ITSC 301: Wireless Security

Module 3 - Layer One Technologies

Table of Contents

- Review Lecture and Lab
- Antennas
- Spread Spectrum
- Encoding, Modulation and Multiplex

Review Lecture & Lab

Review Module 2

- Radio Terminology
- RF History
- RF Basics
- Units & Conversion

Antennas

Introduction

- This module will examine the characteristics of antennas, modulation techniques and other Layer 1 technologies to help you design, attack and defend wireless systems.

Learning Outcome

- Evaluate the physical layer characteristics and devices common to wireless networks to select the appropriate layer-1 technologies

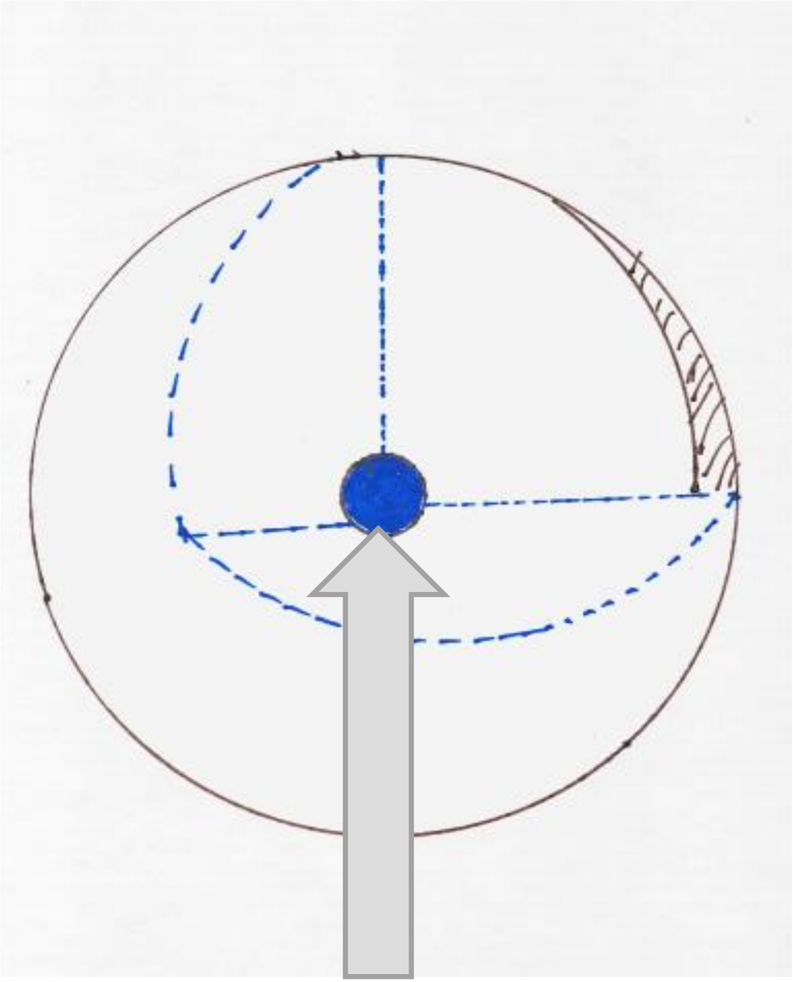
Antennas

- All antennas are passive devices, therefore power radiated will always be less than the power received from the transmitter.
- All antennas are reciprocal devices, therefore the same antenna design may be used to both transmit and receive.
- TX antennas receive electrical energy and convert it to electromagnetic waves to be launched into space.
- RX antennas capture electric and magnetic fields and cause current to flow in conductors, and are then transferred to transmission lines and forwarded to receiver.

Antennas: Definitions

- Isotropic radiation has the same intensity, regardless of the direction of measurement.
- An isotropic field exerts the same action, regardless of how the antenna is oriented.
- Energy is radiated uniformly in all directions from a single point, sometimes called an *isotropic radiator.*

Antennas: Isotropic Pattern



check

Figure 1: Title

Antennas: Half-Wave Dipole

- Simple and popular antenna
- Sometimes referred to as a *Hertz antenna*
- An open transmission line has a voltage maximum at its open end, and a current maximum one-quarter wavelength from the end
- If the balanced transmission line is separated to one-quarter wavelength, the electric field stretches away from the conductors
- If the separation continues, part of the field detaches and forms electromagnetic waves

Creating an Antenna

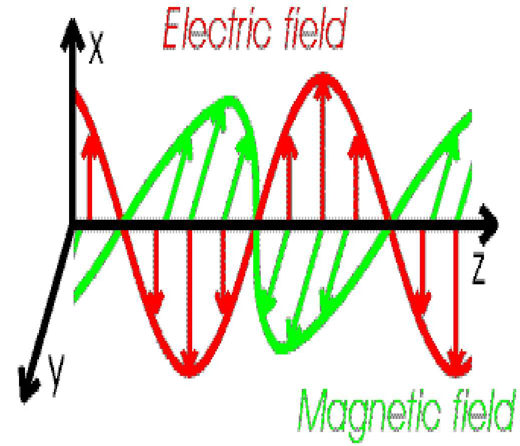


Figure 2: Title
Source: Michigan State University, 2000. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

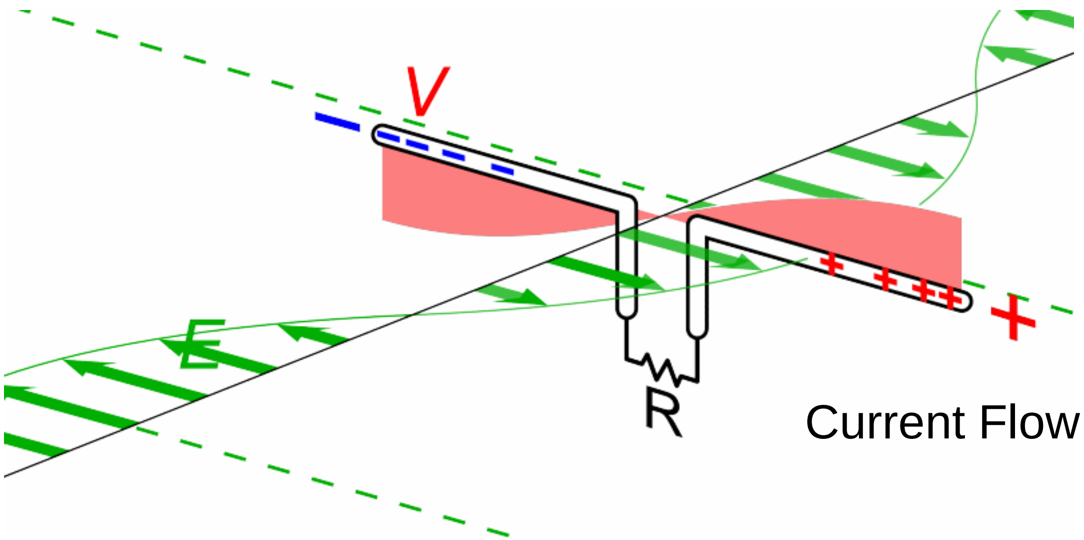


Figure 3: Dipole Receiving Antenna
© 2015, Chetvomo,
https://commons.wikimedia.org/wiki/File:Dipole_receiving_antenna_animation_6_800x394x150ms.gif (CC0 1.0)

Antennas: Gain

- Power gain in one direction will be at the cost of losses in other directions.
- Real antennas incur losses. The energy they receive is less than they are able to launch into space.
- The efficiency of a dipole antenna is approximately 85%
- The directivity of any dipole is 2.14 dbi

Important

Example

A dipole antenna has an efficiency of 85%. Calculate its gain.

