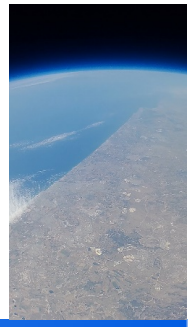
Paz Hameiri

CON trolling the weather

About myself

- I’m a system engineer
- M.Sc. in Electro-Optical Engineering
- Worked fourteen years in the aerospace industry
- Six years of experience with telecommunication systems design
- Launched two weather balloons with elementary school pupils
- DEF CON 29 speaker
- BSidesTLV 2023 speaker





Weather balloon's introduction

- Airman 1st Class Ian Dudley, 30th Space Wing Public Affairs, Vandenberg space force base, California:
  - The balloons carry instrumentation that provides wind speed and direction, atmospheric temperature, and humidity every 100 feet from the surface of the earth to near the edge of space where the balloon finally bursts
- The instrumentation is called “Radiosonde”

Credit: NOAA Photo Library, NOAA Central Library; OAR/ERL/National Severe Storms Laboratory (NSSL) / Wikimedia Commons / Public domain

Weather balloons use

- **William Shmeiser, 30th Operations Support Squadron weather systems director and senior meteorologist, Vandenberg space force base, California:**
  - **“The data goes directly into the NOAA database and is included in the national weather models and analysis you see on television”**
  - **“Depending upon the mission we release from five to 15 balloons during a launch count, sometimes more if weather conditions demand”**
  - **“Upper air balloon support is critical to Vandenberg's launch mission as well as being a huge part of daily weather forecasting; not only on Vandenberg but across the community and the nation.”**

NASA's criteria for safe launch

- **NASA's Falcon 9 Crew Dragon Launch Weather Criteria:**
  - **Do not launch through upper-level conditions containing wind shear that could lead to control problems for the launch vehicle**
  - **Do not launch if downrange weather indicates violation of limits at splashdown in case of Dragon launch escape**

    Downrange weather is monitored at more than 50 locations along the ascent track along the North American eastern seaboard and across the North Atlantic

Who's who in the radiosonde business?

- **Top Radiosonde types, according to World Meteorological Organization launch site data:**

Radiosonde type	Launch Sites	Precentage
Vaisala RS41	186	29.8
GTS-1 (China)	82	13.1
Vaisala RS92	67	10.7
Lockheed Martin LMS06	66	10.6
Meteomodem M10	48	7.7
Graw DFM-09	40	6.4
Meisei iMS-100	36	5.8

Credit: Mark Jessop / Twitter / 9:00 AM Sep 7, 2019

Vaisala RS41 transmission frame

- Most common models: RS-41SG and RS41-SGP
- Basic frame: 320 Bytes, divided into blocks
- Two layers of error detection and correction:
  - Each numbered block comprises CRC-16 bytes
  - Reed Solomon is applied at the complete message

Vaisala RS41 frame

Bytes	Block	Content
8	Header	Header
48	ECC	Reed Solomon ECC
1	Frame type	Frame type
44	0x79	Status: frame number, serial number, battery voltage, status bits, sonde type, board temp., control data, subframe (0-51)
46	0x7A	Measurements: ambient & sensors temp., humidity, ambient pressure
34	0x7C	GPS info: time, space vehicles number & reception quality
93	0x7D	GPS raw data: space vehicles relative distance and velocity
25	0x7B	GPS position: ECEF position X/Y/Z, ECEF velocity X/Y/Z, number of SVs, velocity accuracy, PDOP
21	0x76	Empty block

Vaisala RS41 subframes: 51 * 16 Bytes

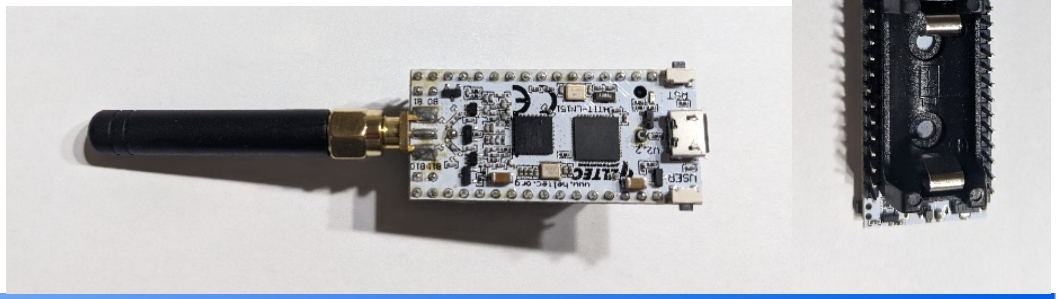
- Calibration data
- Transmission frequency
- Sonde type
- Software version
- Mainboard type
- Components serial numbers
- Burstkill data
- Diagnostics data
- More…

