United States Military Dependence on GPS and Vulnerability to Radio Frequency Interference

By Jonathan Traester, ECE '19

Introduction

The Global Positioning Service (GPS) is the most widely used navigation in the world. Most Americans likely think of GPS as a tool that map applications on their smartphones employ to get them from one place to another. If GPS suddenly went down, many Americans would struggle to navigate anywhere out of the ordinary, and would be forced to turn to outdated, less efficient, and more error prone navigation techniques such as MapQuest or physical maps. GPS dependent services such as Uber and Lyft, for example, would no longer function as the drivers would not be able to locate their clients. Although these are some issues the average American would face, the consequences of military GPS failure would be far more drastic than civil navigation inconvenience. If the GPS dependent services of the United States military and law enforcement no longer functioned, American lives could be at risk.

As United States military systems have become increasingly dependent on GPS, the navigation system's susceptibility to catastrophic tampering has become an imminent threat for armed forces. The following sections of this report will explore the technical details of GPS functionality, how GPS can be compromised with signal interference, and the dependence of GPS within the United States military.

How GPS Works

The Navigation System with Timing and Ranging (NAVSTAR) Global Positioning System (GPS) utilizes the positions of satellites with known orbits to calculate a position fix of a user on the ground, in water, or in the air above Earth. The GPS system was originally built at a cost of 21 billion dollars by the United States [1]. The system was originally planned to be used solely by the United States military, but was opened up in 1980 as a globally available system.

The GPS satellite constellation originally consisted of a baseline of 24 satellites in 6 orbital planes [3]. Each satellite is at an altitude of roughly 20,200 km and orbits the Earth twice per day. The United States has committed to maintaining the functionality of at least 24 satellites, but currently manages 31 operational satellites [5]. The active constellation consists of an expandable baseline of 27 satellites, with 4 backup units, as seen in Figure 1.

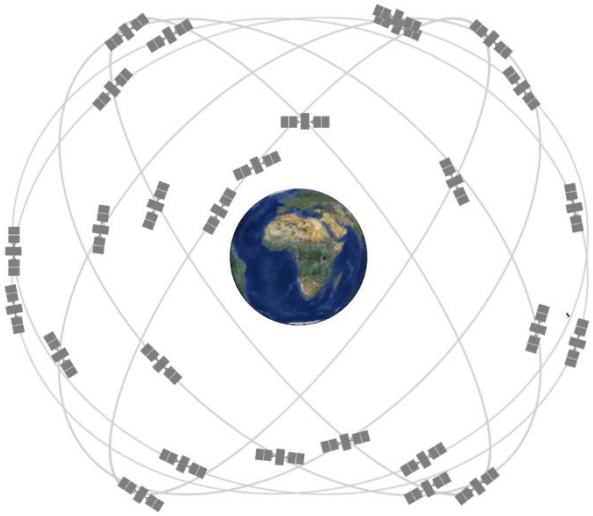

Figure 1 – Current Expandable 27 -Satellite Baseline [5]

Each of these satellites sends signals to the receiver on Earth when in range. The satellites are equipped

with atomic clocks that send exact time signals to the receivers [8]. The receivers calculate the time it takes to detect the signals from four satellites to calculate how far away the satellites are from the receiver. Then, using the known locations of the four satellites, it is possible to solve for an exact position in three dimensions: East, North, and altitude.

All GPS satellites transmit continuous-time signals on the same two center frequencies called L1 and L2 [4]. The United States has reserved the highest accuracy GPS utilization for its own government and military systems. L1 carries both a signal for civilian users as well as an encrypted signal for Department of Defense authorized users. L2 carries just the signal for authorized users [4]. The L2 signals reserved for United States military are not only of higher accuracy, but are also used by military forces to ensure they are receiving a legitimate signal, rather than a spoofed GPS signal.

The information transmitted by the satellites is modulated by a code unique to each satellite, allowing the receivers to differentiate between satellites sending information on the same carrier frequencies [4].

