Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair

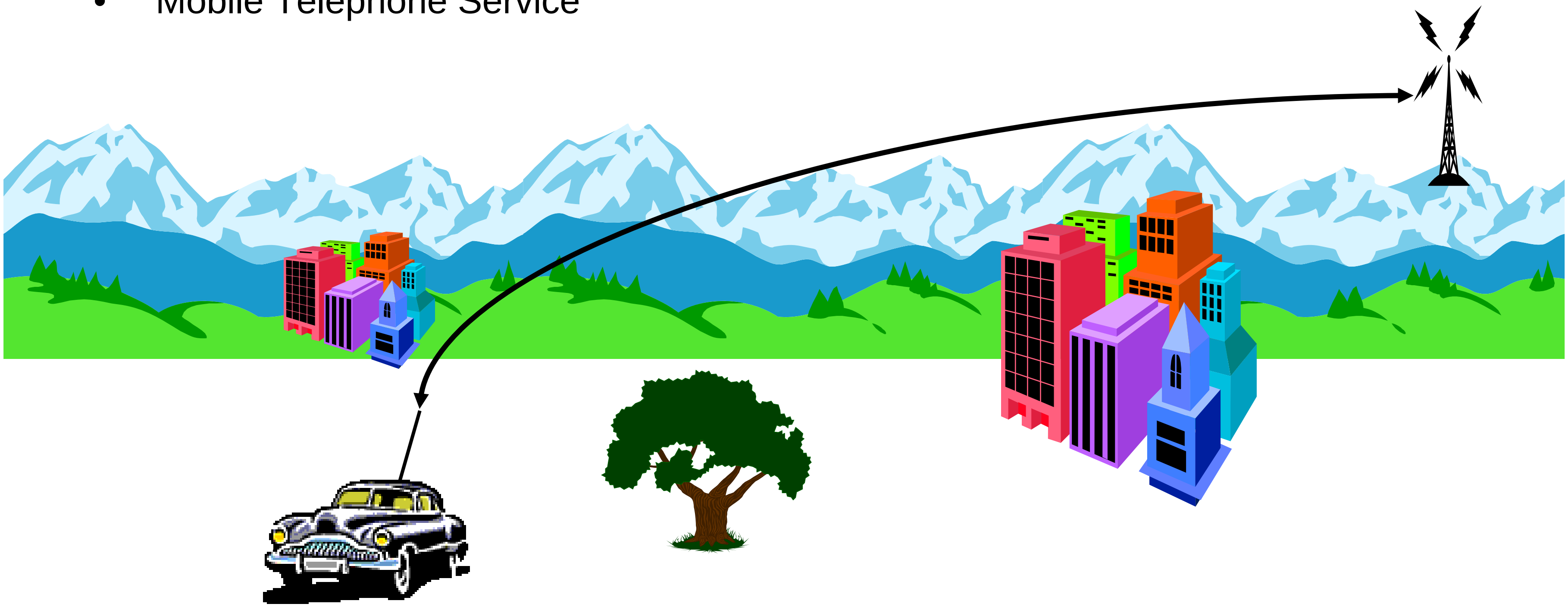
bmcnair@stevens.edu

Week 2

Topics in Wireless Systems

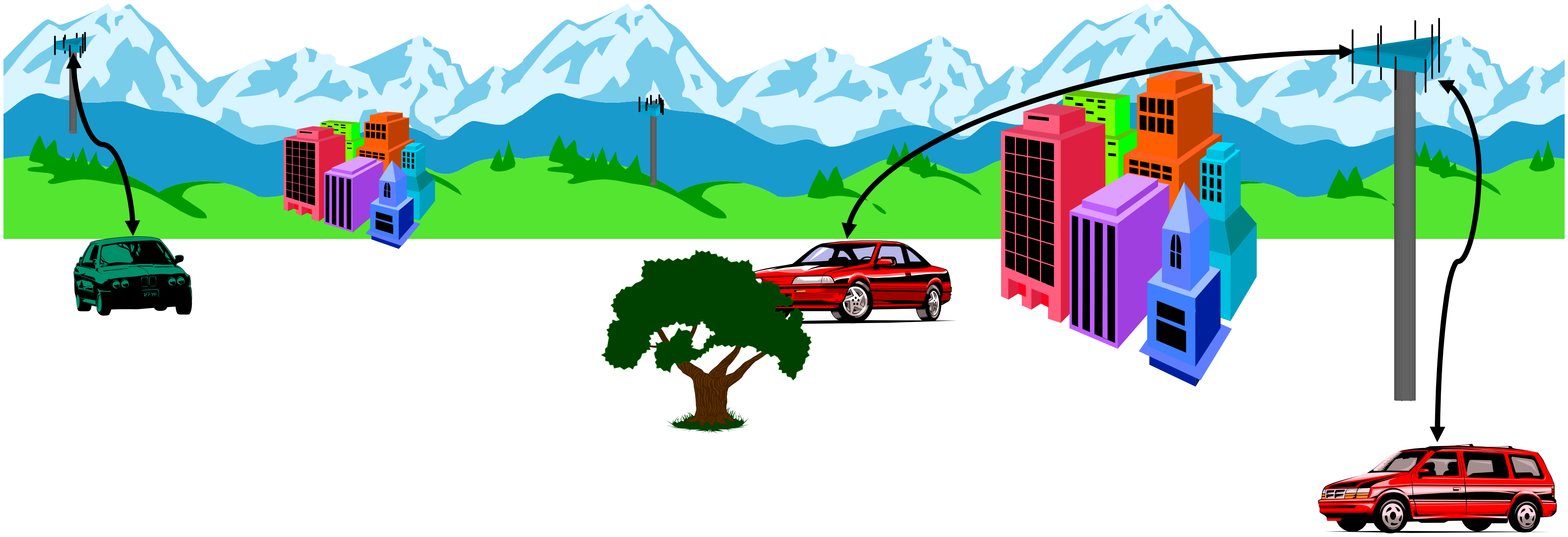
0^{th} Generation Wireless Systems

- Mobile Telephone Service



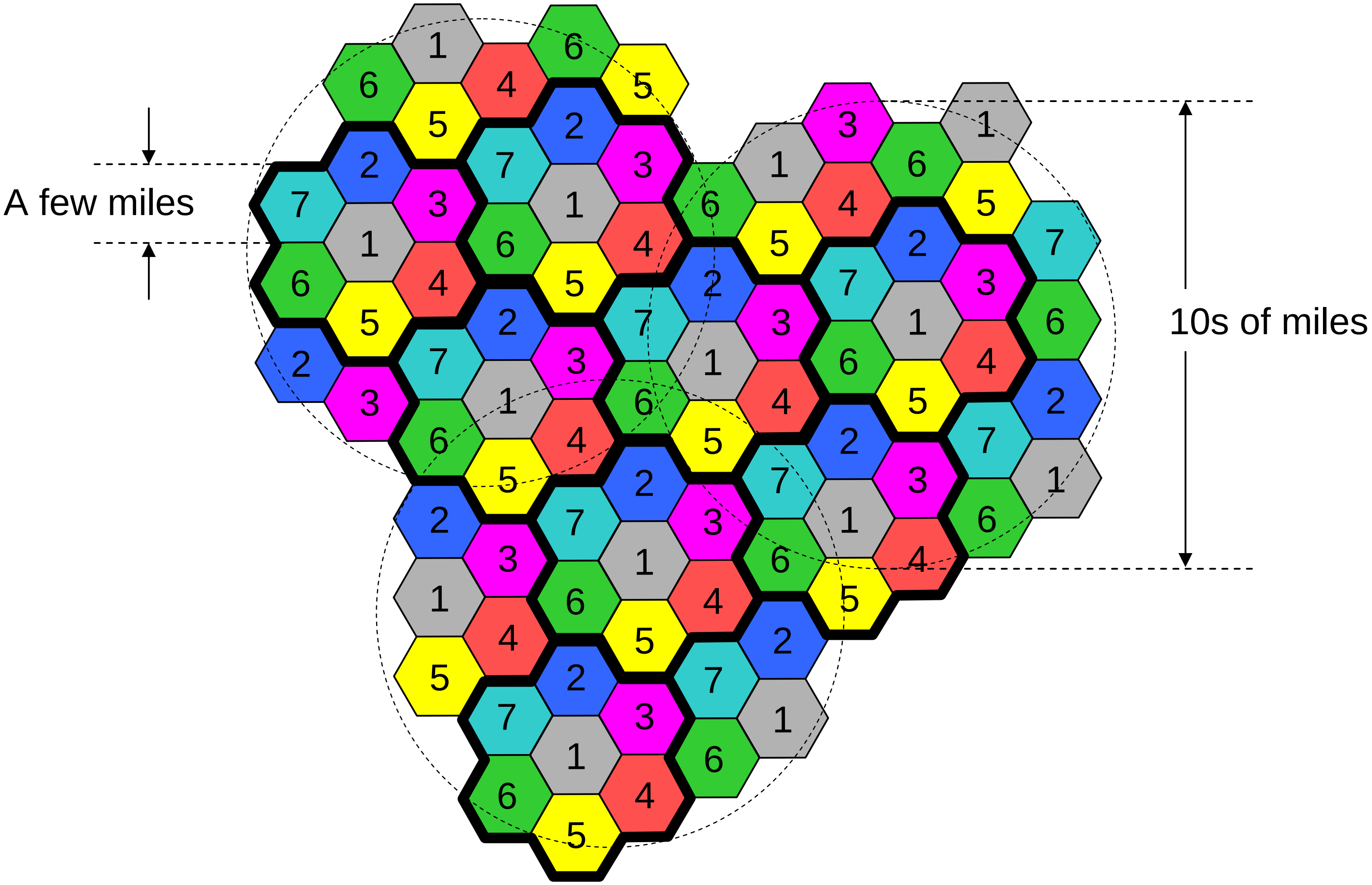
- Few, high-power, long-range basestations
  -> No sharing of spectrum
    -> few users
      -> expensive

Cellular Systems – 1^{st} Generation



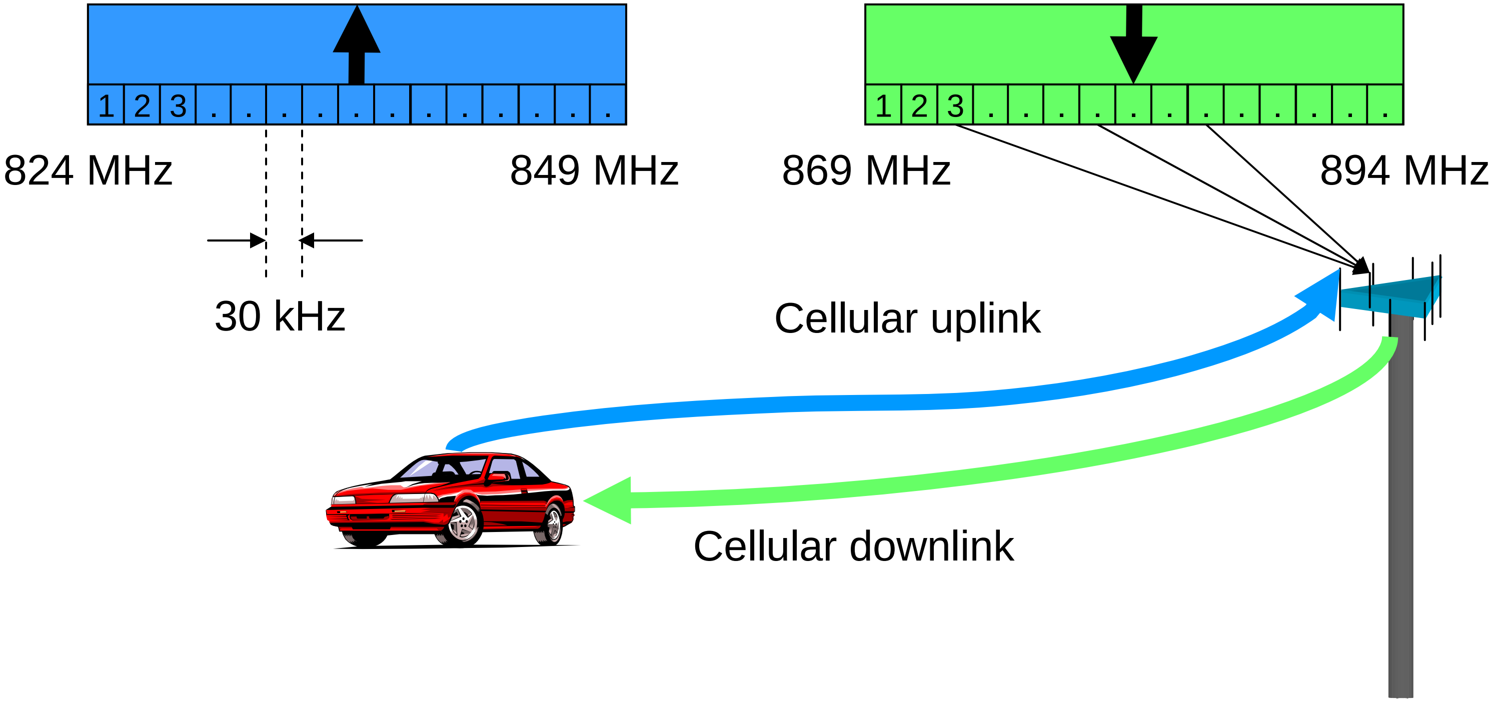
Frequency Re-use

- Covering the MTS service area with cells:



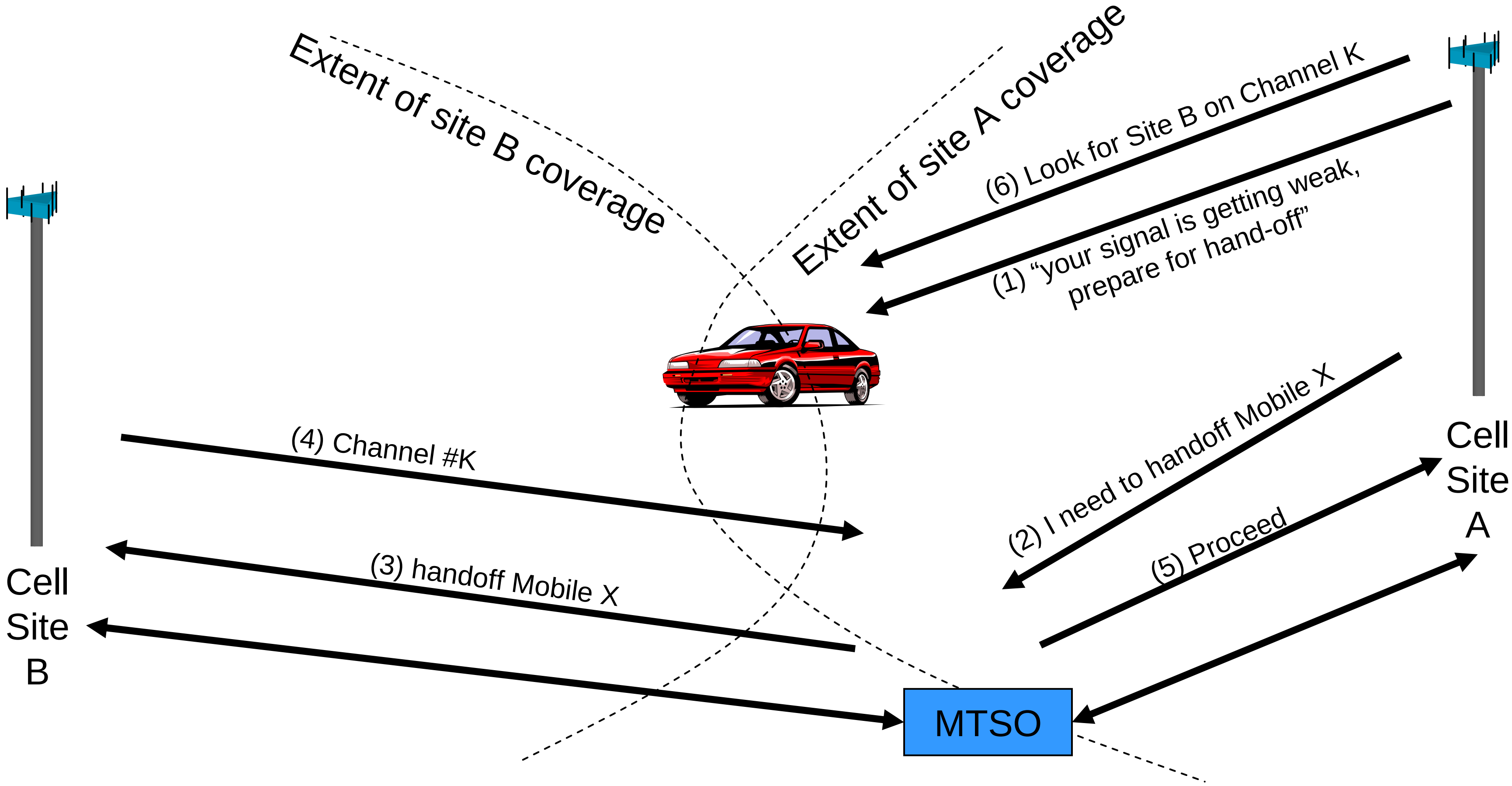
Full Duplex Communications in Cellular

- North American AMPS frequencies:

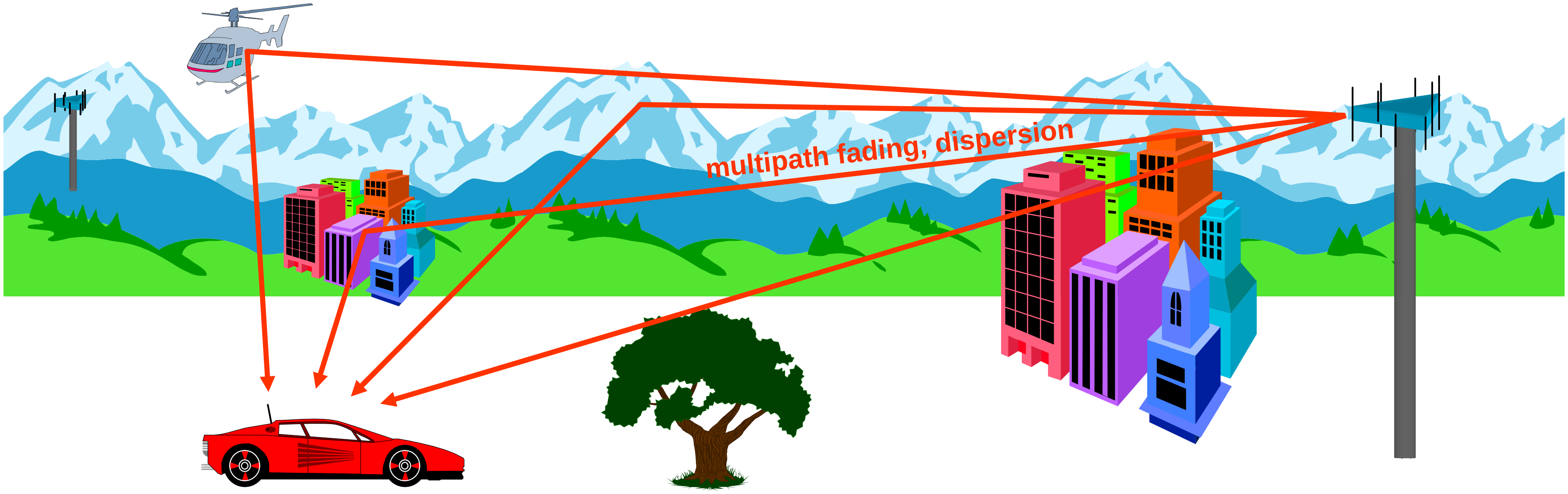


Cellular "Hand-off"

- Providing coverage as mobile moves between cell site coverage areas

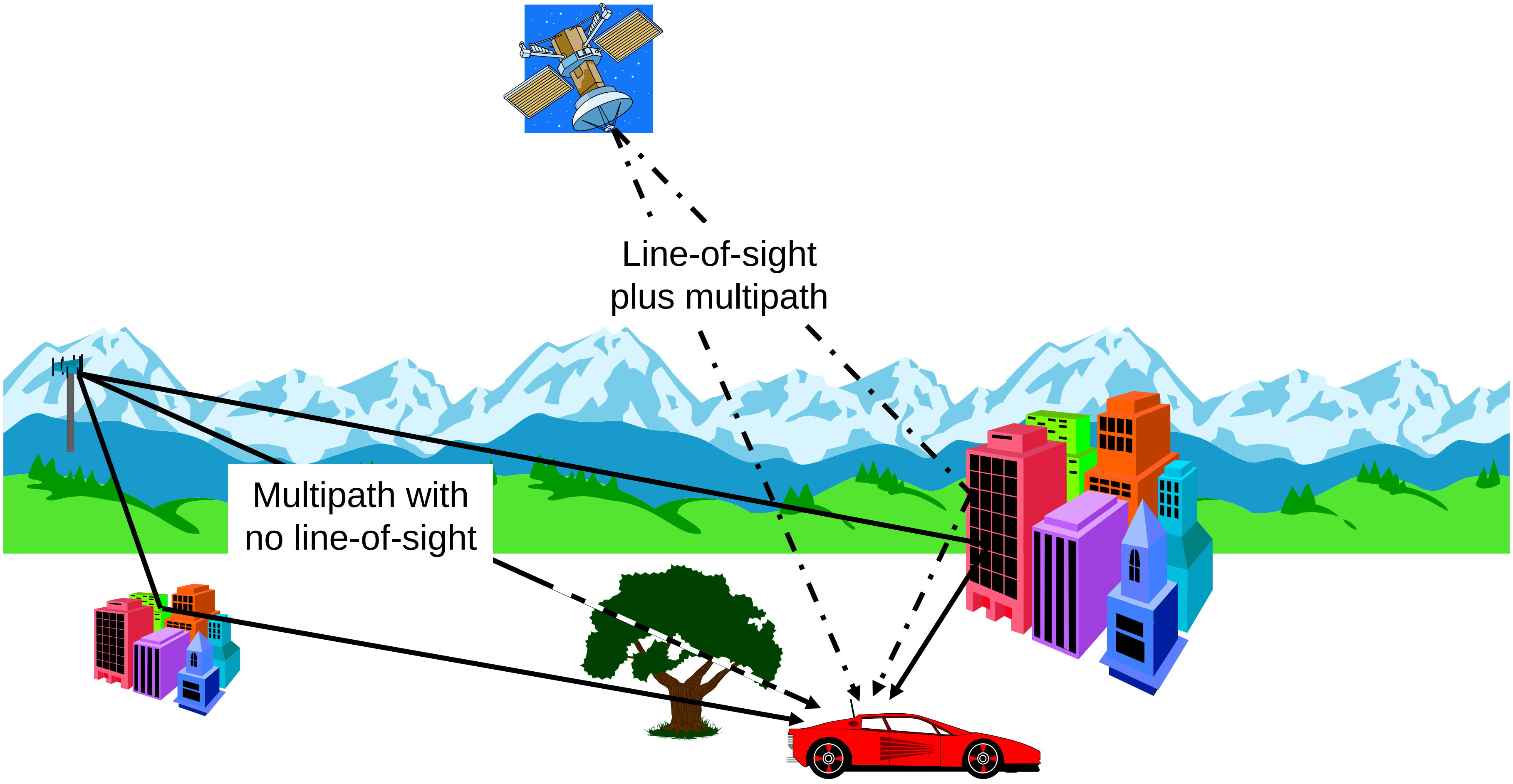

Extent of site B coverage
Extent of site A coverage
(6) Look for Site B on Channel K
(1) "your signal is getting weak, prepare for hand-off"
Cell Site A
Cell Site B
(4) Channel #K
(3) handoff Mobile X
(2) I need to handoff Mobile X
(5) Proceed
MTSO

Channel dispersion

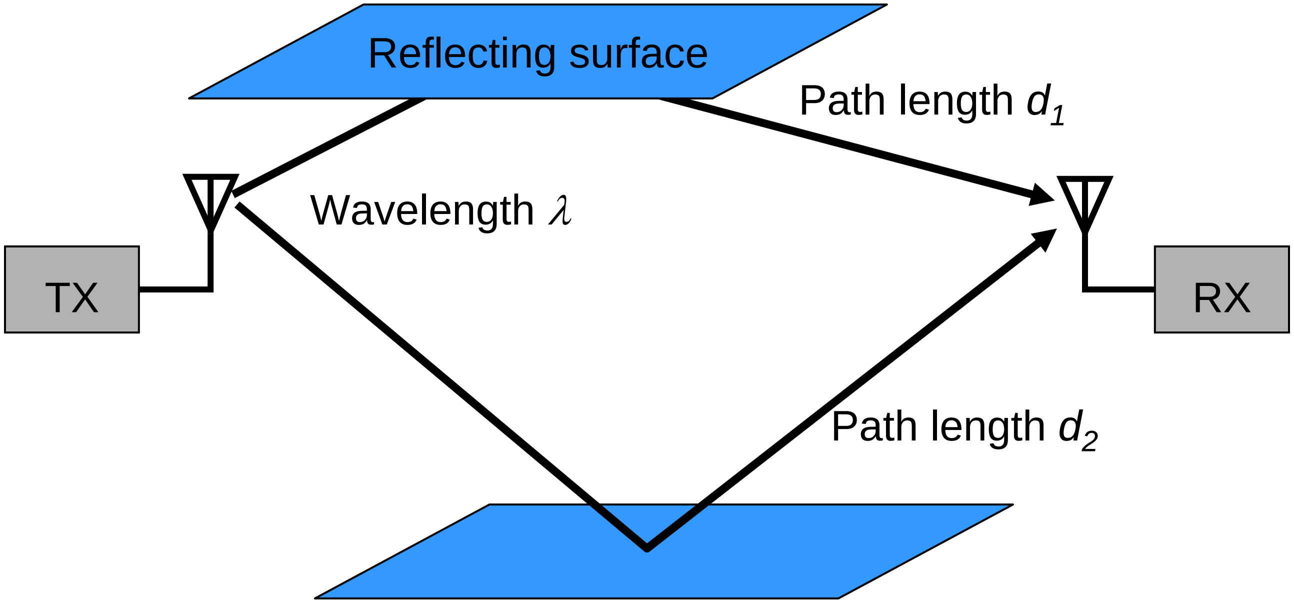


- Multipath reflections create time dispersion of the received signal
- Movement of the receiver, transmitter or objects in the environment create changes in the multipath environment

Characterizing the RF Fading Environment



Effects of Multipath

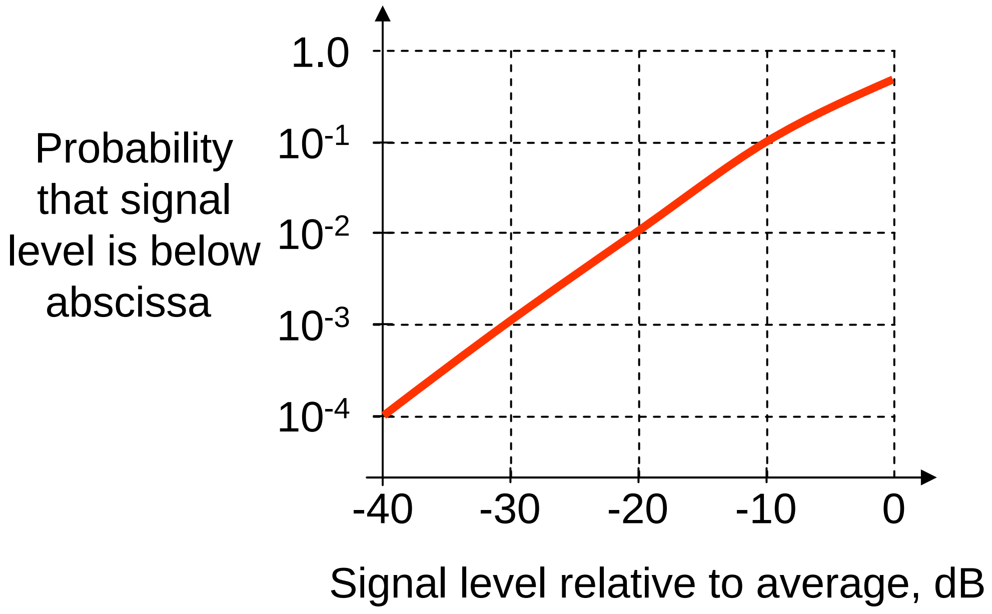


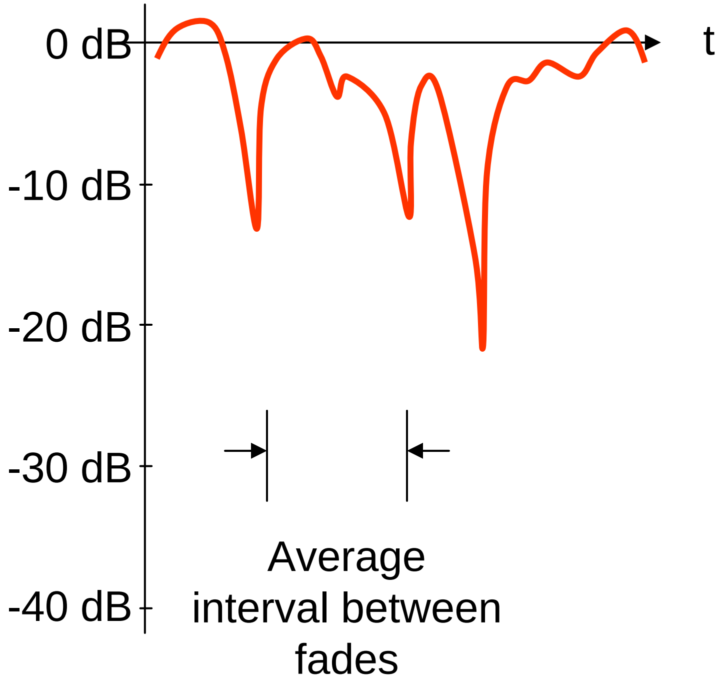
- Conditions for complete, destructive interference between path_1 and path_2 :

