SDR/Software Defined Radio for Maritime Applications

Maritime Hacking Village

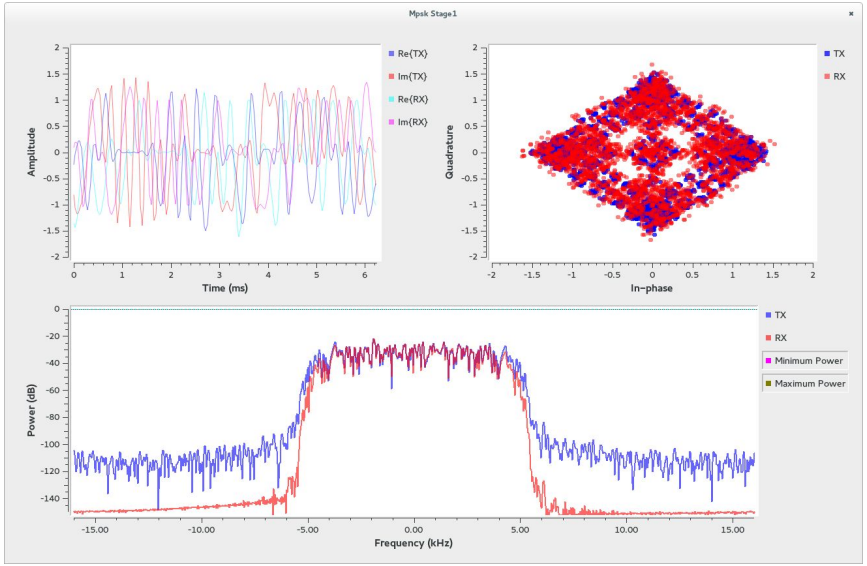
UNCW MCH

December 16, 2025

Part 1: Intro to SDR/Software Defined Radios

SDR: GNU Radio

- Most popular general purpose SDR software suite/ development environment
- Released 2001
- Dataflow oriented programming environment
- Support for C++ and Python bindings
    - Additional language support through FFI
- Compute intensive blocks are typically written in C++, abstractions in Python or the visual language
- Module structure for visualization, sources, sinks, transforms, etc.



GNU Radio: Language Bindings

```cpp
#ifdef HAVE_CONFIG_H
#include "config.h"
#endif

#include <gnuradio/io_signature.h>
#include <gnuradio/pdu.h>
#include "websocket_pdu_impl.h"

namespace gr
{
    namespace ais_simulator
    {

        /*
         * Get on correct executor.
         */
        void session::run()
        {
            // We need to be executing within a strand to perform async operations
            // on the I/O objects in this session. Although not strictly necessary
            // for single-threaded contexts, this code is written to be thread-safe
            // by default.
            net::dispatch(d_ws.get_executor(),
                          beast::bind_front_handler(
                              &session::on_run,
                              shared_from_this()));
        }

        /*
         * Close websocket.
         */
        void session::close()
        {
            if (d_ws.is_open())
            {
                d_ws.close(websocket::close_code::normal);
            }
        }
```

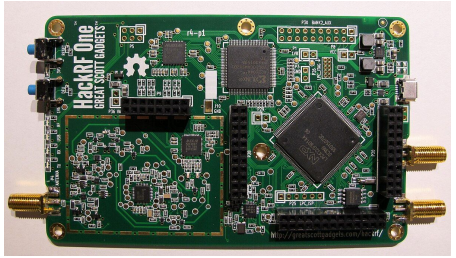
```python
class top_block(gr.top_block):
    def __init__(self, c, amp, lna, sr, br, ppm, ip, port):
        gr.top_block.__init__(self, 'AIS Simulator')

        # Blocks
        osmosdr_sink_0 = osmosdr.sink(args="numchan=" + str(1) + " " + '')
        osmosdr_sink_0.set_sample_rate(sr)
        osmosdr_sink_0.set_freq_corr(ppm, 0)
        osmosdr_sink_0.set_center_freq(161975000 + 50000 * c, 0)
        osmosdr_sink_0.set_gain(14 if amp else 0, 0)
        osmosdr_sink_0.set_if_gain(lna, 0)
        osmosdr_sink_0.set_bb_gain(16, 0)
        osmosdr_sink_0.set_antenna("", 0)
        digital_gmsk_mod_0 = digital.gmsk_mod(
            samples_per_symbol=int(sr / br),
            bt=0.4,
            verbose=False,
            log=False,
        )
        websocket_pdu_0 = ais_simulator.websocket_pdu(ip, str(port))
        blocks_pdu_to_tagged_stream_0 = pdu.pdu_to_tagged_stream(gr.types.byte_t, 'packet_len')
        blocks_multiply_const_vxx_0 = blocks.multiply_const_vcc((0.9, ))
        ais_build_frame = ais_simulator.bitstring_to_frame(True, 'packet_len')

        # Connections
        self.msg_connect((websocket_pdu_0, 'out'), (blocks_pdu_to_tagged_stream_0, 'pdus'))
        self.connect((blocks_pdu_to_tagged_stream_0, 0), (ais_build_frame, 0))
        self.connect((ais_build_frame, 0), (digital_gmsk_mod_0, 0))
        self.connect((digital_gmsk_mod_0, 0), (blocks_multiply_const_vxx_0, 0))
        self.connect((blocks_multiply_const_vxx_0, 0), (osmosdr_sink_0, 0))
```

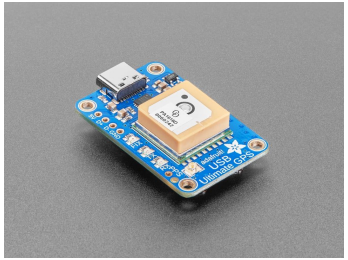
Basic SDR Demo: Today's Hardware

- HackRF + PortaPack loaded with Mayhem firmware
  - Roughly one per student; working in pairs and pairs of pairs
- dAISy 2+ AIS receiver
  - Several floating around the room; limited supply
- Adafruit GPS receiver
  - One per 4 students
- SMA cables + attenuators to hook everything up

- **ALL TRANSMISSION, UNLESS OTHERWISE NOTED, MUST BE DONE USING A WIRED CONNECTION**

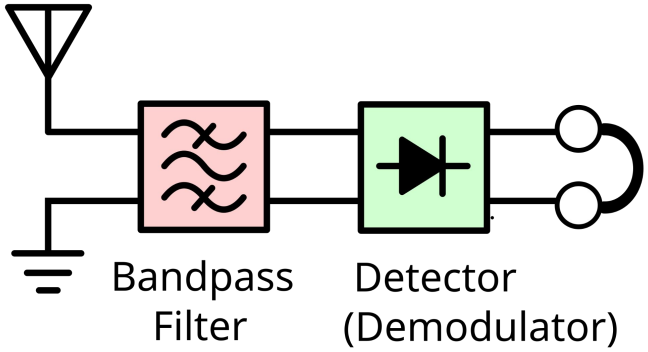
- **OVER-THE-AIR, UNAUTHORIZED TRANSMISSION OF SPOOFED/MALICIOUS AIS, GPS, OR OTHER FCC RESTRICTED FREQUENCY BANDS IS ILLEGAL**

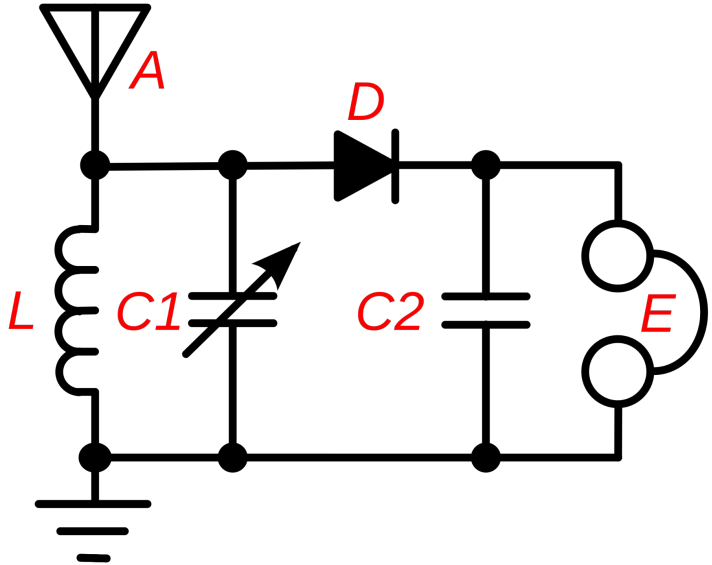




RF Basics: Simple Crystal Radio

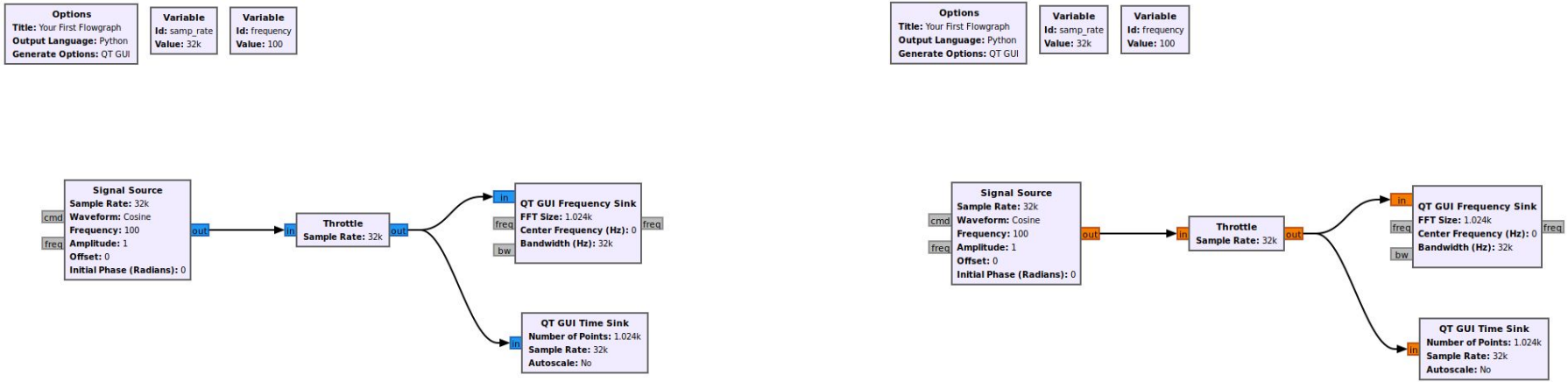
- A: antenna
- L: tuning coil
- D: crystal detector; rectifies RF current to pulses
- E: speaker

