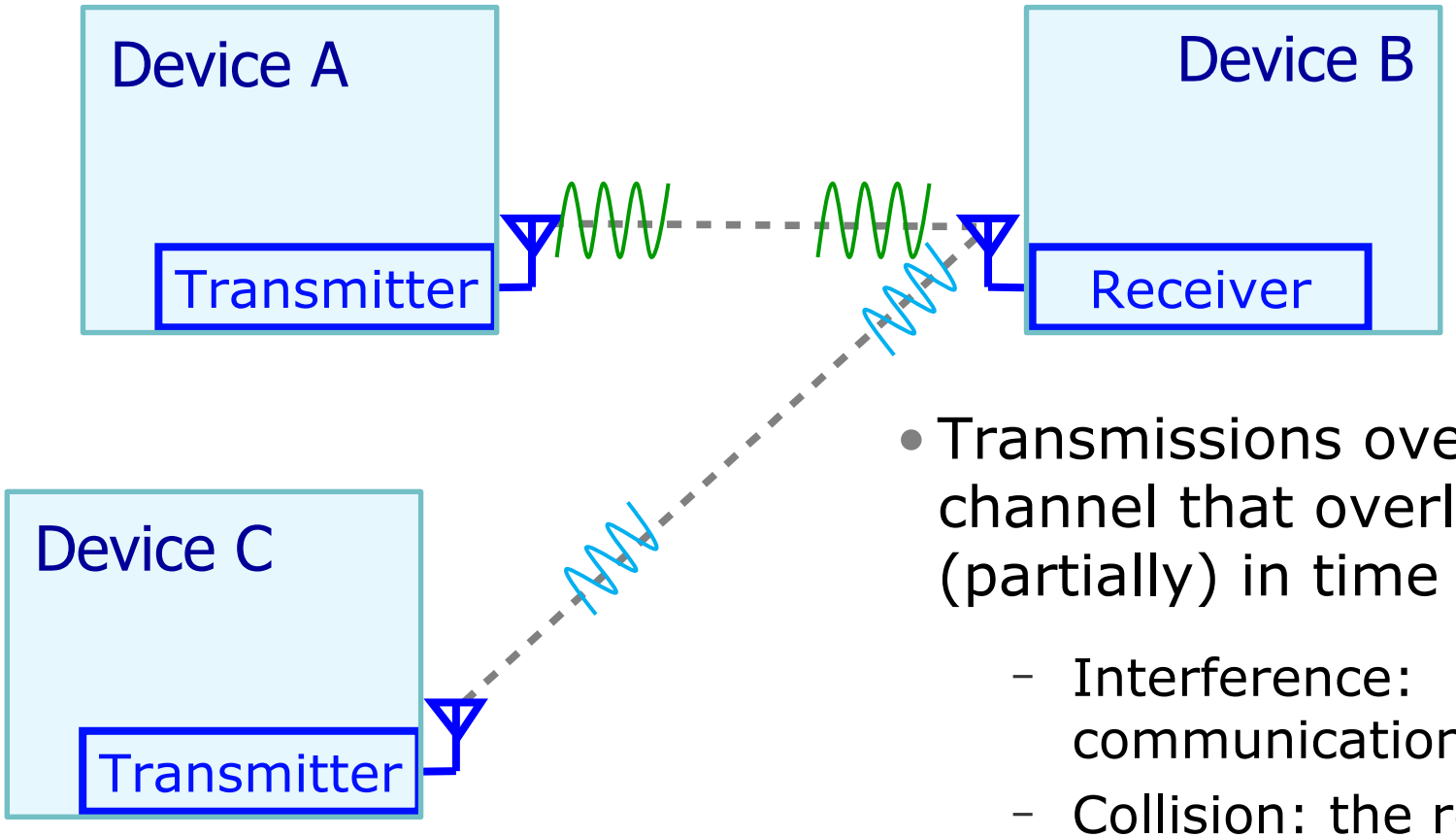
ROYAL INSTITUTE
OF TECHNOLOGY

Networked System Security

Jamming and physical layer attacks

Panos Papadimitatos
Networked Systems Security Group
www.ee.kth.se/nss

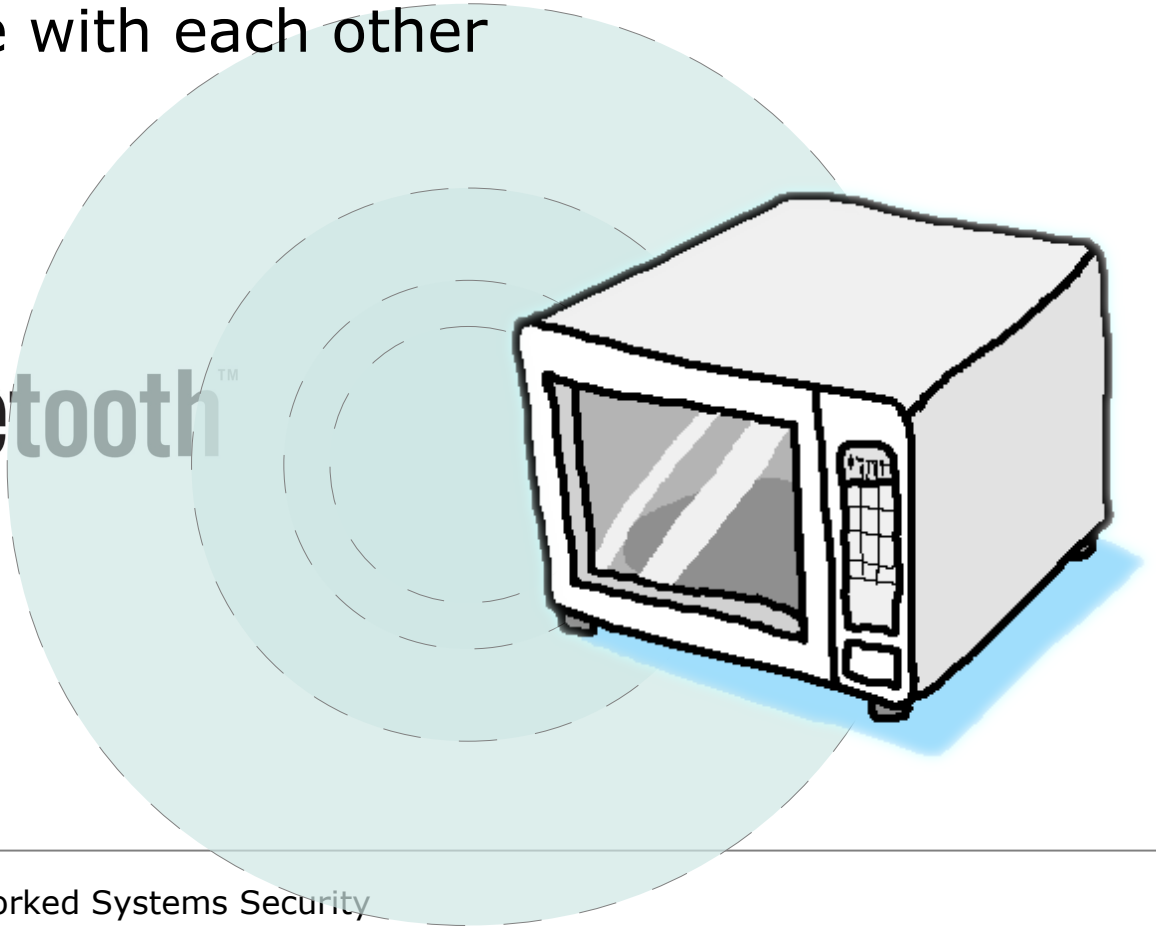
Wireless Communication (WCOM)



- Transmissions over the same channel that overlap (partially) in time
  - Interference: communication degradation
  - Collision: the receiver cannot successfully decode any signal

Unintentional jamming or Interference

- Finite usable frequency spectrum
- Wireless networks, Bluetooth, and microwave ovens are close enough to interfere with each other



ROYAL INSTITUTE OF TECHNOLOGY

Frequency spectrum

Band name	Frequency	Example uses
LF, Low frequency	30–300 kHz	Navigation, time signals, AM longwave broadcasting, RFID, amateur radio
MF, Medium frequency	300–3000 kHz	AM mediumwave broadcasts, amateur radio, avalanche beacons
HF, High frequency	3–30 MHz	Shortwave broadcasts, citizens' band radio, amateur radio and over-the-horizon aviation
VHF, Very high frequency	30–300 MHz	FM, television broadcasts and line-of-sight aircraft communications. Land Mobile and Maritime Mobile communications, amateur radio, weather radio
UHF, Ultra high frequency	300–3000 MHz	Television broadcasts, microwave ovens, microwave devices/communications, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS, FRS and GMRS radios, amateur radio

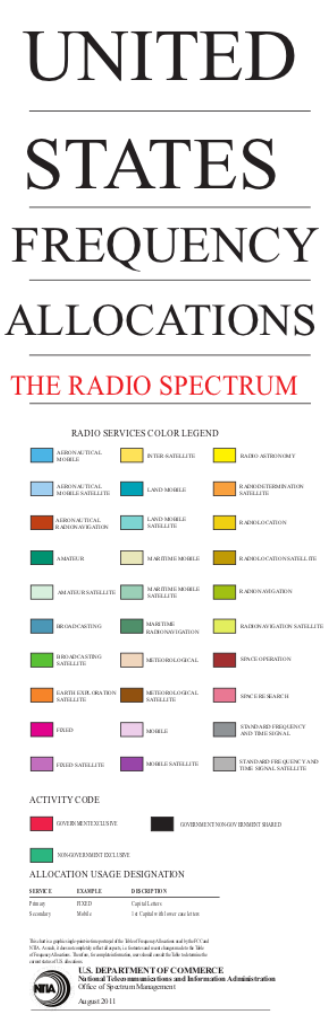
src: Wikipedia, Radio spectrum

ROYAL INSTITUTE OF TECHNOLOGY

Frequency spectrum (cont'd)

- Frequency bands reserved for a particular use
  - Government
  - Specific technology
    - E.g., GSM and other cellular network bands
- Frequency bands are more or less free-to-use
  - Industrial, scientific and medical (ISM) bands, e.g., 2.45 GHz
  - Wi-Fi and other popular technologies operate in the ISM band
    - Built to resist interference
- Differences between regions and countries

Frequency spectrum (cont'd)



Wireless networks we deal with

src: United States Department of Commerce

ROYAL INSTITUTE OF TECHNOLOGY

Error Control Coding (ECC)

- Introduce redundancy to handle errors
  - Use more data to say the same thing
- Mitigate interference or partial jamming
- Many types; for example:
  - Repetition codes
  - Parity
  - Cyclic redundancy check (CRC)
  - Forward error correction, e.g.,
    - Hamming
    - Erasure code

ECC: Parity bit

- Can detect one bit error
- Count number of ones
  - Even or odd parity
  - Make the entire number of bits even (with the parity bit)
  - E.g., even parity:
    - Set the parity bit to “1” if # of 1's is odd, to “0” if even
- Example:
  - Want to send A, 1000001
  - Even number of ones, 0 parity bit
  - Send 1000001**0**
  - Receive E, 1000101**0**
  - Odd number ones, so there was an error