$$A_1 = A_2$$

$$d_1 - d_2 = (k + .5)\lambda$$

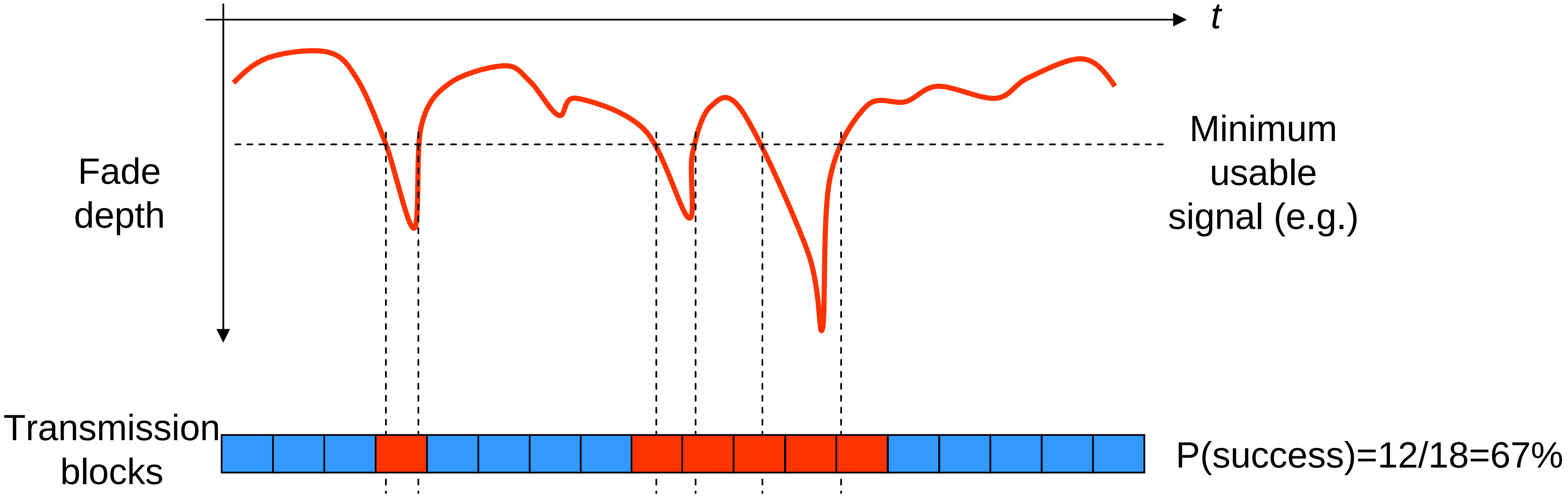
Rayleigh Fading





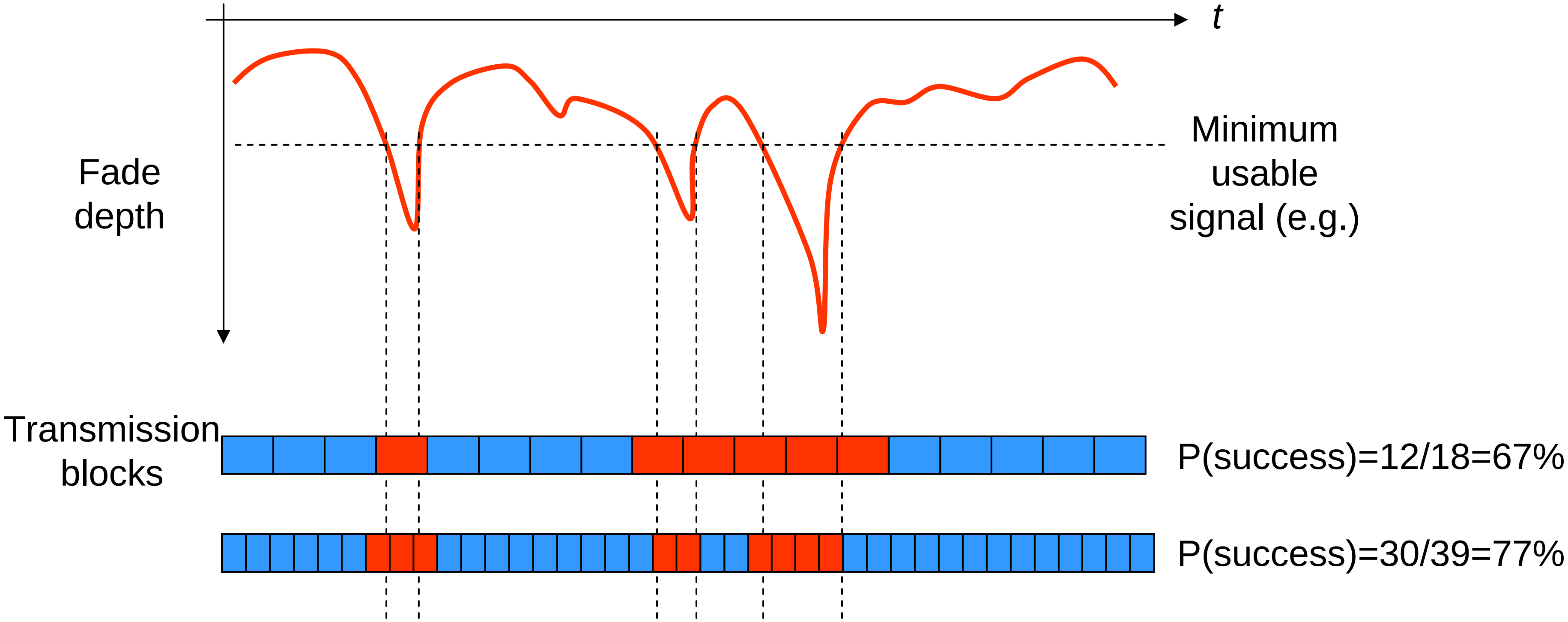
Dealing with the RF Environment

- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:



Dealing with the RF Environment:
Understand the channel characteristics

- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:

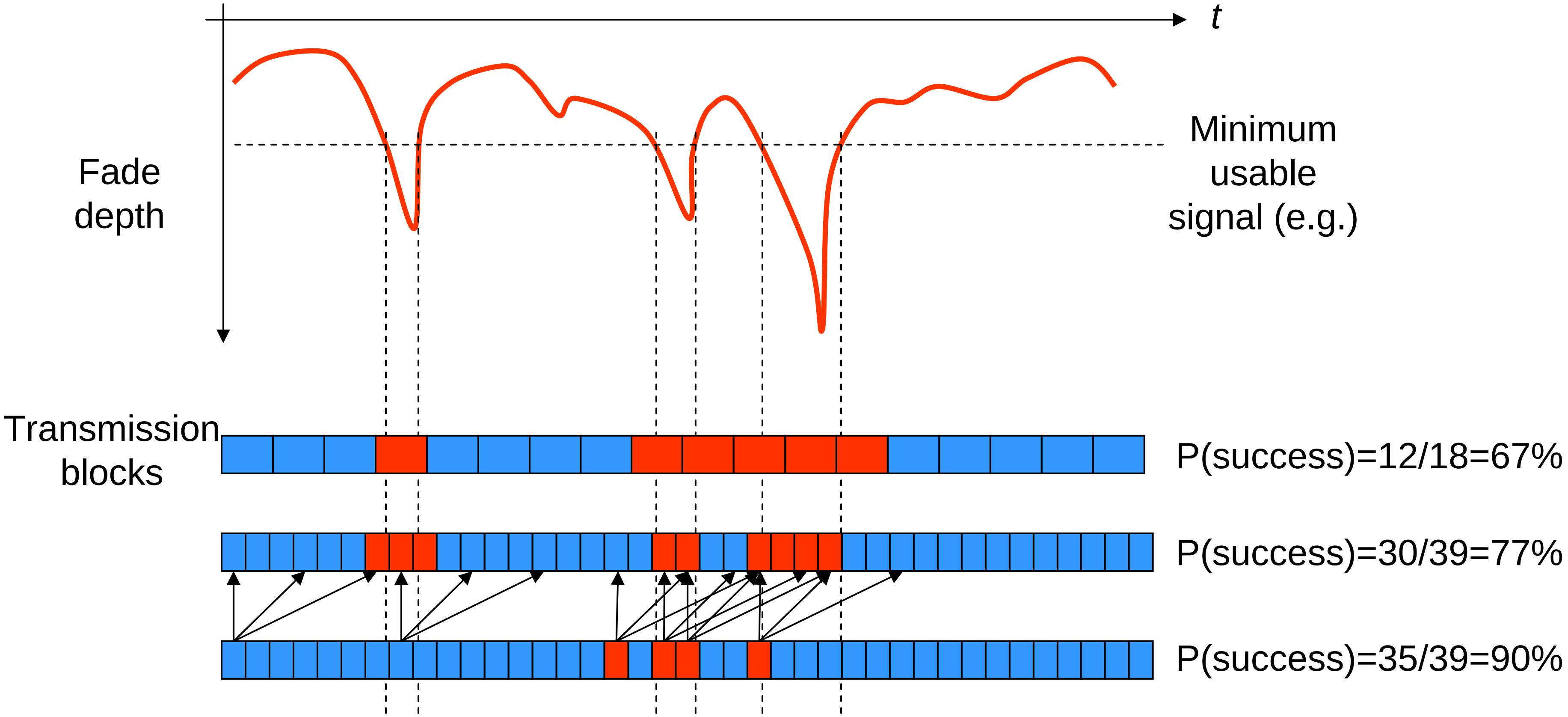


P(success)=12/18=67%

P(success)=30/39=77%

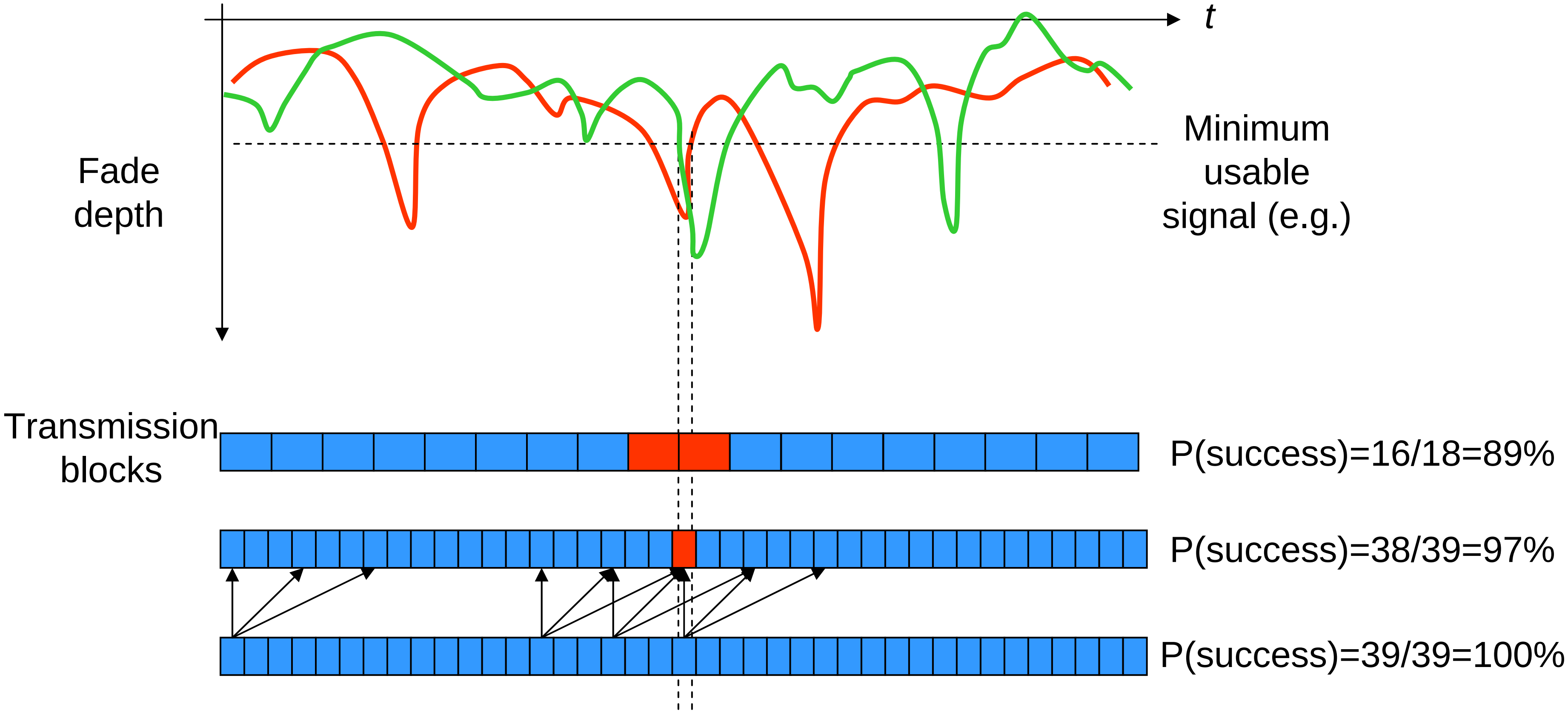
Dealing with the RF Environment: Interleaving

- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:



Dealing with the RF Environment: Diversity

- Consider a ***two*** representative fading profiles measured at two antennas. Assume that a transmission block is lost if any part of it is in fade at ***both***:



P(success)=16/18=89%

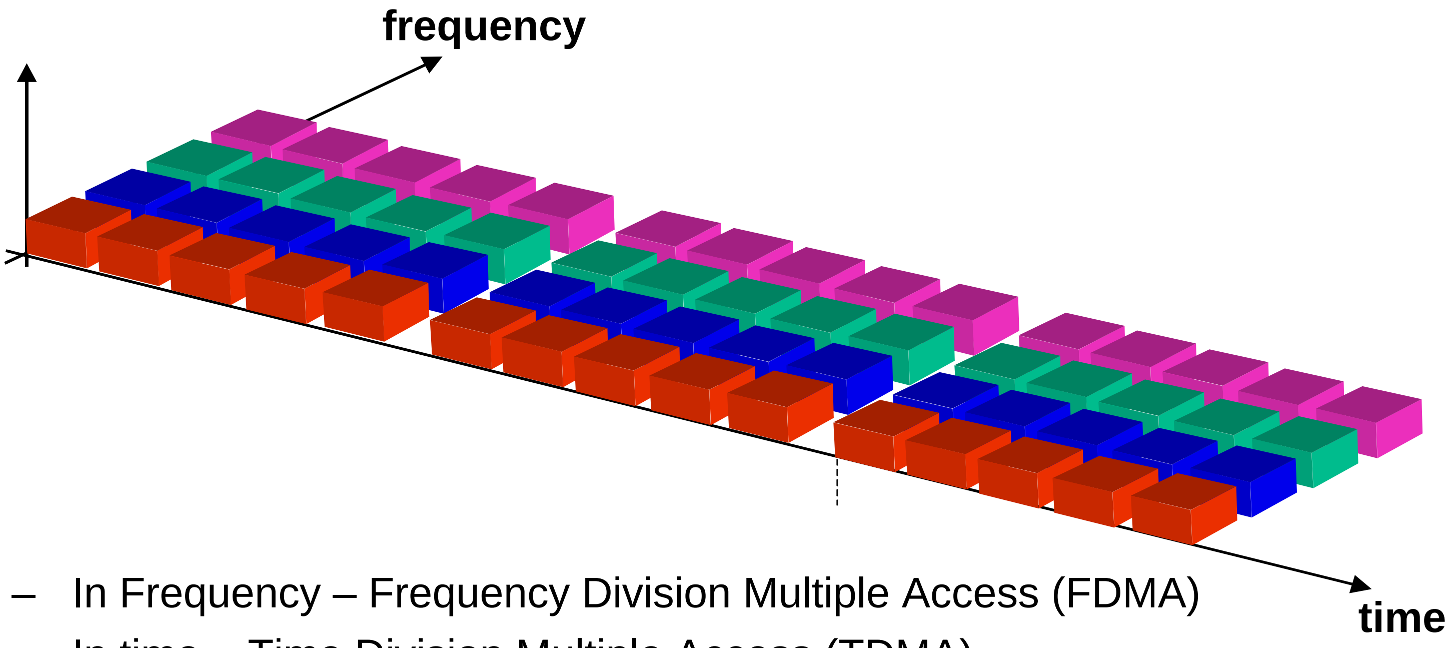
P(success)=38/39=97%

P(success)=39/39=100%

For description of diversity experiments, see http://www.novidesic.com/pubs/ICUPC97F.pdf and http://www.novidesic.com/pubs/vtc2000-a34283.pdf

Multiple Access Techniques

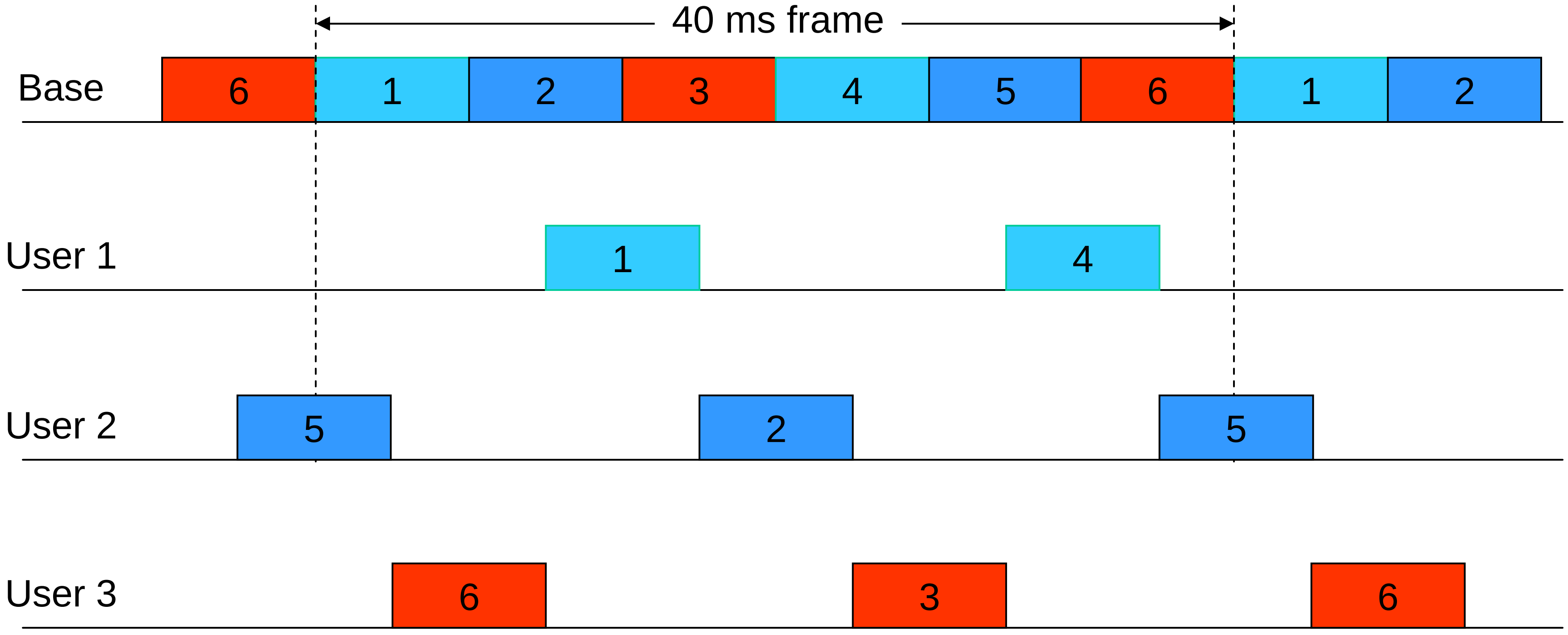
- Commonplace multiple access techniques:



  - In Frequency – Frequency Division Multiple Access (FDMA)
  - In time – Time Division Multiple Access (TDMA)

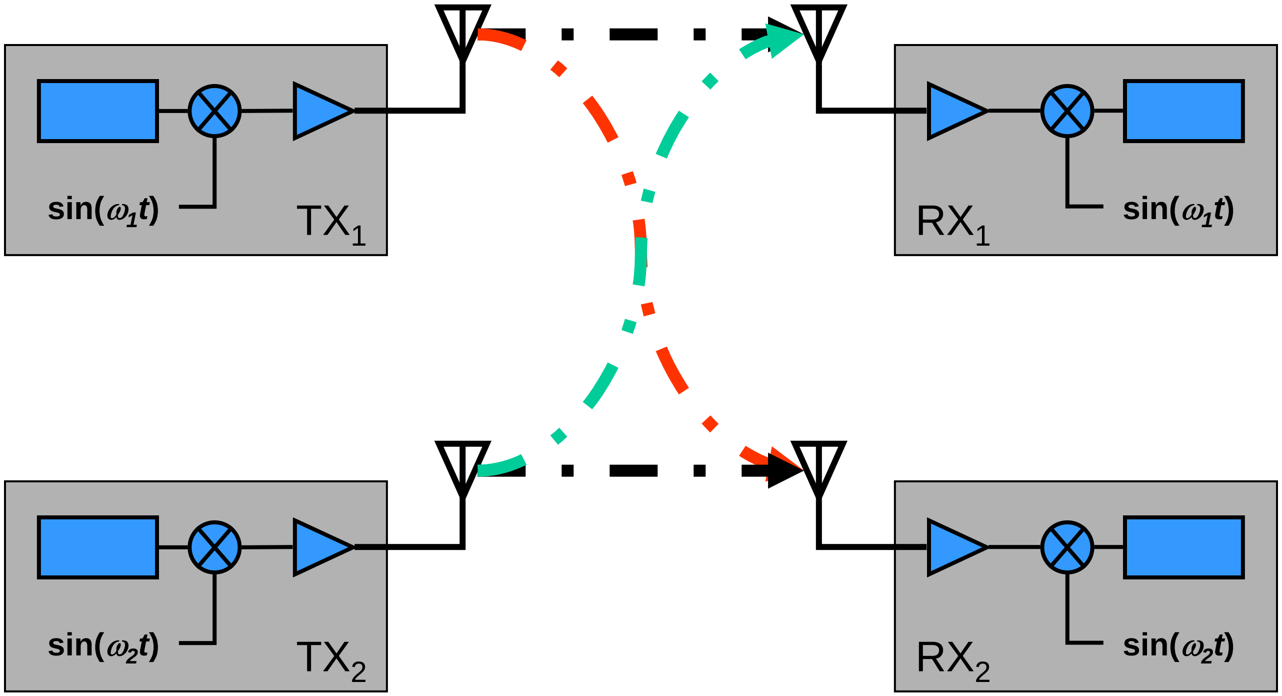
TDMA – 2nd Generation

- IS-54/IS-136:



CDMA – 2nd Generation

- Consider a two channel frequency division system:

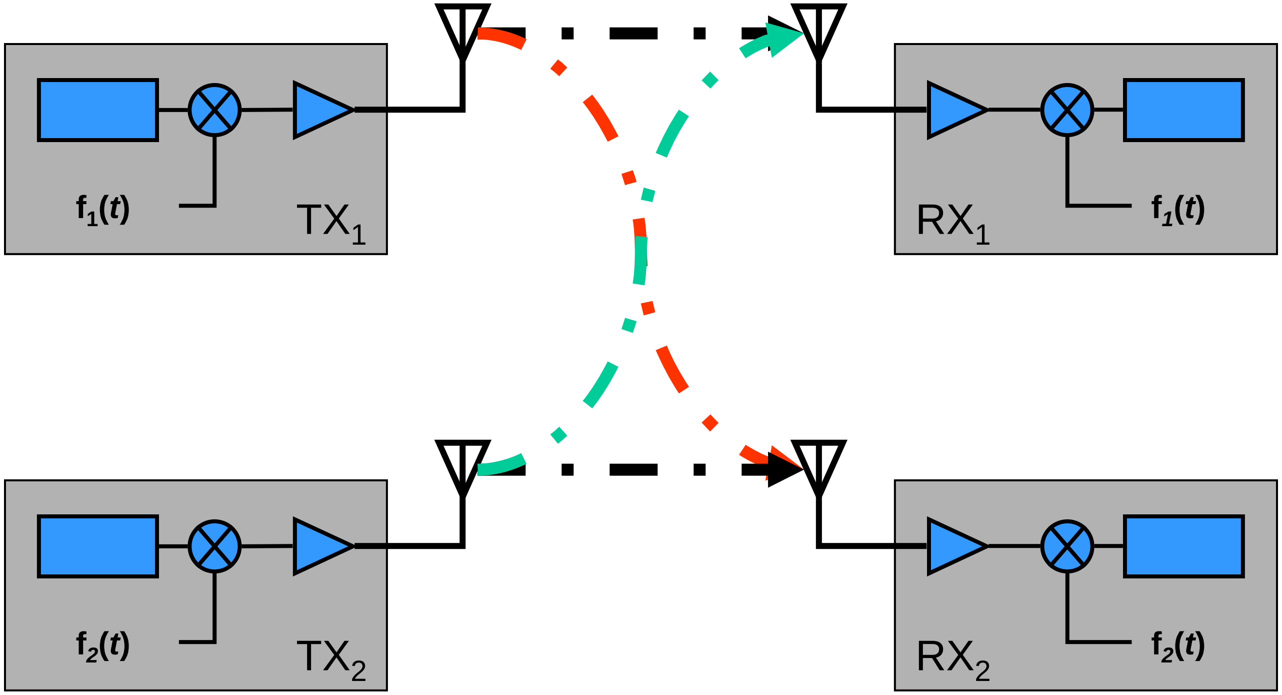


- Fundamentally, what allows RX_1 to receive TX_1 while rejecting TX_2?

$$\text{For } \omega_1 \neq \omega_2, \quad \int \sin(\omega_1 t)\sin(\omega_2 t)dt = 0$$

CDMA – 2nd Generation

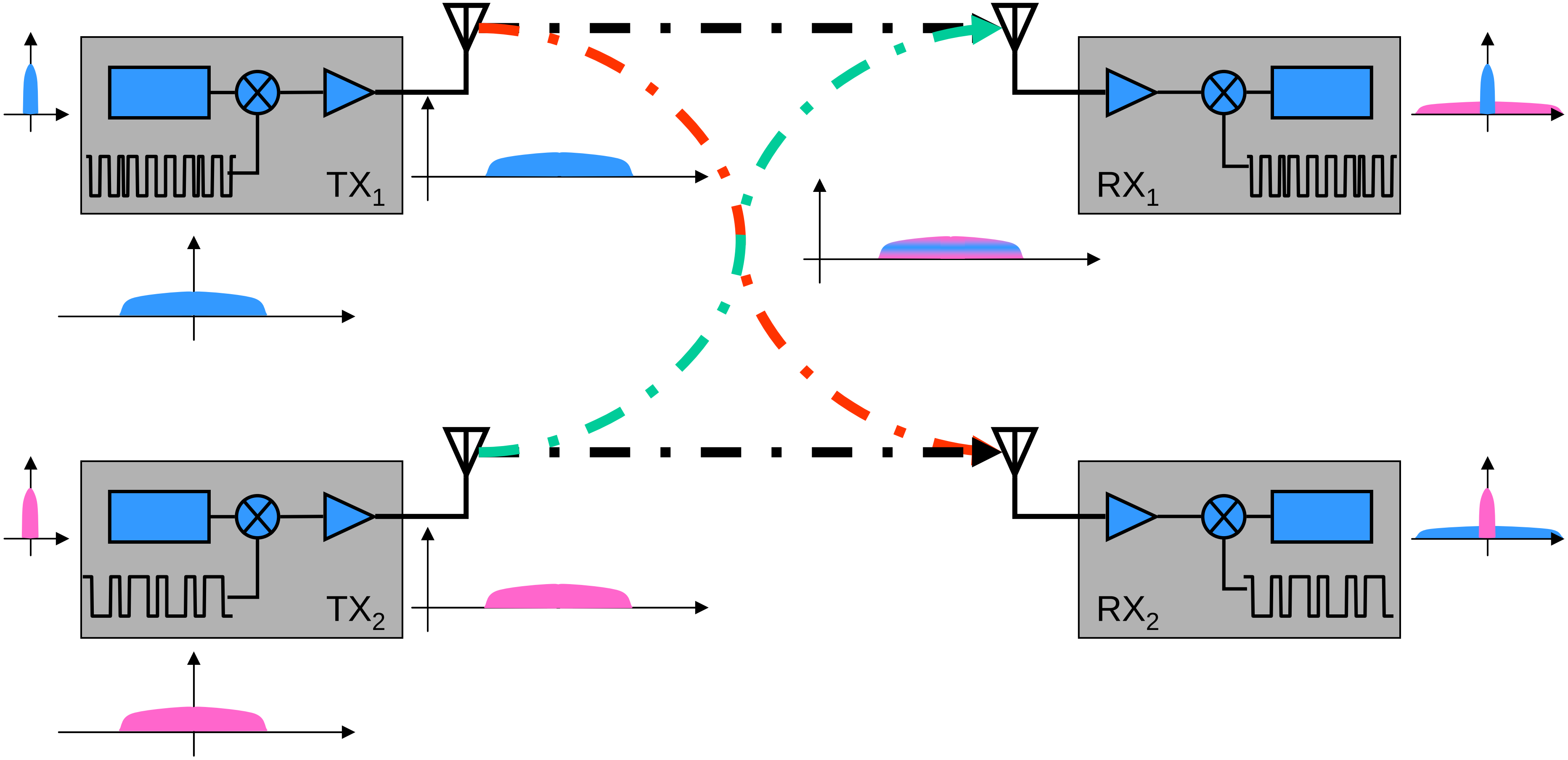
- What is magical about sinusoids? Consider some arbitrary functions:



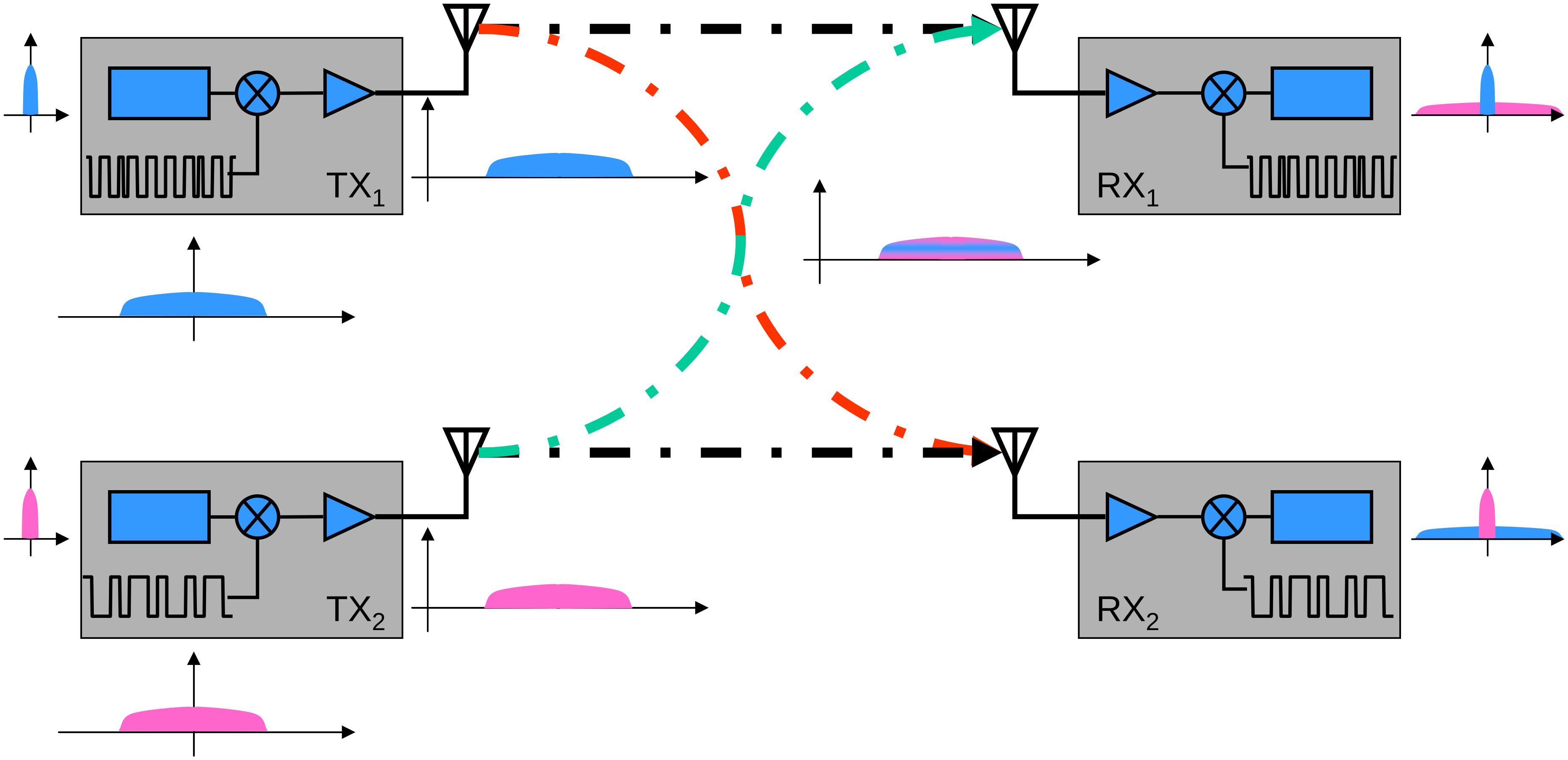
- Constraint on f_1, f_2:

$$\int f_1(t)\, f_2(t)\, dt = 0$$

CDMA Spreading and Despreading

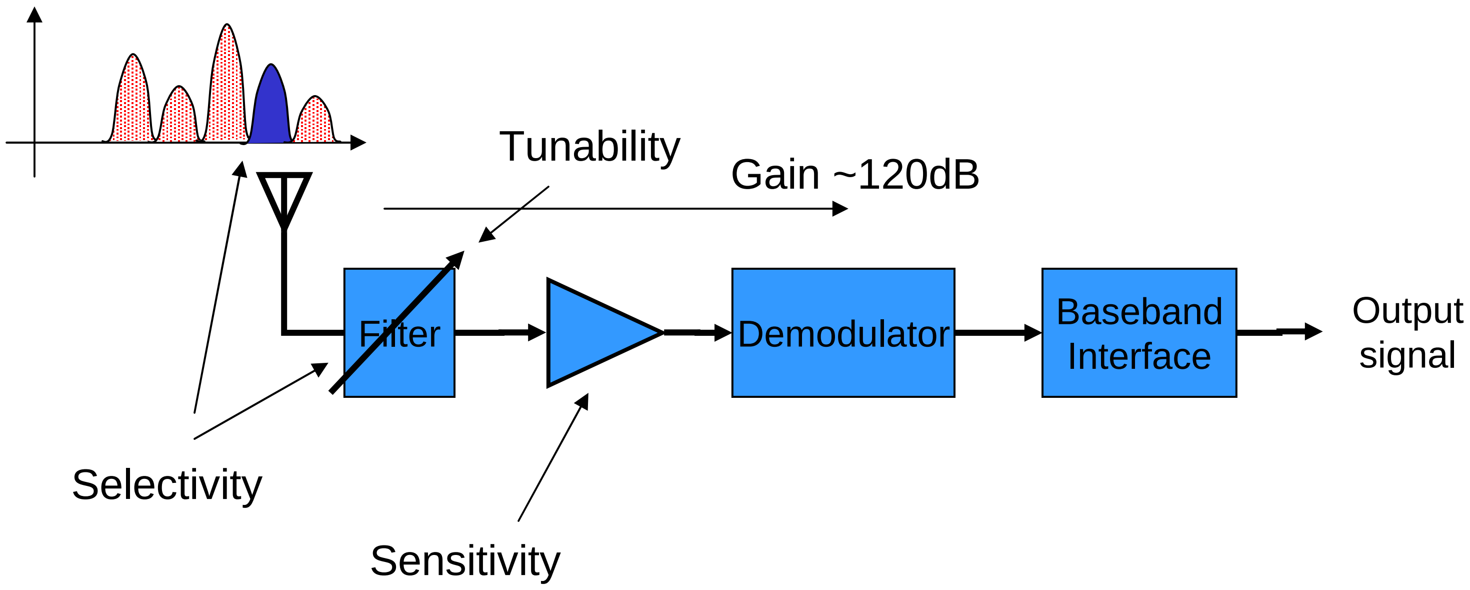


CDMA Spreading and Despreading

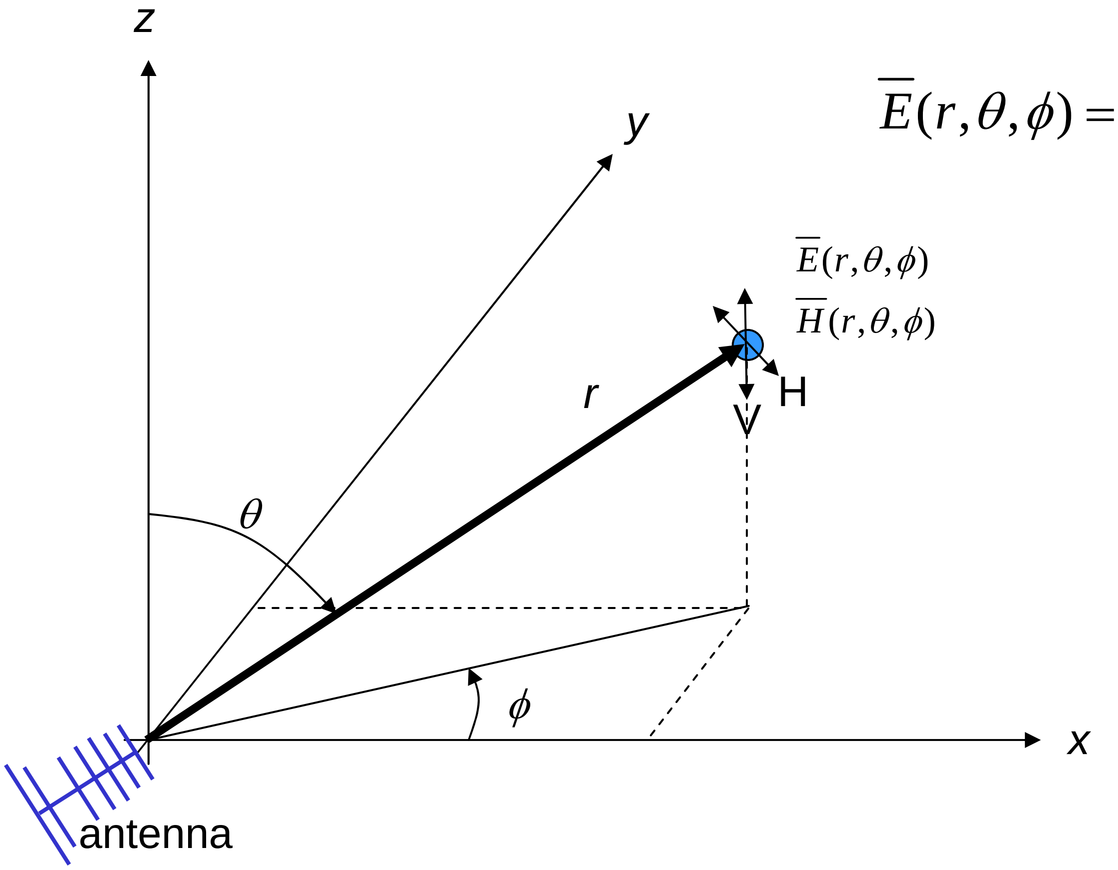


Spreading factor ~ (RF Bandwidth)/(Baseband bandwidth)

General Receiver Considerations



Radiation from an Antenna



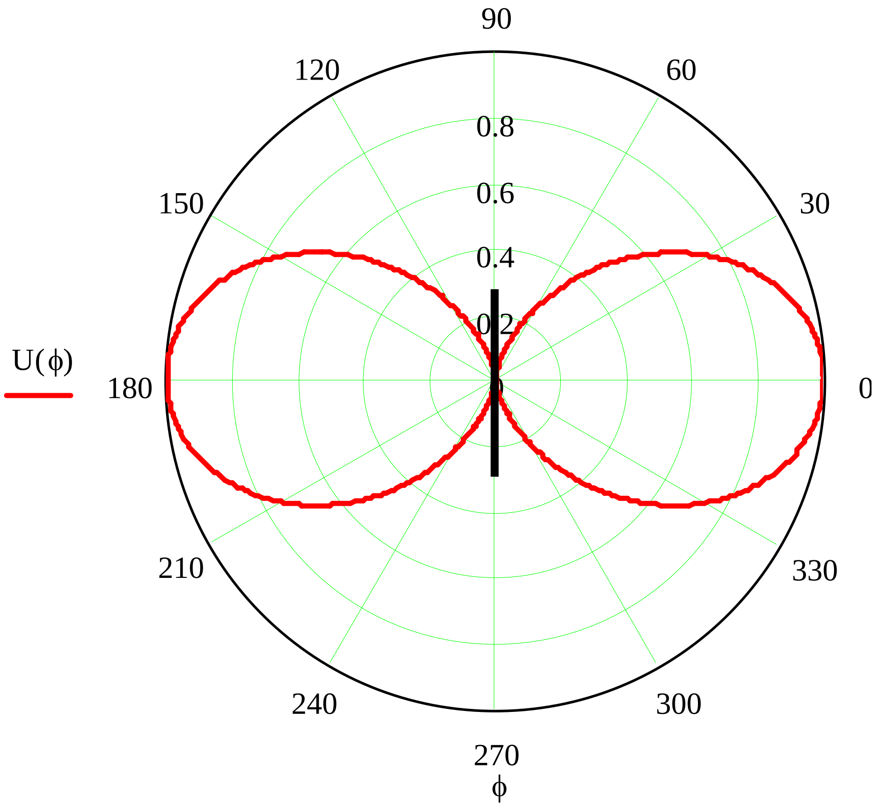
$$\overline{E}(r,\theta,\phi)=\left[\hat{\theta}F_\theta(\theta,\phi)+\hat{\phi}F_\phi(\theta,\phi)\right]\frac{e^{-j\frac{2\pi r}{\lambda}}}{r}$$

$$H_\phi=\frac{E_\theta}{377\Omega}$$

$$H_\theta=\frac{-E_\phi}{377\Omega}$$

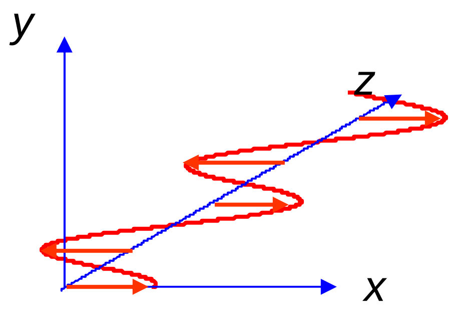
$$\overline{S}=\overline{E}\times\overline{H}^*$$

