII-3 (Upper)

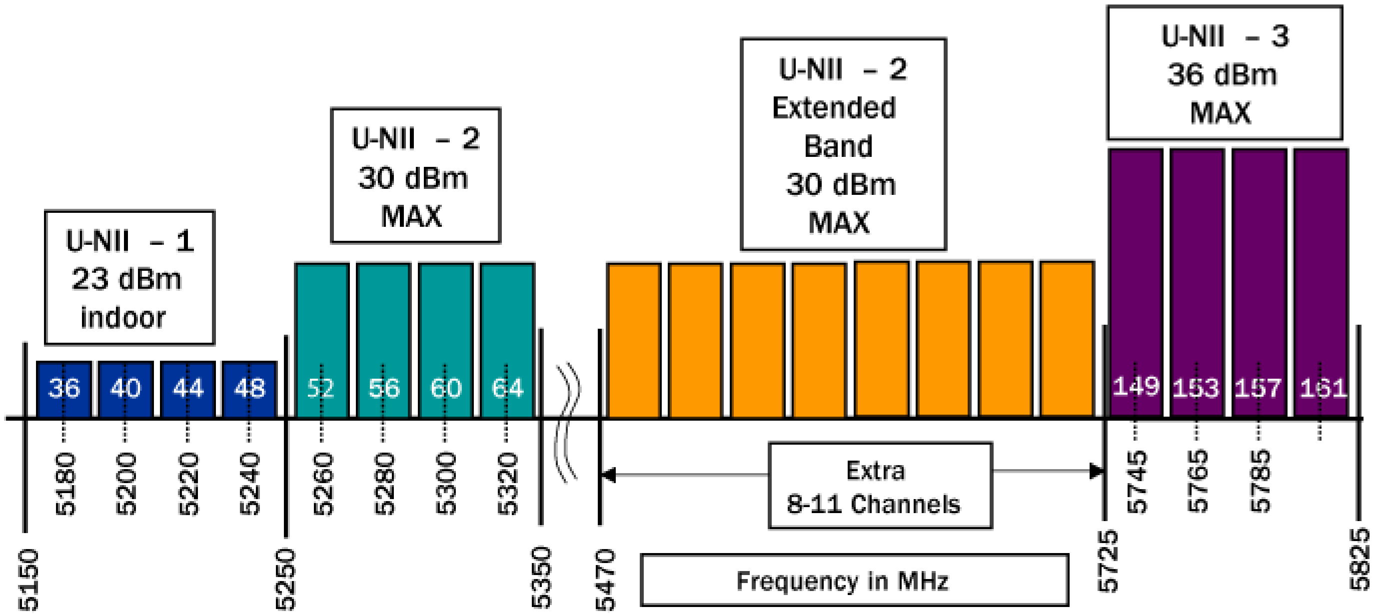
ISM Bands Summary

Band	Frequency MHz	Band-width MHz	Channels	Applications
900 MHz	902-928	26	1	GSM, baby monitors, cordless phone, headsets Foliage penetration
2.4 GHz	2.400-2.4835	83.5	14	Wireless LAN 802.11, microwaves, cordless phone
5.8 GHz	5.725-5.875	150	23	WLANs, Monitors, cordless phones, outdoor Point to point I

5 GHz UNII Bands Summary

UNII Band	Category	GHz	Band-width	Channels	FCC max Power -mW	Applications
UNII-1	Lower	5.15-5.25	100	4	50	Indoor
UNII-2	Middle	5.25-5.35	100	4	250	Indoor/outdoor
UNII-2 Extended	Extended	5.47-5.725	255	11	250	Indoor/outdoor
UNII-3	Upper	5.725-5.825	100	4	1000	Indoor/outdoor Point to point

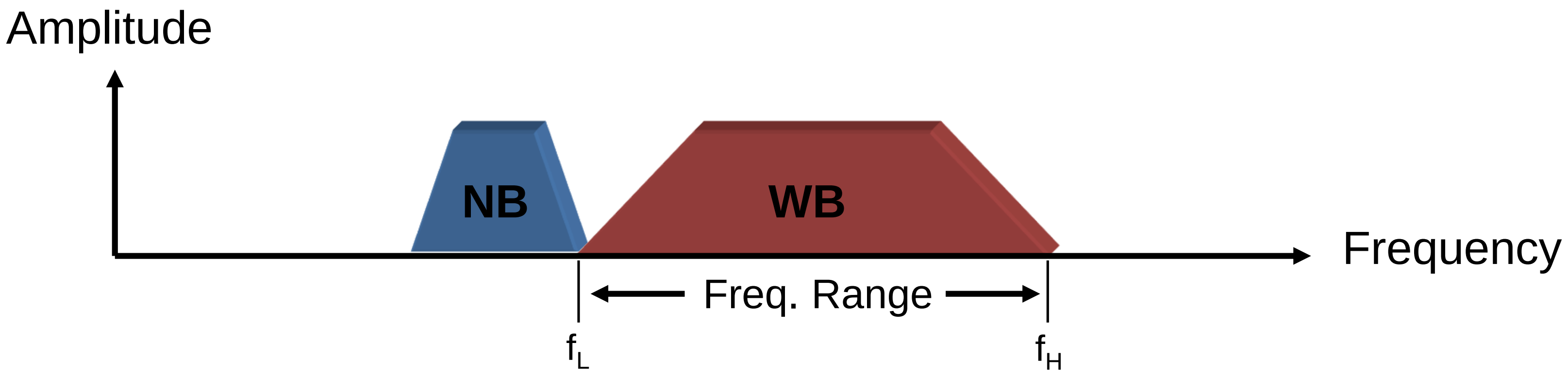
UNII Bands



U-NII – 1
23 dBm
indoor
U-NII – 2
30 dBm
MAX
U-NII – 2
Extended
Band
30 dBm
MAX
U-NII – 3
36 dBm
MAX
36
40
44
48
52
56
60
64
149
153
157
161
5180
5200
5220
5240
5260
5280
5300
5320
5745
5765
5785
5150
5250
5350
5470
5725
5825
Extra
8-11 Channels
Frequency in MHz

Narrow and Wide Band

- Narrow and Wide Band – a relative comparison of a group or range of frequencies used in a telecommunications system. Narrow Band would describe a small range of frequencies as compared to a larger Wide Band range.

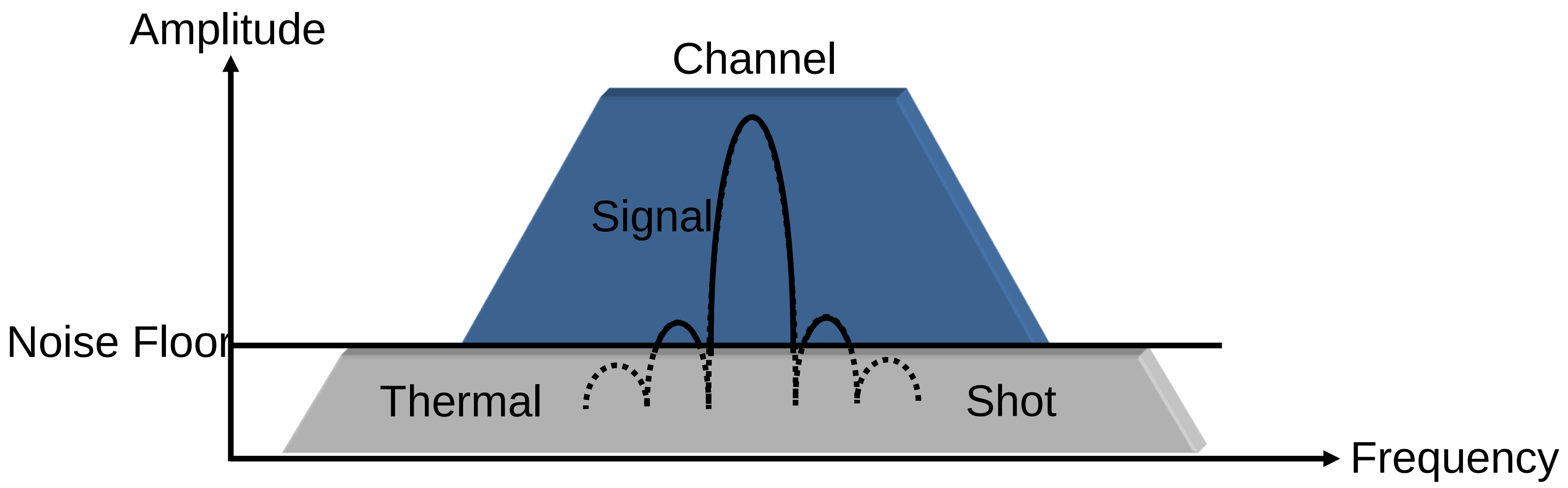


Narrowband vs. Spread Spectrum Technology

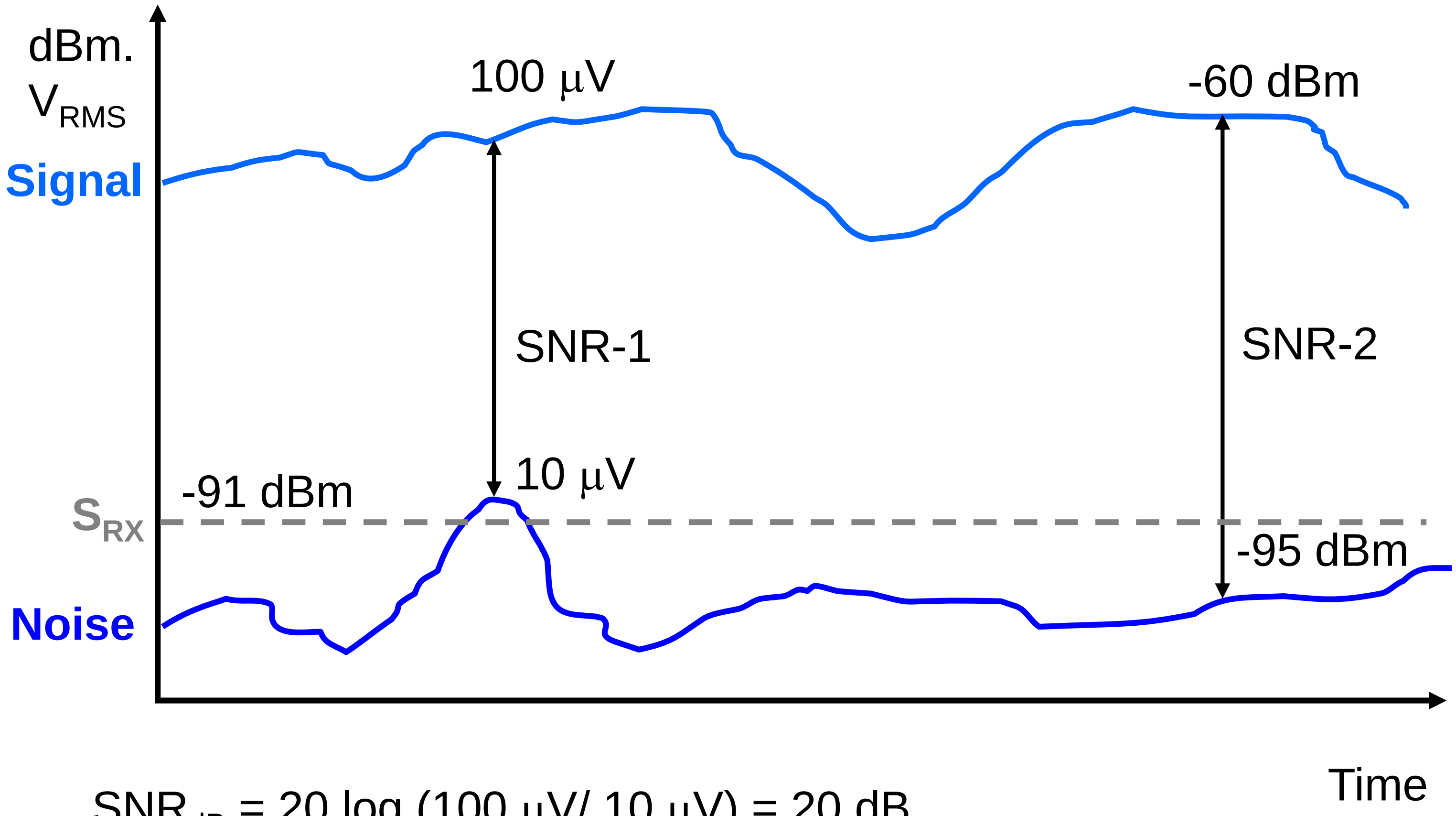
Narrowband	Spread Spectrum and OFDM
Uses high power levels concentrated close to the carrier frequency	Uses a range or "spread" of frequencies
Characterized by higher output power levels	Characterized by lower output levels
Bandwidth of the radiated signal is very close to the information bandwidth	Bandwidth of the radiated signal is greater than the information bandwidth
More prone to interference	Less prone to interference
Causes tremendous interference with other devices communicating on the same or close frequencies	Causes less interference due to the low power levels of the communications
Generally requires a license from the local regulatory agency	Requires no license when using unlicensed WLAN technology