ECC: Cyclic Redundancy Check

Cyclic redundancy check (CRC)

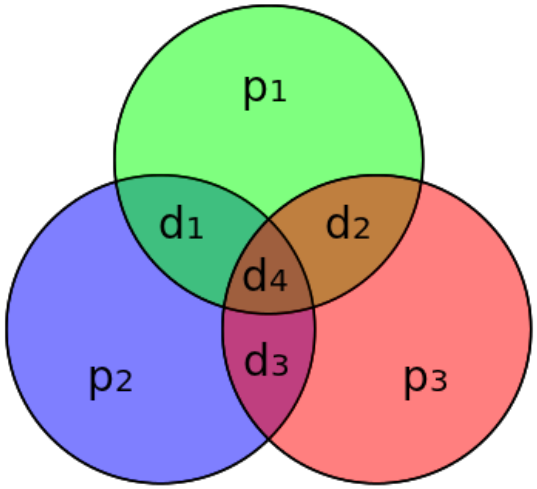
- Uses polynomial division to detect errors
  - m(x) x^n = q(x) g(x) + r(x)
  - Message m(x)
  - Generator polynomial g(x) of degree n
  - Reminder r(x) is the CRC value
- Easy to implement in hardware
- Parity check is a CRC with g(x) = x + 1

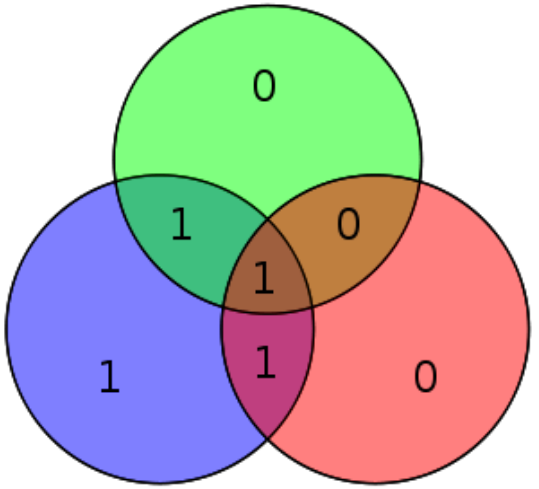
ROYAL INSTITUTE OF TECHNOLOGY

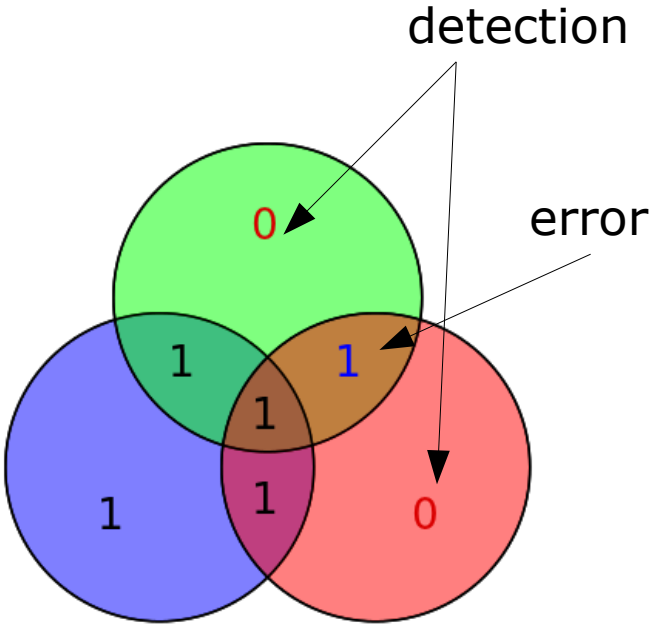
ECC: Hamming codes

- Example is the Hamming(7,4)
- Encodes 4 bits of data to 7 bits code words
- Can detect up to two bit errors, and correct one
- Can be seen as a constellation of parity bits

ECC: Hamming(7,4)







- Four data bits
  - d1, d2, d3, d4
- Three parity bits
  - p1, p2, p3

- Sent Message

- Error introduced
- Two parity checks fail
- This error can be corrected

src: Wikipedia, Hamming(7,4)

ROYAL INSTITUTE OF TECHNOLOGY

ECC: Erasure codes

- Erasure codes have rate r=k/n
  - Data length k
  - Code word length n
- Can recover data from a number of errors and/or erasures
- Reed-Solomon
  - Can correct up to (n-k)/2 errors and/or erasures
  - Used in CD, DVD, BluRay, QR codes ...

Jamming

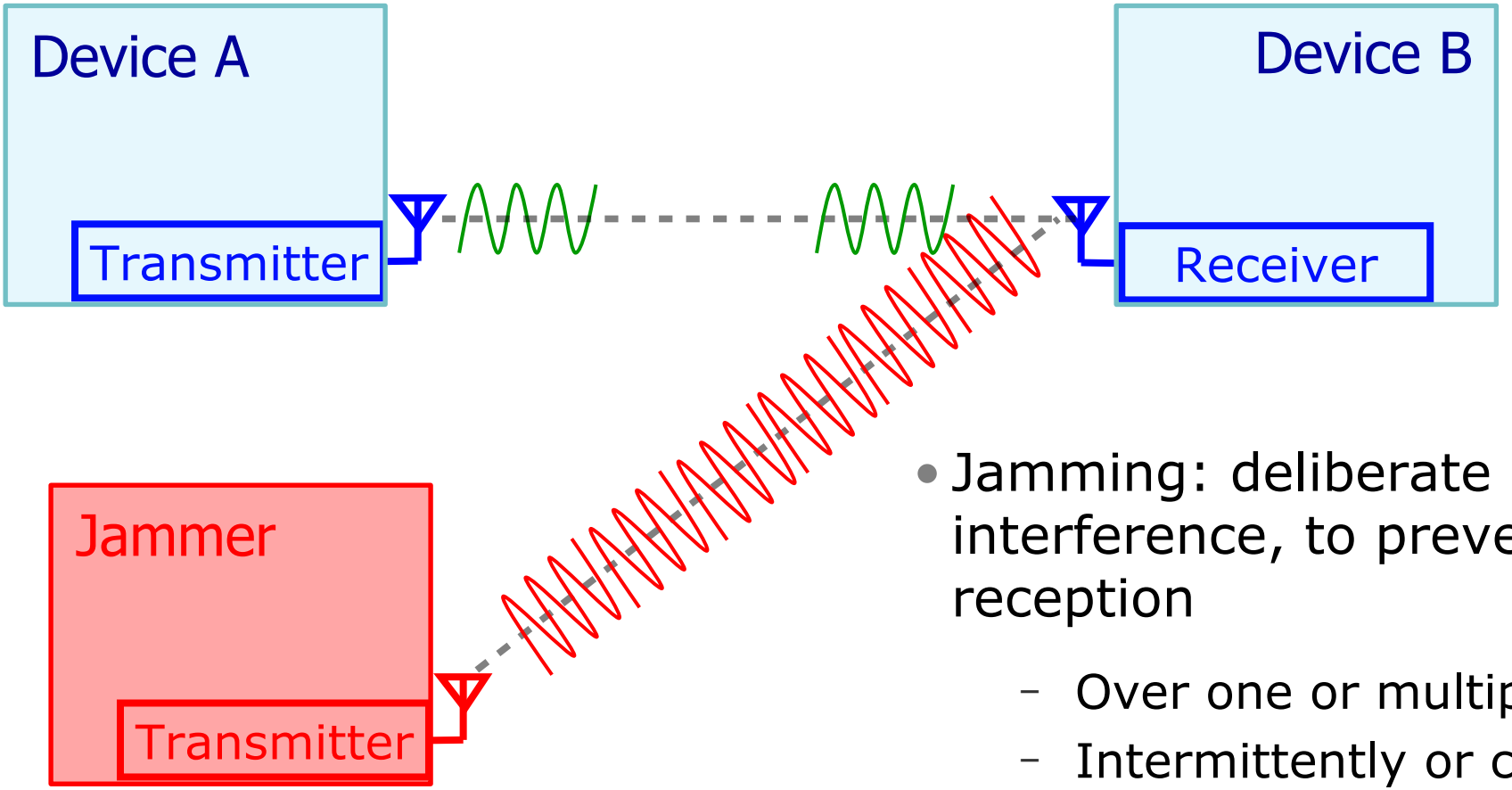
- Disrupting communication
- Concern mostly for wireless networks
- Long-known problem
- Deliberate interference

src: Spaceballs

Jamming (cont'd)

- Numerous commercially available devices (jammers)
  - Against WiFi, GSM, PCS, GPS, Bluetooth
- Applications in law enforcement, anti-terrorism, military operations

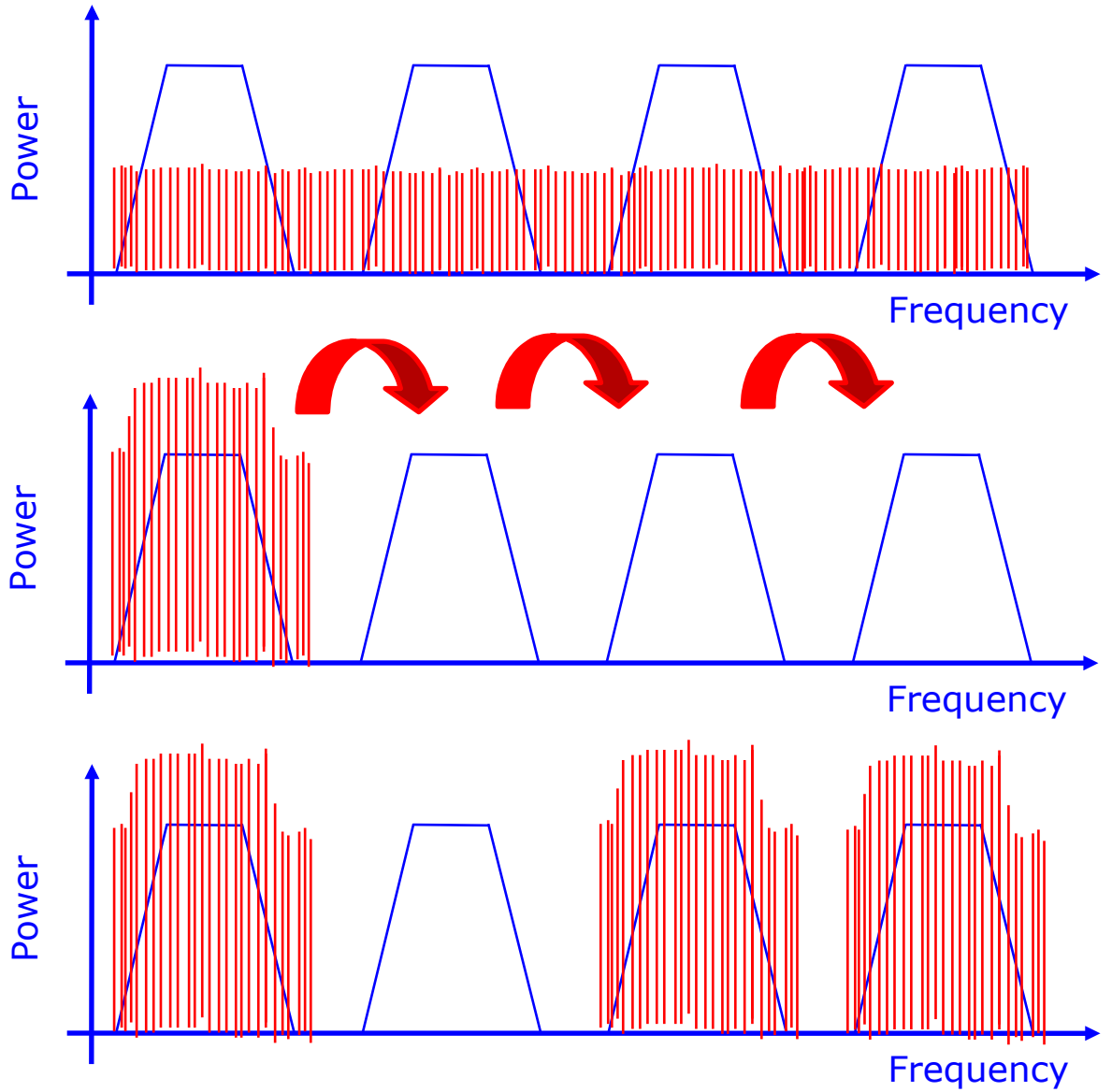
Jamming (cont'd)