The standard positioning service codes for civilian users is labeled as C/A code, which stands for course/acquisition [4]. The code for DoD authorized users is labeled as P(Y) code.

Additionally, GPS transmits a navigation data message [4]. This message carries the GPS satellite time, the satellite clock offset, satellite status and health, and the satellite ephemeris date and almanac, which is the coarse orbit, status information for all satellites, and data regarding error correction.

As seen in Figure 2, L1 carries the C/A code as well as the P(Y) code and navigation message, while L2 carries just the P(Y) code for authorized DoD users [11]. The transmission scheme is a type of spread spectrum transmission. This transmission method allows receivers to differentiate between satellites that are transmitting on the same frequencies.

Direct Sequence Spread Spectrum (DS-SS) is employed to spread the signal energy over the bandwidth of the signal [4]. DS-SS equips the system with a built in defense against narrowband interference, because narrowband only targets a specific section of the bandwidth, typically around the carrier. Unfortunately, DS-SS does not effectively prevent broadband interference, which is discussed in greater detail in the following sections.

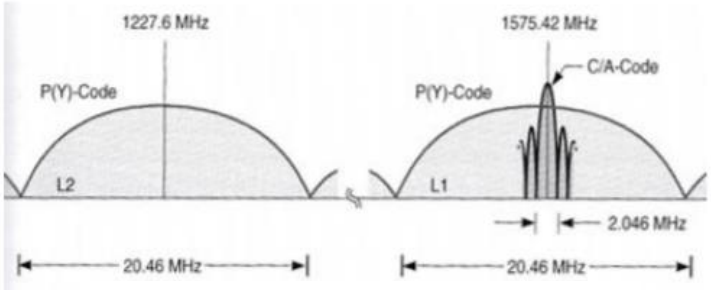

Figure 2 – Power Spectra of GPS Signals on L1 and L2 [11]

Military Dependence and Vulnerability

Nearly all military navigation and tracking systems have adopted GPS as their primary tool [6]. The navigation system is required on all United States military systems, and is a NATO standard.

GPS is a dual-use system, which means that both civilian and military have access to essentially the same technology [1]. Although P(Y) codes are reserved for only military, the accuracy and functionality of the civil system is almost the same. After the United States government opened the technology up to the public, most advances in the GPS system were made by commercial companies. Thus, most of the GPS technology that the United States military uses is commercial off-the-shelf technology. As a result, the military uses GPS

technology that may have been designed for peacetime, rather than times of war where more stringent technology may be required [1].

Since GPS is a public technology, it is possible for any entity to understand exactly how the system was designed. This opens risk of enemy entities developing effective technology to reduce functionality of the GPS system that the United States military depends upon.

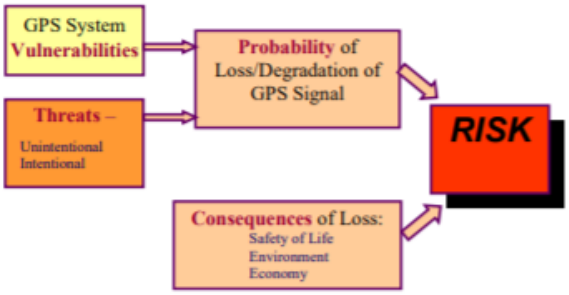

Figure 3 – GPS Risk Assessment [9]

Vulnerabilities to GPS functionality can take the form of unintentional interference, intentional interference, and human factors issues [6]. Signal jammers are quite simple to make, and pose a massive risk to United States military systems. A standard 100 watt lightbulb is 10^{18} times more powerful than a GPS signal going to a receiver [6]. It does not take much power to generate a signal that can interfere with a weak GPS signal. Jammers are inexpensive and deadly to a GPS, as described in technical detail in the following section.