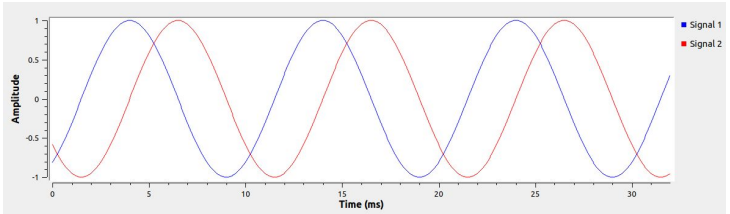


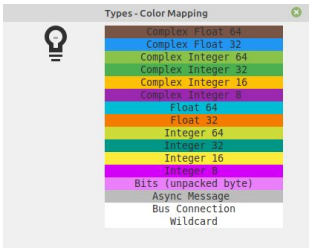


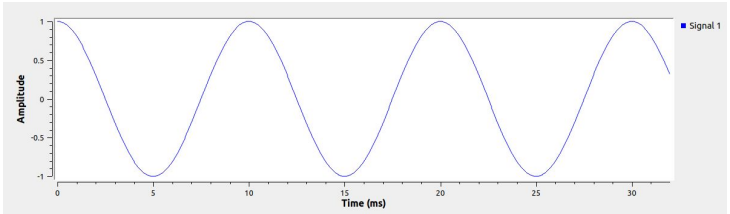
Demo Time: Basic FM Receiver

FM Demo: Visual Environment Basics

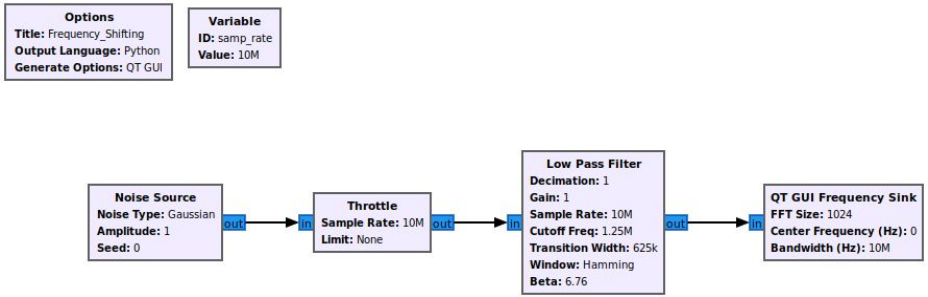


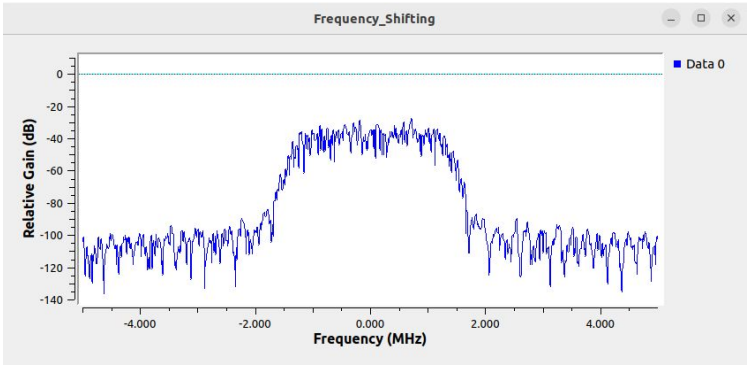


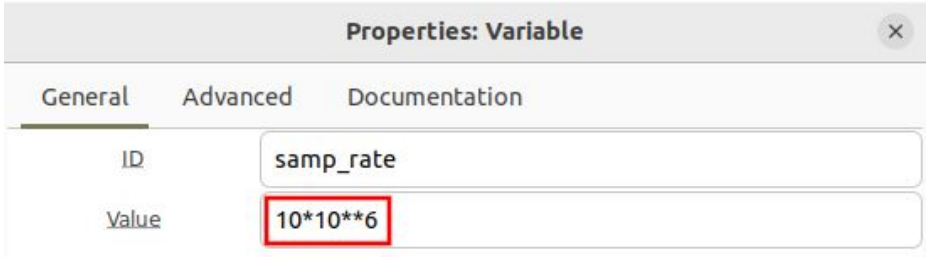


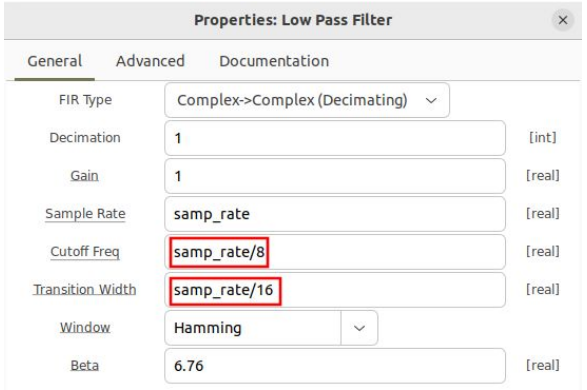


FM Demo: Basic Filtering









FM Demo: Getting Started

Channel Rate

Incoming sample rate of the FM baseband (integer)

Audio Decimation

Input to output decimation rate (integer)

Deviation

Maximum FM deviation (default = 75000) (float)

Audio Pass

Audio low pass filter passband frequency (float)

Audio Stop

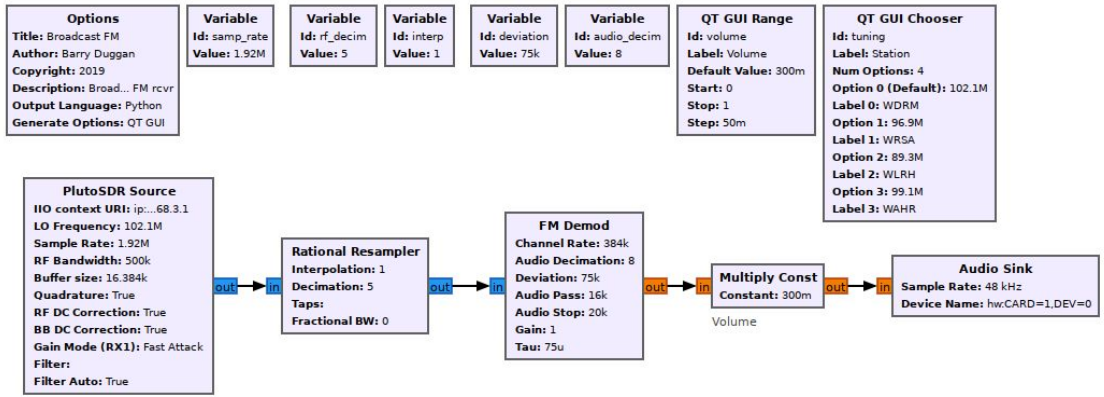
Audio low pass filter stop frequency (float)

Gain

Gain applied to audio output (default = 1.0) (float)

Tau

De-emphasis time constant (default = 75e-6), specify tau=0.0 to prevent de-emphasis (float)



Demo Time: Dataflow Exploration

SDR References

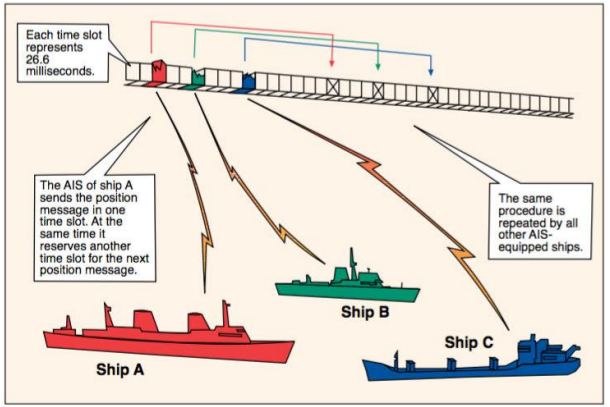
1. https://en.wikipedia.org/wiki/GNU_Radio
2. https://wiki.gnuradio.org/index.php?title=Category:Block_Docs
3. https://wiki.gnuradio.org/index.php/Tutorials
4. https://github.com/portapack-mayhem/mayhem-firmware