- Jamming: deliberate interference, to prevent signal reception
  - Over one or multiple channels
  - Intermittently or continuously
  - Varying transmission power
  - Violation of regulations

Different types of jamming

- Barrage jamming
- Swept-spot jamming
- Multi-spot jamming



Anti-jamming actions

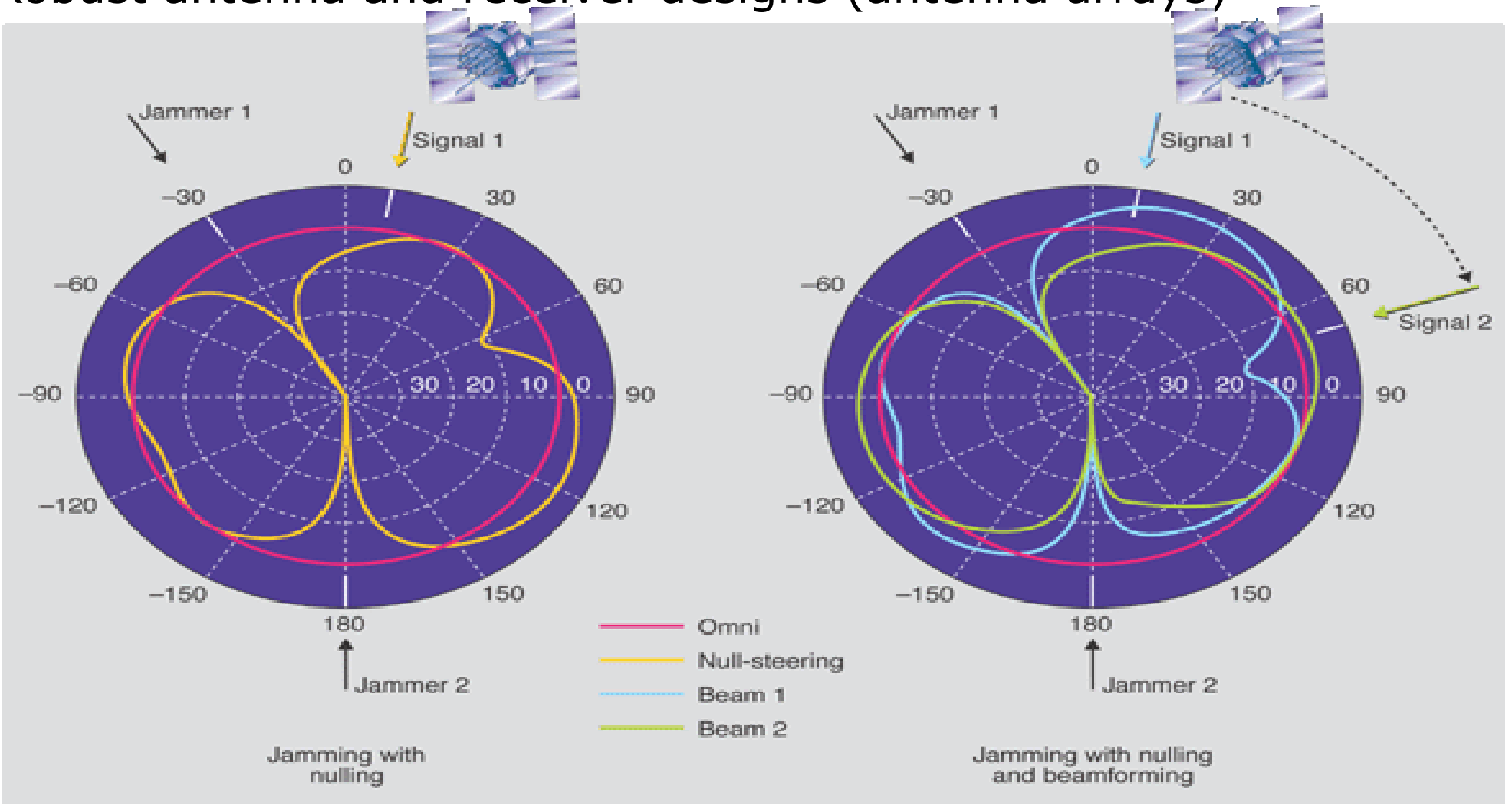
- Handle interference
  - Correct errors, e.g., error correcting codes (at a higher layer)
  - Different frequency and modulation techniques
  - Increase transmission power
- Effective against unintentional interference
- Effective against jamming up to a point
- Alternative: React to jamming
  - Avoid jammer
  - Localize and remove jammer

Anti-jamming actions (cont'd)

- Popular technologies operate with:
  - Multiple channels, e.g., IEEE 802.11a/b/g/n, IEEE 802.15.4
  - DSSS, FHSS, OFDM
- Resilience depends (primarily) on:
  - Pre-established knowledge
    - Channel hopping pattern
    - Spreading codes
  - Spread spectrum communication parameters
  - Jammer strength (jammer to signal ratio)

Robust Antennas

- Robust antenna and receiver designs (antenna arrays)



src:www.aero.org

ROYAL INSTITUTE OF TECHNOLOGY

Direct Sequence Spread Spectrum (DSSS)

- Modulate the signal x(t) with a wide-band pseudo-noise signal c(t)
  - x'(t) = x(t)c(t)
- DSSS makes signal detection harder
- DSSS creates a signal that more resembles white noise
- Is harder to jam the whole signal
- Used in e.g. 802.11b

DSSS (cont'd)

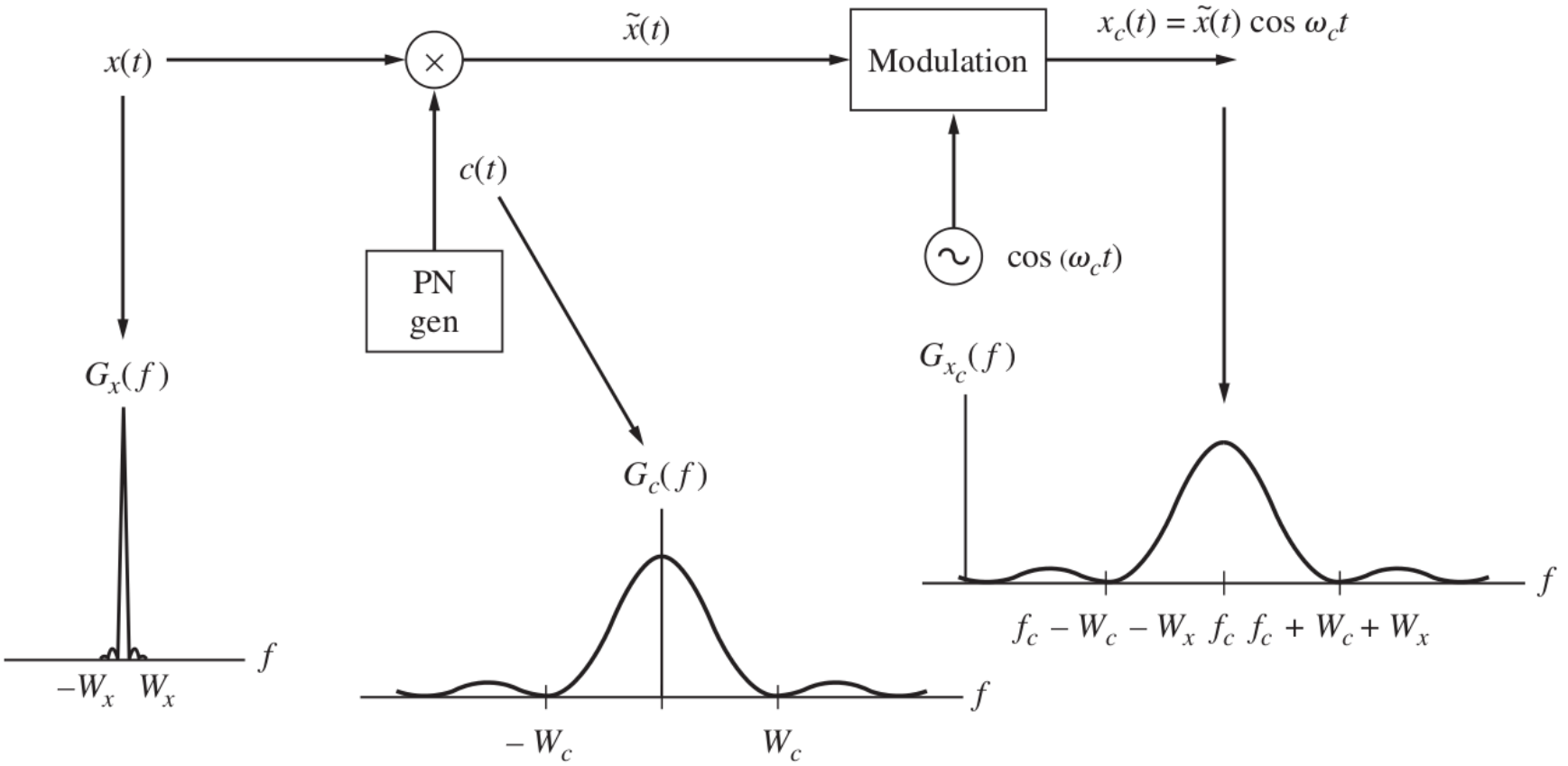
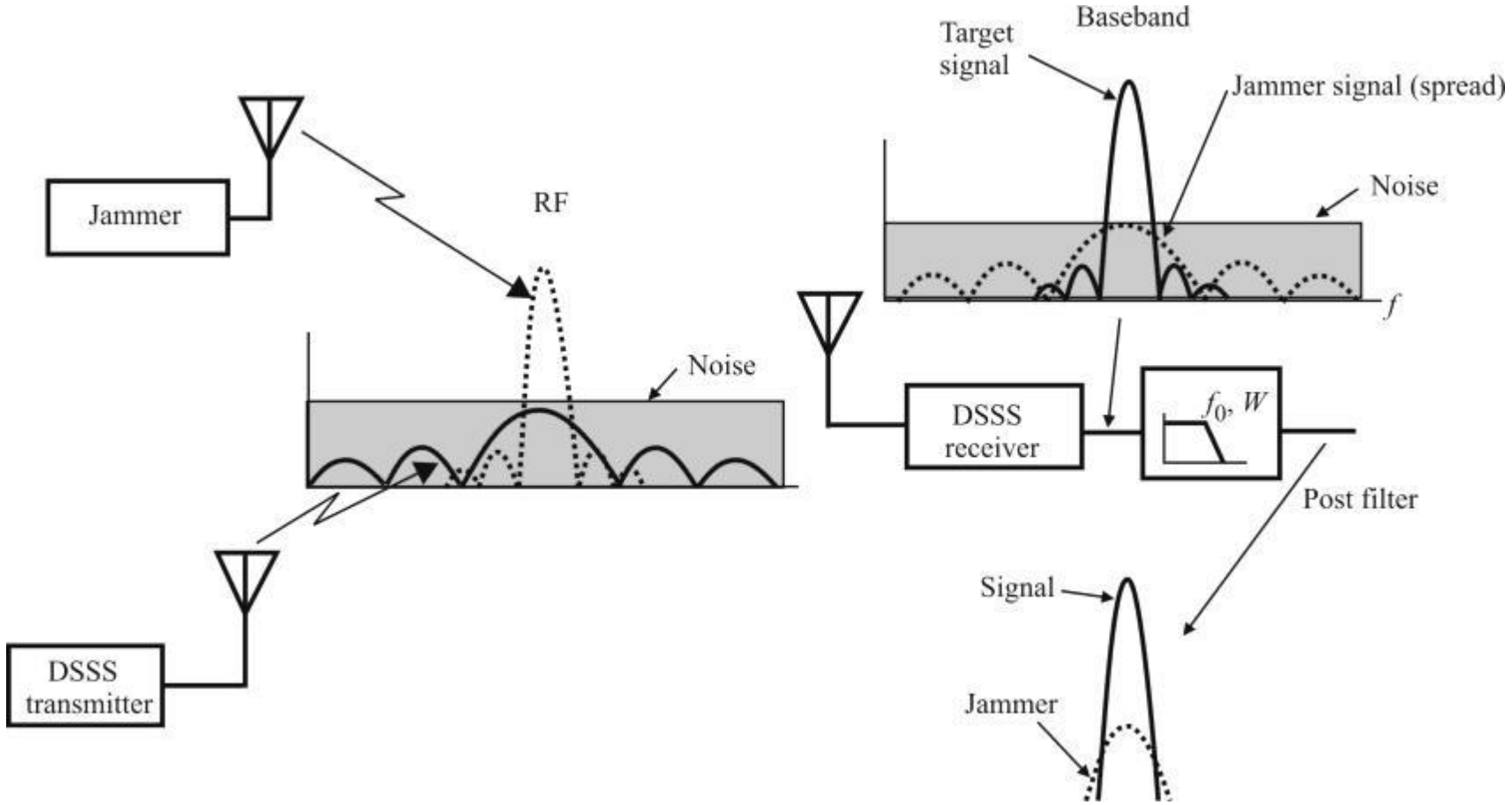


