Wireless Network Security

Lecture 2

Basics of Signal Jamming

DSSS, FHSS, J/S etc.

Srdjan Čapkun

Recommended Readings

- Electronic Warfare 101: David Adamy (Chapters 7 and 9)

Communication Jamming

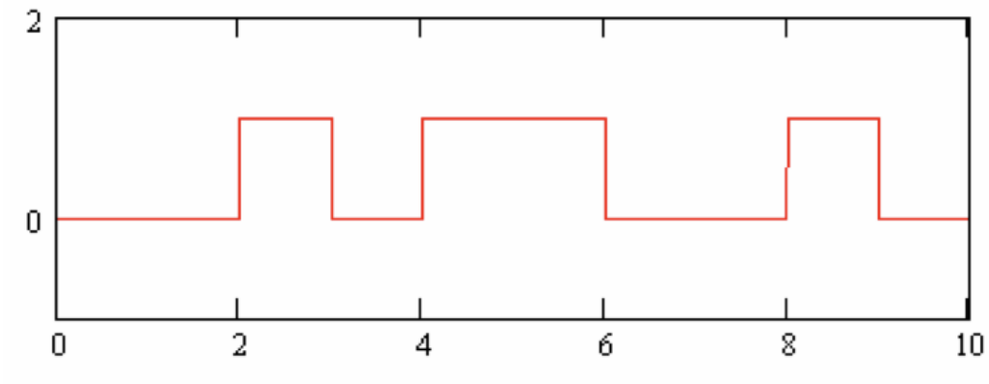
Definition: Entirely preventing or reducing the ability of communicating parties to pass information by the deliberate use of EM signals

The term has been broadly used in a number of contexts and can also refer to unintentional prevention of communication.

Communication Jamming

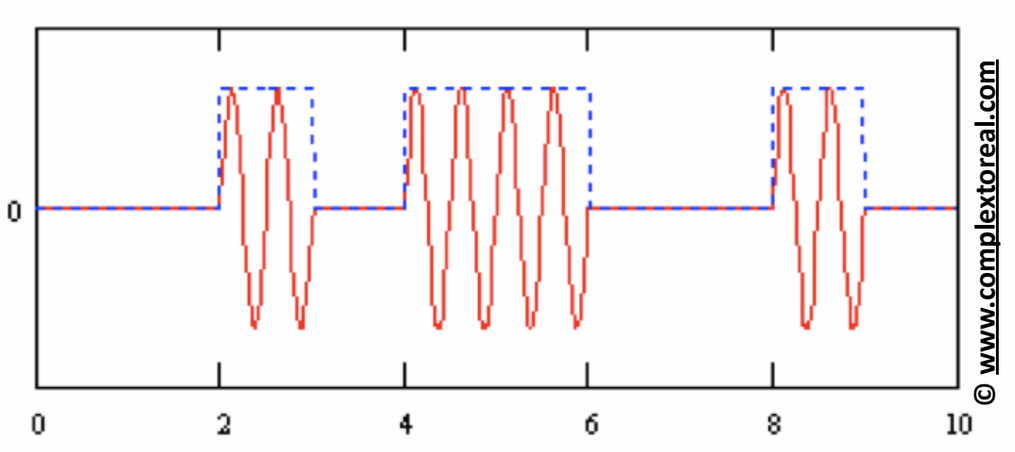
- Carrier: an RF signal that “carries” information
- Carrier typically has a much higher frequency than the information (baseband) signal

Baseband (information) signal: m(t)



Carrier: sin(2π*f*t) *(or cos(2π*f*t))*

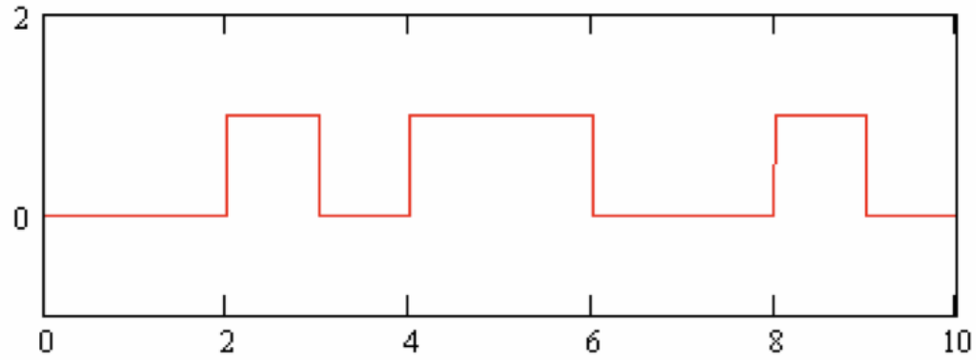
Modulated signal:
ASK(t)=s(t)sin(2πft)
Amplitude Shift Keying



Communication Jamming

- *Carrier:* an RF signal that "carries" information
- Carrier typically has a much higher frequency than the information (baseband) signal

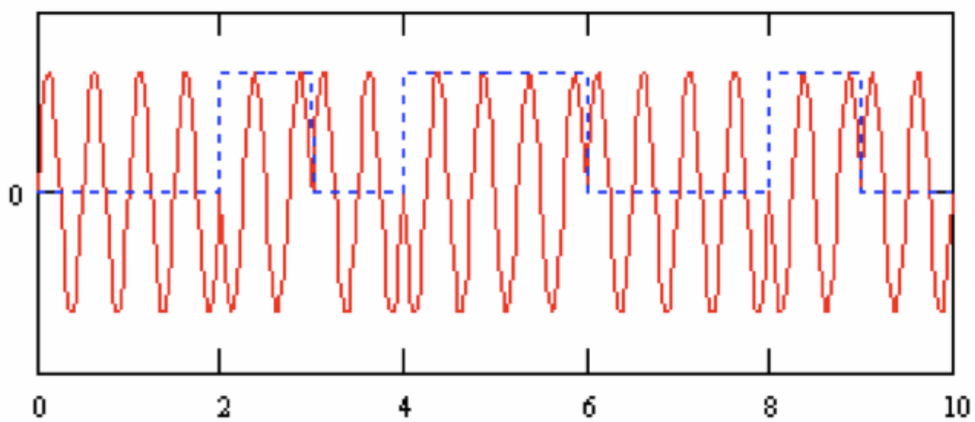
Baseband (information) signal: m(t)



Carrier: sin(2π*f*t) *(or cos(2π*f*t))*

Modulated signal:
BPSK(t) = sin(2πft),b=1
= sin(2πft+π),b=0
Binary Phase Shift Keying (BPSK)

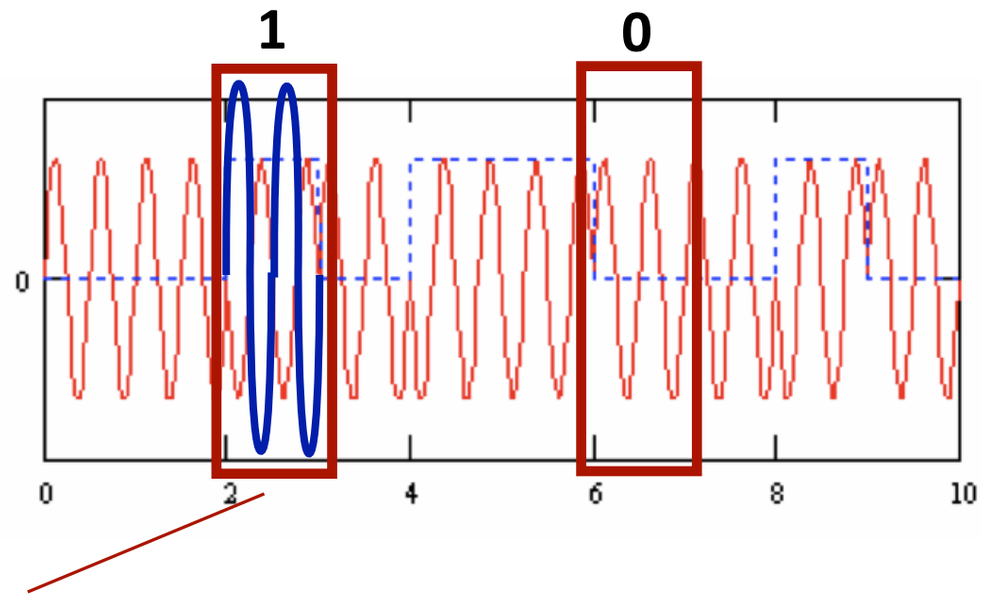
Note: sin(2πft)=cos(2πft+*π*/2)



Communication Jamming

- Symbols: Can carry one or more bits of information, depending on the modulation scheme.

Modulated signal:
BPSK(t) = sin(2πft),b=1
= sin(2πft+π),b=0
Binary Phase Shift Keying



symbol (carrying bit 1)

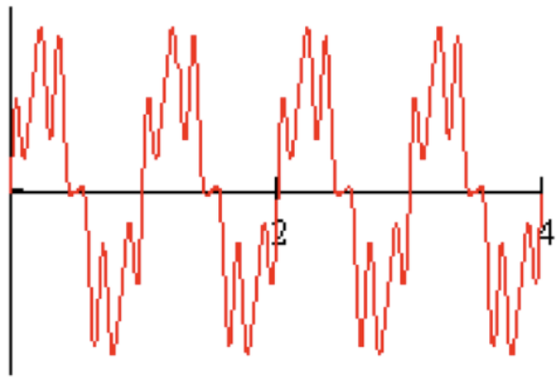
- *Symbol Jamming:* corrupt symbols such that the receiver
  - cannot interpret them or
  - interprets them incorrectly
- *Communication Jamming:* corrupt enough bits such that the information cannot be reconstructed *(despite Error Correction)*

Communication Jamming

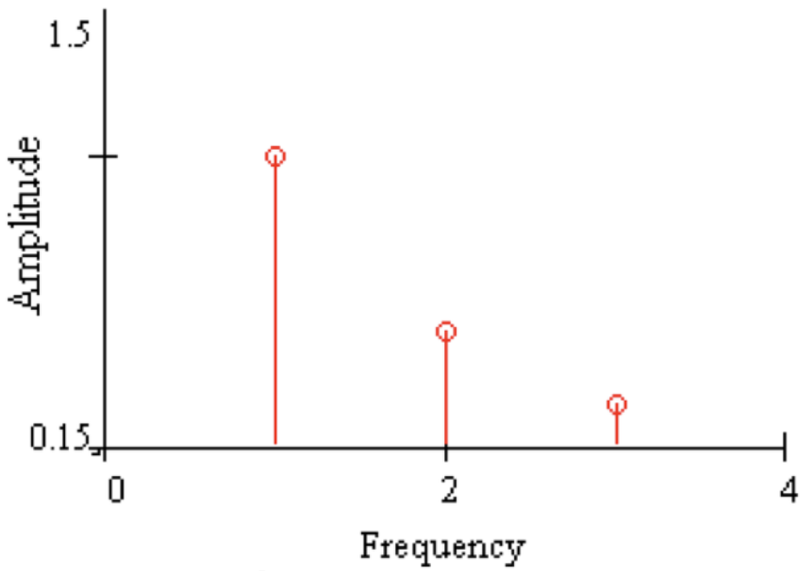
- Jamming individual symbols
  - Individual symbols or bits are jammed
  - Most communication systems will do error detection and correction
  - Beyond a certain threshold of corrupted bits (given for each ECC scheme) the messages cannot be recovered
  - Targeted low-power jamming of individual bits is not easy and might require synchronization