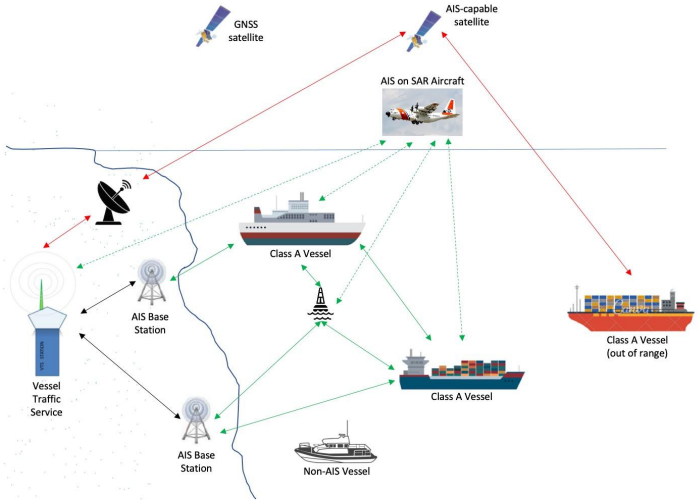
Part 2: Maritime SDR

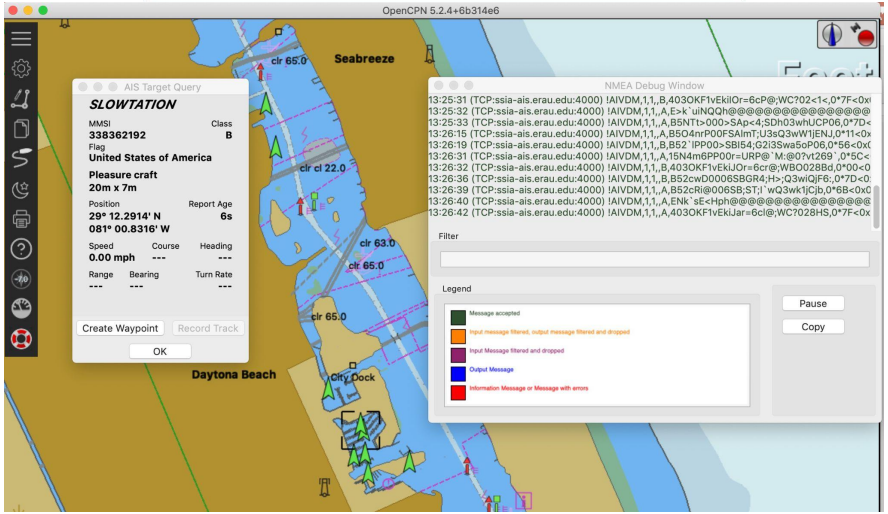
AIS

AIS: Recap

- 161.975 MHz, 162.025 MHz
- GMSK
- TDMA
- 25 kHz bandwidth
- AIVDM line format





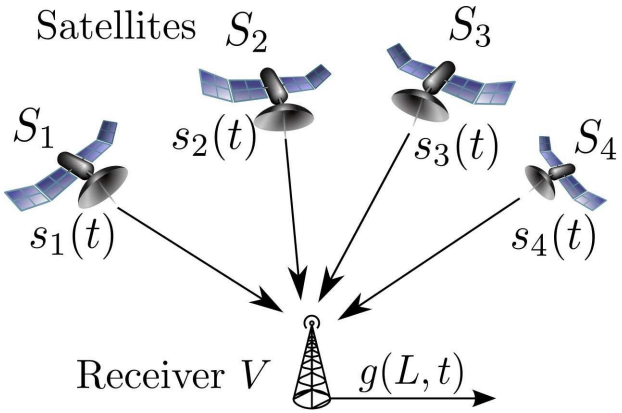


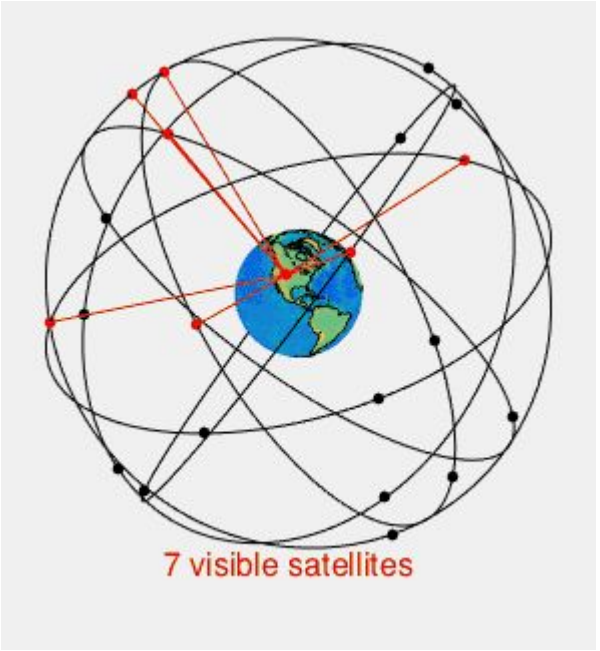
Demo Time: AIS Spoofing

AIS References

1. https://github.com/liberasinc/dc32-ics-ais
2. https://www.garykessler.net/library/ais_pi.html
3. https://github.com/bistromath/gr-ais
4. https://www.opencpn.org

GPS





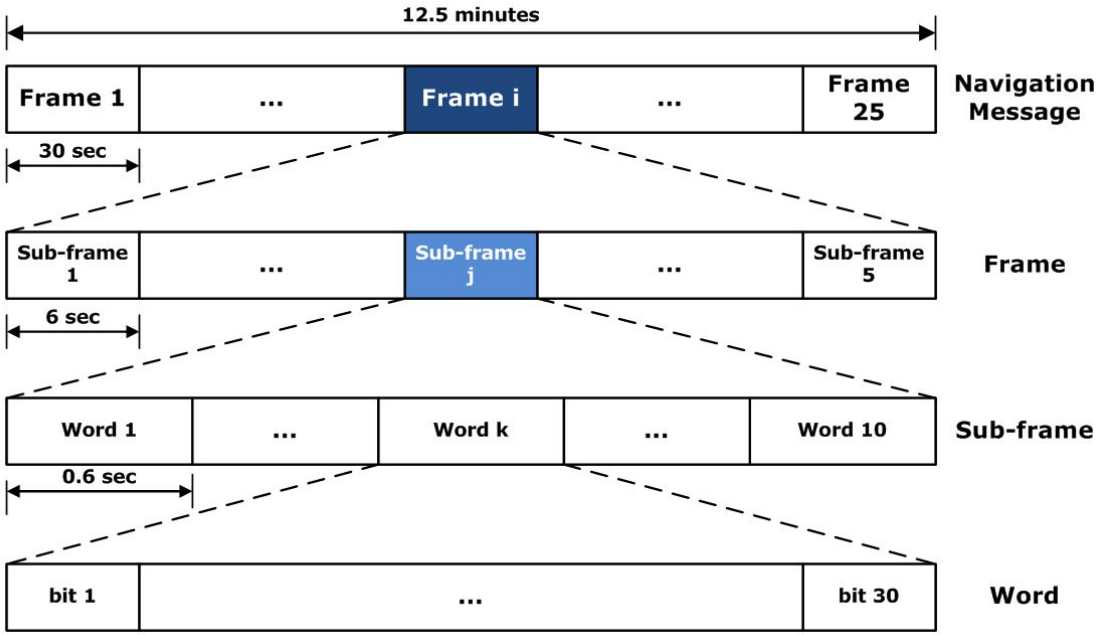
GPS Wiki Figure Dump: Bands

Band	Frequency	Description
L1	1575.42 MHz	Coarse-acquisition (C/A) and encrypted precision (P(Y)) codes, plus the L1 civilian (L1C) and military (M) codes on Block III and newer satellites.
L2	1227.60 MHz	P(Y) code, plus the L2C and military codes on the Block IIR-M and newer satellites.
L3	1381.05 MHz	Used for nuclear detonation (NUDET) detection.
L4	1379.913 MHz	Being studied for additional ionospheric correction.
L5	1176.45 MHz	Used as a civilian safety-of-life (SoL) signal on Block IIF and newer satellites.