Figure 15.1–1 DSSS transmitter system and spectra.

src: Carlson, Communication Systems

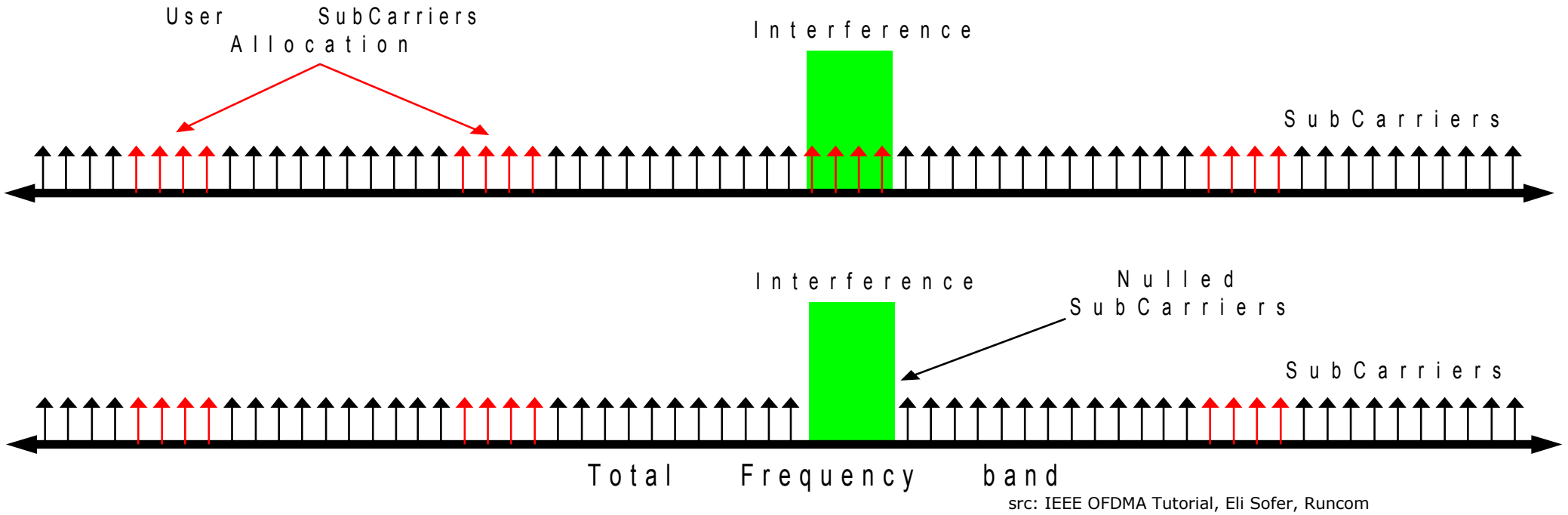
DSSS (cont'd)



src: Poisel, *Modern Communications Jamming Principles and Techniques*

Orthogonal Frequency-Division Multiplexing (OFDM)

- OFDM is a specialized FDM with orthogonal carrier signals
- Used, e.g., in 802.11g and 802.11n
- Easy interference rejection/avoidance



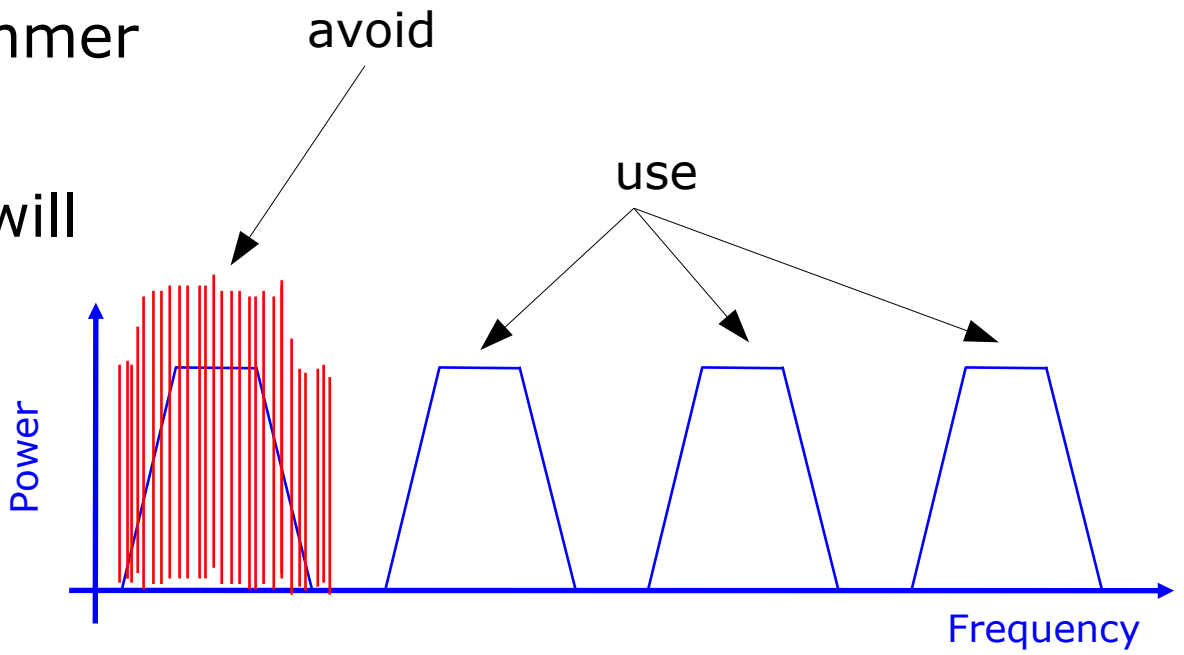
src: IEEE OFDMA Tutorial, Eli Sofer, Runcom

Anti-jamming actions (cont'd)

- We want to avoid the jammer
- System diversity
  - Multiple channels available
  - Use each channel for a period of time
  - Then, "jump" to another channel
  - Assumption: the jammer is constrained
    - n available channels
    - The jammer can prevent communication (jam) in up to t < n channels

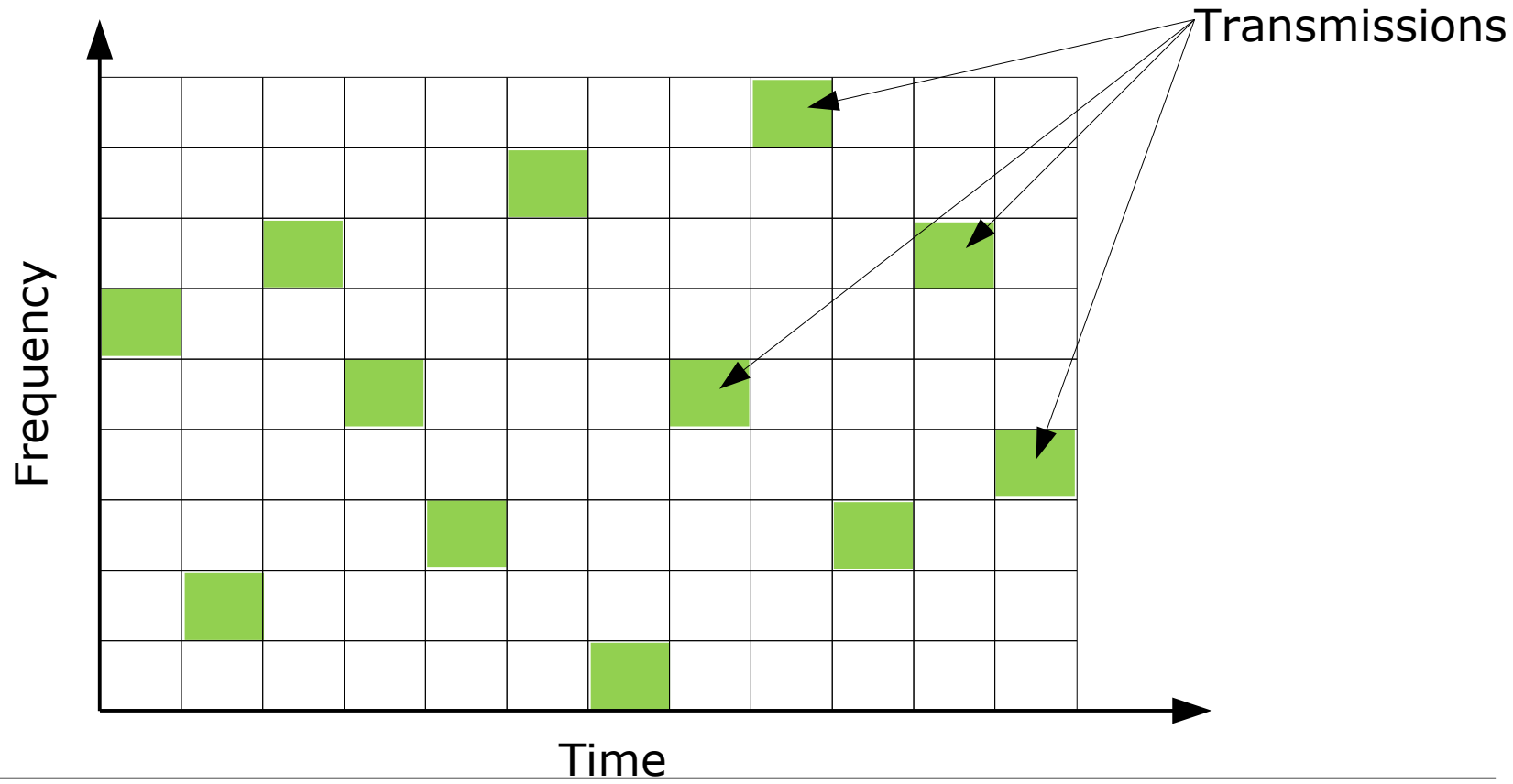
Anti-jamming actions (cont'd)