Noise Floor

- Noise –A disturbance, especially a random and persistent disturbance, that obscures or reduces the clarity of a signal. Anything you do not want. (unwanted signal)



Signal to Noise Ratio

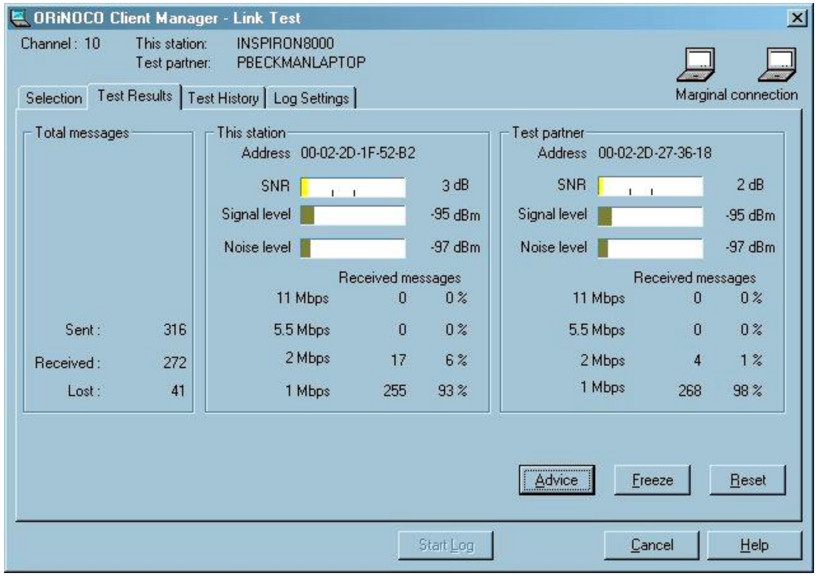


SNR_{dB} = 20 log (100 µV/ 10 µV) = 20 dB

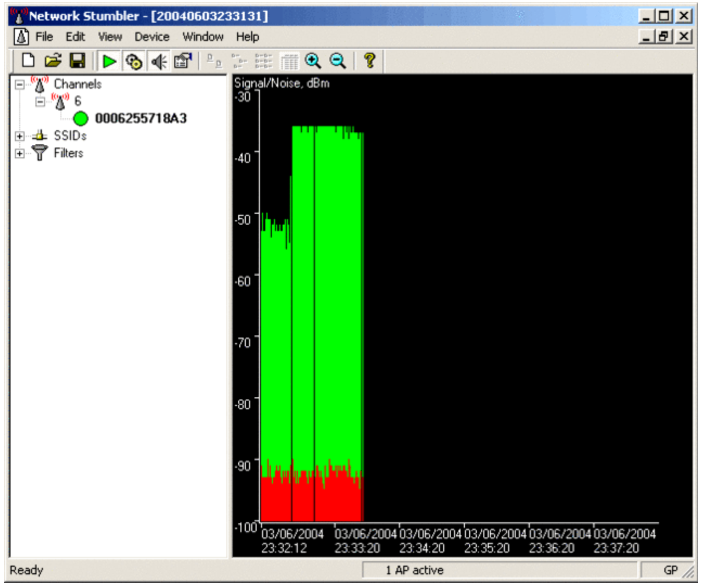
SNR_{dB} = -60 dBm – (-95 dBm) = 35 dB

Signal to Noise Ratio

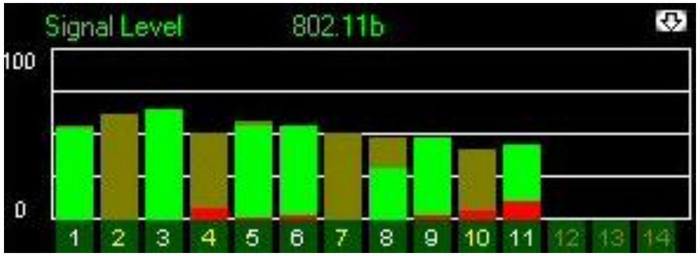
Orinoco Client



NetStumbler



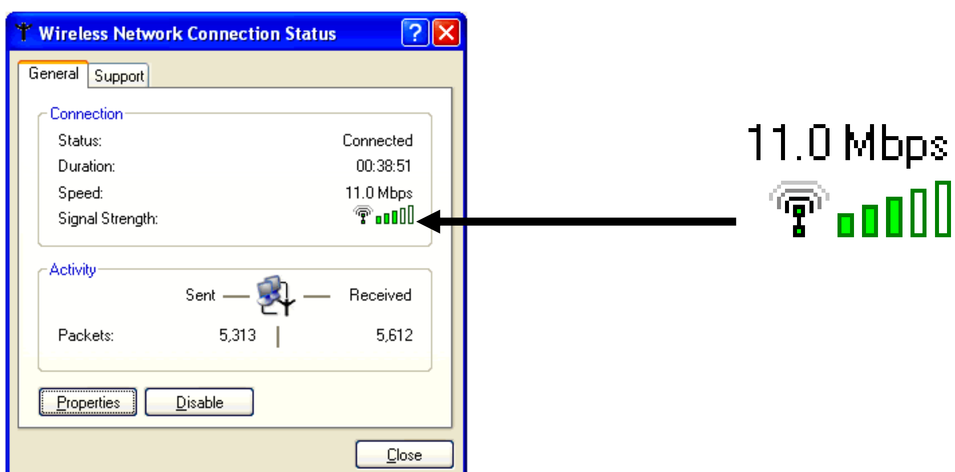
AirMagnet



CH	MAC Address	S	N	
1	Agere:61:2F:06	25	0	25
11	D-Link:F9:CC:4D	53	12	41

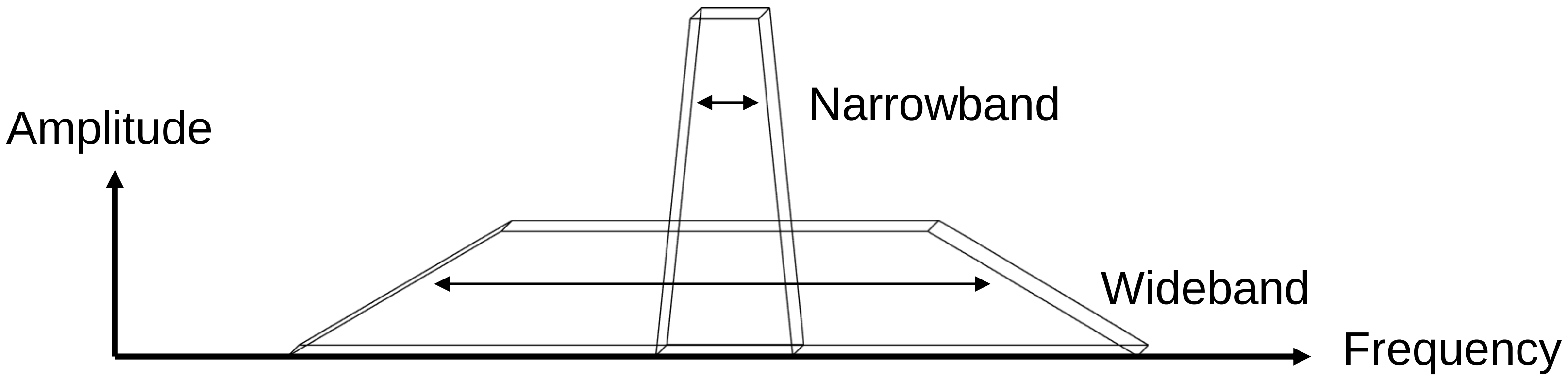
Windows Wireless 802.11b

Windows Signal Level	Signal to Noise Ratio	Data Rates
Excellent	26 dBm and above	11Mpbs
Very Good	25dBm to 21dBm	11Mpbs
Good	20dBm to 16dBm	11Mpbs
Low	15dBm to 11dBm	11Mpbs
Very Low	10dBm to 8dBm	5.5Mbps
Very Low	8dBm to 6dBm	2Mbps
Very Low	6 dBm and under	1Mbps



Introduction to Spread Spectrum Techniques

- Spread Spectrum – a telecommunications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information.



Spread Spectrum Transmission

- Advantages over narrowband:
  - Resistance to narrowband interference
  - Resistance to spread spectrum interference
  - Lower power requirements
  - Less interference on other systems
  - More information transmitted
  - Increased security
  - Resistance to multipath distortion

Uses of Spread Spectrum Techniques

- Military - For low probability of interception of telecommunications.
- Civil/Military - Range and positioning measurements. GPS – satellites.
- Civil Cellular Telephony.
- Civil Wireless Networks – 802.11 and Bluetooth.

