Defeating Spread Spectrum Communication with Software Defined Radio

Michael Ossmann
Great Scott Gadgets

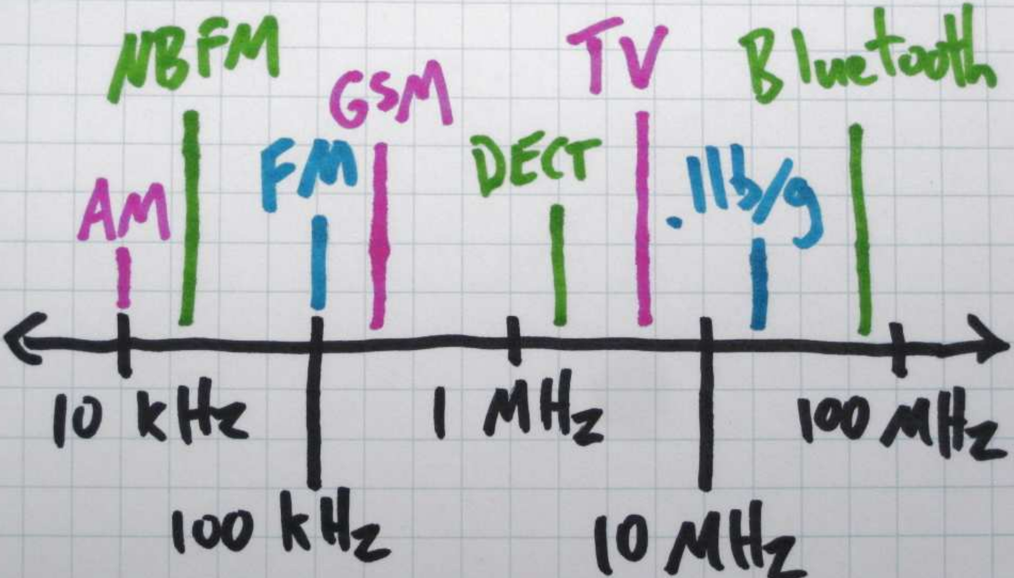
EDSC 2013

Spread Spectrum Communication

using more RF bandwidth than necessary in exchange for some benefit "bandwidth"

width (in Hz) of the range of frequency components of a signal

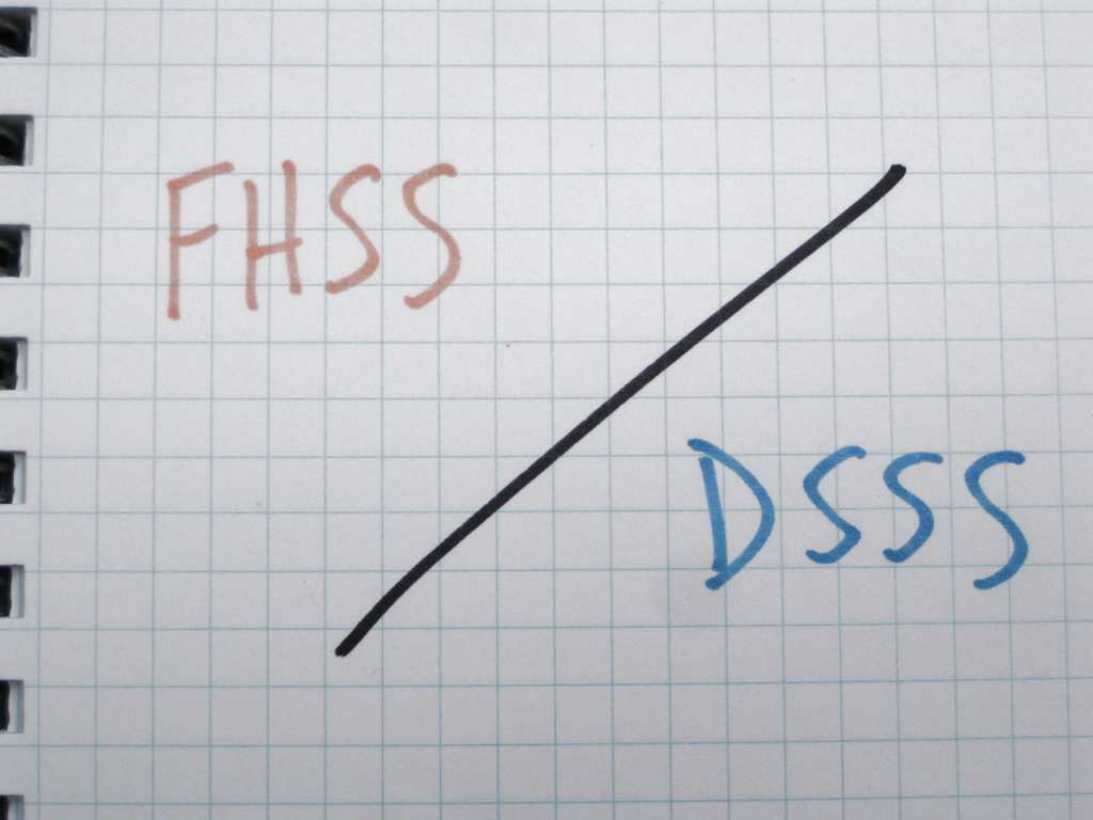
bandwidth


NBFM
GSM
TV
Bluetooth
FM
DECT
AM
.11b/g
10 kHz
100 kHz
1 MHz
10 MHz
100 MHz

Spread Spectrum Benefits

"the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density"

