GPS Spoofing Countermeasures

Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Los Alamos National Laboratory
Los Alamos, New Mexico, 87545

Abstract:

Civilian Global Positioning System (GPS) receivers are vulnerable to a number of
different attacks such as blocking, jamming, and spoofing. The goal of such
attacks is either to prevent a position lock (blocking and jamming), or to feed the
receiver false information so that it computes an erroneous time or location
(spoofing). GPS receivers are generally aware of when blocking or jamming is
occurring because they have a loss of signal. Spoofing, however, is a
surreptitious attack. Currently, no countermeasures are in use for detecting
spoofing attacks. We believe, however, that it is possible to implement simple,
low-cost countermeasures that can be retrofitted onto existing GPS receivers.
This would, at the very least, greatly complicate spoofing attacks.

Introduction:

The civilian Global Positioning System (GPS) is widely used by both government
and private industry for many important applications. Some of these
applications include public safety services such as police, fire, rescue and
ambulance. The cargo industry, buses, taxis, railcars, delivery vehicles,
agricultural harvesters, private automobiles, spacecraft, marine and airborne
traffic also use GPS systems for navigation. In fact, the Federal Aviation
Administration (FAA) is in the process of drafting an instruction requiring that
all radio navigation systems aboard aircraft use GPS [1]. Additional uses include
hiking and surveying, as well as being used in robotics, cell phones, animal
tracking and even GPS wristwatches. Utility companies and telecommunication
companies use GPS timing signals to regulate the base frequency of their
distribution grids. GPS timing signals are also used by the financial industry, the
broadcast industry, mobile telecommunication providers, the international
financial industry, banking (for money transfers and time locks), and other
distributed computer network applications [2,3]. In short, anyone who wants to
know their exact location, velocity, or time might find GPS useful.

Unfortunately, the civilian GPS signals are not secure [1]. Only the military GPS
signals are encrypted (authenticated), but these are generally unavailable to

civilians, foreign governments, and most of the U.S. government, including most of the Department of Defense (DoD). Plans are underway to upgrade the existing GPS system, but they apparently do not include adding encryption or authentication to the civilian GPS signal [4,5].

The GPS signal strength measured at the surface of the Earth is about –160dBw ($1x10^{-16}$ Watts), which is roughly equivalent to viewing a 25-Watt light bulb from a distance of 10,000 miles. This weak signal can be easily blocked by destroying or shielding the GPS receiver's antenna. The GPS signal can also be effectively jammed by a signal of a similar frequency, but greater strength. Blocking and jamming, however, are not the greatest security risk, because the GPS receiver will be fully aware it is not receiving the GPS signals needed to determine position and time. A more pernicious attack involves feeding the GPS receiver fake GPS signals so that it believes it is located somewhere in space and time that it is not. This "spoofing" attack is more elegant than jamming because it is surreptitious.

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory (LANL) has recently demonstrated the ease with which **civilian** GPS spoofing attacks can be implemented [6]. This spoofing is most easily accomplished by using a GPS satellite simulator. Such GPS satellite simulators are uncontrolled, and widely available. To conduct the spoofing attack, an adversary broadcasts a fake GPS signal with a higher signal strength than the true GPS signal. The GPS receiver believes that the fake signal is actually the true GPS signal from space, and ignores the true GPS signal. The receiver then proceeds to calculate erroneous position or time information based on this false signal.

How Does GPS work?

The GPS is operated by DoD. It consists of a constellation of 27 satellites (24 active and 3 standby) in 6 separate orbits and reached full official operational capability status on July 17, 1995 [7]. GPS users have the ability to obtain a 3-D position, velocity and time fix in all types of weather, 24-hours a day. GPS users can locate their position to within ± 18 ft on average or ± 60-90 ft for a worst case 3-D fix [8].

Each GPS satellite broadcasts two signals, a civilian unencrypted signal and a military encrypted signal. The civilian GPS signal was never intended for critical or security applications, though that is, unfortunately, how it is now often used. The DoD reserves the military encrypted GPS signal for sensitive applications such as smart weapons.