Communication Jamming

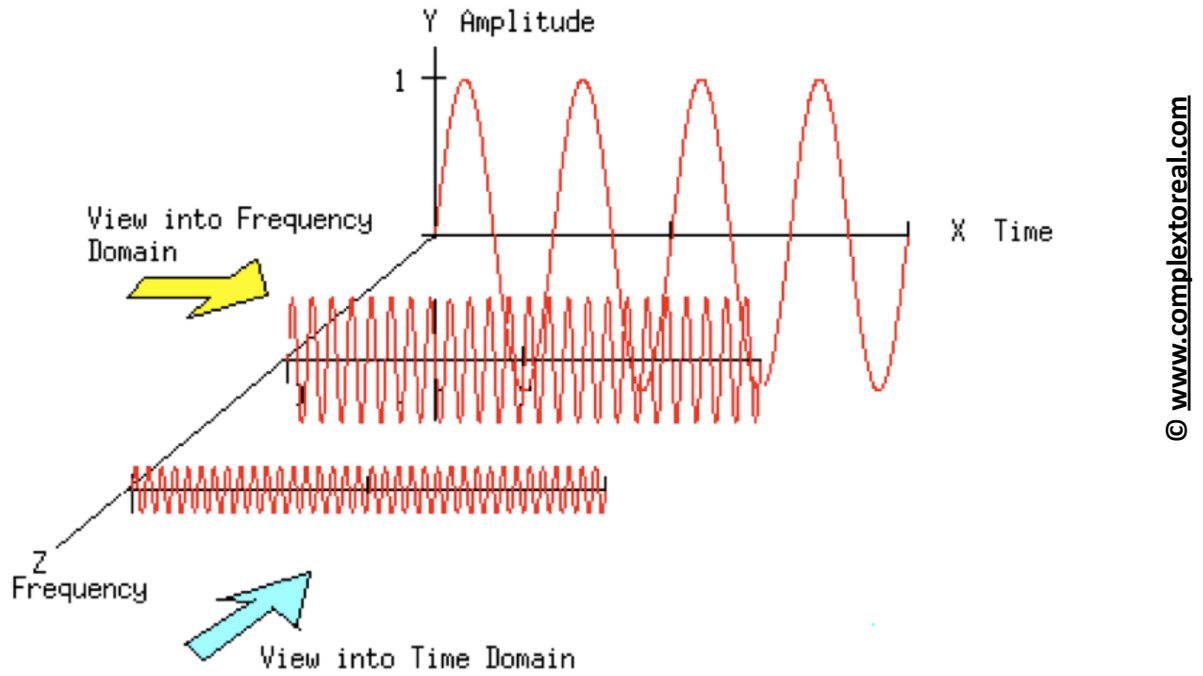
- *Frequency representation of signals:*
  - It is important to understand which RF frequencies are used in communication



periodic signal



signal spectrum



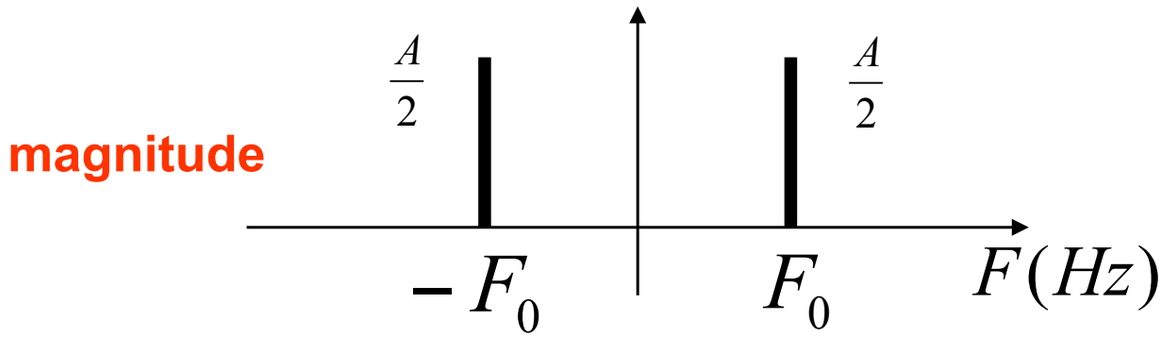
decomposed to its *basic frequency and its harmonics*

Communication Jamming

- *Frequency representation of signals:*
  - complex representation

$$x(t) = A\cos(2\pi F_0 t + \alpha)$$

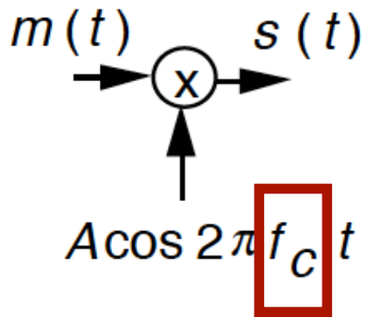
$$= \left(\frac{A}{2}e^{j\alpha}\right)e^{j2\pi F_0 t} + \left(\frac{A}{2}e^{-j\alpha}\right)e^{-j2\pi F_0 t}$$



Frequency Representation

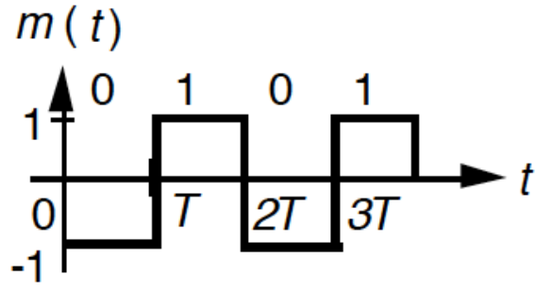
Communication Jamming

- *Example spectrum*



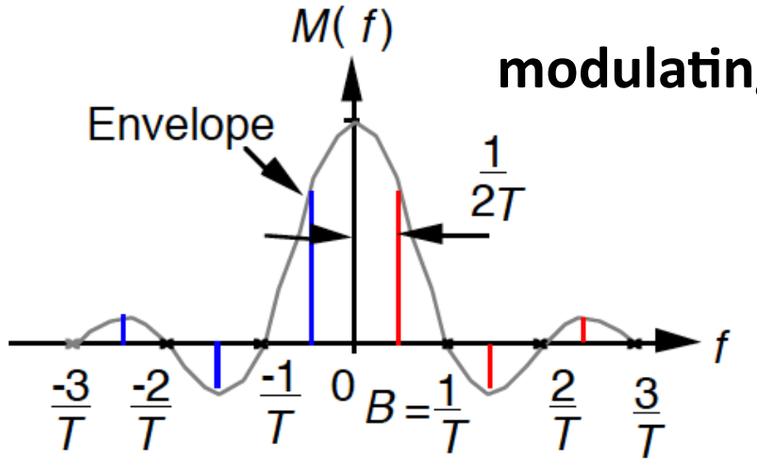
carrier frequency

message (modulating signal)

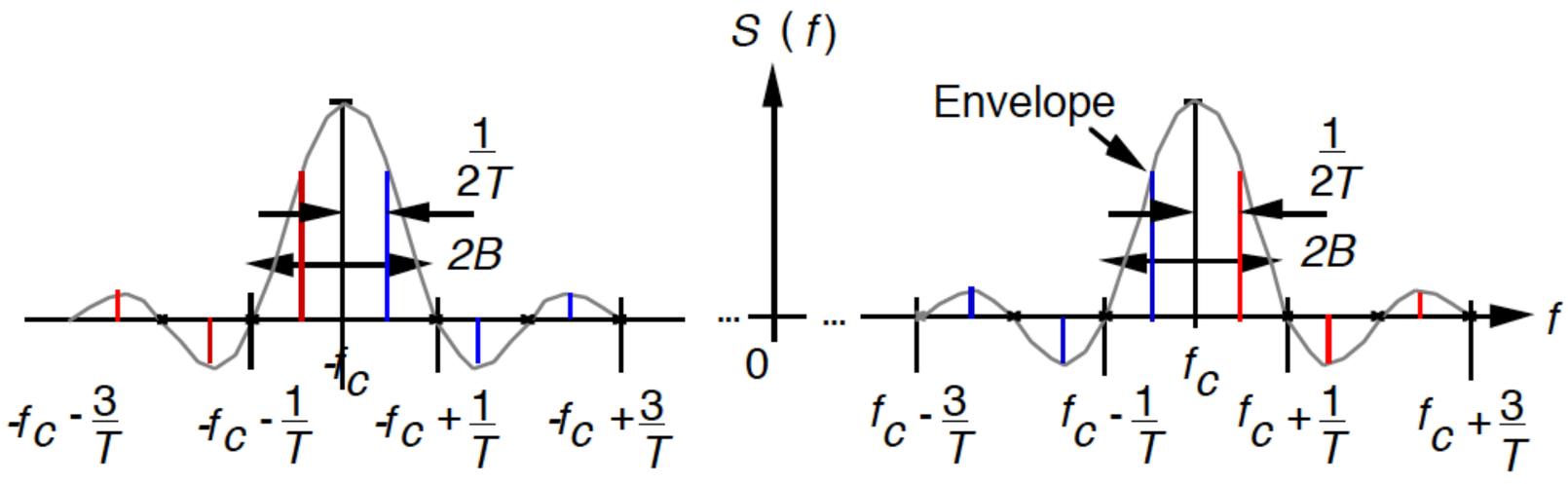


(a)