—Wikipedia



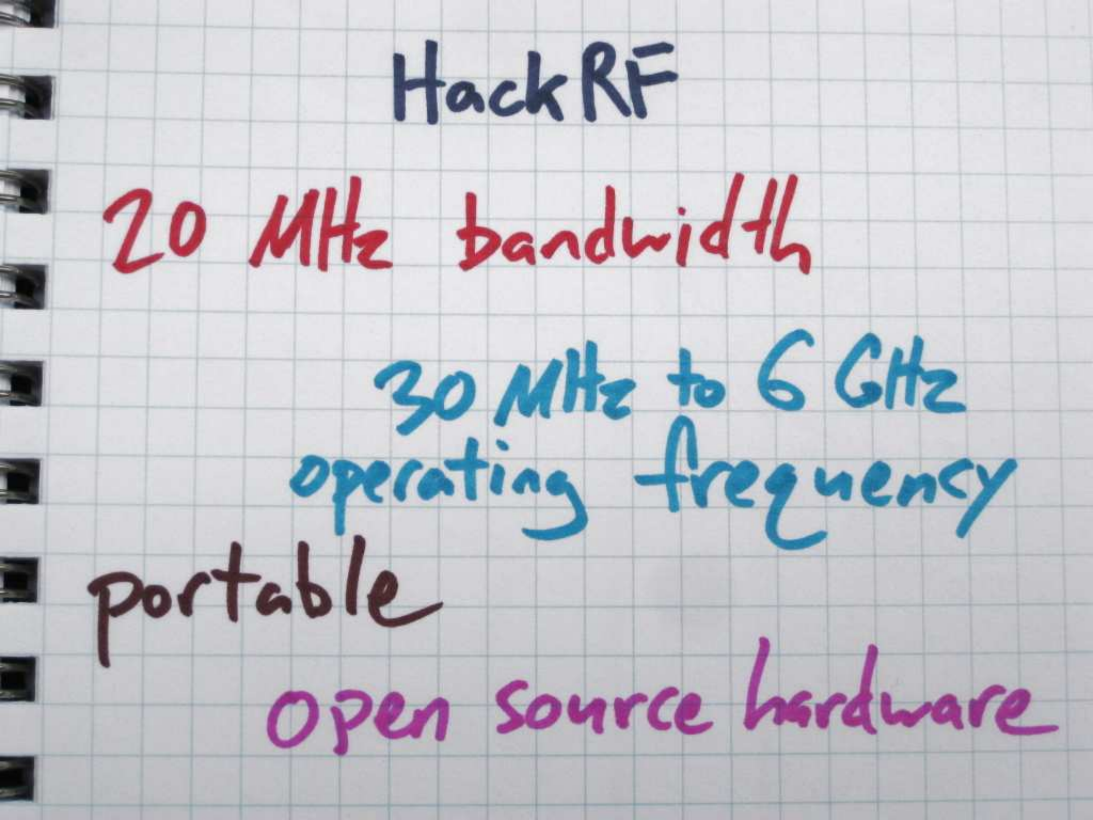
FHSS

DSSS

Software Defined Radio (SDR)

radio implemented with Digital Signal Processing (DSP)

HackRF Jawbreaker
6 December 2012
http://greatscottgadgets.com/hackrf/
P4 ANTENNA
P29 CPLD_JTAG
XILINX