Band	Frequency (MHz)	Phase	Original usage	Modernized usage
L1	1575.42 (10.23 × 154)	I	Encrypted precision P(Y) code	
		Q	Coarse/acquisition (C/A) code	C/A, L1 Civilian (L1C), and Military (M) code
L2	1227.60 (10.23 × 120)	I	Encrypted precision P(Y) code	
		Q	unmodulated carrier	L2 Civilian (L2C) code and Military (M) code
L3	1381.05 (10.23 × 135)		used by Nuclear Detonation (NUDET) Detection System Payload (NDS): signals nuclear detonations/ high-energy infrared events. Used to enforce nuclear test ban treaties.	
L4	1379.9133... (10.23 × 1214/9)		—	being studied for additional ionospheric correction
L5	1176.45 (10.23 × 115)	I	—	Safety-of-Life (SoL) Data signal
		Q		Safety-of-Life (SoL) Pilot signal

GPS: L1 C/A

Bits	Information
1–8	Preamble
9–14	PRN of transmitting satellite
15–20	Message type ID
21–37	Truncated TOW count
38	Alert flag
277–300	Cyclic redundancy check

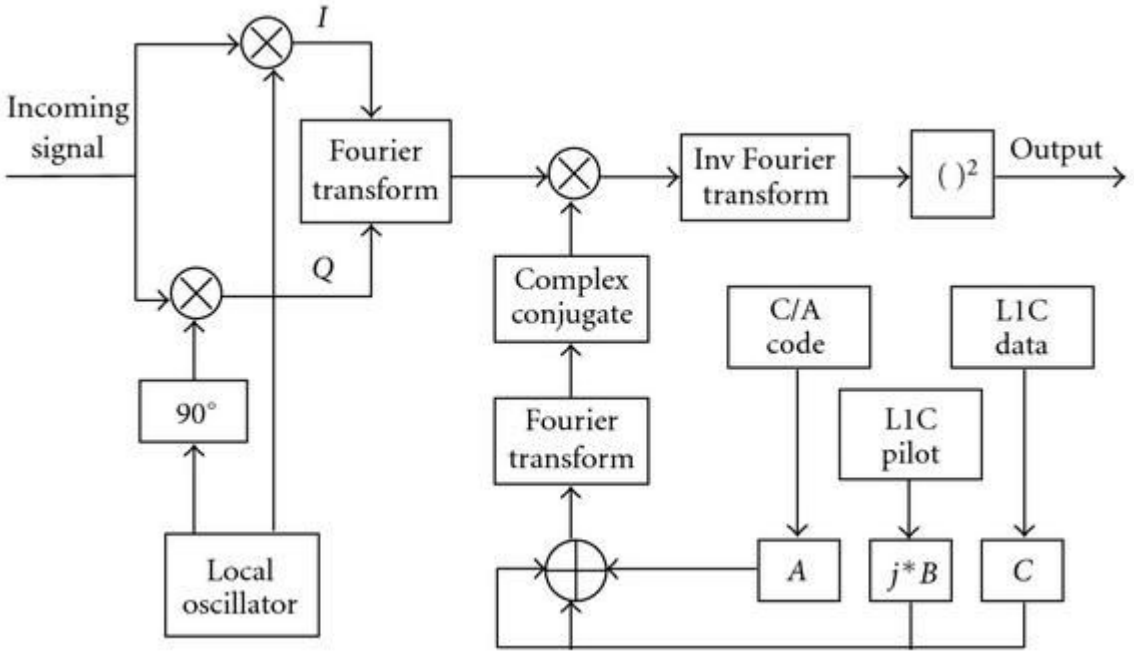


GPS: L1 C/A Message

Type ID	Description
10–11	Ephemeris and health
12, 31, 37	Almanac parameters
13–14, 34	Differential correction
15, 36	Text messages
30	Ionospheric and group delay correction
32	Earth orientation parameters
33	UTC parameters
35	GPS/GNSS time offset

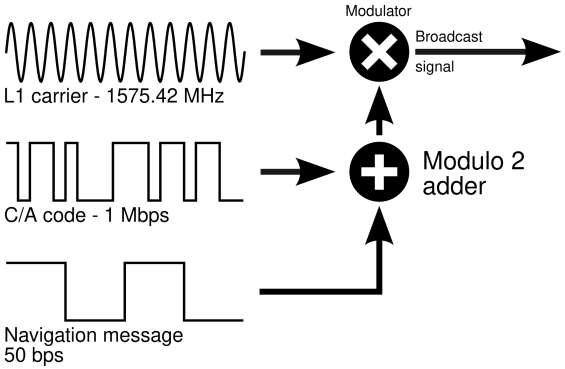
Sub-frame	Word	Description
1	1–2	Telemetry and handover words (TLM and HOW)
	3–10	Satellite clock, GPS time relationship
2–3	1–2	Telemetry and handover words (TLM and HOW)
	3–10	Ephemeris (precise satellite orbit)
4–5	1–2	Telemetry and handover words (TLM and HOW)
	3–10	Almanac component (satellite network synopsis, error correction)

GPS: L1 C/A Block Diagram

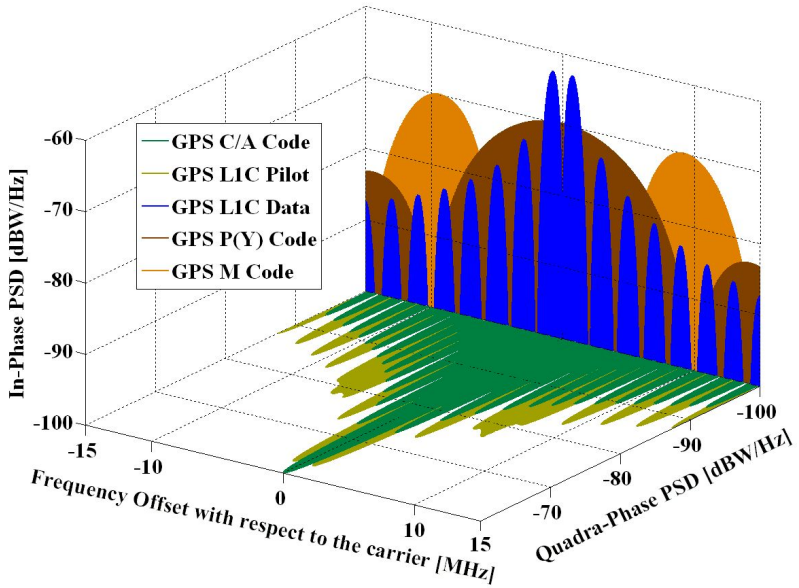


Combined GPS L1 C/A-L1C acquisition scheme. [5]

Local oscillator for the reference frequency is modulated with the target code (C/A vs. L1C).



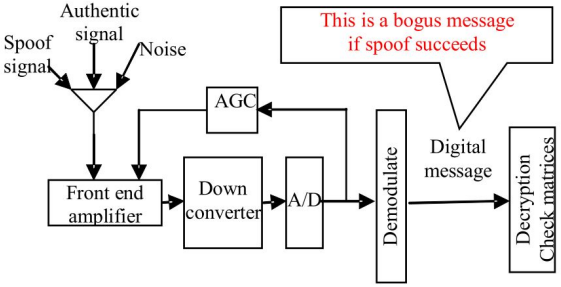
GNSS System	GPS	GPS		GPS	GPS
Service Name	C/A	L1C		P(Y) Code	M-Code
Centre Frequency	1575.42 MHz	1575.42 MHz		1575.42 MHz	1575.42 MHz
Frequency Band	L1	L1		L1	L1
Access Technique	CDMA	CDMA		CDMA	CDMA
Signal Component	Data	Data	Pilot	Data	N.A.
Modulation	BPSK(1)	TMBOC(6,1,1/11)		BPSK(10)	$BOC_{sin}(10,5)$
Sub-carrier frequency [MHz]	-	1.023	1.023 & 6.138	-	10.23
Code frequency	1.023 MHz	1.023 MHz		10.23 MHz	5.115 MHz
Primary PRN Code length	1023	10230		$6.19 \cdot 10^{12}$	N.A.
Code Family	Gold Codes	Weil Codes		Combination and short-cycling of M-sequences	N.A.
Secondary PRN Code length	-	-	1800	-	N.A.
Data rate	50 bps / 50 sps	50 bps / 100 sps	-	50 bps / 50 sps	N.A.
Minimum Received Power [dBW]	-158.5	-157		-161.5	N.A.
Elevation	5°	5°		5°	5°



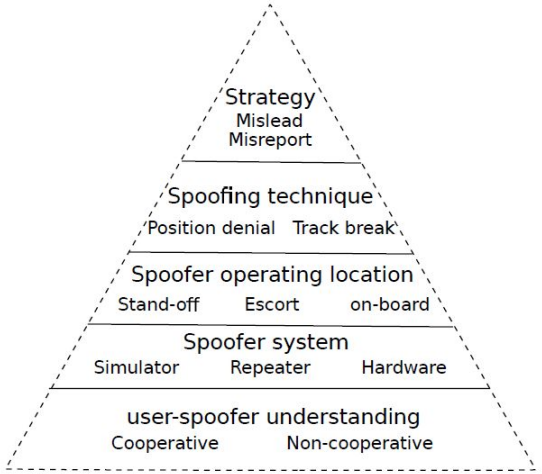
GPS: Threat Scenarios

GPS spoofing attacks can be split:

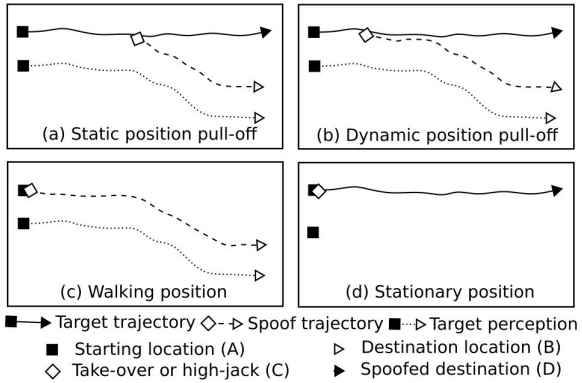
- Position denial attacks deny the target receiver from detecting authentic GPS signals
- Track break attacks provide consistently false signals to deviate the trajectory of a mobile system.



