Jammers and Spammers: Vulnerabilities of the Global Navigation System

Mary Matthews

Tufts University

December 15, 2015

Abstract

The Global Positioning System (GPS), has found numerous applications since its inception; aside from playing a key in worldwide transportation, GPS data is used in multiple facets of daily life. This paper examines some pitfalls associated with increased reliance on GPS, primarily those stemming from the use of the L1 signal, which is used for civilian purposes. This will also take note of any measures that are being taken to prevent these vulnerabilities from being exposed, or at least minimize the damage caused by exploiting these weaknesses.

To The Community

The United States has reached a point where GPS, once a technology primarily used for military applications, is heavily integrated into daily life. Besides the obvious navigation applications for both commercial vehicles (delivery trucks, airplanes, boats, etc.) and integrations into mapping applications for cars and phones, GPS receivers have found uses in other aspects of our lives. By making them accessible to smartphone applications, they've been used to 'check-in' to various locations (Facebook, Swarm), track fitness (Track My Run), gaming (Ingress) and have even been used for dating[1] (Tinder, Grindr), just to name a few.

GPS's timing capabilities are also used in a myriad of ways; probably one that most people are unaware of is that GPS is used in financial institutions. Since stock-trading has gone digital, and the speed at which transactions can occur has increased, time-synchronization has become key when performing trades. Synchronized once per second, systems apply GPS-derived time stamps to each trade that is made.

Probably one of the most important things to note, is the proliferation of drones, which extensively use GPS. One of the "must-have" Christmas items of 2015, drones have finally reached a price point where they are cheap enough for many consumers to consider purchasing; the Consumer Technology Association predicts that over 400,000 drones will be bought by Americans this year (Selukh, 2015). In fact, drones have come so popular, the Federal Aviation Administration (FAA)[2] has had to rapidly update its rules and policies around civilian drone usage, such as limiting use within a 5 mile radius of airports, within national parks and within populated areas like Washington DC. These are likely to change, as Amazon has announced plans for Amazon Prime Air, which will use drones to deliver small packages, cutting down delivery times from a matter of days to a matter of hours (even minutes). The FAA has granted Amazon permission to perform limited testing within certain parts of the US, and Amazon has also been performing some testing at a location in Canada. Google also

[1] Or activities loosely related to dating.
[2] From a legal standpoint, drone are classified as aircrafts, and thus fall under the jurisdiction of the FAA.

has a drone-delivery project in the works (Project Wing), which is currently being tested in Australia, and has even begun talks with the FAA about bringing it to the US. Google seems optimistic; project lead Davis Voss has predicted that Project Wing could be delivering goods to people as soon as 2017.

Yet in all this excitement, the discussions around GPS and security tend to focus more on the tools that use GPS, not the system itself. For example, with increased drone usage, a major concern is the violation of privacy; what is to stop the government, companies or even the neighborhood voyeur from spying on individuals? One part of the solution to this problem is the FAA's evolving regulations, another is the concept of geo-fencing, where GPS receivers would override user-input once it has been determined that they have entered a no-drone-zone, either forcing the drone to land, or navigate back to open space. This is partially implemented, but operates under the assumption that the GPS data used to make that determination is functioning perfectly.

Despite the fact that researchers have been voicing concerns about this issue since the late 90's, the public doesn't seem to be informed about this topic. The security surrounding GPS is taken for granted, and there is little to no conversation about whether GPS is actually a safe tool to use. How is GPS data processed, and what security measures are in place to ensure that data's integrity? What risks do we expose ourselves to as we become increasingly reliant on this tool? The goal of this paper is to serve as a gateway into these issues, by highlighting some recent research into how GPS can be exploited and what safeguards need to be put in place. Hopefully by raising some of these concerns, we can introduce a healthy amount of skepticism into the public mind when it comes the use of GPS and ensure backup measures are available for times when GPS fails.

