Wireless Network Security

Lecture 1

Basics of Wireless Communications

Srdjan Čapkun

BBC News | Sport | Weather | Capital | Culture | Auto

British Broadcasting Corporation

NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environ

29 June 2012 Last updated at 10:54 GMT

Researchers use spoofing to 'hack' into a flying drone

American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).

Drones are mostly used for military operations

A University of Texas at Austin team used 'spoofing' - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

The same method may have been used to bring down a US drone in Iran in 2011.

Analysts say that the demo shows the potential danger of using drones.

Drones are unmanned aircraft, often controlled from a hub located thousands of kilometres away.

Related Stories

Tests begin on 'unmanned' plane

Drones: What are they and how do they work?

http://www.bbc.com/news/technology-18643134

The Christian Science Monitor

WORLD | MIDDLE EAST

Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

By Scott Peterson, Staff writer / Payam Faramarzi*, Correspondent | DECEMBER 15, 2011

http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video

GPS signal generators

ETH Zürich

ANDY GREENBERG SECURITY 03.21.16 10:33 AM

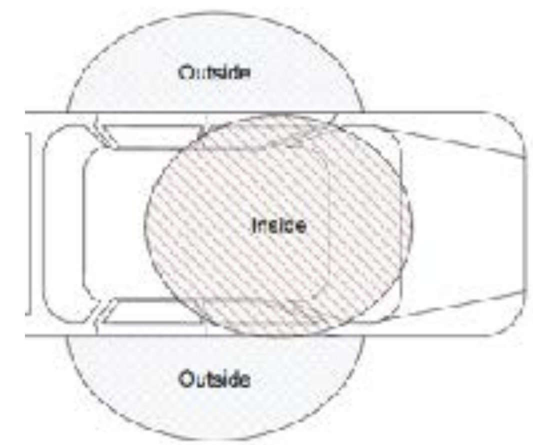
RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS

If:

- correct ke
- reply wit

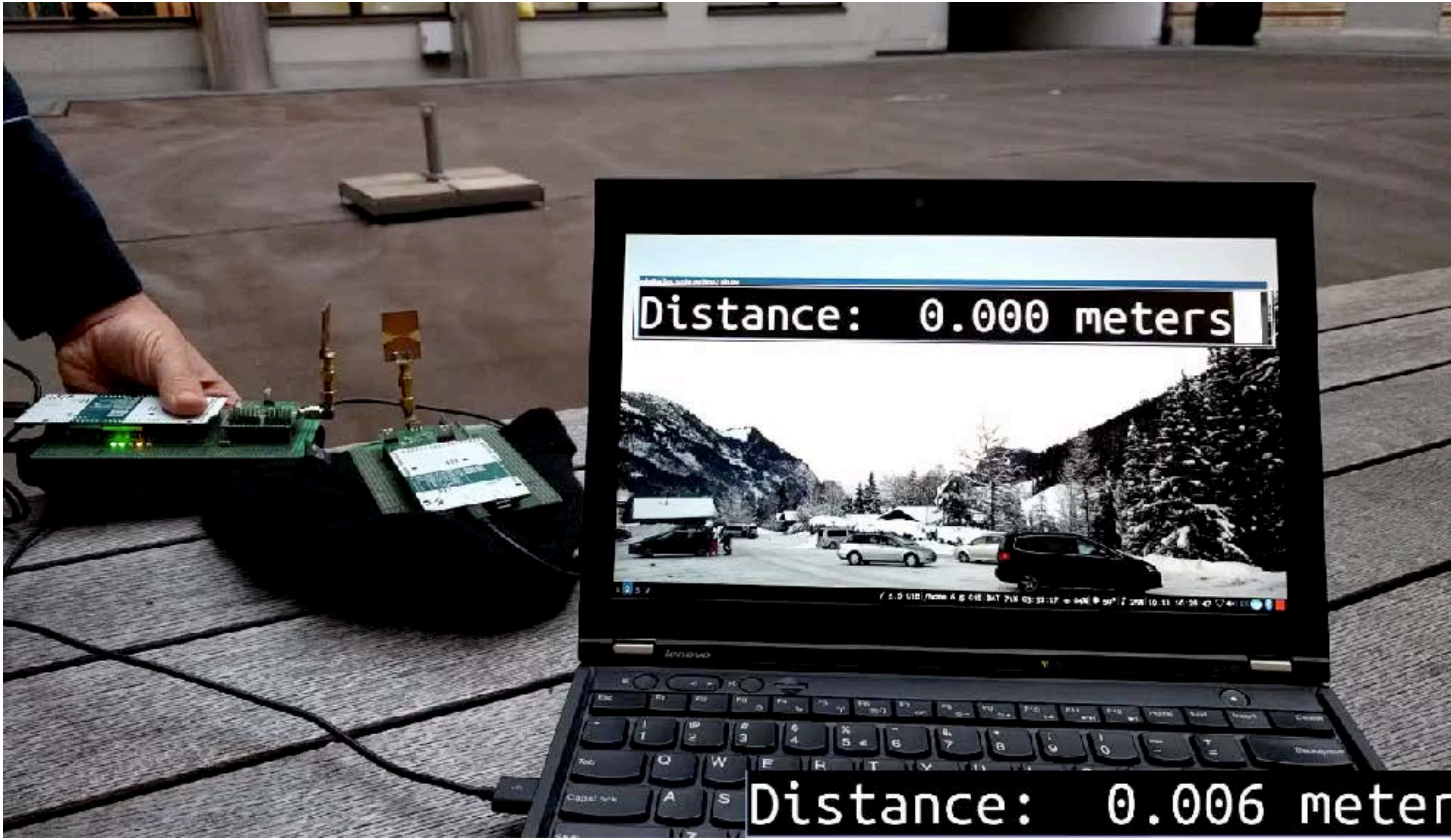
then:

- open doc



Tages-Anzeiger Auto Bild THE SUNDAY TIMES MIT Technology Review Les Echos The New York Times VOX

Secure Distance Measurement Radio



ETH zürich

ETH zürich

Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures

Daniel Moser, Patrick Leu, Aanjhan Ranganathan, Srdjan Capkun
ETH Zürich

Vincent Lenders
armasuisse

Fabio Ricciato
University Ljubljana

ETH zürich

USABLE 2FA BASED ON AMBIENT SOUND

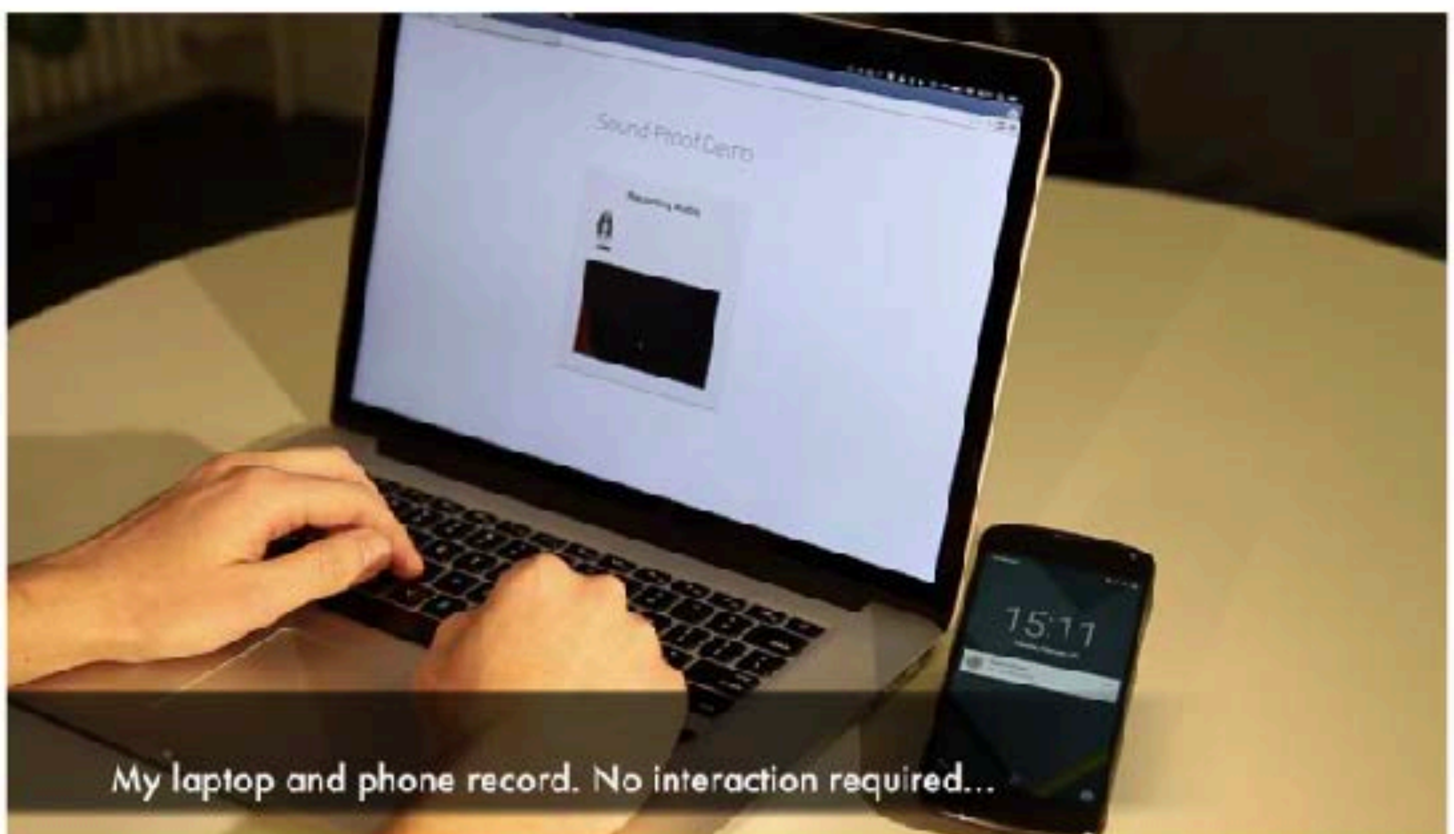
engadget

Two-factor system uses ambient sounds to verify your login

Mariella Moon, @mariella_moon
08.16.15

5 Comments

273 Shares



SW/HW hacking of Legacy and Embedded Systems

- Fridges, lightbulbs, insulin pumps, energy substations, PLCs, …

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

NEWS

IoT malware behind record DDoS attack is now available to all hackers

The Mirai trojan enslaved over 380,000 IoT devices, its creator claims

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS

FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson @selenalarson

January 9, 2017: 3:53 PM ET

Recommend 1.6K


SKY.GO
A man
&
the interferer.
Tesla Model S.

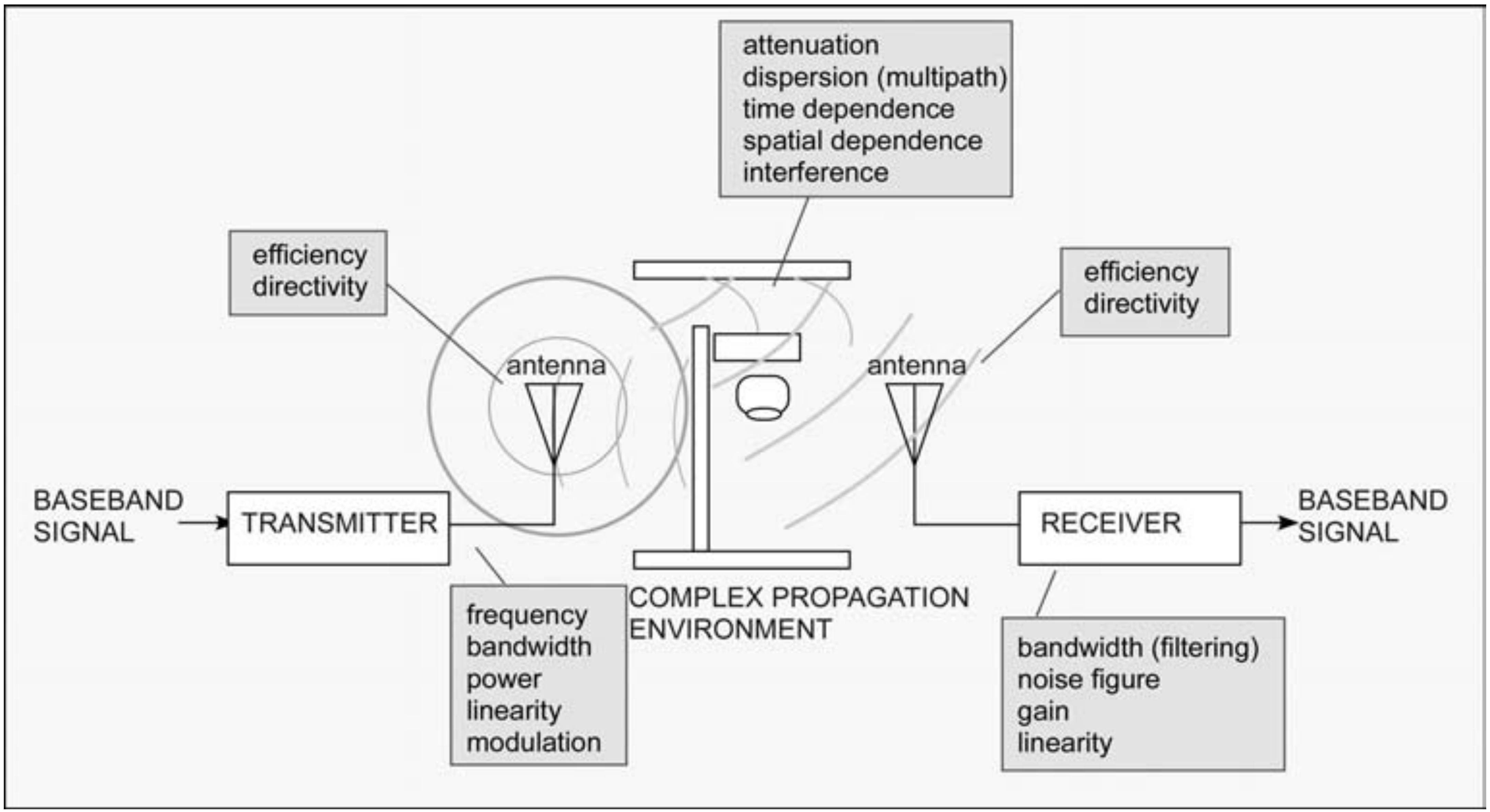
Recommended Readings

- RF Engineering for Wireless Networks, Daniel Dobkin (Ch. 2)
- Complex to Real complextoreal.com (Signal fundamentals & Modulation)
- Software Defined Radio for the Masses (Part 1)
- Electronic Warfare 101, David Adamy (Ch 3 and 4)

CyBOK Physical Layer and Telecommunications Security

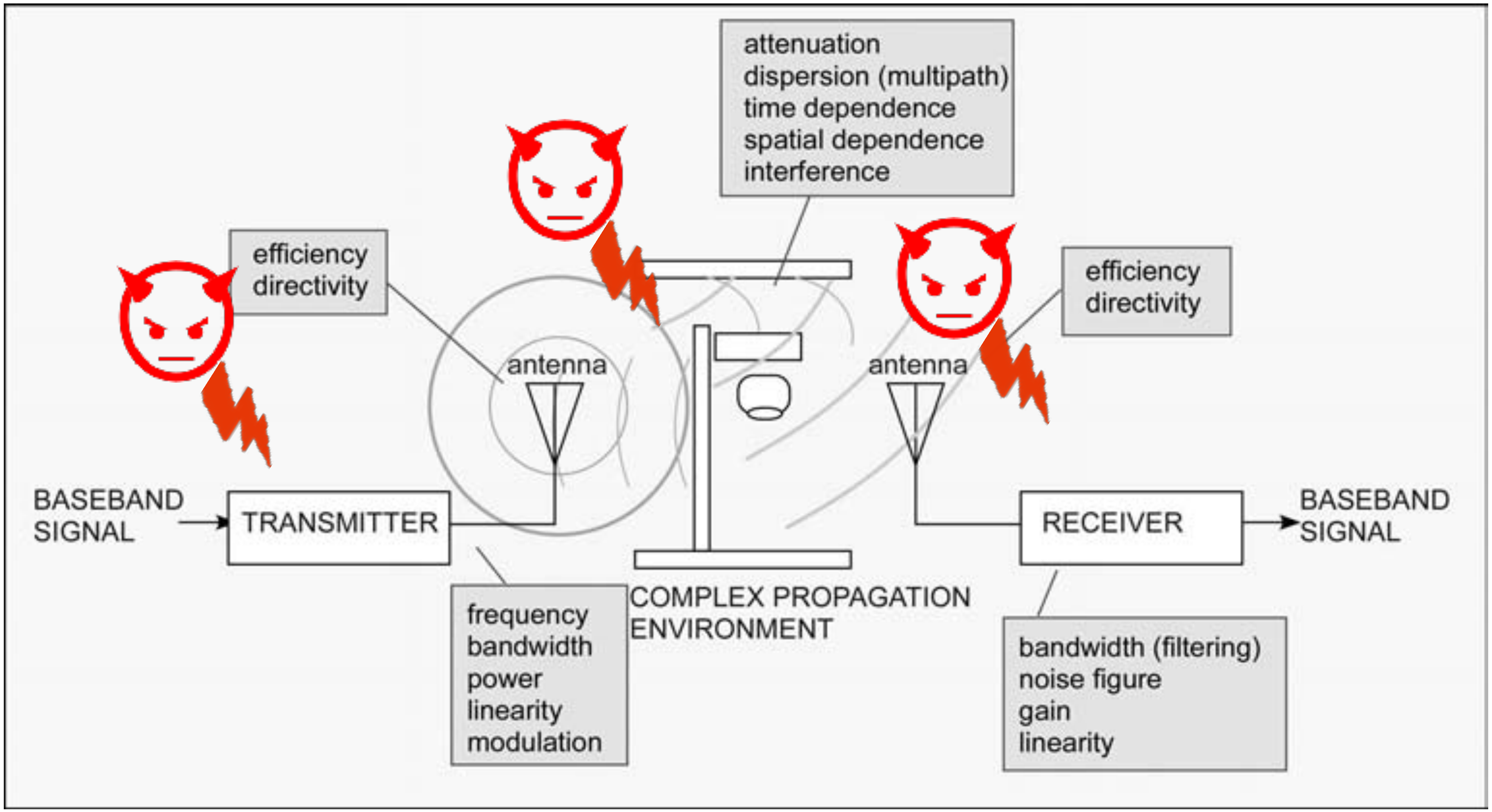
https://www.cybok.org/media/downloads/Physical_Layer_and_Telecommunications_Security_KA_-_Issue_1.0_September_2019.pdf