1. Directivity of 2.14 dbi converted to power ratio.
   D = log-1 2.14/10 = 1.638
2. Gain = Directivity X efficiency 1.638X 0.85=1.39
3. Gain converted to dbi = 10log 1.39 = 1.43 dbi
4. Gain is the ratio of an antenna's increase in reference to an ideal antenna.

Antennas: Dipole

- Dipole antenna pattern imposed on an isotropic pattern:

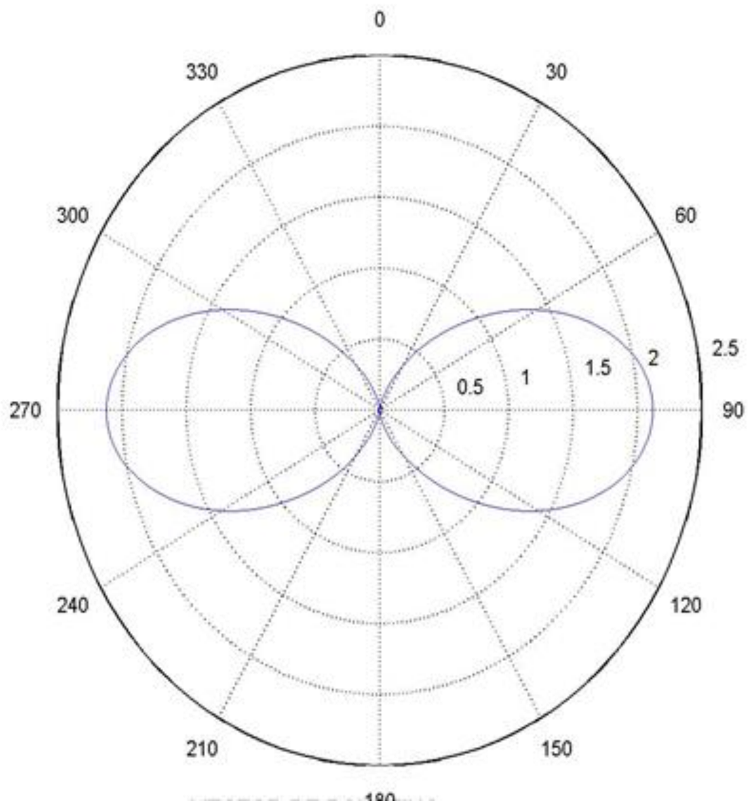


Figure 4: Title
Source: ?

Antennas: Beam Width

- Flashlights emit a beam of light energy, as do directional antennas
- The width of the beam is the angle between its half power points
- The power level is 3 db less than at maximum point
- A half wave dipole has a beam width of 78° in one plane and 360° in the other
- A half wave dipole has what we would call a *broad beam width*

Important

Antennas: Half-Wave Dipole

- Simple and popular antenna
- Sometimes referred to as a *Hertz antenna*
- An open transmission line has a voltage maximum at its open end, and a current maximum one-quarter wavelength from the end
- If the balanced transmission line is separated to one-quarter wavelength, the electric field stretches away from the conductors
- If the separation continues, part of the field detaches and forms electromagnetic waves

Antennas: Folded Dipole

- Same length as a half wave dipole, but with two parallel conductors connected at both ends and separated by a short distance
- Has wider bandwidth than half wave dipole
- Used in TV and FM broadcast receivers
- Uses a 300 ohm balanced line, sometimes called a twin lead
- Current is divided by two, voltage is multiplied by two, therefore folded dipole has four times the feed point impedance

Antennas: Folded Dipole

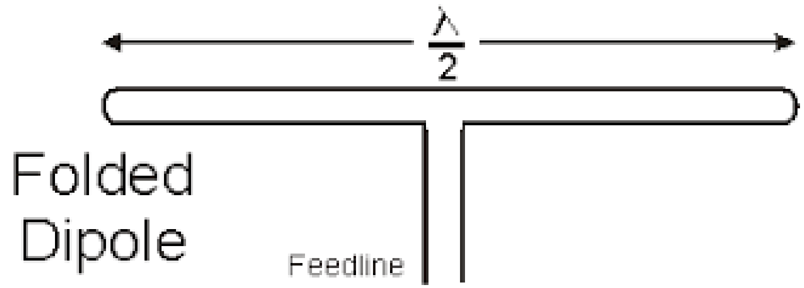


Figure 5: Title
Source: ?

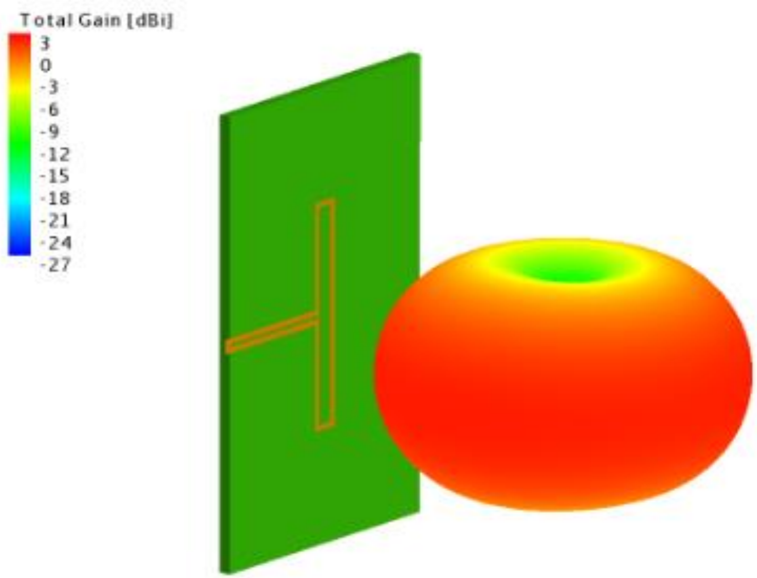


Figure 6: Folded Dipole
Source: Antenna Magus, 2018. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Antennas: Ground Plane

- Serves as a reference ground allowing the antenna to function
- Acts as the return path for dipole two element, half wave long, center-fed antenna.
- The nearer a ground plane measures to zero ohms, the better.