Introduction to the Global Positioning System

When starting a discussion about the Global Positioning System (GPS), it is very important to establish what it is not. Some may use Global Navigation Satellite System (GNSS) interchangeably with GPS, which is not entirely correct. There are several GNSSs in operation, including GPS, Russia's Global Orbiting Navigation Satellite System (GLONASS) and China's Beidou system; there is another currently in development, the European Union's Galileo project. Each system consists of a low-orbiting network of satellites designed to provide location information to receivers on Earth. For the purposes of this paper, the discussion will focus primarily on the use of GPS, not the other GNSSs.

GPS is a constellation of at least 24 satellites and a ground control network, first launched by the Department of Defense (DoD) in 1978 and deemed fully operational in 1995. The system is actually designed to support up to 30 satellites, with six orbital planes that have 5 spots: one spare, and four with active satellites.[3]

[3] This is designed such that a GPS receiver can have access to a minimum of 4 satellites at once (in most areas, there can be 6-8).

The status of the satellites are publically available, and the number that are currently in operation can be checked on the DoD's GPS website. GPS can be used to provide the following information to GPS receivers: position (both vertical and horizontal), relative velocity, and time. At one point, this network only provided precision up to 100 meters by using selected availability (which purposefully introduced errors) on civilian signals, but this was turned off on May 1, 2000, and as updates are made to the network, this capability will be completely removed. This feature was implemented as a way to limit navigation resolution, specifically to deter enemies who might use GPS to target weapons. However, benefits of allowing civilian signals to have the same precision as the military frequencies proved to be an effective argument to abolish selective availability (and since then, the US has looked into other ways to ensure GPS is not misused). As a result, most commercially available GPS receivers are now accurate within 10 meters; differential GPS (DGPS) uses an addition land-based receiver, and is able to provide results that are accurate within a single meter. All satellites transmit using the same frequencies, the L1 C/A (1575 MHz) and the L2 (1227 MHz) bands. The L2 signal is encrypted and reserved to military use. The L1 C/A signal is not encrypted (although are portions that are pseudo-random, and can be used for verification purposes), and is what is used for civilian applications.

Vulnerabilities of GPS

Before even talking about some the techniques that employed to subvert GPS signals, it's important to note that the system is not without its inherent flaws. It has well-established that the GPS signal is relatively weak by the time it reaches receivers back on Earth. This has caused the system to be error prone due to fairly normal occurrences. Its performance can be impacted by the presence of tall buildings, dense tree cover, and even cloudy skies. Powerful solar flares have even been known to shut down the system temporarily. This is due to the fact that solar flares can alter the properties of some of the molecules within Earth's atmosphere, which ends up making the particles absorb radio signals.

Attacks which target GPS focus on the receiver, not the satellites nor other sections of the ground system. One reason is because the consequences of doing so are extremely high – since the system in maintained by the US government, any perceived attack on the system may be treated as a terrorist threat or an act of war. Although criminals may not be deterred by legal ramifications, another reason is that it's not an effective use of resources; a system that would be capable of targeting a satellite or incapacitating one of the ground control units would likely take a considerable amount of money to construct, and would require a large of power to operate.

This leaves the receiver as the primary target; this makes considerable sense, since receivers are widely available as standalone products or embedded into everyday items, which makes them an ideal candidate for

experimentation. Other research has also demonstrated that it's easier to tamper with the incoming signal, since it's relatively weak by the time it reaches receivers. These types of attacks tend to use one of two strategies, signal jamming or signal spoofing. Signal jamming blocks the GPS signal in its entirety, rendering a receiver and any system dependent on it useless. Signal spoofing involves creating a false GPS signal targeted at the receiver.

In a discussion of GPS vulnerabilities (and particularly drones), an example that inevitably comes up is the 2011 Iran-U.S. RQ-170 incident, where Iran took down an American drone flying in Iran's airspace. In an interview with the Christian Science Monitor, an Iranian engineer claimed to have taken down the drone with a combination of GPS spoofing and jamming techniques. Although certain aspects of this story are worth following, this paper will not include that incident in its examination. This is because the engineer who claims responsibility has yet to provide sufficient evidence to prove his case, and many experts have criticized the plausibility of this explanation. In addition to lack of evidence, neither government has confirmed many of the specifics surrounding the incident, so the discussion that could take place would be based on speculation, and thus not be appropriate to delve into with this paper. Instead, we're going to examine research that has been presented to the scientific community, along with events that are well-documented or easy to reproduce.