[24]



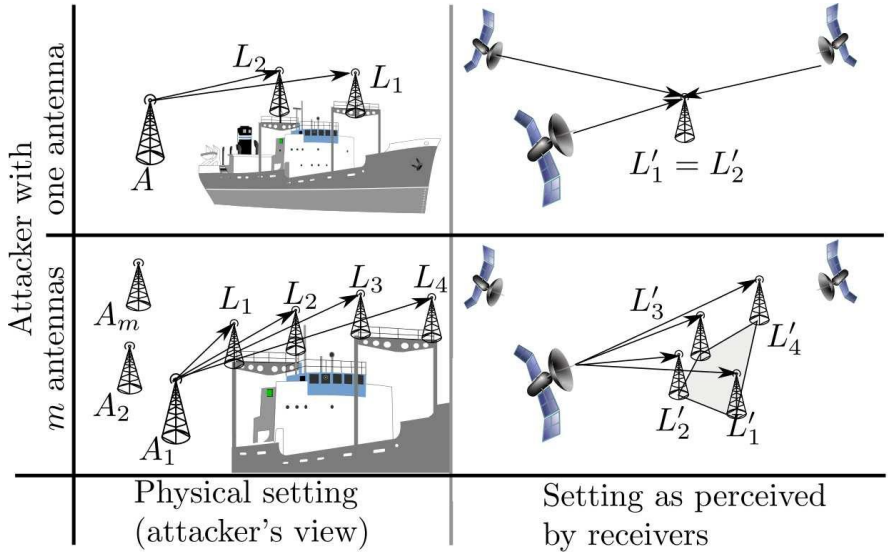
[21]



Detecting Spoofing: Signal Strength

Track signal strength across channels:

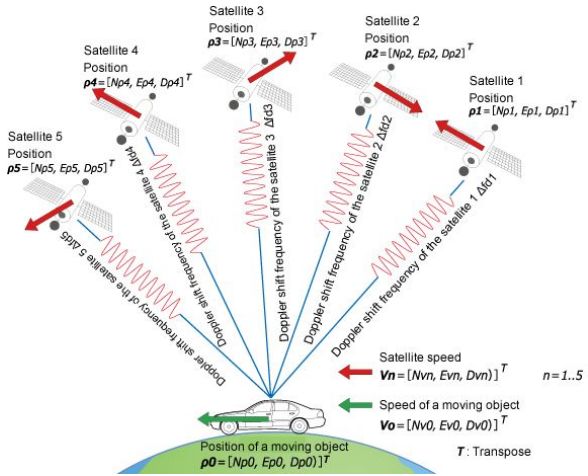
- Signal strength exceeds a pre-set threshold that a legitimate satellite will never exceed in practice
- Moving average expectation of relative signal strength from one moment to the next and alert on significant deviations
- Signal strength of each satellite in relation to each other
  - Spoofed signals would then be expected to provide near-uniform signal strength across channels
  - Legitimate satellites would be expected to have natural deviation due to signal attenuation

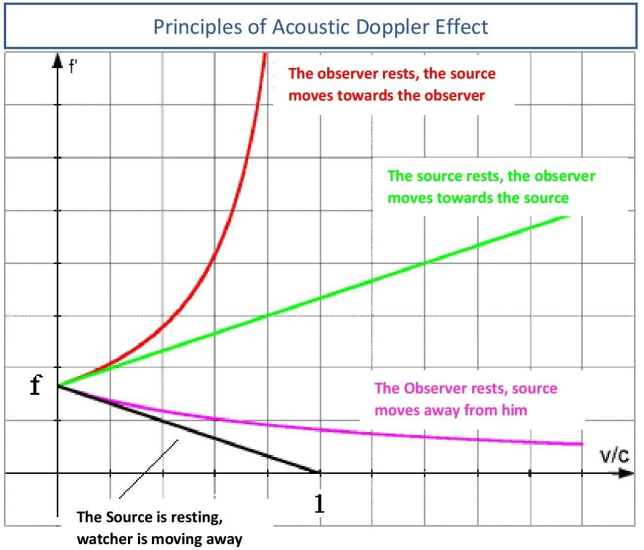


[15]

Detecting Spoofing: Doppler Shift

- We expect an attacker to transmit all spoofed signals from a single (potentially mobile) location
- Assessing Doppler shift of each channel can determine if multiple satellites originate from single tx location





f…frequency
f'…observers registered frequency
v…velocity
c…sound velocity

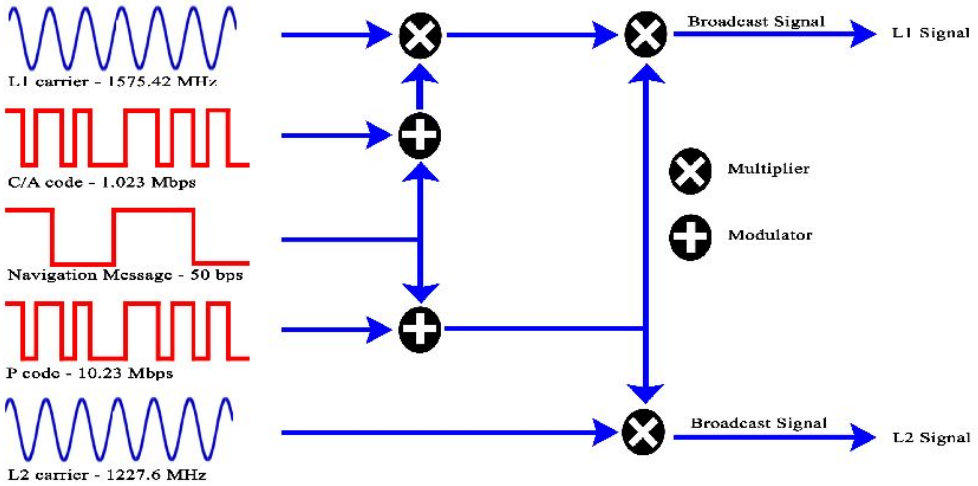
[31]

Detecting Spoofing: Range Rate

Range rate: rate at which the code and phase range measurements change [24].

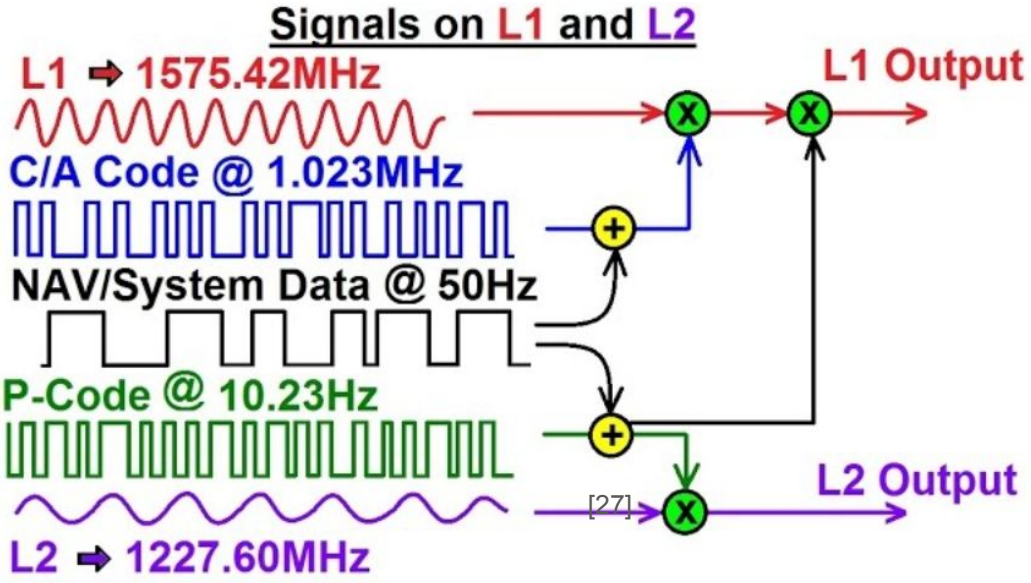
For a static receiver, an attacker can spoof the phase measurement more easily than on a mobile receiver. (Why?)

Both range measurements can be compared against other channels as a feature in classification.



Detecting Spoofing: Cross-Correlate L1 and L2 Signals

- For GPS receivers capable of receiving both L1 and L2 GPS signals …
- A receiver can compare the two signals with the expectation that they will be identical [24, 26].
- The range rate method can also be applied this way, comparing L1 & L2 range rates.