Antennas: Yagi

- The Yagi-Uda is the most popular type of parasitic array
- A parasitic array has only one element fed by a transmission line
- The other elements absorb and re-radiate power from the driven element
- The driven element is a half wave or folded dipole
- Reflectors are longer than 1/2 wavelength
- Directors are less than 1/2 wavelength

Antennas: Yagi Array

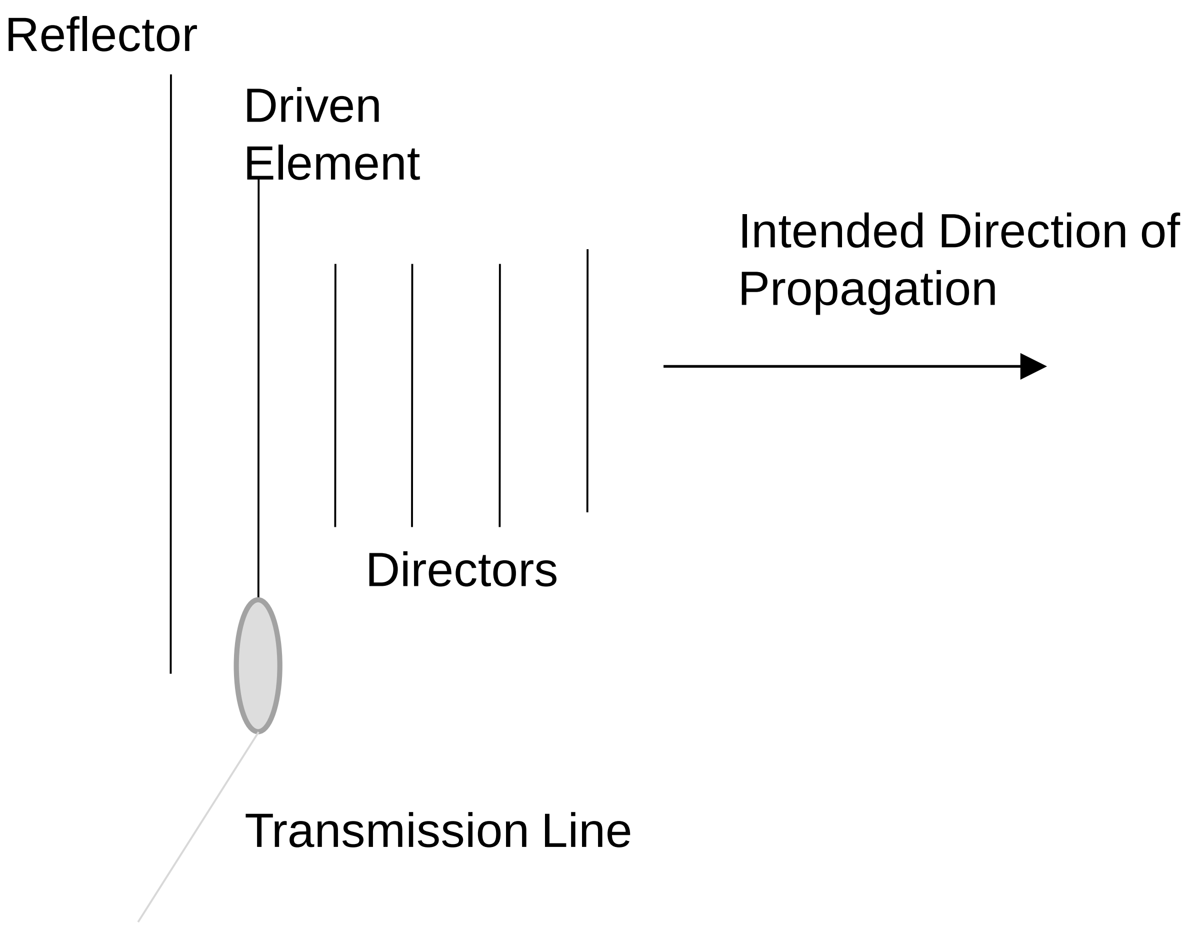


Figure 7: Title

© 2018, Southern Alberta Institute of Technology

Antennas: Yegi Array

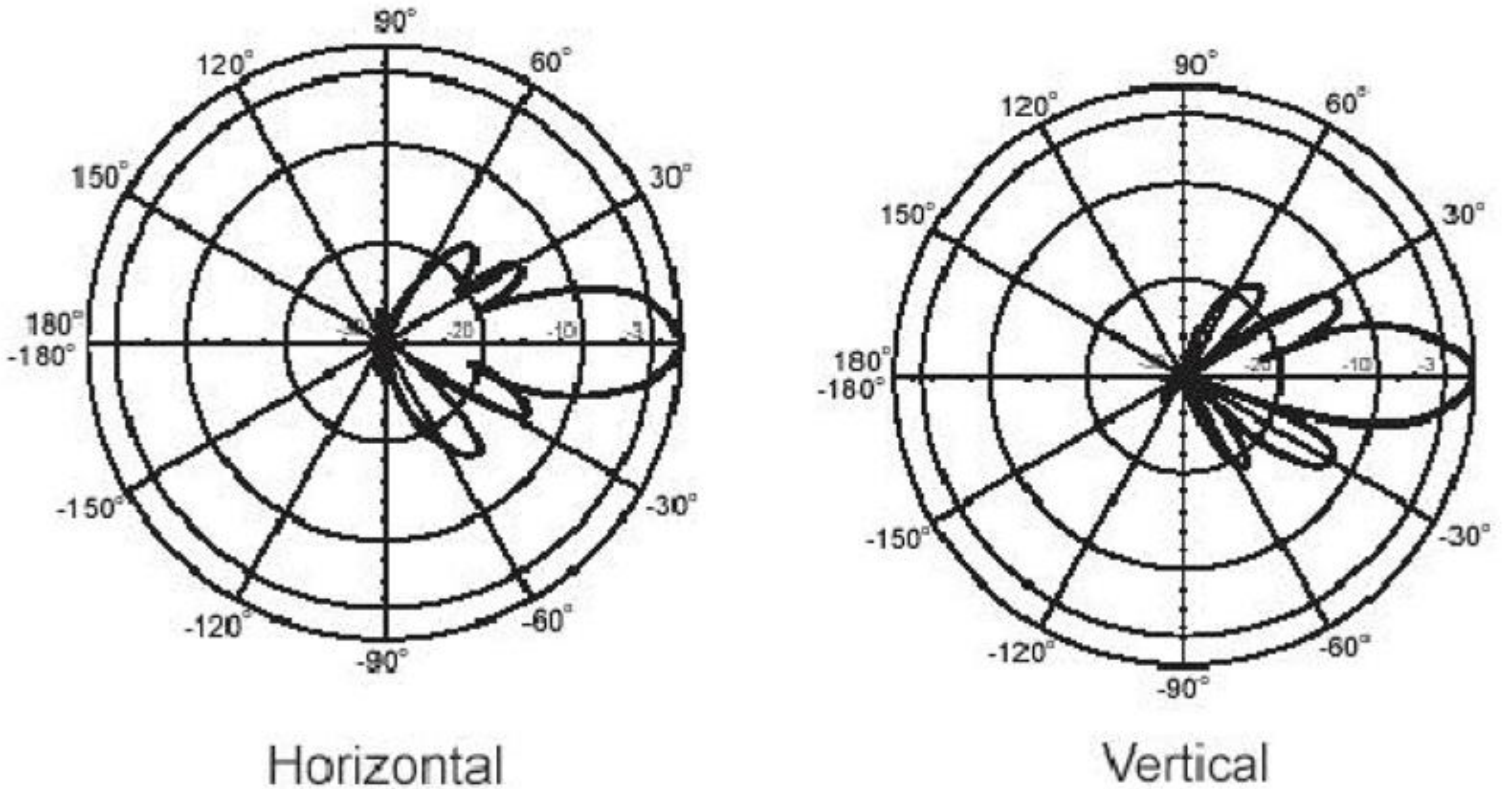


Figure 8: title

Source: D-Link, 2018. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

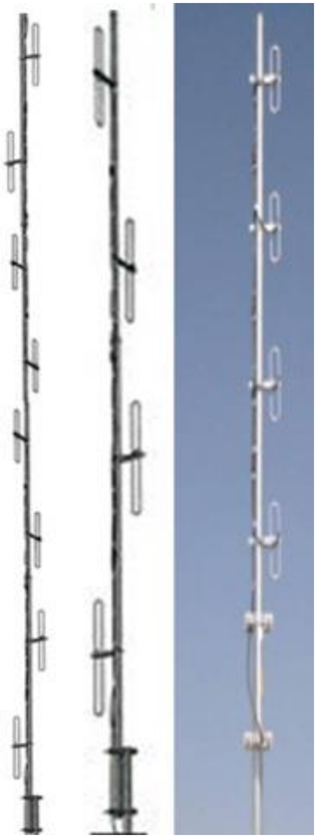
Antennas: Collinear

- Phased arrays can be constructed by joining several simple half-wavelength dipole antennas
- Signals in phase are added
- Half wavelength elements are each fed with 1/4 wavelength transmission lines
- *Collinear* because the axes of elements are along the same line
- Collinear antennas are often mounted with main axis vertical
