UNIVERSITÀ DEGLI STUDI
DI SALERNO

The domination of the electromagnetic spectrum

Convenzione: Elettronica S.p.A.

Technical Report

Author

G. Cattaneo

Version Number: 10 – 2012-08-11 21:47:05Z

The domination of the electromagnetic spectrum
Technical Report University of Salerno

© 2012 Giuseppe Cattaneo. All rights reserved

This document has been typeset by LaTeX and the DIThesis class.

Version Number:10 – 2012-08-11 21:47:05Z

Author's email: cattaneo@unisa.it

Abstract

This document presents an overview of the Global Positioning System providing the reader with the main underlying vulnerabilities and the countermeasures that have been proposed.

Contents

Chapter 1

The Global Positioning System

1.1 Introduction

The Global Positioning System (GPS) project was started in 1973 by the U.S. Department of Defense (DoD) to provide both military and civilian users all over the world with more sophisticated features with respect to the previous projects already developed. The first official release was fully operational 21 year later in 1994 and it used 24 satellites.

It was the first satellite navigation system to be space-based and dedicated devices (receivers) can provide the users with location and time information if there are at least four satellites in the line of sight.

Although the GPS was originally introduced by U.S. Military, since its appearance it became the main component of many civilian applications. Even the global air traffic system has been influenced by the availability of the GPS.

Since 1994 the basic system has evolved with different steps which lead to the third generation GPS III satellites and a totally renewed ground system called Next Generation Operational Control System (OCX) part of a radical modernization project.

The basic concept of GPS is that each satellite transmits a message, on timely basis, containing information regarding its exact position and an absolute system time when the message has been sent. Starting from these information and knowing the speed of the light, the receiver can establish the distance from each satellite whose signal has been received and decoded. After that, there are several algorithms, such as trilateration, able to compute the location (three dimensional position commonly expressed as latitude, longitude, altitude) of the receiver using data received from at least 4 satellites.

Of course, reading the position repeatedly enable the receiver to compute derived information such as speed and direction of the movement.

Whereas military applications use the secure GPS Precise Positioning Service also called *Selective Availability* (or shortly *SA*), civilian applications use the Standard Positioning Service or *Coarse Acquisition* (or shortly *C/A*), which is less accurate, unauthenticated and the receivers have reduced capabilities [1]. In year 2000 the SA

[1] Civilian receivers must not be capable to work at an altitude greater than 18.000 meters and at speed greater than 1850 Km/h otherwise these would be considered weapons and the same export

feature have been discontinued.

1.2 History

1.3 The GPS Architecture

GPS actually consists of three main components (commonly named segments):

SS the Space Segment composed of a set (ranging from 24 to 32) satellites in medium Earth orbit.

CS the Control Segment composed of a master and an alternate control stations to connect all the ground antennas and the monitoring stations.

US the User Segment composed of millions of military and civilian devices.

The Space Segment

The SS was originally based on three set of eight satellites (or Space Vehicles SV) moving on three circular orbits. To provide a better coverage, this plan has evolved to 32 satellites on 6 orbits with 4 SV. These orbits have been calculates so as to ensure that in any location on the ground there are at least six SV in the line of sight.

All the orbit radius are about 26600 Km and each SV takes about 12 hours (more precisely half sideral day or 11 hours and 58 minutes) to complete its orbit.

The actual number of satellites dynamically changes over the time. In march 2008 there were 31 SVs broadcasting their signals and new launches have been planned for new generation SVs while the old SVs are retired from the service. During its evolution GPS became more reliable and accurate introducing a consistent redundancy with at least nine visible SVs from any point on the Earth.

The Control Segment

The CS groups all the ground stations dedicated to the control and the management of the GPS. Among them is worth to mention:

1. A Master Control Station (MCS),
2. a Secondary (backup) Control Station,
3. a set of 4 Ground Antennas,
4. a set of 6 Monitor Stations.

Many U.S. organizations provide their support to the design and the management of the GPS ensuring efficiency and proactive error detection. For instance MSC shares ground antennas with the U.S. Air Force Satellite Control Network (AFSCN) and monitor stations with National Geospatial-Intelligence Agency (NGA).

licenses necessary for ballistic missiles would be necessary

One of the main activity of the CS is the tracking of the orbits of the SVs. For this job the MCS shares the NGA monitoring stations located in Argentina, Australia, Baharein, Ecuador, England, Washington DC and some dedicated U.S. Air Force monitoring stations based in Hawaii, Kwajalein, Ascension Island, Diego Garcia, Colorado Springs and Cape Canaveral. More precisely, the 2nd Space Operations Squadron (2SOPS) of the U.S. Air Force is in charge of exchange all communication streams to and from each SV by means of the ground antennas available inside the CS network.