Building Blocks of a Wireless System



Source: Dobkin, RF Engineering for Wireless Networks

Attacker can control …



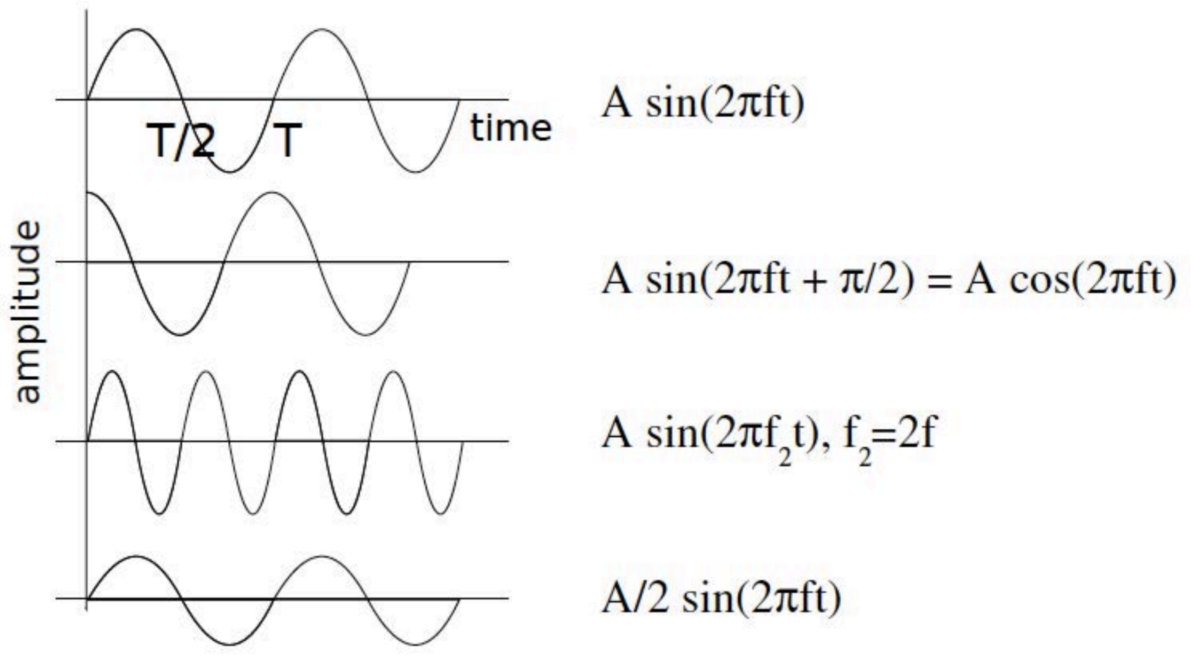
Radio Frequency Signal

Radio Communication (RF)

- Communication using EM radiation with waves at frequencies 3kHz-300GHz
- Waves are created by an alternating current at a desired communication frequency

$s(t) = A \sin(2\pi ft + \Theta)$

- A = amplitude, f = frequency (Hz), t = time, Θ = phase
- T = period = 1/f
- λ = wavelength = c/f (the distance that the signal travels during



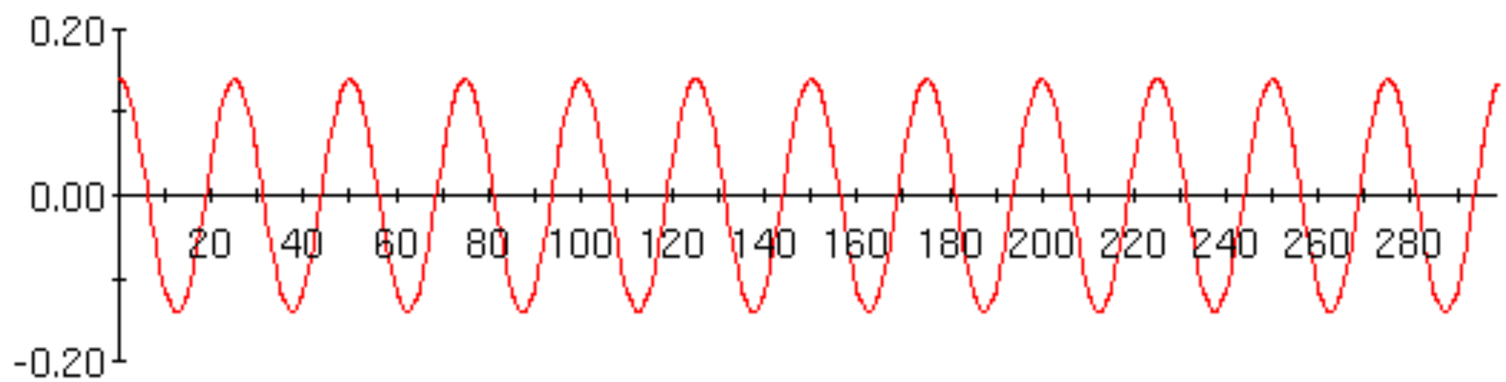
Wireless Communication Basics

Baseband: Signal containing only the information that we want to communicate

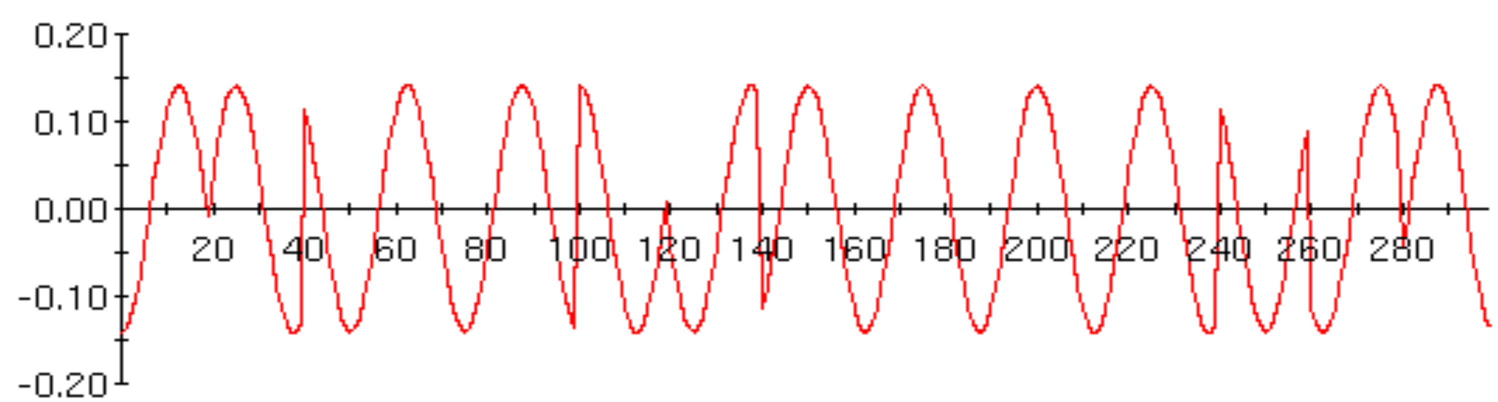
Carrier: Typically, a pure sinusoid of a particular frequency and phase that *carries* the information

Modulated Signal: A carrier that has been loaded or *modulated* with the information signal.

Carrier

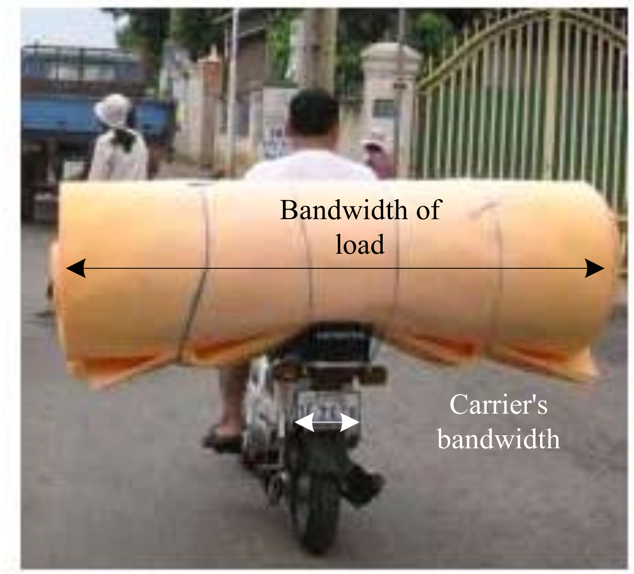


Modulated

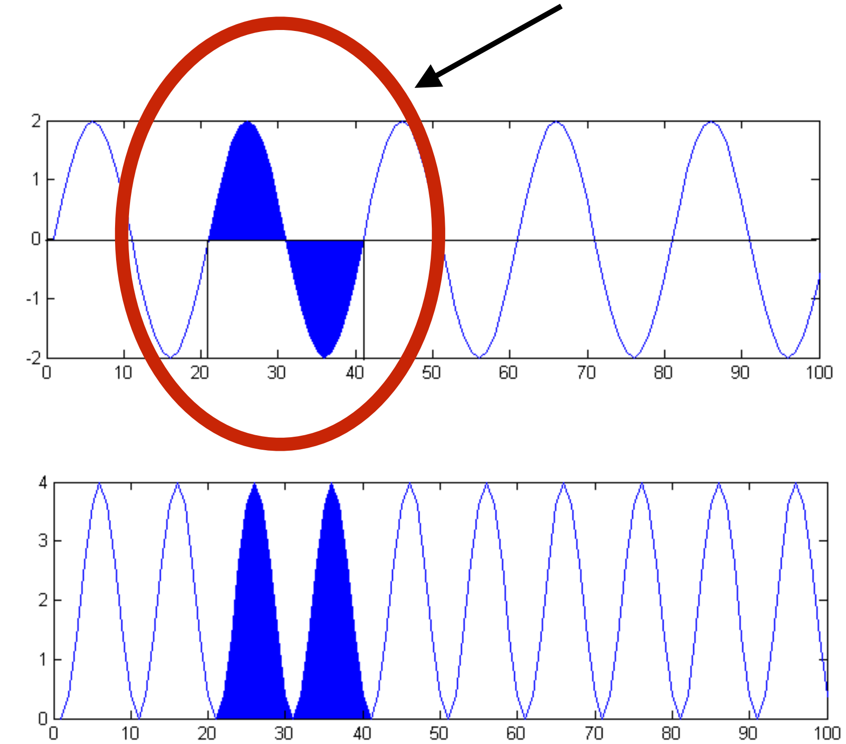


Wireless Communication Basics

Bandwidth: measure of frequency content of the signal. E.g., human voice (baseband) contains frequencies from 30 Hz to 10 kHz.



signal has zero area for N periods



Signal Energy

$$E_x = \sum_{n=0}^{N-1} |x_n|^2$$

Signal Power

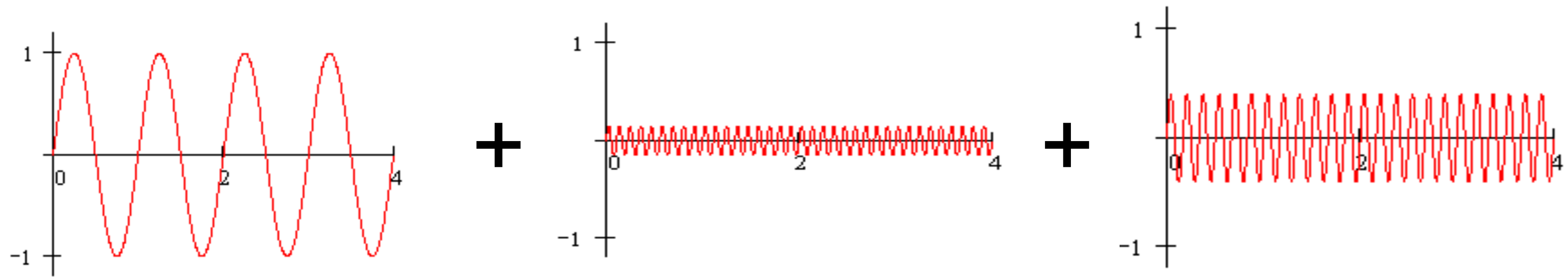
$$P_x = \frac{E_x}{N} = \frac{1}{N}\sum_{n=0}^{N-1} |x_n|^2$$

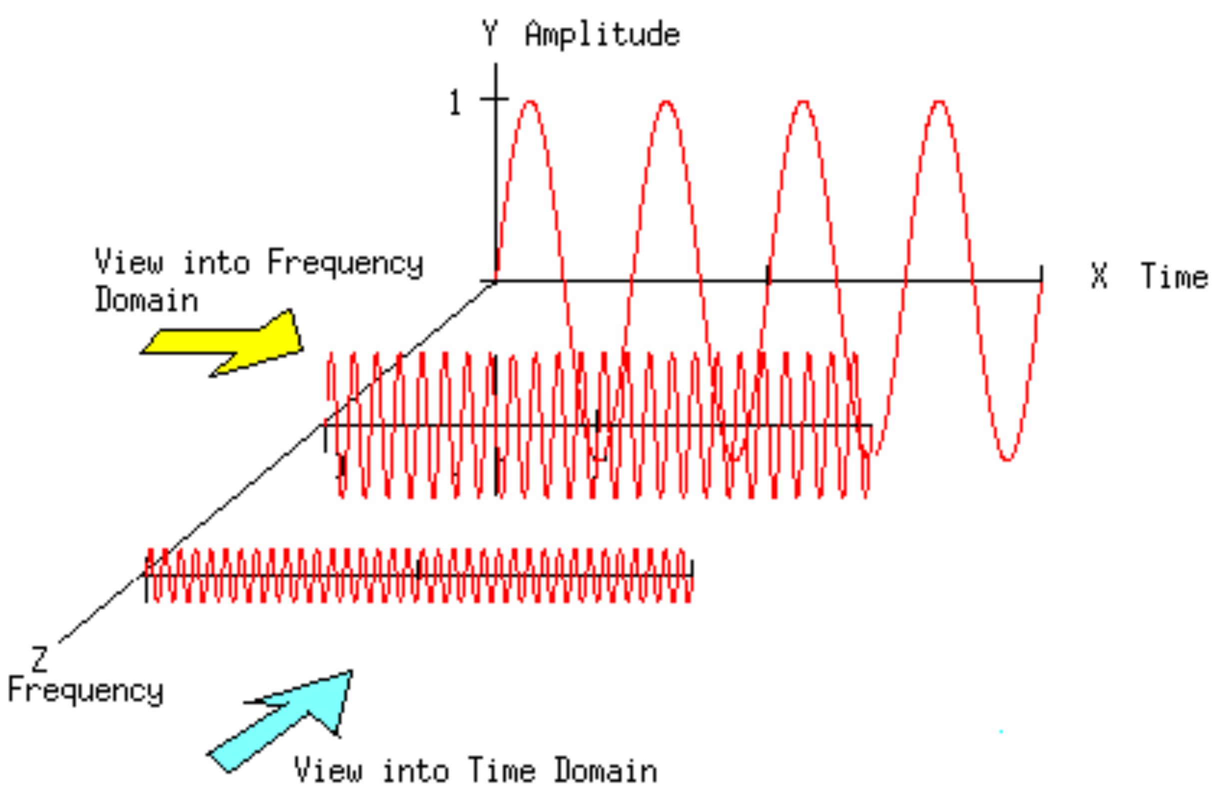
Energy per bit

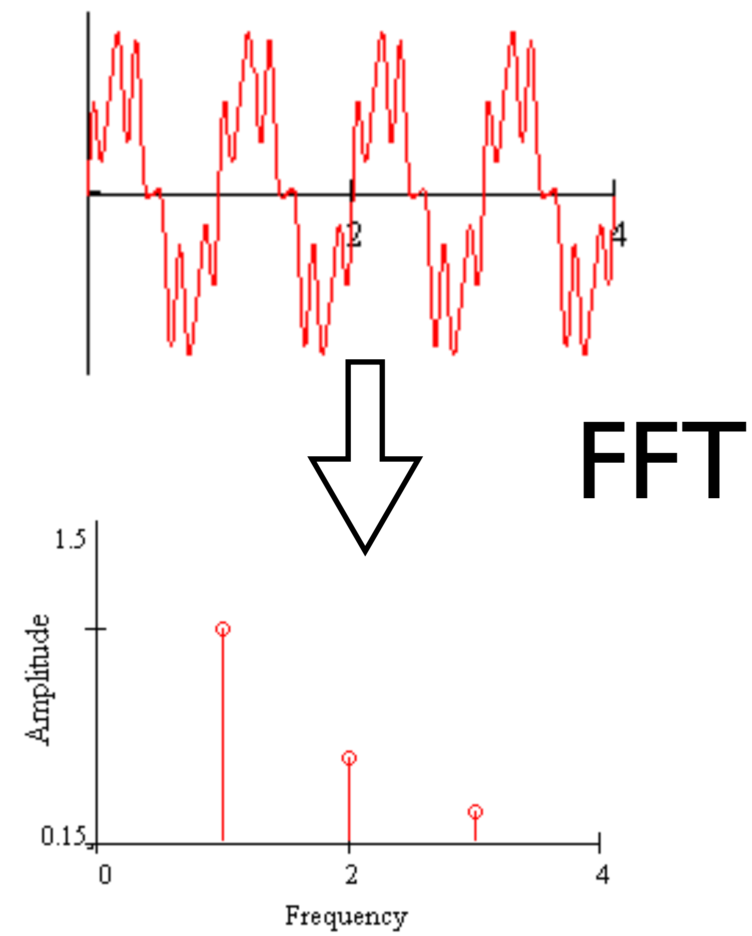
$$E_b = \frac{Avg\left[x^2(t)\right]}{R_b}$$

bit rate

Time and Frequency Transforms







Time and Frequency Transforms

Euler formula:

$$e^{j\omega t} = \cos(\omega t) + j\sin(\omega t)$$

$$e^{-j\omega t} = \cos(-\omega t) + j\sin(-\omega t) = \cos(\omega t) - j\sin(\omega t)$$

