Spoofing a Multi-Band RTK GNSS Receiver with HackRF One and GNSS Jammer

gpspatron.com/spoofing-a-multi-band-rtk-gnss-receiver-with-hackrf-one-and-gnss-jammer/

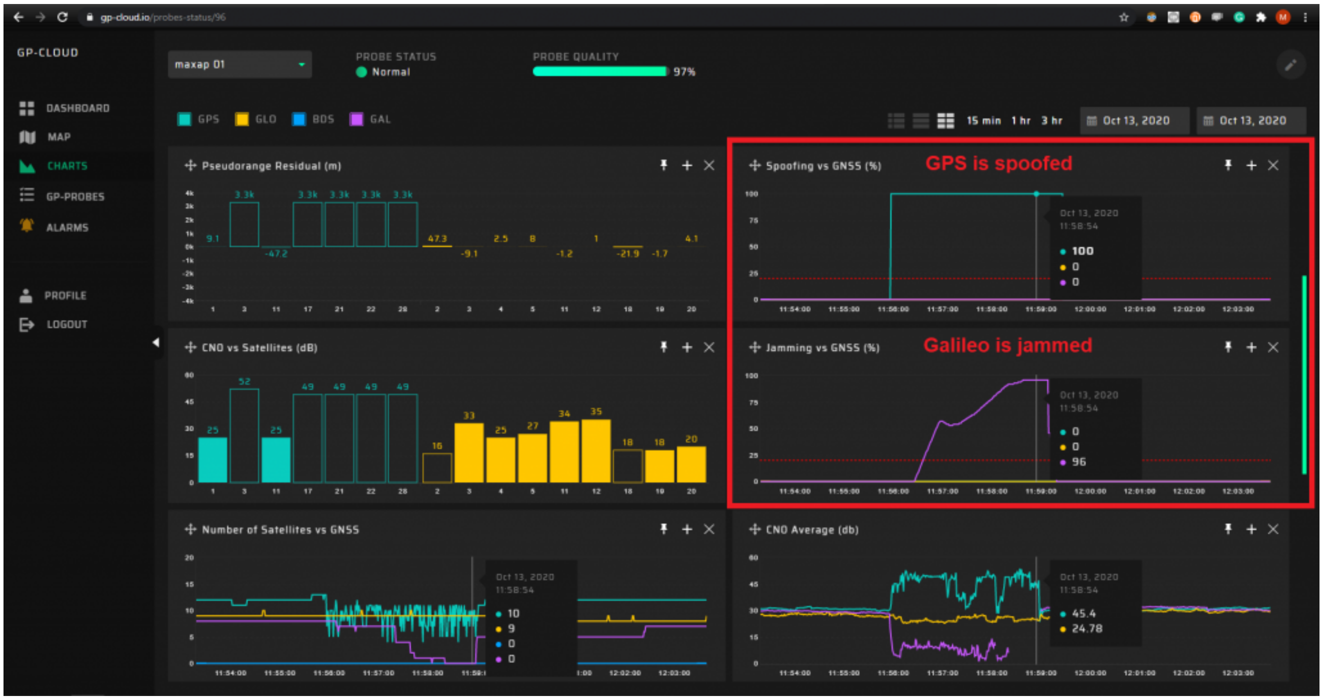
March 4, 2021

Another boring long-read 🙂
We value your time, so we posted a video about this experiment on youtube: https://youtu.be/Ya_B7tqA-X8
To learn more details, please enjoy the article.

Introduction

You might have heard that multi-band multi-constellation GNSS receivers are more secure against spoofing. Indeed, a multi-band spoofer is more expensive than a one-band. And open-source projects on GitHub can simulate only GPS L1.

But, there is one trick. It is possible to generate a counterfeit signal only for GPS L1 and suppress the other signals/bands. In real life, we face such attacks every day. For example, here the GPS is spoofed and Galileo is jammed:



This is a common attack scenario from wildlife.

In this video, we demonstrated that the combination of affordable GPS L1 spoofer and multi-constellation jammer can hack the UBLOX M8T module with embedded spoofing detection and mitigation algorithms.

In this article, we reveal the result of vulnerability testing of multi-band multi-constellation RTK receiver UBLOX ZED-F9T. We use the combination of GPS L1 spoofer based on gps-sdr-sim/HackRF One and multi-band GNSS jammer.

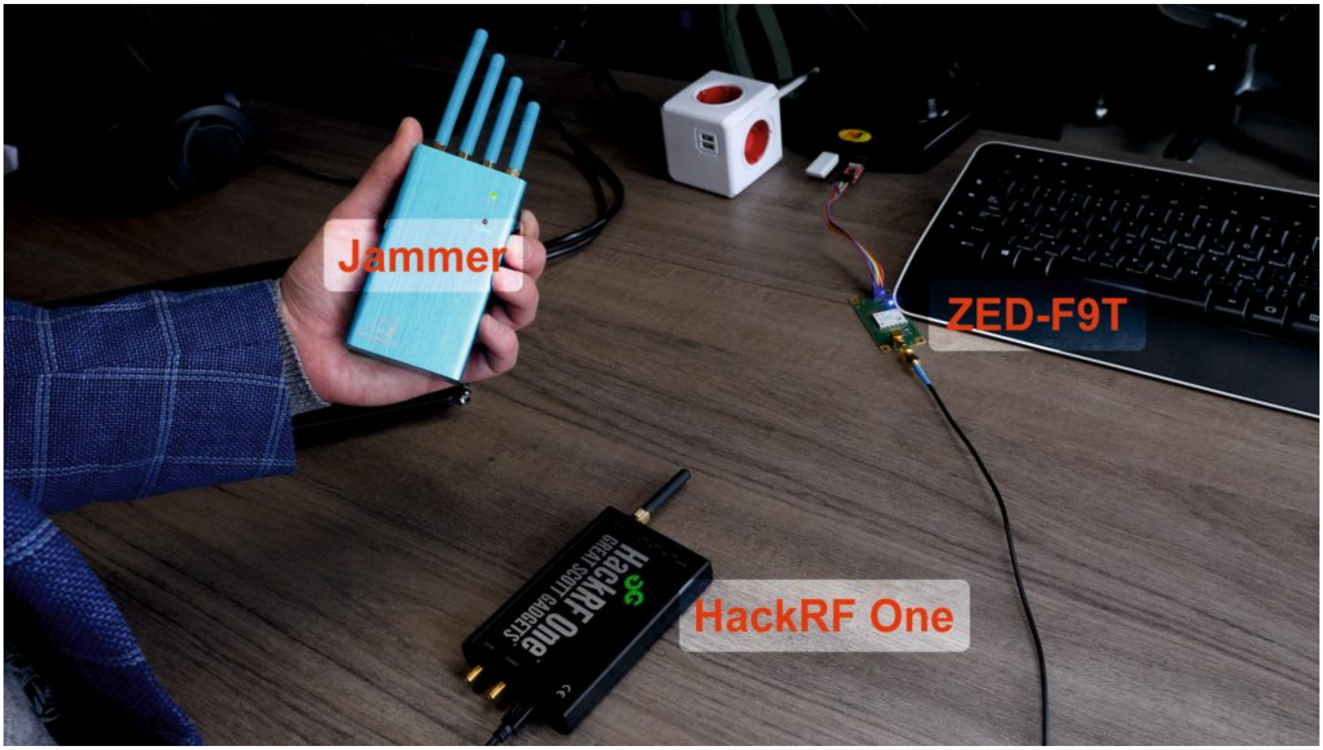
Setup

The experiment was conducted under live-sky conditions over-the-air (do not attempt this at home :-).

Why deal with radiated RF signals? To assure our subscribers that multi-band multi-constellation GNSS spoofing is not a theoretical problem from scientific articles, and expensive laboratory-grade equipment is not further required.

Tools were utilized:

- ZED-F9T
- HackRF One
- gps-sdr-sim
- almanac and ephemeris files
- Multi-band GNSS jammer
- U-Center



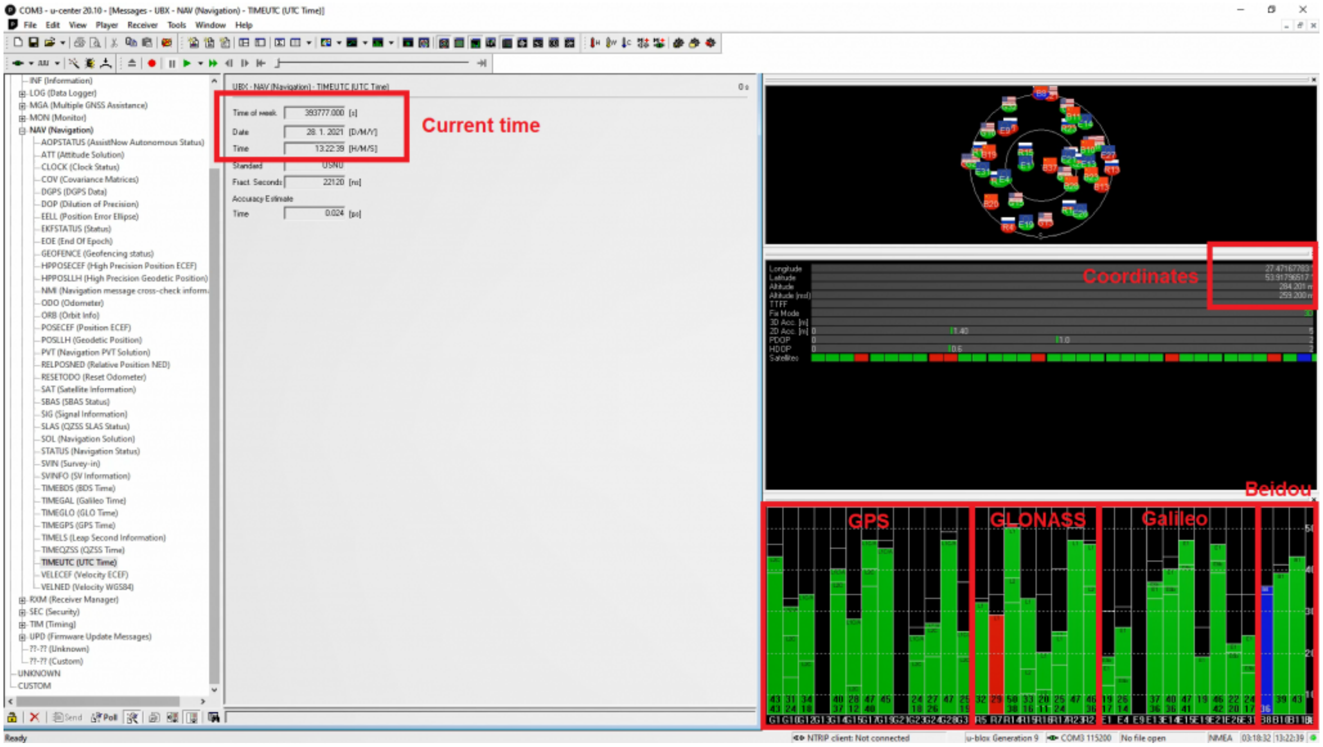
The GNSS antenna of the receiver was placed on a windowsill two meters to the right.

UBLOX ZED-F9T Configuration

We used U-Center to configure the GNSS module and set the following settings:

- Used GNSS constellations – GPS, Galileo, GLONASS, Beidou
- Interference monitoring – Enable

The receiver saw 11 GPS, 9 Galileo, 8 GLONASS, and 3 Beidou genuine satellites on two RF bands:



COM3 - u-center 20.10 - [Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)]

UBX - NAV (Navigation) - TIMEUTC (UTC Time)

Time of week 383777.000 [s]
Date 28. 1. 2021 [D/M/Y]
Time 13:22:39 [H/M/S]
Standard USNO
Fract. Seconds 22120 [ns]
Accuracy Estimate
Time 0.024 [ns]

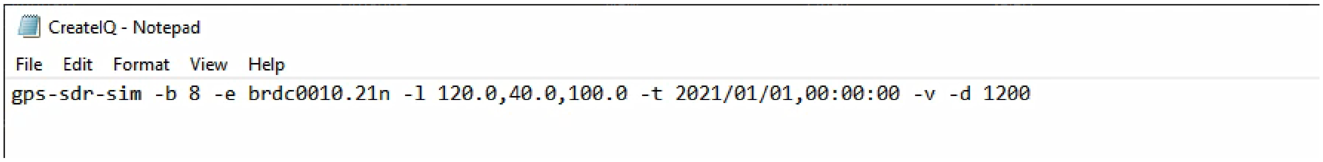
Longitude 27.47167783
Latitude 53.91796517
Altitude 284.201 m
Altitude (msl) 259.200 m
TTFF
Fix Mode 3D
3D Acc. [m]
2D Acc. [m] 0 1.40 5
PDOP 0 1.0 2
HDOP 0 0.6 2

Spoofer’s Configuration

We do not describe in detail how to configure and run the spoofer.. Just google “gps-sdr-sim HackRF One”. In general, you need to conduct two steps. First, IQ data file generations, second IQ data playing on SDR.

Our spoofer’s configuration:

- Coordinates Lat,Lon,Hgt – 120.0, 40.0, 100.0
- Scenario start time YYYY/MM/DD,hh:mm:ss – 2021/01/01,00:00:00

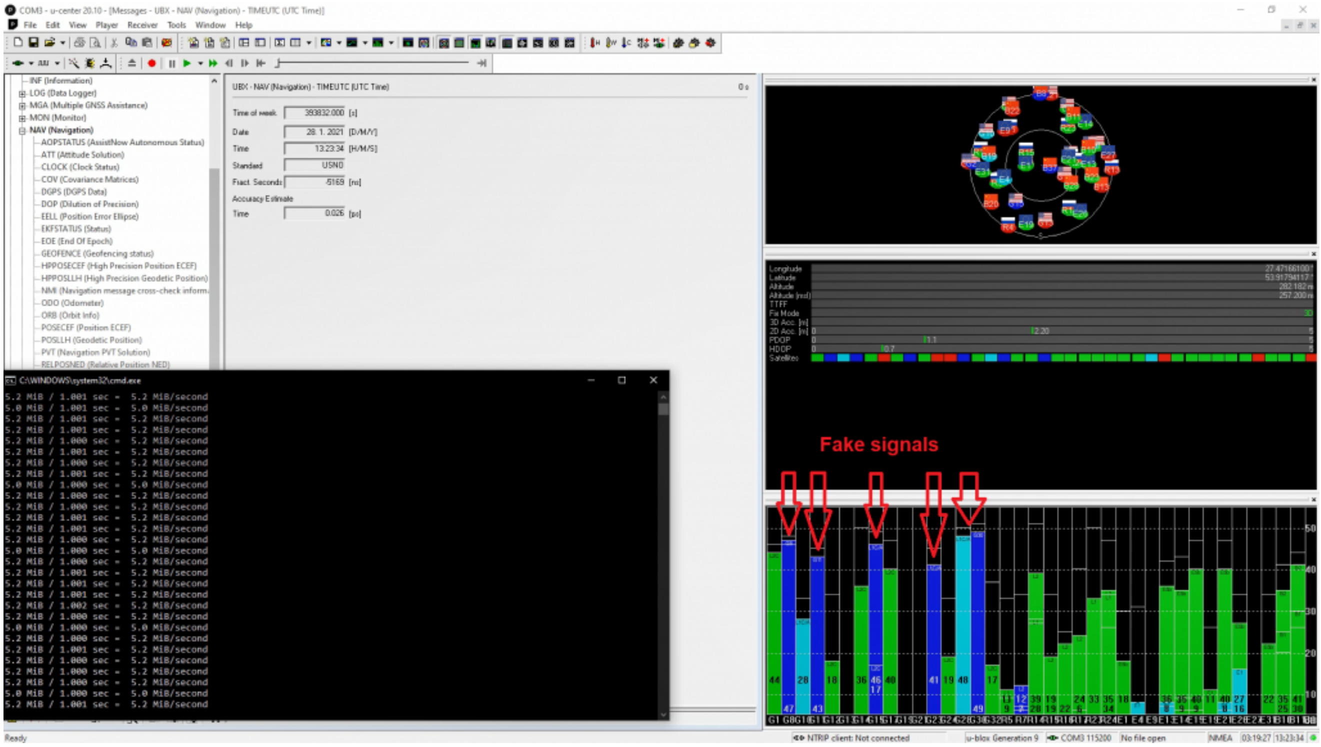


CreateIQ - Notepad

```
gps-sdr-sim -b 8 -e brdc0010.21n -l 120.0,40.0,100.0 -t 2021/01/01,00:00:00 -v -d 1200
```

Spoofing

The receiver perceived counterfeit signals after the spoofer was turned on but didn’t use them. Generated signals differed from the genuine one in Doppler, pseudo ranges, and timestamp\ephemeris data. This attack is called non-coherent or asynchronous. A non-coherent attack can be successful only when the receiver loses the original signals.


COM3 - u-center 20.10 - [Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)]
File Edit View Player Receiver Tools Window Help
INF (Information)
LOG (Data Logger)
MGA (Multiple GNSS Assistance)
MON (Monitor)
NAV (Navigation)
AOPSTATUS (AssistNow Autonomous Status)
ATT (Attitude Solution)
CLOCK (Clock Status)
COV (Covariance Matrices)
DGPS (DGPS Data)
DOP (Dilution of Precision)
EELL (Position Error Ellipse)
EKFSTATUS (Status)
EOE (End Of Epoch)
GEOFENCE (Geofencing status)
HPPOSECEF (High Precision Position ECEF)
HPPOSLLH (High Precision Geodetic Position)
NMI (Navigation message cross-check inform...
ODO (Odometer)
ORB (Orbit Info)
POSECEF (Position ECEF)
POSLLH (Geodetic Position)
PVT (Navigation PVT Solution)
RELPOSNED (Relative Position NED)
Fake signals
Ready
NTRIP client: Not connected
u-blox Generation 9
COM3 115200
No file open
NMEA
03:19:27
13:23:34

UBX - NAV (Navigation) - TIMEUTC (UTC Time)

Time of week: 393832.000 [s]
Date: 28. 1. 2021 [D/M/Y]
Time: 13:23:34 [H/M/S]
Standard: USNO
Fract. Seconds: -5169 [ns]
Accuracy Estimate
Time: 0.026 [µs]

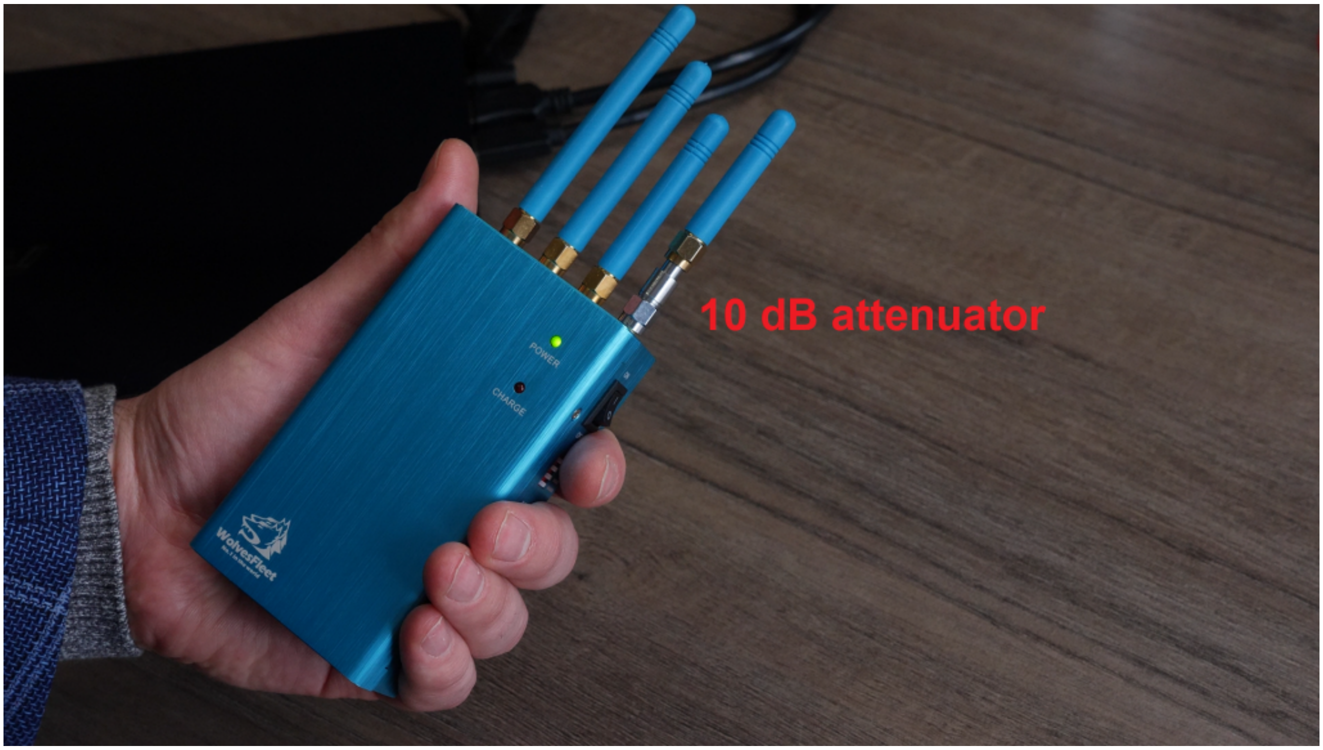
Longitude: 27.47166100 °
Latitude: 53.91794117 °
Altitude: 282.182 m
Altitude (msl): 257.200 m
TTFF
Fix Mode: 3D
3D Acc. [m]
2D Acc. [m]: 2.20
PDOP: 1.1
HDOP: 0.7
Satellites

C:\WINDOWS\system32\cmd.exe

```
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.002 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
```

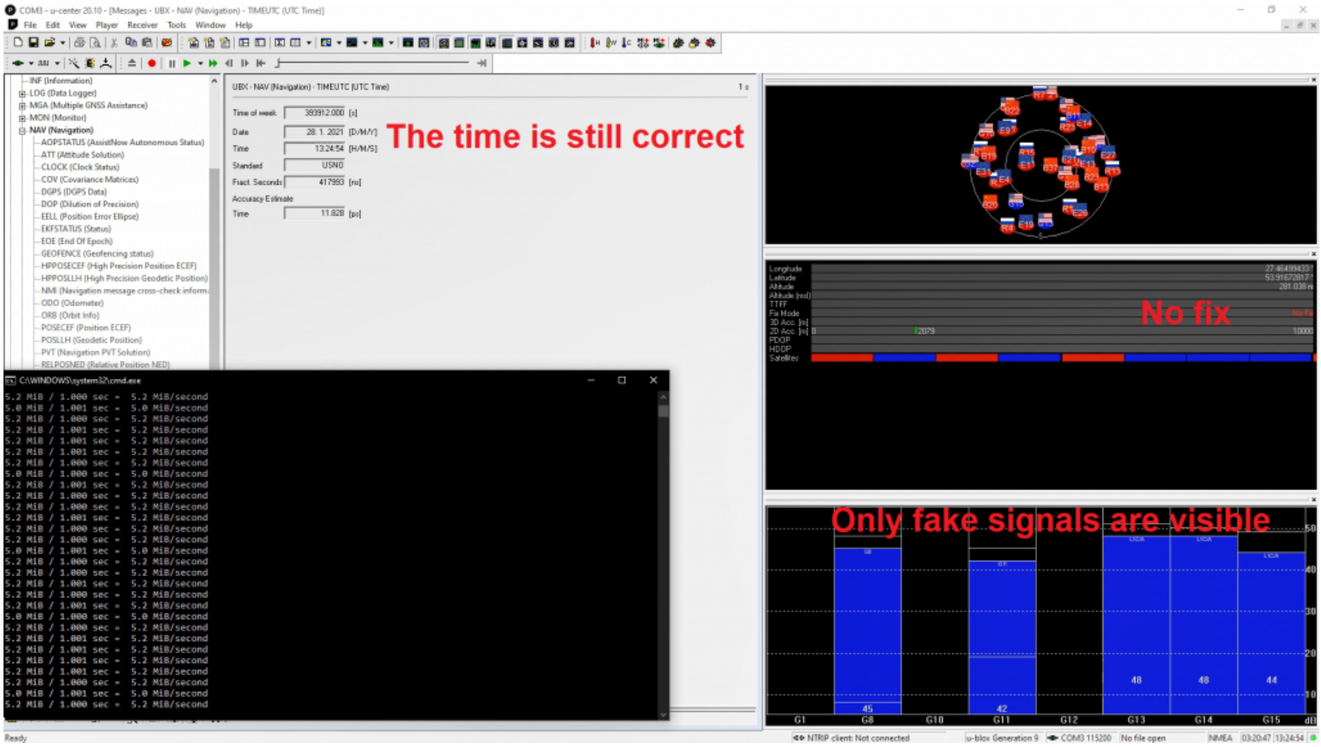
Add Multi-Band Jamming

There are two tasks for the jammer. First, we need to block real and fake signals to force the receiver into the search mode. Second, we need to decrease the jammer’s power for the L1 band. A better way to do that is by using a 10 dB attenuator:



And actually, this is the most challenging. Selecting the suitable power/distance combination between HackRF One, jammer, and target antenna is complicated.

If all done perfectly and the power is aligned, you will see something like this:


COM3 - u-center 20.10 - [Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)]
File Edit View Player Receiver Tools Window Help
INF (Information)
LOG (Data Logger)
MGA (Multiple GNSS Assistance)
MON (Monitor)
NAV (Navigation)
AOPSTATUS (AssistNow Autonomous Status)
ATT (Attitude Solution)
CLOCK (Clock Status)
COV (Covariance Matrices)
DGPS (DGPS Data)
DOP (Dilution of Precision)
EELL (Position Error Ellipse)
EKFSTATUS (Status)
EOE (End Of Epoch)
GEOFENCE (Geofencing status)
HPPOSECEF (High Precision Position ECEF)
HPPOSLLH (High Precision Geodetic Position)
NMI (Navigation message cross-check inform.
ODO (Odometer)
ORB (Orbit Info)
POSECEF (Position ECEF)
POSLLH (Geodetic Position)
PVT (Navigation PVT Solution)
RELPOSNED (Relative Position NED)
G1
G8
G10
G11
G12
G13
G14
G15
dB
10
20
30
40
50
45
42
48
48
44
NTRIP client: Not connected
u-blox Generation 9
COM3 115200
No file open
NMEA
03:20:47
13:24:54
Ready

UBX - NAV (Navigation) - TIMEUTC (UTC Time)

Time of week: 383912.000 [s]
Date: 28. 1. 2021 [D/M/Y]
Time: 13:24:54 [H/M/S]
Standard: USNO
Fract. Seconds: 417993 [ns]
Accuracy Estimate
Time: 11.828 [ps]

The time is still correct

Longitude: 27.46499433 °
Latitude: 53.91672817 °
Altitude: 281.038 m
Altitude (msl)
TTFF
Fix Mode: No Fix
3D Acc. [m]
2D Acc. [m]: 2079
PDOP
HDOP
Satellites

No fix

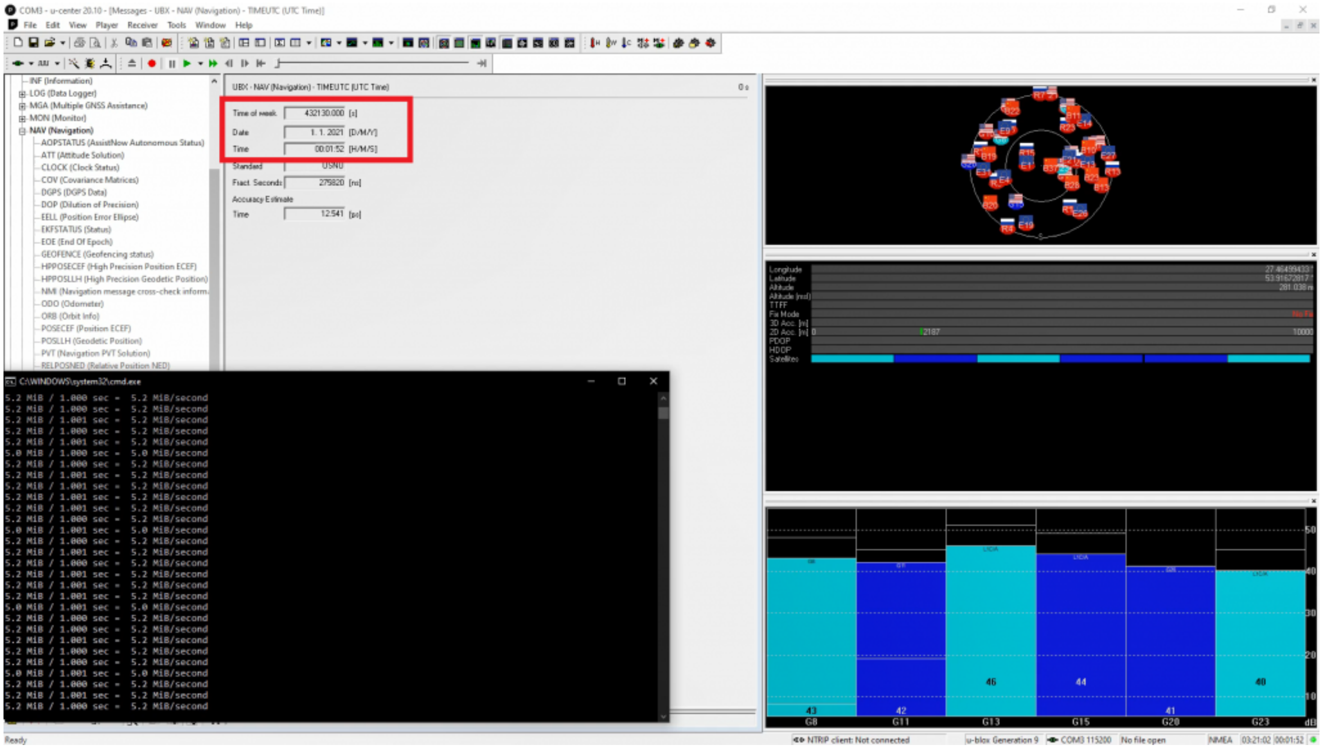
Only fake signals are visible

C:\WINDOWS\system32\cmd.exe

```
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
```

The receiver saw only simulated signals but still didn't use them.

In 45 seconds, the receiver changed the timestamp to simulated:


COM3 - u-center 20.10 - [Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)]
File Edit View Player Receiver Tools Window Help
INF (Information)
LOG (Data Logger)
MGA (Multiple GNSS Assistance)
MON (Monitor)
NAV (Navigation)
AOPSTATUS (AssistNow Autonomous Status)
ATT (Attitude Solution)
CLOCK (Clock Status)
COV (Covariance Matrices)
DGPS (DGPS Data)
DOP (Dilution of Precision)
EELL (Position Error Ellipse)
EKFSTATUS (Status)
EOE (End Of Epoch)
GEOFENCE (Geofencing status)
HPPOSECEF (High Precision Position ECEF)
HPPOSLLH (High Precision Geodetic Position)
NMI (Navigation message cross-check inform.
ODO (Odometer)
ORB (Orbit Info)
POSECEF (Position ECEF)
POSLLH (Geodetic Position)
PVT (Navigation PVT Solution)
RELPOSNED (Relative Position NED)
G8
G11
G13
G15
G20
G23
dB
Ready
NTRIP client: Not connected
u-blox Generation 9
COM3 115200
No file open
NMEA
03:21:02
00:01:52

UBX - NAV (Navigation) - TIMEUTC (UTC Time) 0 s

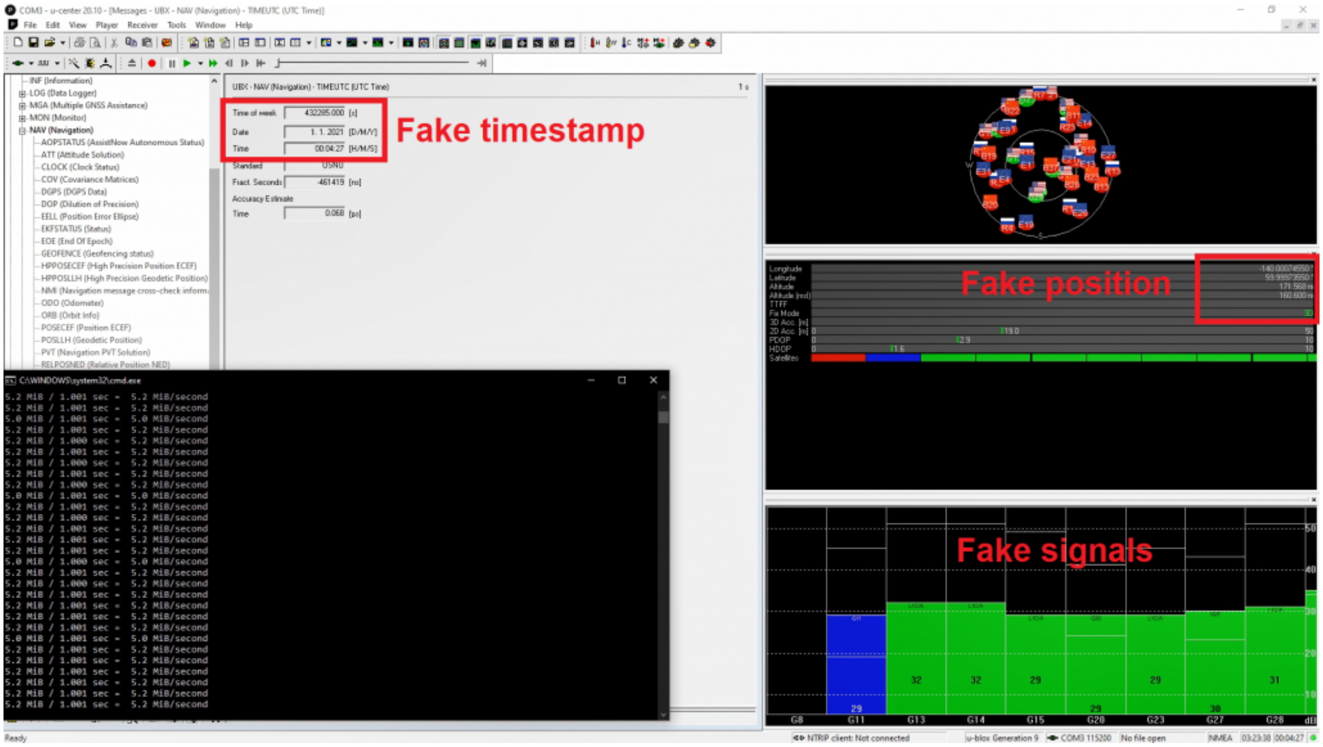
Time of week 432130.000 [s]
Date 1. 1. 2021 [D/M/Y]
Time 00:01:52 [H/M/S]
Standard USNO
Fract. Seconds 275820 [ns]
Accuracy Estimate
Time 12.541 [µs]

Longitude 27.46499433 °
Latitude 53.91672817 °
Altitude 281.038 m
Altitude (msl)
TTFF
Fix Mode No Fix
3D Acc. [m]
2D Acc. [m] 0 2187 10000
PDOP
HDOP
Satellites

C:\WINDOWS\system32\cmd.exe

```
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
```

And at last, in 3 minutes after jammer was activated, coordinates were changed too:


COM3 - u-center 20.10 - [Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)]
File Edit View Player Receiver Tools Window Help
Fake timestamp
Fake position
Fake signals
G8
G11
G13
G14
G15
G20
G23
G27
G28
dB
Ready
NTRIP client: Not connected
u-blox Generation 9
COM3 115200
No file open
NMEA
03:23:38
00:04:27

UBX - NAV (Navigation) - TIMEUTC (UTC Time) 1 s

Time of week 432285.000 [s]
Date 1. 1. 2021 [D/M/Y]
Time 00:04:27 [H/M/S]
Standard USNO
Fract. Seconds -461419 [ns]
Accuracy Estimate
Time 0.068 [µs]

Longitude -140.00074550 °
Latitude 59.99973550 °
Altitude 171.568 m
Altitude (msl) 160.600 m
TTFF
Fix Mode 3D
3D Acc. [m]
2D Acc. [m] 0 19.0 50
PDOP 0 2.9 10
HDOP 0 1.6 10
Satellites

C:\WINDOWS\system32\cmd.exe

```
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.000 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.000 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.0 MiB / 1.001 sec =  5.0 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
5.2 MiB / 1.001 sec =  5.2 MiB/second
```

Conclusion

1. The combination of gps-sdr-sim and multi-band GNSS jammer can deceive a multi-band multi-constellation receiver. We proved that under the live-sky conditions.

Disclaimer

In this research, we did not attempt to discredit UBLOX’s products. We believe they have terrific products. All GNSS receivers are susceptible to spoofing due to the nature of signals.