The control commands are used to synchronize the atomic clocks installed on the SVs up to an absolute precision of few nanoseconds and to correct the flight paths (ephemeris) of each SV with respect to the orbital model targeted. When a SV must change its orbit, first it is marked in state *unhealthy, then the correction is executed and, at the end, is marked again* healthy or ready to broadcast its data stream.

Another crucial component of the CS is the Operational Control Segment (OCS) which has been introduced in 2007 to replace the first mainframe operated at Schriever Air Force Base. It provides the operational capabilities to support GPS users and keeps the GPS operational checking for the expected quality of service. After the introduction of the new OCS, the system have been upgraded with a stronger security architecture dedicated only to the U.S. army. This segment will be in use up to the planned migration to the Next Generation GPS Operation Control System (OCX). These further steps for the modernization of the GPS will be described in a dedicated section.

The User Segment

The US consists of all the GPS enabled user devices. Since its first appearance GPS receivers became very popular and the number of applications enabled by the GPS services is still increasing.

A GPS device is able to receive a number of (initially only 4, currently up to 20) channels. This represent the number of satellite data streams that the device can concurrently process. It is a typical digital device with a radio section (an antenna tuned to the target frequencies), a highly accurate internal clock and a processor. Of course the device could manage a screen to visualize the current position on a map for example.

Finally there are several protocol (proprietary or open) which GPS receivers use to send the current location through a serial connection to an external device like a Personal Computer or a Smart Phone. One of the most widely adopted is the NMEA 0183 protocol, initially proposed by the National Marine Electronics Association.

Accuracy

internal clock

1.3.1 GPS Communication

Message Format

Each SV continuously broadcasts a message containing information such as its position and its deviation from the predicted trajectory, internal clock values (times-

tamp), status. Using the GPS dictionary, a GPS receiver can obtain a lock if there is an unobstructed line-of-sight to the SV.

Two encoding are used: Whereas encryption is used for restricting access to military services, an open cleartext encoding is used for public services.

The total size of the message is 1,500 bits and it is structured in 5 subframes of 300 bits each as shown in table 1.1. It is sent at a baud rate of 50 bps taking therefore 750 seconds for the entire message to be received. A subframe is a set of 10 x 30 bits data words and considering that subframe 4 and 5 are circularly switched among 25 sets of values, the transmission of the entire data set requires 25 x 1,500 = 37,500 bits messages and a total time of 6 x 5 x 25 = 750 seconds.

Table 1.1. Message Format

subframe 1	subframe 2	subframe 3	subframe 4	subframe 5
Internal clock values, GPS global time	Ephemeris (i.e. detailed SV orbit)		Almanac component (SV network synopsis, error correction, etc.)	

The first subframe encode the absolute time expressed as a week number, the seconds-into-week number and the SV status. The week number starts on January 6, 1980, and it is transmitted as a ten-bit binary values therefore it becomes zero again every 1,024 weeks (about 20 years). The modernization project is planning to extend to 13 bits the field for the week number covering 8,192 weeks (157 years).

Subframes 2 and 3 transmit the ephemeris providing detailed information about the SV position and its orbit.

Subframes 4 and 5 contains error correction data and coarse information about orbits and status for all the satellites of the system (up to 32 SV are part of the so called constellation). This is called *almanac*. The ephemeris are updated every 2 hours and remain valid for 4 hours. the almanac is updated every 24 hours.

Satellite frequencies

All SVs transmit on the same two frequencies 1,575.42 MHz (L1) and 1,227.60 (L2) as described in table 1.2. These frequencies have been reserved world-wide by the Federal Communications Commision.

Signals are encoded using the standard *code division multiple access* (CDMA) as channel access method used by many radio communication technologies. Receivers can distinguish each SV, because a unique binary sequence known as Gold code has been assigned to each SV. In other worlds signals are spread using publicly known spreading codes (pseudo-random sequences (PRN)) to encode low bit-rate data in high-rate carrier. Of course these codes (PRN) must be known to receivers in order to decode the message therefore the codes used by military services are kept secret, this enforcing signal hiding and, as a consequence, source authentication.

Two different encoding types for CDMA are used: the C/A code publicly accessible and the *precise* (P) code for restricted access services. The L1 carrier is modulated by both the C/A and P codes, while the L2 carrier is used only by the P

code. When the message is encoded for military applications it can be encrypted becoming P(Y) code that, as consequence, is available only to receivers which know the decryption key in use to the SU.S. Military Force.