Radiation Pattern

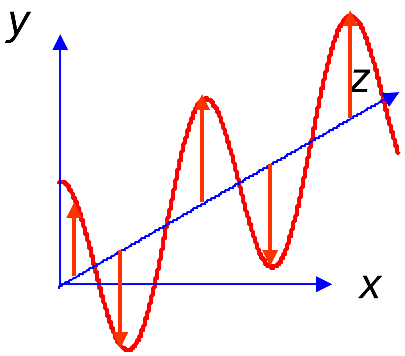


Polarization

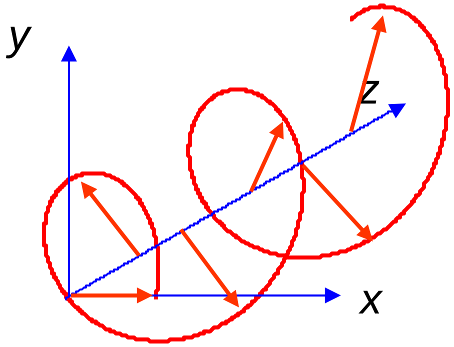
Horizontal



Vertical

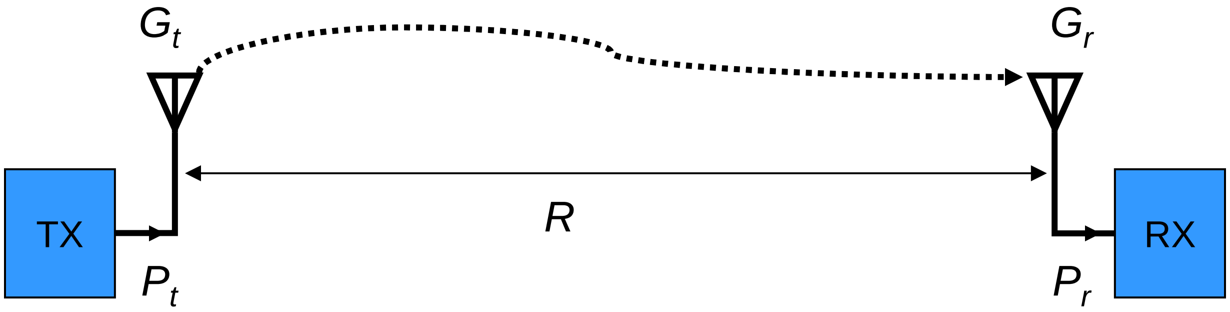


Circular
(Left-Hand)

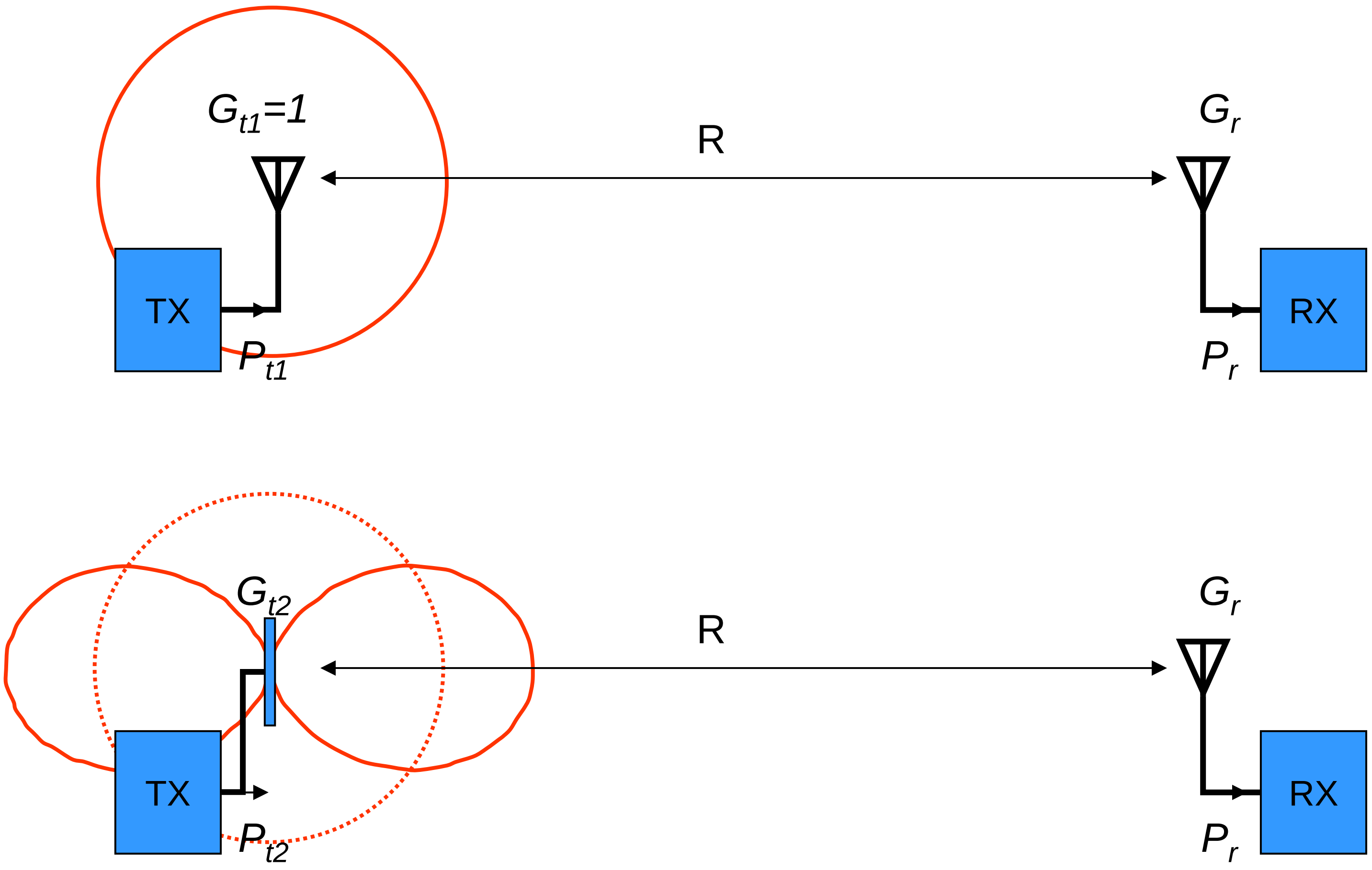


The Friis Equation

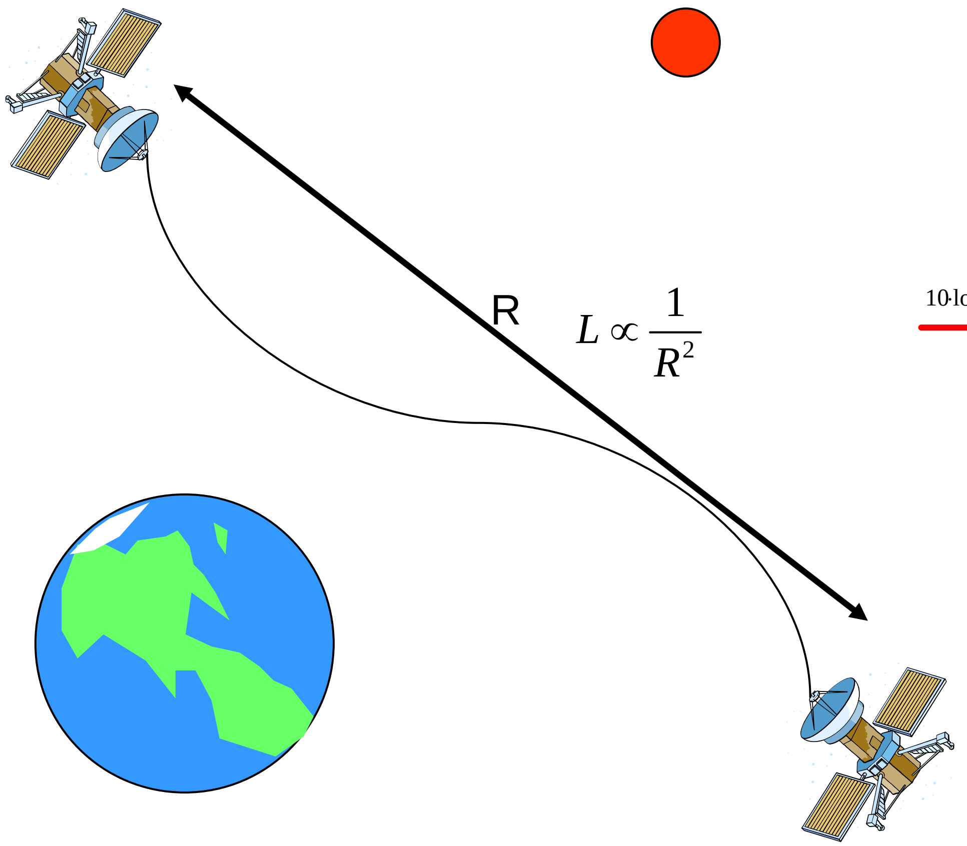
$$P_r = \frac{G_t G_r \lambda^2}{(4\pi R)^2} P_t$$