modulating signal spectrum

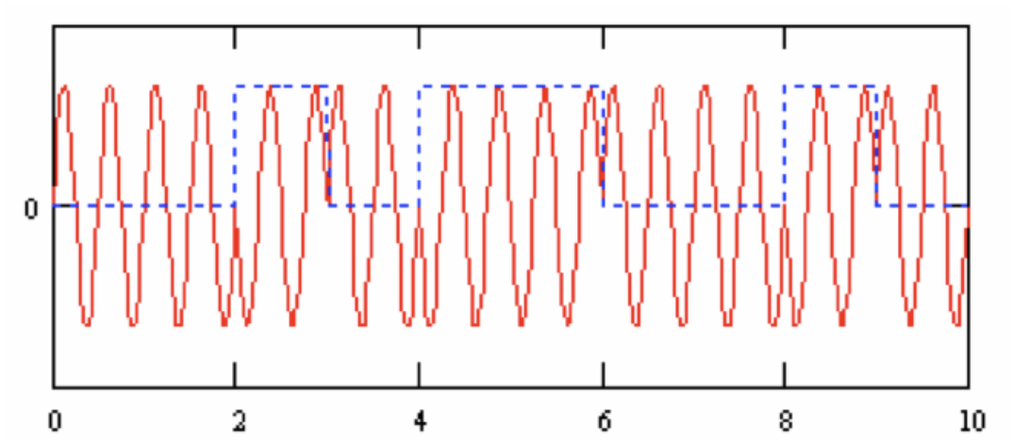


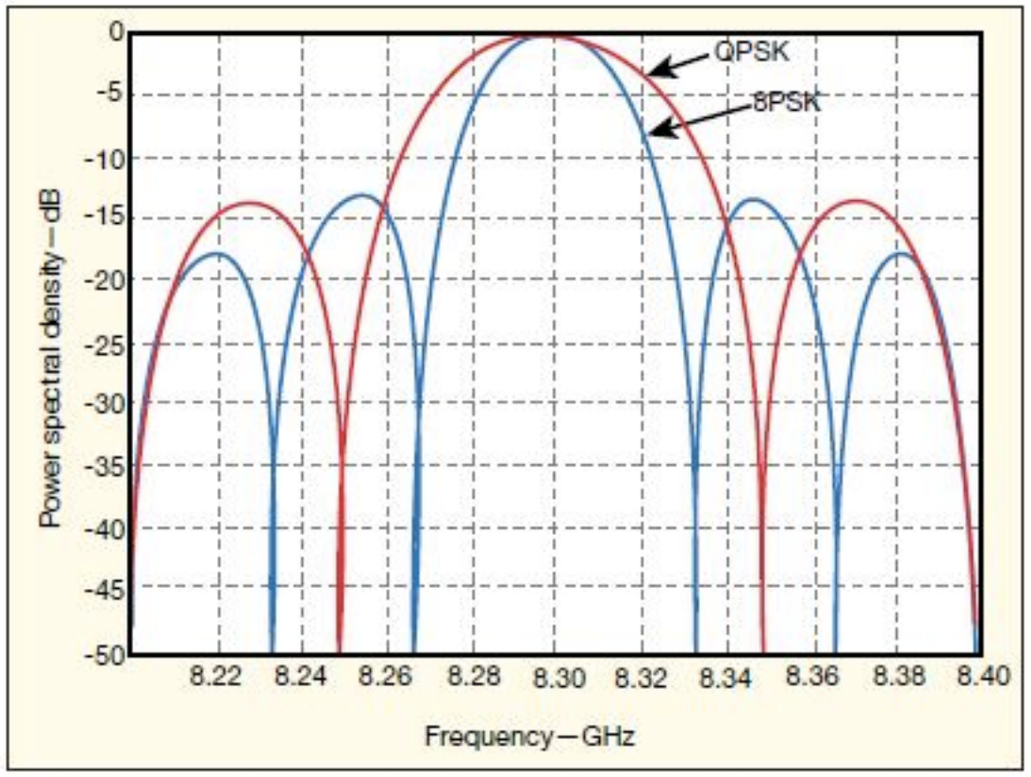
(b)



Communication Jamming

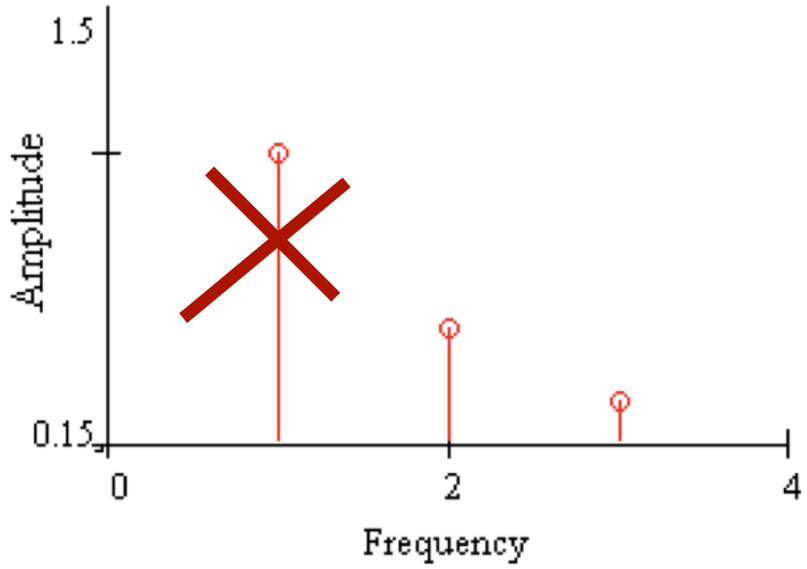
- *Example spectrum* (BPSK)





Communication Jamming

- *Frequency:*
  - To jam, the attacker needs to *transmit on the right frequencies during the right time. (e.g., all)*
  - Partial jamming might not prevent communication (the receiver might still reconstruct the signal)



example spectrum

P – transmitted power
G - antenna gain
F – communication frequency
D - distance

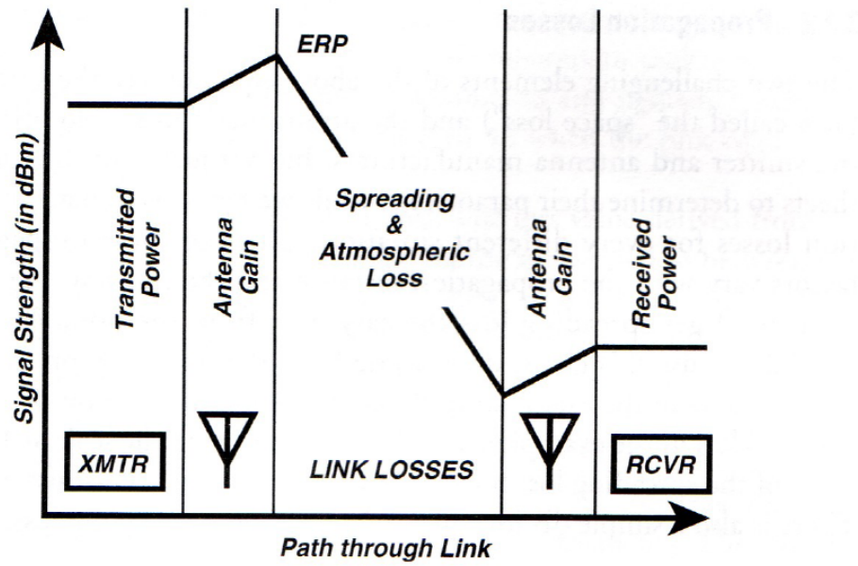
Communication Jamming

- *Assuming that the attacker uses the full signal spectrum.*
  - It is all about power!

$$S = P_T + G_T - 32 - 20\log(F) - 20\log(D_S) + G_R$$

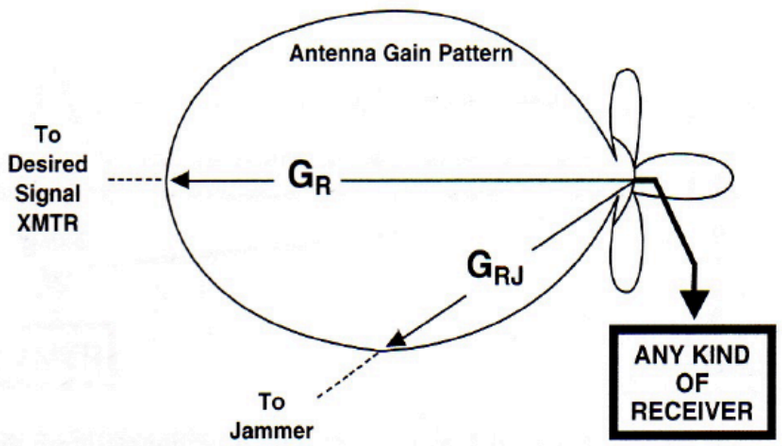
$$J = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ}$$

spreading losses directional gain



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

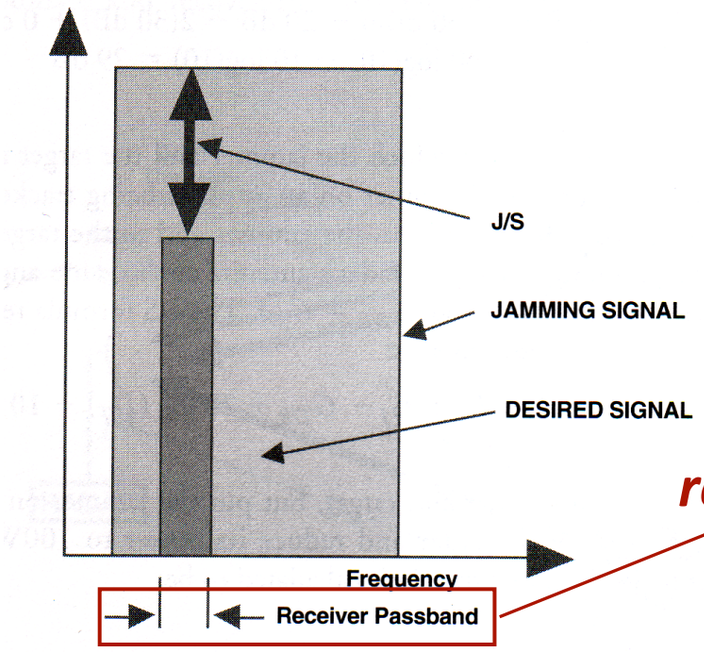
- *Jamming-to-Signal ratio (J/S):*
  - `J/S = J-S (dB)`
  - In most communication systems `J/S=0` results in successful jamming



If the receiving antenna is not omnidirectional, its gain to the jamming signal will be different (usually less) than its gain to the desired signal.

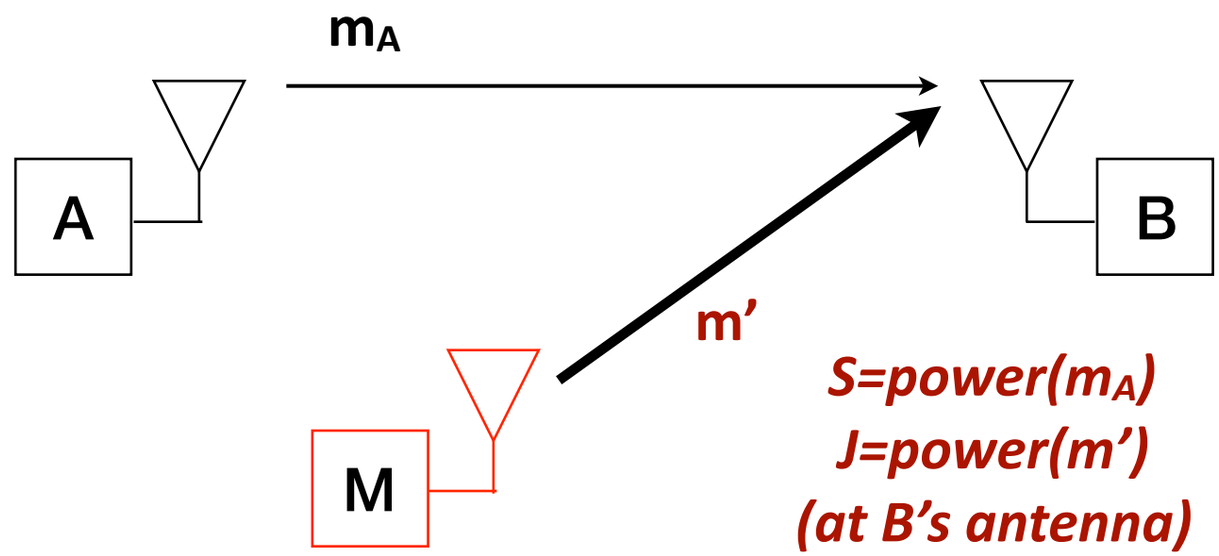
P – transmitted power
G - antenna gain
F – communication frequency
D - distance

Communication Jamming



The jamming-to-signal ratio is simply the ratio of the power of the two received signals within the frequency passband of the receiver.