In Hoey and Benshoof's paper on GPS vulnerabilities, the primary mitigation strategy is to "remember the technology is merely a tool to enhance response capabilities" [6]. Older, less-technical navigation strategies are outdated, slow, and inaccurate. Furthermore, it is likely that although military officers are taught backup navigation techniques, much of the military personnel is out of practice with other navigation techniques, because they have been using GPS every day for well over a decade.

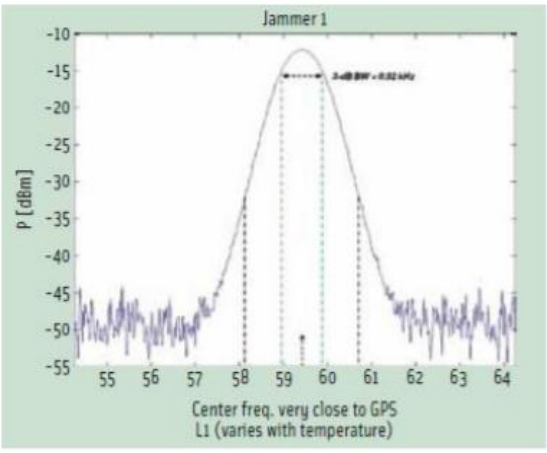

Figure 4 – Spectrum of a narrowband RFI signal [10]

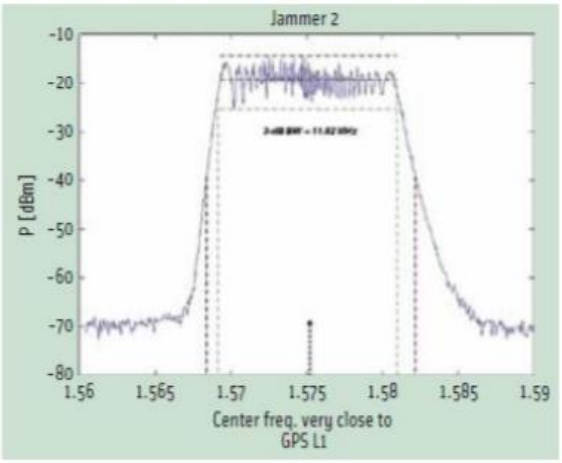

Figure 5 – Spectrum of a broadband RFI signal [10]

GPS Signal Interference

Signal interference comes in the forms of intentional and unintentional interference, and can lead to inaccurate or completely dysfunctional signals [7]. Unintentional interference often takes the form of broadcast television, VHF transmitters, and personal electronic devices. Intentional interference is often jamming, spoofing, and meaconing. This report will focus on signal jamming, because it is the simplest, cheapest, and most common method of interference.

Technology for GPS jamming is inexpensive, simple to build, and available on the open market. Radio frequency interference (RFI) is either pulsed or continuous [4]. Continuous wave RFI can be either narrowband or broadband. Narrowband RFI is

typically achieved via transmitting signals concentrated in a small bandwidth around the center frequencies of GPS, L1 and L2. Broadband targets a larger range, sometimes up to the entire range of C/A or even P(Y) signals.

Several functional GPS jammers for civil use are available on the market. In a study conducted by Mitch et al, 18 different civil GPS jammers were tested and characterized. Nearly all the jammers transmitted signals broader than the civilian bandwidth, and some of the jammers had a greater bandwidth than the larger DoD-reserved signals [12]. Most of the jammers employed a form of broadband radio frequency interference. The GPS jammers in this study were largely effective in disrupting and corrupting NAVSTAR signals with simple technology [12]. This was not the only study that found simple GPS technology to be highly effective.

A study done by Kraus et al, tailored from the Mitch et al study, analyzed continuous wave and broadband interference of several civil GPS jammers. Most of the jammers employed a center frequency of roughly L1, which is the GPS center frequency that carries the civil data [10]. The study upheld the theory that narrowband continuous wave jamming is not nearly as effective as broadband RFI due to the spread spectrum of NAVSTAR signals.