$$\cos(\omega t) = \frac{e^{j\omega t} + e^{-j\omega t}}{2}$$

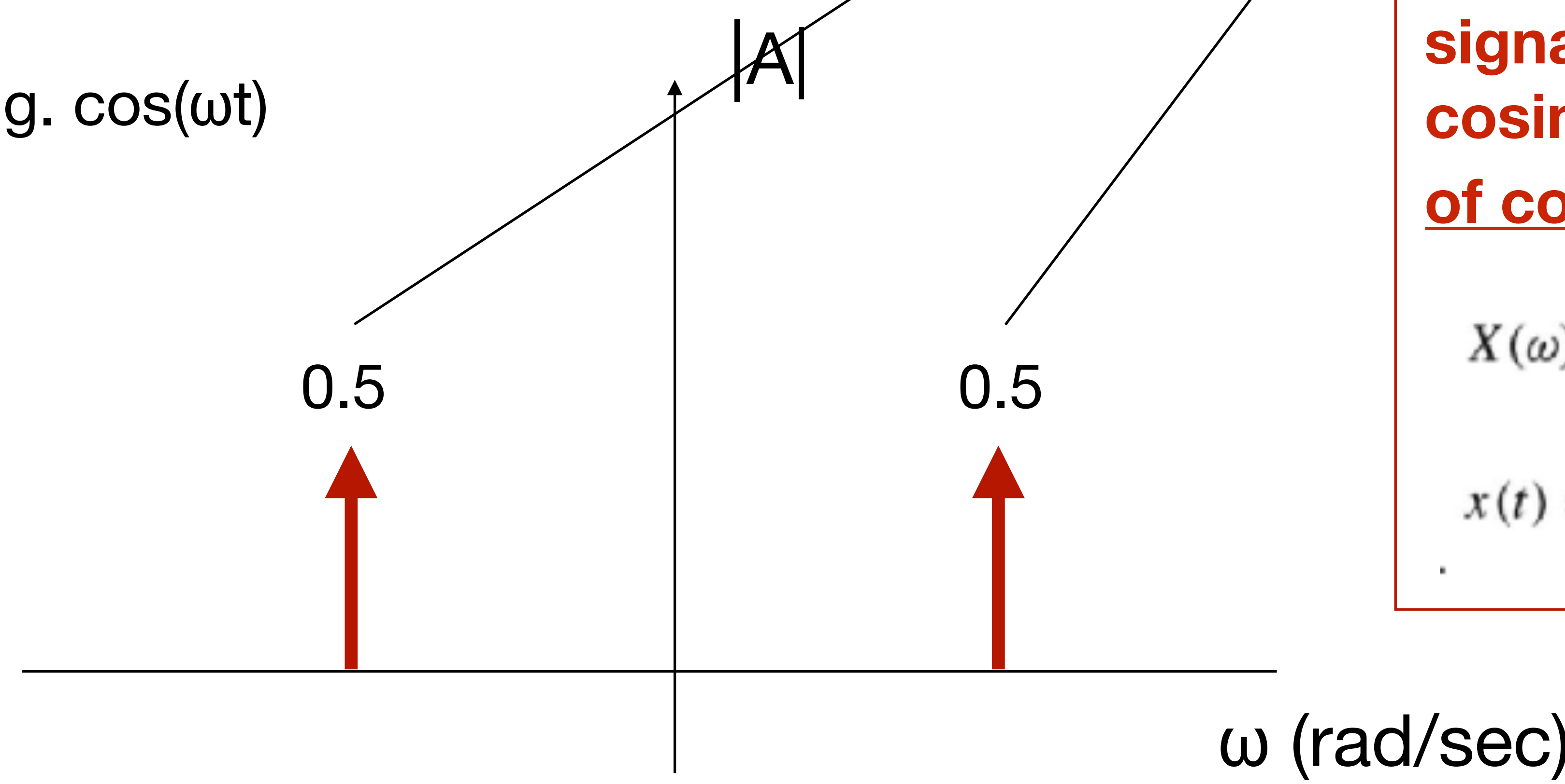
$$\sin(\omega t) = \frac{e^{j\omega t} - e^{-j\omega t}}{2j}$$

$$\sin\left(\frac{\pi}{2} - \theta\right) = \cos\theta$$

$$\cos\left(\frac{\pi}{2} - \theta\right) = \sin\theta$$

Frequency Spectrum is the plot of the amplitude projected onto the complex exponential $e^{\omega t}$

e.g. cos(ωt)



Fourier Transform transforms a signal that has a physical sine and cosine representation <u>into a space of complex exponentials $e^{\omega t}$</u>

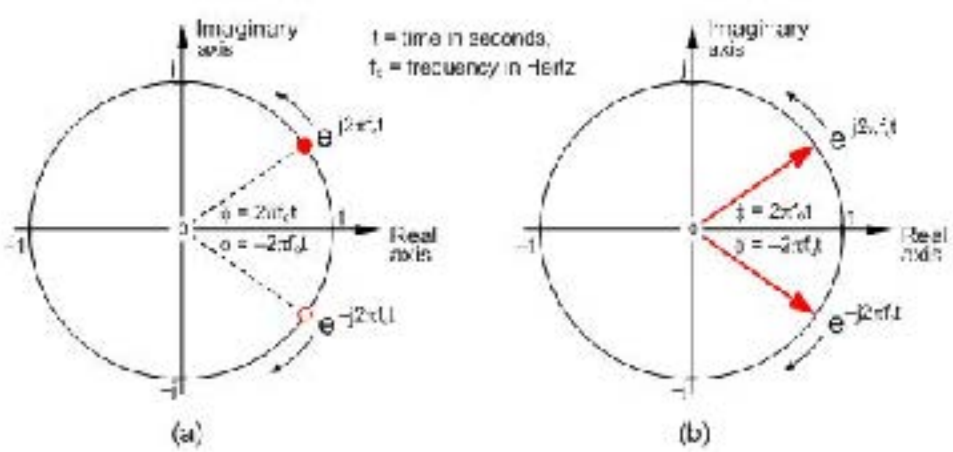
$$X(\omega) = \mathcal{F}[x(t)] = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}dt$$

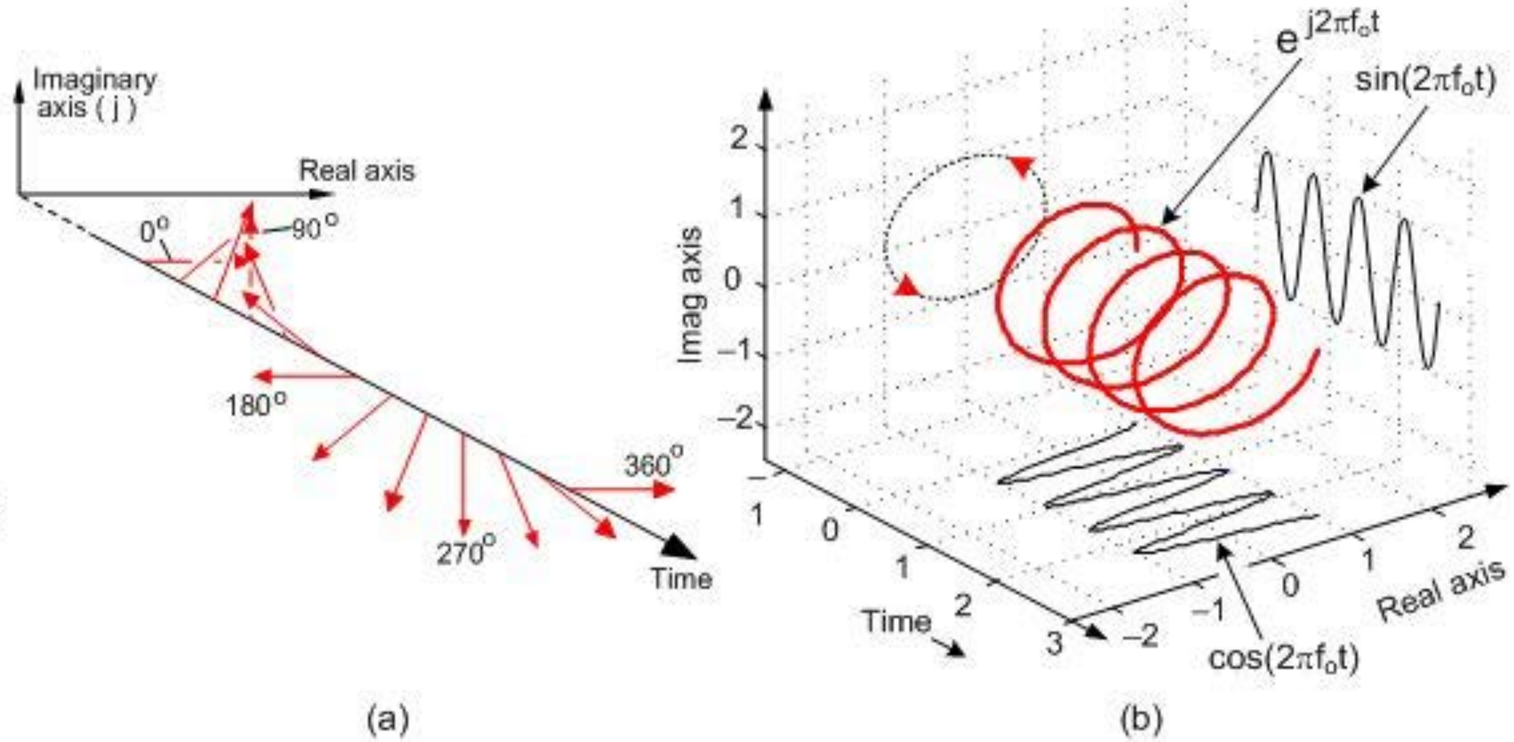
$$x(t) = \mathcal{F}^{-1}[X(\omega)] = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(\omega)e^{j\omega t}d\omega$$

$$\omega = 2\pi f$$

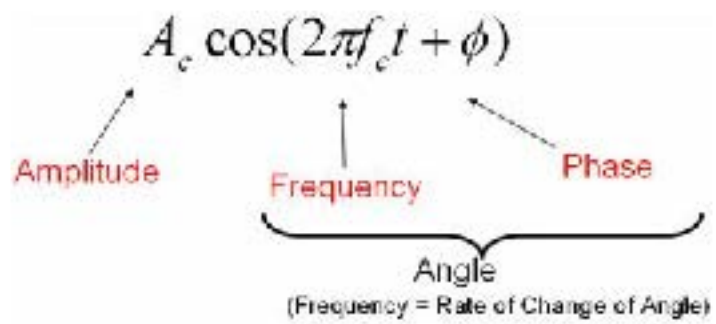
Time and Frequency Transforms

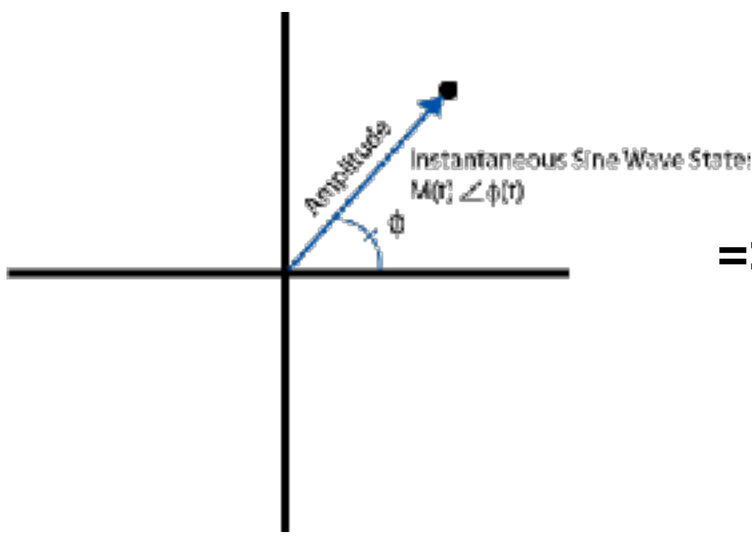
How to visualize complex exponentials?



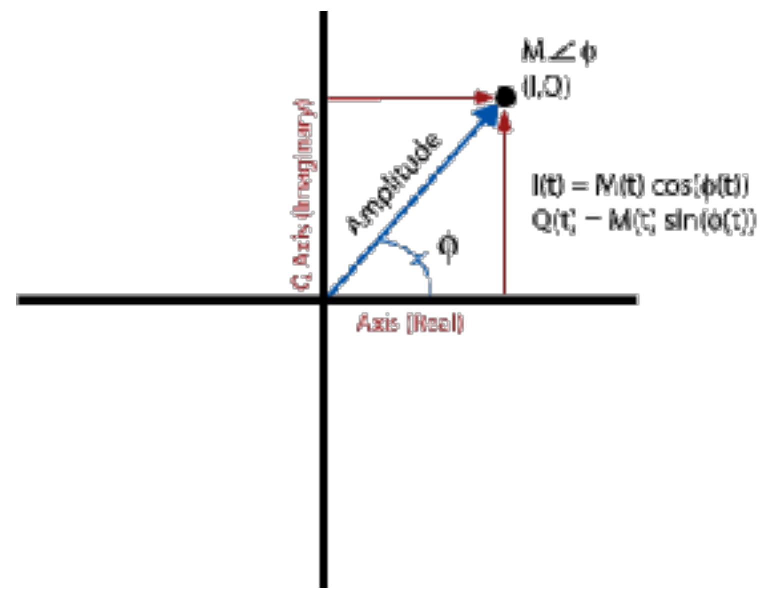


I-Q Signal Representation



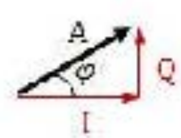


=> (IQ)



$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$$

$$A\cos(2\pi f_c t + \varphi) = A\cos(2\pi f_c t)\cos(\varphi) - A\sin(2\pi f_c t)\sin(\varphi)$$



$$I = A\cos(\varphi)$$
$$Q = A\sin(\varphi)$$

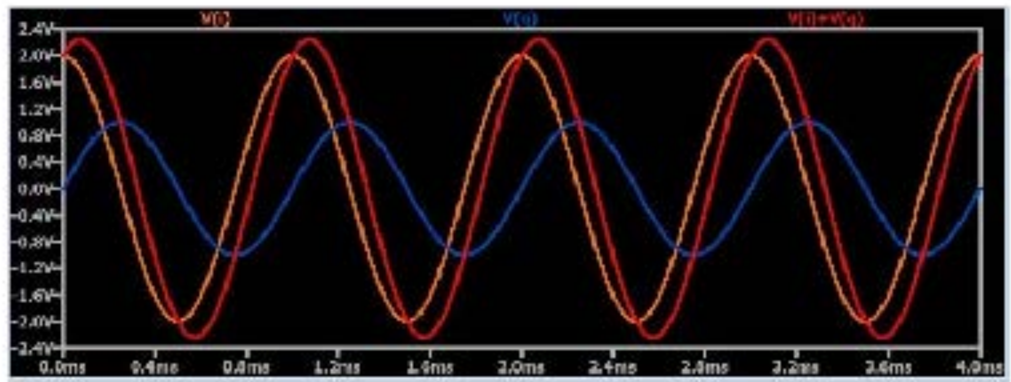
$$A\cos(2\pi f_c t + \varphi) = I\cos(2\pi f_c t) - Q\sin(2\pi f_c t)$$

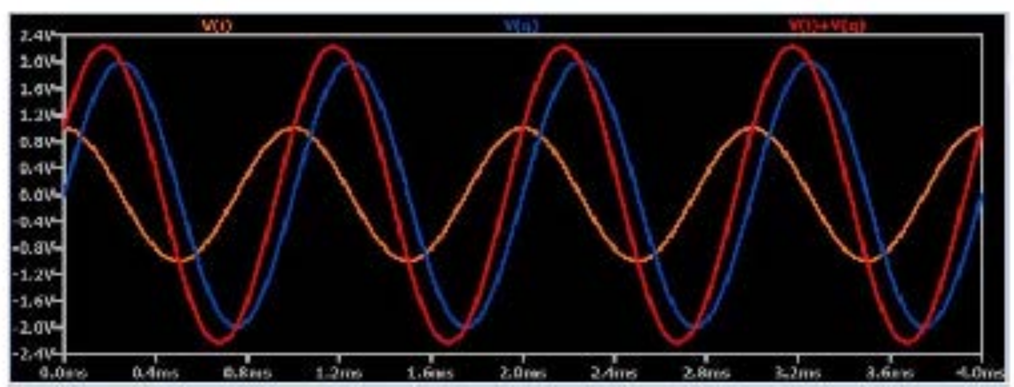
where I is the amplitude of the in-phase carrier
Q is the amplitude of the quadrature-phase carrier

http://www.ni.com/tutorial/4805/en/

I-Q Signal Representation

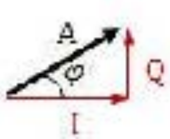
Precisely varying the phase of a high-frequency carrier sine wave in a hardware circuit according to an input message signal is difficult.





$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$$

$$A\cos(2\pi f_c t + \varphi) = A\cos(2\pi f_c t)\cos(\varphi) - A\sin(2\pi f_c t)\sin(\varphi)$$



$$I = A\cos(\varphi)$$
$$Q = A\sin(\varphi)$$

$$A\cos(2\pi f_c t + \varphi) = I\cos(2\pi f_c t) - Q\sin(2\pi f_c t)$$

where I is the amplitude of the in-phase carrier
Q is the amplitude of the quadrature-phase carrier

$$a\sin x + b\cos x = c\sin(x+\varphi)$$

where the original amplitudes a and b sum in quadrature to yield the combined amplitude c,

$$c = \sqrt{a^2 + b^2},$$

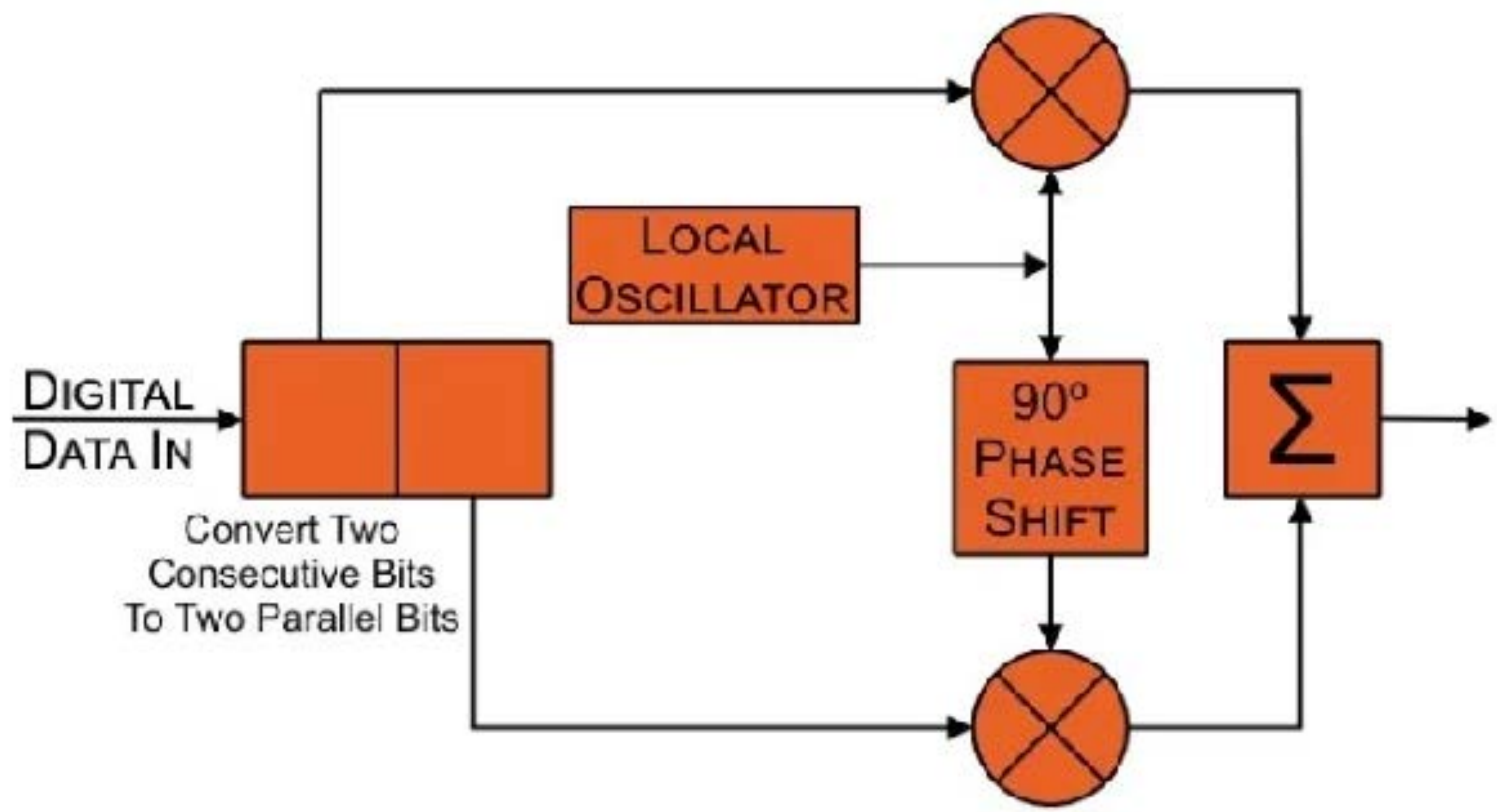
and, using the atan2 function, the initial value of the phase angle $x + \varphi$ is obtained by

$$\varphi = \operatorname{atan2}(b, a).$$

https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/

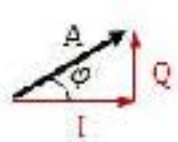
I-Q Signal Representation

Precisely varying the phase of a high-frequency carrier sine wave in a hardware circuit according to an input message signal is difficult.