Detecting Spoofing: Perform Residual Analysis

- Since the signal received is

$$S_r = S_S + kS_A + N_T .$$

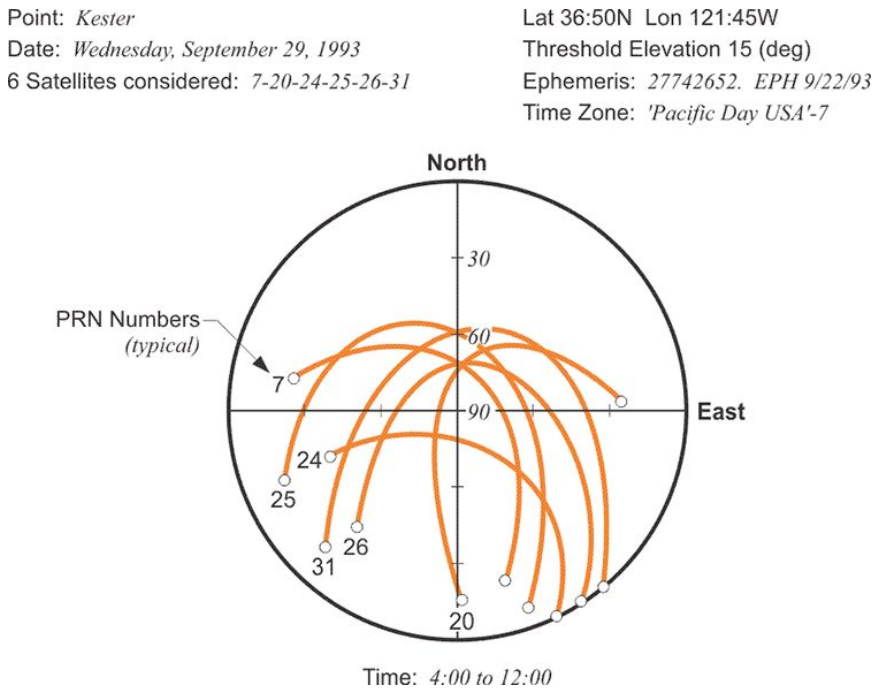
- where k is the ratio of authentic signal to spoofed signal strength
- We can attempt to filter out the dominant signal (Ss) to recover a second, authentic, signal (Sa).
- If Sa can be recovered, spoofing is present [24].

Detecting Spoofing: Verify Ephemeris Data

The ephemeris data included in a GPS signal is used to calculate satellite position.

Comparing the ephemeris and almanac data can determine:

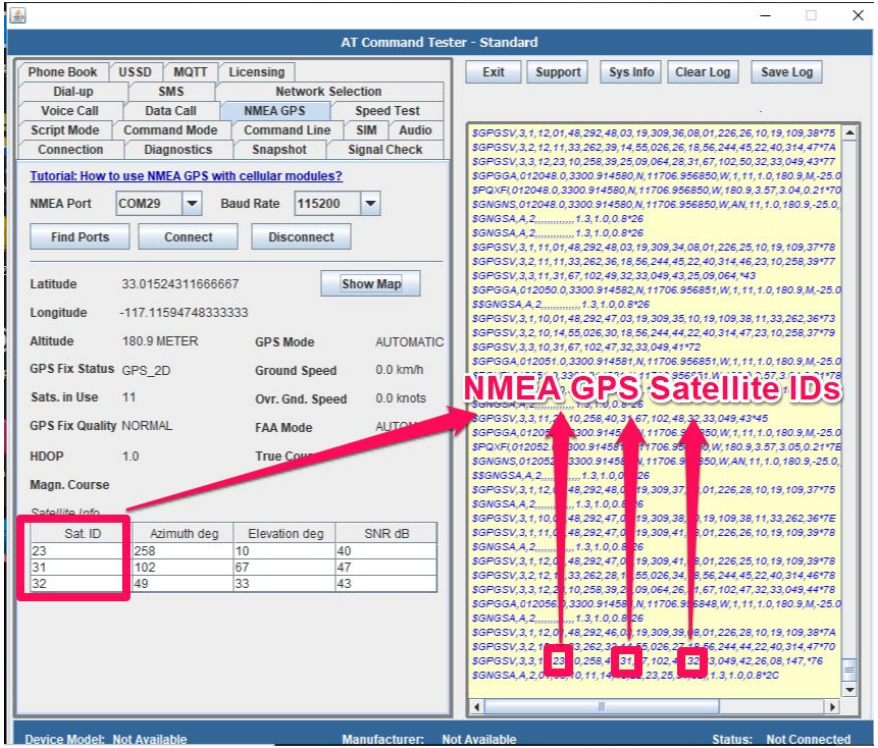
- if the signal provides fixed satellite information, and
- the position does not deviate from the almanac data [24].



Detecting Spoofing: Monitor Identification Codes

A spoofed GPS signal may transmit from more satellites than one would expect to legitimately receive (due to visibility constraints).

Tracking the number of visible satellites, as well as their identification codes could be provided as a feature for anomaly classification [18].

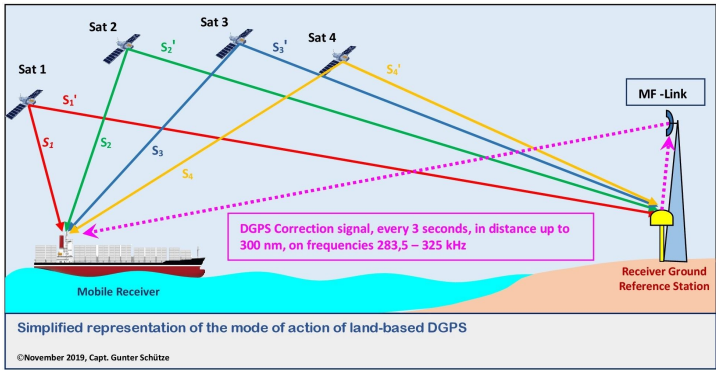


Detecting Spoofing: Monitor Signal Timing

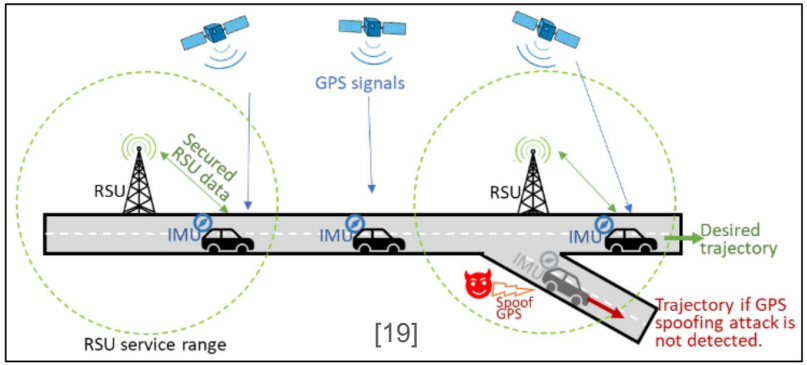
- An attacker may fail to adequately space spoofed signals for each spoofed satellite, leading to multiple satellite signals arriving at the receiver simultaneously.
    - The inter-satellite timing can be provided as a feature to a simple anomaly classification system [16].
- A receiver integrated w/ a high-precision real-time clock (RTC) could compare the time derived from the received GPS signals and perform a comparison with the locally derived high-precision RTC.
    - Any deviation indicates potential spoofing [16].

Detecting Spoofing: Correlate Sensors

- Any available secondary sensors that provide direct or proxy measurements of position or trajectory can be used to sanity check the received GPS measurement.
- For instance, cellular infrastructure can be used as a low-precision ground truth for position, creating a bounded region for valid GPS measurements [9, 19].
- In a mobile context, such as on-board a vessel, sensors and control signals used to direct the vessel's movement can be used to create a short-term projection of position using the previous time's position …
- Creating a probability distribution of expected GPS position,
- Which can be used to assess confidence in the veracity of the received GPS position and informing the next time step [18].



[31]



[19]

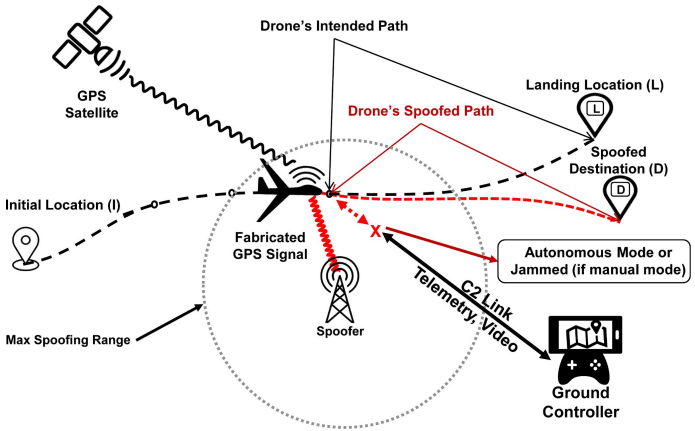
Detecting Spoofing: Triangulation

Triangulation can be performed by triangulating the transmit location using an antenna array of at least 4 antennas.

Given a known fixed distance between each antenna, simple sphere-intersection based on the RSSI of each antenna for the given GPS channel can be used to identify the approximate transmit location and compared against the ephemeris and almanac data to

- Identify deviations from the purported satellite position
- Approximately identify the position of the attacker.
    - However, this requires careful design and calibration of the antenna array.

Combined with out-of-band data, such as CCTV, this technique can help port security identify and remove rogue transmitters.