This paper will be focusing on the civilian (unencrypted) GPS signal. Any discussion of civilian GPS vulnerabilities are fully unclassified [9]. The carrier wave for the civilian signal is the same frequency (1575.2 MHz) for all of the GPS satellites. The C/A code provides the GPS receiver on the Earth's surface with a unique identification number (a.k.a. PRN or Pseudo Random Noise code). In this manner, each satellite transmits a unique identification number that allows the GPS receiver to know which satellites it is receiving signals from. The

Nav/System data provides the GPS receiver with information about the position of all the satellites in the constellation as well as precise timing data from the atomic clocks aboard the satellites.
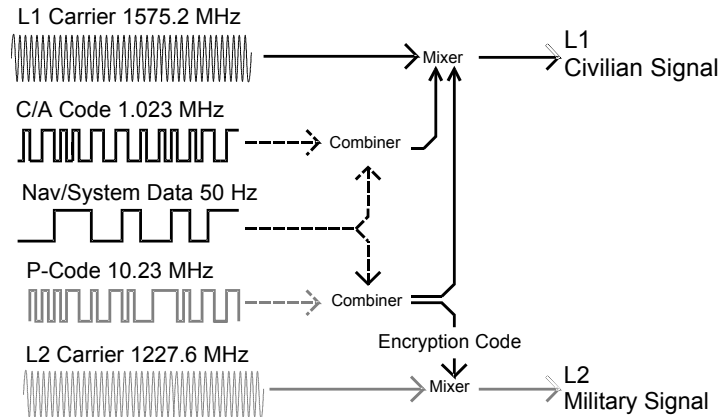
GPS Satellite Signals

Figure 1: GPS signal structure.

The receiver continuously listens for the GPS signals from space. The GPS receiver locks onto the signals from several GPS satellites simultaneously. The actual number of satellites the receiver locks onto is determined by: 1) the number of satellites in view of the receiver and 2) the maximum number of satellites the receiver hardware is designed to accommodate. Because of the C/A code identification, the GPS receiver knows exactly which satellites it is receiving data from at any given time.

Once the identification codes for each of the received satellite signals are recognized, the GPS receiver generates an internal copy of the satellites identification codes. Each satellite transmits its identification codes in 1-millisecond intervals. The receiver compares its internally generated code against the repeating C/A code from space and looks for any lag from the expected 1-millisecond interval. Any deviation from the 1-millisecond interval is assumed to be the travel time of the GPS signal from space. Once the travel time (ΔT) is determined, the receiver then calculates the distance from itself to each satellite using the following formula: Distance = ΔT x Speed of Light.
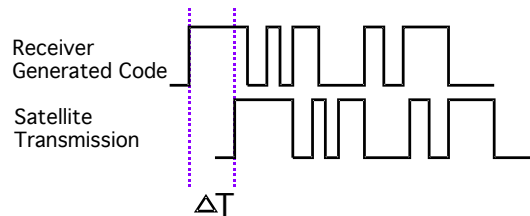

Figure 2: Example of GPS signal time delay.

One problem with this method is that the clocks on the receiver are not as accurate as the atomic clocks onboard the satellites. In addition to the time correction from the NAV/SYS data information from the satellites, the GPS receiver has a clever method of determining its own clock error, which we will discuss in a few moments.

As previously mentioned, the receiver receives the signals from several GPS satellites simultaneously. Therefore, the distance to several satellites are known at any given time. Figure 3 gives a conceptual overview given the distance of three GPS satellites (denoted by the star symbol). Note that in Figure 3 that the ranges to the satellite, as measured by the GPS receiver, do not overlap at a single point. The measured and true ranges differ due to the clock errors in the receiver mentioned earlier. The result is a distance error seen by the receiver, which is represented by the dotted line in figure 3.
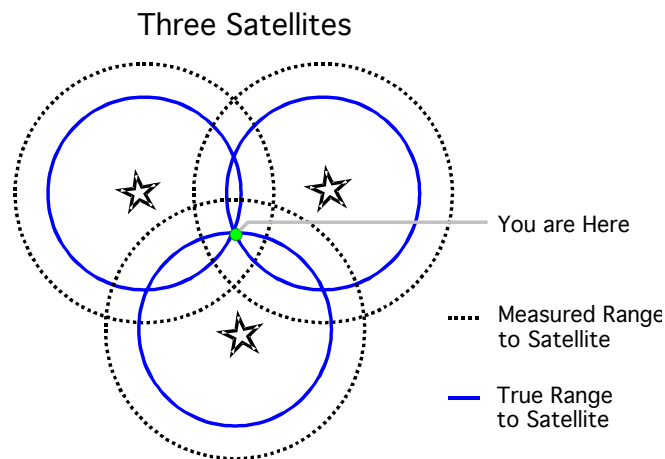
Three Satellites