Signal Jamming

Signal jamming is a highly-illegal, heavy-handed approach, which can disable a GPS receiver. These jammers are often marketed under the guise of creating a "quiet zone", which may sound ideal in a variety of places, like restaurants or libraries, which would benefit from limited electronics use. However, it is illegal to sell, purchase or use one of these jammers, as they interfere with communications. Jammers can be employed to cover up criminal activities; for example, GPS trackers that are part of a car's security system are often difficult to find (especially if there are multiple instances of these trackers attached to a single car). Car thieves often will employ signal jammers to ensure that the location of the car they've stolen cannot be traced. The main issue with signal jamming is that it has an area of effect, and cannot accurately target a particular receiver. This has caused issues when trucks or other vehicles employing signal jamming have passed close to transportation hugs. In particular, the effect of GPS jammers can have devastating effects on ports, since boats tend to be heavily reliant on GPS; jammers can also be placed in shipping containers which may have enough proximity to a ship's GPS in order to mess with the ship's system, or other GPS trackers used to track a container's location. Signal jamming can even have results on a national level; since 2010, North Korea has jammed GPS signals in South Korea multiples times, each instance lasting multiple days. These attacks were able to effect large portions of South Korea, and were powerful enough to even disrupt the military signals. This might be seen as a

way for North Korea to level the playing field against more technologically advance nations; if enemies cannot GPS, then any system or weapon dependent on GPS guidance would becomes useless. Regardless of intent, this has prompted South Korea and other nations to look into solutions to both prevent GPS signal jamming and finding backups for when GPS signals are being drowned out.

Signal Spoofing

If there is a person to ask about GPS spoofing, Todd Humphreys (an assistant professor at the University of Texas at Austin) would certainly rank as one of the foremost experts in the area. He has published numerous articles on GPS-spoofing techniques, given a TED talk, testified before Congress, and has even conducted several impressive demonstrations showing that GPS spoofing is indeed a threat to take seriously. One of his most notable experiments is from 2013, where he and his team were able to take control of an $80 million superyacht by tricking the boat's GPS.

In cooperation with the captain of the "White Rose of Drachs", the experiment took place in June of 2013, off the coast of Italy. At over 30 miles away from shore, the yacht's navigation relied solely on GPS signals. Humphreys's team used their custom GPS spoofing device to first intercept GPS valid GPS signals, which they then used to create counterfeit data which aligned perfectly with those that the yacht's receivers would pick up. They then gradually started sending fake data targeted at the ship's receivers. As the team increased the strength of their signal, they were able to successfully trick both the primary and backup GPS systems on board; since neither system was reporting any errors nor inconsistencies, the attack went unnoticed. Also since the magnified signal they were sending out was at most 3 times the strength of the normal GPS signal, it didn't trigger any noise detection. According to Humphreys's, this was a key element, since noise detection is one way to tell if signals are being tampered with. However, there is typically a glaring difference in the magnitude of a jamming versus a GPS signal, so it would be simple to detect. Since Humphreys's team was able to create a signal that so closely copied the original, it was near impossible to detect.

This allowed Humphreys's team to subtly shift the ship's direction, by sending signals that indicating that the ship was drifting slightly off of its planned path. The need for course-corrections are fairly common, as they could be caused by something as simple as fluctuations in current strength, and are carried out directly by the captain or by an auto-piloting system. Indicating that the ship was moving starboard relative to its planned trajectory would require that the captain would apply a course correction by shifting the ship's path slightly toward the port side. This is precisely what happened and after tricking the crew into performing this adjustment several times, Humphrey's team successfully navigated the ship onto a parallel path which was hundreds of meters away from its original track. Considering that the spoofing device was made from about $2000 worth of

parts, that 90 percent of the world's freight is moved by sea (Zaragoza, n.d.), *and* most boats rely purely on GPS signals when sailing across oceans, the implications of this experiment should certainly be cause for alarm.