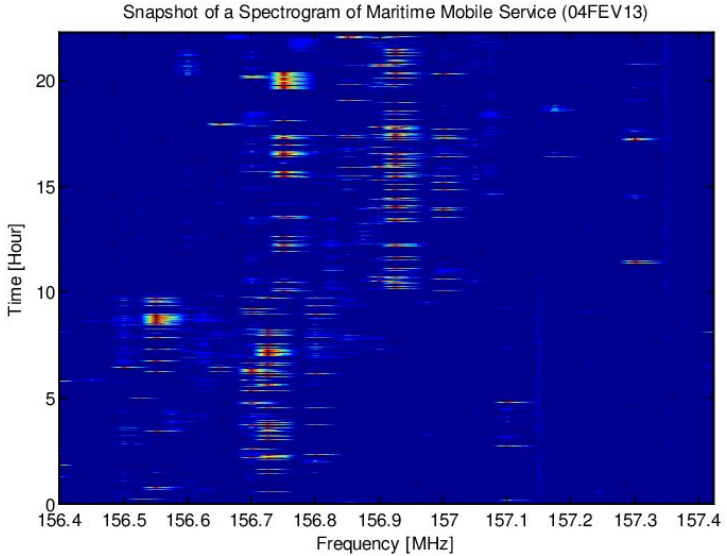
[30]

GPS References

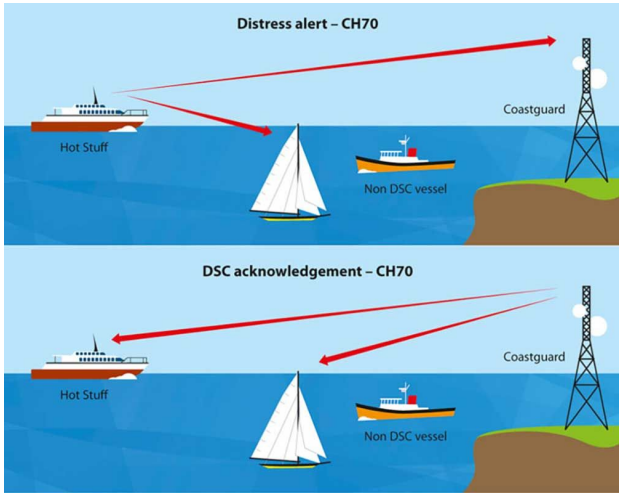
1. https://en.wikipedia.org/wiki/GPS_signals
2. https://en.wikipedia.org/wiki/Global_Positioning_System
3. https://gssc.esa.int/navipedia/index.php/GPS_Navigation_Message
4. https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan
5. Florence, Macchi-Gernot & Petovello, Mark & Lachapelle, Gérard. (2010). Combined acquisition and tracking methods for GPS L1 C/A and L1C signals. International Journal of Navigation and Observation. 2010. 10.1155/2010/190465.
6. Penttinen, Jyrki T.J. (2015). The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems. John Wiley & Sons. ISBN 978-1-119-94488-1.
7. Ranganathan, Aanjhan, Hildur Ólafsdóttir, and Srdjan Capkun. "Spree: A spoofing resistant gps receiver." Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking. 2016.
8. Foruhandeh, Mahsa, et al. "Spotr: GPS spoofing detection via device fingerprinting." Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2020.
9. Wang, Feilong, Yuan Hong, and Xuegang Ban. "Infrastructure-enabled GPS spoofing detection and correction." IEEE Transactions on Intelligent Transportation Systems 24.12 (2023): 13878-13892.
10. Abrar, Murad Mehrab, et al. "GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles." arXiv preprint arXiv:2405.08359 (2024).
11. Ghanbarzade, Ali, and Hossein Soleimani. "GNSS/GPS spoofing and jamming identification using machine learning and deep learning." arXiv preprint arXiv:2501.02352 (2025).
12. Zeng, Kexiong Curtis, et al. "A practical GPS location spoofing attack in road navigation scenario." Proceedings of the 18th international workshop on mobile computing systems and applications. 2017.
13. Jung, Ji Hyuk, et al. "An analysis of GPS spoofing attack and efficient approach to spoofing detection in PX4." IEEE Access 12 (2024): 46668-46677.
14. Jullian, Olivia, et al. "Deep learning detection of GPS spoofing." International Conference on Machine Learning, Optimization, and Data Science. Cham: Springer International Publishing, 2021.
15. Tippenhauer, Nils Ole, et al. "On the requirements for successful GPS spoofing attacks." Proceedings of the 18th ACM conference on Computer and communications security. 2011.
16. Jansen, Kai, et al. "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.
17. KAMEL, IBRAHIM. "GPS Spoofing Attacks in FANETs: A Systematic."
18. Warner, Jon S., and Roger G. Johnston. "GPS spoofing countermeasures." Homeland Security Journal 25.2 (2003): 19-27.
19. Oligeri, Gabriele, et al. "Drive me not: GPS spoofing detection via cellular network: (architectures, models, and experiments)." Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. 2019.
20. Xue, Nian, et al. "Deepsim: Gps spoofing detection on uavs using satellite imagery matching." Proceedings of the 36th Annual Computer Security Applications Conference. 2020.
21. Bethi, Pardhasaradhi, and Srihari Pathipati. "Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies." 2020 IEEE 17th India Council International Conference (INDICON). IEEE, 2020.
22. Haider, Zeeshan, and Shehzad Khalid. "Survey on effective GPS spoofing countermeasures." 2016 Sixth International Conference on Innovative Computing Technology (INTECH). IEEE, 2016.
23. Kerns, Andrew J., et al. "Unmanned aircraft capture and control via GPS spoofing." Journal of field robotics 31.4 (2014): 617-636.
24. Wen, Hengqing, et al. "Countermeasures for GPS signal spoofing." Proceedings of the 18th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2005). 2005.
25. https://www.onosokki.co.jp/English/hp_e/products/keisoku/automotive/lc8_principle.htm
26. Qaisar, Sana Ullah, and Andrew G. Dempster. "Cross-correlation performance comparison of L1 & L2C GPS codes for weak signal acquisition." Int. Symp. on GPS/GNSS. 2008.
27. https://www.youtube.com/watch?v=IcxrGIdOGYo
28. https://www.e-education.psu.edu/geog862/node/1739
29. https://m2msupport.net/m2msupport/get-the-gps-satellite-id-from-the-nmea-gpgsv-sentence/
30. Khan, Shah Zahid, Mujahid Mohsin, and Waseem Iqbal. "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions." PeerJ Computer Science 7 (2021): e507.
31. https://www.marine-pilots.com/articles/14342-gps-part-1-structure-mode-of-operation-technical-and-physical-fundamentals-of-gps
32. https://owaysonline.com/global-positioning-system-on-ships/
33. https://jeremyclark.ca/wp/telecom/rtl-sdr-for-satellite-gps/

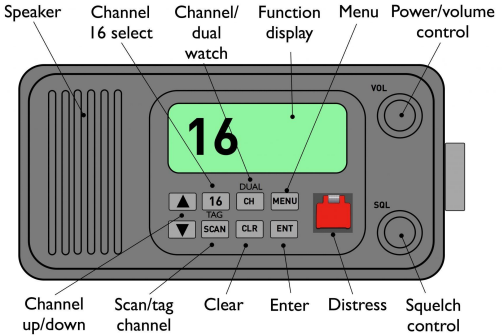
GPS Demo Time

VHF/DSC


Snapshot of a Spectrogram of Maritime Mobile Service (04FEV13)
Time [Hour]
0
5
10
15
20
156.4
156.5
156.6
156.7
156.8
156.9
157
157.1
157.2
157.3
157.4
Frequency [MHz]

[1]


Distress alert – CH70
Hot Stuff
Coastguard
Non DSC vessel
DSC acknowledgement – CH70
Hot Stuff
Coastguard
Non DSC vessel


Speaker
Channel 16 select
Channel/ dual watch
Function display
Menu
Power/volume control
16
VOL
SQL
DUAL
CH
MENU
TAG
SCAN
CLR
ENT
Channel up/down
Scan/tag channel
Clear
Enter
Distress
Squelch control

[2]

VHF Audio

- Broadcast audio channels for port operations and ship-to-ship communications.
- Dedicated channels for coast guard operation.
- Frequency modulated analog signal.