- They are then omni-directional in the horizontal plane
- They are used as base station antennas

Important

Antennas: Collinear

Half Lambda Dipole Collinear Array



Dipole Collinear Array Radiation Patterns

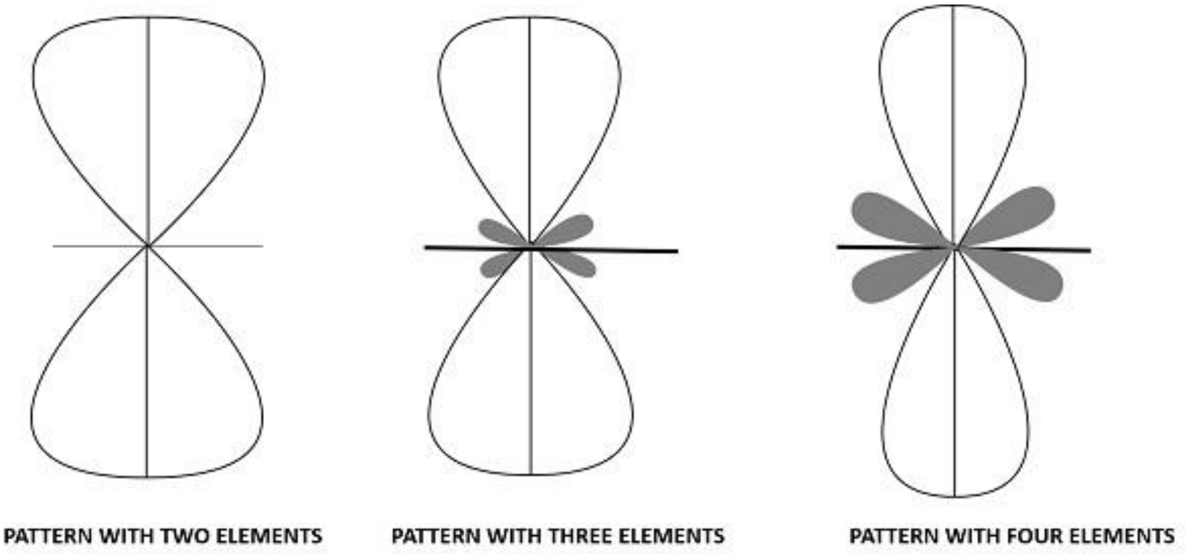


Figure 10: title
Source: Tutorials Point, 2018. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Figure 9: title
Source: Antenna Experts, 2018. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Antennas: End Fire Array

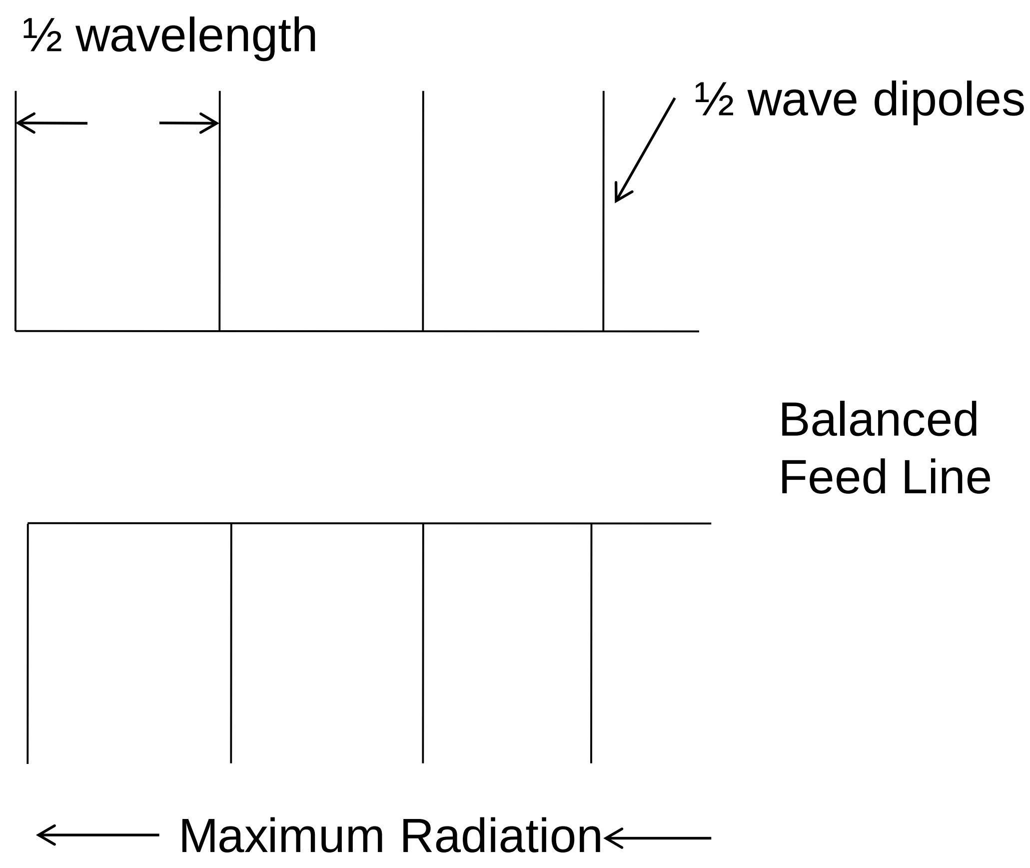


Figure 11: Title
© 2018, Southern Alberta Institute of Technology

Antennas: Horn Antenna

- Horn antennas are generally used where a waveguide is deployed
- Sometimes used as feed horns for parabolic antennas
- See http://en.wikipedia.org/wiki/Horn_antenna

Antennas: Parabolic Reflector

- Any ray where the source is the focus point will strike the reflecting surface parallel to the axis of the parabola.
- A parabolic reflector uses a small antenna as the focal point for a larger parabolic reflecting surface.