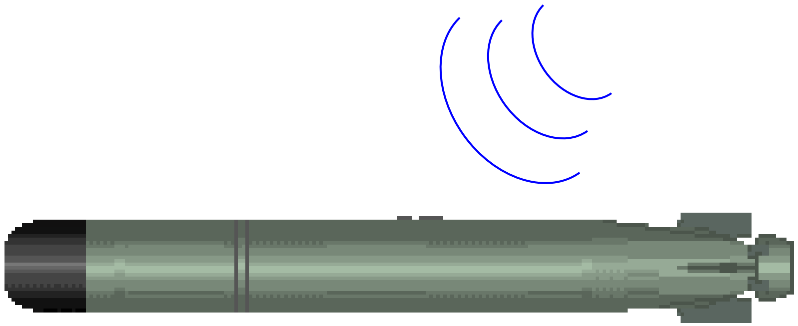
Types of Spread Spectrum Techniques

1. Time Hopping, (THSS)
2. Frequency Hopping, (FHSS)
3. Direct Sequence Spread Spectrum, (DSSS)
4. Hybrid, DSSS/FHSS

Frequency Hopping

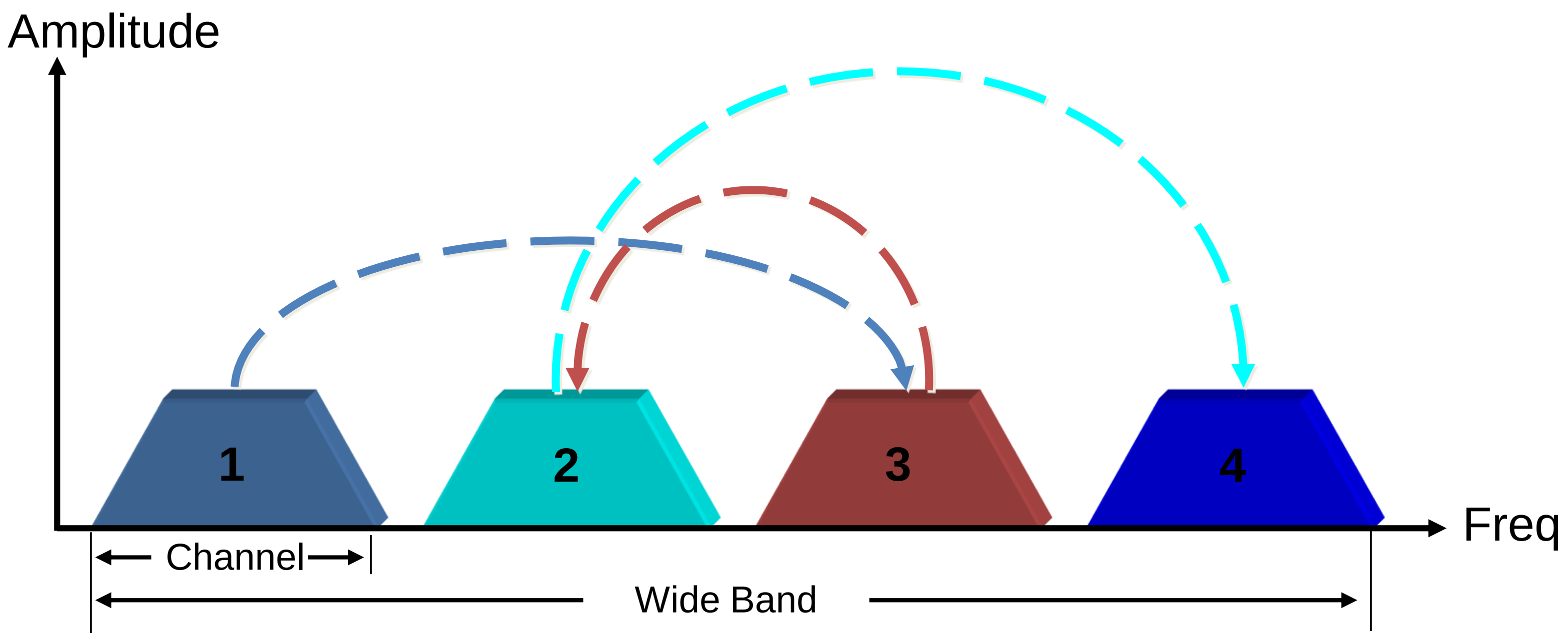
- Hedy Lamarr and composer George Antheil, patent number 2,292,387

  circa 1942



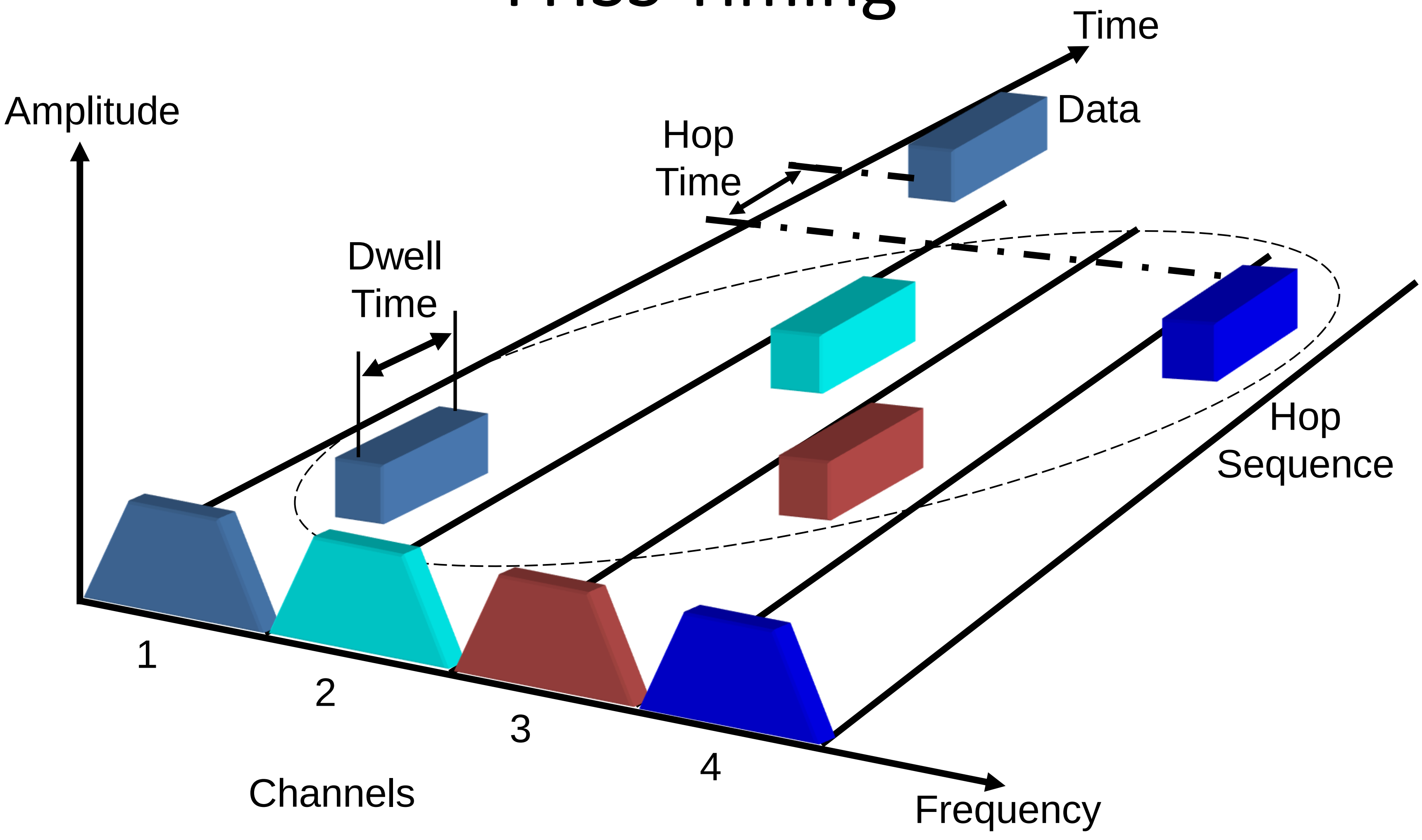
FHSS

- FHSS - **f**requency-**h**opping **s**pread **s**pectrum.
  - 802.11, Bluetooth, & Home RF.



Frequency Hop Sequence: 1, 3, 2, 4

FHSS Timing



Time
Amplitude
Data
Hop
Time
Dwell
Time
Hop
Sequence
1
2
3
4
Channels
Frequency

FHSS Concepts

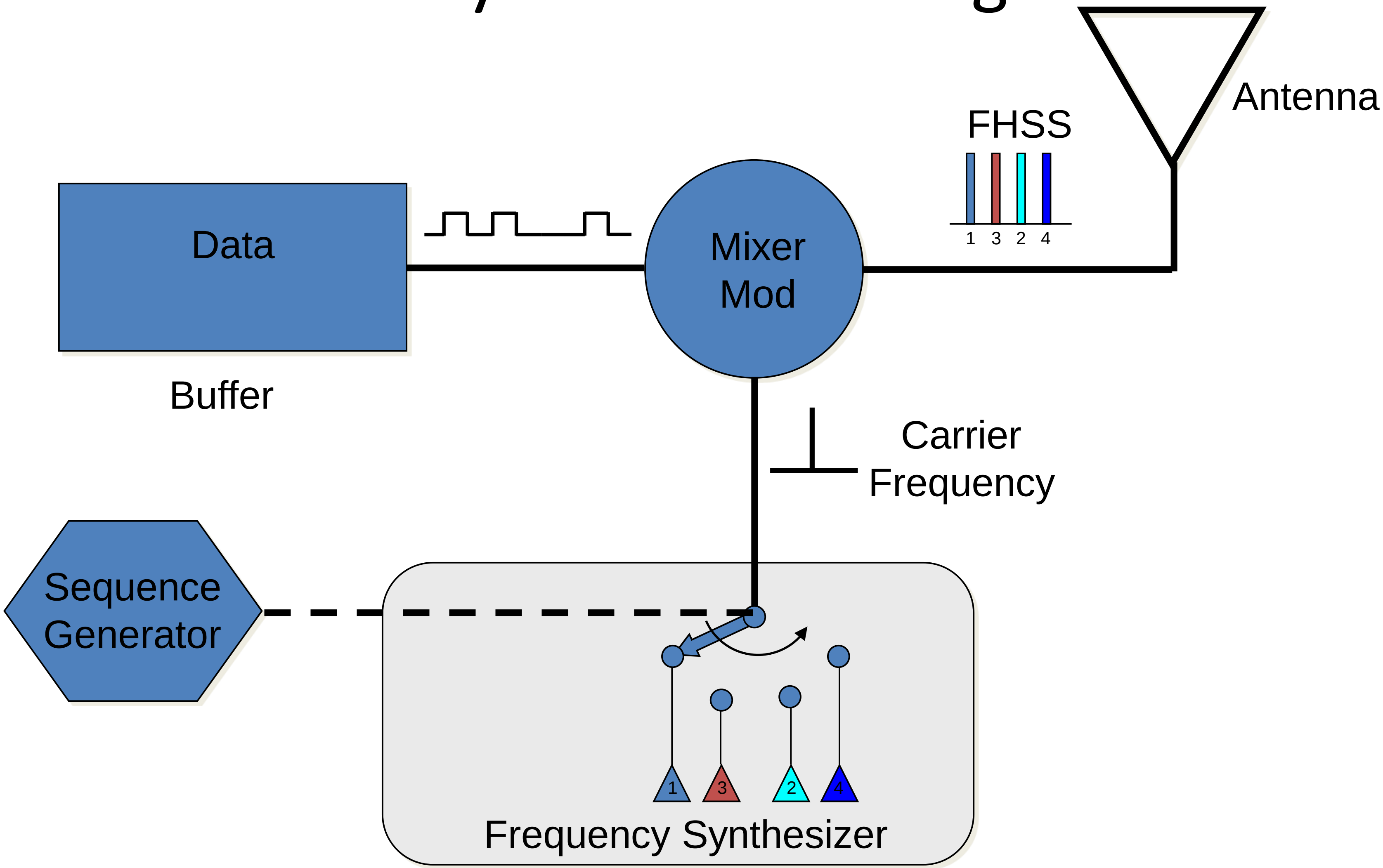
- Dwell Time
  - The amount of time spent on a specific frequency in an FHSS hopping sequence is known as the dwell time.
  - 1 MHz of bandwidth each, provide 79 optional frequencies on which to dwell for the specified length of the dwell time.
- Hopping Sequence
  - The hopping sequence is the list of frequencies through which the FHSS system will hop according to the specified dwell time. This hopping sequence is also known as a hopping pattern or hopping set.
- Hop Time
  - The duration of time required to hop from one frequency in the hopping sequence to the next is called the hop time.