A more recent development in GPS spoofing was presented at Defcon earlier this year by the Unicorn Team. Belonging to Qihoo 360, a Chinese internet security company, this team specializes in security surrounding radio technologies. Unicorn Team's primary goal with their work has been creating a low-cost GPS emulator, since up until that point, the costs for purchasing one was in the thousands. Pointing to Humphrey's GPS simulators, which were relatively inexpensive, the Unicorn Team also raised the issue that it was difficult to create your own simulator without already being experts in the area of navigation, so they wanted to see if they could also create an emulator composed of commonly used parts, specifically those used with software defined radio.

To accomplish these goals, they used a combination of GPS antennae, software defined radio and some open-source coding projects to record GPS signals and then retransmit the data. This was an early success, as phones readily accepted this information. The next step was to figure out how to create their own data, and pass it off as genuine. This proved to be a more difficult challenge, as they needed to make a lot of modifications to the coding tools they were using. They also needed to closely examine the Ephemeris data (publically available) provided by GPS signals in order to help them create more realistic messages.

Ultimately, Unicorn Team's hard work paid off, and not only were they able to trick receivers into using false coordinates, but they also were able to trick them into using incorrect times. The team was able to demonstrate success with a variety of devices, including different models of smartphones, an embedded car navigation system and even a drone. The interesting part with the drone is that they selected a model DJI drone, which has some geo-fencing capabilities built it. In this case, the drone was programmed to land if it detected if was in a no-fly area. Unicorn Team was able to circumvent this programming, and made the drone fly in a forbidden part of Beijing by tricking the drone into thinking it was in Hawaii. They also forced the drone to land by feeding it a location within one of the forbidden zones. Not only does this research demonstrate how simple it is to take control of a drone by manipulating GPS signals, but also that it can be done with parts that cost only a few hundred dollars and publically available code.

Defenses and Recommendations to Mitigate Vulnerabilities

Now that it has been firmly established that attacks on GPS receivers can have disastrous results, what kinds of strategies do experts recommend to mitigate this threat? Despite the implications of these experiments, both Humphreys and Unicorn Team feel optimistic about the use of GPS.

At the end of their Defcon presentation, Unicorn Team suggests using a combination of technologies. One strategy would involve verifying GPS data using information from the other GNSSs (GLONASS, Beidou or Galileo). This is perhaps not as effective as hoped, considering that the techniques employed by Humphreys's team are capable of targeting receivers for those systems with a few minor modifications. Another strategy they suggest is verifying GPS data within applications, either by using algorithms to detect false GPS signals, or by using other sources to confirm location. Cellular networks and Wifi hotspots can both fulfill this function, as cell-towers and Wifi routers both tend to maintain static locations. They also touch lightly on the idea of extending GPS messages to include digital signatures, making it more difficult to spoof. The main issue with this idea is the actual implementation; it will cost a large amount of money, and more importantly, most receivers are expecting messages in a certain format, so any changes to that message format would need to be phased in gradually and still have a period of legacy support as the switch is made.

Humphreys also agrees that updates to the GPS message needs to be made, suggesting that more random data is embedded into messages. He also emphasizes that no single defense is perfect, so employing a combination of defenses would be the best strategy. One strategy would be to employ more techniques to determine whether the integrity of the GPS signal has been compromised. For signal jamming, this problem is not too difficult, as there are already a slew of devices that can detect when jamming is being employed, and there are even a few tools that can help detect and locate the source of the jamming signal. There are even products being developed to augment the GPS signal and reduce the efficacy of signal jamming.

For spoofing, this proves to be more of a challenge. Luckily, researchers have been working on systems to determine whether received GPS data is genuine. In a follow-up experiment to Humphreys's yacht hack, a team from Cornell developed a system that is able to process GPS signals in real-time to figure out whether spoofing is being employed. The system is also capable of recording data for further in-depth analysis. This team was able to test its system on Humphreys's GPS spoofer and was able to accurately detect when the spoofer was generating falsified data.