You are Here

Measured Range
to Satellite

True Range
to Satellite

Figure 3: 2-D representation of finding a position.

At this point, the receiver knows it is somewhere in the area of overlap shown by the dotted line (figure 3). The receiver then interpolates this overlap area to find the center. The result of this interpolation gives two important pieces of information; 1) what the position of the receiver is and 2) the clock error of the receiver. In essence the receiver uses the correct position information to determine its own clock error.

The more satellites involved, the smaller the area of overlap and the better the position fix will be. In theory, three satellites are all that is needed for a position fix. However, in practice, four or more satellites are needed to acquire an accurate latitude, longitude and altitude fix.

Note that only one satellite is required for a time fix. The position is initially found in an X,Y,Z Earth centered/Earth Fixed co-ordinate frame and then converted to Latitude, Longitude and Altitude.

Countermeasures:

Several of the countermeasures we propose are based on signal strength, which must (at least initially) be higher for the fake signal than the true signal from space. Some of the other countermeasures involve recognizing the characteristics of the satellite simulator itself.

Many (if not all) GPS receivers display the signal strength and satellite number for each of the satellites it is receiving data from. We are unaware of any receivers that store this data and compare the information from one moment to the next.

One or more of the following countermeasures should allow suspicious GPS signal activity to be detected:

1) Monitor the absolute GPS signal strength: This countermeasure involves monitoring and recording the average signal strength. We would compare the observed signal strength to the expected signal strength of about –163 dBw (5x 10^{-17} watts). If the absolute value of the observed signal exceeds some preset threshold, the GPS receiver would alert the user. This countermeasure is based on the idea that relatively unsophisticated GPS spoofing attacks will tend to use GPS satellite simulators. Such simulators will typically provide signal strengths many orders of magnitude larger than any possible satellite signal at the Earth's surface. This is an unambiguous indication of a spoofing attack.

2) Monitor the relative GPS signal strength: The receiver software could be modified so that the average signal strength could be recorded and compared from one moment to the next. An extremely large change in relative signal strength would be characteristic of an adversary starting to generate a counterfeit GPS signal to override the true satellite GPS signals [6]. If the signal increases beyond some preset threshold, an alarm would sound and the end user could be alerted.

3) Monitor the signal strength of each received satellite signal: This countermeasure is an extension of the above two techniques. Here, the relative and absolute signal strengths are tested individually for each of the incoming satellite signals. Signals from a GPS satellite simulator will tend to make the signal coming from each artificial satellite of equal strength. Real satellite signals, however, vary from satellite to satellite and change over time. The idea here is that if the signal characteristics are too perfect, there is probably something wrong and the user should be alerted. Like the previous two countermeasures, this countermeasure could be implemented by modifying the existing software code of the GPS receiver.

4) Monitor satellite identification codes and number of satellite signals received: GPS satellite simulators transmit signals from multiple satellites (typically 10)—more than the number of real satellites often detected by a GPS receiver in the field at a given time. Many commercial GPS receivers display satellite identification information, but do not record this data or compare to

previously recorded data. Keeping track of both the number of satellite signals received and the satellite identification codes over time may prove helpful in determining if foul play is occurring. This is especially true of an unsophisticated spoofing attack where the adversary does not attempt to mimic the true satellite constellation at a given time.