FHSS Concepts

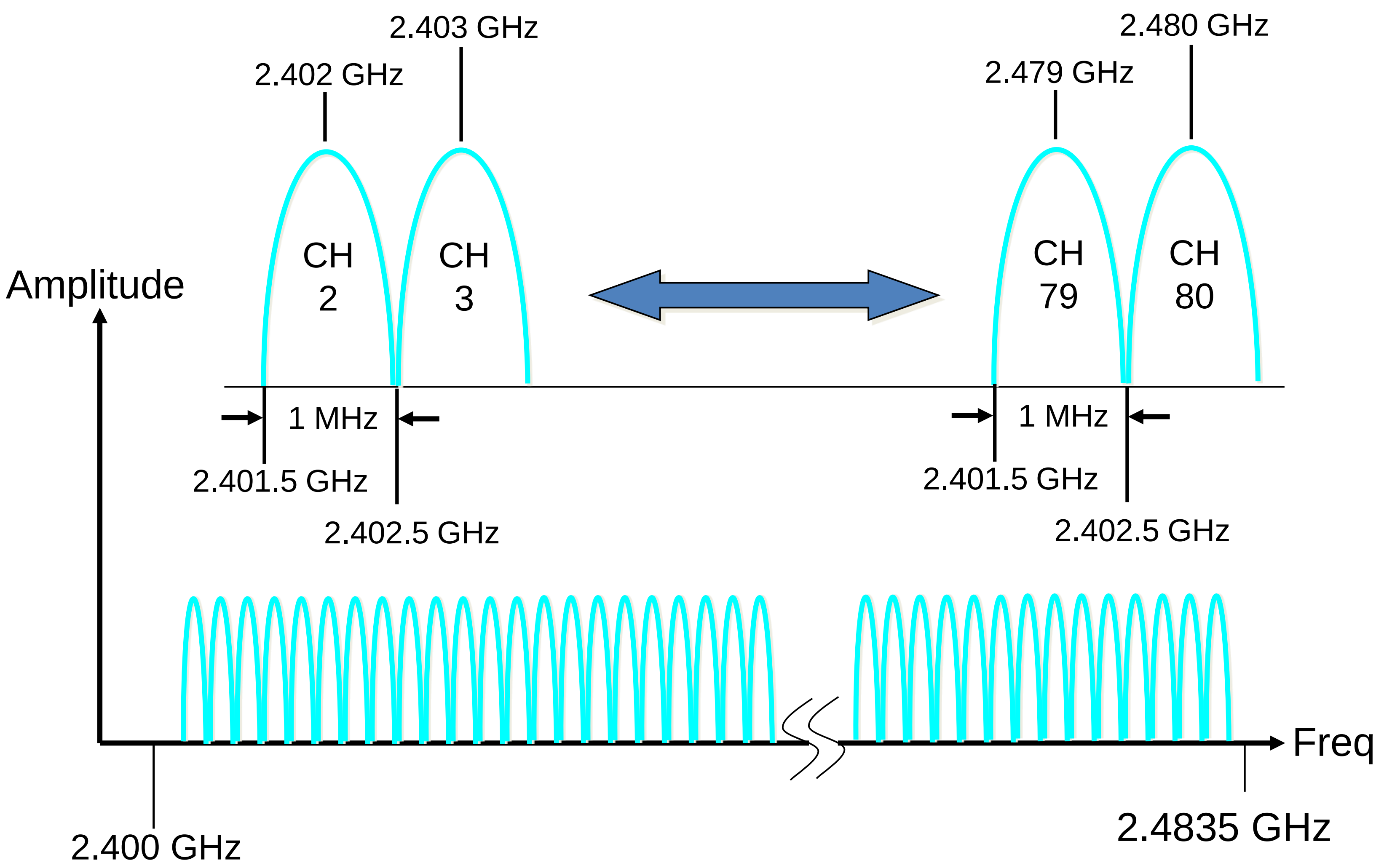
FHSS Dwell Times and Hopping Sequence Cycles

Dwell Time	Time for One Pass	Number of Passes	Milliseconds on a Hop
50 ms	3,750 ms	8	400
100 ms	7,500 ms	4	400
200 ms	15,000 ms	2	400
400 ms	30,000 ms	1	400

FHSS System Block Diagram



FHSS Channel Allocation

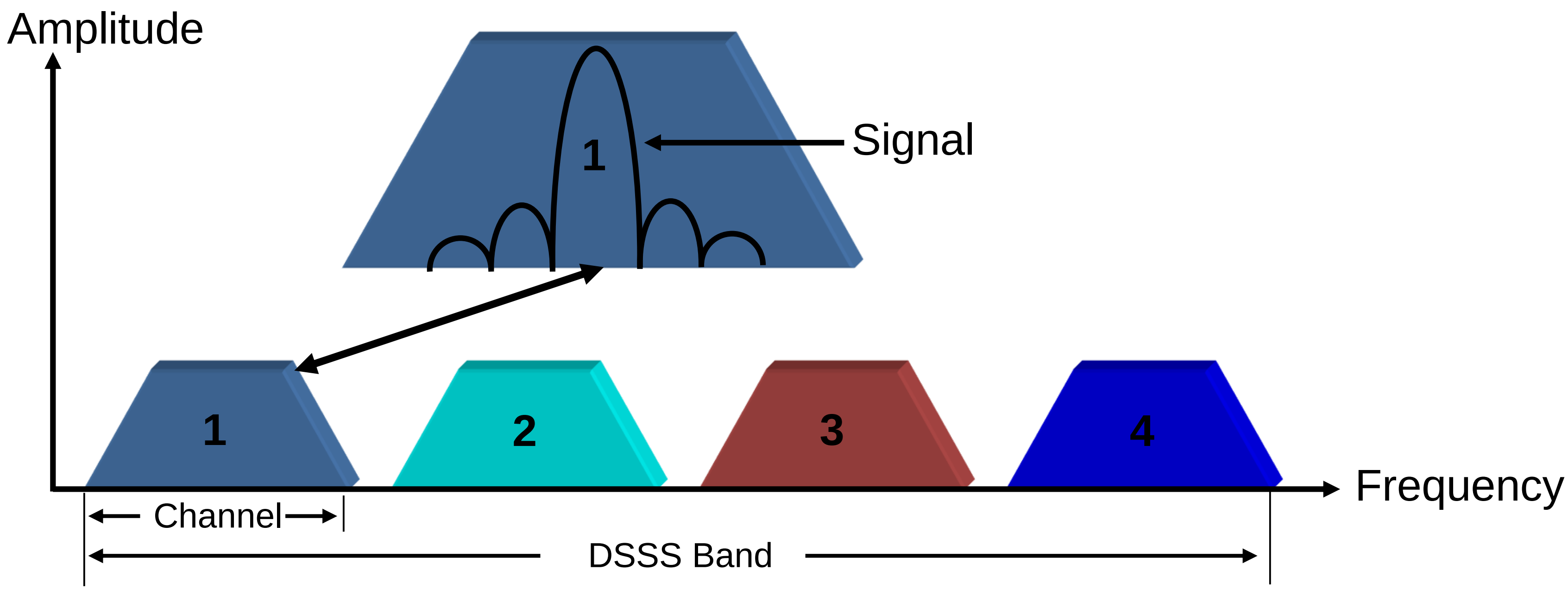


FHSS Overview

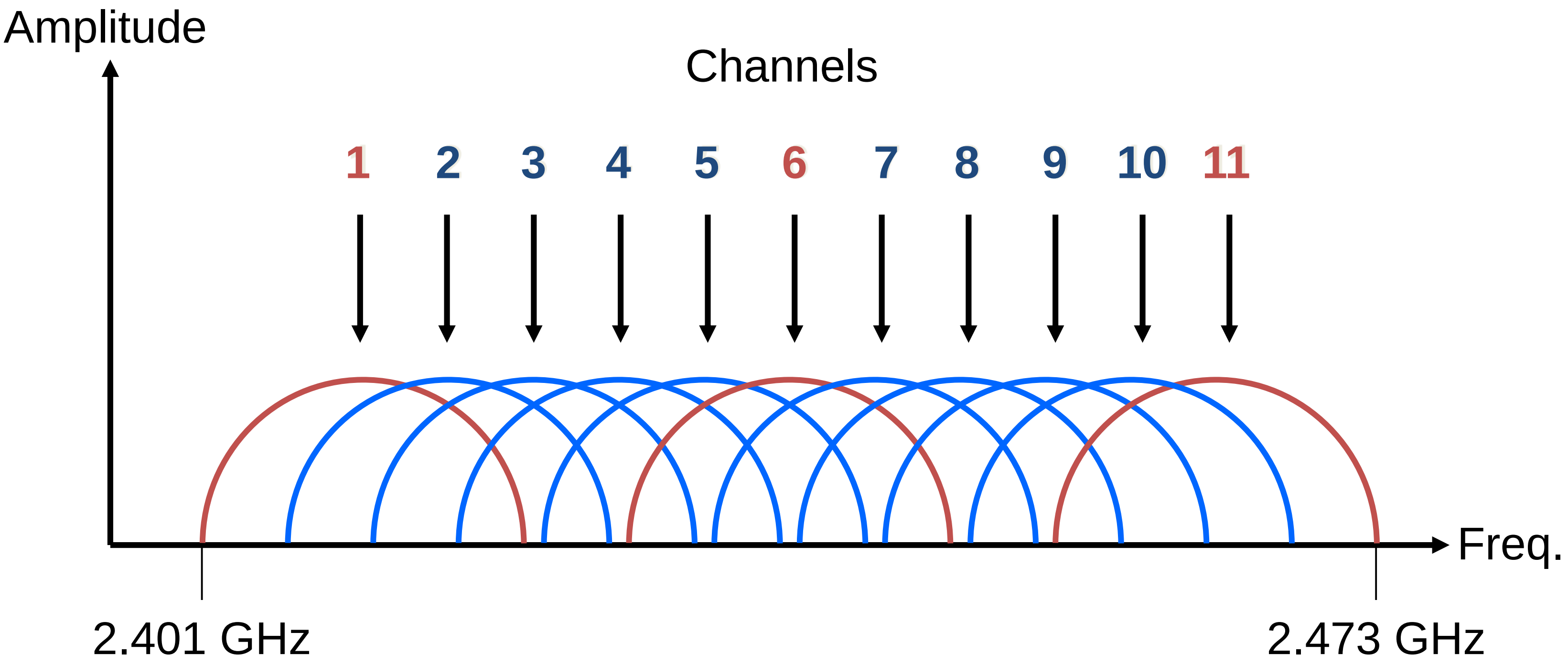
- FHSS Modulation
  - Gaussian Frequency Shift Keying (GFSK)
    - 2GFSK
    - 4GFSK
- Maximum speed 2 Mbps (available speed 1 or 2 Mbps)
- Resilience to interference
- Mainly used in Bluetooth where speed is not main concern.
  - Wireless headset, wireless mice, wireless keyboards, etc.