Table 1.2. Frequencies

Band	Frequencies	Description
L1	1575.42 MHz	C/A and encrypted precision P(Y) messages, L1 civilians (L1C) and military (M) messages on future Block III satellites.
L2	1227.60 MHz	P(Y) messages + L2C and military messages on the BlockIIR-M or newer satellites.
L5	1176.45 MHz	Planned in the modernization process for future uses.

The modernization project have planned a new frequency band 1176.45 MHz (L5) to be used to broadcast GPS signals. It falls into a range reserved for aeronautical navigation. The first Block IIF satellite providing these services has been launched in 2009. *"L5, the third civil GPS signal, will eventually support safety-of-life applications for aviation and provide improved availability and accuracy."* [1]

Message Demodulation and Decoding

All the satellite signals are modulated in the same L1 carrier frequency and can be decoded after demodulation. Knowing the Gold code (PRN) of each SV signals, the receiver can implement the concept of *channel*.

In facts, once a lock on one SV has been obtained, the receiver can acquire the almanac determining the satellites it should listen for. For each SV (from 1 to 32) a dedicated decoder is activated and it will be in charge of monitoring and decoding signals received by a single SV. When the signal is detected the SV can be identified using its distinct C/A code pattern.

Since a recent and up-to-date almanac is necessary to start decoding messages, there can be a delay of up to 30 seconds before a receiver can provide the user with the first position.

1.3.2 Algorithms for computing the position

The GPS is based on the signals broadcasted by a number of SVs denoted SV_i from known locations $L_i^{SV} \in \mathbb{R}^3$. Each SV is equipped with an accurate and synchronized clock T^S. Signals propagates at the light speed c. A receiver U, receiving the messages sent from SVs, can determine its position located at the coordinates $L = (x, y, z) \in \mathbb{R}^3$. As the Euclidean distance between the receiver and each SV_i is $d_i = \mid L_i^{SV} - L \mid$ the signal from each SV has a time delay $t' = \frac{d_i}{c}$.

A more general approach, based on signal theory, establishes that the receiver is in a range g:

$$g(L,t) = \sum iA_i s_i \left(t - \frac{\mid L_i^{SV} - L \mid}{c} \right) + n(L,t) \tag{1.1}$$

where A_i is the attenuation suffered by the signal $s_i(t)$ and the term $n(L,t)$ generically denotes all the background noises. Since the receiver clock cannot be as accurate as the light speed would require (an atomic clock would be too expensive), and the receivers cannot participate in a two-way clock synchronization algorithm, in practice U would suffer of a clock offset δ with respect to the global system time denoted as $t = T^S + \delta$.

This is equivalent to add a fourth (after the location (x, y, z)) scalar unknown δ which can be included in the equation 1.1 as follows:

$$g(L,T^S) = \sum iA_i s_i \left(t - \frac{d_i}{c} - \delta \right) + n(L,T^S) \tag{1.2}$$

where the range distances d_i have been substituted. Defining pseudoranges as:

$$R_i = d_i + c \times \delta \tag{1.3}$$

Considering that signals from at least 4 SV_i have been received and decoded, including the SV_i coordinates the equation 1.3 results in a system of equations that can be solved providing the values for (x, y, z) and δ and therefore the exact position and time, without rely on an exact local clock. In facts, if the location of SV_i is $L_i^{SV} = (x_i^{SV}, y_i^{SV}, z_i^{SV})$ the 1.3 can be rewritten as follows:

$$(x - x_i^{SV})^2 + (y - y_i^{SV})^2 + (z - z_i^{SV})^2 = (R_i - \Delta)^2 \forall SV_i \tag{1.4}$$

From a geometric point of view, given a Δ for each SV 1.4 defines the equation of a sphere with center in L_i^{SV}

Due to the presence of data noise the set of equation 1.4 for more than 4 SVs might not have a unique solution. There are many numerical methods that can be used to solve the system such as Bancroft's method, Trilateration, or the least-mean-square approach or Newton-Raphson multidimensional method.

1.3.3 Spectrum issues

1.3.4 The Modernization Process for GPS

The OCX new role

1.4 Concept of Operations for GPS Jamming/Spoofing

eeee [2, 3]

Chapter 2

Real World Examples

Bibliography

[1] Air force successfully transmits an l5 signal from gps iir-20(m) satellite [online] (2009). Available from: http://www.losangeles.af.mil/news/story.asp?storyID=123144001.

[2] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. On the requirements for successful gps spoofing attacks. In *ACM Conference on Computer and Communications Security* (edited by Y. Chen, G. Danezis, and V. Shmatikov), pp. 75–86. ACM (2011). ISBN 978-1-4503-0948-6.

[3] Warner, J. S. and Johnson, R. G. Think GPS Cargo Tracking = High Security? Think Again. Tech. rep. (2003). Available from: http://gfp.bluetundra.com/node/1590.