5) Check the time intervals: With most GPS satellite simulators, the time between the artificial signal from each satellite and the next is a constant. This is not the case with real satellites. In other words, the receiver may pick up the true signal from one satellite and then a few moments later pick up a signal from another satellite, etc. With the satellite simulator, the receiver would pick up signals from all of the "satellites" simultaneously. This is an exploitable feature of the satellite simulator that could be used to tell if the signals were coming from the true source or a false simulator-based source.

6) Do a time comparison: Many current GPS receivers do not have an accurate clock. By using timing data from an accurate, continuously running clock to compare to the time derived from the GPS signal, we can check on the veracity of the received GPS signals. If the time deviates beyond some threshold, the user can be alerted to the possibility of a spoofing attack. As the VAT has demonstrated, very accurate clocks can be small and inexpensive, and operate on very low power.

7) Perform a sanity check: A small, solid-state accelerometer and compass can be used to independently monitor the physical trajectory of the receiver (heading, velocity, etc.), mounted, for example, on a moving truck. The information provided by this approach can be used to double check the current position fix reported by the GPS receiver based on a previously reported position. In a sophisticated spoofing attack, the adversary would send a false signal reporting the moving target's true position and then gradually walk the target to a false position. This is how an attack on a cargo truck might occur for instance. The accelerometer would serve as a relative (not absolute) backup positioning system, which could be used to compare to the position reported by the GPS receiver. A discrepancy between the accelerometer and the receiver would raise a red flag and alert the user.

All of the strategies 1-7 can be implemented by retrofitting existing GPS receivers; it is not necessary to redesign them. Strategies 1-5 can be implemented primarily through software alone. Strategy 6 could be implemented through software, or else a more accurate clock could be fitted onto the existing GPS receiver.   Strategy 7 would require both hardware and software implementation to work properly. We believe a proof of principle for countermeasures 1-7 can be demonstrated fairly quickly.

Conclusion

Although the countermeasures proposed in this paper will not stop spoofing attacks, they will alert the user of the GPS receiver to suspicious activity. This will decrease the odds that a spoofing attack can succeed, and will also require

adversaries to deploy more sophisticated methods than the simple attack we have previously demonstrated [6]. We believe the potential countermeasures proposed in this paper can be implemented easily and inexpensively, including by retrofitting existing GPS receivers.

Disclaimer & Acknowledgements

References:

[1] John A. Volpe National Transportation Systems Center, *Vulnerability Assessment Of The Transportation Infrastructure Relying On The Global Positioning System, Final Report.*, Department of Transportation, 2001, http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-v4.6.pdf.

[2] S. J. Harding, *Study into the impact on capability of U.K. commercial and domestic services resulting from the loss of GPS signals*, Qinetiq, 2001, www.radio.gov.uk/topics/research/topics/other/gpsreport/gps-report.pdf.

[3] L. Brutt, *NS/EP Implication of GPS timing*, Office of the manager National Communications System; Technical Notes, Technology and Standards Division **6** (2) (1999), www.ncs.gov/n2/content/technote/tnv6n2/tnv6n2.htm.

[4] Committee on the Future of the Global Positioning System; National Research Council; Aeronautics and Space Engineering Board, *The Global Positioning System: A Shared National Asset- Recommendations for Technical Improvements and Enhancements.* (National Academy Press, 1995), www.nap.edu/books/0309052831/html/index.html.

[5] Air Force release, *Air Force NAVSTAR Global Positioning System Fact Sheet*, Florida Today Space Online (1999), www.floridatoday.com/space/explore/stories/1999b/100399f.htm.

[6] J. Warner and R. Johnston, *A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing*, Journal of Security Administration, **25**, 19 (2002).

[7] US Coast Guard, *GPS - Frequently Asked Questions*, 2003, http://www.navcen.uscg.gov/faq/gpsfaq.htm.

[8] US Air Force, *GPS Support Center*, (2003), https://www.peterson.af.mil/GPS_Support/.

[9] Headquarters Air Force Space Command, *NAVSTAR Global Positioning System Operations Protect Guide*, Peterson Air Force Base.