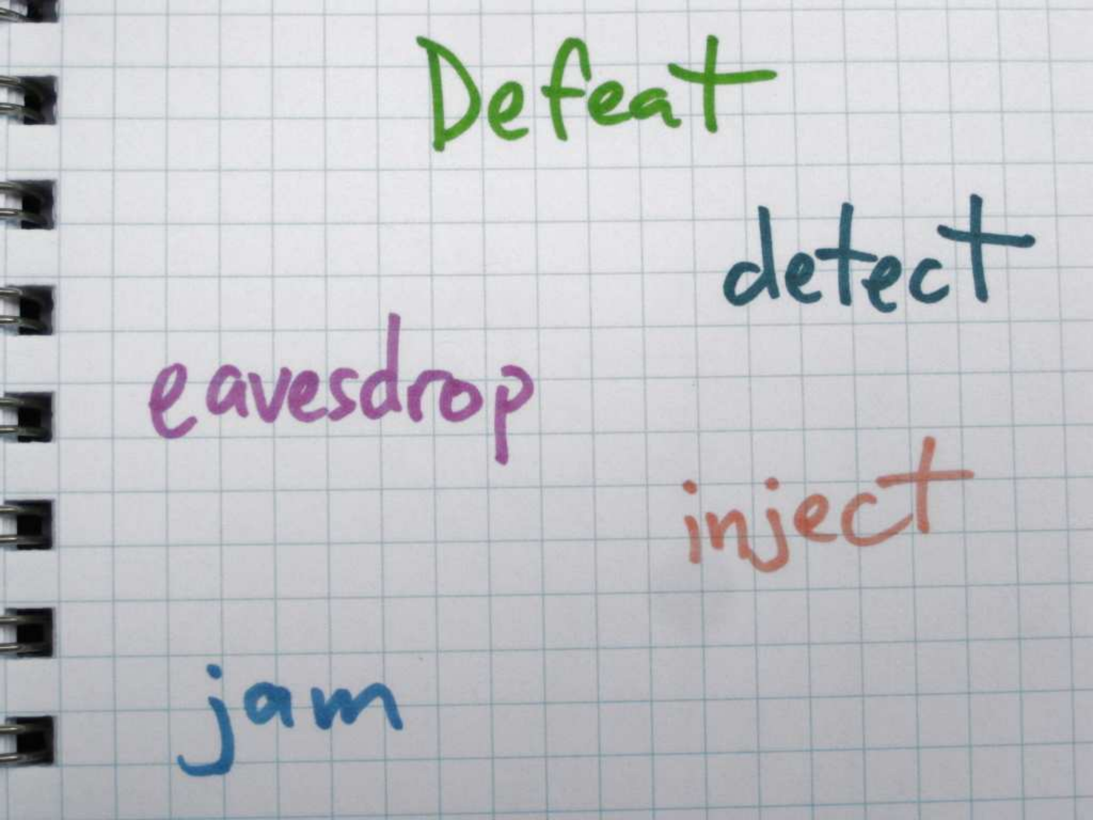
HackRF

20 MHz bandwidth

30 MHz to 6 GHz
operating frequency

portable

open source hardware



Defeat

detect

eavesdrop

inject

jam

FHSS

Frequency Hopping

Spread Spectrum

Secret Frequencies

Nevil Maskelyne

vs.

Guglielmo Marconi

1903

"I can tune my instruments so that no other instrument that is not similarly tuned can tap my messages."

— Marconi

"There was a young
fellow of Italy
who diddled the public
quite prettily."

—Maskelyne

Nikola Tesla

1903 patent: "Method of Signaling"

"without any danger of the signals or messages being disturbed, intercepted, interfered with in any way."

George Antheil and Hedy Lamarr

1942 patent:

"Secret Communication System"

player piano mechanism

FHSS Today

Classic Bluetooth

Bluetooth Low Energy (aka Bluetooth Smart)

802.11 FHSS

proprietary systems

Defeating FHSS

hop-along

all channels

intentional aliasing

Hop-along

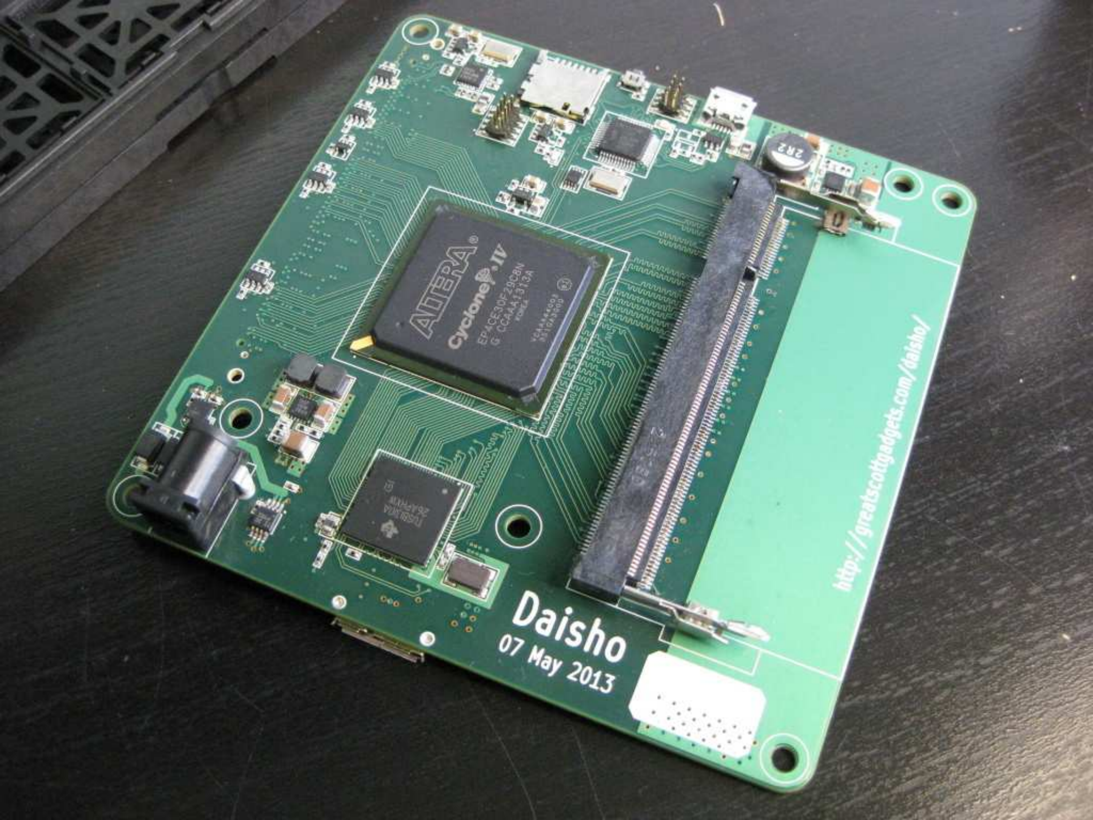
Can implement without SDR: Ubertooth
hedyattack

hopping sequence predicted from sparse observations

All Channels

SDR can transmit or receive on many channels simultaneously

eavesdrop or jam without predicting hopping sequence


ALTERA
Cyclone IV
EP4CE30F29C8N
G CCAAA1313A
Daisho
07 May 2013
http://greatscottgadgets.com/daisho/
2R2

