Detecting GPS Jamming and Spoofing Using Data Collected From GPS Receivers in Android Devices

Emilia Michalek[a], Deniz Caglar[b], and Kirill Levchenko[b]
[a] University of Illinois at Urbana-Champaign, Champaign, IL
[b] Department of Electrical & Computer Engineering University of Illinois at Urbana-Champaign, Champaign, IL

Introduction: How Does GPS Work?

- The US Global Positioning System (GPS) is one of the many systems that fall under the category of a Global Navigation Satellite System (GNSS). Some of these systems are global while others are region-specific.
    - Apart from GPS, other navigation systems include the European Galileo system, the Chinese BeiDou Navigation Satellite System (BDS), and the Russian Federation GLObal Navigation Satellite System (GLONASS). (Kaplan & Hegarty, 2017)
- GPS is a system designed to allow communication between satellites and GPS receivers in devices like phones to determine the receiver's geographical location.
- This system utilizes the signals received from multiple satellites containing both ranging code (communicating a precise time measurement at the moment of sending the signal) and ephemeris info (providing data such as the position and velocity of the satellite at the given time). (Kaplan & Hegarty, 2017) The receiver uses this information in combination with an internal clock to determine its location relative to each satellite. Overlapping these measurements from multiple satellites gives the final receiver location as shown in Figure 1 below.

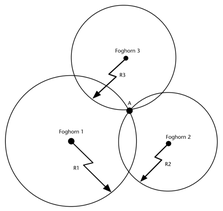

Figure 1. Determining location through overlapping ranges of possibility. This illustration shows how a receiver's location (point A) can be determined using the calculated relative position of the receiver to three separate satellites. (Kaplan & Hegarty, 2017)

What is Jamming and Spoofing?

- Jamming and Spoofing occurs when someone wants to interfere with the GPS signal your device is receiving.
    - **Jamming** is the broadcasting of noise on the same frequency as the GPS signal causing the receiver to lose sight of the real signal, thereby losing navigation capabilities.
    - **Spoofing** occurs when a signal is sent out to both drown out the real satellite signal and to broadcast a fake signal overtop, effectively convincing the device it is still receiving a legitimate signal.
- Spoofing is more dangerous in this sense because it may not be detected, yet the receiver device will likely be incorrectly navigated.

Purpose: Why Do We Need to Be Able to Detect Jamming and Spoofing?

- Jamming and Spoofing are techniques often used maliciously. These can be directed at a receiver with the intent of taking away its navigational capability or even to steer the receiver itself, as is often the case with spoofing.
    - A spoofed signal is interpreted by a receiver the same way a non-malicious satellite signal would be. This means that the device can be "convinced" it is somewhere it isn't, meaning it can also be steered if its destination is known because it will continue to try and correct its path based on where its being told it deviates.
    - These techniques are most commonly found in military or war-related applications.
- Both jamming and spoofing can also be implemented for the personal benefit of the spoofer or jammer as it may be directed at a personal or tracking device to interrupt the signal or convince the device or tracker that it is in a desired location when it is not.

Methods

- Our focus at this point in the study has been collecting and analyzing data from GPS receivers in Android phones. The primary tool we used for this was the GnssLogger App by Google, which provided us with files containing raw GNSS measurements.
- We collected baseline records on three different Android devices as well as records with possible authentic spoofing and/or jamming instances from Ankara, Turkey collected by Deniz Caglar.
- Our first approach with the files we collected was to extract the data we were interested in and plot it as a function of time using the Python matplotlib library as well as ephemeris files and functionality from the Skyfield package.
- Although the graphs were very rough, they gave us a better sense of what each piece of data represented and how it could be useful moving forward.

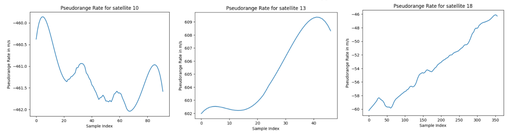

Figure 2. Plotting the Data. The 3 plots shown above are an example of one of the data points we plotted to examine more closely: Pseudorange Rate (m/s). The file we pulled this data from was one of our baseline records where the receiver was stationary while collecting data. Examining these graphs along with the description of the measurement in question allowed us to discover that this measurement can tell us whether a satellite is approaching the receiver, passing directly over the receiver, or moving away from it.