Antennas: Parabolic Reflective Surface

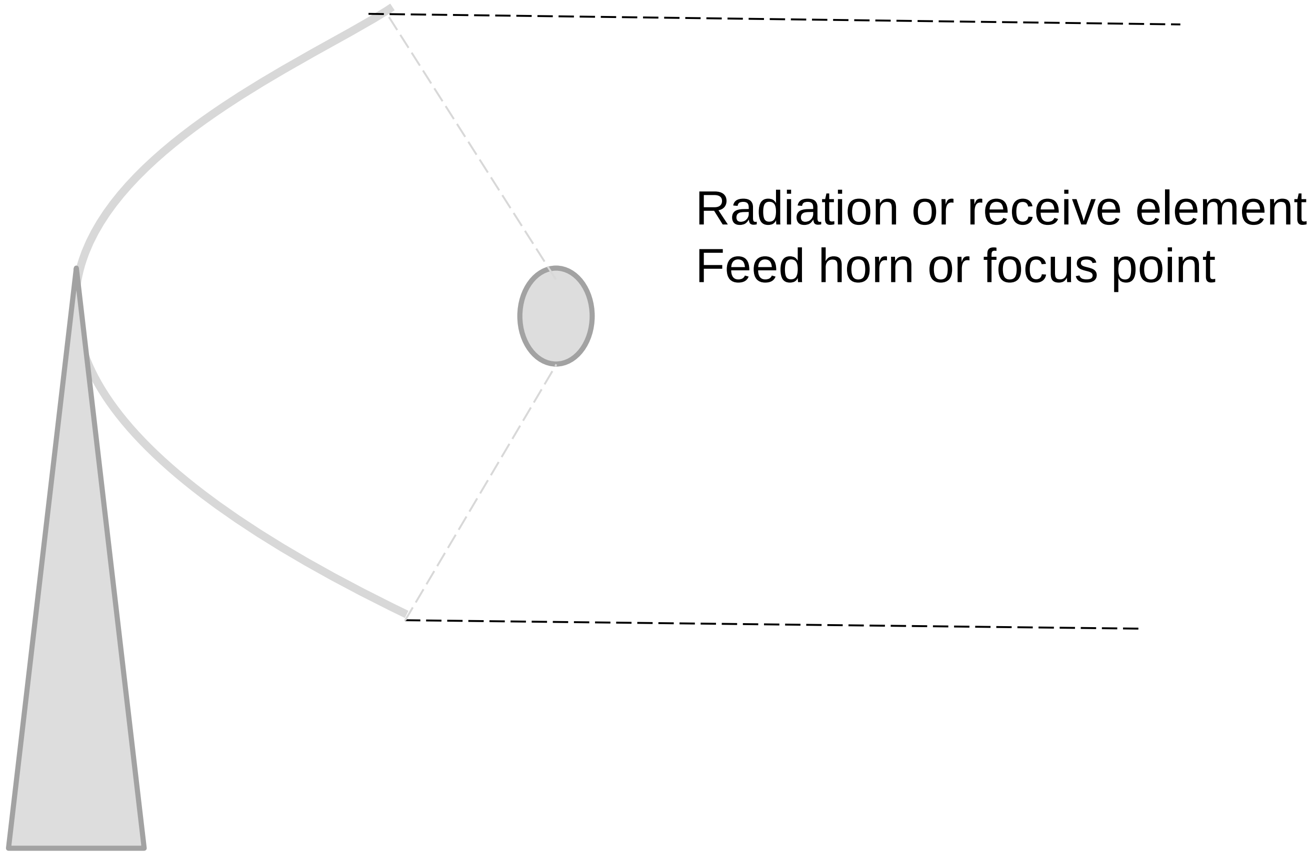


Figure 12: Title

802.11 Antenna

- Antenna Measurement https://en.wikipedia.org/wiki/Antenna_measurement
- Radiation Pattern https://en.wikipedia.org/wiki/Radiation_pattern
- Wifi https://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)

Spread Spectrum

Spread Spectrum

Why use spread spectrum?

- Power is reduced nearly to the noise floor
- Power is costly and difficult to transport
- Minimum power to operate end device is most desirable
- More secure, as it is offers greater resistance to eavesdropping
- Greater immunity to fading effects

Spread Spectrum

- Process converts a signal from narrowband to wideband, and then back to narrowband