$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$$

$$A\cos(2\pi f_c t + \varphi) = A\cos(2\pi f_c t)\cos(\varphi) - A\sin(2\pi f_c t)\sin(\varphi)$$



$$I = A\cos(\varphi)$$
$$Q = A\sin(\varphi)$$

$$A\cos(2\pi f_c t + \varphi) = I\cos(2\pi f_c t) - Q\sin(2\pi f_c t)$$

where I is the amplitude of the in-phase carrier
Q is the amplitude of the quadrature-phase carrier

$$a\sin x + b\cos x = c\sin(x+\varphi)$$

where the original amplitudes a and b sum in quadrature to yield the combined amplitude c,

$$c = \sqrt{a^2 + b^2},$$

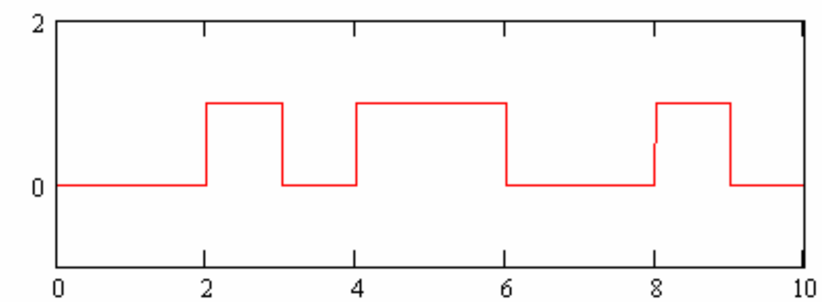
and, using the atan2 function, the initial value of the phase angle $x+\varphi$ is obtained by

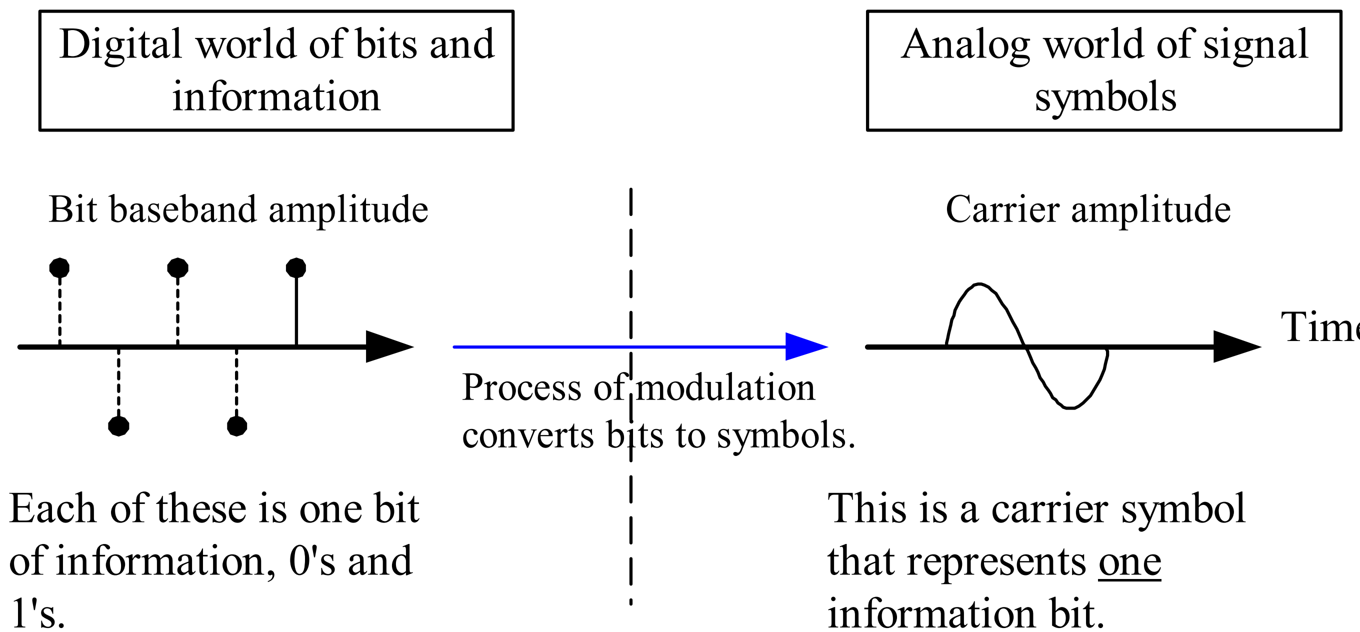
$$\varphi = \operatorname{atan2}(b, a).$$

https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/

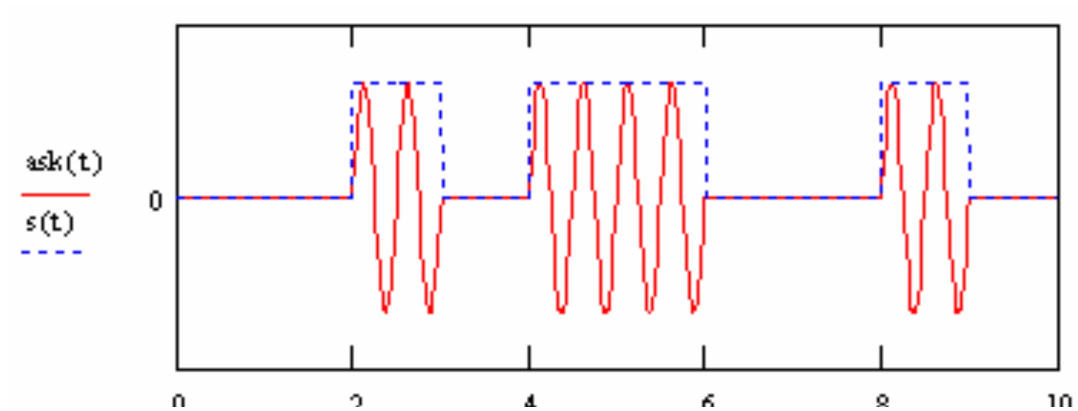
Modulation Techniques

Baseband

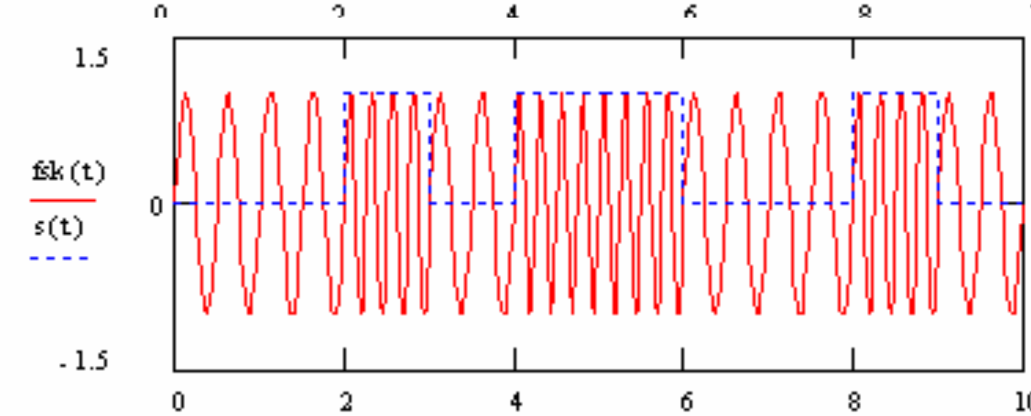




$$ASK(t) = s(t)\sin(2\pi f t)$$

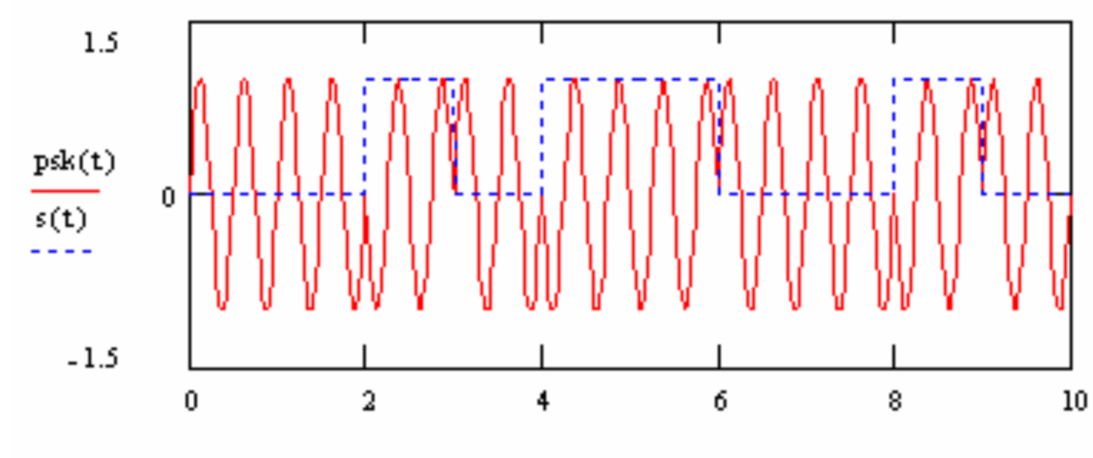


$$FSK(t) = \begin{cases} \sin(2\pi f_1 t) & \textit{for bit } 1 \\ \sin(2\pi f_2 t) & \textit{for bit } 0 \end{cases}$$



Modulation Techniques

$$PSK(t) = \begin{cases} \sin(2\pi f t) & for\ bit\ 1 \\ \sin(2\pi f t + \pi) & for\ bit\ 0 \end{cases}$$



IQ representation of M-ary PSK

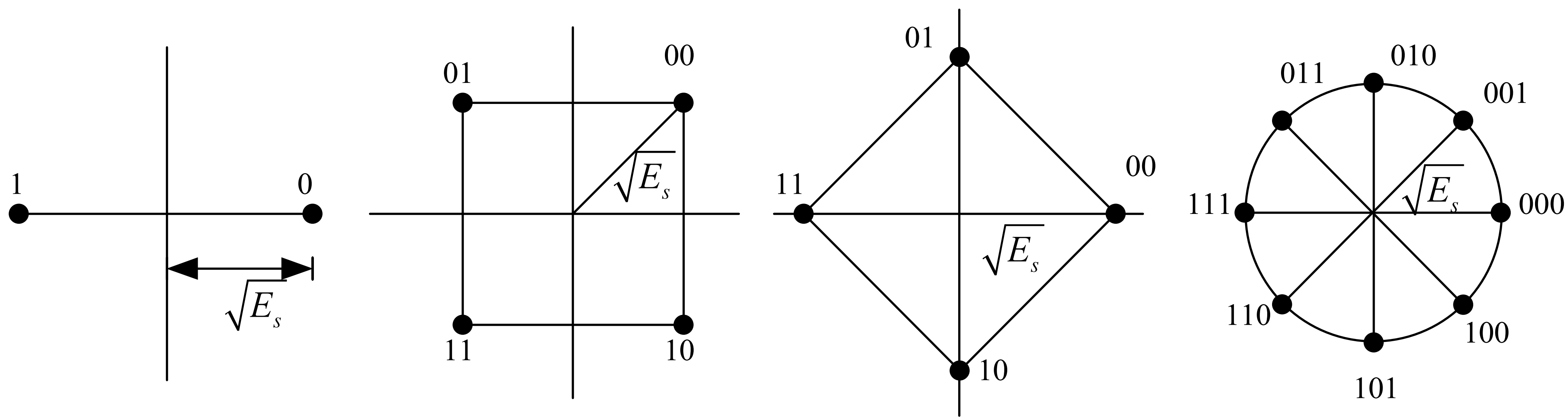
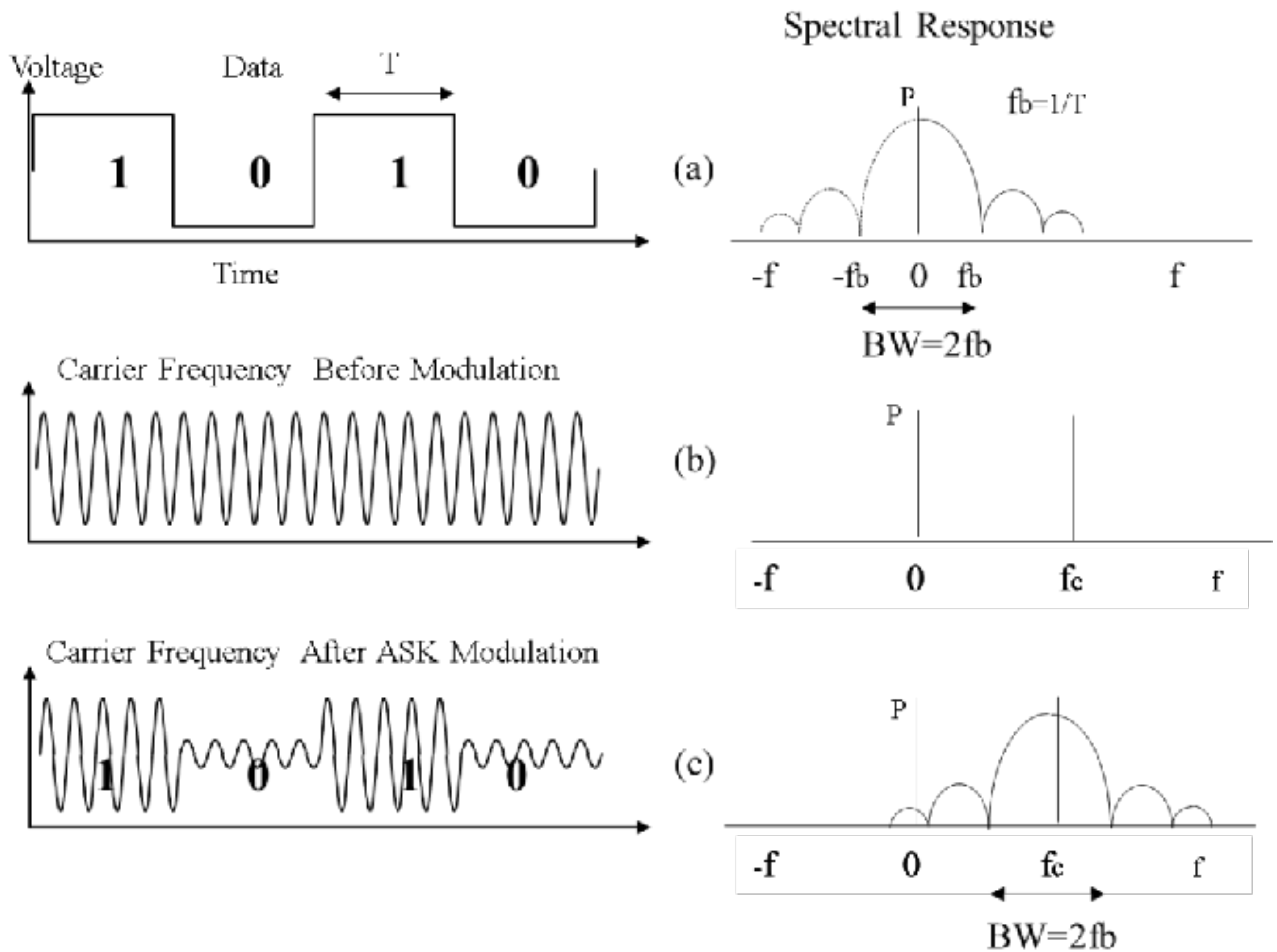