receiver filters



S=power(m_A)
J=power(m')
(at B's antenna)

$$S = P_T + G_T - 32 - 20\log(F) - 20\log(D_S) + G_R$$

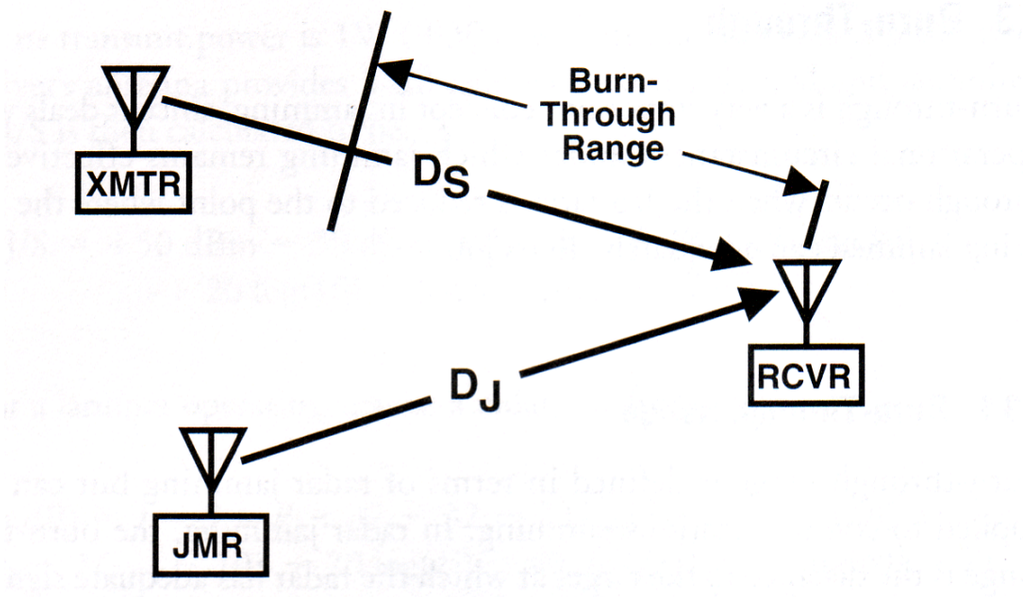
$$J = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) - G_{RJ}$$

spreading losses — directional gain

- Example:
  - jammer uses 100W (50dBm), antenna gain 10dB, distance 30km
  - transmitter uses 1W (30dBm), antenna gain 3dB, distance 10km
  - J/S = 17dB => probably successful jamming

Communication Jamming

- Burn-through range: The range from which the sender succeeds in communicating with the receiver, despite jamming.



Other Types of Jamming

Types of Jamming

Type of Jamming	Purpose
Communications jamming	Interferes with enemy ability to pass information over a communications link
Radar jamming	Causes radar to fail to acquire target, to stop tracking target, or to output false information
Cover jamming	Reduces the quality of the desired signal so it cannot be properly processed or so that the information it carries cannot be recovered
Deceptive jamming	Causes a radar to improperly process its return signal to indicate an incorrect range or angle to the target
Decoy	Looks more like a target than the target does; causes a guided weapon to attack the decoy rather than its intended target

Communication Jamming

- Parameters that influence jamming

The Effect of Each Parameter in the Jamming Situation on J/S

Parameter (Increasing)	Effect on J/S	Type of Jamming
Jammer transmit power	Directly increases on J/S dB for dB	All
Jammer antenna gain	Directly increases J/S dB for dB	All
Signal frequency	None	All
Jammer-to-receiver distance	Decreases J/S as the distance^2	All
Signal transmit power	Directly decreases J/S dB for dB	All
Radar antenna gain	Decreases J/S dB for dB	Radar (self-protect)
Radar antenna gain	Decreases J/S 2 dB per dB	Radar (stand-off)
Radar-to-target distance	Increases J/S as the distance^4	Radar
Radar cross-section of target	Directly increases J/S dB for dB	Radar
Transmitter-to-receiver distance	Increases J/S as the distance^2	Comm
Transmit antenna gain	Directly decreases J/S dB for dB	Comm
(Directional) receiver antenna gain	Directly decreases J/S dB for dB	Comm

Communication Jamming: Implications

- Jamming has implications beyond Denial of Service attacks:
- Example: *Public WiFi Localization Systems*
  - (Access Point MAC, Location Pairs) stored in a database.
  - Mobile device detects APs and retrieves their locations.
  - Based on these locations, computes its location.

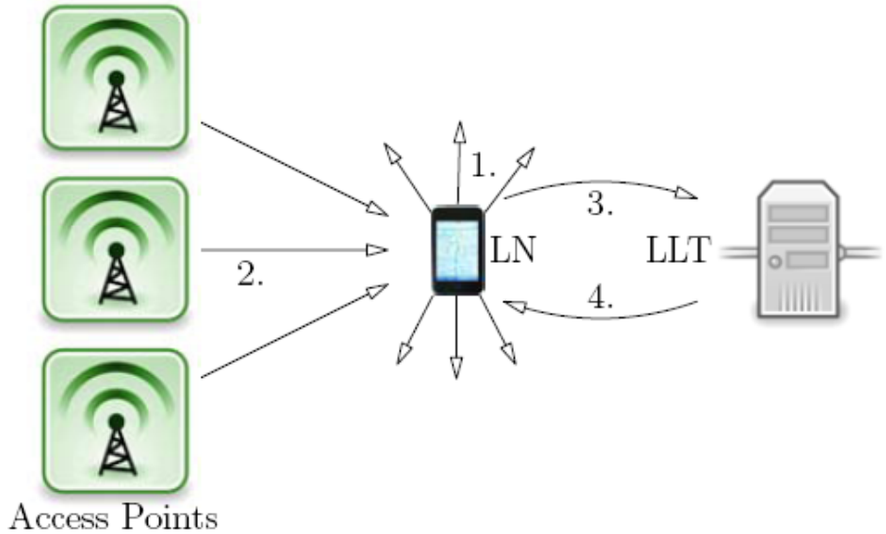
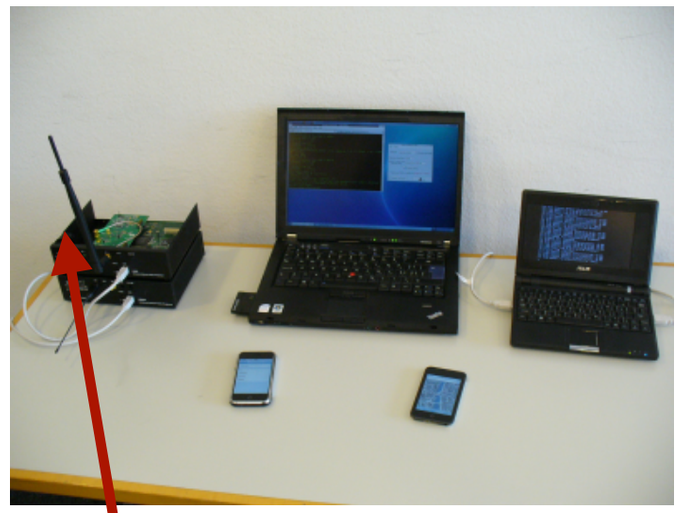


Figure 1: The Skyhook localization process. 1. The LN broadcasts a probe request frame. 2. APs reply with a response beacon frame. 3. The LN queries the LLT server. 4. The server returns data about observed APs. 5. The LN computes its location.

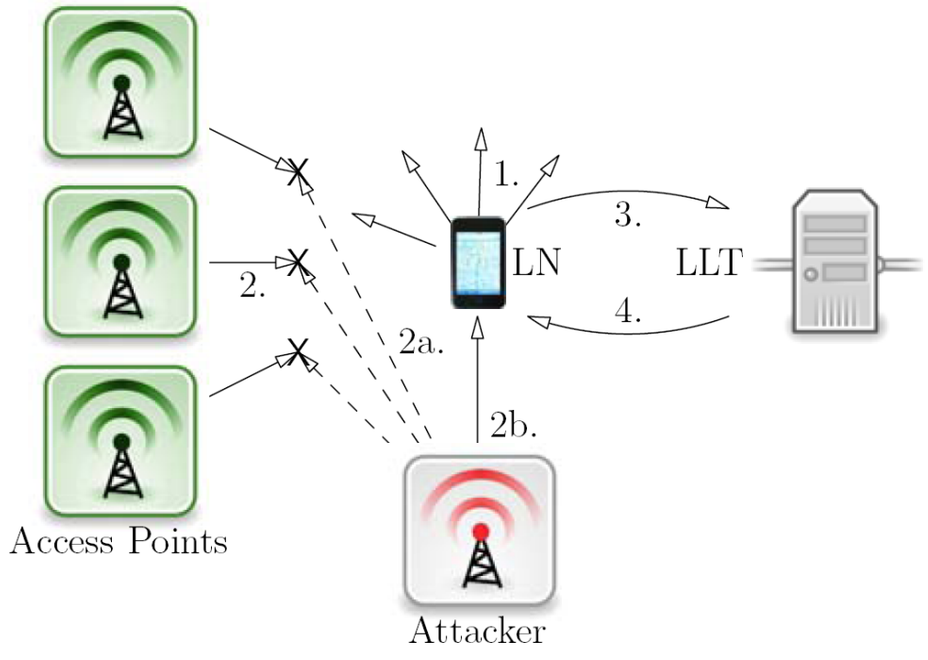
http://www.syssec.ch/press/location-spoofing-attacks-on-the-iphone-and-ipod

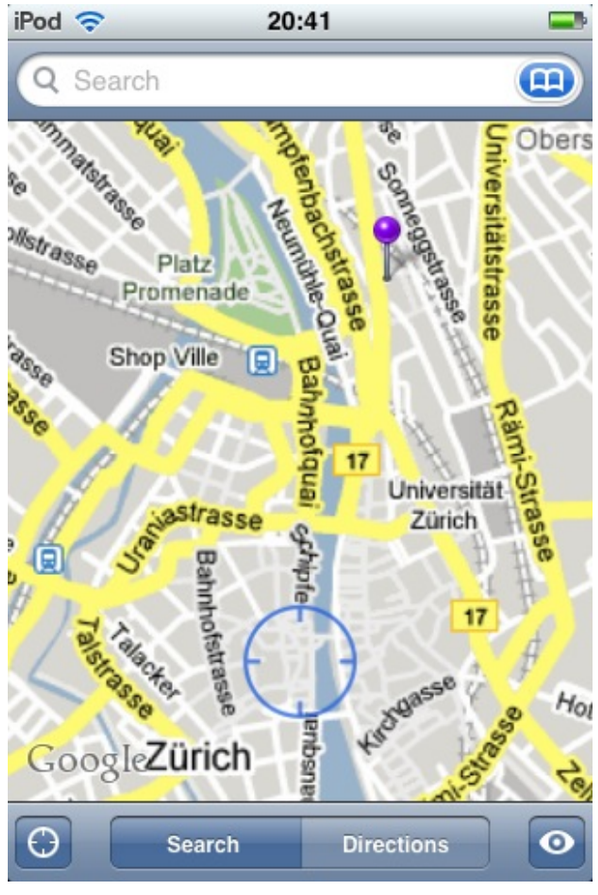
Communication Jamming: Implications

- Example: *Public WiFi Localization Systems*
  - When a Mobile is localized,
    - ***jam legitimate APs***
    - insert MACs of APs from another location
  - This results in the Mobile displaying an incorrect location