DSSS

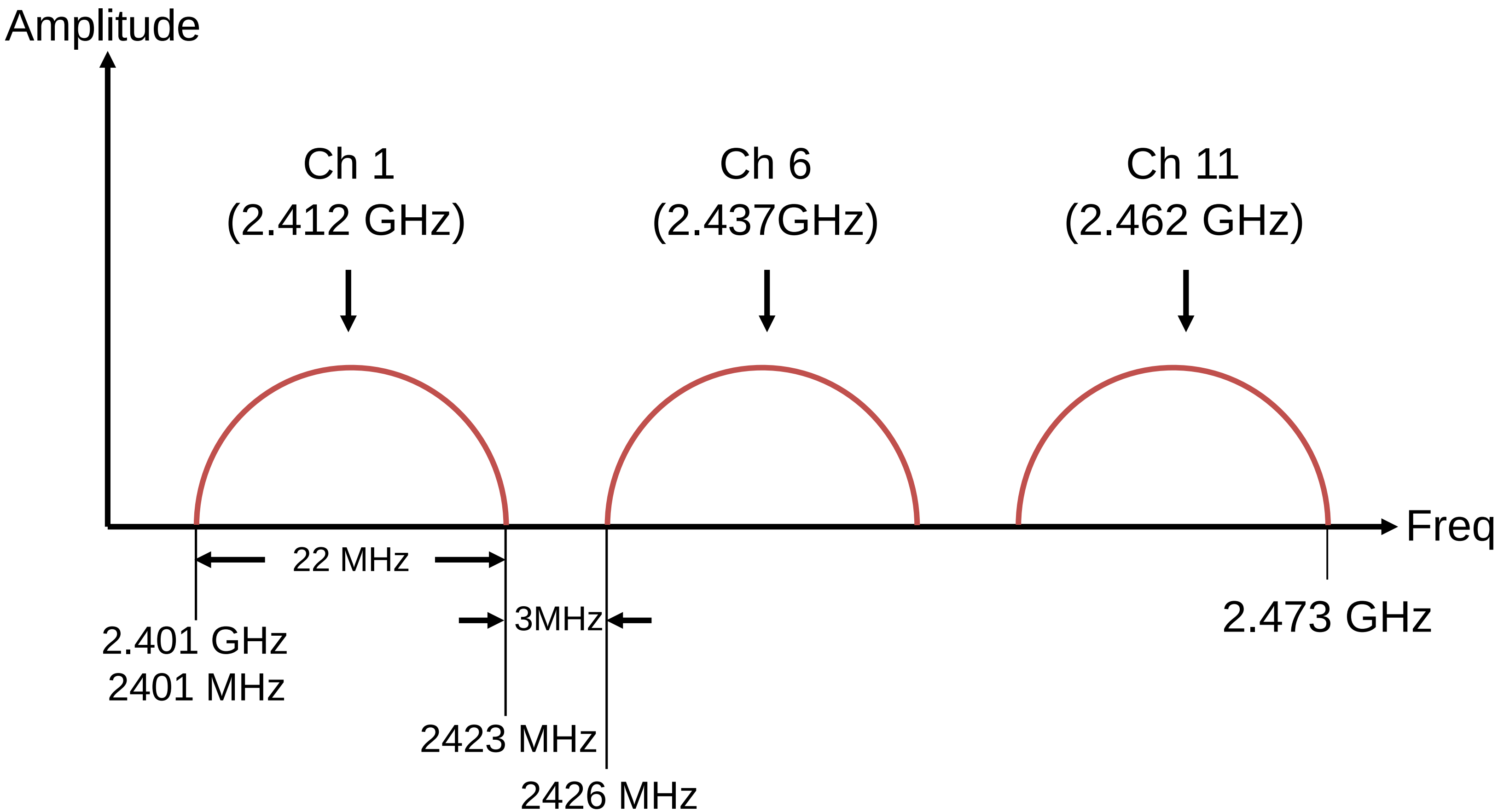
- DSSS - **d**irect-**s**equence **s**pread **s**pectrum.
  - WLAN, 802.11.



DSSS Channel Allocation



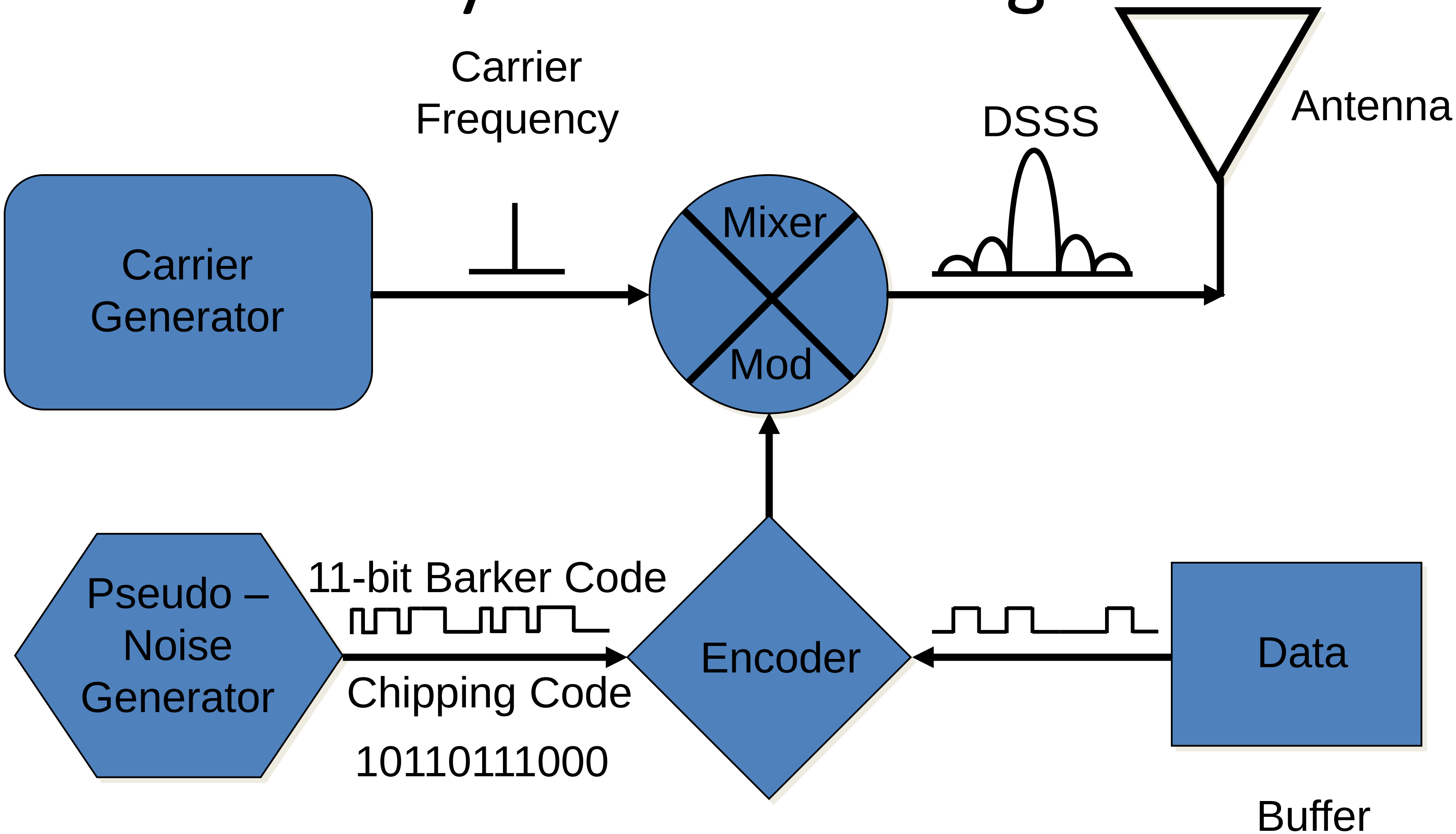
DSSS 3 Non-overlap Channels



DSSS Concepts

- DSSS systems encode the information to transfer
- Redundant information is added (processing gain)
- Transmitted data is much larger than original data
  - 0 -> PN sequence of 01001000111 (11 bit)
  - 1 -> PN sequence of 10110111000 (11 bit)
- Data encoding is done before modulation

DSSS System Block Diagram



DSSS Overview

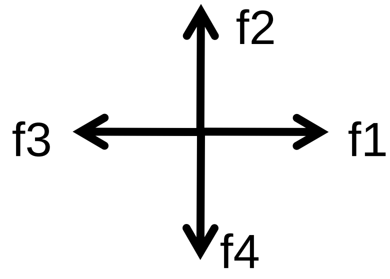
- DSSS Modulation
  - DBPSK at 1 Mbps
  - DQPSK at 2 Mbps
  - standard provided for higher data rates
- DSSS transmits redundant copies of the data
- DSSS systems are also resistant to narrowband interference
  - because DSSS systems use narrow bandwidths and do not hop from one frequency to another, they may be more susceptible to interference than FHSS systems.

Comparing FHSS & DSSS

Frequency Hopping Spread Spectrum, FHSS 802.11		Direct Sequence Spread Spectrum, DSSS 802.11b	
Dwell Time 400 mS	Higher Cost	No Dwell Time	Lower Cost
Lower Throughput (2 or 3 Mbps)	Lower Interoperability	Higher Throughput (11 Mbps)	Higher Interoperability
Better Immunity to Interference	More User Density (79)	Poorer Immunity to Interference	Less User Density (3)

OFDM
Orthogonal Frequency Division Multiplexing

- Frequency division multiplexing (FDM) is a technology that transmits multiple signals simultaneously over a single transmission path, such as a cable or wireless system.
- **Orthogonal** means to establish right angle relationships between frequencies
- OFDM distributes the data over a large number of carriers that are spaced apart at precise frequencies and null out of channel sidebands



OFDM Overview

- OFDM offers high data rates and exceptional resistance to interference and corruption
- OFDM is actually a digital modulation method that splits the signal into multiple narrowband subcarriers at different frequencies
  - In a way, OFDM splits a high-speed information signal into multiple lower-speed information signals and then transmits these lower-speed signals in parallel.
  - OFDM is now used in both the 5 GHz U-NII bands (IEEE 802.11a) and the 2.4 GHz ISM band (IEEE 802.11g), though it was first introduced to WLANs through the IEEE 802.11a standard
  - The benefits of OFDM include spectral efficiency (meaning that the use of the electromagnetic spectrum is more efficient than with other technologies), resistance to RF interference, and lowered multipath distortion.
- Also used in ADSL and WiMax

IEEE 802.11n
Draft

- IEEE 802.11n is planned to use High Throughput–OFDM (HT-OFDM) as its primary communications mechanism.
  - 20MHz and 40 MHz bands
  - Data rates up to 600 Mbps
- EEE 802.11n PHY will operate in one of three modes
  - Non-HT mode
    - OFDM
    - Backward compatibility to a, b, g
  - HT mixed mode
    - Supports OFDM and ERP-OFDM
  - Greenfield mode
    - Only ERP-OFDM
    - Highest data rates

Encoding and Modulation

- Encoding - To change or translate one bit stream into another.

  Barker Code, Complementary Code Keying
- Modulation – Appling information on a carrier signal by varying one or more of the signal's basic characteristics - frequency, amplitude and phase.

  DBPSK (Differential Binary Phase Shift Keying) DQPSK (Differential Quaternary PSK)

Convolution Coding

- Convolution coding is a method of channel coding by adding additional redundant information to provide error correction.
- Convolution codes operate on serial data, one or a few bits at a time and may use Exclusive-Or logic and shift registers.
- This type of error correction is used in wireless OFDM schemes.