Figure 4 and Figure 5 exhibit two spectrums of a narrowband and broadband jamming signal respectively [10]. The narrowband jamming signal seen in Figure 4 has a 3dB bandwidth on the order of 10kHz, centered around the center frequency L1. The idea is that by jamming the carrier frequency L1, the data will not be readable by the receiver. However, the spread spectrum disperses the power around the entire bandwidth, thus allowing the receiver to still acquire data. The broadband signal seen in Figure 5 has a bandwidth of about 12MHz, which covers more than half of the P(Y) bandwidth, centered around L1.

Broadband interference such as the signal seen in Figure 5 is much more effective at corrupting GPS signal [4]. Without RFI, the receivers can extract low powered GPS signal data by knowing the satellite's signature code. But, a high enough noise level due to RFI leads to inadequate processing gain. Thus, a high enough jammer-to-signal ratio can easily corrupt GPS signals at the same frequency, especially since the GPS signals have such low power. Additionally, as signal jammer hardware approaches the receiver, the jammer power increases and corrupts the GPS signal.

Summary

With the United States military nearly dependent on GPS, and the system's vulnerability to jamming, a backup system to GPS that does not rely on NAVSTAR technology is essential. Every United States military system uses GPS, and civil infrastructure is becoming increasingly dependent on the NAVSTAR system. Signal jammers are inexpensive, simple to build, and highly effective. Critical United States systems that are prone to signal interference need a backup system that can estimate their position in a relatively timely manner. Even a system that can achieve a rough position fix would be a highly useful alternative to outdated navigation techniques.

References

1. Adams, T. (2001). GPS Vulnerabilities. *Military Review*,*81*(2). Retrieved from https://www.questia.com/library/journal/1P3-70549670/gps-vulnerabilities.

2. Alterman, S. (1995). GPS Dependence: A Fragile Vision for US battlefield Dominance. *Journal of Electronic Defense, 18*(9). Retrieved from http://go.galegroup.com.ezproxy.library.tufts.edu/ps/i.do?id=GALE|A17613495&v=2.1&u=mlin_m_tufts&it=r&p=AONE&sw=w

3. Gabor, M. (n.d.). GPS Overview. *University of Texas Austin*. Retrieved November 1, 2018, from http://www.csr.utexas.edu/texas_pwv/midterm/gabor/gps.html#anchor1735013

4. Glomsvoll, O. (2014). Jamming of GPS & GLONASS Signals. *Nottingham Geospacial Institute*. Retrieved from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2389675/Glomsvoll.pdf?sequence=

5. GPS.gov. (2018). Space Segment. *National Coordination Office for Space-Based Positioning, Navigation, and Timing*. Retrieved from https://www.gps.gov/systems/gps/space/.

6. Hoey, D., & Benshoof, P. (2005). Civil GPS Systems and Potential Vulnerabilities. *Defense Technical Information Center*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a440372.pdf

7. Hofmann-Wellenhof, B. (2008): GNSS—Global Navigation Satellite Systems: GPS, GLONASS, Galileo and more. Wien and New York: Springer.

8. Integrated Mapping. (2014). How GPS Works. Retrieved from https://www.maptoaster.com/maptoaster-topo-nz/articles/how-gps-works/how-gps-works.html

9. John A Volpe National Transportation Systems Center. (2001). Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.

10. Kraus, T., Bauernfeind, R., Dötterböck, D. and Eisfeller, B. (2011). Car Jammers: Interference Analysis in GPS World, October 2011, pp. 28-35.

11. Misra, P. and Enge, P. (2001) Global Positioning System Signals, Measurements, and Performance. Ganga Jamuna Press, MA.

12. Mitch, R. H., Dougherty, R. C., Psiaki, M. L., Powell, S. P., O'Hanlon, B. W., Bhatti, J. A., & Humphreys, T. E. (2011). Signal Characteristics of Civil GPS jammers. In *24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011* (Vol. 3, pp. 1907-1919)