USRP platform





http://www.syssec.ch/press/location-spoofing-attacks-on-the-iphone-and-ipod

Physical Layer Security

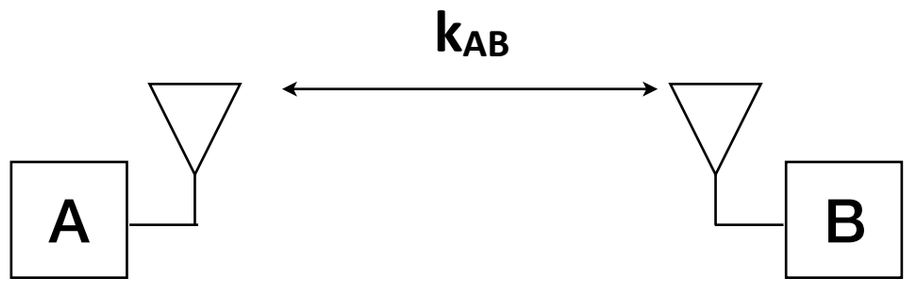
Jamming-resistant communication

Jamming Resistant Communication

- Basic principle of Jamming Resistant Communication:
  - If you cannot fight, *RUN, HIDE (and WAIT)*
- Techniques for Jamming Resistant Communication:
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Chirp

Jamming Resistant Communication

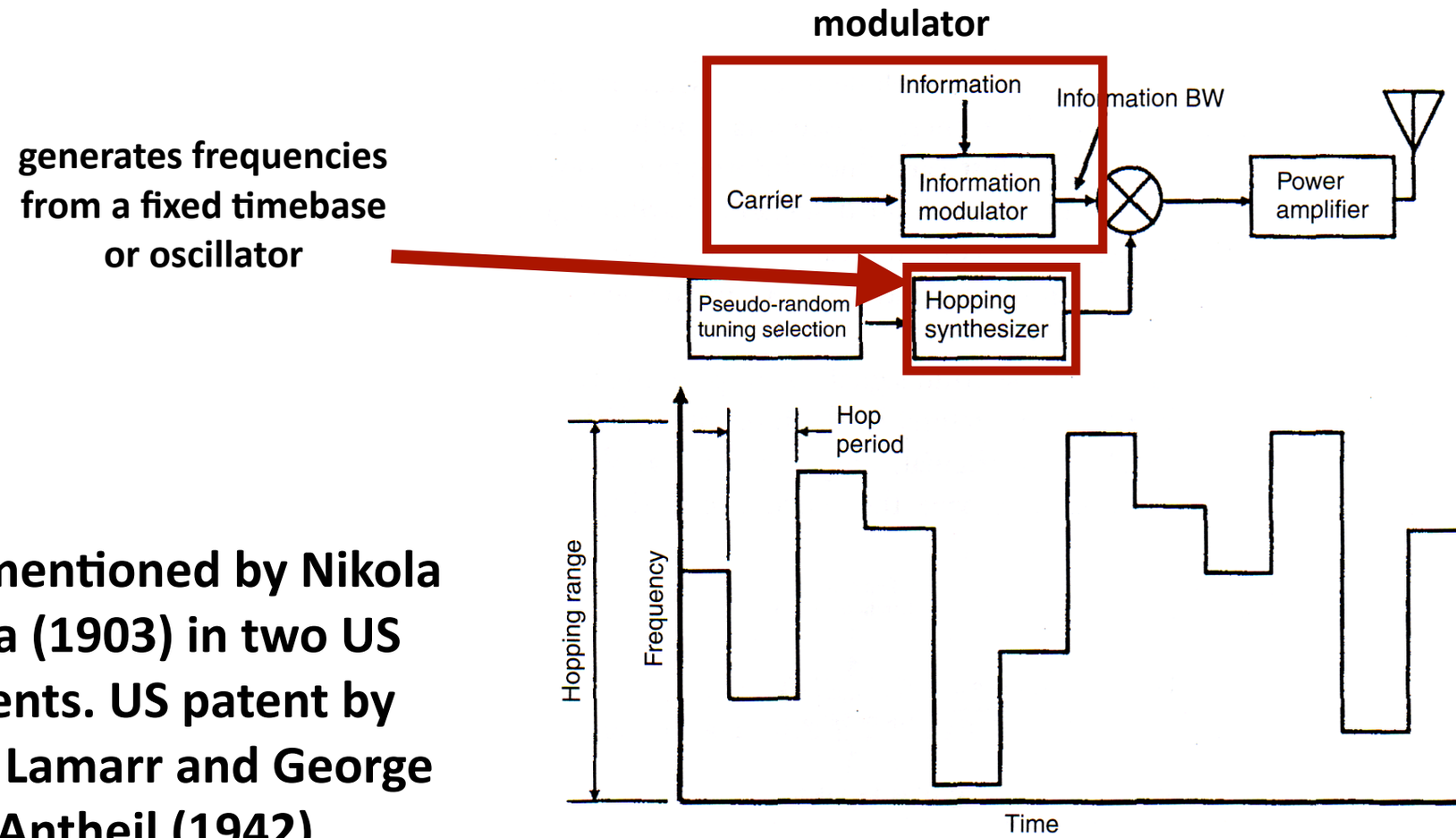
- Basic principle of Jamming Resistant Communication:
  - If you cannot fight, *RUN and HIDE*
  - But we need an advantage over the attacker:
    a shared secret key between the sender and the receiver



Frequency Hopping Spread Spectrum

- Using the shared key, the sender and the receiver derive a pseudorandom hopping sequence
- Sender and receiver are synchronized
- *The attacker cannot guess the next hop or detect-and-jam*

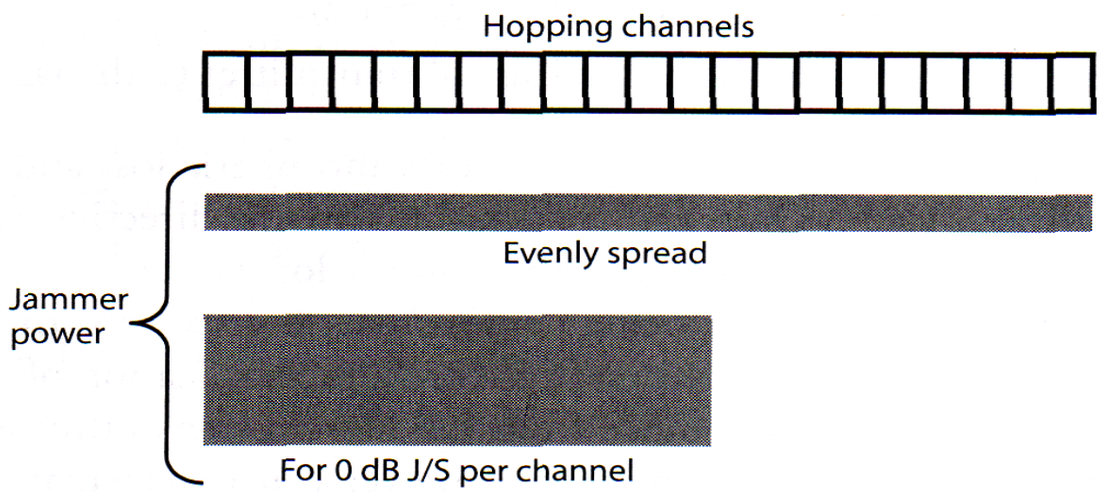
First mentioned by Nikola Tesla (1903) in two US patents. US patent by Hedy Lamarr and George Antheil (1942)



Frequency-hopped signals hop between randomly selected frequencies over a wide frequency range.

Frequency Hopping Spread Spectrum

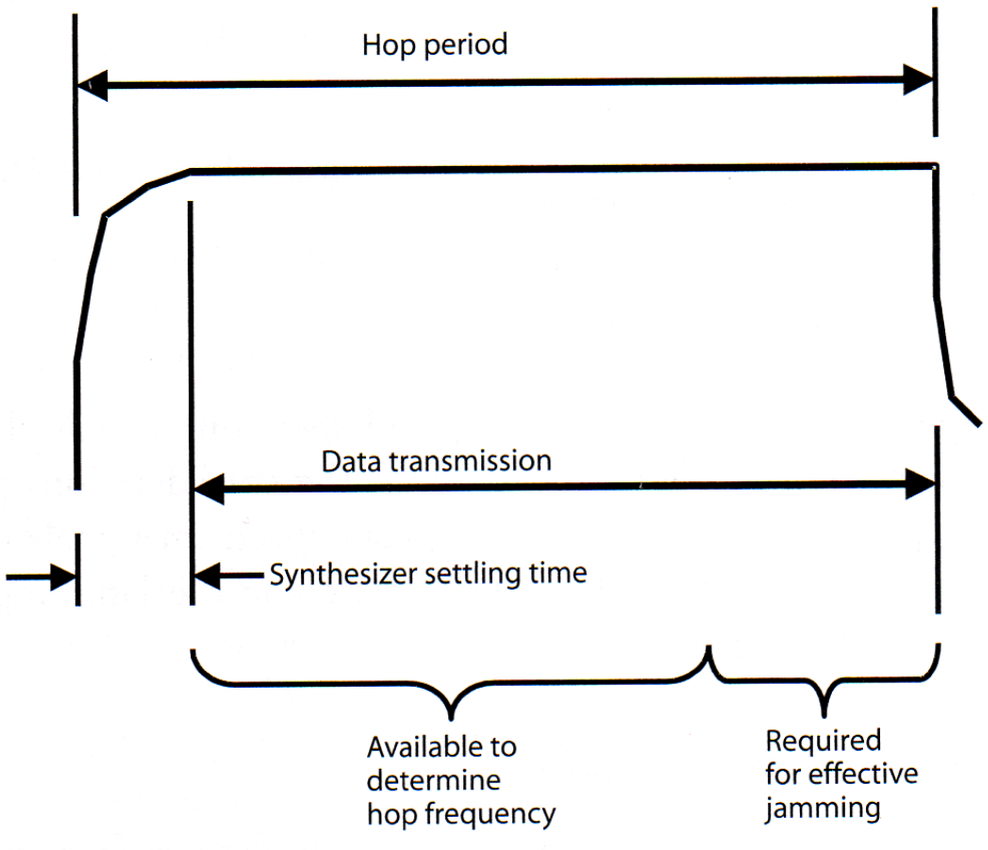
- *FHSS Partial Band Jammer*
  - Distributes its power such that the jamming power per channel is equal to the received signal strength
  - `J/S=0dB` provides sufficient Bit Error Rate



A partial-band jammer distributes its available power to achieve 0 dB J/S in each jammed channel at the jammed receiver.