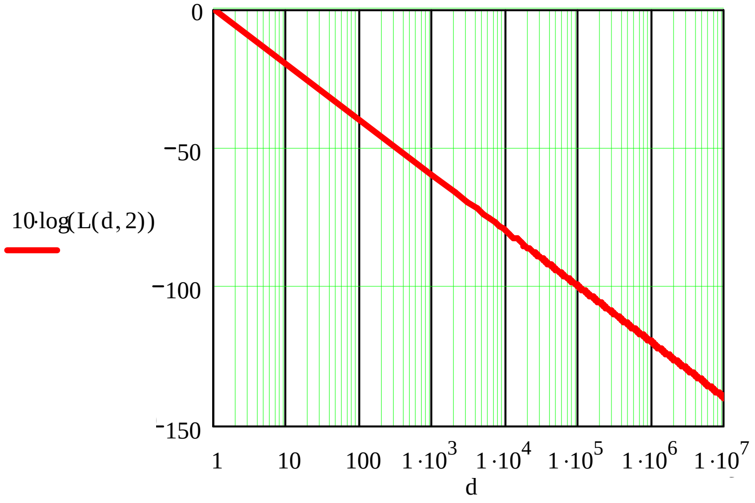
EIRP



Free Space Propagation



$$L \propto \frac{1}{R^2}$$

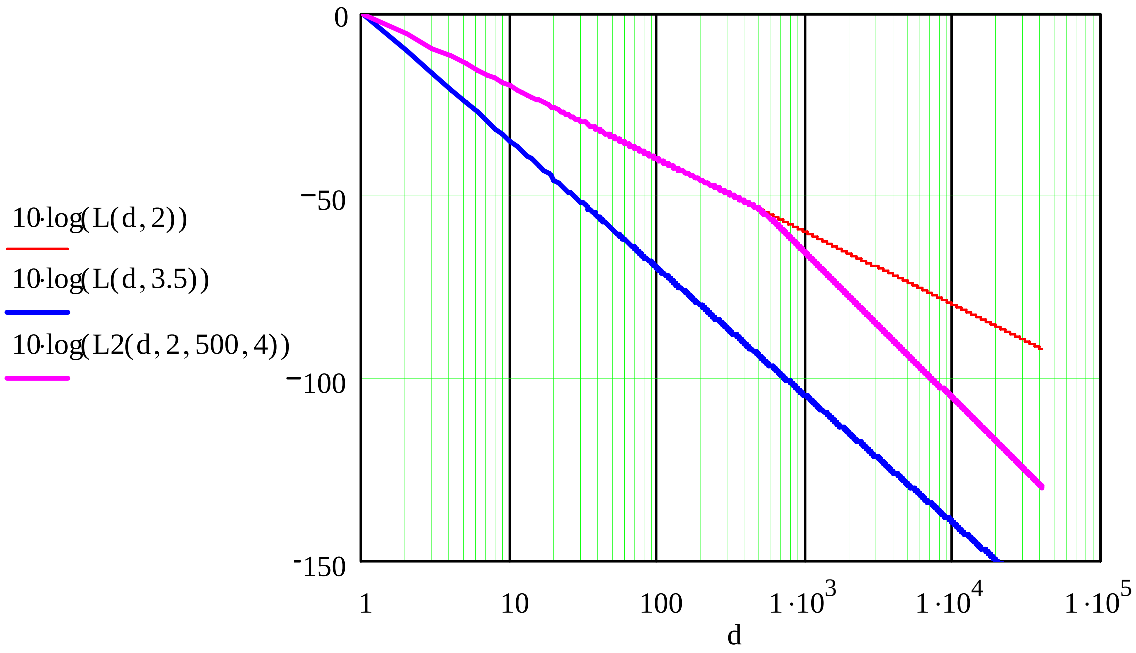


Realistic Path Loss

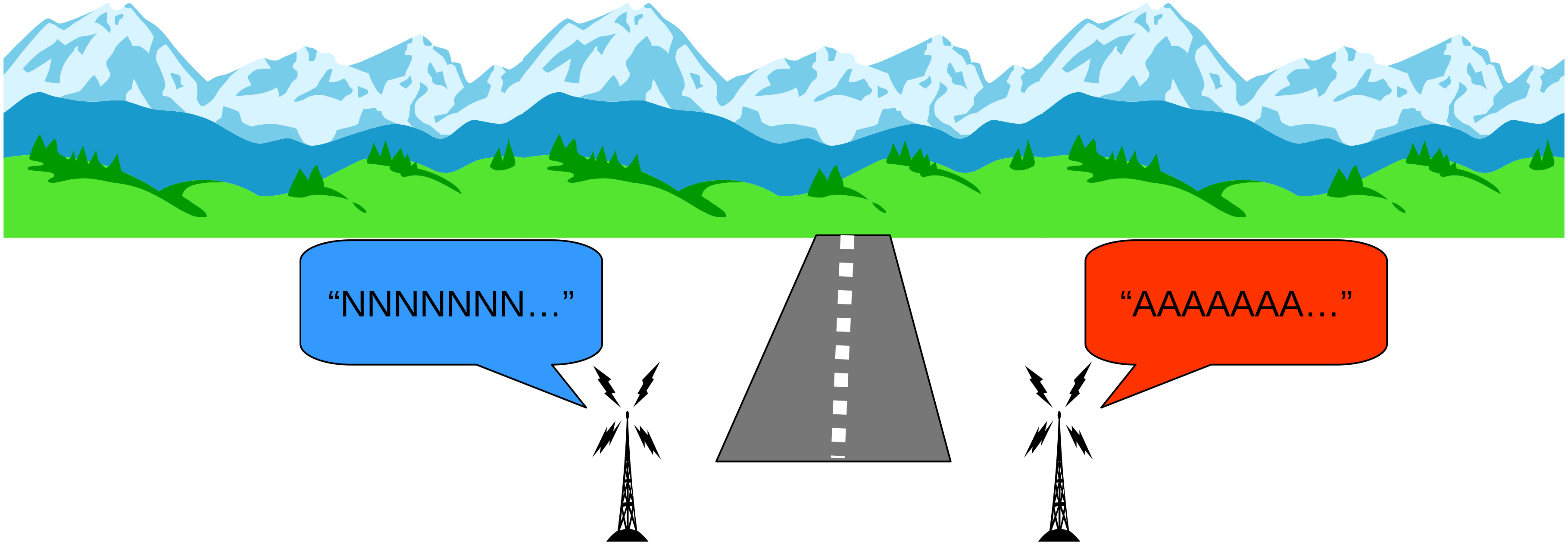
$$L \propto \frac{1}{R^n}$$

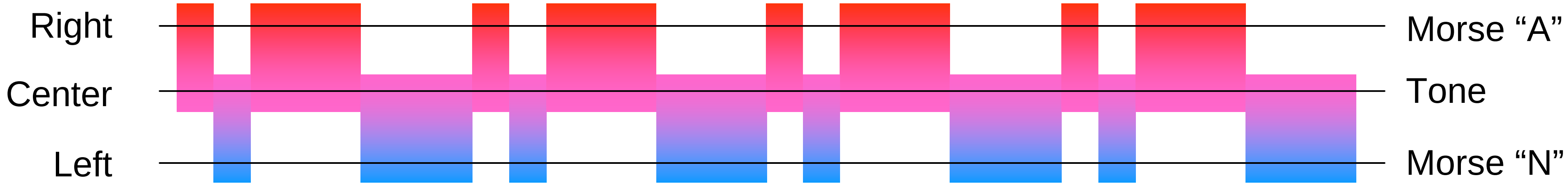
Environment	n
Free space	2
Urban	2.7-3.5
Shadowed urban	3-5

$$L \propto \begin{cases} \dfrac{1}{R^2} & R \le d \\ \dfrac{1}{R^4} & R > d \end{cases}$$



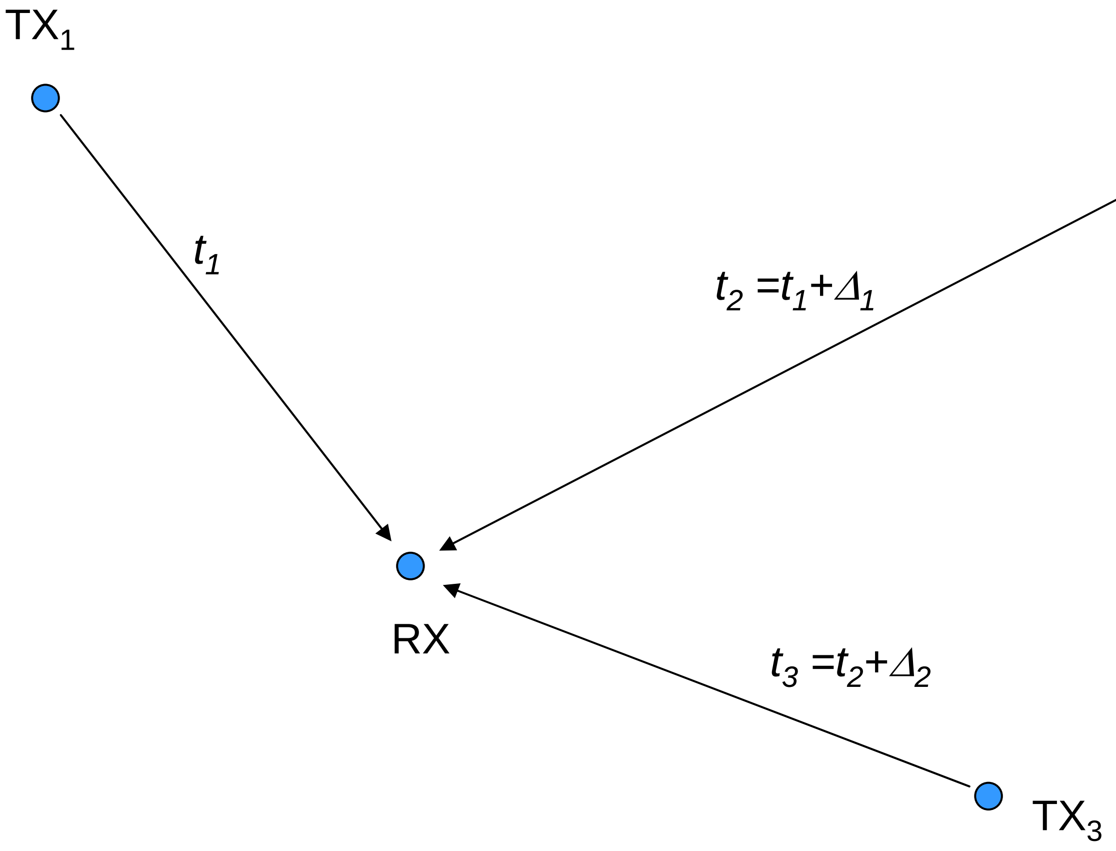
The Earliest Radio-location services



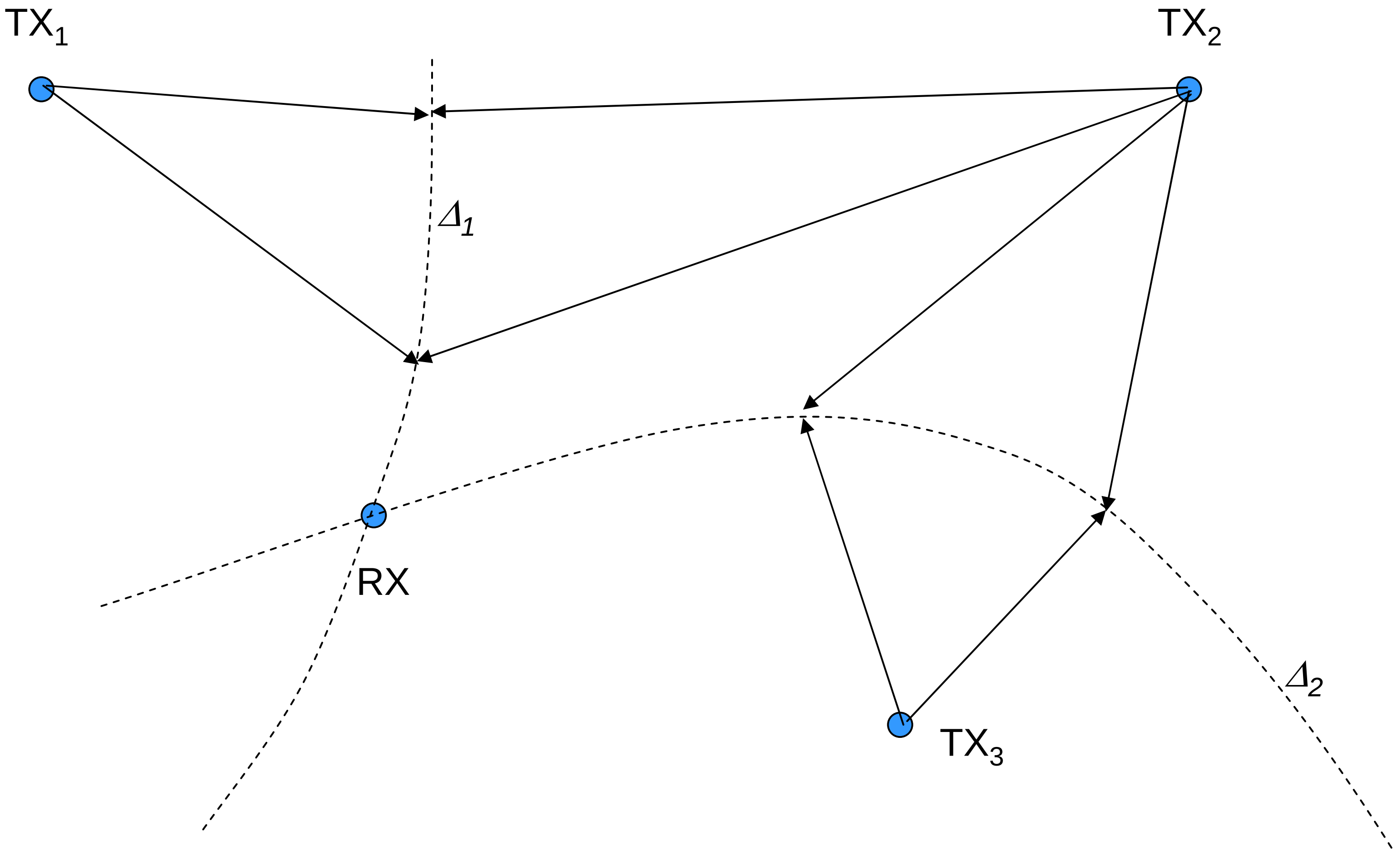


Note: Right and left may be reversed!

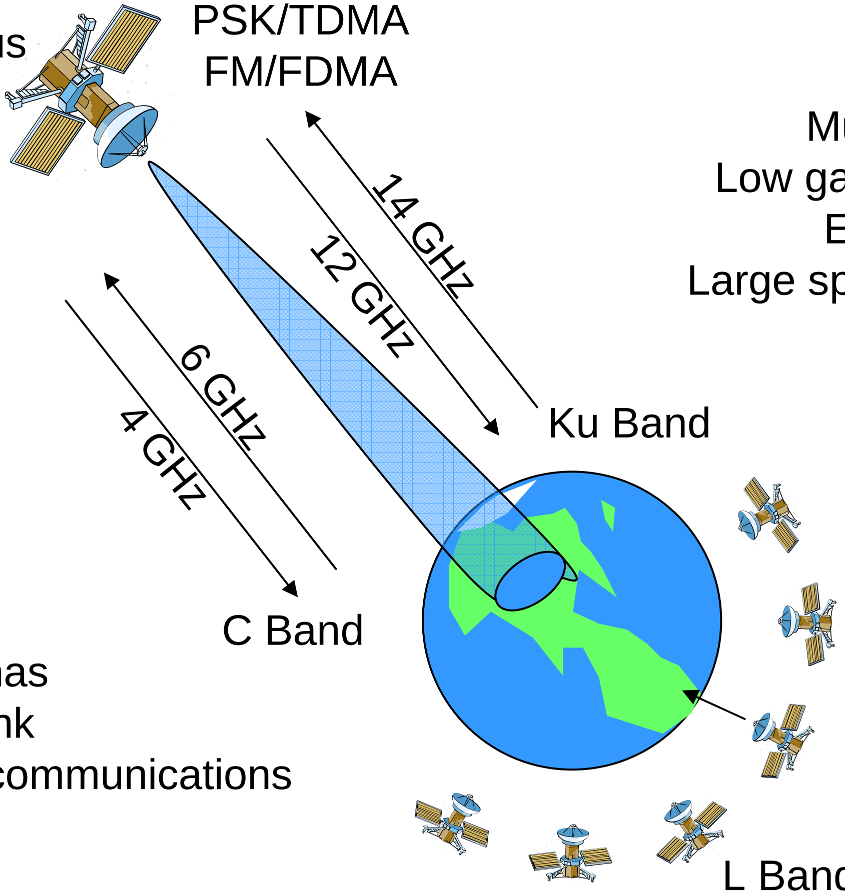
Geolocation Services



Geolocation Services



Representative Wireless Communications Systems
Satellite



GEO-Geosynchronous
orbit: 24000 mi

PSK/TDMA
FM/FDMA

Broadcast TV,
Long distance
communications

14 GHz

12 GHz

Ku Band

6 GHz

4 GHz

C Band

Multiple satellites
Low gain receive antennas
Encrypted links
Large spreading factor for A/J

LEO-Low Earth
orbit: 200-1000 mi

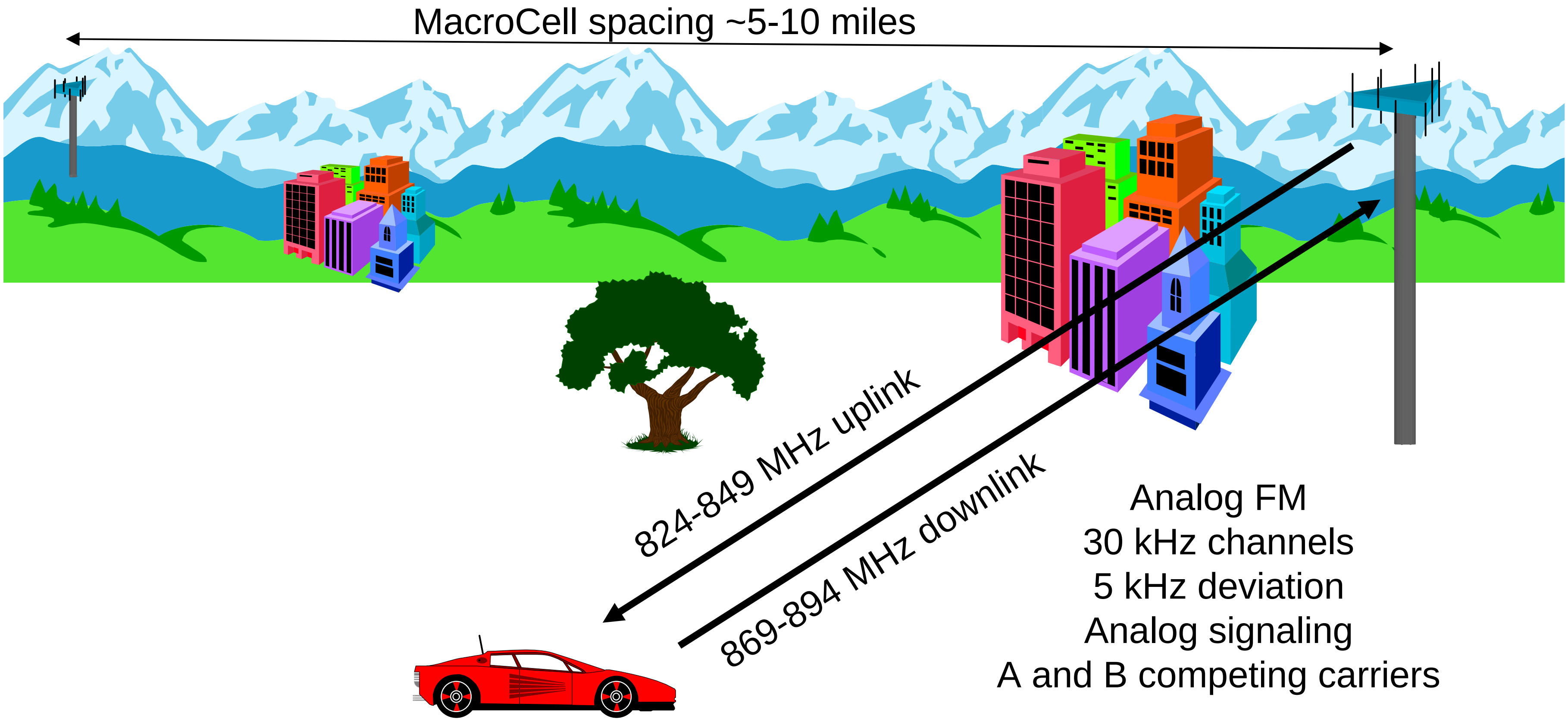
PSK
Spread-spectrum

GPS
Geolocation

High path loss
High gain antennas
High power uplink
Open or minimally protected communications