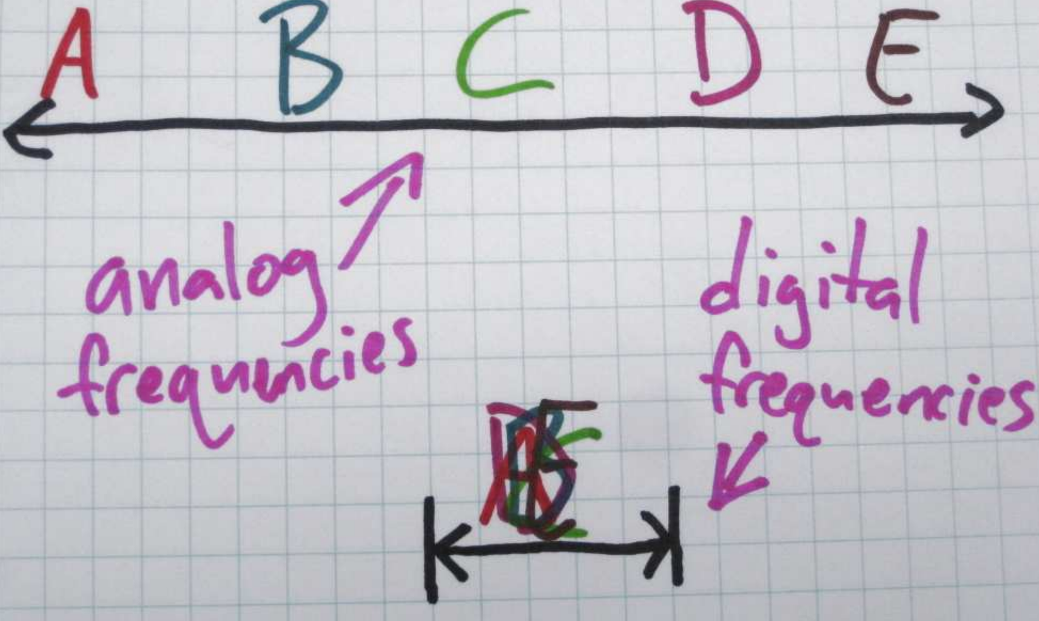
Intentional Aliasing

Building an All-Channel Bluetooth Monitor

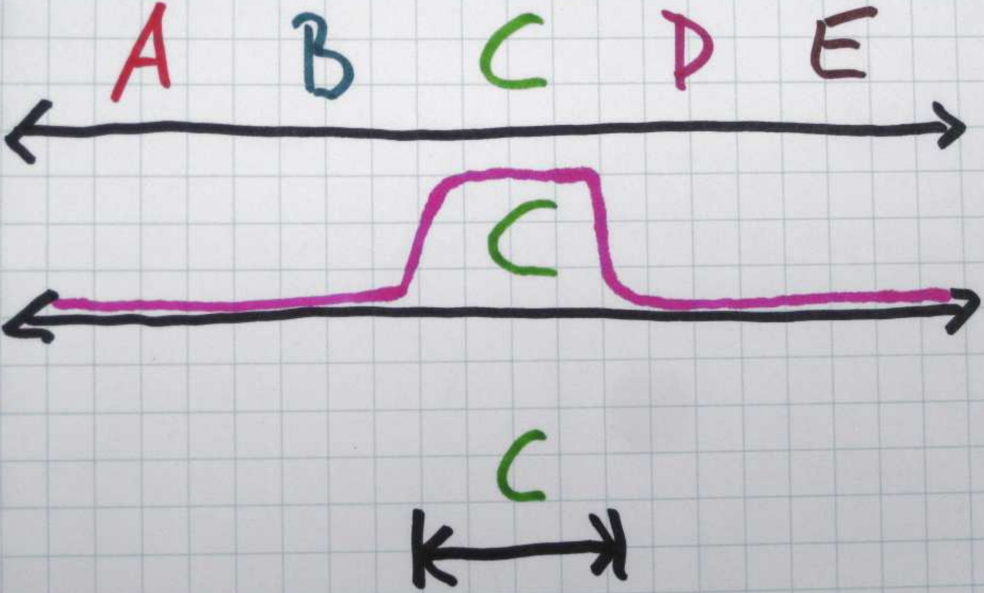
Ossmann and Spill

ShmooCon 2009

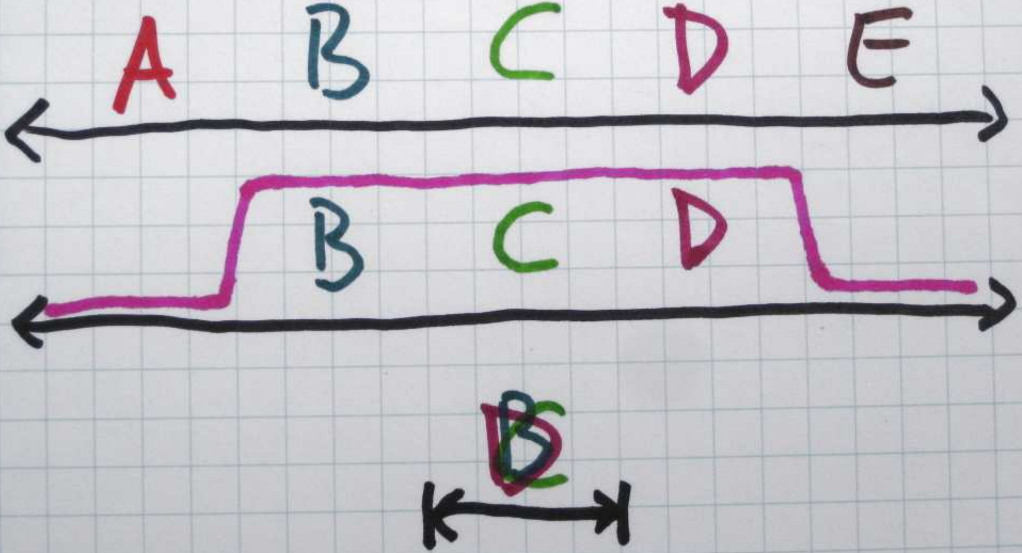
Aliasing

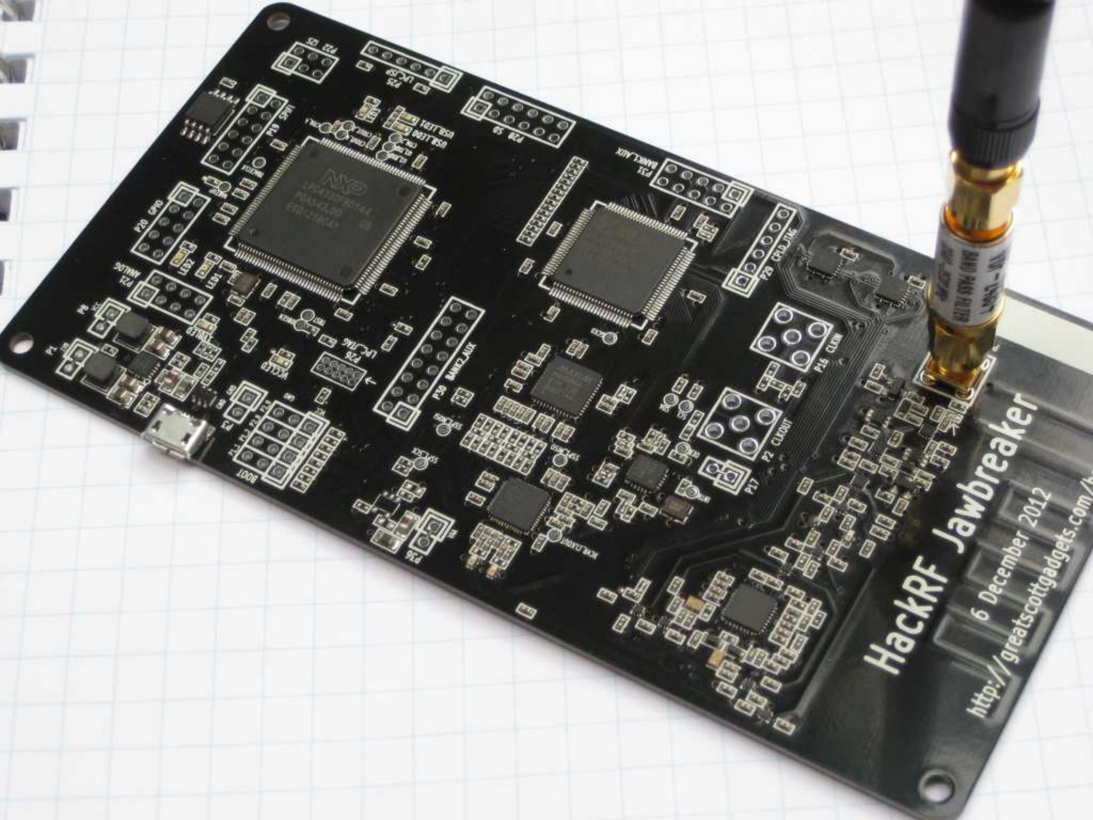


Anti-aliasing Filter

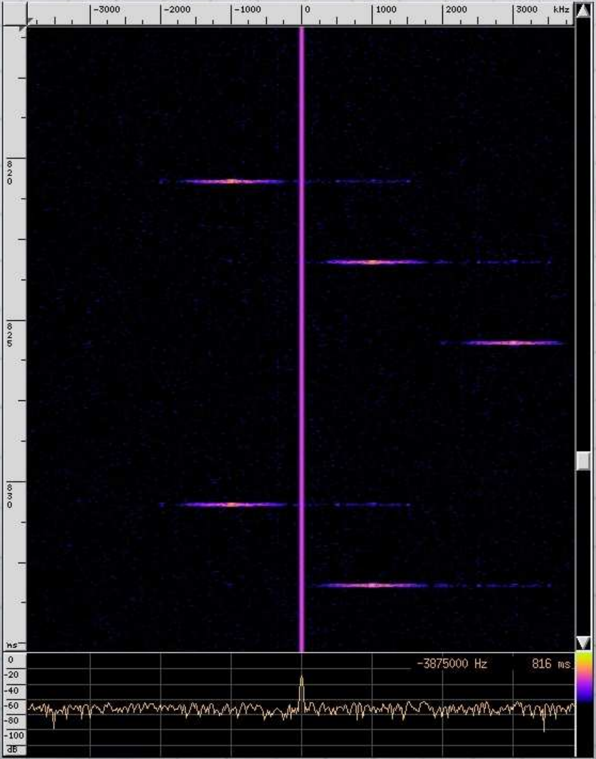