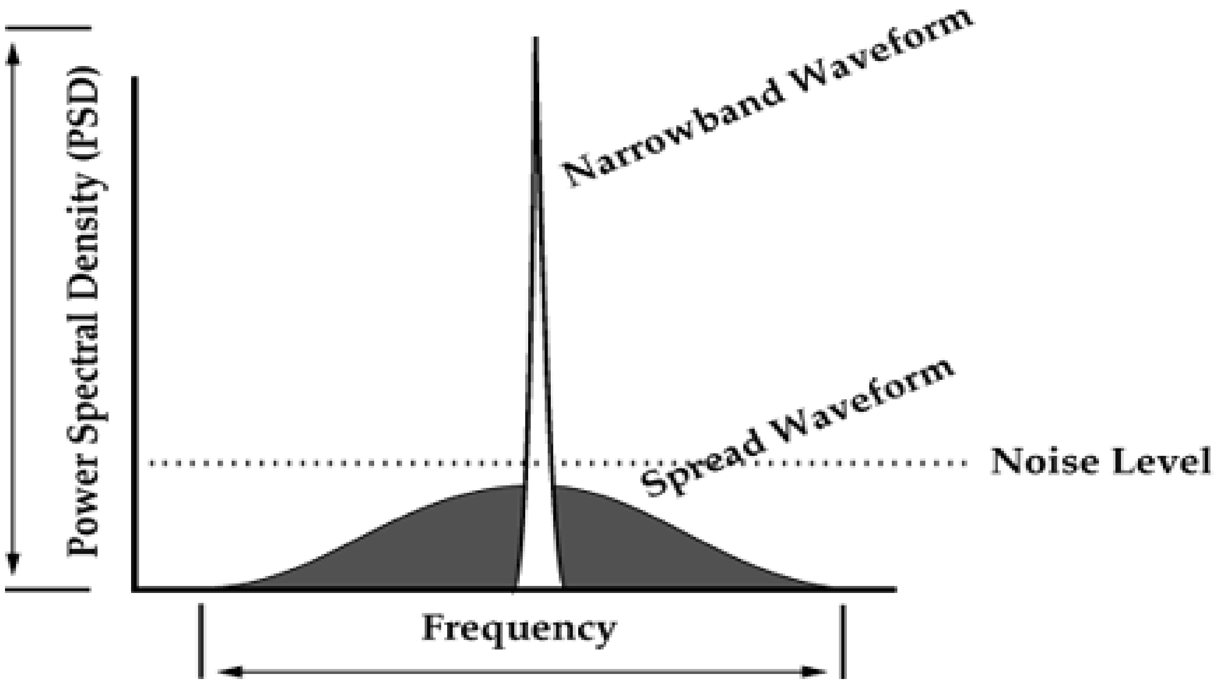


Figure 13: title

Source: Price, H., 1995. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Spread Spectrum

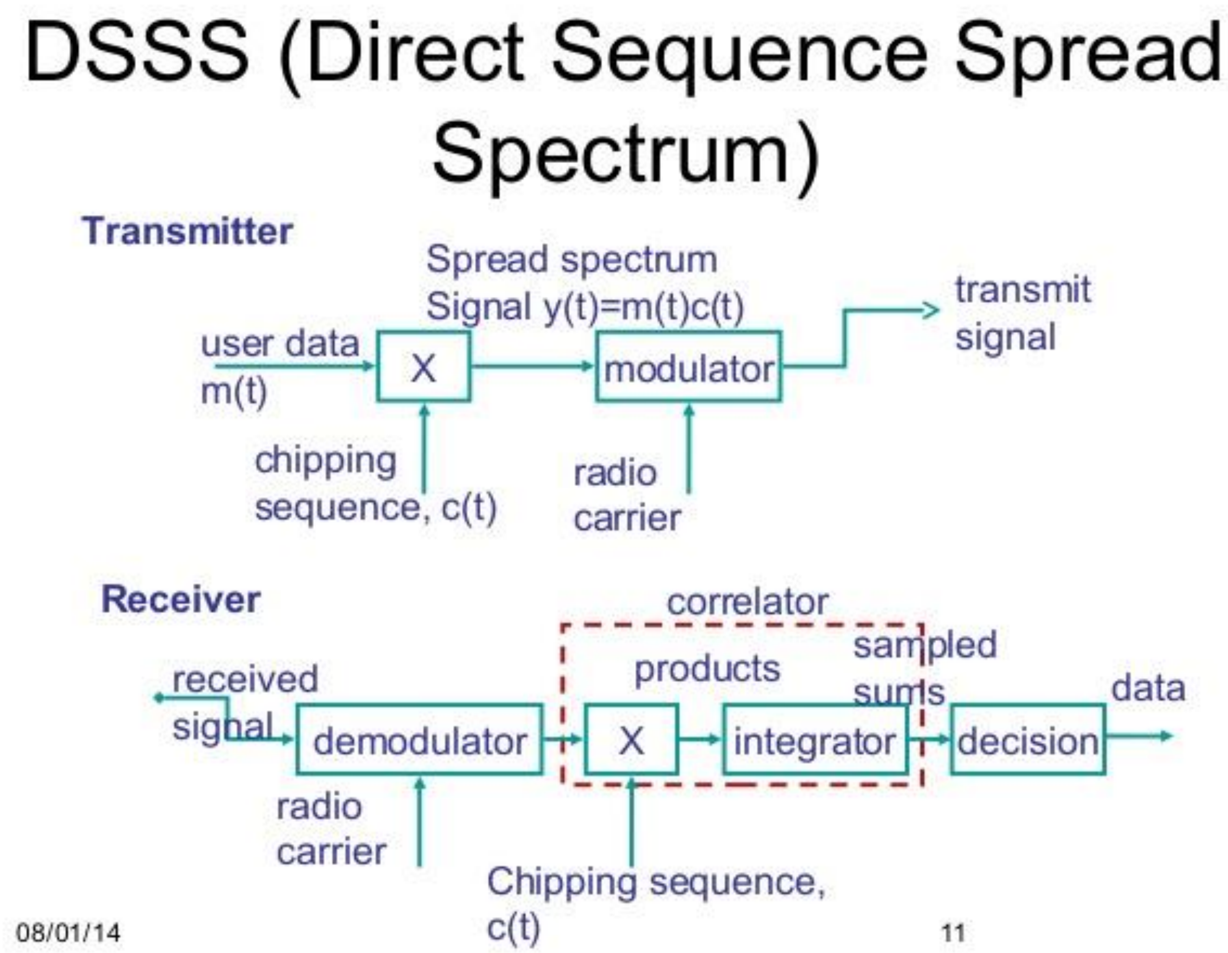


Figure 14: title

Source: Ajala, J., 2014. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Direct Sequence Spread Spectrum

- Each RF channel support 64 orthogonal channels using DSS (Direct Sequence Spread Spectrum)
  - One pilot channel (phase reference)
  - One sync channel (Precise GPS timing reference)
  - Seven paging channels (control and paging)
  - 55 traffic channels
- 1.25 MHz of BW for 55 voice channels = 22.7 kHz/channel
- Offers greater spectrum efficiency than GSM

Spread Spectrum

Direct Sequence Technique

- Each baseband signal is combined with a pseudo-random noise (PN) at a high rate
- Each signal is orthogonal (at right angles) but this allows them to receive as originals
- Deviation from the exact orthogonal relationship produces noise
- Too much noise results in a decreased signal-to-noise ratio and a high bit error rate

Spread Spectrum

- Walsh codes are a class of PN sequences
- 64 orthogonal Walsh codes are repeated after each 64 bits
- This creates 64 logical channels per single RF channel
- Walsh code 0 is used as a pilot or keep alive channel for phase alignment

Spread Spectrum

- Long codes provide privacy by scrambling the message data
- Short PN sequences (215 chips) distribute energy so it appears Gaussian and noise-like.
- Walsh codes provide orthogonal spreading so only the receiver with the same code can recover it
  - Other user signals seem like noise to the receiver. A 64-bit Walsh code returns a 64x processing gain. Each channel is assigned a unique Walsh code from 0 to 63. Walsh codes used to differentiate all channels in forward link.
- Channels spread using appropriate length code based on data rate.
  - Walsh codes are unique within channels of same user, as well across different users in same cell

Spread Spectrum

- Data is first scrambled for privacy and user identification by the user-specific long code
- Then the in-phase and quadrature components are mapped
- Channel gain, power control and Walsh spreading occur
- The signal is then spread by the complex PN sequence, followed by baseband filtering and frequency modulation
- Spreading narrowband over wideband has been achieved