- We want to avoid the jammer
- Can we predict the frequencies the jammer will jam?
- Can the jammer predict the frequencies we will transmit on?



Frequency-hopping spread spectrum (FHSS)

- Transmit over a part of the available bandwidth for a short period of time
- Used in Bluetooth and is common in military radio.



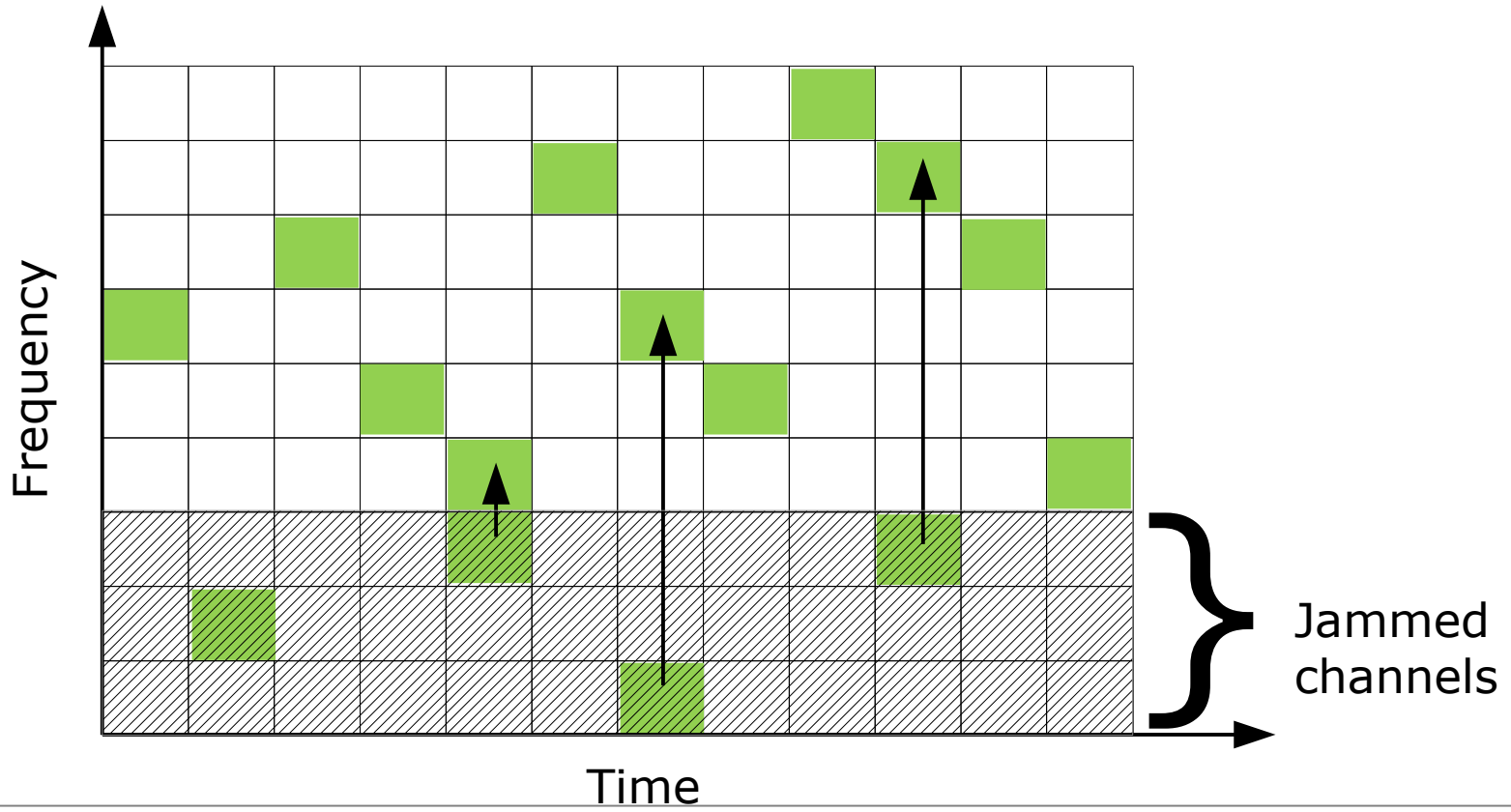
ROYAL INSTITUTE OF TECHNOLOGY

FHSS (cont'd)

- FHSS patterns should be hard to determine
  - Essentially a secret key
- Adaptive FHSS patterns
  - Choose appropriate channels

Bluetooth FHSS

- 79 communication channels
- Used as Adaptive Frequency Hopping (AFH)



ROYAL INSTITUTE OF TECHNOLOGY

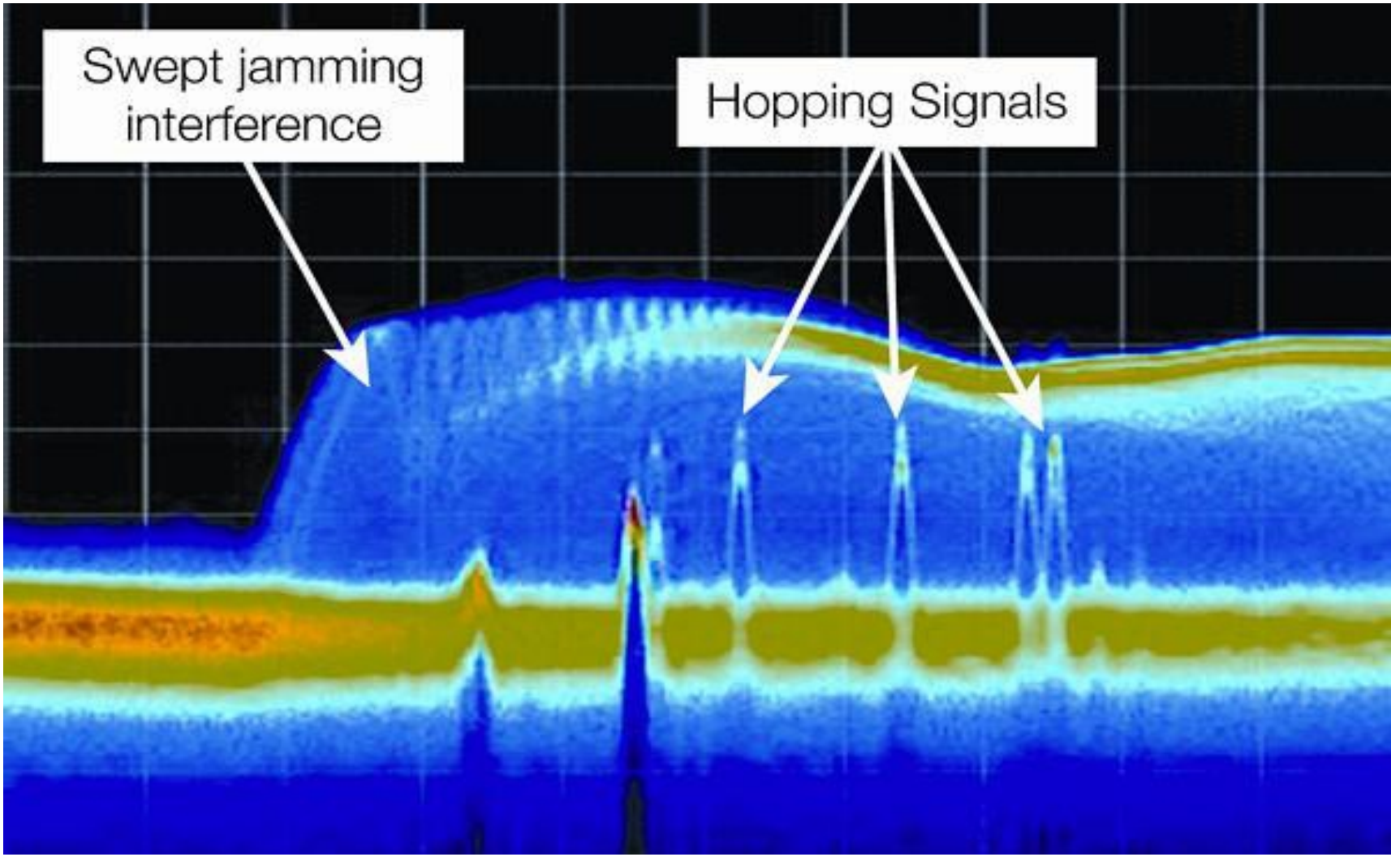
FHSS (cont'd)

- Bootstrapping without pre-shared information?
  - Uncoordinated Frequency Hopping
    - Random FHSS for both sender and receiver; the sender hops much faster than the receiver
    - Transmission of data fragments, from which the receiver has to reconstruct the message
    - Communication possible when both sender and receiver are simultaneously at the same channel

Jamming (cont'd)

- Bottom line: Jammer can overpower receivers
  - Technology known to adversary
  - Sufficiently high transmission power
  - Sufficient proximity to victims

Jamming (cont'd)