Intentional Aliasing

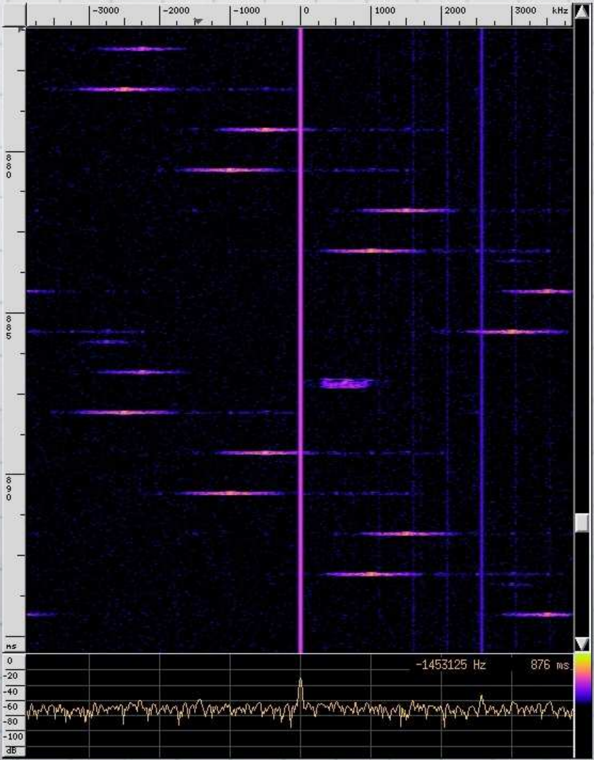



HackRF Jawbreaker
6 December 2012
http://greatscottgadgets.com/h
NXP
P20 GPIO
P21 ANALOG
P19 SPIFI
P22 I2S
P25 LPC_ISP
P28 SD
P31 BANK1_AUX
P29 CPLD_JTAG
P30 BANK2_AUX
P26 LPC_JTAG
P16 CLKIN
P2 CLKOUT
P17
P35
BOOT
LED1
LED2
LED3
VCCLED
USB_LED0
USB_LED1