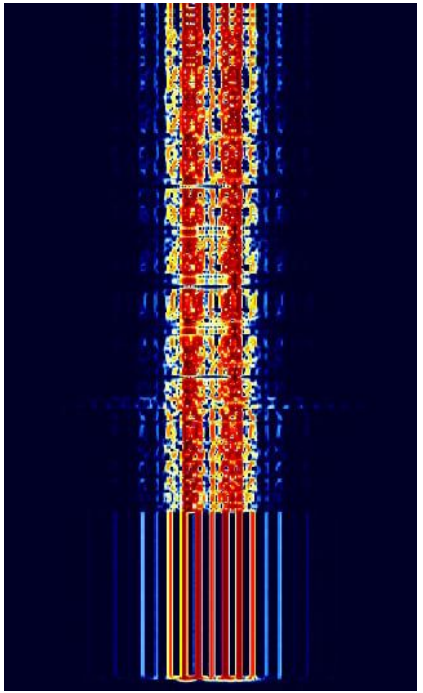
Channel Number	Ship Transmit MHz	Ship Receive MHz	Description of Communications
1A	156.050	156.050	Port Operations and Commercial, VTS. (New Orleans/Lower Mississippi)
5A	156.250	156.250	Port Operations or VTS. (Houston, New Orleans and Seattle)
6	156.300	156.300	Intership Safety
7A	156.350	156.350	Commercial
8	156.400	156.400	Commercial (Intership only)
9	156.450	156.450	Boater Calling. Commercial and Non-Commercial.
10	156.500	156.500	Commercial
11	156.550	156.550	Commercial. VTS in selected areas.
12	156.600	156.600	Port Operations. VTS in selected areas.
13	156.650	156.650	Intership Navigation Safety (Bridge-to-bridge). Ships >20m length maintain a listening watch on this channel in US waters.
14	156.700	156.700	Port Operations. VTS in selected areas.
15	--	156.750	Environmental (Receive only). Used by Class C EPIRBs.
16	156.800	156.800	International Distress, Safety and Calling. Ships required to carry radio, USCG, and most coast stations maintain a listening watch on this channel.
17	156.850	156.850	State Control
18A	156.900	156.900	Commercial
19A	156.950	156.950	Commercial
20	157.000	161.600	Port Operations (duplex)
20A	157.000	157.000	Port Operations
21A	157.050	157.050	U.S. Coast Guard only
22A	157.100	157.100	USCG Liaison/Maritime Safety Information Broadcasts. Announced on channel 16.
23A	157.150	157.150	U.S. Coast Guard only
24	157.200	161.800	Public Correspondence (Marine Operator)
25	157.250	161.850	Public Correspondence (Marine Operator)
26	157.300	161.900	Public Correspondence (Marine Operator)
27	157.350	161.950	Public Correspondence (Marine Operator)
28	157.400	162.000	Public Correspondence (Marine Operator)
63A	156.175	156.175	Port Operations and Commercial, VTS. (New Orleans/Lower Mississippi area)
65A	156.275	156.275	Port Operations
66A	156.325	156.325	Port Operations
67	156.375	156.375	Commercial. Bridge-to-bridge communications in lower Mississippi River. Intership only.
68	156.425	156.425	Non-Commercial
69	156.475	156.475	Non-Commercial
70	156.525	156.525	Digital Selective Calling (voice communications not allowed)

Demo Time: VHF FM

Digital Selective Calling

- Digital modulation on HF & VHF bands for distress beacons.
- Includes the MMSI and context surrounding the distress to request services.
- Continuous Frequency Shift Keying

- 100 fire, explosion
- 101 flooding
- 102 collision
- 103 grounding
- 104 listing, in danger of capsizing
- 105 sinking
- 106 disabled and adrift
- 107 undesignated distress
- 108 abandoning ship
- 109 piracy/armed robbery attack
- 110 man overboard



[4]

Parameter	DSC VHF BFSK
Fc = VCO Center Frequency Phase Continuous BFSK	1700Hz
F mark	2100Hz
F space	1300Hz
F separation	Fc +/- 400Hz=800Hz
R Data Rate	1200bps
Tb=1/R	833.3usec
Condition 1 for Orthogonal Decoding of Continuous BFSK (Ref.6 = X)	F1=n x 1/(4Tb) F2=m x 1/(4Tb) int x 300Hz
Condition 2 for Orthogonal Decoding of Continuous BFSK (Ref.6 = X)	F1-F2=n x1/(2Tb) n x 600Hz
Minimum Frequency Separation	1/(2Tb)=600Hz
Decoding (Ref. 6 & 7)	Fmrk/Fsp Mixers – No Fmrk/Fsp BPF or IQ – Yes

[12]

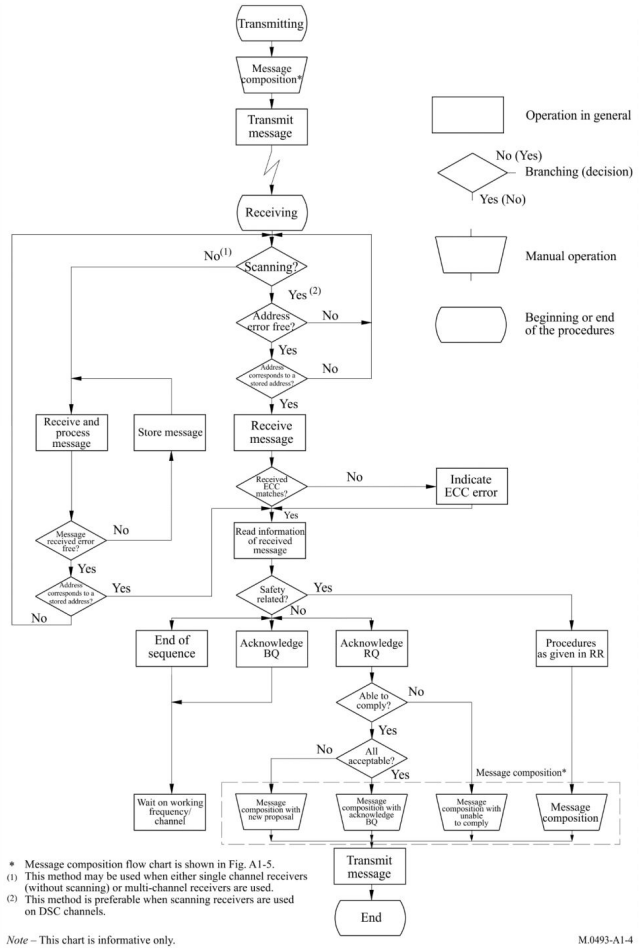
DSC: Specification

Distress alerts

Frequency band	Type of com	Applicable to: Ship station Class A Tx	Ship station Class A Rx	Ship station Class D Tx	Ship station Class D Rx	Ship station Class E Tx	Ship station Class E Rx	Hand-held Class H Tx	Hand-held Class H Rx	MOB Device Class M Open loop Tx	MOB Device Class M Open loop Rx	Coast station Tx	Coast station Rx	Technical format of call sequence: Format specifier (2 identical)	Self-ID (5)	Message 1: Nature of distress (1)	Message 2: Distress coordinates (5)	Message 3: Time (2)	Message 4: Subsequent communications (1)	EOS (1)	ECC (1)	EOS (2 identical)	Rec. ITU-R M.821 expansion sequence* (9)
VHF	Distress (RT)	●	●	●	●			●	●	●	—	—	●	112	Self-ID	100 to 110	Pos1	UTC	100**	127	ECC	127	expan1
MF/HF	Distress (RT)	●	●			●	●					—	●	112	Self-ID	100 to 110	Pos1	UTC	109	127	ECC	127	expan1

Distress acknowledgements

Frequency band	Type of com	Applicable to: Ship station Class A Tx	Ship station Class A Rx	Ship station Class D Tx	Ship station Class D Rx	Ship station Class E Tx	Ship station Class E Rx	Hand-held Class H Tx	Hand-held Class H Rx	MOB Device Class M open loop Tx	MOB Device Class M open loop Rx	Coast station Tx	Coast station Rx	Technical format of call sequence: Format specifier (2 identical)	Category (1)	Self-ID (5)	Tele-command (1)	Message 0: Distress ID (5)	Message 1: Nature of distress (1)	Message 2: Distress coordinates (5)	Message 3: Time (2)	Message 4: Subsequent communications (1)	EOS (1)	ECC (1)	EOS (2 identical)	Rec. ITU-R M.821 expansion sequence* (9)
VHF	Distress acknowledgement (RT)	●	●	—	●			—	●	—	●	●	●	116	112	Self-ID	110	Distress ID	100 to 110	Pos1	UTC	100**	127	ECC	127	expan1
	Distress acknowledgement (EPIRB)	●	●	—	●			—	●	—	—	●	●	116	112	Self-ID	110	Distress ID	112	Pos1	UTC	126	127	ECC	127	expan1
	Distress self-cancel	●	●	●	●			●	●	●	—	—	●	116	112	Self-ID	110	Self-ID	100 to 110	Pos1	UTC	100**	127	ECC	127	expan1



* Message composition flow chart is shown in Fig. A1-5.
(1) This method may be used when either single channel receivers (without scanning) or multi-channel receivers are used.
(2) This method is preferable when scanning receivers are used on DSC channels.

Note – This chart is informative only.

M.0493-A1-4

Stretch Demo Time/Homework: DSC Transmitter

VHF/DSC References

1. Bolas, Eduardo, et al. "Opportunistic Usage of Maritime VHF Band—Deployment Challenges for a New Regulatory Framework." *Wireless Engineering and Technology* 2014 (2014).
2. https://www.safe-skipper.com/vhf-dsc-radio-how-best-to-communicate-at-sea/
3. https://www.sigidwiki.com/wiki/Category:VHF
4. https://www.sigidwiki.com/wiki/Category:Marine
5. https://www.udxf.nl/MID-MMSI-list.pdf
6. https://www.coaa.co.uk/dscdecoder.htm
7. https://www.ndblist.info/datamodes.htm
8. https://akwg.cap.gov/media/cms/US_VHF_Marine_Frequency_List_01C6E75413CF3.pdf
9. https://www.itu.int/rec/R-REC-M.493/en
10. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.493-16-202312-I!!PDF-E.pdf
11. https://jeremyclark.ca/wp/telecom/rtl-sdr-for-marine-vhf-scanner-on-gnu-radio/
12. https://jeremyclark.ca/wp/telecom/marine-gmdss-dsc-vhf-decoder_a/