Vaisala RS41 RF properties

- Frequency: 400.15 – 406 MHz
- Output power: min 60mW (18dBm)
- Modulation: GFSK
- Data downlink: 4,800 bits/s

Strategy 1: Jamming attack

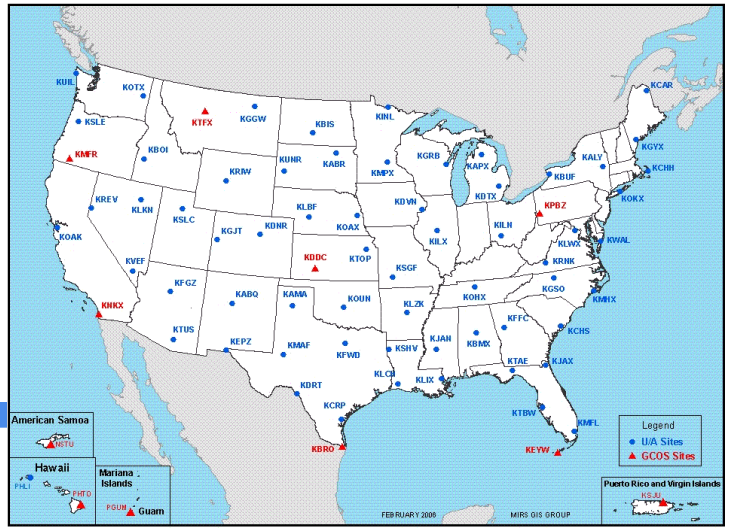
- Use a powerful transmitter to transmit jamming signals
- My choice: HELTEC AUTOMATION Lora Node 151, 433MHz
  - SX1278 LoRa chip
  - STM32L151CCU6 MCU
  - Maximum transmission power: 20dBm
  - ½AA Lithium battery
  - 20$ on eBay
  - 25 grams with the battery



Jamming alert

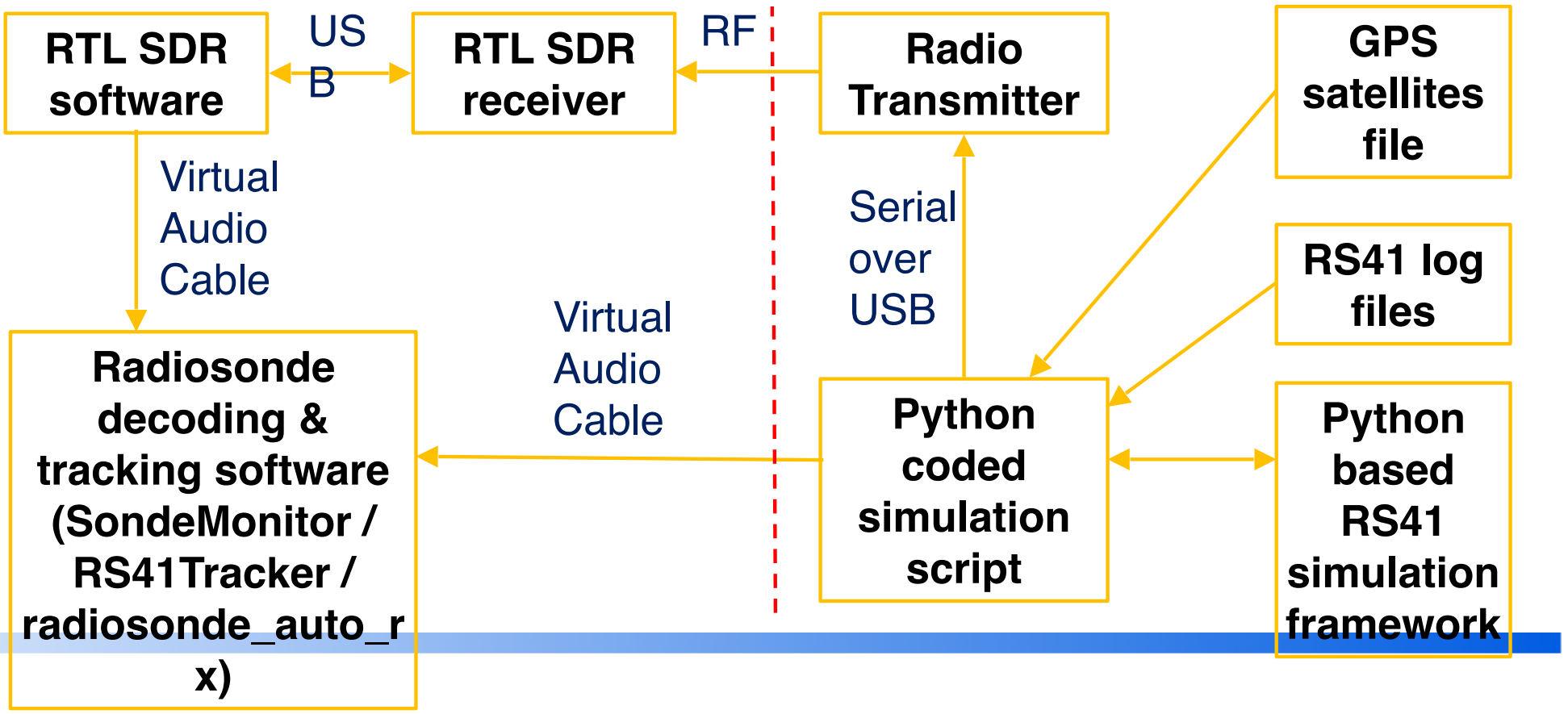
- The US National Weather Service is running or supporting 102 sites
- Weather balloons are simultaneously launched at 6 AM and 6 PM EST
- What will happen if 50 people will decide to simultaneously jam the signals?

According to ABC News meteorology team, many missing balloons could lead to errors in weather models and forecasts.



Credit: NOAA / Weather.gov

RS41 simulator development environment



Messages generation with the framework

- Synthesize frames and subframes
  - Requires a behavioral model for each measurement
  - Shortcut: Take the calibration data out of a log file
- Use log files:
  - Alter specific data items, as required
  - Synthesize the GPS data, serial numbers, fine details, etc.

Strategy 2: Spoofing attack

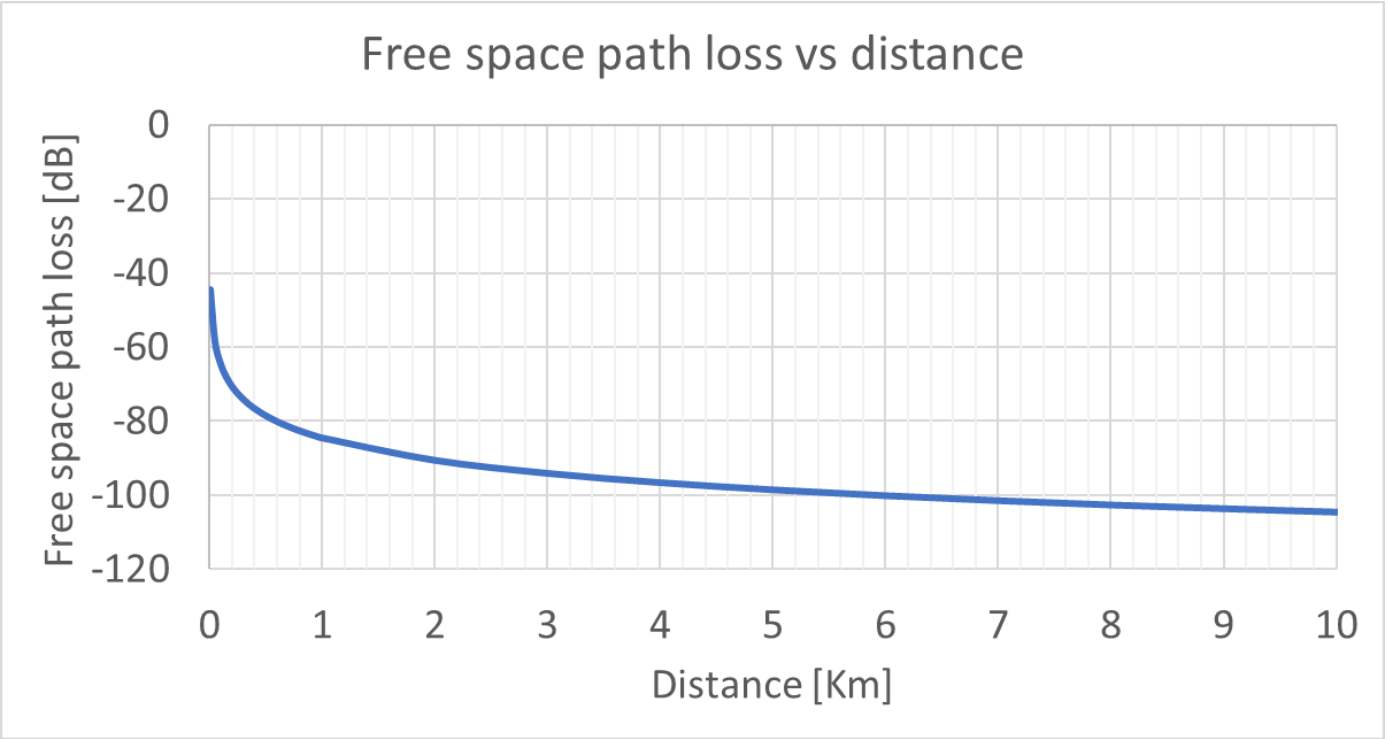
- Use a powerful transmitter to transmit spoofed messages
- Technique:
  - Receive all the subframes from an active radiosonde (at least 51 frames)
  - Prepare for spoofing (setup the transmitter, encode message/s, etc.)
  - Jam the radiosonde transmission to raise the data's uncertainty level
  - Transmit spoofed messages
  - Jam the radiosonde transmission to raise the data's uncertainty level
  - Stop

Ride on the signal to noise ratio

- Use a powerful transmitter to transmit spoofed messages
- At the receiver:
  - Spoofing transmitter = Signal
  - Radiosonde signal = Noise
- Requires good signal to noise ratio:

SNR [dB]	Reception
5 to 10	Indistinguishable
10 to 15	Unreliable
15 to 25	Poor
25 to 40	Good
41 or higher	Excellent

Ride on the signal to noise ratio



RS41-SGM - Introduction

- Intended for military use
- Radio silence until a specified height or time has been reached
  "Radiosonde transmission does not reveal the balloon launch location"
- The data is recorded during the radio silence
- "Transmitted data is also encrypted", 128-bit key

RS41-SGM – Military? Are you serious?

- Most properties were not changed (Frequency, framing, etc.)
- Only the measurements and the GPS data are encrypted
- The encryption is not always activated:
  - Transmits unencrypted blocks
  - Identifies as an RS41-SGM
- Easy to position, easy to estimate the launch site
- Frequent launches indicate military activity

Coping with spoofing

- Don’t encrypt the messages
  - Keys management is a headache
  - Synchronizing reception sites is a headache
  - Might not be welcomed by some customers
  - Bad for the radiosonde community
  - Information collection is public-funded – the data belongs to the public

Coping with spoofing

- Authenticate the messages
  - Modify the messages to comprise an authentication tag
  - Customers who are not interested in message authentication can keep using their equipment as is
  - The community can keep using their equipment as is
  - Authentication can be done offline

Epilogue

- The framework should be used to develop and test tools for the radiosonde community
- Source code:
  - https://github.com/CuriosityRocks/RS41Simulator

- Thank you ☺

References

- Vredenbregt L., "How many weather balloons are out there? Hundreds, it turns out", https://abcnews.go.com/Politics/weather-balloons-hundreds-turns/story?id=97082985, Feb 13, 2023.
- Dudley I., "Weather balloons and rocket science", https://www.vandenberg.spaceforce.mil/News/Features/Display/Article/737270/weather-balloons-and-rocket-science/
- bazjo, "RS41 Decoding", https://github.com/bazjo/RS41_Decoding
- rs1729, "RS", https://github.com/rs1729/RS
- projecthorus, "radiosonde_auto_rx", https://github.com/projecthorus/radiosonde_auto_rx
- sondehub, https://github.com/projecthorus/radiosonde_auto_rx
- "Upper-air Observations Program", https://www.weather.gov/upperair/
- Mass C., "Wind Shear: When the Atmospheric Seems to be Tearing Itself Apart", https://cliffmass.blogspot.com/2017/05/wind-shear-when-atmospheric-seems-to-be.html

References

- Jessop M., "Top Radiosonde types", https://twitter.com/vk5qi/status/1170215238978830339
- Lada B., "3 weather obstacles that SpaceX faces when launching rockets into space", https://www.accuweather.com/en/space-news/types-of-weather-that-can-delay-a-spacex-rocket-launch/352407
- Nasa, "Falcon 9 Crew Dragon Launch Weather Criteria", FS-2020-05-568-KSC, www.nasa.gov
- Frielingsdorf J., "An Open-Source Documentation and Implementation of the Vaisala RS41 Data Preparation Algorithms", WMO Technical Conference on Meteorological and Environmental Instruments and Methods of Observation, Oct. 11, 2022
- Cadence PCB Solutions, "What is Signal to Noise Ratio and How to calculate it?", https://resources.pcb.cadence.com/blog/2020-what-is-signal-to-noise-ratio-and-how-to-calculate-it
- Vaisala, "Vaisala Radiosonde RS41-SGP Data Sheet", www.vaisala.com, B211444EN-E, 2017
- Vaisala, "Vaisala Radiosonde RS41-SG Data Sheet", www.vaisala.com, B211321EN-K, 2020
- Vaisala, "Vaisala Radiosonde RS41-SGM Data Sheet", www.vaisala.com, B211448EN-E, 2017