Frequency Hopping Spread Spectrum

- *FHSS Follower Jammer*
  - First detects on which frequency communication is taking place and then jams.
  - Protection: message encodings that enable message recovery despite of x% of it being corrupted



Bluetooth:

79 channels, 1MHz each

1000 hops/second

Jaguar V system:

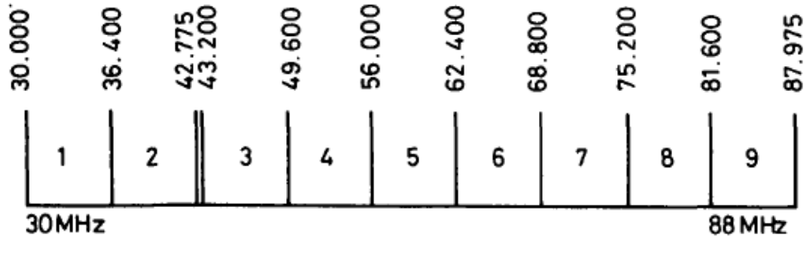
50W

2320 channels

50-500 hops/second

Jaguar-V frequency-hopping radio system
IEEPKOC, Vol. 129, Pt. F, No. 3, JUNE 1982

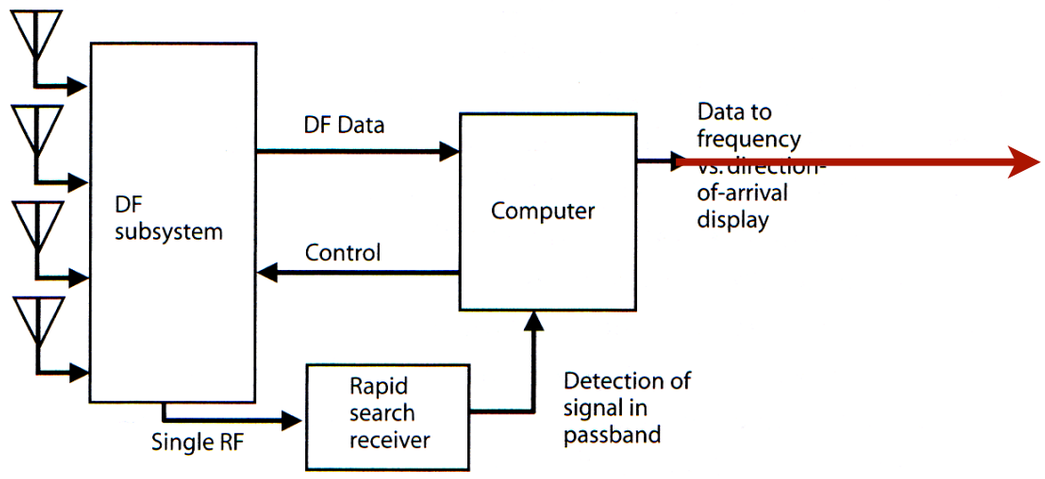
A follower jammer must determine the frequency of the hop and set its jamming frequency during 67% of the data transmission time.



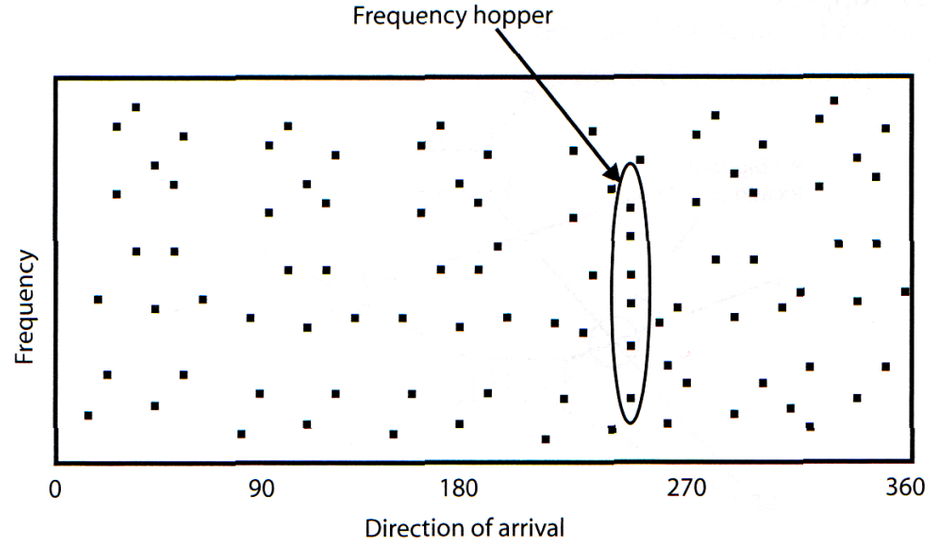
1 hop band =256 channels spaced by 25kHz
=6.4 MHz

Frequency Hopping Spread Spectrum

- *Detectability / Localization of FHSS transmitters*
  - FHSS transmitters do not really “hide”
  - Using AoA techniques can be detected
  - Other possible techniques include differential RSS localization, TDoA, etc ...



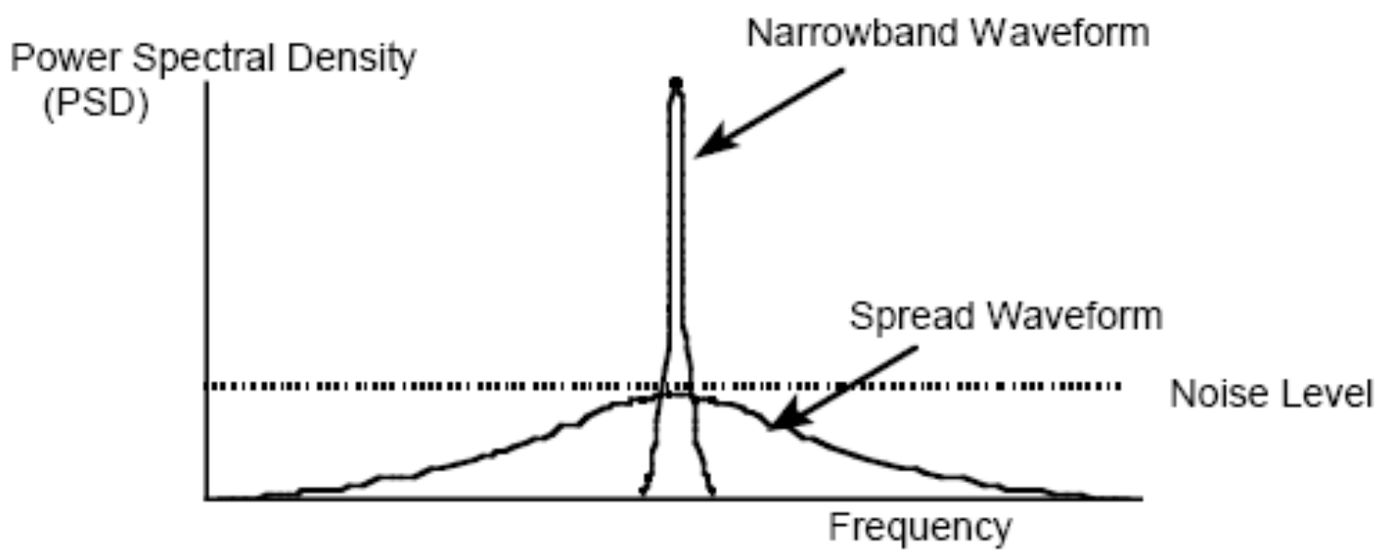
9 A sweeping DF system for frequency hoppers includes a rapid search receiver to detect occupied channels. Then the search is stopped while a DF is taken.



i.40 When collected DOA data shows multiple frequencies at one angle of arrival, a frequency hopper is identified.

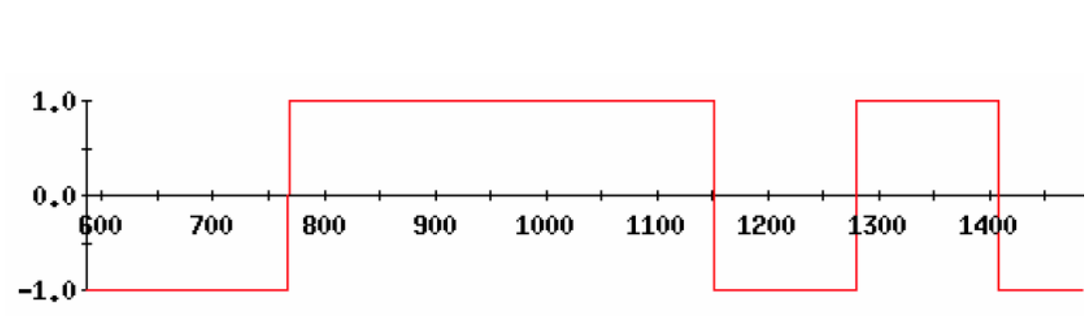
Direct Sequence Spread Spectrum

- DSSS
  - Spread the signal using a secret code (derived from a key)
  - Signal is “hidden” in noise *(we need noise)*

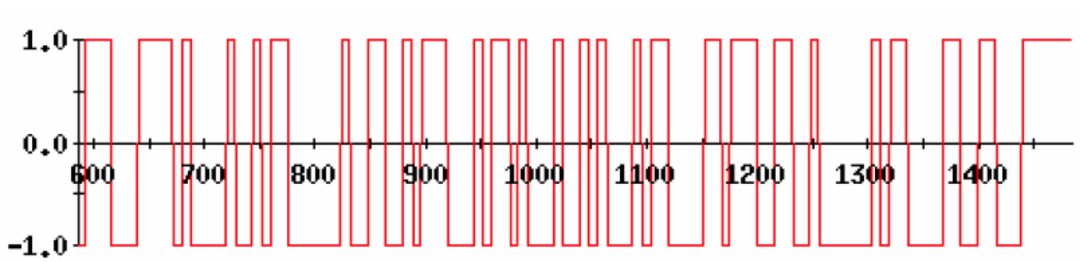


Direct Sequence Spread Spectrum

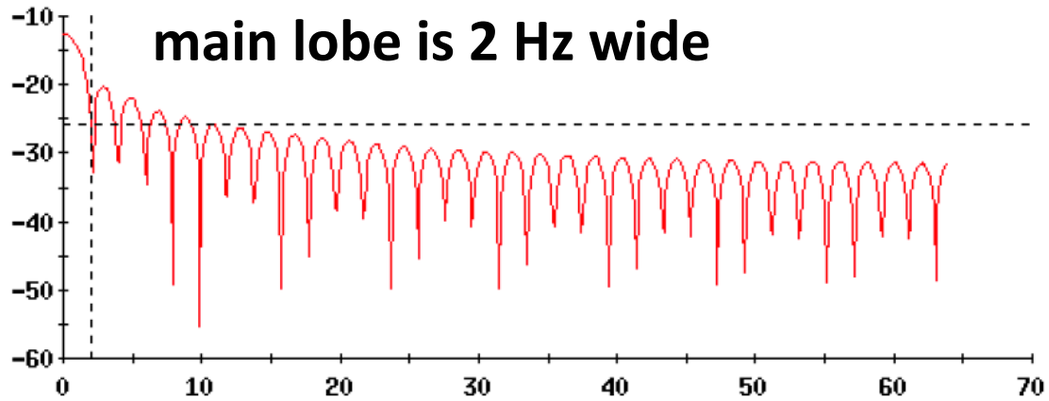
- *DSSS*
  - Spreading (baseband)
  - To spread, we need to transmit with a higher symbol (bit) rate. *Makes sense?*