BAND PASS FILTER

Without Aliasing



With Aliasing



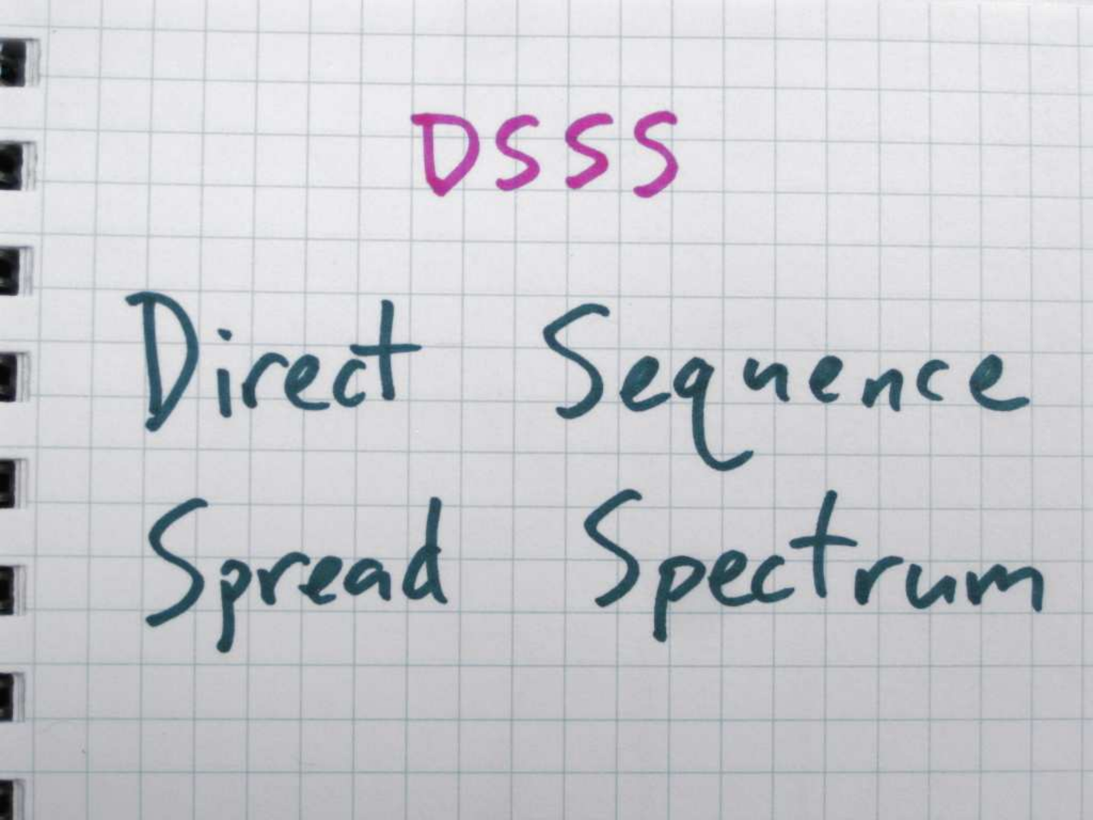
HackRF

maximum filter bandwidth: 30.8 MHz

great for FHSS in the 902 to 928 MHz ISM band

FHSS Defeated

Can detect, eavesdrop, inject, and jam with any of the three techniques (but I don't recommend TX with intentional aliasing)