Spread Spectrum

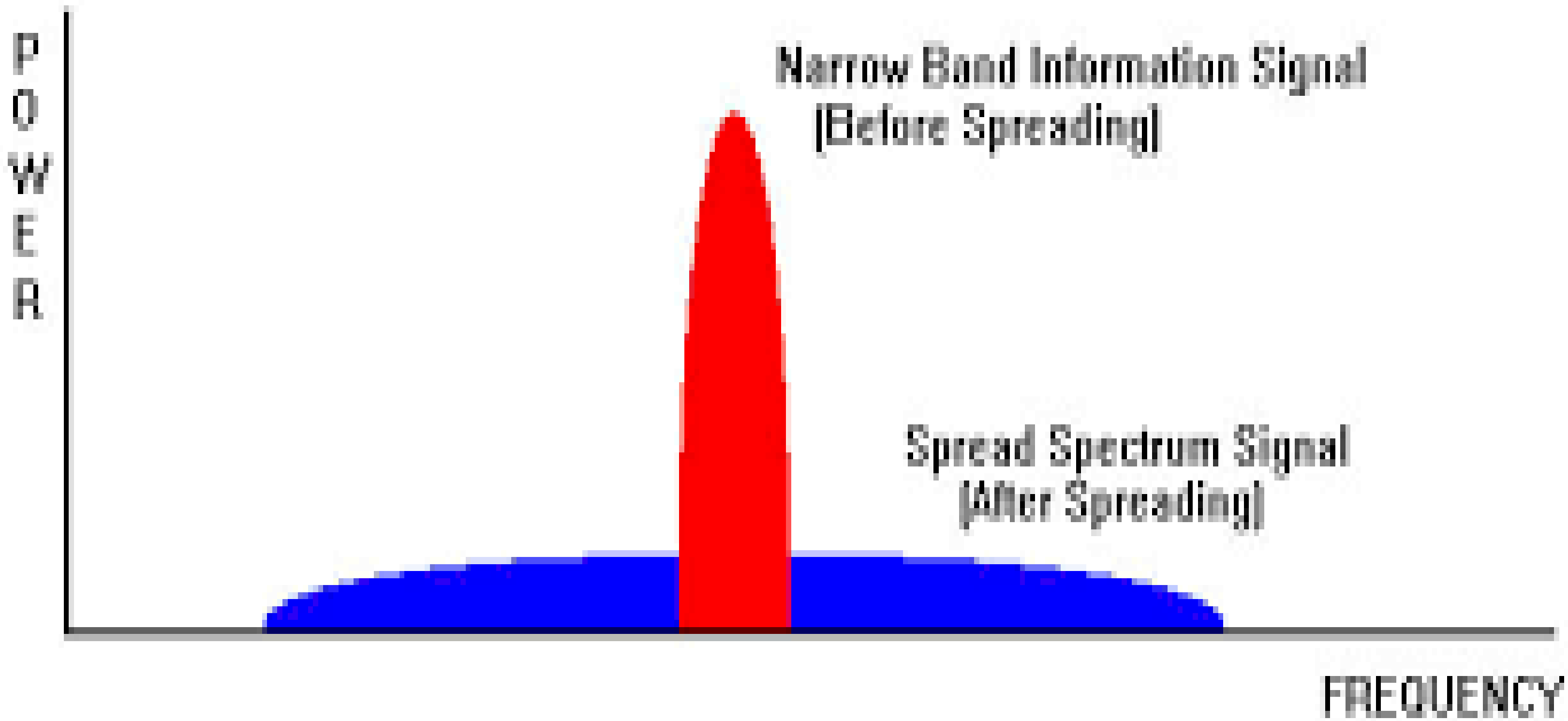


Figure 15: title
Source ?

Spread Spectrum

- In frequency hopping systems, the carrier frequency of the transmitter abruptly changes (*hops*) in accordance with a pseudo-random code sequence
- The order of frequencies selected by the transmitter is dictated by the code sequence
- The receiver tracks these changes and produces a constant IF signal

Orthogonal Frequency-Division Multiplexing

- Method of encoding digital data on multiple carrier frequencies.
- Key advantage of OFDM is that fast Fourier transforms (FFTs) may be used to simplify implementation.
  - Fourier transforms convert signals between time domain and frequency domain.
  - See https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing

Quadrature Amplitude Modulation

- Two carrier waves of the same frequency, usually sinusoids, are out of phase with each other by 90° and are called *quadrature carriers* or *quadrature components*
- At least two phases and at least two amplitudes used
- See Digital QAM: https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation

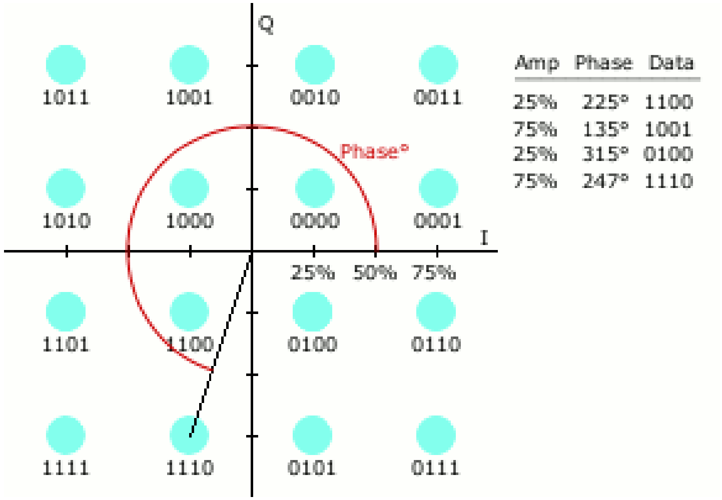


Figure 16: QAM Demonstration
© 2011, CJdamaster, https://en.wikipedia.org/wiki/File:QAM16_Demonstration.gif ([CC-BY-SA 3.0]())

Encoding, Modulation and Multiplex

Digital Radio Concepts

Time Division Multiple Access

- In 1990, TDMA was introduced by combining three digital voice channels into one 30 kHz RF channel
- For 7 or 12 cell clusters, traffic capacity more than tripled
- IS-136 is the standard and operates in both 800 MHz and 1900 MHz PCS band

Digital Radio Concepts

Time Division Multiple Access

One TDMA Frame

40 ms 1944 bits

Slot One Voice A	Slot Two Voice B	Slot Three Voice C	Slot Four Voice A	Slot Five Voice B	Slot Six Voice C

6.67 ms
324 bits

1 RF channel = 25 frames/s = 1/25x = 40 ms
1 frame = 1944 bits, 1944X25 = 48.6 kb/s
1 frame = 6 time slots, 40ms//6 = 6.67 ms
1 voice channel requires 2 time slots

Digital Radio Concepts

TDMA Voice Time Slot

CDVCC = coded digital verification color code
SACCH = slow associated control channel
Synch = synchronization

Synch 28 bit	SACCH 12 bits	Data 130 bits	CDVCC 12 bits	Data 130 bits	Reserved 12 bits

Forward channel

← 6.67 ms 324 bits →

Guard 6 bits	Ramp 6 bits	Data 16 bits	Sync 28 bits	Data 122 bits	SACCH 12 bits	CDVCC 12 bits	Data 122 bits

Reverse channel

Code Division Multiplexing (CDM)

- Also known as code division multiple access (CDMA)
- An advanced technique that allows multiple devices to transmit over the *same* frequencies at the *same* time using different codes
- **Used for mobile communications**

CDMA

- One RF channel = 1.25 MHz modulated by a 1.2288 Mb/s bit stream
- All frequencies can be used in all cells, magnifying capacity
- Base and mobiles transmit on different channels separated by 80 Mhz
- Use spread spectrum techniques
- Soft handoffs between cell sites is possible since no frequency changes are necessary

Digital Radio Concepts

- CDMA Open Loop power control is determined using this equation.