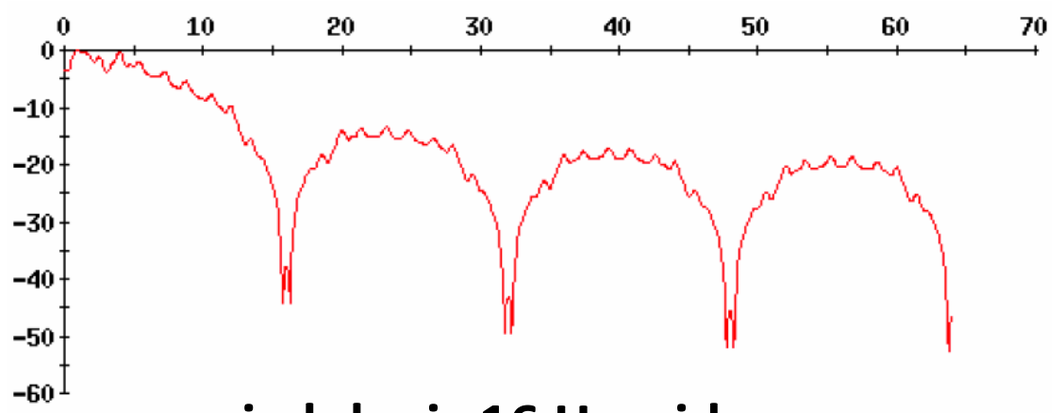
symbol rate is 2



symbol rate is 16



main lobe is 2 Hz wide



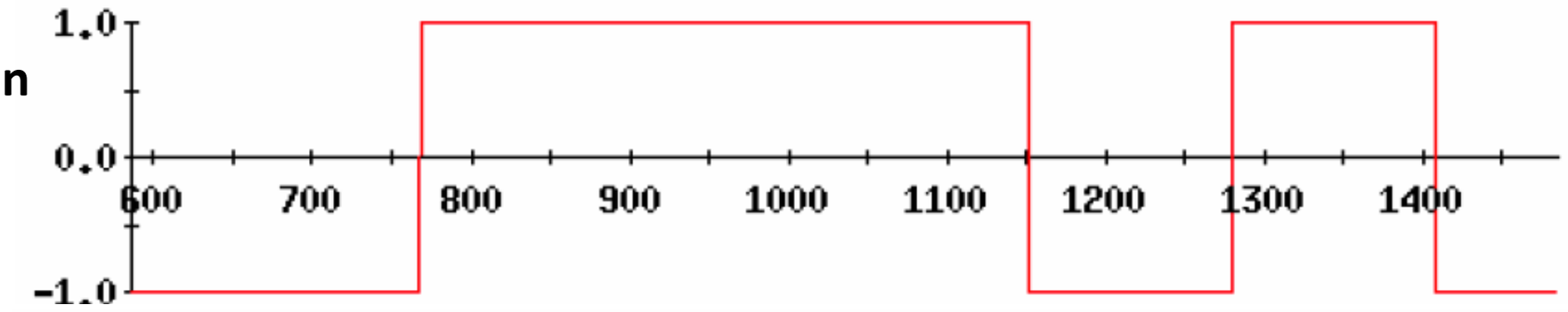
main lobe is 16 Hz wide

Frequency Representation

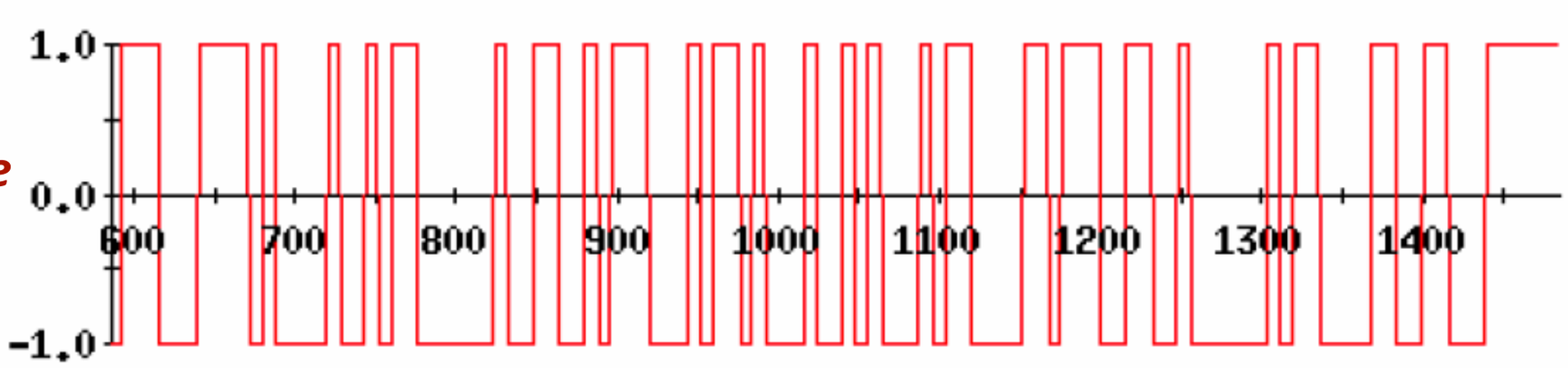
Direct Sequence Spread Spectrum

The ratio of the chip rate to the information bit rate is the *processing gain (PG)*

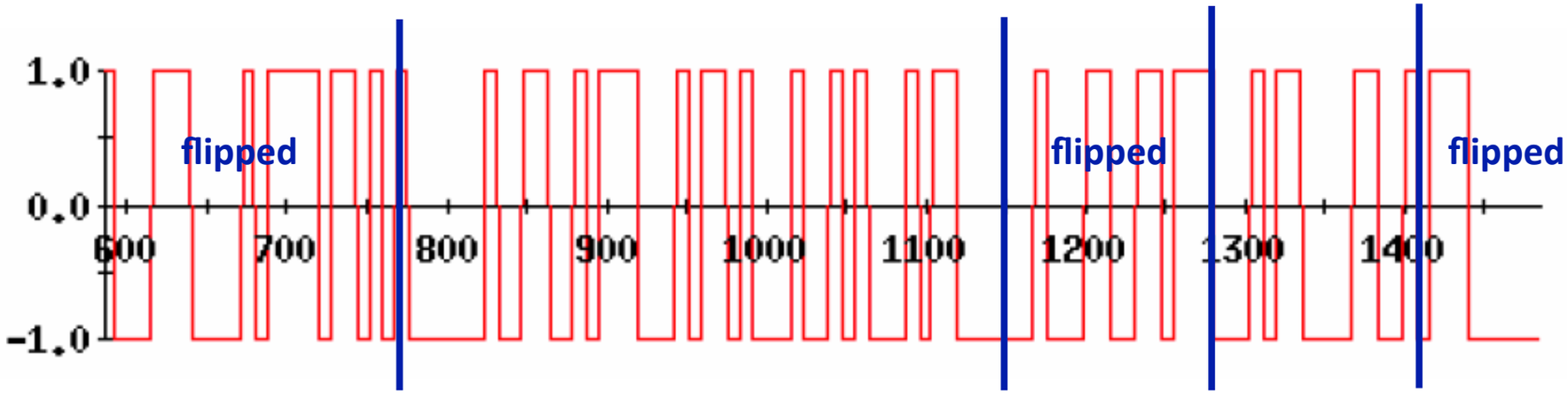
information (bits)



spreading code (chips)

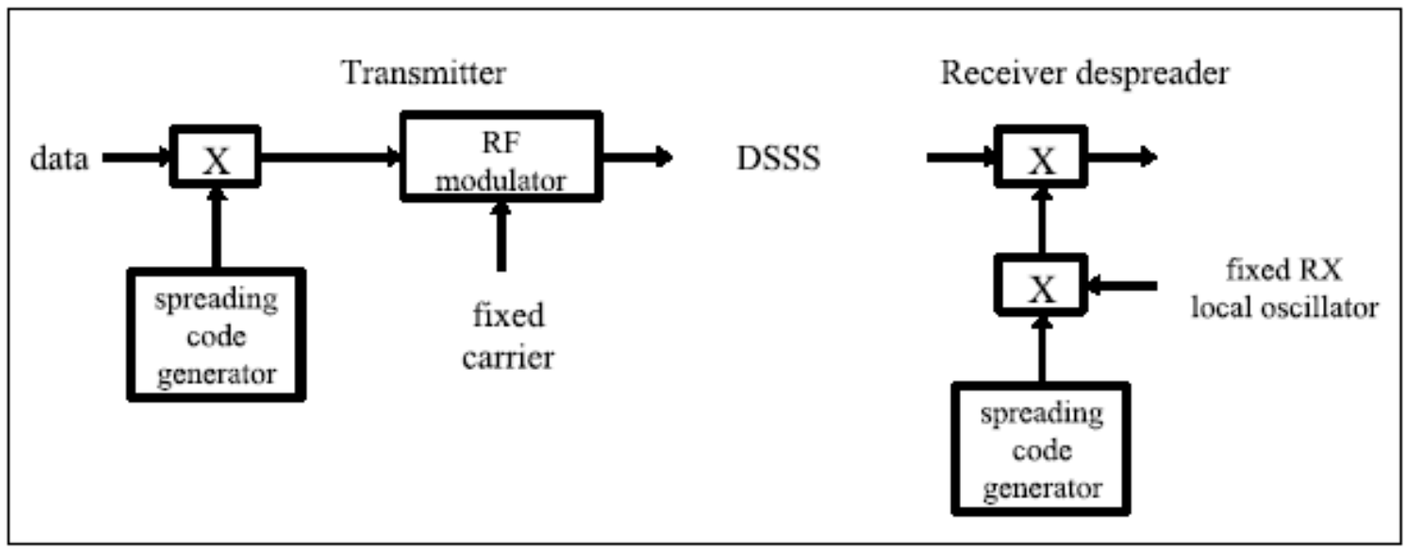


spread signal



Direct Sequence Spread Spectrum

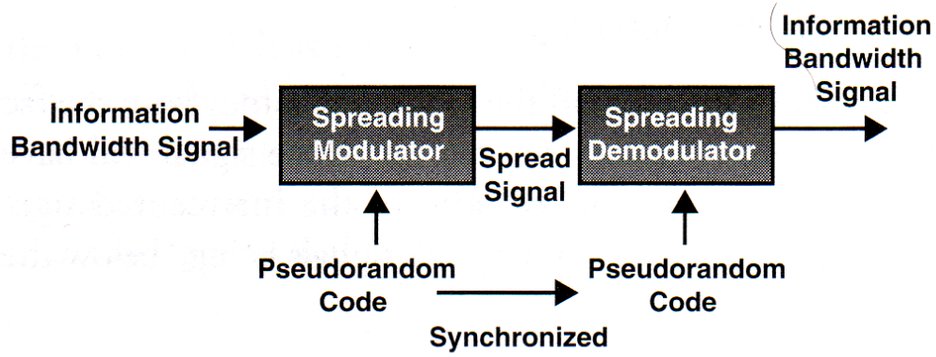
- Spreading and Modulation

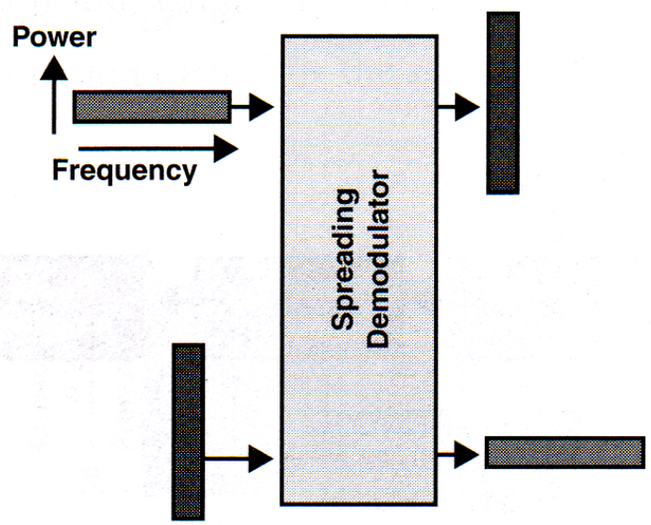


- Spreading code is produced by a spreading code generator
- Some systems operate with public spreading codes (to mitigate interference)
- For anti-jamming purposes, pseudo random sequences need to be long and infrequently repeat (wide spread)
- They need to have *good auto and cross correlation properties*