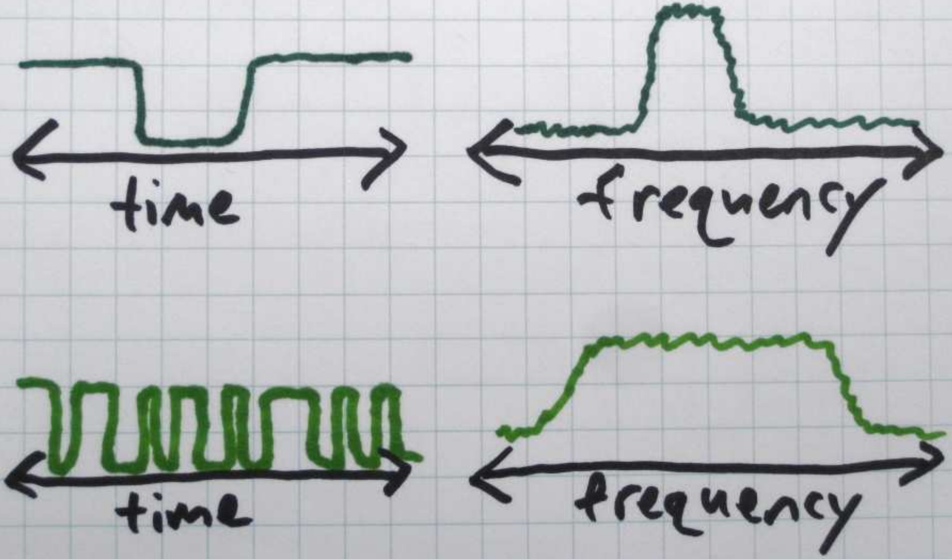


DSSS

Direct Sequence

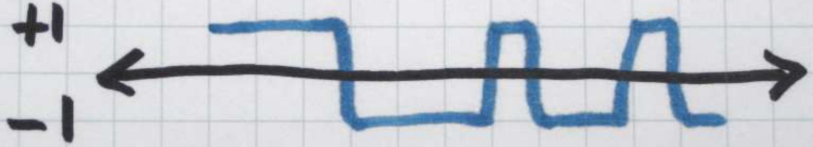
Spread Spectrum

More bps → Wider Bandwidth

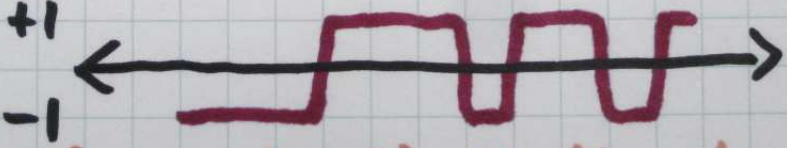


A Bunch of Chips for Every Bit

to send 1:

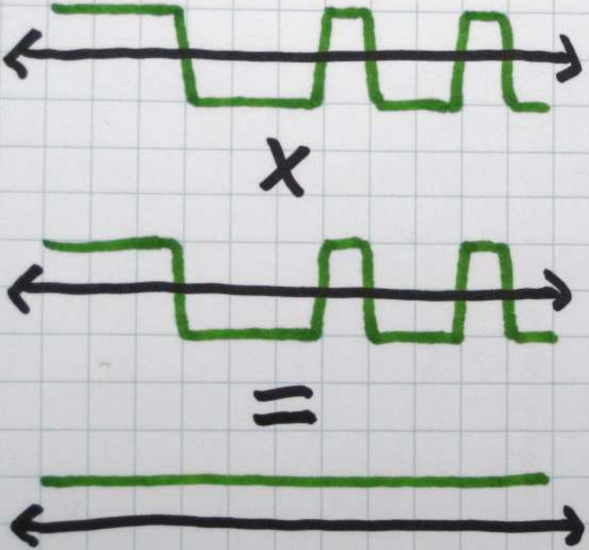


to send 0:



1 Mbps → 11 M chips/s

Correlation



multiply

accumulate

(11)

DSSS Examples

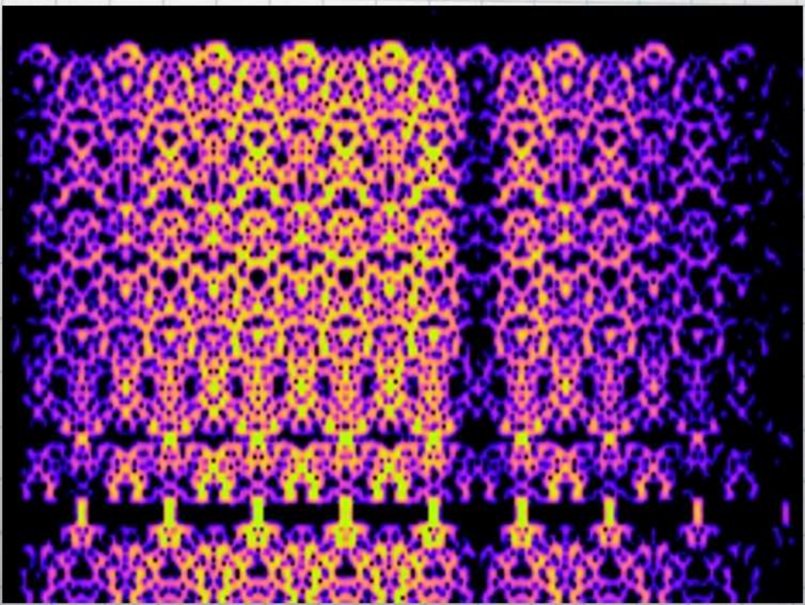
802.11 b/g (especially management frames)

802.15.4 (ZigBee)