Figure 12 – M-PSK modulations, a. BPSK, b. QPSK, c. also QPSK, d. 8PSK

Integrity, fingerprinting, LPI communication …

Frequency and Bandwidth of a Signal

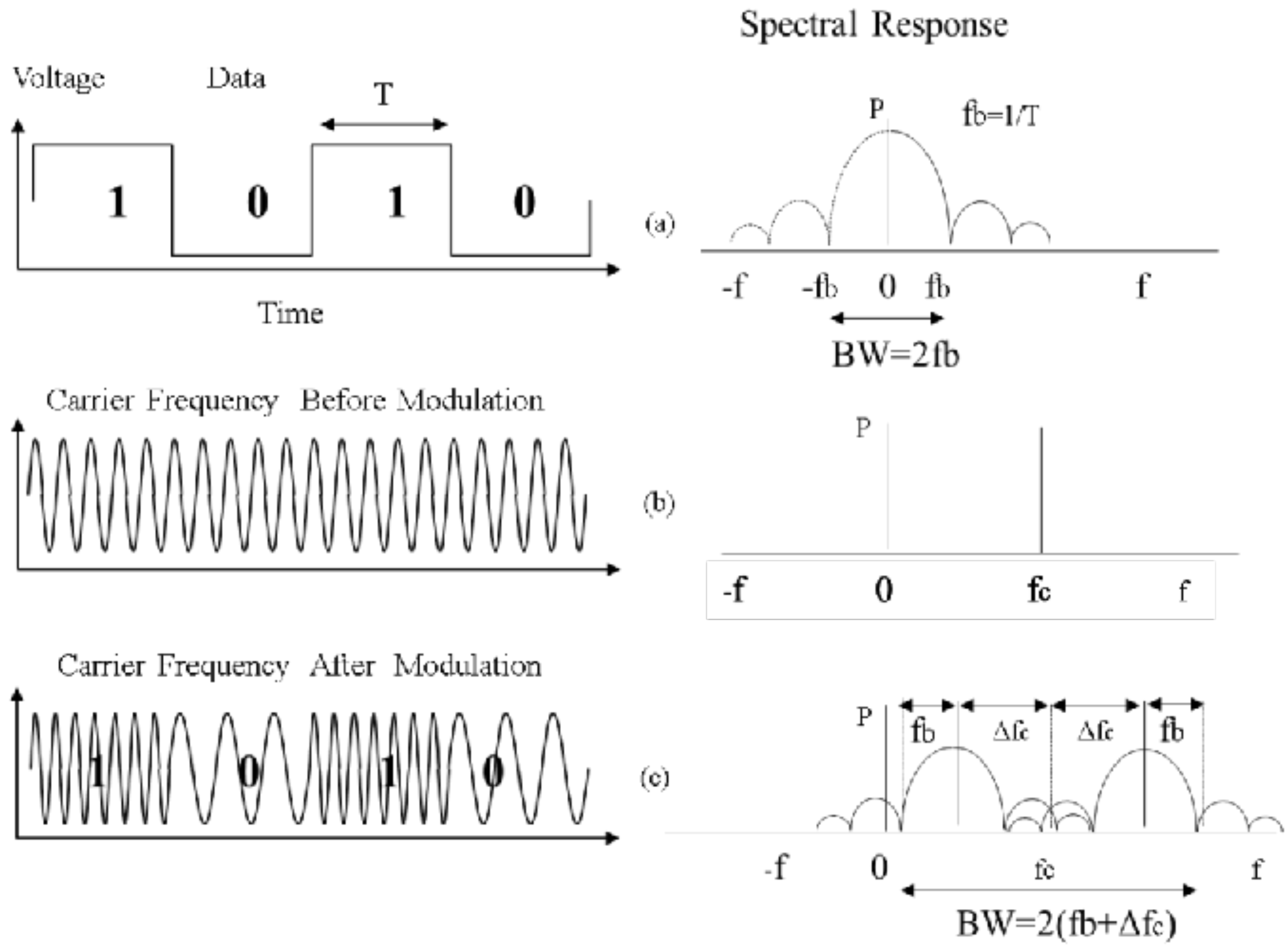
ASK



Note: Different modulation techniques will require different bandwidths for the same data rate.

Frequency and Bandwidth of a Signal

FSK

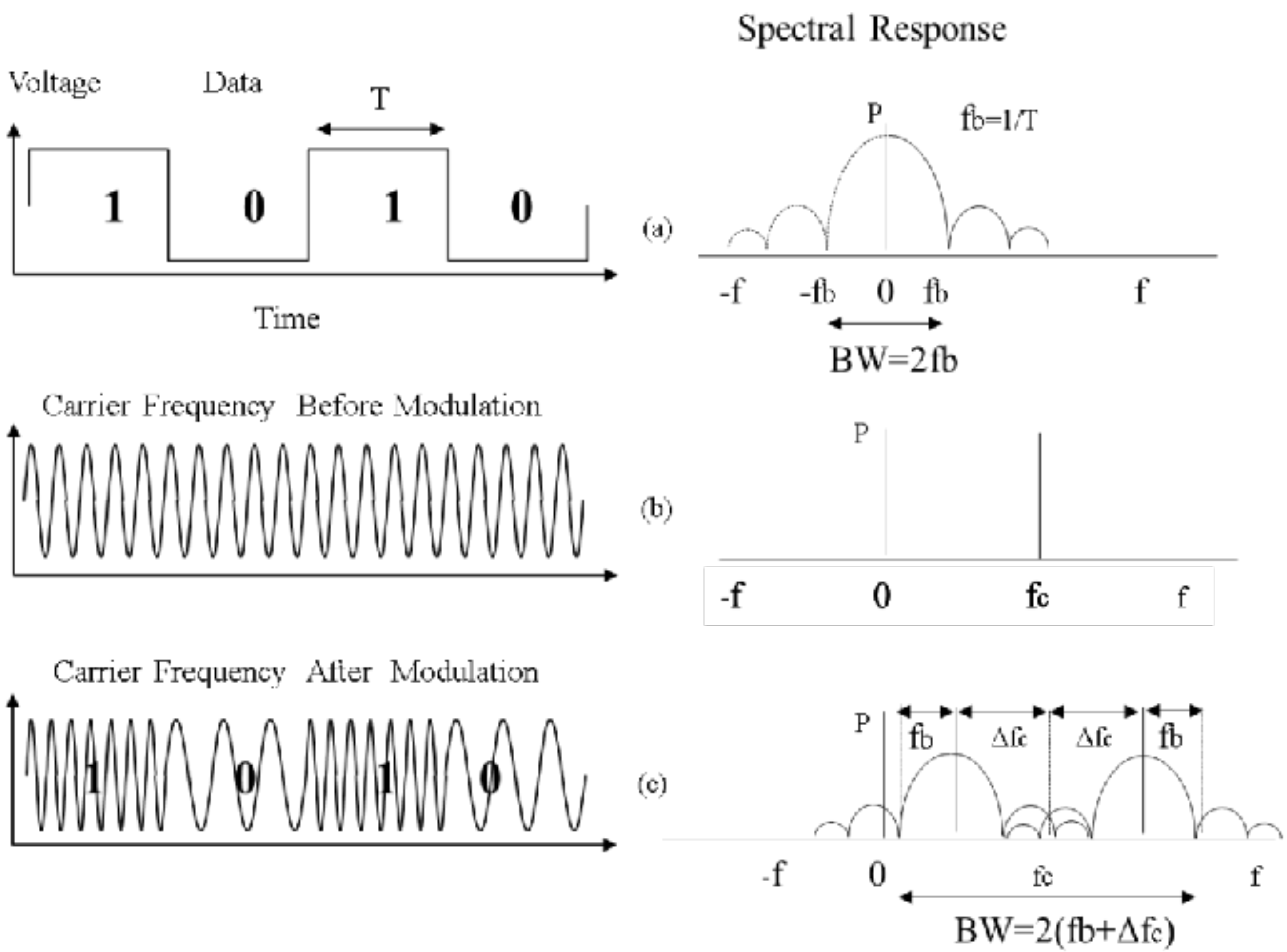


Negative frequencies, complex representation :D

http://whiteboard.ping.se/SDR/IQ

Frequency and Bandwidth of a Signal

FSK



Negative frequencies, complex representation :D

http://whiteboard.ping.se/SDR/IQ

Complexity Only Increases E.g. OFDM

Orthogonal Frequency-Division Multiplexing

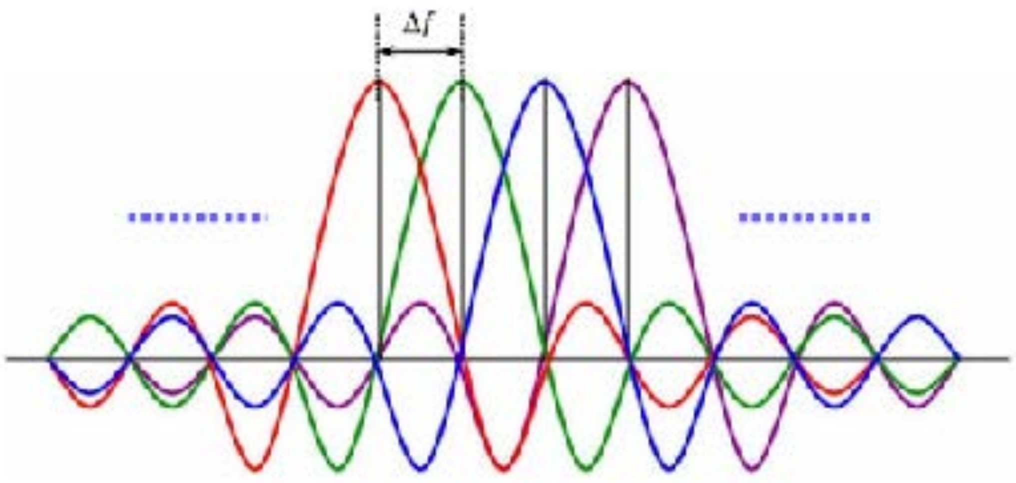
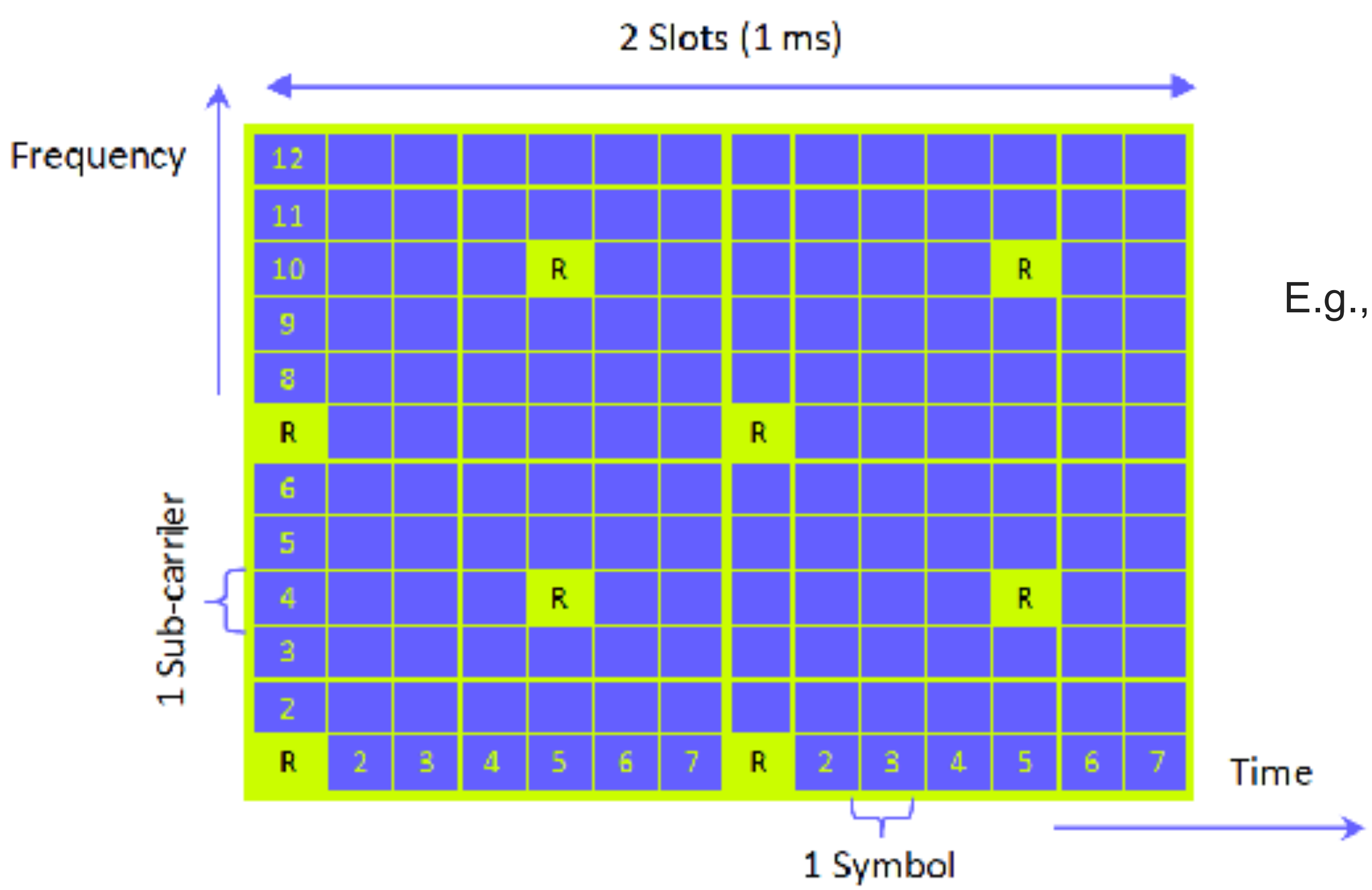


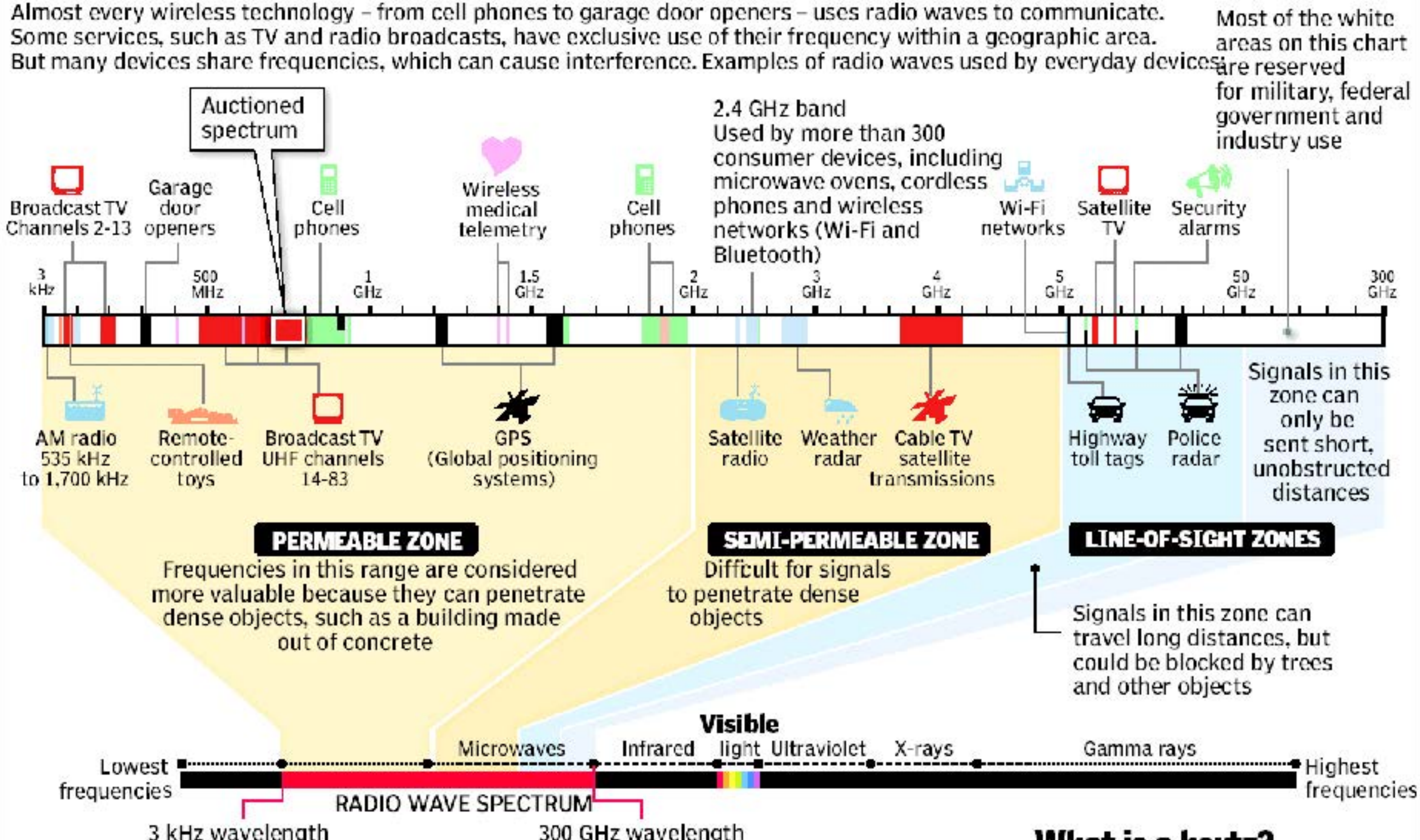
FIGURE 1 OFDM SUBCARRIER SPACING.