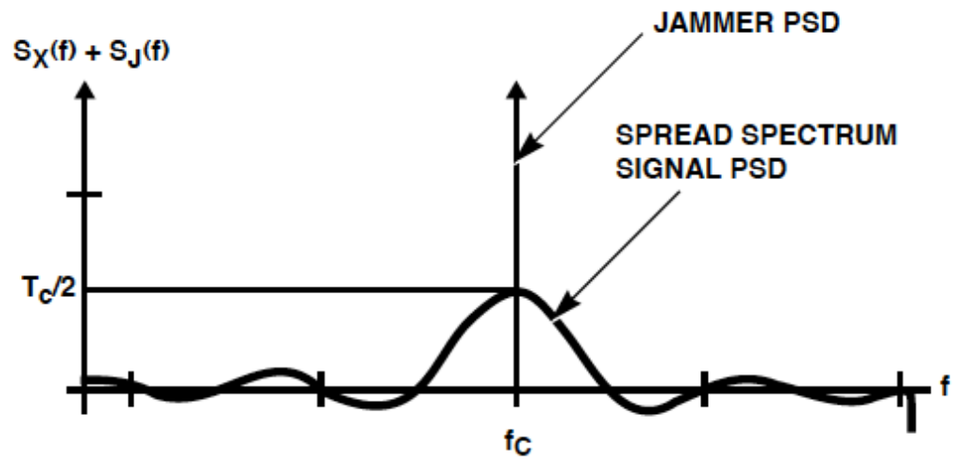
Direct Sequence Spread Spectrum

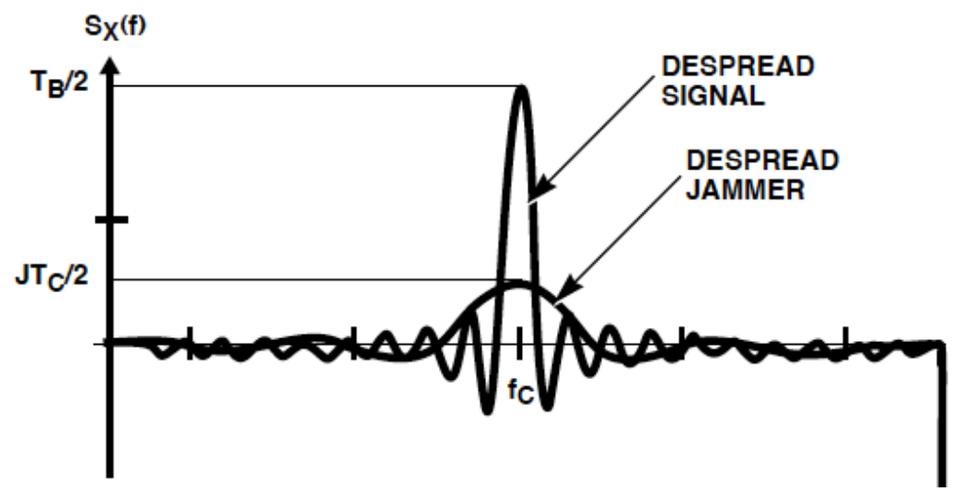
- DSSS under Narrow-band Jamming
  - Using a code on a narrow-band jamming signal spreads the signal (cross/auto correlation properties of the codes).





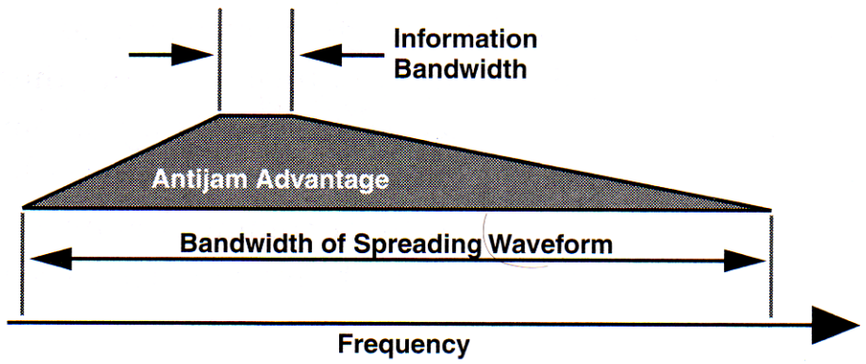
The same process that collapses the frequency spectrum of the spread-spectrum signal back to its information bandwidth spreads any nonsynchronized signal by the same factor.





Direct Sequence Spread Spectrum

- *DSSS under Narrow-band Jamming*
  - Jamming margin

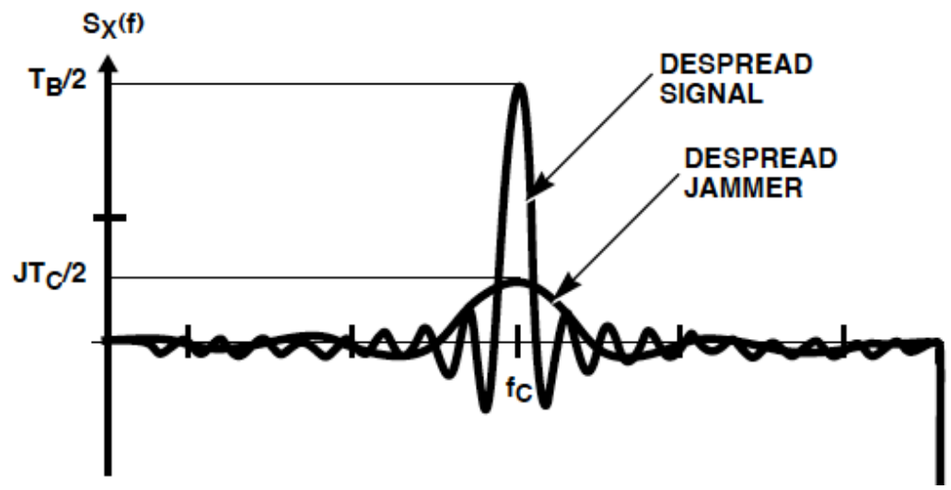


In order to jam a spread-spectrum signal, it is necessary to get sufficient jamming energy through the despreading process, which discriminates against nonsynchronized signals by the ratio of the spreading bandwidth to the information bandwidth.

Jamming margin: $M_J = G_P - L_{SYS} - SNR_{OUT}$

where

M_J = the jamming margin (in decibels);
G_P = the processing gain (in decibels);
L_{SYS} = the system losses (in decibels);
SNR_{OUT} = the required output SNR.

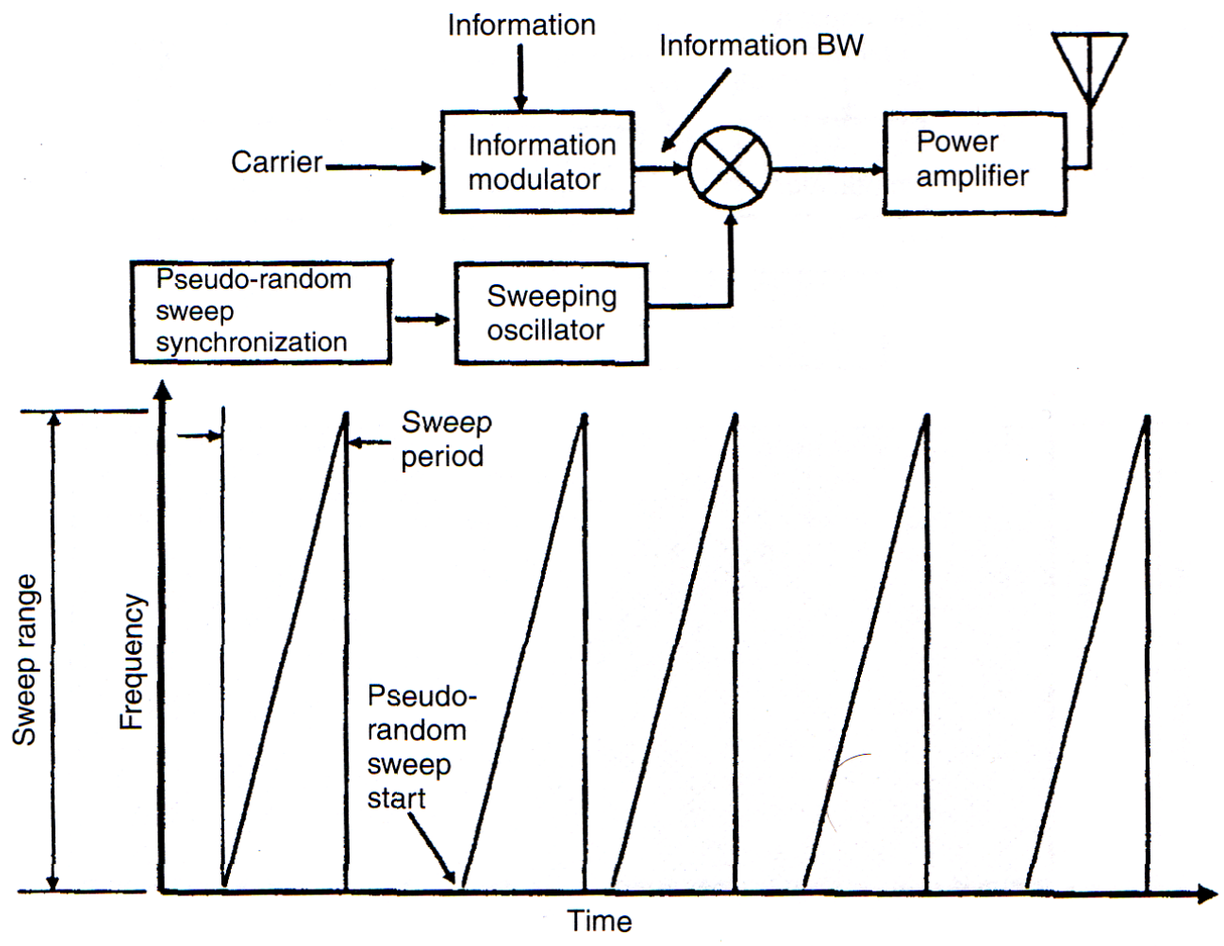


Direct Sequence Spread Spectrum

- Summary
  - DSSS hides the signal in noise
  - Signal detection is now more difficult (w/o code)
    - Can be done through energy detection (requires strong signal) or signal characteristic (constant chip rate)
      (Dillard&Dillard, Detectability of Spread Spectrum Signals, 1989)
  - Signal interception/modification difficult - LPI
  - Narrowband jamming now requires much higher power
  - Broadband jamming still effective (if you have enough power)

Chirp Signals

- Random start and then sweep ... (can be used with FH)
  - Prevents narrow-band and partial-band jamming
  - Follower jammers might be an issue



Chirp signals are rapidly swept over a frequency much wider than the information bandwidth of the transmitted signals.

Jamming

- *Jamming is power play with hide and seek*
  - Difficult to defend against can be only made more difficult
  - Typically combined with jammer detection and “neutralization”

e.g. Jamming 802.11b

- 802.11b uses DSSS
  - spreading codes are publicly known
  - e.g. Barker sequence for 802.11b at 1Mbps and 2Mbps = “1 0 1 1 0 1 1 1 0 0 0”
  - spreading codes are the same for all channels
- Jamming
  - jammer knows the codes and therefore can jam any channel by transmitting symbols using the same codes ...
  - even if the attacker uses adjacent channels the throughput will be affected
  - there is no solution for this DoS attack on 802.11