FCC Rules for FHSS

- Prior to 8-31-00
  - Use 75 of the 79 channels
  - Output $Power_{max}$ = 1 Watt
  - $Bandwidth_{max}$ = 1 MHz
  - Data $Rate_{max}$ = 2 Mbps
- After 8-31-00
  - Only 15 of the 79 channels required
  - Output $Power_{max}$ = 125 mW
  - $Bandwidth_{max}$ = 5 MHz
  - Data $Rate_{max}$ = 10 Mbps

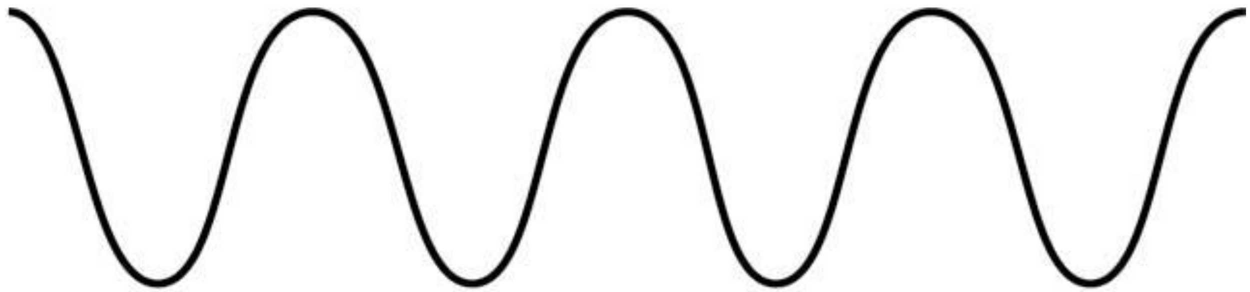
Co-location

- Co-location is the ability to place multiple devices in a frequency space minimal interference
- FHSS has many more frequencies/channels then DSSS which only has 3 co-location channels.
- However, 3 DSSS access points co-located at 11 Mbps each would result in a maximum throughput of 33 Mbps. It would require 16 access points co-located for FHSS to achieve a throughput of 32 Mbps.

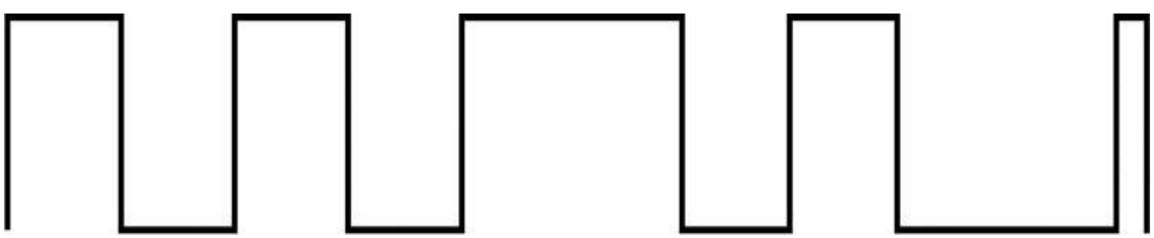
Modulation

- Carrier signal is a continuous electrical signal
  - Carries no information
- Three types of modulations enable carrier signals to carry information
  - Height of signal
  - Frequency of signal
  - Relative starting point
- Modulation can be done on analog or digital transmissions

Analog vs. Digital Transmissions



Analog Signal = A signal that has continuously varying voltages, frequencies, or phases. All amplitude values are present from minimum to maximum signal levels.

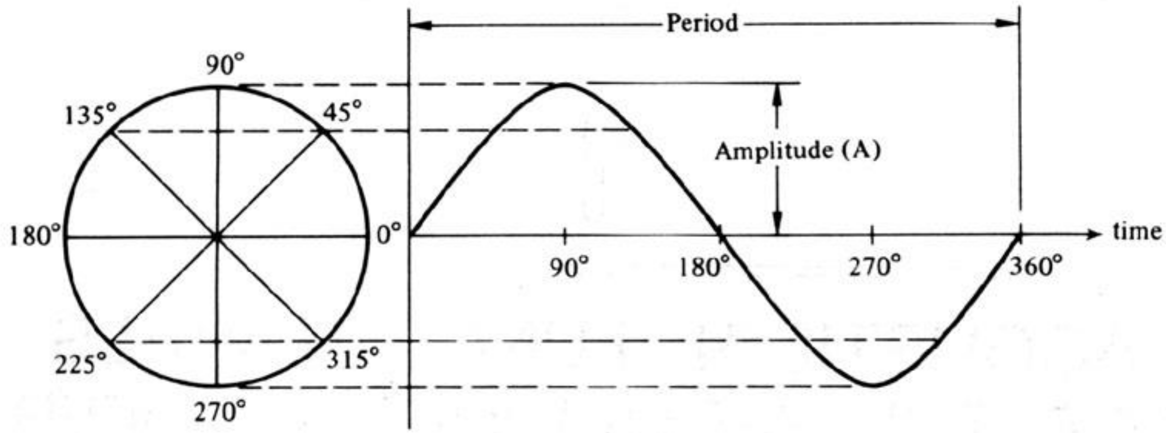


Digital Signal = A signal in which information is carried in a limited number of different discrete states or levels; High/Low, One/Zero, 1/0

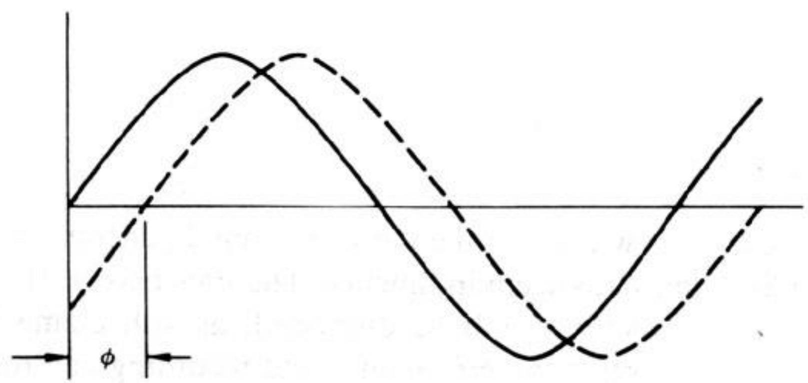
Analog and Digital Modulation

- **Analog Transmission** use analog carrier signals and analog modulation.
- **Digital Transmission** use analog carrier signals and digital modulation.
- **Modem (MOdulator/DEModulator):** Used when digital signals must be transmitted over analog medium
  - On originating end, converts distinct digital signals into continuous analog signal for transmission
  - On receiving end, reverse process performed
- **WLANs** use digital modulation of analog signals (carrier signal)

Frequency and Period



(a)

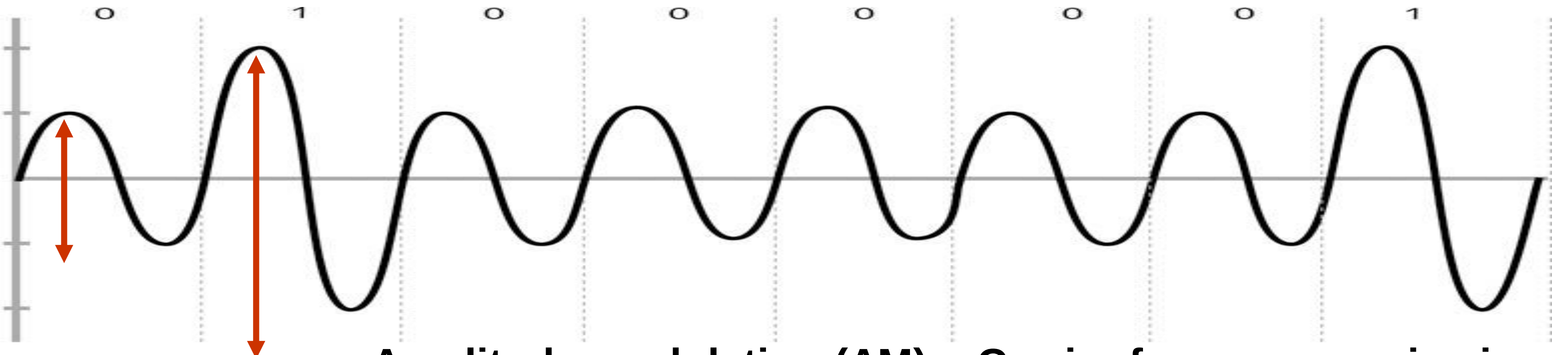


(b)

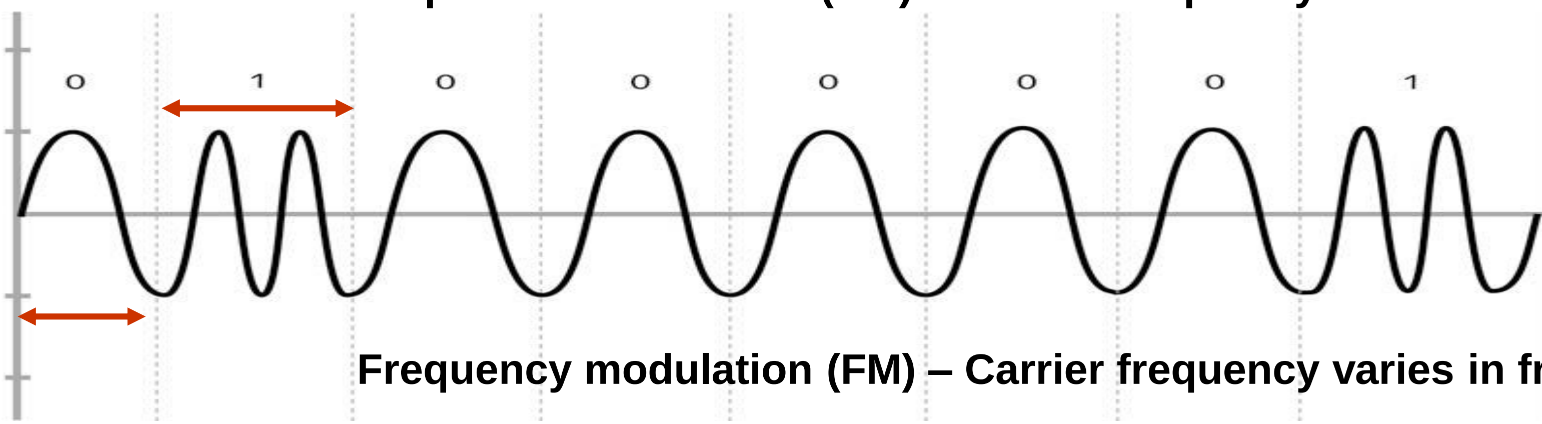
Analog Modulation

- **Amplitude:** Height of carrier wave
- **Amplitude modulation (AM):** Changes amplitude so that highest peaks of carrier wave represent 1 bit while lower waves represent 0 bit
- **Frequency modulation (FM):** Changes number of waves representing one cycle
  - Number of waves to represent 1 bit more than number of waves to represent 0 bit
- **Phase modulation (PM):** Changes starting point of cycle
  - When bits change from 1 to 0 bit or vice versa

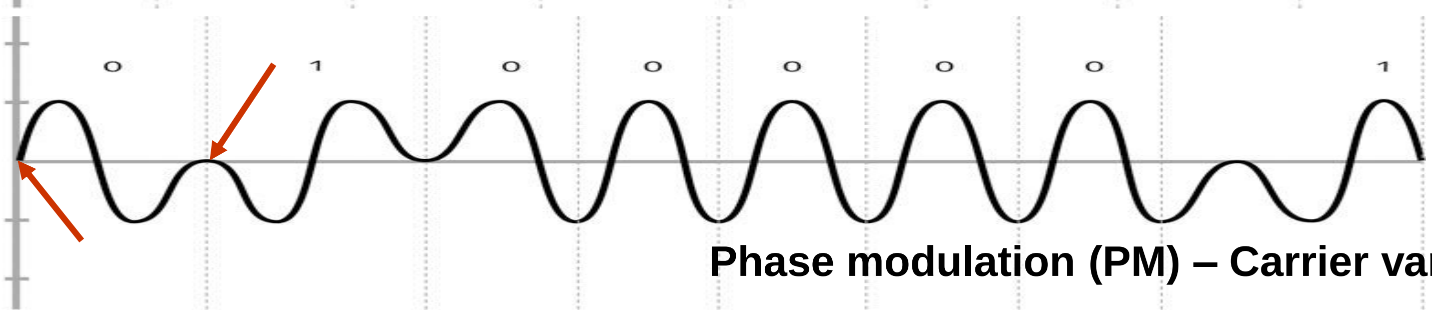
Analog Modulation



Amplitude modulation (AM) – Carrier frequency varies in amplitude



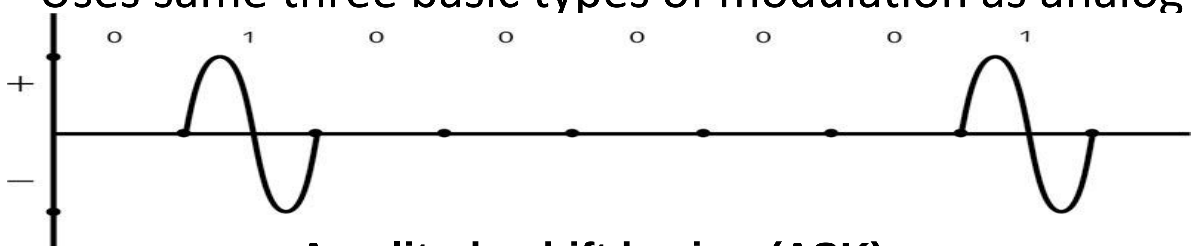
Frequency modulation (FM) – Carrier frequency varies in frequency