E.g., LTE…

Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:



The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz

What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

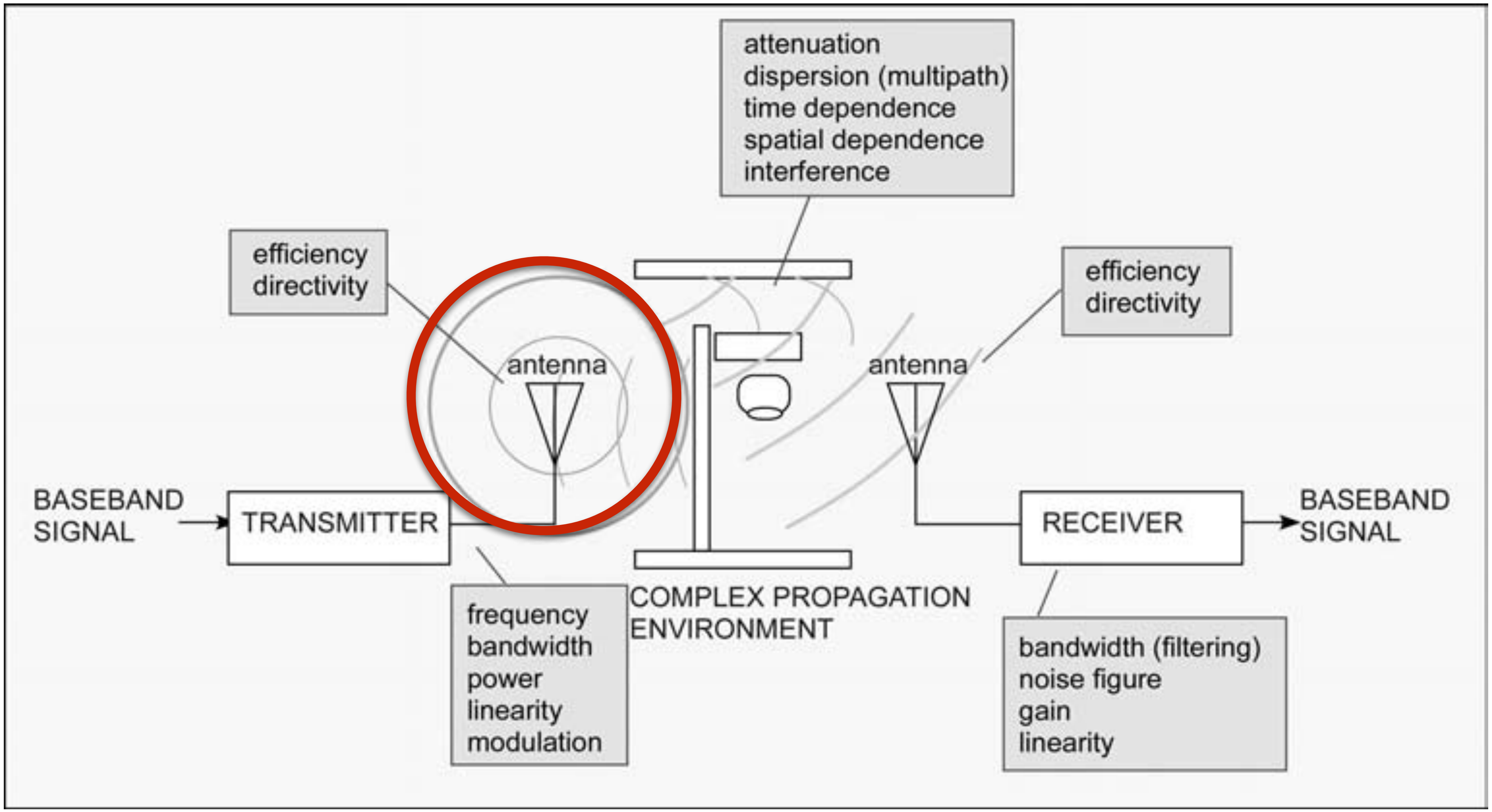
1 kilohertz (kHz) = 1,000 hertz

1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

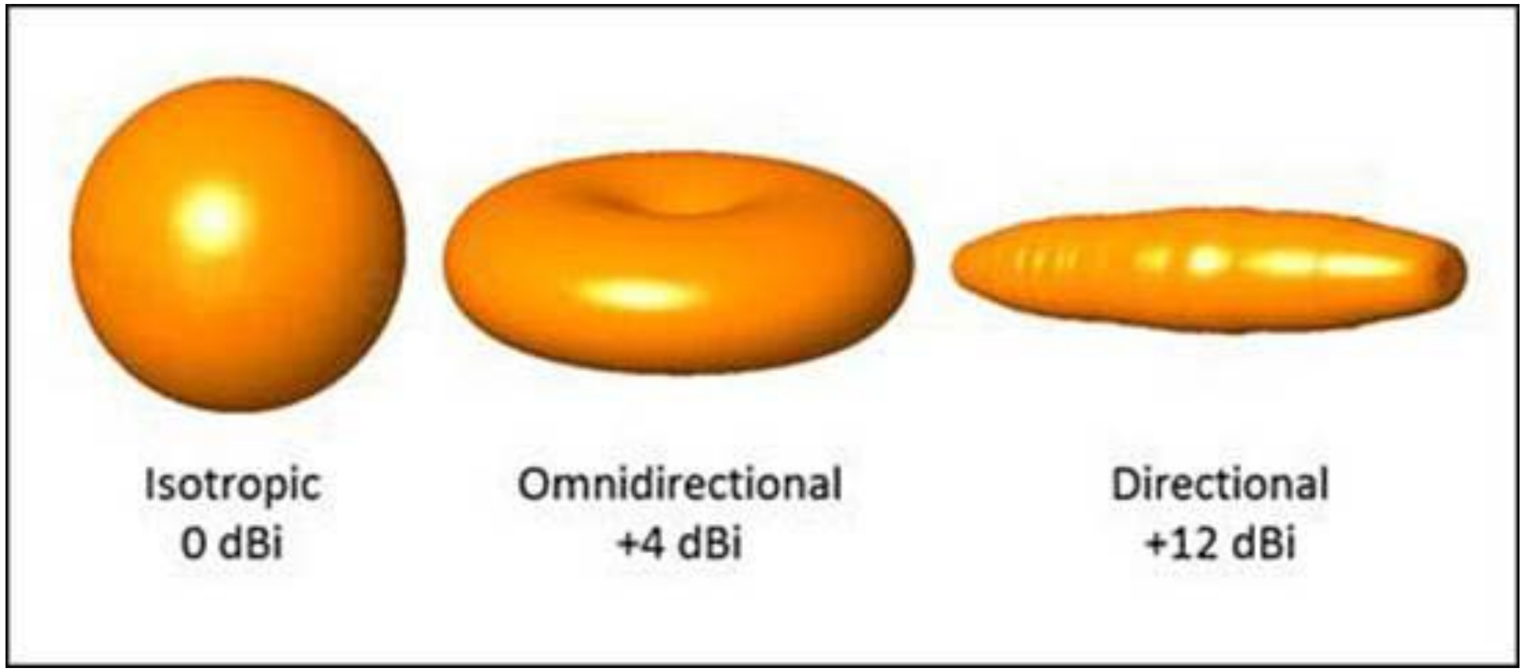
Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

Building Blocks of a Wireless System

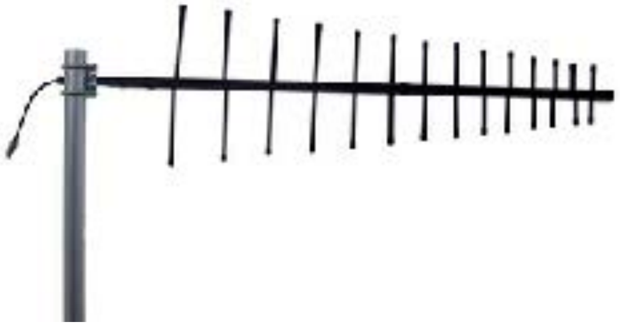


Source: Dobkin, RF Engineering for Wireless Networks

Antennas and Propagation



omni/dipole



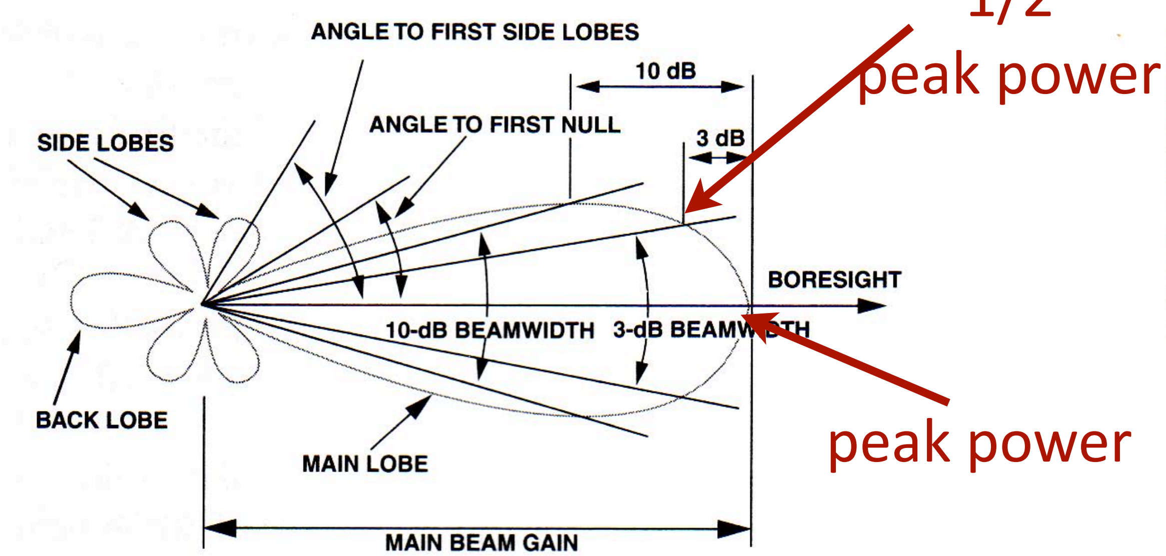
yagi

horn

cantenna

Antennas and Propagation

- Gain vs Beamwidth



Antenna parameter definitions are based on the geometry of the antenna gain pattern.

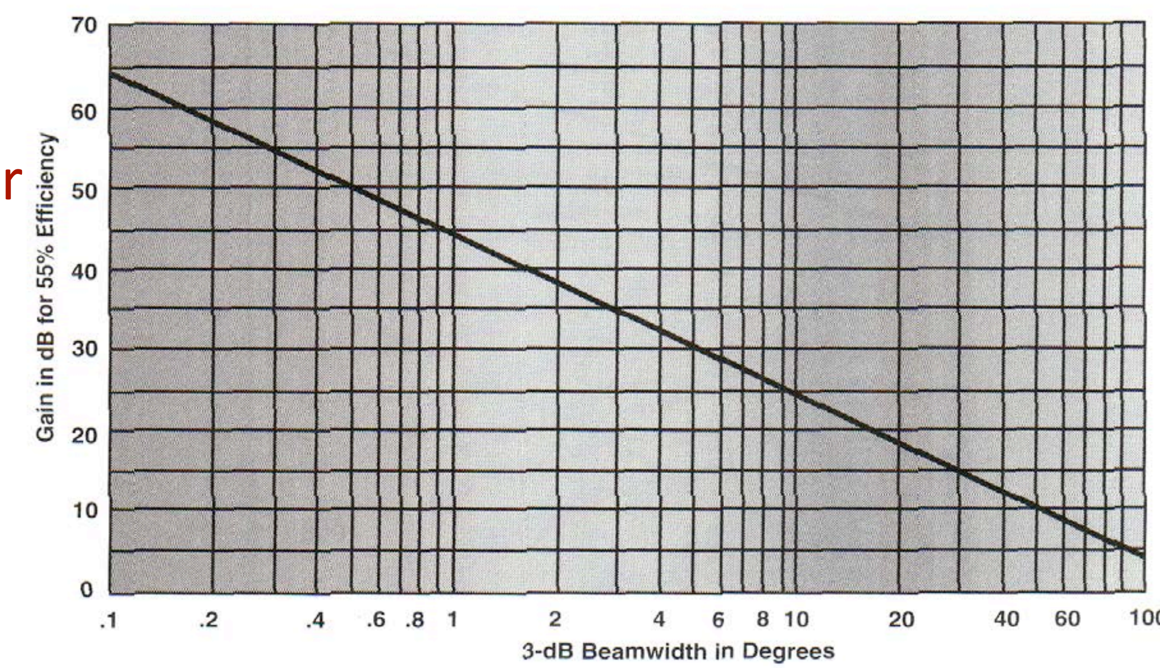
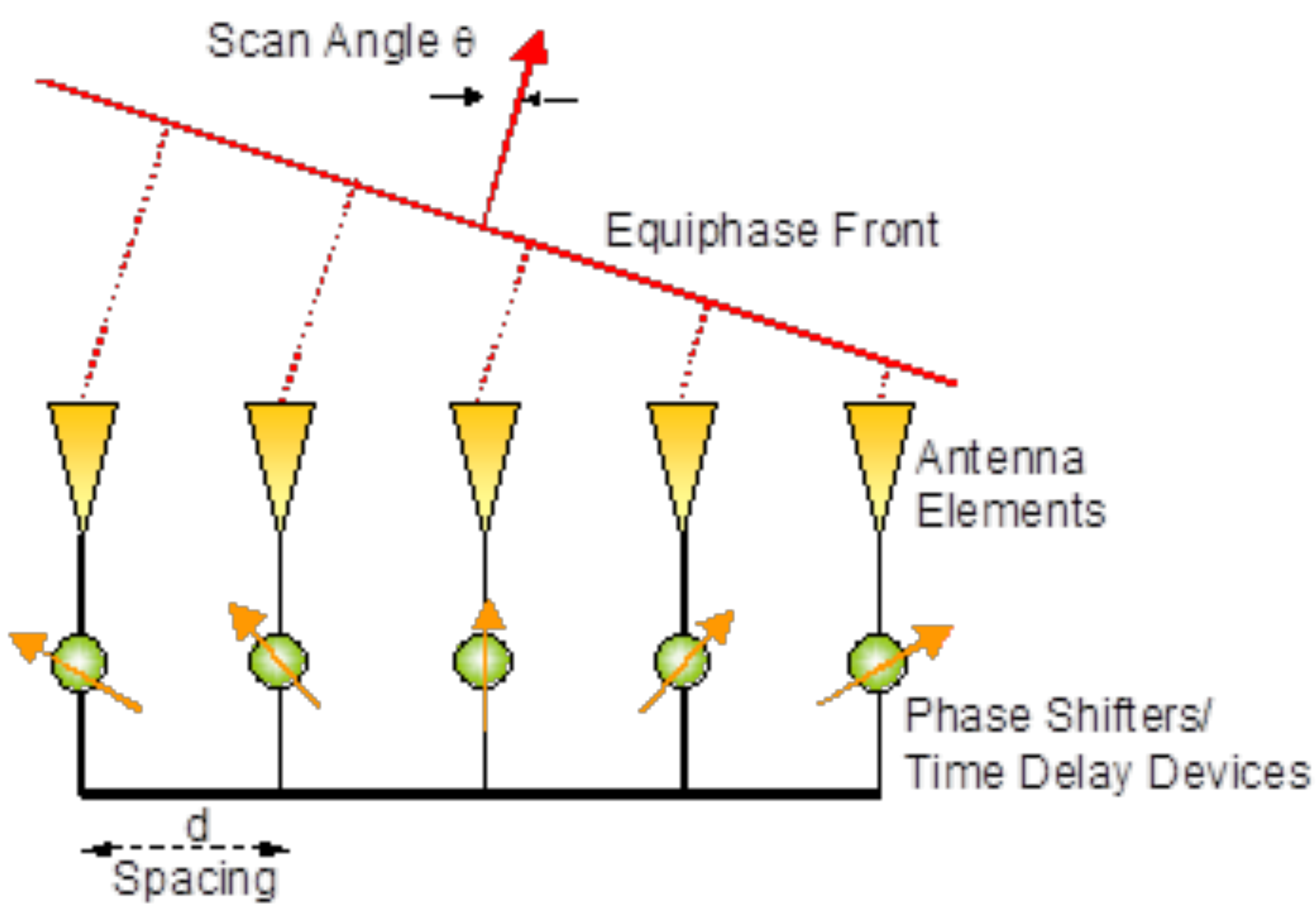


Figure 3.4 There is a well-defined tradeoff of gain versus beamwidth for any type of antenna. This chart shows the gain versus beamwidth for a parabolic antenna with 55% efficiency.

Phased Arrays (Beam steering antennas)

- phase of the signal to each antenna is adjusted such that all the signals will be in phase when viewed from a certain direction

- can ***steer*** the antenna array to transmit signals or receive signals from specific direction