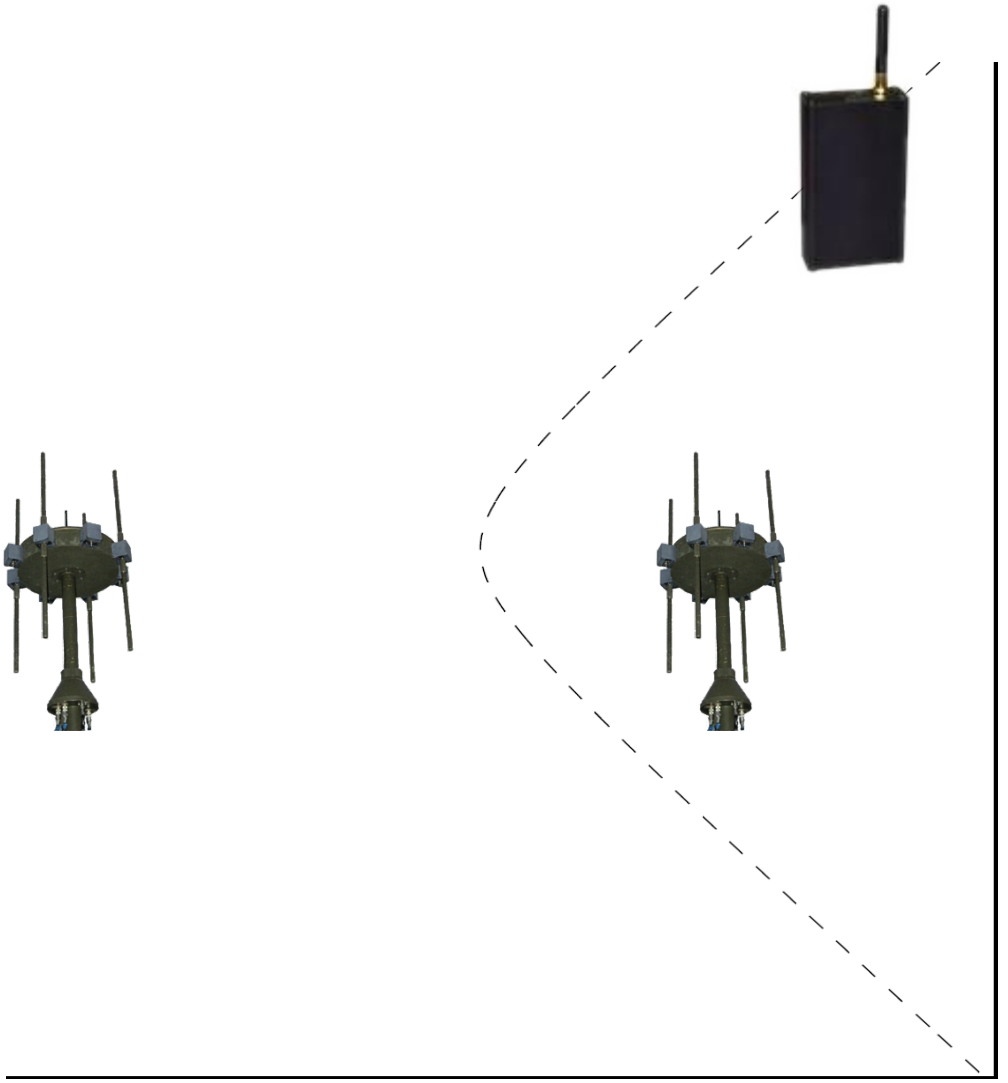
src: Graphic by Tektronix

Anti-jamming actions (cont'd)

- Jammer localization
- Detect the location and remove the jammer (physically)
  - Determine the jamming signal direction from multiple points, using either directional antennas or time/frequency difference of arrival.

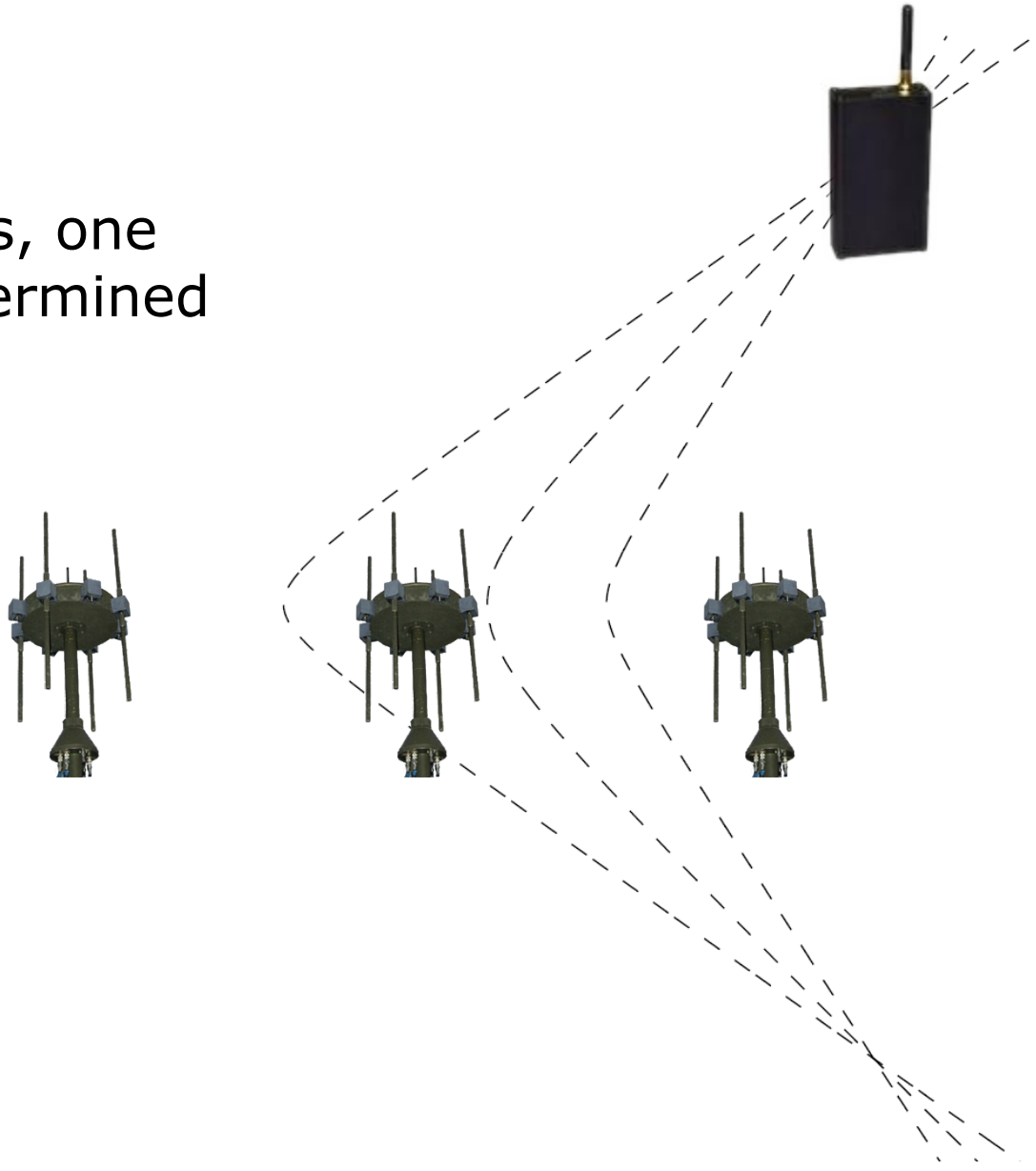
Jammer localization: TDOA

- TDOA: Time Difference of Arrival
- Two received signals
  - $x1(t) = s(t)$
  - $x2(t) = s(t + \Delta)$
- Can be cross-correlated to find a location hyperbola
  - $r(\tau) = E[x1(t)\, x2(t+\tau)]$



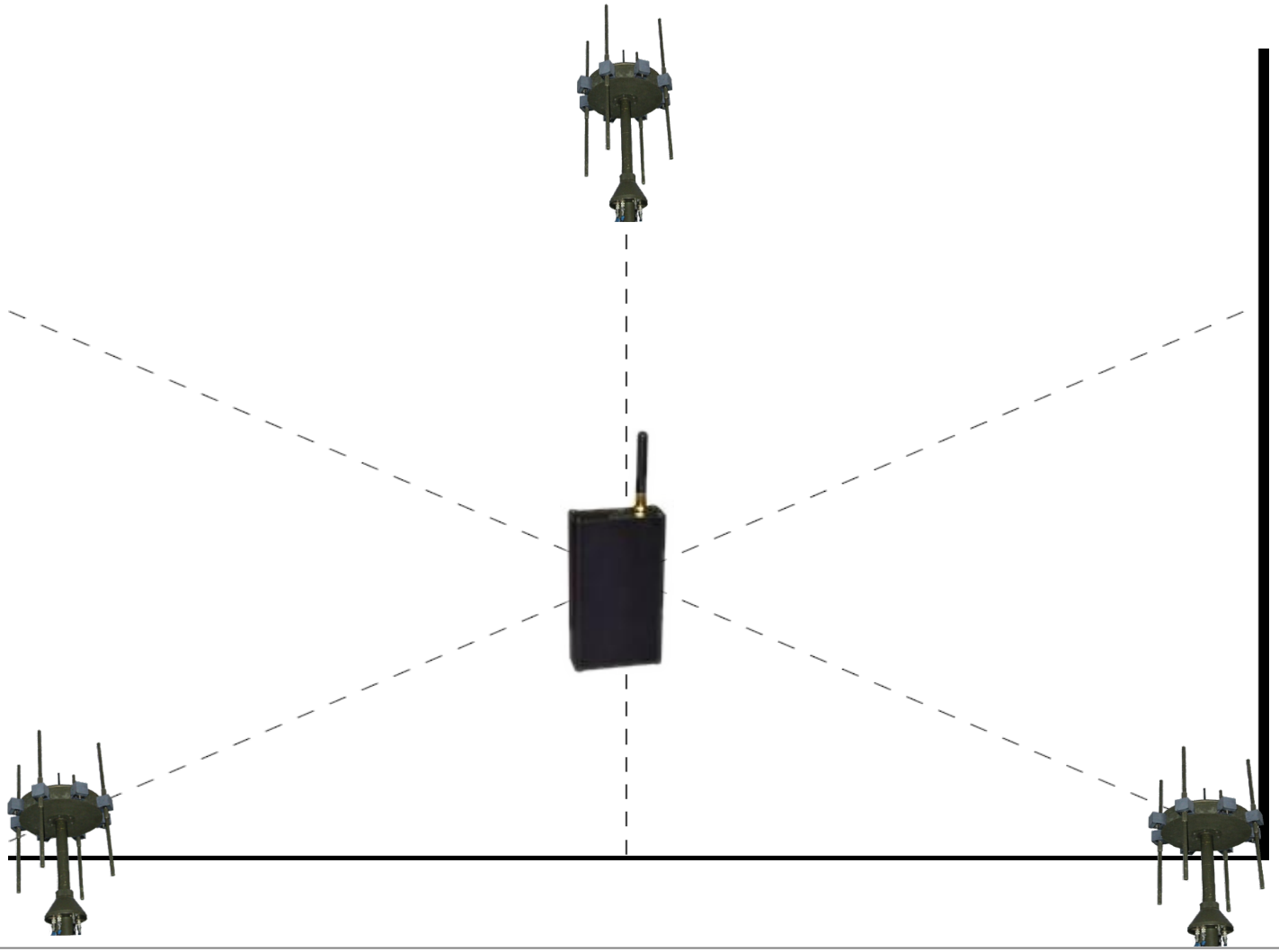
Jammer localization: TDOA (cont'd)