Researchers aren't the only source of improvements for dealing with this problem. The DoD is currently introducing 3 new civilian frequencies, which will aid both in system accuracy, and help to overcome some signal weakness issues (like trees). The FAA already has strict regulations which require airplanes to have alternative systems in place to aid in navigation should GPS fail. The eLORAN system, which would solve this issue for boats, is currently in testing phases, and is not susceptible to the same signal tampering attacks as GPS.

Conclusion

GPS receivers are a huge vulnerability; the data we use is unencrypted, unauthenticated and has almost no protection, since it is left out in open. Research has shown that it's no longer a difficult task to tamper with

the signal that is being transmitted, either by generating false data, or blocking the signal in its entirety. But by acknowledging these security flaws, we can understand the risks posed by relying on this technology. Despite the fact that many of the systems reliant on GPS do not currently employ many of the security measures available to them, governments are beginning to add more regulations around GPS use, primarily by ensuring that alternative systems are in place when GPS signals fail. Researchers are also actively making steps towards fixing these vulnerabilities, primarily through detecting when the signal has been compromised and adding tools that can be used to verify GPS data. Despite the fact that the current state of security surrounding the global positioning system looks grim, overall, the future of the system looks promising, presuming that fixing any flaws is made a priority.

References

(n.d.). Retrieved from Federal Avatation Administration: http://www.faa.gov/

Becerra, L. (2015, November 3). *Google Says Project Wing Drones WIll Be Delivering To Our Doorsteps By 2017*. Retrieved from Gizmodo: http://gizmodo.com/google-says-project-wing-drones-will-be-delivering-to-o-1740260543

Farivar, C. (2013, July 29). *Professor fools $80M superyacht's GPS receiver on the high seas*. Retrieved from ARS Technica: http://arstechnica.com/security/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas/

Huang, L., & Yang, Q. (2015, August 8). *GPS Spoofing: Low-Cost Simulator.* Retrieved from DEF CON Communications: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf

Humphreys, T. E. (n.d.). *GPS Spoofing and the Financial Sector*. Retrieved from Cockrell School of Engineering: http://radionavlab.ae.utexas.edu/images/stories/files/papers/summary_financial_sector_implications.pdf

NovAtel. (2012, June). *Mitigating Threat of GPS Jamming*. Retrieved from Novatel: http://www.novatel.com/assets/gajt/pdf/gajt-white-paper.pdf

Official U.S. Government information about the Global Positioning System (GPS) and related topics. (n.d.). Retrieved from http://www.gps.gov

O'Hanlon, B. W., Psiaki, M. L., & Humphreys, T. E. (2013). *Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals*. Retrieved from Cockrell School of Engineering: http://radionavlab.ae.utexas.edu/images/stories/files/papers/rt_spoof_detection.pdf

Olson, P. (2015, August 7). *Hacking a Phone's GPS May Have Just Got Easier*. Retrieved from Forbes: http://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/

Scott, L. (2015, 30 April). *Jamming Signals Criminal Activity in Intermodal Ports*. Retrieved from GPS World: http://gpsworld.com/protecting-position-in-critical-operations/

Selukh, A. (2015, December 14). *No Longer A Toy: Regulators Say Drone Operators Are Pilots*. Retrieved from NPR: http://www.npr.org/sections/thetwo-way/2015/12/14/459661265/no-longer-just-a-toy-regulators-say-drone-operators-are-pilots

Waterman, S. (2012, August 23). *North Korean jamming of GPS shows system's weakness*. Retrieved from The Washington Times: http://www.washingtontimes.com/news/2012/aug/23/north-korean-jamming-gps-shows-systems-weakness/?page=all

Wesson, K. D., Evans, B. L., & Humphreys, T. E. (2013, December 3). *A Combined Symmetric Difference and Power Monitoring GNSS Anti-Spoofing Technique*. Retrieved from Cockrell School of Engineering: http://radionavlab.ae.utexas.edu/images/stories/files/papers/sandwichGSIP2013.pdf

Zaragoza, S. (n.d.). *Humpreys Research Group Successfully Spoofs and $80 million Yacht at Sea*. Retrieved from Cockrell School of Engineering: https://www.ae.utexas.edu/news/features/humphreys-research-group