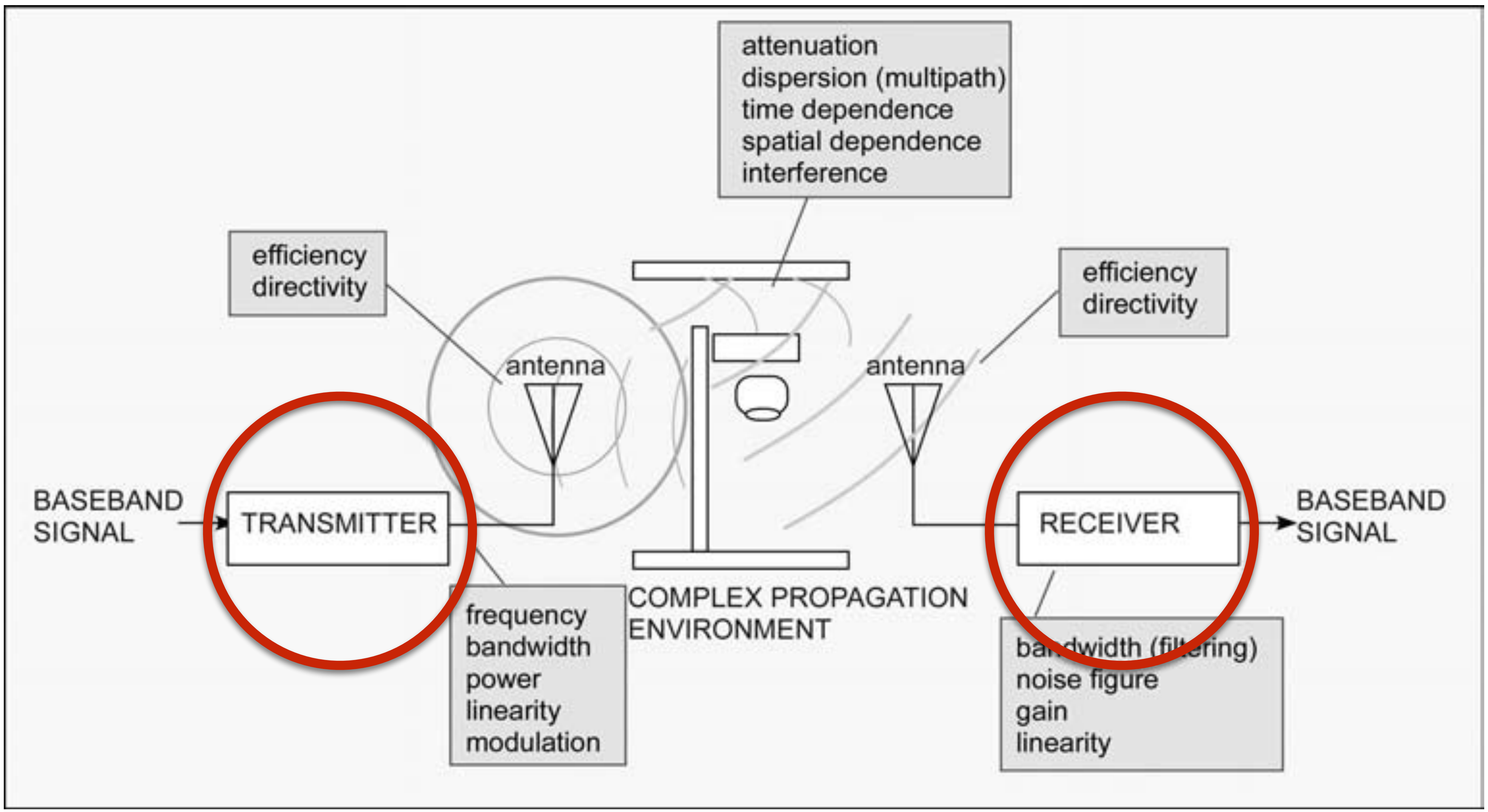


Example applications

- MIMO (e.g., 802.11ac, 5G,..)
- selective target jamming

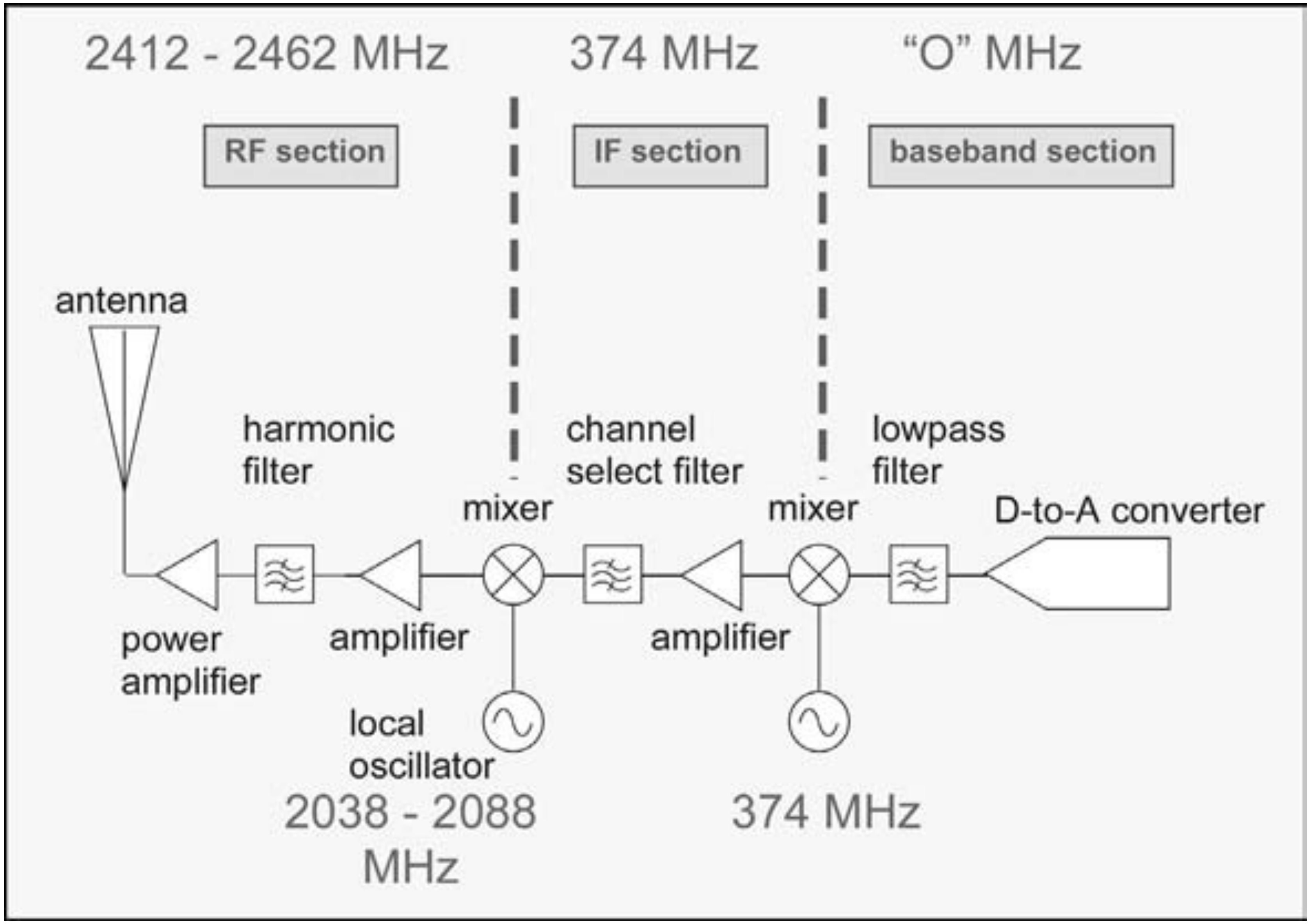
Can they be used to achieve security (e.g., confidentiality)?

Building Blocks of a Wireless System



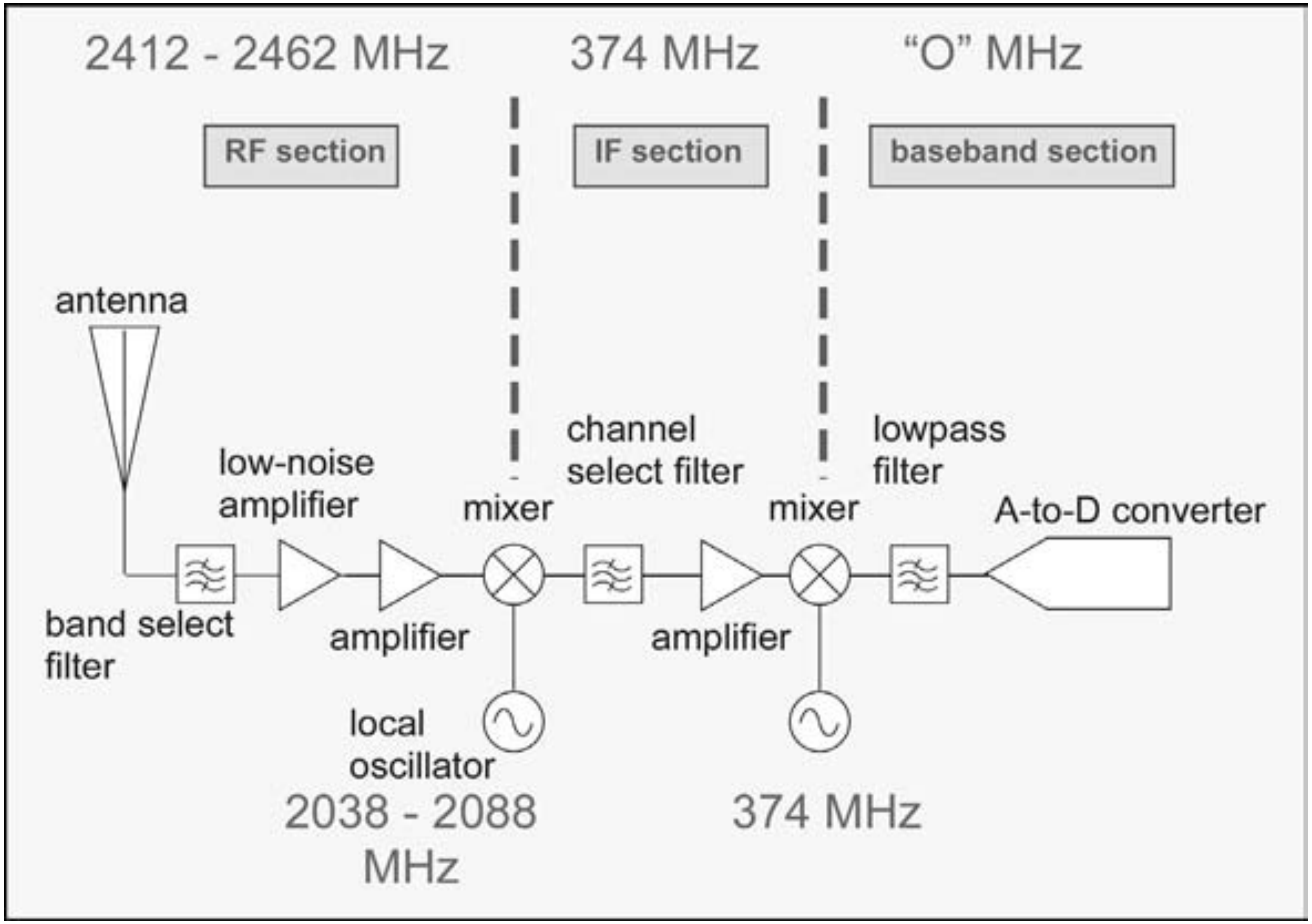
Source: Dobkin, RF Engineering for Wireless Networks

Generic Transmitter Architecture



Key Properties: Transmitted power, carrier frequency, information bandwidth, modulation type

Generic Receiver Architecture



Key Property: Receiver sensitivity (depends on the antenna, low noise amplifier, mixer)

Software Defined Receivers (SDR)

- low-cost (starts from $20)
- traditional components such as mixers, amplifiers, modulator, demodulators implemented in software
- signal processed in PC
- flexible, low-power…

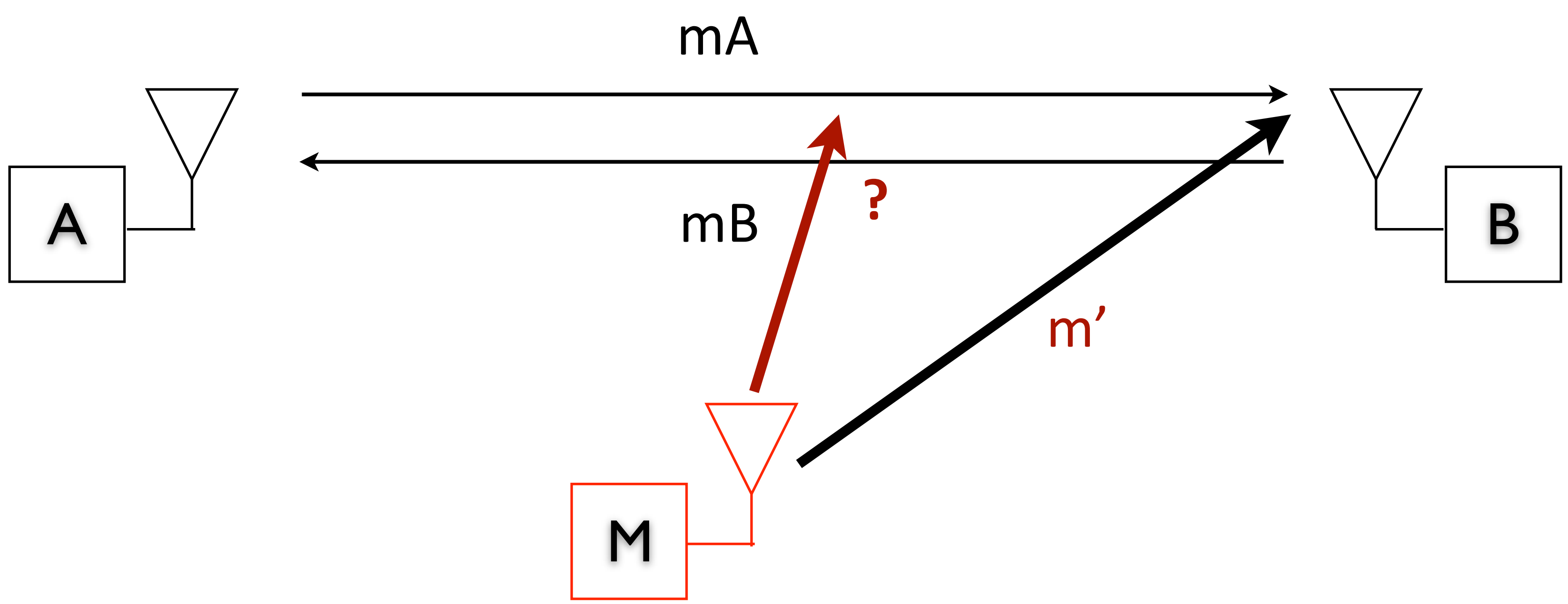
increasingly important in modern day electronic warfare

e.g., GPS spoofing now possible with less than $100

Security of Wireless Networks (a few pointers)

Wireless Networks

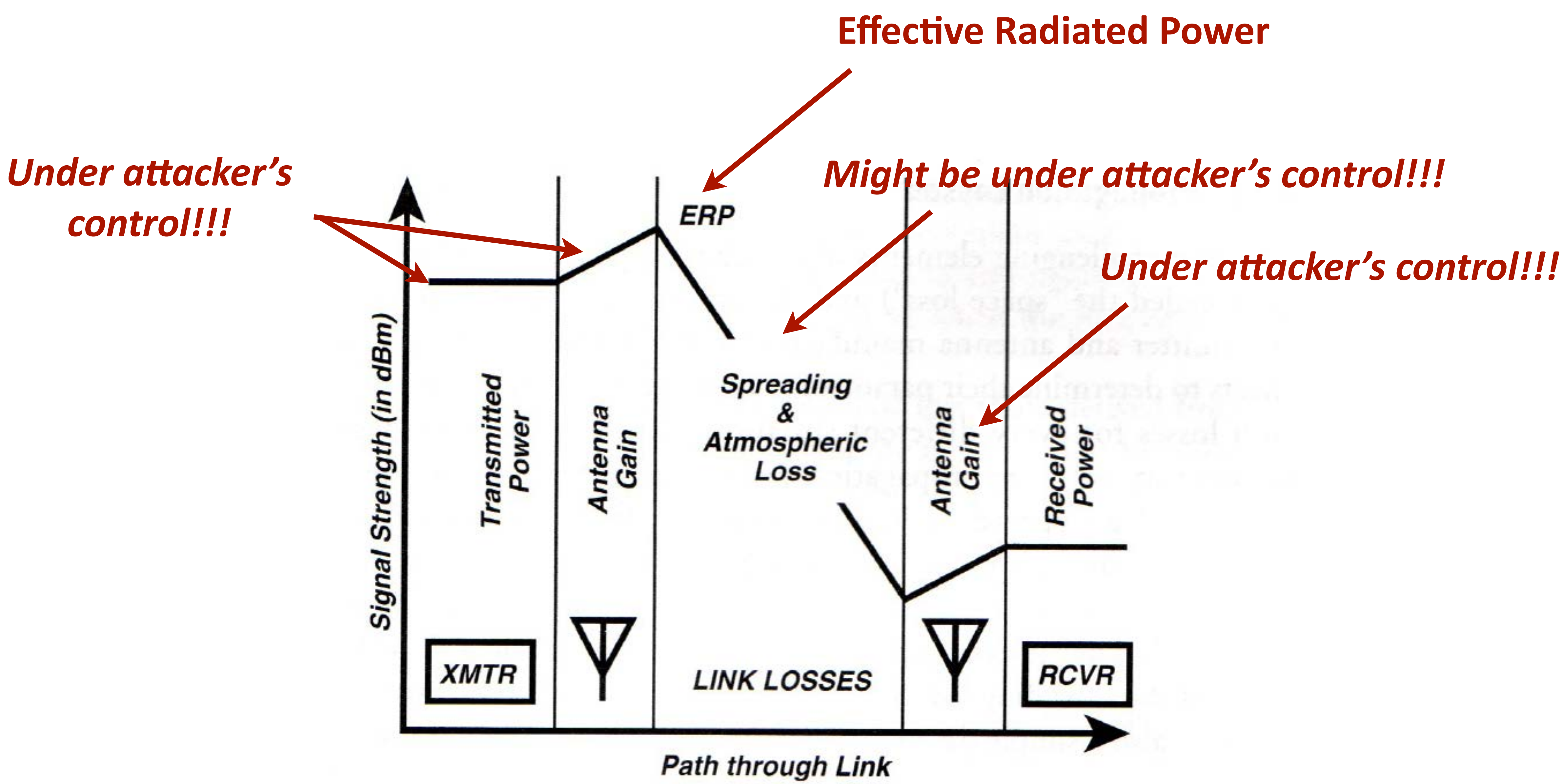
- We step back now. Do we need encryption/MACs/signatures to protect *confidentiality and authenticity* of messages in wireless networks?



- Can the attacker eavesdrop and insert/modify messages on a wireless channel?
- And why is the arrow pointing at B?

Radio Signal Propagation and Losses

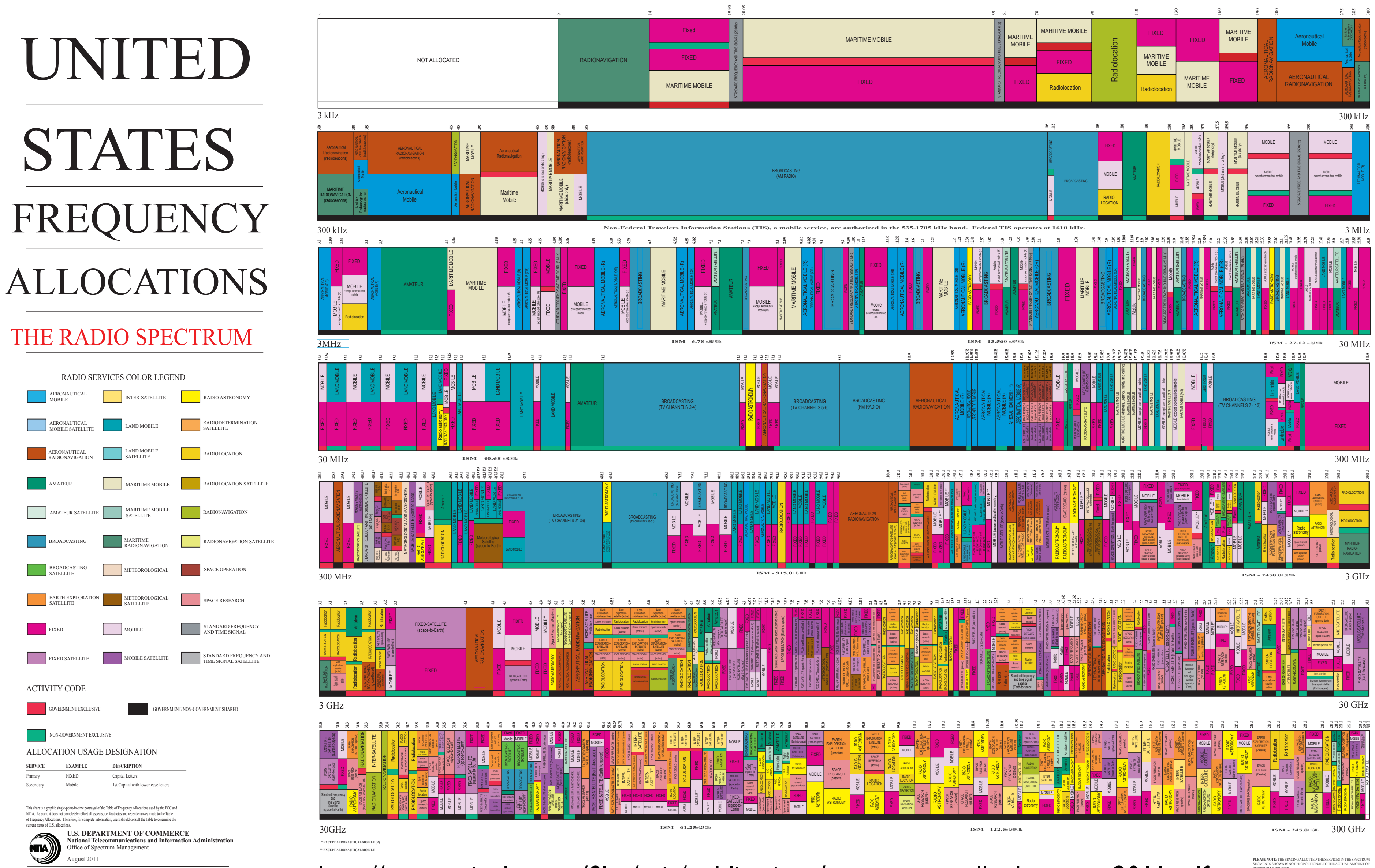
- Channel equation: Calculating the signal strength at the receiver