- With three receivers, one location can be determined

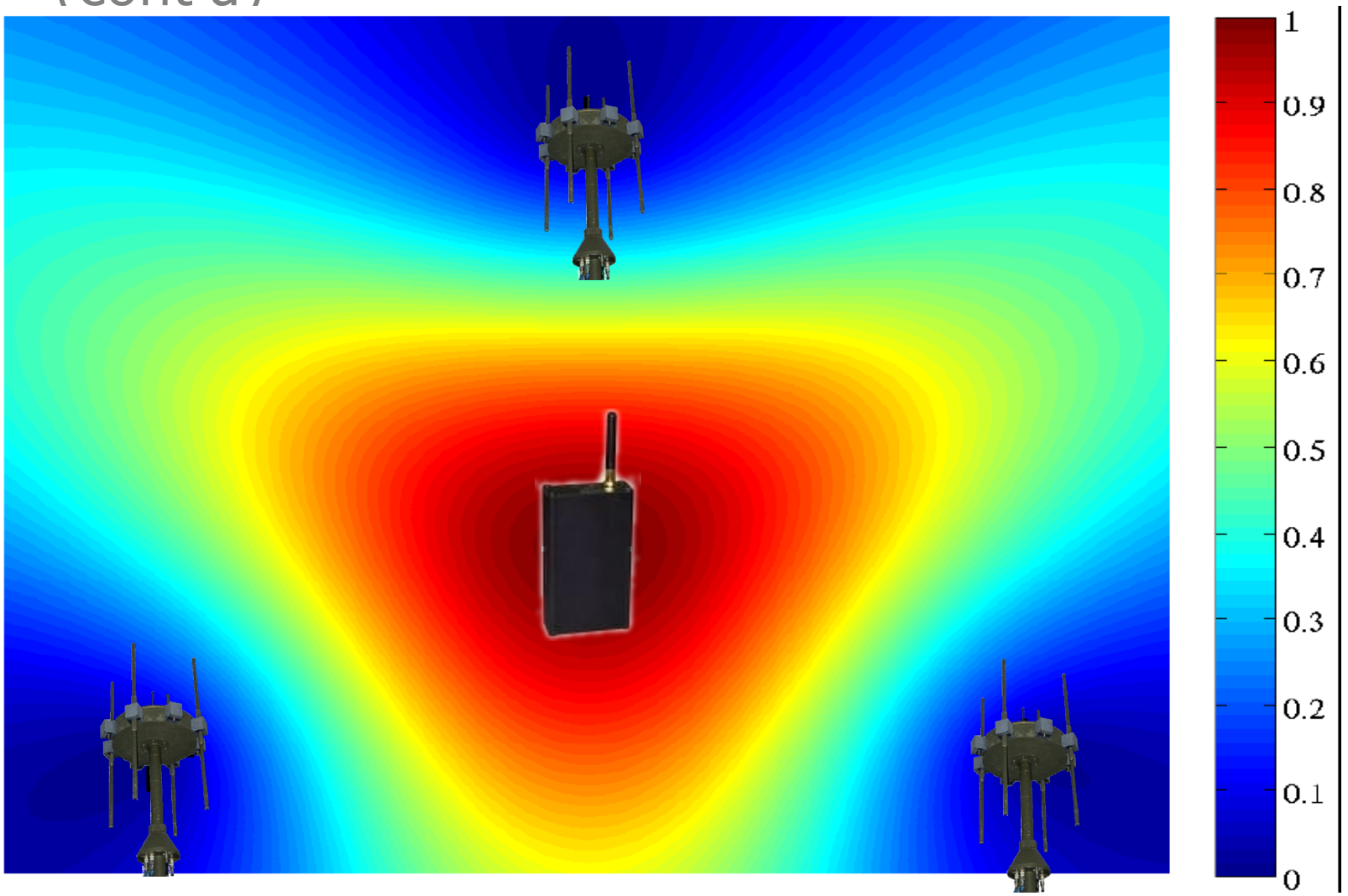


Jammer localization: TDOA (cont'd)

- With three receivers, one location can be determined



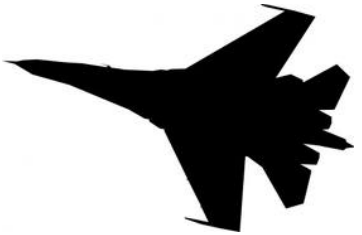
Jammer localization: TDOA (cont'd)



- Example of cross correlation

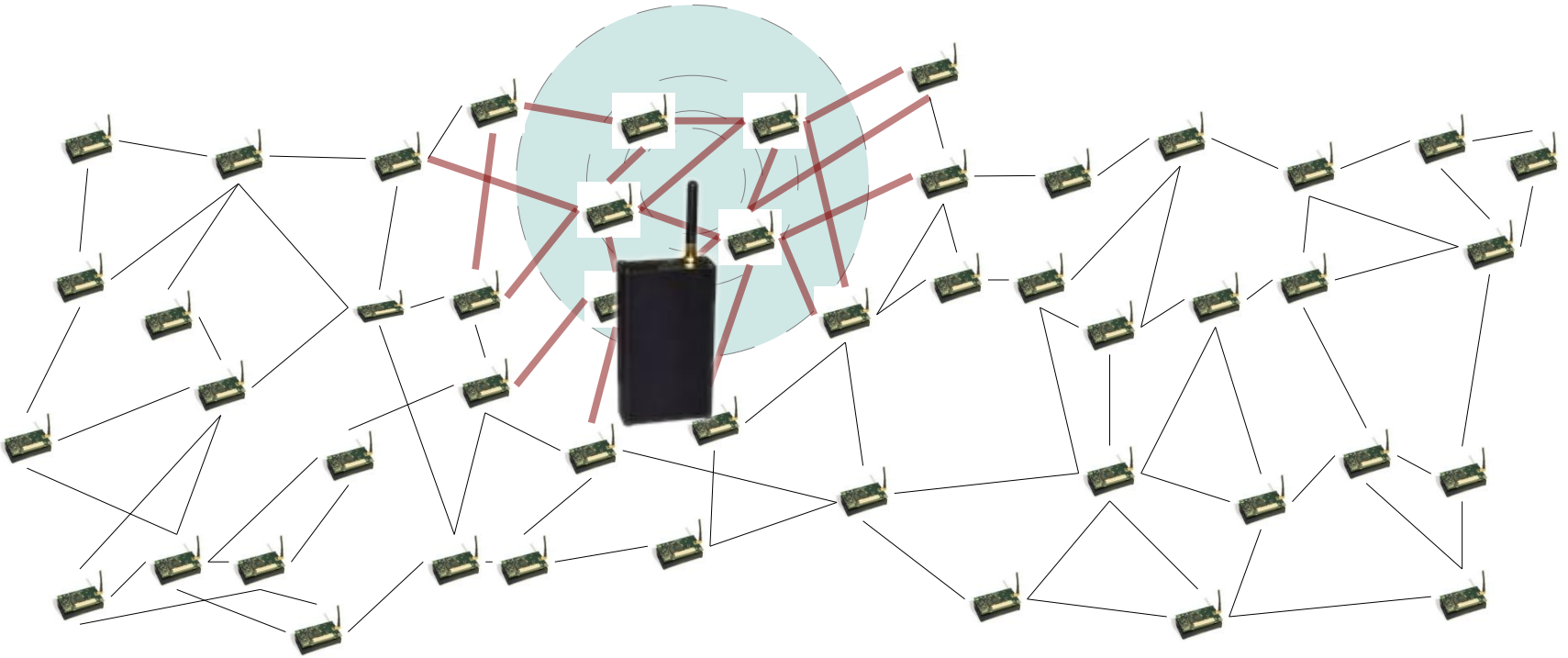
Jammer localization: FDOA

- Frequency Difference of Arrival (FDOA)
  - Also called Differential Doppler
- Works in a similar way as TDOA, but looks at frequency shifts
- Can be combined with TDOA
- Good for fast-moving targets



Impact of Jamming

- Presence of jammer => Wireless links down within its zone of influence



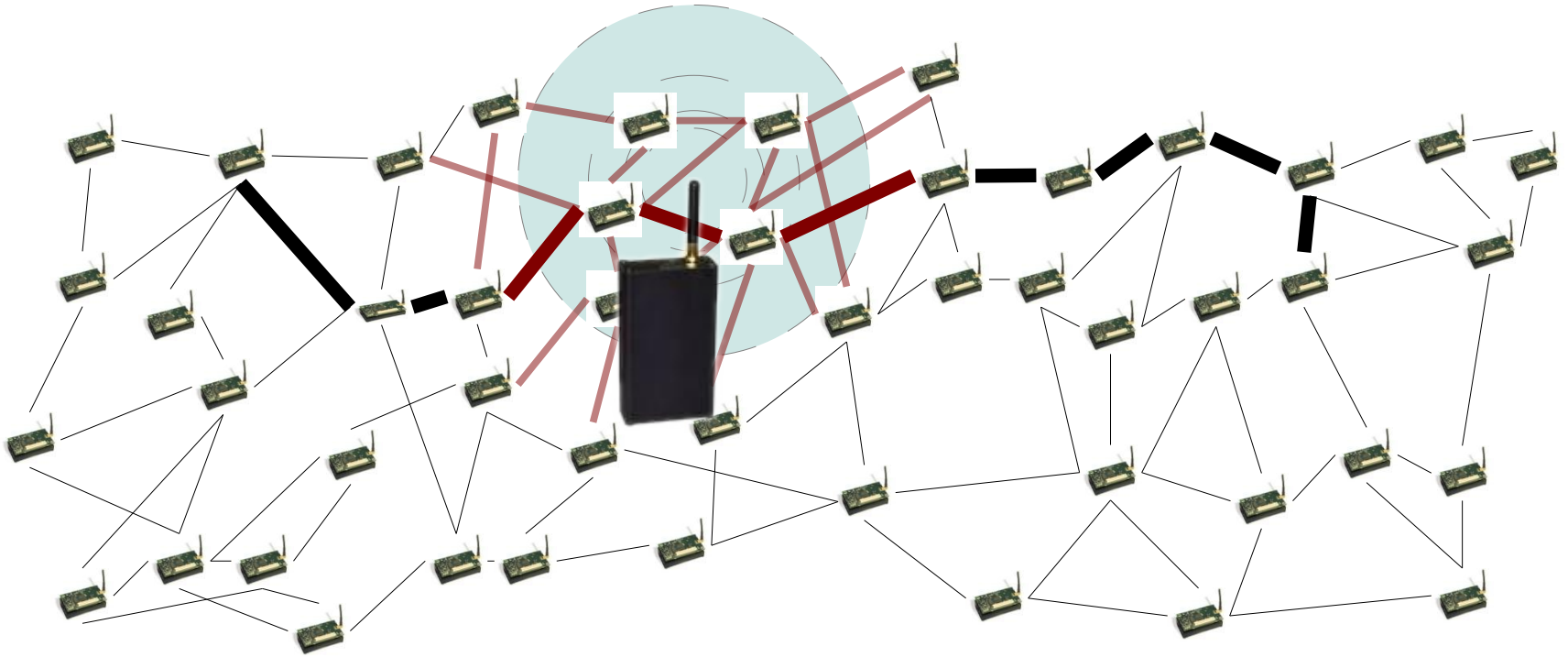
ROYAL INSTITUTE OF TECHNOLOGY

Impact of Jamming (cont'd)