Phase modulation (PM) – Carrier varies in phase

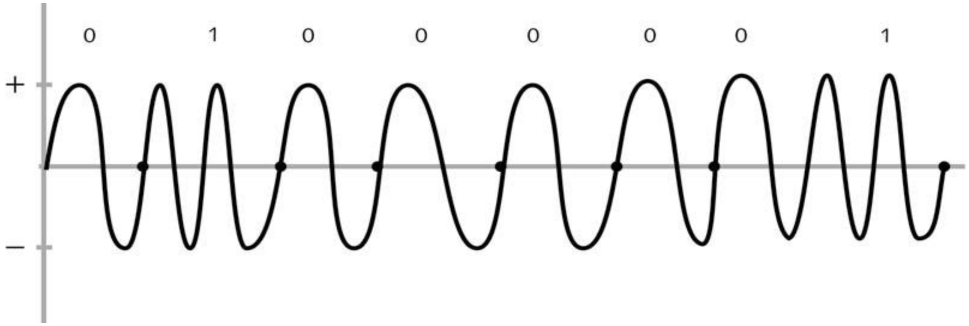
Digital Modulation

- Advantages over analog modulation:
  - Better use of bandwidth
  - Requires less power
  - Better handling of interference from other signals
  - Error-correcting techniques more compatible with other digital systems
- Unlike analog modulation, changes occur in discrete steps using binary signals
  - Uses same three basic types of modulation as analog

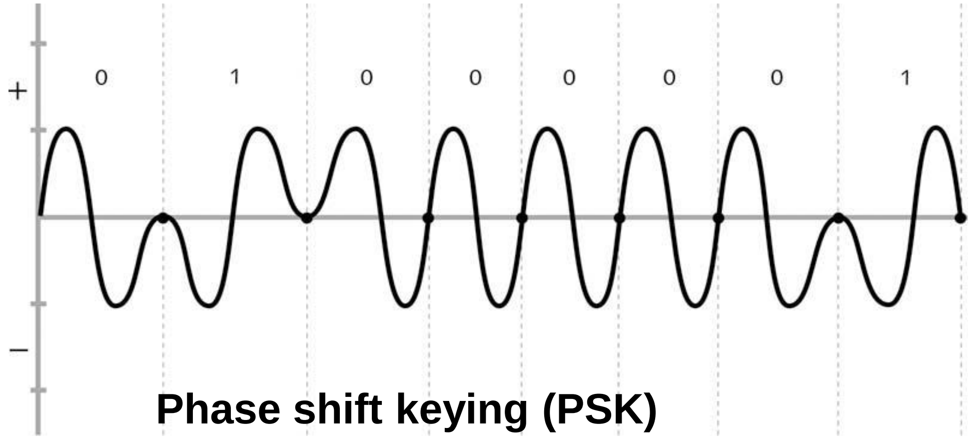


Amplitude shift keying (ASK)

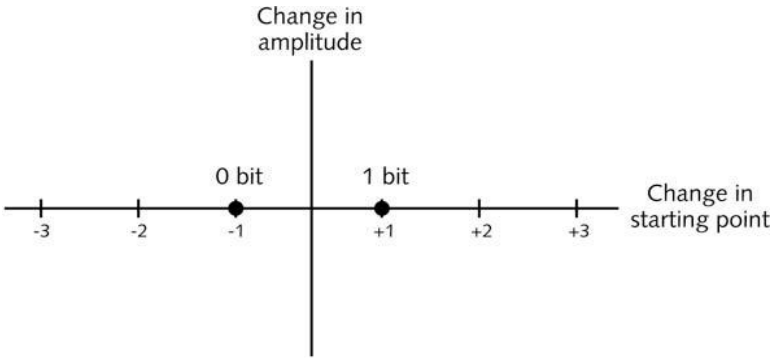
Digital Modulation



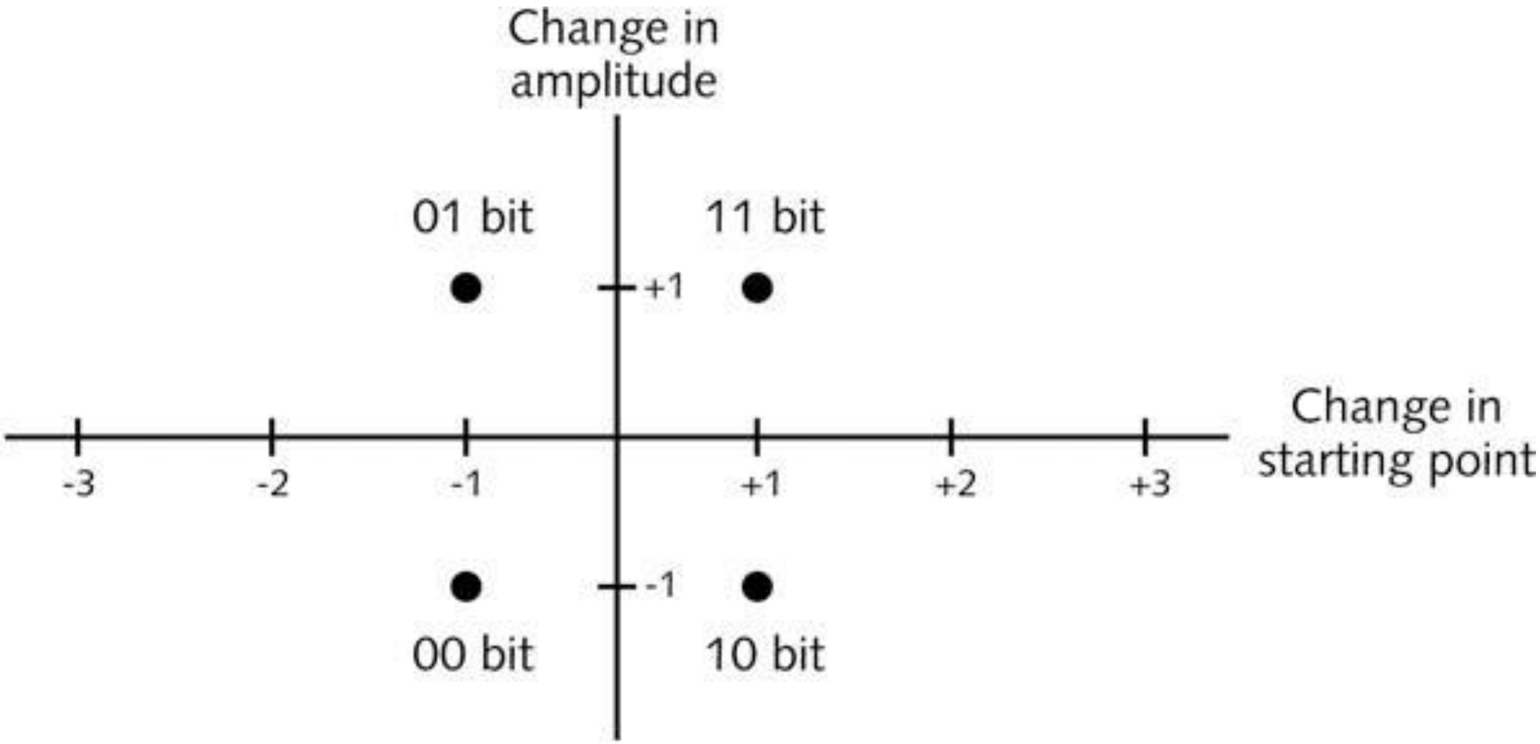
Frequency shift keying (FSK)



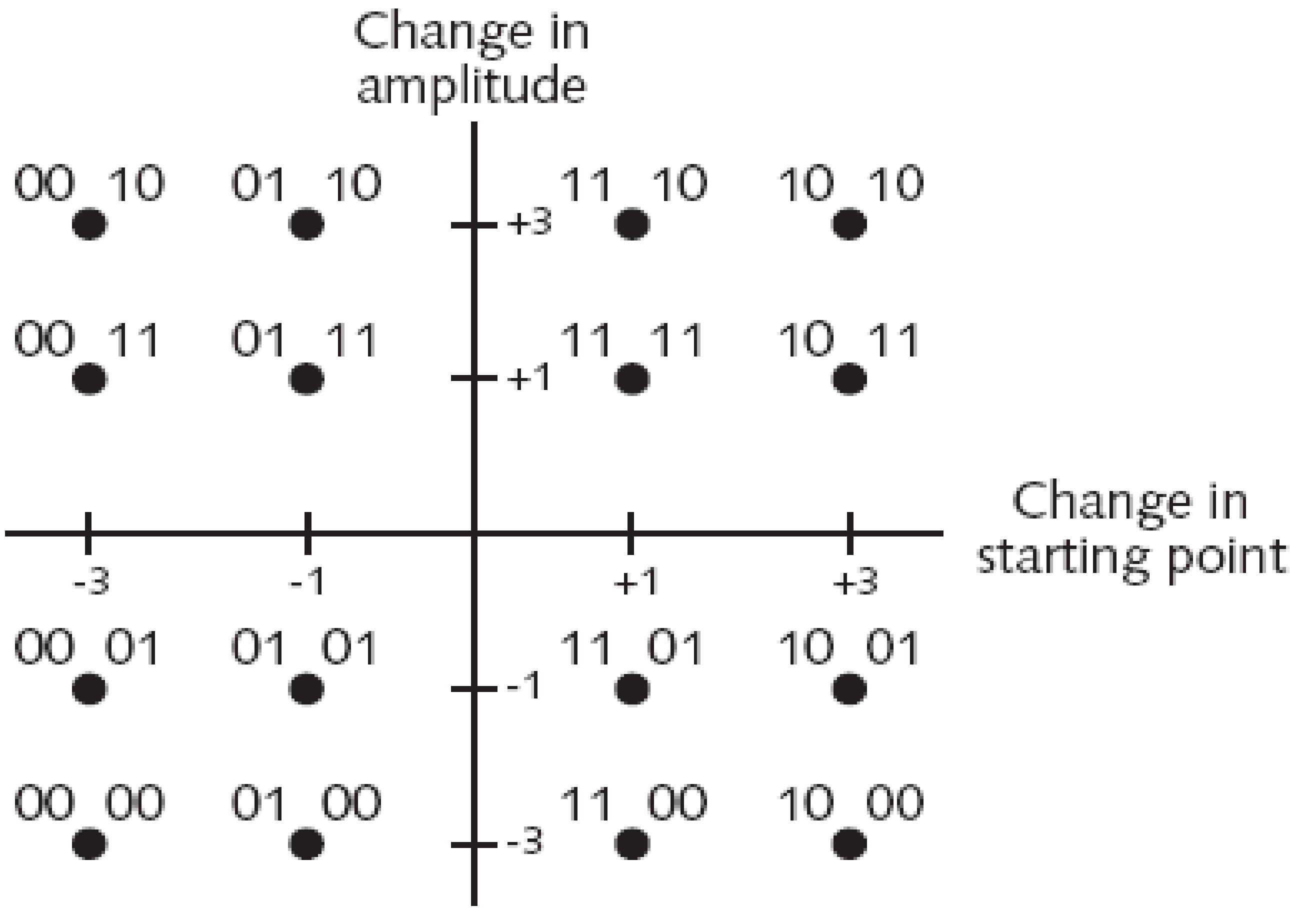
Phase shift keying (PSK)