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

Wireless Communication: Basics

- Communication frequencies are typically known
- If not, can be discovered by *broadband receivers*
- We can try to “run or hide” *(FHSS,DSSS)*



http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf

Wireless Communication: Basics

- Decibel: dB, dBi, dBm, ...
  - dBm = dB value of signal strength / 1 miliwatt (mW)
    used to describe signal strength.
  - dBW = dB value of signal strength / 1 watt (W)
    used to describe signal strength.
  - dBi = dB value of antenna gain relative to the gain of an isotropic antenna
    (0dBi is the gain of an isotropic antenna)

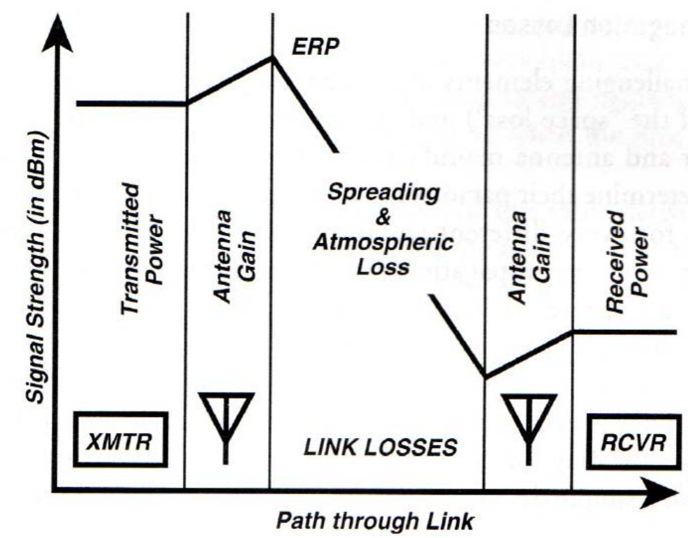
- A linear number is converted into dB, by the following formula:
  - $N(dB)=10\log_{10}(N)$
  - $N(dBm)=10\log_{10}(N/1mW)$
  - e.g. 1W = +30dBm
  - Note: $\log(x)+\log(y)=\log(xy)$;
    $\log(x)-\log(y)=\log(x/y)$
- A linear number is converted into dB, using the following formula:
- N(dB) = 10log10(N)
- N(dBm) = 10log10(N/1mW)
- e.g. 1W = +30dBm

Wireless Communication: Basics

- *Channel equation:*
- Example
  - Transmitted Power (1W) = +30 dBm
  - Transmitting Antenna Gain = +10 dB
  - *Spreading Loss = 100 dB*
  - Atmospheric Loss = 2 dB
  - *Receiving Antenna Gain = +3 dB*
  - `Received Power`

    `= +30dBm + 10 dB – 100 dB – 2 dB + 3 dB`

    `= -59 dBm`



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

©D. Adamy, A First Course on Electronic Warfare

Under attacker's control!!! (somewhat)

- *Receiver sensitivity:* The weakest signal from which the receiver can still provide the proper specified output.

Wireless Communication: Basics

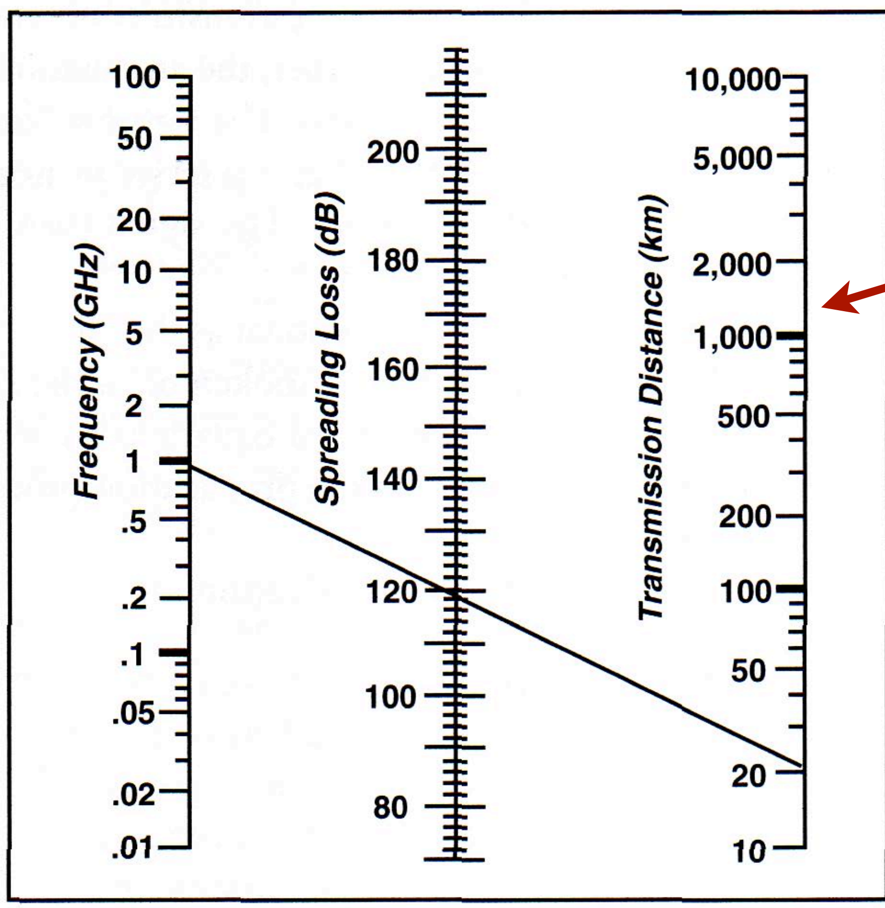
- *Propagation of EM radiation*
  - In *free space* the power density of an EM wave obeys the *inverse-square law* wrt the distance from the source:

$$p \propto 1/d^2$$

  - *Confidentiality*
    - Reduce transmission power
    - “Make sure” that the attacker is not “too close”
  - *Authentication*
    - Attacker is “too far” to be able to send/modify messages!
  - *Does that work?*

Wireless Communication: Basics

- Spreading losses:



Spreading loss can be determined by drawing a line from the frequency (in GHz) to the transmission distance (in km) and reading the spreading loss (in dB) on the center scale.

Under attacker's control!!!
(somewhat)

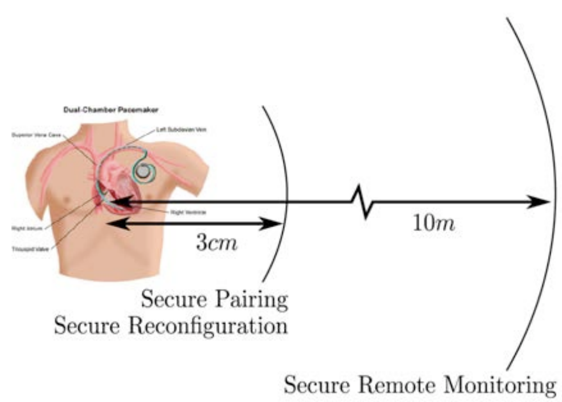
- Calculation (freespace LoS): $L_s(dB)=32.4+20\log_{10}(d \text{ in km})+20\log_{10}(f)$

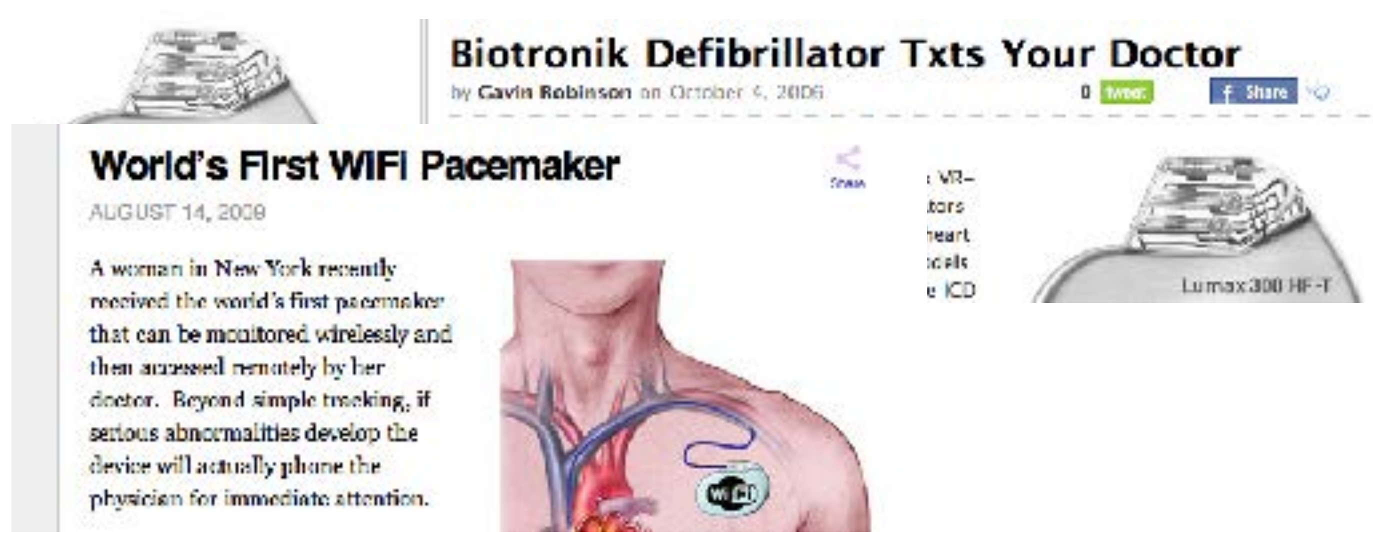
Wireless Communication: Basics

- *Confidentiality*
  - Reduce transmission power
  - “Make sure” that the attacker is not “too close”
- *Authentication*
  - Attacker is “too far” to be able to send/modify messages!
- *Does that work? Sometimes,* ***Generally NO!***
  - Bluetooth communication >1km
  - WiFi > 10km

Wireless Communication: Basics

- Is this important?
  - Yes, if e.g., you want to do e-banking over your WiFi - *integrity/confidentiality (security)*
  - You can get fined if you don't secure access to your network - personal liability (DE) - *regulatory*
  - If you had an RF-enabled implant it might be *(most are today!)* - *safety*
  - *YES, if an application is security/safety critical*





Biotronik Defibrillator Txts Your Doctor

by Gavin Robinson on October 4, 2006

World's First WIFI Pacemaker

AUGUST 14, 2009

A woman in New York recently received the world's first pacemaker that can be monitored wirelessly and then accessed remotely by her doctor. Beyond simple tracking, if serious abnormalities develop the device will actually phone the physician for immediate attention.

- Encryption and MAC/signatures will help? Yes, but ...

Wireless Communication: Basics

- Encryption and MAC/signatures will help? Yes, but ...
  - Let’s introduce authentication and confidentiality
  - Example: *Passive Keyless Entry and Start Systems*

Active keys
Need to be close (<100m) and press
a button to open the car.
Physical key to start the car.

Passive Keyless Entry and Go
Need *to be close (<2m)* and the car opens.
Need *to be in the car* to start the car.
No need for human action!

Passive Keyless Entry and Start System:

- The key is “in the pocket” and *when the user **is near**, the car opens*
- *When the key is **in the car**, the car can be started* by pressing an ignition button)

- Implemented by all major car manufacturers

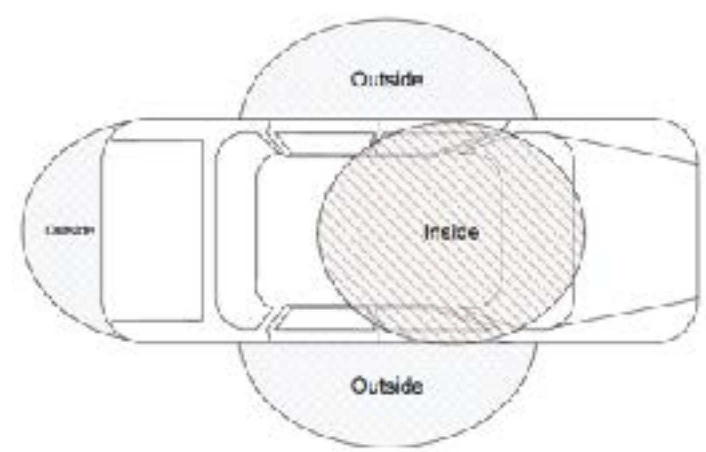
Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Sketch of the protocol:

short range (<2m)
Fresh Challenge
(LF, 120-135 KHz)

Reply **(Authentic and Confidential)**
(UHF, 315-433 MHz)
long range (<100m)

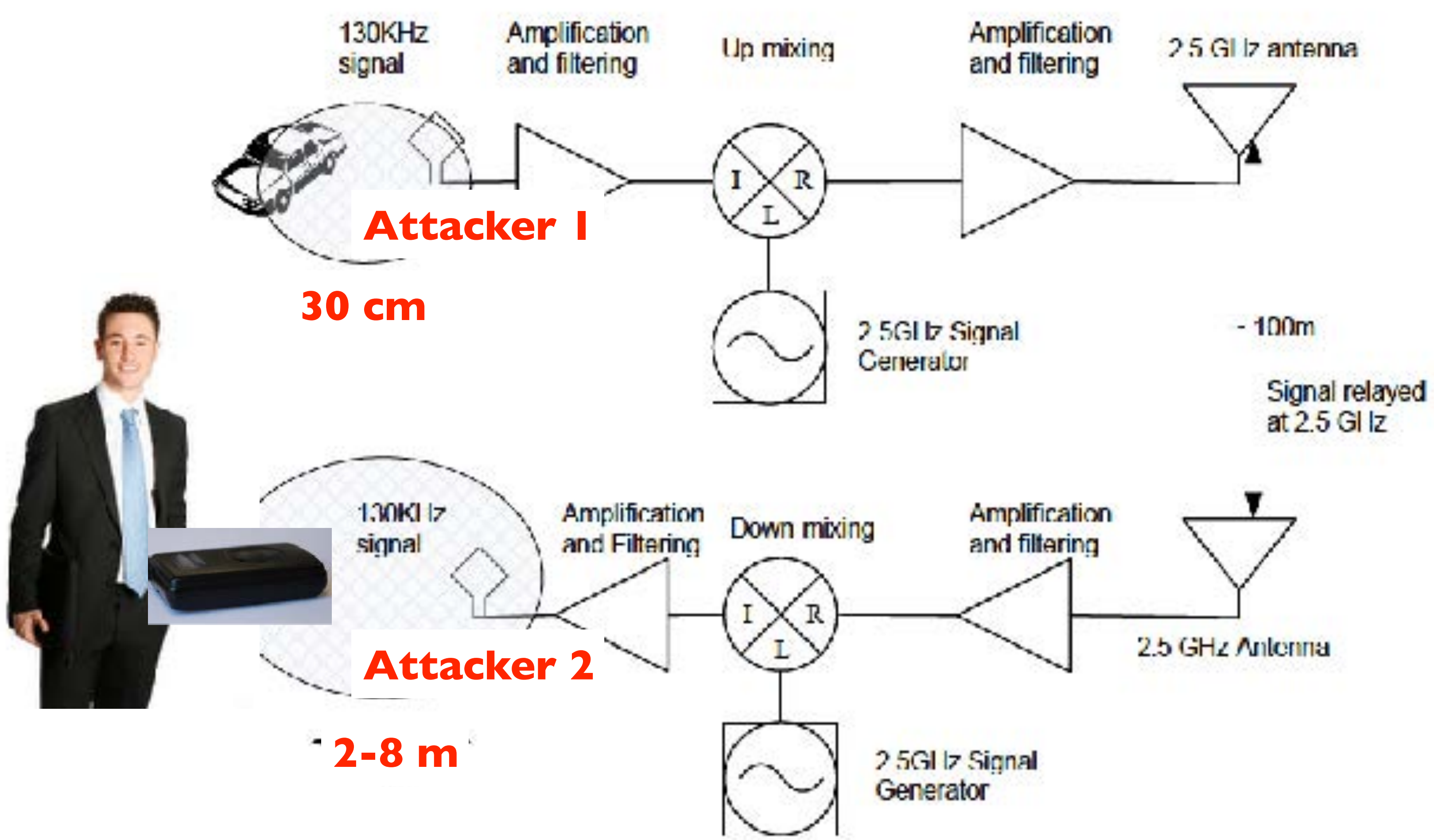
If the correct key
is authenticated,
open the door.



What is wrong with this protocol?

Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Problem: An attacker *relays all communication*
- *Wired or Wireless*



Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars
NDSS 2011

Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Problem: An attacker *relays all communication*

Table 4: Experimental results distances summary. Legend: '✓' relay works without amplification, 'A' with amplification, '-' not tested, '*' value will be updated

Car model	Relay cable						Key to antenna distance (m)			
	7 m		30 m		60 m		No Amplifier		With Amplifier	
	open	go	open	go	open	go	open	go	open	go
Model 1	✓	✓	✓	✓	✓	✓	2	0.4	*	*
Model 2	✓	✓	A	A	A	A	0.1	0.1	2.4	2.4
Model 3	✓	✓	✓	✓	✓	✓	-	-	-	-
Model 4	✓	✓	-	-	-	-	-	-	-	-
Model 5	✓	✓	✓	✓	✓	✓	2.5	1.5	6	5.5
Model 6	✓	✓	A	A	A	A	0.6	0.2	3.5	3.5
Model 7	✓	✓	A	A	-	-	0.1	0.1	6	6
Model 8	✓	A	✓	A	-	-	1.5	0.2	4	3.5
Model 9	✓	✓	✓	✓	✓	✓	2.4	2.4	8	8
Model 10	✓	✓	✓	✓	-	-	-	-	-	-

The range should have been <2m!

Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Is this a sophisticated attack?

Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Countermeasures:
    - Shield the key (immediate)
    - Remove the battery key (immediate)

    - Build a new system (e.g., based on distance bounding)

      uses time as a side information to check the distance / detect the attack

Wireless Communication: Basics

- Example: *Passive Keyless Entry and Start Systems*
  - Wait, was this even an attack?
  - What kind of authentication are we talking about here? Message? Entity?
  - Which security properties does this protocol verify?

- *PKES systems assume that communication implies physical proximity - and this is NOT correct*

  - Property needed: *authenticated proximity verification*
  - Property verified: *message authentication*