GPS Spoofing

By Adam Chapman, ECE '17

Introduction

Many navigation systems rely heavily on GPS signals to determine their location in time and space. By transmitting false GPS signals to these systems, it is possible to remotely take them over. This has potential applications to the problem of rogue drones.

GPS Overview

The Global Positioning System (GPS) is comprised of a network of satellites that continually broadcast timestamped messages describing their locations in space. GPS receivers use these timestamped messages to determine how long it took for the signals from each satellite to reach the receiver. Multiplying this time by the speed of light gives the distance between the receiver and each satellite. These "pseudoranges" may be combined to solve for the receiver's position and the time of day.

GPS Spoofing

The structure of the GPS signal is known to the public and the frequencies that it uses are low enough to be generated with commercial-off-the-shelf equipment. This means that it would not be difficult (or expensive) for an adversary to build a system that creates signals that would appear to a receiver to be from GPS satellites. Transmitting these false GPS signals to receivers may cause them to lock onto the false signals instead of the authentic satellite signals. This is called *GPS spoofing* (Humphreys, Ledvina, Psiaki, 2008). By adjusting the time delays that tell the receiver how far away it is from each satellite, the adversary could alter the position that the receiver solves for. Therefore, if a navigation system relies on GPS to determine its location, GPS spoofing provides a way to effectively take it over.

Overt Spoofing

As the name implies, an overt spoofing approach makes no attempt to conceal the attack. A jam-then-spoof strategy is used: the counterfeit GPS signals are simply broadcast at a significantly higher power level than the authentic satellite signals, which are extremely weak by the time they reach the surface of the Earth. The authentic signals are lost underneath the spoofer's more powerful signals, causing the target receiver to attempt to reacquire lock on satellites. It then finds the spoofer's signals, allowing the spoofer to take over. The problem with this approach is that the receiver will lose GPS lock for some period of time, after which the spoofer's signals could lead to a jump in the positioning solution. Overt spoofing may be defeated by performing simple checks; however, the majority of receivers - including those used in drones - do not bother performing anti-spoofing. This is a vulnerability that adversaries could easily exploit.

Covert Spoofing

In applications that require more delicacy than overt spoofing provides, a covert spoofing approach may be used. To covertly take over a GPS receiver, the spoofer must align counterfeit signals with the authentic ones, then increase the spoofer power level to ensure that the receiver locks onto the false signals (Psiaki, Humphreys, 2016). This allows the receiver to be taken over without causing a loss in GPS lock; without realizing it, the receiver switches from the real satellites to the spoofer's satellites. Figure 1, below, provides a graphical depiction of this. The spoofer may then adjust the delays, pulling the receiver away from the authentic satellites and causing erroneous positioning solutions. This

approach requires tracking of the target and careful timing of the signals so that they arrive aligned with the authentic signals. It is the electromagnetic analog of a quarterback throwing the football in front of the receiver.

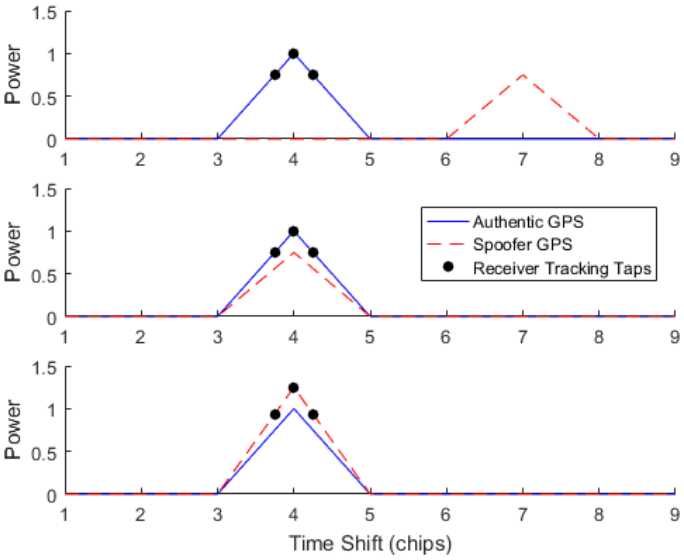

Figure 1: Covert Spoofing Attack
Plot 1: Spoofer generates fake GPS signals (not aligned)
Plot 2: Spoofer aligns signals with authentic GPS signals
Plot 3: Spoofer increases power; the receiver is captured

One of the focuses of this project was to assess the relationship between how well the spoofer signals are aligned with the authentic ones and the power levels required for receiver capture. This would determine how well a spoofing system would need to track its target and time the transmission of its signals. It also determines how much power could be saved by choosing covert spoofing over overt spoofing.

Connection to Drone Interdiction

Systems that rely heavily on GPS to determine their location, such as ships at sea, are highly vulnerable to being spoofed (Bhatti, Humphreys, 2015). This is the case with civilian UAVs (Unmanned Aerial Vehicles, hereafter referred to as drones), which often use GPS alone to determine their location. Civilian drones have become incredibly popular over the last several years, finding uses in photography, surveying, inspection, and even agriculture. With this increased popularity comes an increased risk of the misuse of drones. Common examples of drone misuse include close encounters with airplanes, the smuggling of drugs and other prohibited items into prison yards, and the use of drones by terrorist groups for reconnaissance and bombing operations. This has prompted the government to search for solutions to the problem of drones being flown in restricted areas. Since drones rely on GPS for navigation, spoofing may provide a solution to this problem (Kerns, Shepard, Bhatti, 2014). By sending false GPS signals to a rogue drone, it may be misled into landing in a location of the spoofer's choosing. This could save lives by redirecting bomb-laden drones to safe areas.

Conclusion

Many systems rely on GPS for positioning and timing information. The open nature of the GPS signal structure makes it vulnerable to GPS spoofing, which may be done either overtly or covertly. The former is easy but uses more power (increasing the likelihood of fratricide) and is also more easily detected. The latter is more complicated and requires more components, but uses less power and provides a seamless takeover of the target system. Rogue drones present a grave threat to national security, and GPS spoofing may provide a way to safely redirect them to safe areas.

References

Bhatti, J., & Humphreys, T. (2015). Hostile control of ships via false GPS signals: Demonstration and detection. *Submitted to Navigation, in review*.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr, P. M. (2008, September). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the ION GNSS international technical meeting of the satellite division* (Vol. 55, p. 56)

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617-636.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE*, *104*(6), 1258-1270.