GPS

proprietary systems

Spotting DSSS



Wideband Jamming

DSSS immune to
narrowband jamming

but vulnerable to
wideband jamming

SDR can do either

and can transmit random codes

Weak Signal Detection

"below the noise floor"

directional antennas

math

multiple antennas

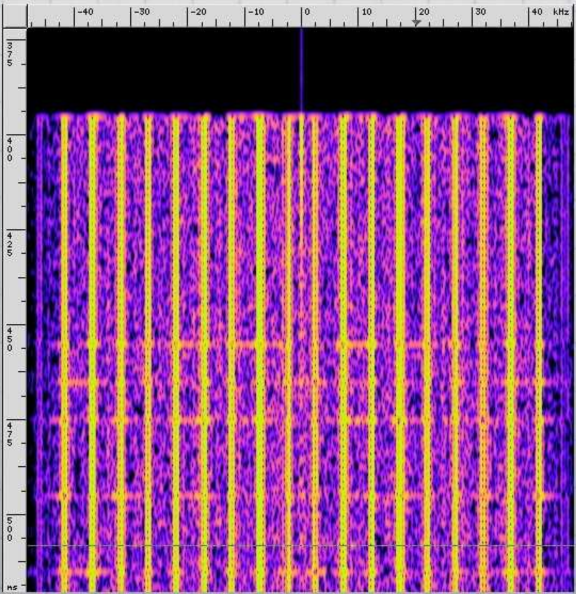
SOS
spot
CONNECT

Code Determination

code needed for eavesdropping and injection

autocorrelation

Insufficient Bandwidth



3 Air Interface

The STX2 complies with the following air interface specifications:

3.1 Modulation

3.1.1 Description

The information data bit shall be XOR-ed with a pseudo random sequence (PN code) to create a DSSS waveform.

The PN sequence is the following maximal length sequence:

- 255 chip PN sequence

PN chip transitions are synchronized with the RF carrier transitions.

The nominal PN rate is 1.25 Mcps with a nominal Bit Rate of 100.04 bps.

3.1.2 Quality

The EVM (Error Vector Magnitude) is less than 15 % RMS for 1020 symbols. This corresponds to an RMS phase error of less than 18 degrees and a magnitude error of less than 10%.

The unit of service of the STX2 is a message. Depending on the length of a message, a message may be split in several Air Interface Packets. The STX2 manages the function of the on-air protocol, so users need not concern themselves much with this section except to understand how the STX performs its function for design timing considerations.

The Air Interface Packet structure is as follows (the preamble is transmitted first). User data is concatenated with housekeeping information to create an Air Interface Packet.

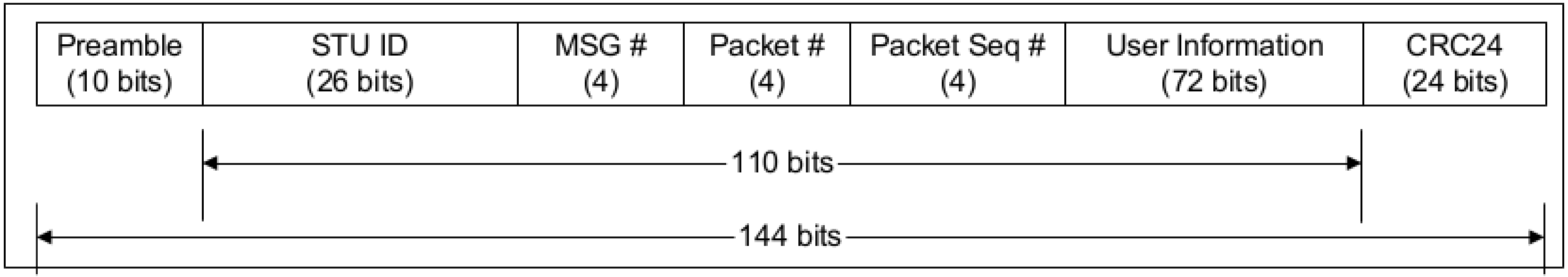
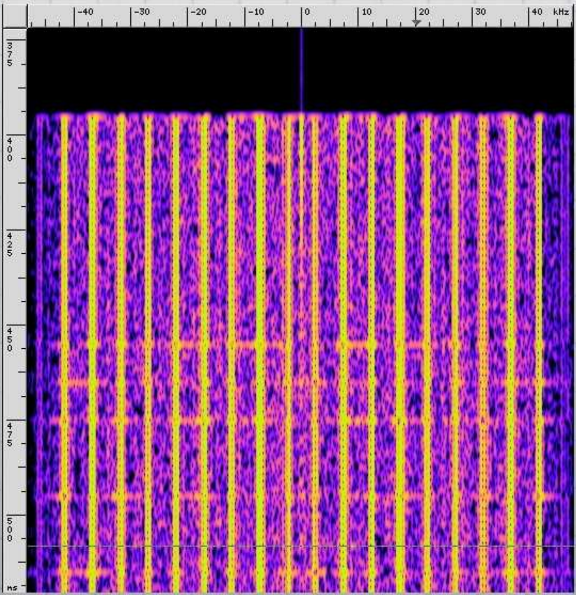


Figure 4, Packet On-Air Structure

Table 1, Air Interface Packet Fields

Preamble (10)	Consists of the 10-bit binary bit pattern 0000001011 Leftmost bit is sent first
STX ID (26)	3 bits for manufacturer ID (000) and 23 bits for unit ID
Message Number (4)	Message number modulo 16. The message number of the last message transmitted shall be saved in non-volatile memory This number is NOT reset upon new configuration.
Packet Number (4)	Number of packets in a message. This is used for messages longer

Insufficient Bandwidth



DSSS Defeated

can detect, eavesdrop, inject, and jam

Spread Spectrum Communication

not for security

Questions

http://greatscottgadgets.com/