- This formula is a cellular network's answer to the Near End Problem.

$$Pt = -76\ db - Pr$$

Pt = transmit power dbm

Pr = receive power dbm

important

Multiplexing Summary

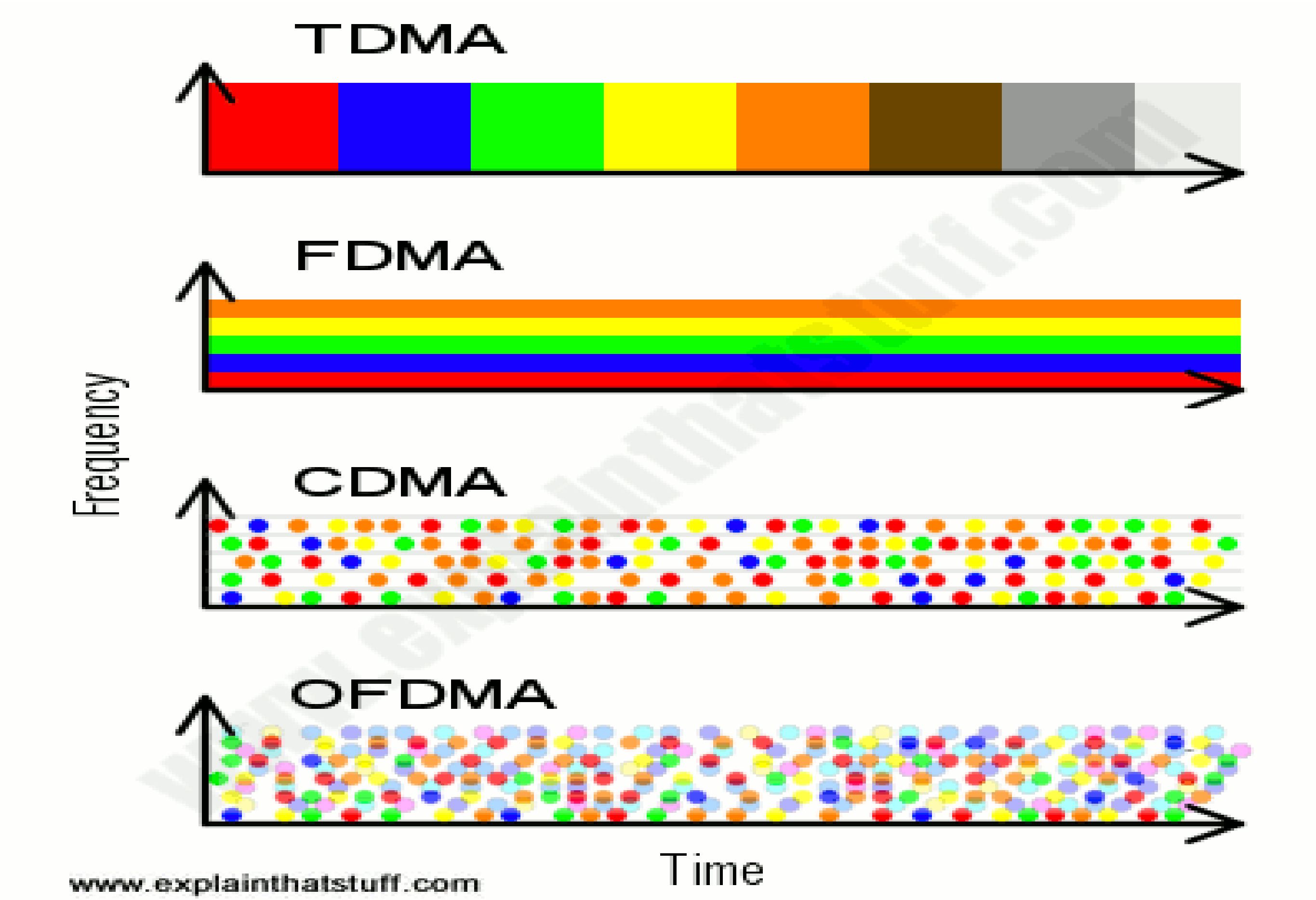


Figure xx: title

Source: Woodford, C., 2018. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Multiplexing Pros and Cons

Multiplexing Type	Advantage	Disadvantage
Frequency Division	Simple	Analog signals only
	Radio and TV	Limited and managed spectrum
	Cable TV	
	Inexpensive	
Synchronous Time Division	Digital	Inefficient use of bandwidth
	Simple	
	Popular with T1 & T3	
Statistical Time Division	Better use of available bandwidth	Complex
	Frames and packets	Precision synchronization
	Policing and QoS	
Coarse/Dense Wavelength Division	Massive and scalable capacity at optical speed	Cost
		Complexity
Code Division	Large capacity	Complexity
	Scalable	
	Security	

References

Ajala, J. (2014). Direct Sequence (DSSS). Retrieved from https://www.slideshare.net/ajal4u/dsss-final

Antenna Experts. (2018). Stacked Dipole Array. Retrieved from https://www.antennaexperts.in/product-detail.asp?cat=omni-stacked-dipole-array-antenna&id=3

Antenna Magus. (2018). Newsletter 3.3. Retrieved from http://www.antennamagus.com/newsletter-3-3.php

D-Link. (2018). 2.4GHz 18dBi High Gain Directional Outdoor Panel Antenna. Retrieved from https://www.dlink.com.sg/product/2-4ghz-18dbi-high-gain-directional-outdoor-panel-antenna/

Michigan State University. (2000). Maxwell's equations and light. Retrieved from https://web.pa.msu.edu/courses/2000fall/phy232/lectures/emwaves/maxwell.html

References

Price, H. E. (1995). Spread Spectrum – It's not just for breakfast anymore! Retrieved from http://www.qsl.net/n9zia/ss.qexss.html

Tutorials Point. (2018). Learn Antenna Theory. Retrieved from https://www.tutorialspoint.com//antenna_theory/antenna_theory_collinear_array.htm

Woodford, C. (2018). Mobile broadband. Retrieved from https://www.explainthatstuff.com/mobilebroadband.html

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4