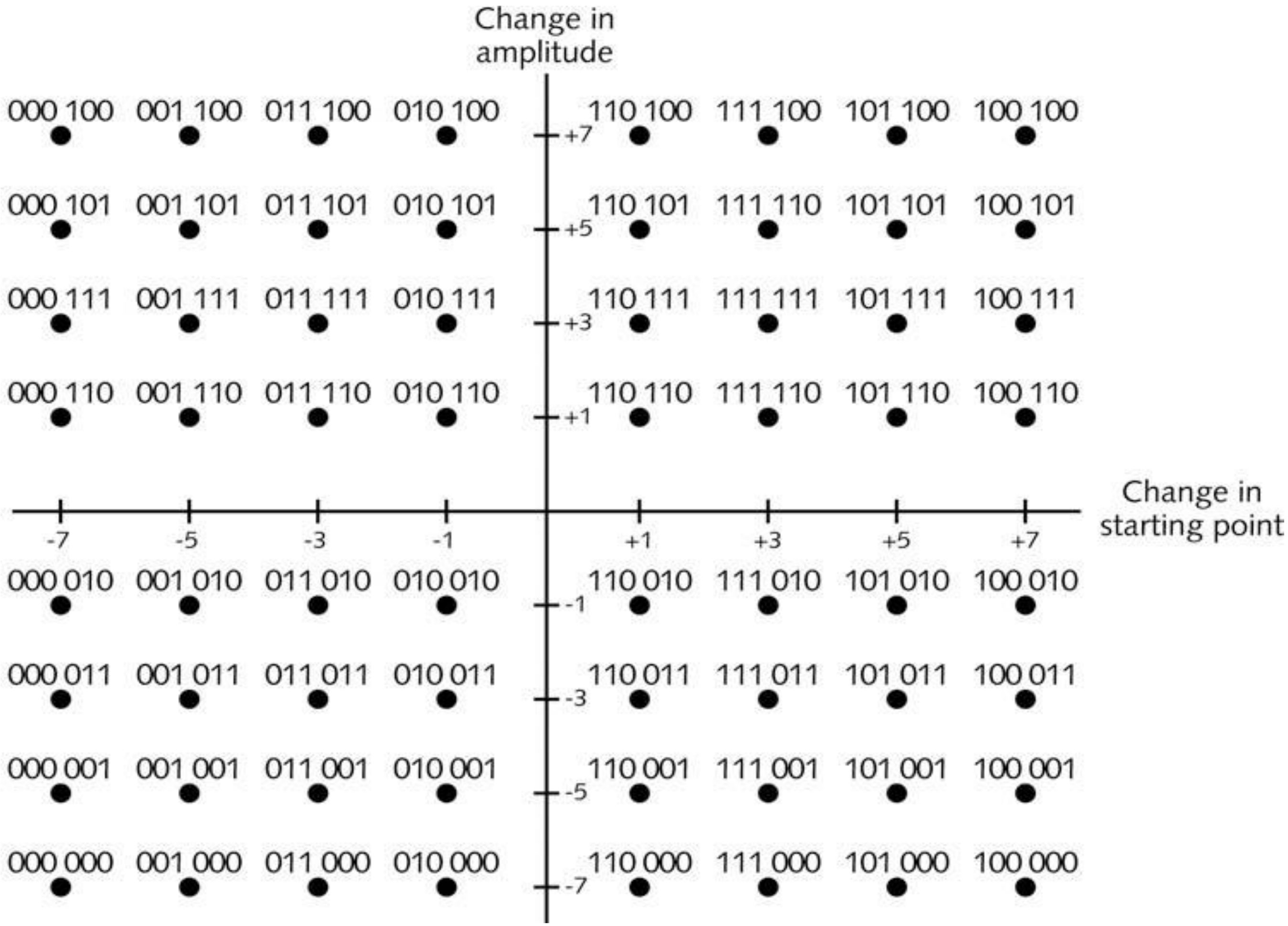
Quadrature phase shift keying (QPSK)



16-QAM Modulation



64-QAM - 64-level Quadrature Amplitude Modulation

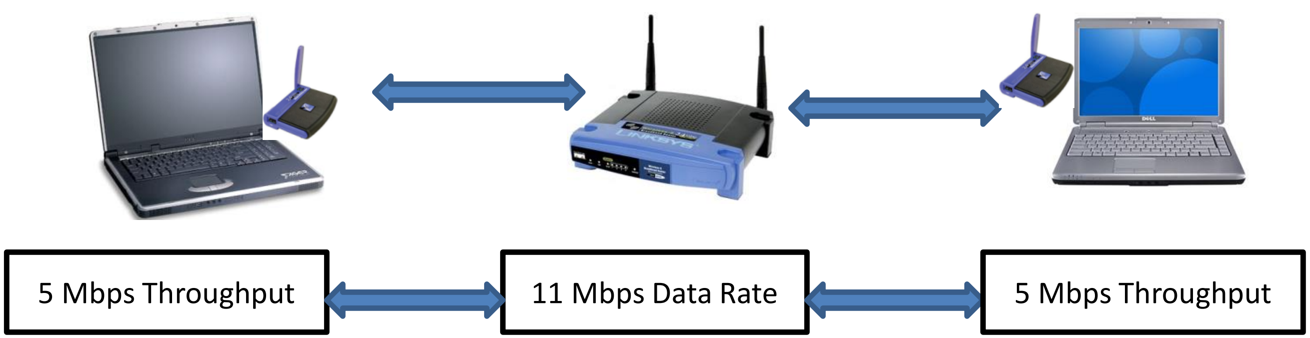


Summary

PHY	Data Rates	Frequency Band	Standards	Max Colocated WLANs	Max Total Service Area Data Rate
FHSS	1 or 2 Mbps	2.4 GHz ISM	IEEE 802.11 1997	79 max, 12 practical	24 Mbps practical
DSSS	1 or 2 Mbps	2.4 GHz ISM	IEEE 802.11 1997	2 or 3	6 Mbps
HR/ DSSS	1, 2, 5.5, or 11 Mbps	2.4 GHz ISM	IEEE802.11b 1999	3	33 Mbps
ERP	1-54 Mbps	2.4 GHz ISM	IEEE 802.11g 2003	3	162 Mbps
OFDM	6-54 Mbps	5 GHz U-NII	IEEE 802.11a 1999	23	648 Mbps

Throughput vs. Data Rate

- Data Rate = Total Data Rate through system
- Throughput = Data Payload Rate
- Data Rate = Data Payload Rate + Overhead
- Overhead = Coding + Modulation+ Bandwidth + Hardware + Software + Retransmission(errors)

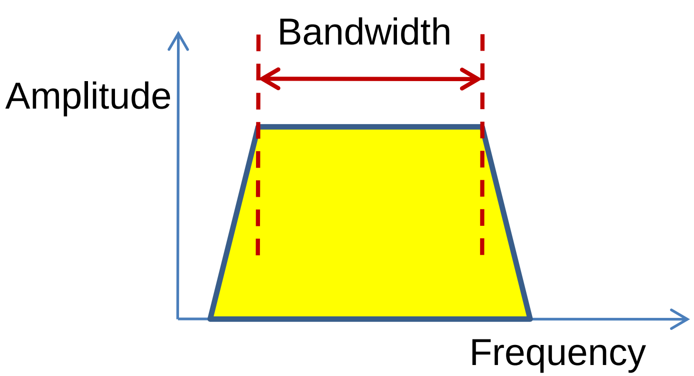


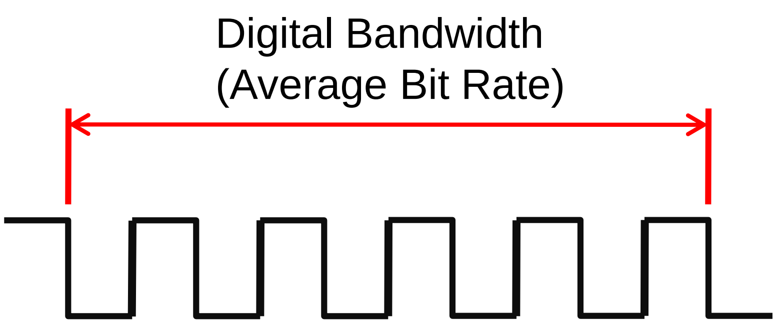
Data Rates and Throughput Estimates

PHY	Standards	Data Rate	Throughput
FHSS	IEEE 802.11-1997	1–2 Mbps	0.7–1 Mbps
DSSS	IEEE 802.11-1997	1–2 Mbps	0.7–1 Mbps
HR/DSSS	IEEE 802.11b-1999	1, 2, 5.5, and 11 Mbps	3–6 Mbps
ERP	IEEE 802.11g-2003	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	3–29 Mbps
OFDM	IEEE 802.11a-1999	6, 9, 12, 18, 24, 36, 48, 54 Mbps	3–29 Mbps
HT	IEEE 802.11n-2009	1–600 Mbps (with 4 spatial streams)	~ 100 Mbps

Bandwidths

- Analog Bandwidth – Frequency in Khz,Mhz (1 Mhz)
- Digital Bandwidth – bits per second (11 Mbps)
- Wireless Bandwidth – Frequency Space made available to network devices (22 Mhz)





Communication Resilience

- Resistance to interference
- FHSS best resilience but lowest throughput
- OFDM next best resilience and higher throughput
- HT-OFDM in IEEE 802.11n will provide the best resilience and the best throughput

Orinoco Gold 802.11b

Frequency Channels	11, 2400 - 2483.5 MHz
Modulation Technique (DSSS)	CCK,DQPSK, DBPSK
Encoding (Spreading)	11 - chip Barker Sequence
Nominal Output Power	15 dBm (31.6 mW)

11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
25m (80ft)	35m (115 ft)	40m (130 ft)	50m (165 ft)
-82 dBm	-86 dBm	-91 dBm	-94 dBm

Orinoco 802.11 abg

Frequency Channels	FCC (26 Channels) 2400-2484; 5150-5250; 5250-5350; 5725-5850 MHz ETSI (32 Channels) 2400-2484; 5150-5250; 5250-5350; 5470-5720 MHz TELEC (18 Channels) 2400-2484; 5150-5250 MHz IDA (22 Channels) 2400-2484; 5150-5250; 5725-5850 MHz
Modulation Technique	802.11a, 802.11g Orthogonal Frequency Division Modulation (64 QAM, 16 QAM, QPSK, BPSK) 802.11b Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK)
Data Speeds	802.11a, 802.11g modes: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11b mode: 11, 5.5, 2, 1 Mbps 2X mode: 108, 96, 72, 48, 36, 24, 18, 12 Mbps
Max Output Power	802.11a, 802.11g: 60 mW EIRP 802.11b: 85 mW EIRP