Using Doppler Shift to Detect Spoofing

- Spoofers have been developed with numerous techniques over the years to create believable satellite signals, however, one aspect that can be easily overlooked and difficult to implement is accounting for Doppler shift in the frequency being broadcasted.
- We can see this aspect being overlooked when searching for potential spoofing hardware such as the Spirent GSS6560 12-Channel GPS Simulation System and others like it. This hardware, we see, can recognize and implement a doppler shift, however it is set as a constant which isn't fully realistic, especially with a moving satellite and receiver.
- The issue resides in the fact that satellites are constantly moving in orbit around the Earth, whereas a spoofer transmitting a signal to some target GPS is likely stationary or at least not moving in orbit the way a satellite would.
    - This creates a situation where an authentic satellite signal traveling at a given velocity and at a given position in orbit (specified in the ephemeris files it transmits) would create a determinable Doppler shift in the frequency as it is being received, while a stationary signal generator would not, or would otherwise exhibit an inaccurate shift.
- We can leverage this fact to aid in our detection of spoofing. Using data provided to us by the signal itself we can calculate what should be the component of the satellite's velocity in the direction of the receiver.
- We can then compute the expected Doppler shift the receiver should be detecting and compare this to the actual Doppler-shifted frequency measured by the receiver.

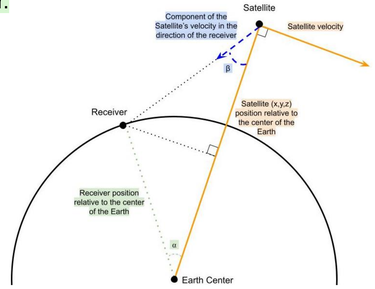

Figure 3. Determining the Component of Velocity in the Direction of the Receiver for Utilization in Calculating the Expected Doppler Shift. Components in orange solid lines represent information taken from Ephemeris data sent by the satellite. Dotted components in green represent information obtained by determining the receiver's theoretical location as usual, using navigational information from multiple satellites. Dashed components in blue were calculated with the use of trigonometry given the angles and lengths of sides in orange and green. Obtaining the component of velocity in the direction of the receiver tells us how fast the satellite is approaching or moving away from the receiver, allowing us to calculate the expected Doppler shift.

Detecting Jamming

- In comparison to spoofing, jamming is simpler to detect in theory; Jamming occurs when an excess of noise interferes with the receiver's ability to receive and decode a GPS signal.
- With this in mind, we can check for the level of noise at the frequency we are receiving and see if it is interfering with our signal to the point of being unable to read it. If it is, we have a case of GPS jamming.
- However, we must also keep in mind that excess noise or an unclear/non-reliable GPS signal is not always the result of purposeful jamming. There are multiple factors that can cause interference with the signal. Physical signal blockades like buildings or even heavy foliage can interfere with a signal reaching the receiver successfully. (Kaplan & Hegarty, 2017)

Future Work

In the future we plan to focus on generating both jamming and spoofing scenarios to further analyze how signs of spoofing and jamming manifest themselves in a controlled dataset. We intend to test an implementation of our theory on detecting spoofing using Doppler shift by putting it up against both controlled jamming and spoofing instances, as well as running it on authentic data collected from Ankara, Turkey.
We hope to develop a solution that will be able to detect jamming and spoofing while using the more limited technology of a typical GPS receiver in an Android phone as opposed to needing specialized equipment.

References

Kaplan, E. D., & Hegarty, C. J. (2017). Understanding GPS/GNSS Principles and Applications (3rd ed.). Artech House.

Google LLC. (2020). GnssLogger App (v3.0.6.4) [Mobile app]. Google Play Store. https://play.google.com/store/apps/details?id=com.google.android.apps.location.gps.gnsslogger&hl=en

Acknowledgments

Special thanks to Professor Kirill Levchenko and Deniz Caglar for their dedicated work on this project, as well as the GearUp team and staff, for organizing the GearUp summer research and transfer program.