- Jamming or a stronger transmitter can be used as a tool for other attacks
- Those who scream the loudest are heard
- Receivers miss information intended for them
- Intelligent use of jamming
  - Erase messages that 'count' more

Impact of Jamming (cont'd)

- Jamming can be used against any communication
  - See the lectures on Secure Routing/Secure communication

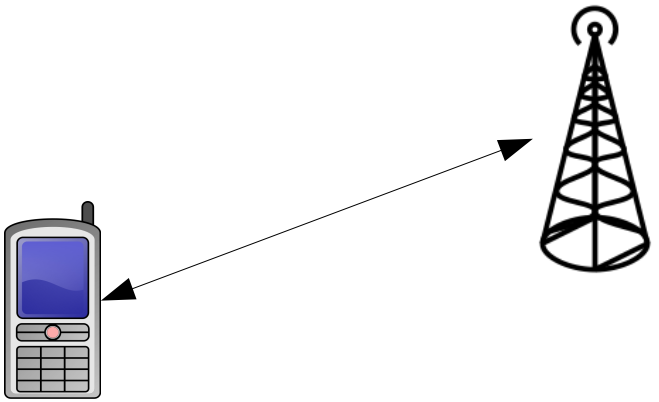


Physical layer attacks

- Adversaries can use a vulnerability at the physical layer
- Attack at a different layer
  - Achieve a goal other than denial of service at the physical layer
- Exploit a vulnerability that is not related only to physical layer functionality
- Examples
  - IMSI catcher
  - SSID overtake
  - Packet (in packet) injection
  - Relaying, localization/distance manipulation (covered in ANSS)

IMSI-catcher

- IMSI: International Mobile Subscriber Identity
- GSM mobiles will connect to the strongest signal
- A Man-In-The-Middle (MITM) attack can be launched this way
  - Encryption is optional
  - Some countries do not use GSM encryption at all



IMSI-catcher (cont'd)

- The mobile will think it is talking to the base station
- Will accept to turn the encryption off
- Rohde & Schwarz has a patent on this
  - EP1051053: *Method for identifying a mobile phone user or for eavesdropping on outgoing calls*

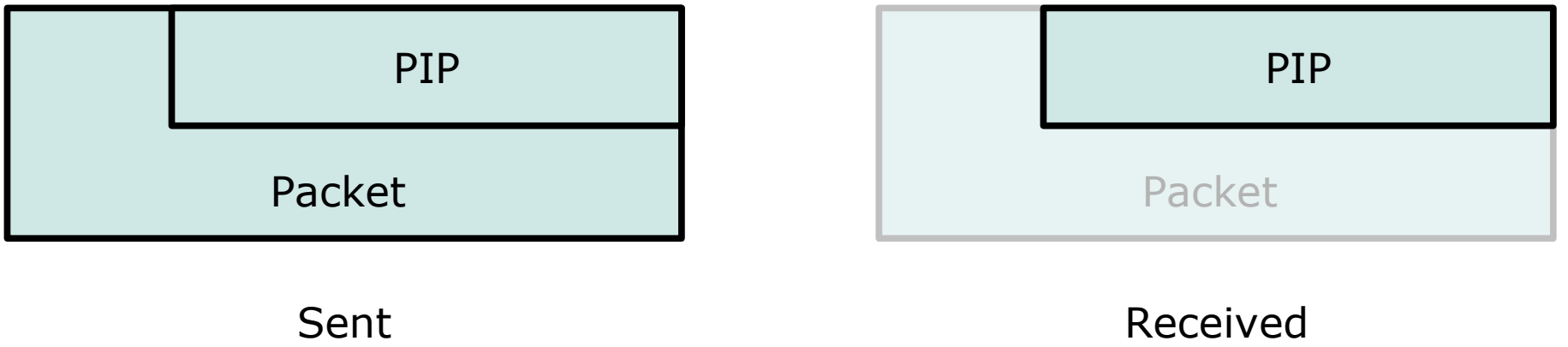
ROYAL INSTITUTE OF TECHNOLOGY

SSID/MAC overtake

- Send a stronger signal than the base station
- Attract network traffic
- Same with clients and Media Access Control (MAC) address
  - MAC filtering does very little for your WLAN security

Packet injection

- Packets can be injected inside legitimate packets
- If the original header is missed/not received
  - Packets in packets (PIP)



ROYAL INSTITUTE OF TECHNOLOGY

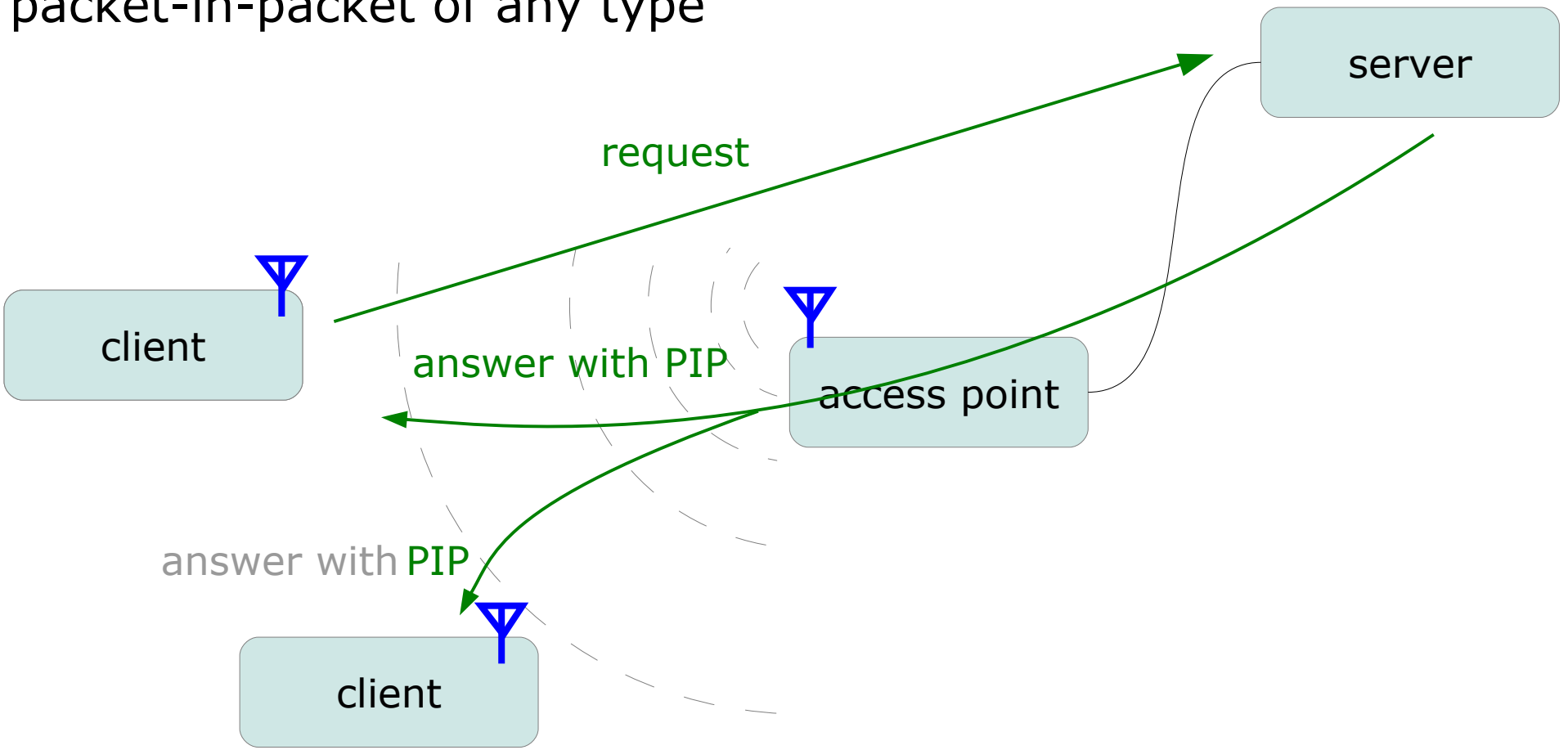
Packet injection (cont'd)

- Further reading: Goodspeed et al, *Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios*
- The title analogy comes from a 1938 radio show
  - War of the Worlds
  - Listeners who tuned in late thought it was a newscast
  - Thus they thought they were being invaded by aliens
  - Because they missed the header saying it was a theater

src: Goodspeed et al, *Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios*

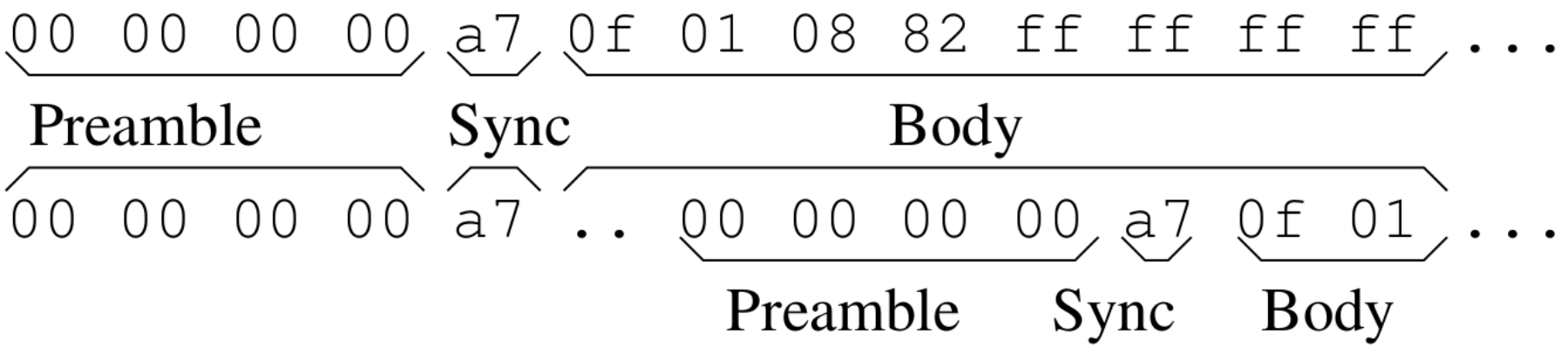
Packet injection (cont'd)

- Can be used remotely, e.g. a client can be made to download a packet-in-packet of any type



Packet injection (cont'd)

- Packets in packets (PIP)
- If the initial header is missed, the receiver will think that the PIP header is the correct one
- Example from the ZigBee protocol:



src: Goodspeed et al, *Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios*

Jamming at upper layers

- Flooding a CSMA/CA network with requests to send can cause a Denial of Service attack
  - See the lecture on (Distributed) Denial of Service

src: Pixar, *Finding Nemo*

ROYAL INSTITUTE OF TECHNOLOGY

Summary

- Usable frequency spectrum is finite
- Jamming, both intentional and accidental, is a problem
- Jamming can be a tool for more complicated attacks
- Ways to mitigate
  - Physical layer techniques
  - Avoiding the jamming
  - Locating and removing the jammer