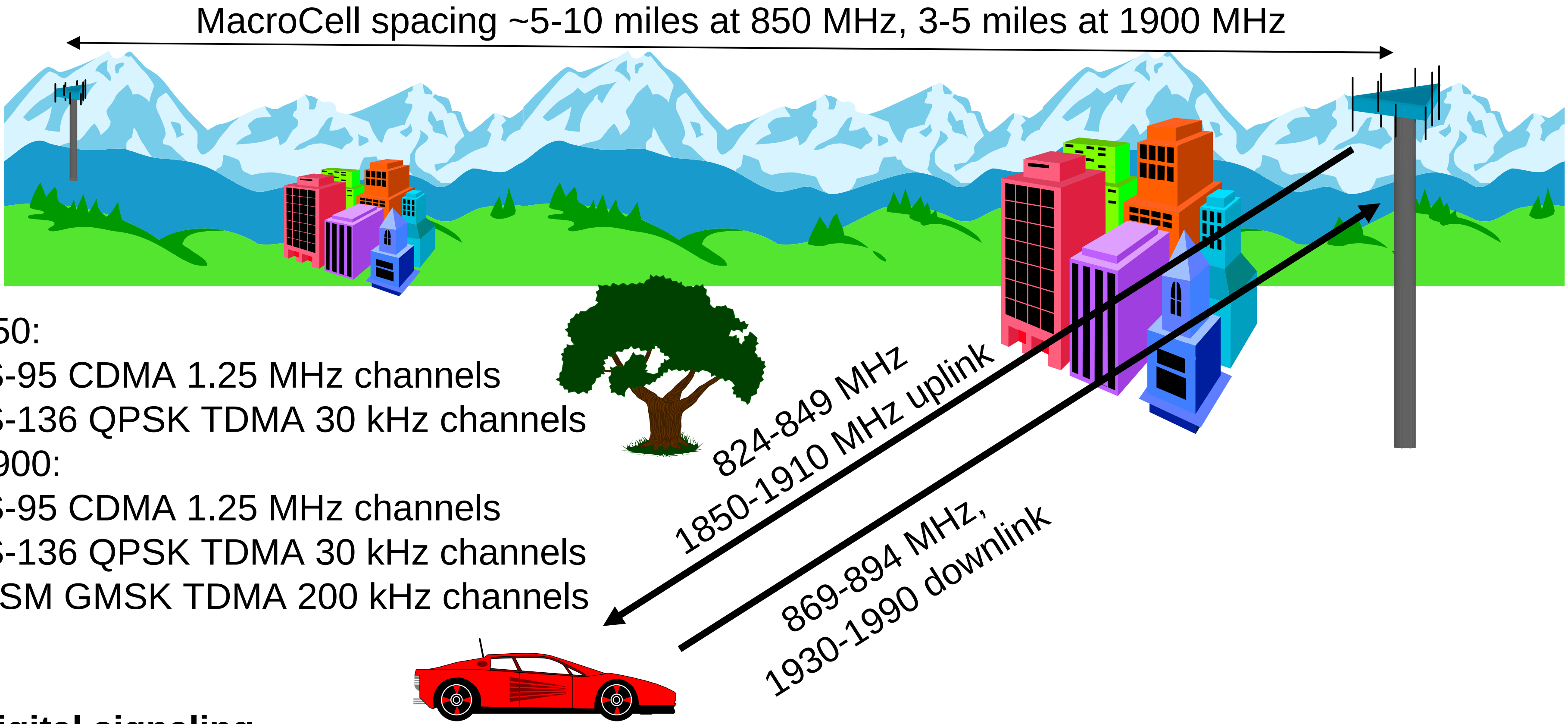
L Band
1.228, 1.575 GHz

Representative Wireless Communications Systems
AMPS Cellular



Analog FM
30 kHz channels
5 kHz deviation
Analog signaling
A and B competing carriers

Representative Wireless Communications Systems
2-G PCS



MacroCell spacing ~5-10 miles at 850 MHz, 3-5 miles at 1900 MHz

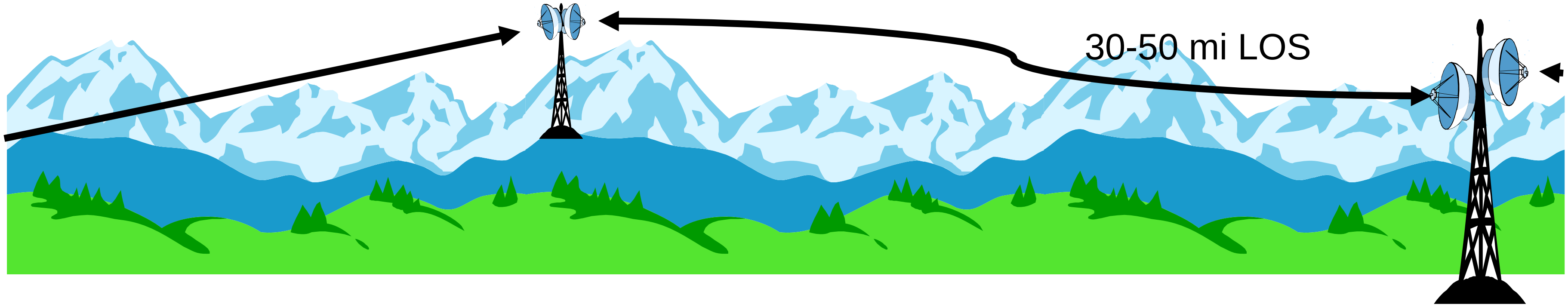
824-849 MHz
1850-1910 MHz uplink

869-894 MHz,
1930-1990 downlink

850:
IS-95 CDMA 1.25 MHz channels
IS-136 QPSK TDMA 30 kHz channels
1900:
IS-95 CDMA 1.25 MHz channels
IS-136 QPSK TDMA 30 kHz channels
GSM GMSK TDMA 200 kHz channels

Digital signaling
A and B competing carriers on 850 MHz
A,B,C,D,E,F competing carriers on 1900 MHz

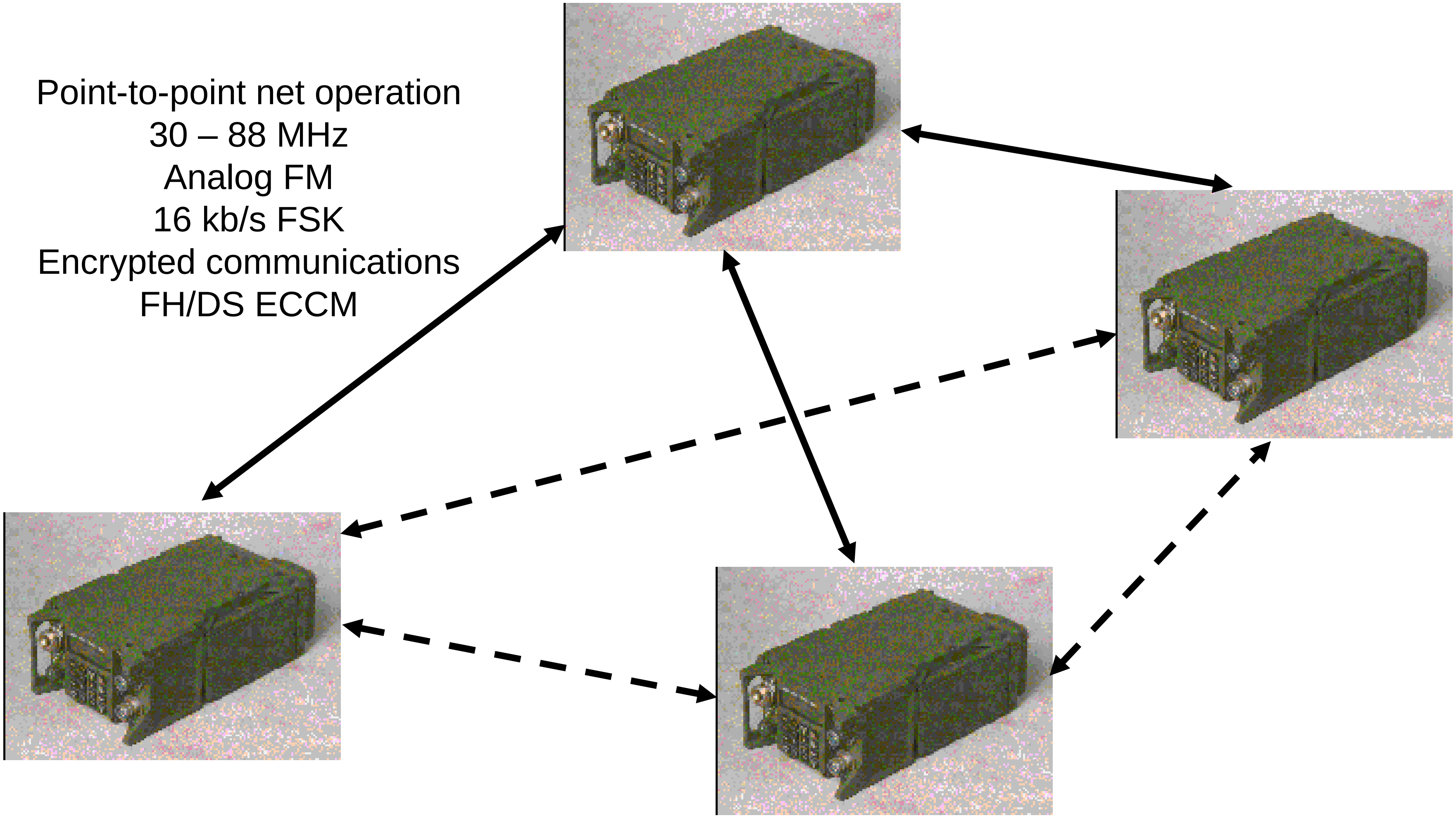
Representative Wireless Communications Systems
Terrestrial Microwave



4-20+ GHz
Analog SSB FDMA
Digital QPSK, 16QAM, 64QAM TDM: DS1-DS3
Multichannel Voice, Data traffic
Generally not encrypted

Representative Wireless Communications Systems
Tactical Military

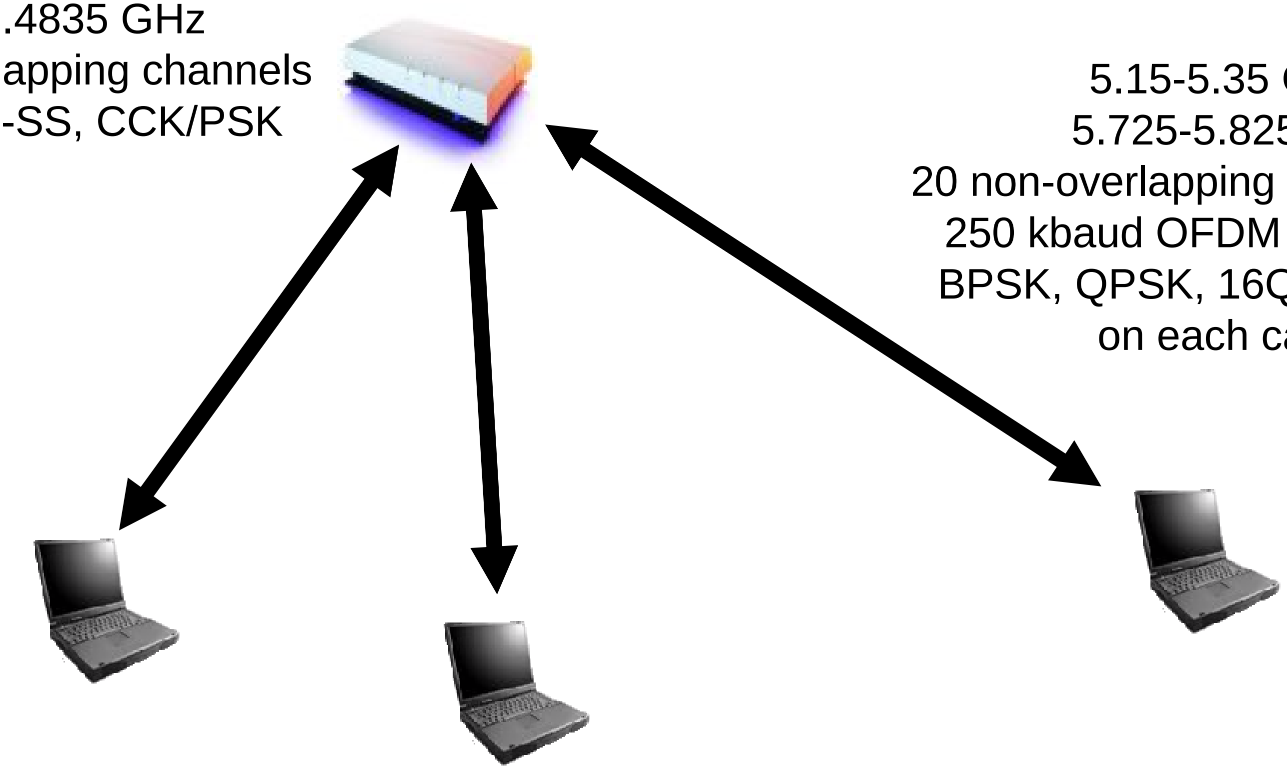
Point-to-point net operation
30 – 88 MHz
Analog FM
16 kb/s FSK
Encrypted communications
FH/DS ECCM



Representative Wireless Communications Systems
802.11 WLAN

802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK



802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
20 non-overlapping TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier