Communications of BAO, Vol. 71, Issue 2, 2024, pp. 409-411

Techniques for Locating GPS Jammers using GNU Radio

M. Sahakyan[1], V. Mkhoyan[1], E. Sivolenko[2], B. Hovhannisyan[2], A. Aharonyan [*2], and S. Makarov[3]

[1]Yerevan State university, Yerevan, Armenia
[2]Russian-Armenian University, Yerevan, Armenia
[3]Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

Abstract

Detecting GPS jammers is crucial for ensuring the integrity and reliability of Global Positioning System (GPS) signals, particularly in environments where jamming devices disrupt navigation and communication systems. These jammers emit radio frequency signals that interfere with legitimate GPS signals, leading to significant disruptions.

To locate these jammers, advanced techniques such as Angle of Arrival (AOA) and Time Difference of Arrival (TDOA) are utilized. AOA uses phased array antennas to determine the direction of the jamming signal, with algorithms like Multiple Signal Classification (MUSIC) and Minimum Variance Distortionless Response (MVDR) enhancing accuracy. TDOA, on the other hand, triangulates the jammer's location by measuring the time difference between signal arrival at multiple sensors.

The integration of unmanned aerial vehicles (UAVs) equipped with directional antennas and sophisticated algorithms further improves the real-time detection of GPS jammers. These UAVs can cover large areas quickly and provide precise bearing measurements, making them invaluable in both military and civilian applications.

Keywords: *GPS, Signal analysis, Jammer, GNSS, Angle of Arrival*

1. Introduction

The necessity for GPS signal jammers and defense against them has grown in importance in the twenty-first century due to the growing usage of GPS signals for worldwide positioning. Our research's goal was to find solutions for GPS locating and jamming issues. Standard GPS antennas, which normally operate in the L1 band at 1575.42 MHz and the L2 band at 1227.6 MHz (newer satellites also broadcast on L5 at 1176 MHz), are frequently used to record GPS signals. This indicates that noise transmissions in these bands are used by jammers to cause disruption.

Even in the absence of additional noise, the amplitudes of the GPS signal are extremely low, making it difficult for receivers to detect the signal [Ferreira et al. (2020)]. When further noise is added, the combined signal is lost due to amplifier cascades. The receiver system was created and tested using a variety of GPS antenna types in a range of weather and terrain circumstances in order to address this problem. We added more noise after making sure that signal detection was reliable enough. The noise was removed from the signal using signal processing techniques and mathematical modifications.

2. Methodology

Several crucial elements were included in the process for identifying and preventing GPS jamming: - Signal Acquisition: We recorded live raw GPS signals using the GPS antennas and USRP N310 receivers. Following digitization, the signals were fed into the processing chain of GNU Radio.

Pre-processing: The first step in signal pre-processing was to improve the signal-to-noise ratio (SNR) and filter out noise. In order to separate the authentic GPS signals from any jamming sources, this step was essential.

*aharon.aharonyan@rau.am, corresponding author

- Jammer Detection: To identify and localize jamming signals, sophisticated algorithms like MUSIC and MVDR were used. The system triangulated the jammers' position by examining the angle of arrival (AOA) and time difference of arrival (TDOA).

- Noise Mitigation: After identifying the jamming signals, other signal processing methods were used to lessen their effects. Adaptive filtering and interference cancellation techniques were among them. -Validation: Extensive field testing was used to confirm the efficacy of the system. In order to assess the precision and dependability of jammer identification and mitigation, the processed signals were compared with ground truth data.

3. Test Setup

We used a thorough test setup that included both hardware and software components to solve the problem of GPS jamming [Moussa et al. (2019),Ferreira et al. (2022)]. The USRP N310, a versatile software-defined radio (SDR) platform with high-fidelity signal processing capabilities and the ability to handle a wide range of frequencies, served as the main piece of hardware in our configuration. With a frequency range of 10MHz to 6GHz and a bandwidth of up to 100MHz, the device can acquire the required signals without experiencing any overflows or underruns due to its 16-bit ADC and 4RX channels. SFP+ 10Gigabit connectors have been used to link it to the host computer. Figure 1 depicts the test configuration.

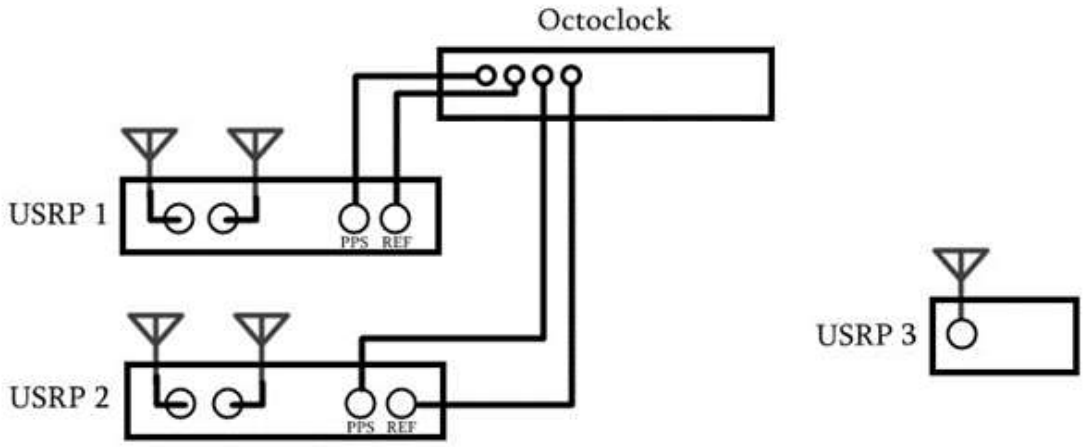

Figure 1. Test Setup: USRP N310s connected to the clock source for receiving external clock and PPS signal for synchronization. USRP N210 used as a jammer.

The software backbone of our system was GNU Radio, an open-source toolkit that allows the development of highly customized signal processing flows. The application is shown in Figure 2. Here

1) USRP Source Configuration: A block called USRP Source is used in the first phase of our signal processing loop. Through the use of the UHD driver, this block connects to our USRP hardware and sets it up to function at the L1 frequency band (1575.42 MHz) with a bandwidth of 200 kHz.

2) Phase Difference Detection: The next step involves processing the three-channel signal that was obtained in order to identify the phase difference between the receivers.

3) Angle and Distance Calculation: To determine the target's angles and distances from our system, a specially designed Python block is used.

4) Data Visualization: Visualizing the processed data is the last step in our procedure.

To make sure the system was reliable, tests were carried out in various terrains and weather situations. This covered rural, suburban, and urban environments, each of which presented different difficulties in processing and detecting signals.

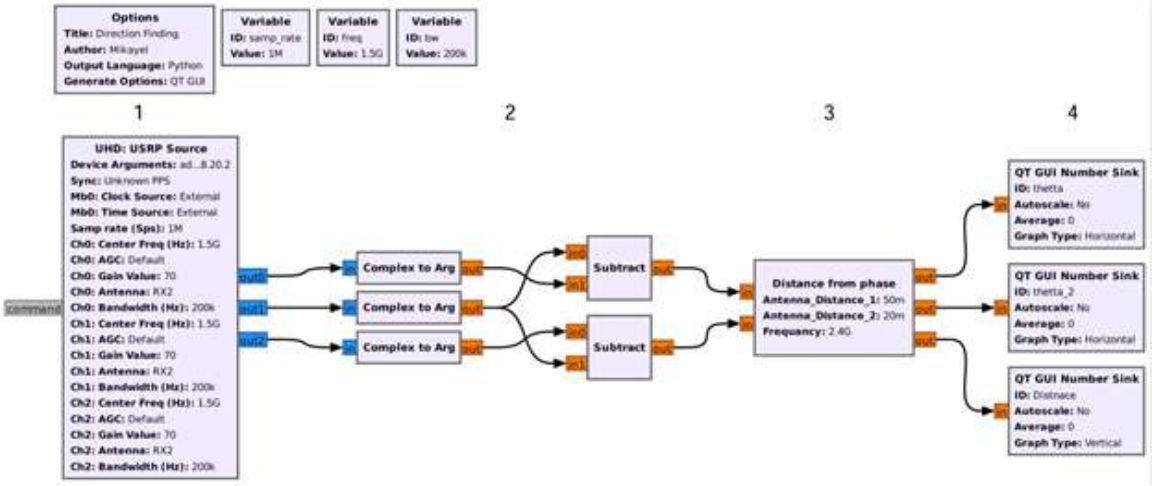

Figure 2. GNU Radio flowgraph.

4. Results

The accuracy of jammer identification was greatly increased by integrating sophisticated algorithms with GNU Radio and USRP N310 receivers. Even under difficult conditions, the system was able to detect jammers with reliability. Following signal processing and computations, Figure 3 shows the results.

Figure 3. Test results.

5. Conclusion

Maintaining the integrity and dependability of GPS signals requires the detection of GPS jammers, particularly in settings where jamming devices interfere with communication and navigation systems. These jammers cause major disturbances by emitting radio frequency signals that obstruct genuine GPS signals.

Antijamming systems can effectively use sophisticated approaches like the ones we have used to locate these jammers.

Acknowledgements

Authors thank a financial support from the Ministry of Science and Higher Education of the Russian Federation (state assignment 075-03-2024-004/5).

References

Ferreira R., Gaspar J., Sebastiao P., Souto N., 2020, Wireless Personal Communications, 115, 2705

Ferreira R., Gaspar J., Sebastião P., Souto N., 2022, Sensors, 22, 1487

Moussa M., Osman A., Tamazin M., Korenberg M. J., Noureldin A., 2019, Sensors, 19, 5532