Department of Informatics
Faculty of Mathematics and Natural Sciences
University of Oslo

GPS and navigation systems

Home exam in INF3510, information security

Written by:
Cindy Madeleine Svendsen Ceesay og
Torbjørn Øien

Index:

Introduction:

For thousands of years humans have used different methods to navigate, we have used the stars compasses, which side the moss grow on trees etc. Being able to navigate and reach our desired destination, have been the an important part of about every civilisation since its very beginning. Now we live in the digital era where computers have made many parts of our lives simpler and navigation is not an exception. These days the celestial constellation that are most used for navigation is a constellation of satellites.

Since its launch in 1978 GPS and its counterparts have become the norm for navigation all over the world. But with new solutions comes new problems. You have probably heard you should never keep a magnet close to a compass or it will throw it off? This can be seen as the first attack on a navigation system in human history. Are our new navigation system as susceptible to attack as its predecessor? And if so what can we do to make it more secure? These are the problems we will look at in our paper, but first we will have to learn a little bit about the navigation system.

Assumptions:

We assume that the person who reads this this already know what Personvernsnemda and Datatilsynet is.

PART 1: Navigation systems

Store norske leksikon says that navigation is the tenet about how we find the road over the sea and between the air. While Oxford dictionary define navigation as the process or activity of accurately ascertaining one's position and planning and following a route. We may thereby define navigation to calculate a position accurately. How this is done depends on which type of navigation we have. We will take a deeper breath into terrestrial, celestial, radar, radio, satellite and in-earth navigation, which we sooner are going to take a look at.

Satellite Navigation

Satellite navigation system uses series of satellites placed in specific orbits around the Earth. The receiver uses at least four satellites to measure the time taken by the signal to travel from your satellite to your receiver antenna. The first two signals that is sent from the satellite is used to calculate the centre and the radi. Knowing your distance from a third satellite fixes your position at one of the two points where the circle intersects the third sphere. A fourth satellite are needed to synchronise your receiver's clock with a common time standard which is strictly adhered to by the clocks on board all the satellites. This satellite corrects the position from the other satellites, and select one of the remaining two points as the units position.

The receiver measures travel times by comparing 'time marks' imprinted on the satellite signals with the time recorded on the receiver's clock. All satellites therefore needs to be synchronised, so that they can start transmitting their signals at precisely the same time. This is achieved by continuously synchronising all on-board atomic clocks with a master clock on the ground that always is precise.

Radar Navigation

Radar navigation is used by the marine and aviation. Radar determines the distance to an object by measuring required time for a radio signal to travel from a transmitter to the object and return. Signals are created by a timing circuit, so that energy leaves the antenna in very short pulses. The pulse repetition rate(PPR) lies on 1000 per second. If any echo is returned by this period the display brightens. A target's actual range is proportional to its distance from the center of the scop. This power will decrease in echo length as it passes through the atmosphere.

Practical power limits may be used to define the dimensions of the radar beam. This result into that the distance to the radar horizon would be the same as the geometrical horizon for the antenna height to the the surface of the Earth. If the signal does not reflect to earth it will be extended by something above it. Parallell indexing is often used to fixed this error.

Parallel indexing is a method where a bearing line drawn parallel to the original course with a known and fixed perpendicular distance between both the lines is used as a reference. This method maintain safe distance from two fixed objects simultaneously. Draw one tangent line on either site of the channel, when the lines are drawn fix them so that some fixed object is located in the center. By this way you know when to change course, if the unit turn up in a danger area. The longer the range between the scale, the lower accuracy of the measuring will be. Hand drawn must happened at the same range, so the working range scale of the radar must meet the accuracy required and that the selected index targeting will be in range. If this is not followed up an error will occur.

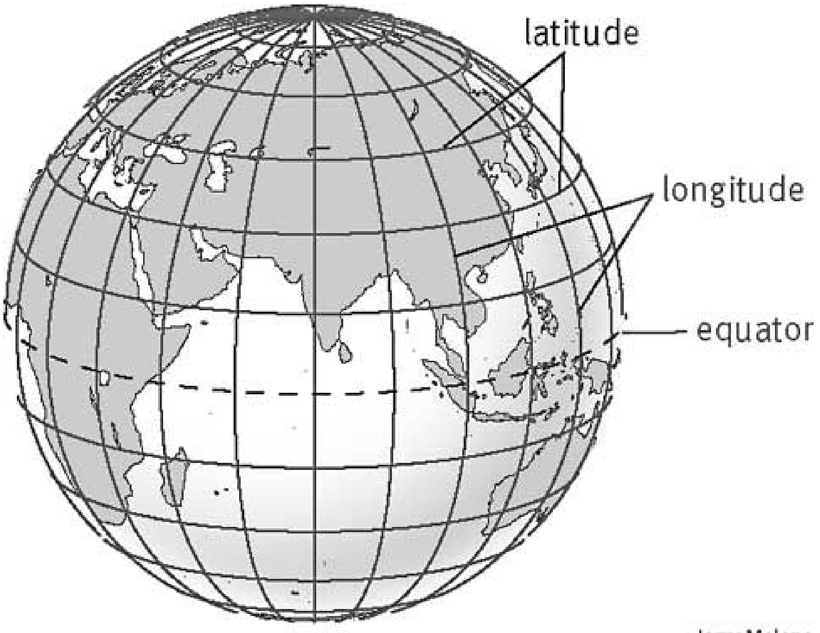
Radio Navigation

NASA says that almost all aircraft uses radio navigation equipment either as a primary or secondary navigation aid. Radio navigation provides information about the receiver's position from a station located on the ground. There are two signals that are being sent, they are both transmitted 30 times per second. The first one are sent every time the variable phase transmission sweeps past magnetic north. It is therefore sent in an non-directional reference phase. The second one however, cycles 360 around the earth, so it is sent in the rotating variable phase.

Celestial navigation

In Celestial navigation(also referred to as astronavigation) the observation of celestial body, for example stars, is input for a filter. In the filter we use the latitude, longitude, practical navigation and lunar distance to measure their height in the horizon and calculate the position. The output of the filter is the best-estimated positions to an unknown land area. It is applied in marine, space navigation systems.

Celestial navigation is also often used as a backup for GPS systems. For instance the fear of becoming hacking and malfunctioning computer navigation systems during national emergency by an enemy made the US navy start to use celestial navigation as a backup for GPS.



Jerry Malone (1)

The American Heritage® Science Dictionary

Copyright © 2002. Published by Houghton Mifflin. All rights reserved

Terrestrial navigation(Kan slettes?)

In terrestrial navigation we can decide direction and length to the position based upon known points at earth, the unit's stability, fuel consumption and the unit's speed. This navigation compromises dead recognizing, visual navigation and some other generic fixing methods. It is used by aeronautical, maritime and land applications.

Part 2: Navigation techniques

Dead reckoning

Dead reckoning(DR) is a method of estimating the position based upon known past position. To find the direction between the previous position and the current point we draw a parallel line, rolling rulers or triangles at least every hour. We update these points with direction and speed when any of these factors changes. When we have at least two lines of positions we enclose it with a circle and label it horizontally with either zone time or the Greenwich Mean time(GMT) rounded up to the nearest minute. We use this point(fix) as the new point to estimate a new position, as DR is dependent on speed.

If an navigator has not taken a fix for an extended period of time, there may be a risk that the DR will no longer show the ship's position. This could be fixed by fix expansion, where the navigator considers all factors and develops an expanding "error circle" around the DR plot. The radius to the error circle then grows with time.

Dead Reckoning is significant to errors, as it is dependent on knowing speed and the last position at all instance to calculate the current position. If the signal is lost due to slippage or surface irregularities the unit will not know it's current position. In order to correct the error we have to get a new fix by another method. A good method is to go to land and figure out it's current position. Another method is to install mobile nodes on the unit, which continuously broadcast it's geographical location.

PART 3

GPS as a trusted component in security systems.

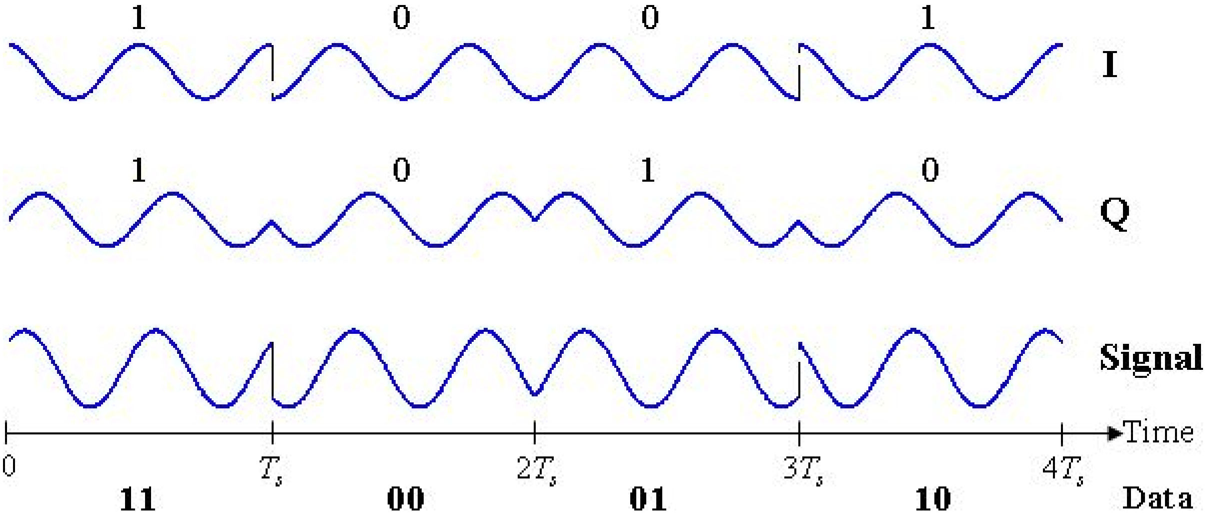
Systems often contains multiple components if the integrity of one of these components was compromised the system would not function as intended, sometimes it is difficult to identify errors as they happen. This can often lead to “grievous consequences”, it’s therefore important to ask ourself when we use GPS in our systems if it is a trusted component, the answer is no. This will be explained further later on but first we must look at why the gps is so vulnerable to attacks.

Assessing security threats against the GPS system

As stated above there are 2 kinds of gps signal; the civilian and the military. The problems discussed under are not found in the military signal as it is encrypted. Any reference to gps signal/system is therefore to the civilian.

To put it simply the gps system consists of two parts, the sender(s) and the receiver. In most cases the sender will be a satellite but there are also examples of Differential GPS or DGPS which are senders on ground level at a fixed position. The purpose of these senders are to increase accuracy of your position (from about 15m to about 10cm).

We have learned that GPS signals are simple radio signals these signals are are read by a gps receiver which performs something called Binary Phase-Shift Keying or BPSK for short this translate the radio wave into a stream of bits. It does so by for example writing a stream of 1 until a shift is detected then it writes a stream of 0.



https://upload.wikimedia.org/wikipedia/commons/b/be/QPSK_timing_diagram.png

This is the same technology that are used for your wifi signal. After the receiver have its binary data it can perform the calculations which ultimately gives us our position and time. And it is at the signal we find the real vulnerability. The data packages that are being sent between your router and computer, smartphone etc. uses encryption for example WPA. This means that if someone else catches the data packages in transmission they can make no sense of what is being sent, it also gives the router a way to authenticate the device it sends to/receives from. The civilian GPS signal does not use encryption. It seems nonsensical that it should be at first glance since the ephemeris data transmitted to your device is basicly just the position of the satellite and time any third party “catching” this data will learn nothing but their own position. The data itself is therefore not important to protect, the problem is authentication.

As stated above the gps system consists of 2 parts the sender and receiver we also know the signal are just radio signal being transmitted at a set of frequencies, we know there is no need to protect the data being sent and that it can’t be authenticated. What this means is that anyone are free to build a sender that can transmit signals identical in every way to the authentic GPS signal. This is in essence how DGPS works it is also the core security risk of the gps system.

The devices made to imitate the GPS signal are called spoofers and are surprisingly simple to build. [http://gps.mae.cornell.edu//humphreys_etal_iongnss2008.pdf] in the article “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer” the researchers buillds this kind of device with relative ease and low cost. We can therefore conclude that getting your hands on a spoofer device is no problem for any dedication person/organisation/country. We know that GPS is used as a core components in many systems and a spoofer gives you an easy attack vector to all of these. There are indeed other attack vectors against the gps system, some will be lightly discussed because it seems nonsensical to assess the security threat of an open second story window when your front door is wide open.

Before we go in deep about spoofing it is also worth mentioning jamming attacks. Every signal based system is vulnerable to jamming attacks it works quite simply by drowning out any meaningful data with noise. Imagine music turned up way to loud at a bar when you are trying to talk to someone. One person works as a sender and are sending information and one person works as a receiver and try to catch the information but all the noise drowns it out. This metaphor also covers that people in bars repeat the same information every 12,5 minute, the information mostly consists of repeating the time, their location and the state they are in.

Spoofing attacks are generally more sophisticated than jamming attacks, and more dangerous simply because it is better to receive no information at all then to receive false information. It is also much simpler to detect a jamming attack then a spoofing one. To my knowledge there are two kind of spoofing devices a stationary and a portable. The stationary simply like a DGPS station “gone evil” and instead of sending the correct data it starts to send wrong data. The portable device are in my opinion even more devious and sophisticated. It consists “mostly” of two parts a receiver and a sender. In an attack scenario the portable spoofer is set up close to the victims receiver or “VR”. Since the spoofer is close to the VR it will get a lock on the same satellites. The spoofer then can send the same data at a higher frequency than one or more of the satellites depending on the spoofer. The receiver will then lock on the spoofing device instead of the satellite(s). Now we are looking at a classic “man in the middle attack” where whoever controls the receiver also controls whatever data the VR is receiving. These attacks can have severe consequences not only for organisations/corporations/countries but also single individuals, imagine the headlines.

“Man arrested after GPS data in phone puts him at the scene of the murder.”

“Error in timestamping at US stock markets $500bn lost, new financial crisis on horizon.”

“Automated harvesting machine runs into cattle pen; millions complain over non-vegan corn flakes.

Data level spoofing attacks

Like many other modern devices GPS receivers run an OS (usually linux/windows) and can be considered small computers. But these devices are not treated as computers and are therefore not patched and vulnerabilities are left in the system. We have previously discussed spoofing attacks as a way “trick” the device with false position/time. It is possible to use these methods to manipulate the device on data level in order to do damage to the OS itself.

Middle of the earth attack:
A part of the ephemeris data is the square root of the semi-major axis of the satellites orbit. (sqrt A) If the satellite were in the middle of the earth this variable would be (sqrt A) = 0. This will of course never happen to a satellite but with a spoofer device there is no problem sending this data to a receiver. In the article[kilde] this attack is tried and one of the receiver tested caught an exception and crashed. The authors of the article guessed it was a divide by 0 error.

GPS receivers use a 10 bit week counter for keeping up with time. This means that every 20 or so year 10 bit = 1024, 1024/52 ≈ 19,7 we get a rollover event. These 10 bits are a part of the ephemeris data and can be spoofed. If the attacker fist send a signal with all 10 bits set, then send a signal with none of the bits set the receiver will think a rollover event has occurred and will add +1 to a counter. This means we can increase the receiver clock with about 20 years every minute or so. It is also worth noting that the week-counter bit sequence is supposed to be increased to 13 bits, in order to reduce the occurrence of the week rollover event from every 20 years to 160 years. This will make these kinds of attacks much more severe than before.

What does these kinds of attack accomplish? It will stop the GPS from being a reliable time source. It can cause problems for the GPS receivers OS. (Going past unix time, some windows OS only work properly within a set of years) A bit like the iphone year 1 bug.

We also have NTP-Servers, NTP stands for Network Time Protocol and is how the clock on most modern computers are set. To get an accurate time these servers needs to be synced up with an accurate clock. The problem is that these clocks are very expensive, the solution was to use GPS signals to get the correct time GPS satellites also contains an atomic clock as stated above. According to the cited article[nr] About 60% of NTP servers use GPS as a timesource. This is an excellent example of how GPS is used as a trusted component in a system. A set of these receivers could be spoofed and this would cause thousands of computers to get the incorrect time or at least cause denial of service.

Some gps receiver can also have its software/maps updated through usb/sd cards. The problem with this is that some of them will run unsigned code the. The researchers in [kilde nr.] tried this and was able to get root access in many of the receivers they tested.

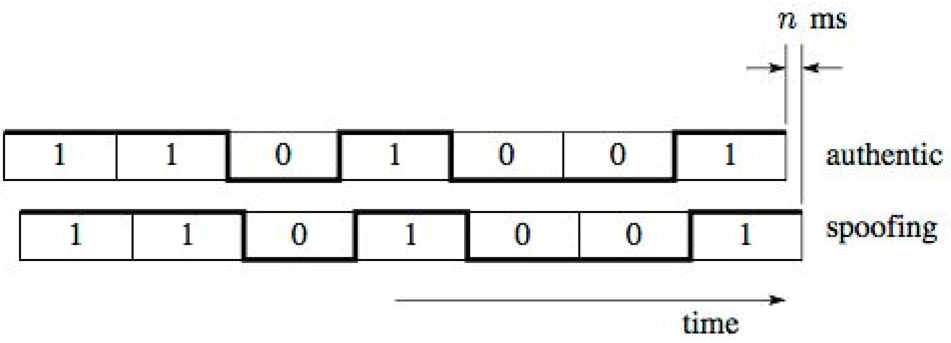
This shows that spoofing attacks on GPS is not only limited to sending false positions, but can also attack the gps on the data level. This is a huge vulnerability in receiver since one spoofing device located “close” to large numbers of GPS receivers could potentially crash most of them.

https://users.ece.cmu.edu/~dbrumley/pdf/Nighswander%20et%20al._2012_GPS%20software%20attacks.pdf

Solutions:

We have seen many different attacks on a GPS receiver but it is also important to look at how these vulnerabilities can be fixed or at least minimized. A GPS receiver is typically too trusting and too dumb. A more secure receiver needs to be smarter and be able to detect an attack and perform countermeasures. Since making huge changes to the GPS system will be hard and probably extremely expensive.

We have discussed that gps receivers in essence are computers but are treated as devices it might be up to the users to make sure that the software are regularly updated to patch security holes in their system. Things like the middle of the earth attack can simply be stopped by throwing nonsensical values. Time desynchronisation attacks can also easily and pretty inexpensively be fixed if the receiver contains a cheap internal clock that is checked against the ephemeris data and then throw away time/date that is obviously wrong. It is important to note that these countermeasures might create new unforeseen security risk.(The more complex the system the more attack vectors) In [http://gps.mae.cornell.edu//humphreys_etal_iongnss2008.pdf] it is proposed a bit latency defence. Earlier in the text we explained how a spoofing attack works. This kind of attack will often have a latency on the bitstream compared to the authentic signal and this makes it possible to detect be a smart receiver. Here it is also important to note that the latency could probably be reduced to ≈ 0 by a more advanced/sophisticated spoofing equipment but it is considerably better than nothing and making a potential attack harder and more expensive will probably discourage many attackers.



[Picture from quoted article.]

In this paper one of the tasks was to analyze and find solutions ourselves many are very obvious like the internal clock and others are sophisticated and smart like the one above. Finding something original seems hard and took a bit of creative thinking, but here it is our proposed original (as far as we know) solution to the gps signal problem.

As we learned above the receiver uses BPSK to get a bitstream from the sine waves in the radio signal. We also know that two signals can vary in for example strength but as long as they contain the phase shifts at the same places they will produce the same bit sequence. It should be possible for a more advanced receiver to analyse and see if the sine waves has somehow changed and detect a spoofing attack this will possibly add extra security especially if it's implemented with the bit latency defence.

PART 4: Information Security

According to the norwegian law of the treatment of personal information §13 the controller and the data processor shall, through planned and systematic measures ensure satisfactory information with regard to confidentiality, integrity and availability, processing of personal data(Norske lover). To achieve satisfactory data the controller and the data processor should document the information and security measures, which is available to the employees of the data controller, the data processor, Datatilsynet and Personvernnemnda. We will in this section discuss what the law means for navigation systems.

Confidentiality

Confidentiality is “the property that information is not made available or disclosed to unauthorized individuals, entities, or processes” (ISO 27001). The norwegian law of the treatment of personal information is there to protect the individuals against aims to protect against privacy moves violated through the processing of personal data. The law is important as third parties should not be available to share the information with whom and what they want to share it with. We can divide confidentiality into three different parts; Secrecy, privacy and anonymity. Secrecy “is the action of not being seen or known by others”(Oxford University Press, 2006). Privacy is “the state in which one is not observed or disturbed by other people”(Oxford University Press, 2006). While anonymity is the condition of being recognized by your name(Oxford University Press, 2006).

Navigation systems saves the exact points on a unit's position. This information can track the unit up. If more than one point is drawn there will be drawn a straight line between these points, that is starting from where the first signal was sent/received and end where the last signal was sent/received. If persons or processes get hold on such information it could feel unpleasant to the user of the unit -As the they could calculate their next action in due to what position you previously have followed or which position you are currently on.

Navigation information should therefore be kept secure against unauthorized access, both by persons and processes. In Norway the data controller could therefore only handle information that is agreed in writing by the controller. “The information may also not without such an agreement be left to someone else for storage or processing”(Personopplysningsloven, $13).

Of course there will always exist a morality and ethics question about who you should share it to: For instance in research where there are always a question about verifiability, because of the need to ensemble the result in groups and modify denominations or entities. To increase the person's safety the firms that handles such vulnerable information have to be careful about what persons they should hire and make sure that persons that handles such information has an agreement of confidentiality and non-disclosure.

GPS integrity

The oxford dictionary describes integrity as the quality of being honest and having strong moral principles. It also describes it as the state of being whole and undivided(integrity, oxford dictionary). Integrity is composed by data integrity and system integrity. Data integrity is the property that data has not been altered or destroyed in an unauthorized manner. (X.800). System integrity however, is the property of safeguarding the accuracy and completeness of assets (ISO 27001).

Integrity characterizes a navigation system's ability to provide this timely warning when it fails to state its accuracy. GPS monitor themselves for navigation data errors, selective availability, anti spoof failures and certain types of clock failures. In a navigation system the word means that the reciever recieves it's a current position from its sender. This is a process that will differ from what kind of navigation system we have, in this section we will therefore discuss the integrity for each system one-by-one. However, integrity is not only about having politible signals. Integration of the systems is also about what systems are used to: For instance navigation systems can be used to track people, which may lead to unlucky effects.

When we started to write on this section we went out to interview Ruter with their accurant time system. They it can happen that the coordinate to the bus does not always match. The reason for this was that the bus can not send data constantly and if the bus for instance take a full-turn the coordinate may not show how the bus stopped.

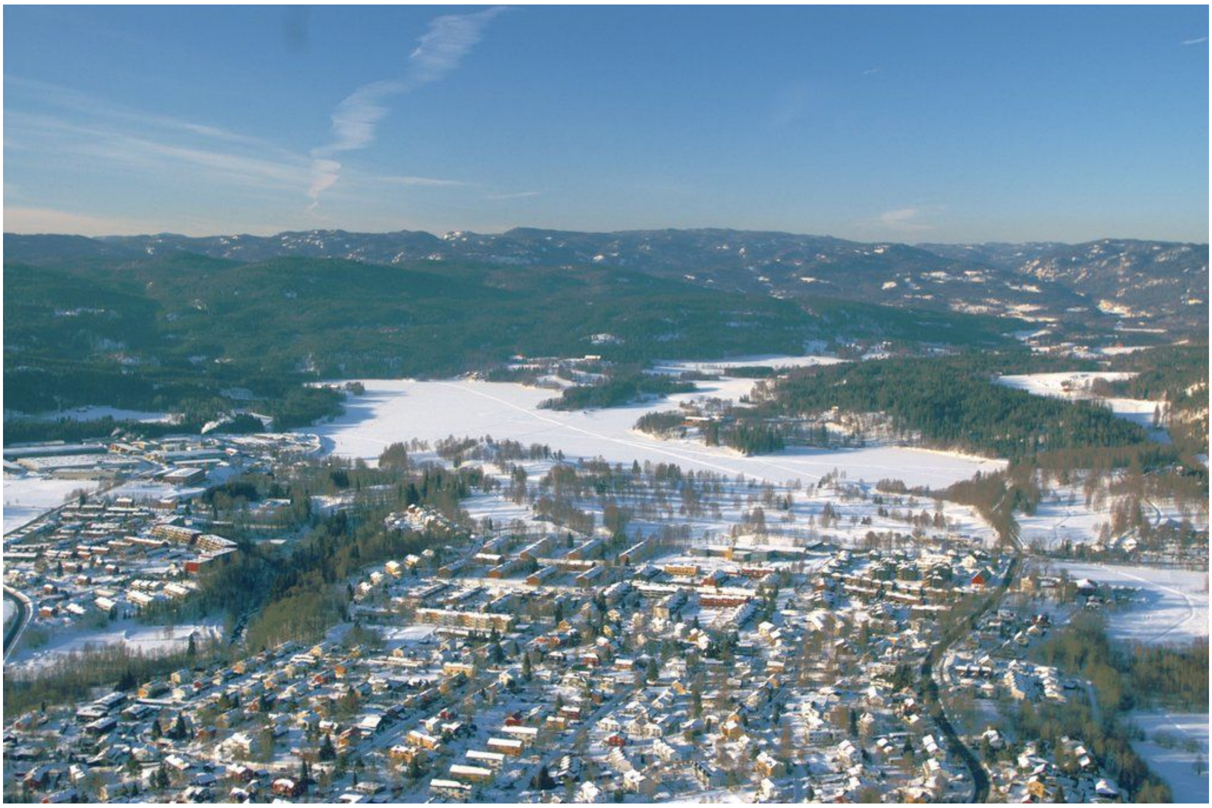
Lately Ruter has had X number of this accidents. Why is that so? Is it something wrong with the system or could it be something else? We asked ourselves. First we that it was something wrong about their system as we were told. Since they shifted out the system every time it sent out a wrong position, and it could not be explained by human intention. After we had take a depth-breath we thought that it also had something to do with either A) how the signal were handled by the sender B) something had happened during the transmitting process 3) Something is wrong with the receiver.

Alternative 1: The signal is wrong handled

Alternative 2: Something has happened during the transmitting process

We have bad GPS data under every circumstance my GPS device record data that does not represent our activity. Segments are then not recorded at the run, because of lost of connection to GPS satellites. The amount of time the signal is in transit between the satellites and your phone allows your device to calculate the distance to each satellite, and thereby triangulate the position to the receiver. The triangulation gives us a position since we already knowns the distance to the GPS sender.

How precise the position is depends upon how many satellites that contribute to calculate the distance. The fewer signals the more uncertainty and inaccuracy increase. If there are fewer than four satellites, many devices will thence produce "signal lost" as it is unable to produce any location estimates. As if you have three visible satellites? in an unknown dimension you can't not know, which constant you should sum the actual distance with to get the pseudorange. The pseudorange defines a sphere of possible positions around the receiver. Notice that the position could also be lost because the view to the GPS signals aren't clear. The loss of signal is also often caused by that huge objects or environmental factors are blocking the signals.



To get a better understanding of the bad GPS signals we will analyze the picture above. It is a picture taken of Bokstadvannet(2337) in Voksenkollen in Oslo. We see that the picture is divided into three sectors; The house area, the field area and the mountain area. The house area is surrounded by a fieldarea and the fieldarea is again surrounded by the mountains. The effect of the signals will therefor slide into each other.

In the house area there are huge appartements, this could block the GPS signals. Tall buildings adds extra time as it can often cause a GPS signal to 'bounce' on its way between your GPS device and the satellites. The device’s calculation of your position will thereby create more distance or loose segments of data. However the bouncy effect will be small as there are some meters between each house. This corrects the distance, so it will be less possible to lose data segments.

At the field area the GPS signal will be great, since it is nothing that blocks the way. However there are several blocks of trees in the field area. Between these trees there are no open room, so it will be hard for the GPS signal to reach the receiver. As a result it will be a great chance for that the signal will not reach the receiver at all.

The mountain area will have the worst GPS signals: There are steep mountainsides that cause temporary loss of data. This could cause less time than you actually traveled, as pre- and post-signal-loss points will be treated just as any other two subsequent points and connect them with a straight line -eventhough it has been more time that has elapsed between them.

The GPS signal refracted through the troposphere, as the charged plasma of the ionosphere bends the path of the GPS radio signal. These changes is caused by temperature, pressure, and humidity data but they may also indicate signal interference. We don’t know enough to predict the effects natural phenomenons or predict when they are coming.

Alternative 3: Something is wrong with the receiver.

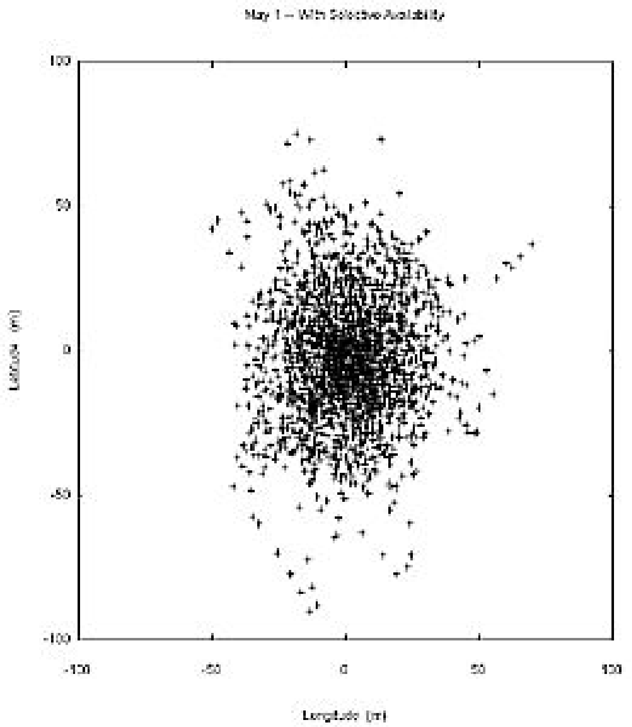
Conclusion integrity:

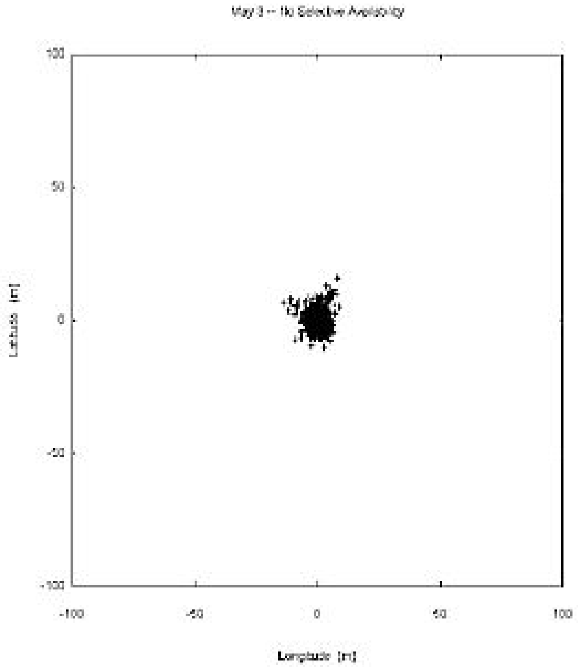
If we draw a line between what we have discussed in the world of GPS we could define integrity as how well the gps shows the receiver's position. For example when you are on a walk a well GPS signal would be able to show the exact route the receiver moved. A bad GPS signal however would show the same route, but will miss some points of movements and therefor not show the whole route: The GPS will draw a straight line between the points where the receiver receives the signal. What makes the difference between a good and bad signal?

Availability

GPS availability is in Oxford Dictionary defined as “The quality of being able to be used or obtained”(Availability, Oxford Dictionary). ISO 27001 however, defines availability as “the property of being accessible and usable upon demand by an authorized entity” (Lecture 1, UiO). In the world of navigation systems we could define the availability as how accessible, obtainable and ready for service or use the navigation systems is.

Before May the 1, 2000 the GPS had only a selective availability(SA), which meant that the GPS signal was available for the U.S government only. GPS was intended to prevent the enemy from using the signal. It therefore moved an enemy’s calculated position to bounce 338 feet out from their position.





GPS was available for civilians during the gulf war as well, since there were quite a lot of military that used the GPS system in user mode so it was easier for the US army to just turn of the SA. This led to that civilians could access the GPS from 500 meters.

The civilian use brought with it a lot of technologies. Civilians Could by equipment that tracked the SA signal and used a signal that was accurate to up to 300 feet. “The removal of S/A will improve the unclassified positioning and time precision of GPS by an order of magnitude and provide civilians with improved access to our master clock” (pobonline, Larry Hothem). The 1th of May 2000 the president therefore decided to turn the SA off and set all satellites to zero. The army noticed the difference when they turned of the signal -as you could see on the pictures.

GPS was installed in BOEING 767-224 ER, which al-qaeda hijacked 15 minutes after a normal take-off. The flight crashed into the North tower of the World Trade center. As it was said that US would turn on the SA it was considered as a national need the industry discussed to return to SA. The proposal were turned off by the president. He said SA would never be turned on again.

Before the GPS it was common to locate the user by asking of their position and then of triangulate the position from the strength of signals transceiver stations had. It was hard for a private person to track other persons and if the position was calculated it was not accurate; The position was only a estimation. The industry integrated the global positioning system into their work, once the selective availability was turned off.

It was especially practical in the mobile industry, since the GPS became handy in both emergency situations and when a lost cell phone owner had to find it way back home. This is really handy, but a problem comes with how the data about our positions is stored. According to CNN your cell phone registers GPS data as long as your telephone is on. All cell phone companies hold on to the GPS data your cell phone have, some of them for years. This data may reveal your personal relationships with others, which habits you have and what you do minute for minute. Trur google/facebook også gjør dette.

The Global positioning system also showed up to be handy in industries that had workers that worked outside of the office space. With the GPS the industries could now track drivers up, so they always know which route they follow. They could also calculate the most timesaving route so, the drivers could follow the most effective route to the customer. You may have seen those ads from Peppes pizza, where you got a free pizza if they do not deliver the pizza within an amount of time. However, the gps also brought in a safety for the management: The system made it possible to overwatch their employees, as their accurate route was shown.

Is it legal to track other people up? According to the CISSP book it is legal to this long as the person that track people up, for instance the management, neither act as a cop or is a cop. The government however, have access to the data that is kept at the companies; Unless the court concludes that such tracking requires a warrant. To not give any police officer right to permanent record and record monitoring everyone's position, there are several police departments that has made regulations as a part of their policy. The government is also limited by the constitution, which protects the individual liberty and justice and place restrictions of the power of the government.

Threats:

The main threat in availability is denial of Service (DoS). It is the prevention of authorized access to resources or the delaying of time critical operations.

Conclusion:

We have learned that the magnet that threw off one of our first navigation systems was just “the tip of the iceberg.” Now that it has been integrated so deep into the very core of our society a calculated attack on a single receiver could do serious damage. As we are writing this US naval officers have to learn how to navigate by the stars like in the days of old, is this the beginning of the end of our modern navigation system?

[http://www.skyandtelescope.com/astronomy-news/u-s-navy-resumes-celestial-navigation-training-04042016/]

Probably not, we have found out that there are “magnets” that can throw off our modern GPS. We do however have the opportunity to make a smarter and better “compas”. We can think of information security as a race between the “attackers and defenders”. As smarter, more advanced ways to stop attacks emerge smarter attacks will follow, there is little to be done about this. The only thing we can do is keep coming up with solutions when security threats emerge. And maybe we must reconsider the integrity of the gps signal and stop treating it like a message sent from above :-)

Threats happens during storage, transmission and processing. We have administrative, technical and physical controls to prevent and control the effect of the threats. Which method we use depends on if the threats is caused by either accident or intension. As we may identify the person that caused the threats upon what type of threats we have. In this section we may discuss pros and cons with navigation methods and how to hack them.

Kildeliste:

1. B. Hofmann-Wellenhof,Klaus Legat,M. Wieser. (2003). Navigation: Principles of Positioning and Guidance. SpringerWienNewYork. Austria.
2. Dead Recognizing.: http://msi.nga.mil/MSISiteContent/StaticFiles/NAV_PUBS/APN/Chapt-07.pdf
3. ESA. (2015, 18. December). About Satelite Navigation. In ESA. Readed 14. mars 2016 from http://www.esa.int/Our_Activities/Navigation/About_satellite_navigation2
4. http://msi.nga.mil/MSISiteContent/StaticFiles/NAV_PUBS/APN/Chapt-13.pdf
5. Ording, Svein. (2009, 14. februar). Navigasjon. I Store norske leksikon. Hentet 14. mars 2016 fra https://snl.no/navigasjon.

6. University of Oslo(2006, 25. Januar). Information Security Management and Human Factors for Information Security. Hentet 1. April 2016 fra http://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/lectures/inf3510-2016-l02-isman-humfact.pdf
7. Oxford University Press(2016). Anonymous. Oxford dictionary. Hentet 1. April 2016 fra http://www.oxforddictionaries.com/definition/english/anonymous
8. Oxford University Press(2016). Anonymity. Oxford dictionary. Hentet 1. April 2016 fra http://www.oxforddictionaries.com/definition/english/anonymity
9. Oxford University Press(2016). Privacy. Oxford dictionary. Hentet 1. April 2016 fra http://www.oxforddictionaries.com/definition/english/privacy
10. Oxford University Press(2016). Secrecy. Oxford dictionary. Hentet 1. April 2016 fra http://www.oxforddictionaries.com/definition/english/secret
11. Fossheim , Hallvard J. (2015, 12. August). Konfidensialitet. De nasjonale forskningsetiske komiteene. Hentet 1. April 2016 fra https://www.etikkom.no/fbib/temaer/personvern-og-ansvar-for-den-enkelte/konfidensialitet/
12. Langely, Richard B. (1999, March). The integrity of GPS. university of New Brunswick. http://www2.unb.ca/gge/Resources/gpsworld.march99.pdf
13. Oxford university press, "integrity" in Oxford Dictionary, 2016. Picked up 2016, 12.April at http://www.oxforddictionaries.com/definition/english/integrity.
14. http://gpsworld.com/gnss-systeminnovation-digging-gps-integrity-12254/#
15. https://support.strava.com/hc/en-us/articles/216917707-Bad-GPS-Data-What-Why-How
16. Midtskogen, Steinar(2006, 7. March). Bokstadvannet(2377) in Flyfoto fra Voksenkollområdet. Picked up 15. April 2016 at http://voksenlia.net/flyfoto/
17. Brown, Lieca. "Selective Availability Turned Off" at http://www.pobonline.com/articles/84412-selective-availability-turned-off. Readed: April the 20th 2016
18. Wolpin, Steward. "Commerical GPS Turns 25: How the Unwanted Military Tech Found Its True Calling" at

http://mashable.com/2014/05/25/commercial-gps-25-anniversary/#aHmNQ.nB6Zqk. Readed: April the 20th 2016

19. The norwegian law
20. Petersn, J. K.. Auerbach publications. Understanding surveillence technologies, spy devices, privacy, history and applications. Written: 2007. Readed; May the 10th 2016.
21. Crump, Catherine. **"How GPS tracking threatens our privacy" at** http://edition.cnn.com/2011/11/07/opinion/crump-gps/. Written november the 7th 2011. Readed May the 10th 2016.

What is GPS?

Global Positioning System is a radionavigation networksystem componed by [24 dette er feil] satelites. It is comprised by a space segment, control segment and user segment, which service positioning, navigation and timing(PNT).

The space segment consists of all the satellites in the GPS constellation, which undergoes continuous change as new satellites are launched and others are decommissioned on a periodic basis. Each satellite orbits the Earth following one of six orbital planes (Figure 5.6), and completes its orbit in 12 hours. The orbital planes are arranged to ensure that at least four satellites are "in view" at any given time, anywhere on Earth (if obstructions intervene, the satellite's radio signal cannot be received). They inclines 55° from the equator in a Medium Earth Orbit (MEO) at about 20,200 kilometers (12,550 miles). Three satellites are needed by the receivers to determine position, while the fourth enhances the measurement and provides the ability to calculate elevation. Since four satellites must be visible from any point on the planet and the satellites are arranged into six orbital planes, the minimum number of satellites needed to provide full coverage at any location on Earth is 24.

Although the GPS satellites are examples of impressive engineering and design, they are not error free. Gravitational variations that result from the interaction between the Earth and Moon can affect the orbits of the satellites. Disturbances from radiation, electrical anomalies, space debris, and normal wear and tear can also degrade or disrupt a satellite's orbit and functionality. From time to time, the satellites must receive instructions to correct these errors, based on data collected and analyzed by control centers on the ground. If necessary, the Master Control Center can modify satellite orbits by radio signal commands transmitted via the control segment's ground antennas.

Two types of control centers exist: monitor stations and control stations. These stations are on earth. The control stations monitures and maintain the GPS satelites. Monitor Stations record discrepancies between known and calculated positions caused by slight variations in satellite orbits. Data describing the orbits are produced at the Master Control Station at Colorado Springs, uploaded to the satellites, and finally broadcast as part of the GPS positioning signal. GPS receivers use this satellite Navigation Message data to adjust the positions they measure.

The user segment are recivers that process the navigation signals from the GPS satelittes and calculate position and time. GPS satellites broadcast signals at two radio frequencies reserved for radio navigation use: 575.42 MHz (L1) and 1227.6 MHz (L2). The public portion of the user segment until 2012 relied only on the L1 frequency; L2 frequency has been used for two encrypted signals for military use only. Gradually, starting in 2005, new satellites have started to use L2C (a civilian use of the L2 frequency) for non-encrypted, public access signals that do not provide full navigation data. GPS receiver makers are now able to make dual-frequency models that can measure slight differences in arrival times of the two signals (these are called "carrier phase differential" receivers). Such differences can be used to exploit the L2 frequency to improve accuracy without decoding the encrypted military signal.

Satelite Raning: How does GPS find the signals?

GPS satellites broadcast “pseudo-random codes” which contain the information about the time and orbital path of the satellite. The receiver then interprets this code so that it can calculate the difference between its own clock and the time the signal was transmitted. When multiplied by the speed of the signal (which travels at the speed of light), the difference in times can be used to determine the distance between the satellite and receiver.

the GPS constellation is configured so that a minimum of four satellites is always "in view" everywhere on Earth. If only one satellite signal was available to a receiver, the best that a receiver could do would be to use the signal time to determine its distance from that satellite, but the position of the receiver could be at any of the infinite number of points defined by an imaginary sphere with that radius surrounding the satellite (the “range” of that satellite). If two satellites are available, a receiver can tell that its position is somewhere along a circle formed by the intersection of the two spherical ranges. When distances from three satellites are known, the receiver's position must be one of two points at the intersection of three spherical ranges. GPS receivers are usually smart enough to choose the location nearest to the Earth's surface. At a minimum, three satellites are required for a two-dimensional (horizontal) fix. Four ranges are needed for a three-dimensional fix (horizontal and elevation). The process of acquiring a two-dimensional fix is illustrated in Figure 5.8

PSN

A common method of error correction is called **differential correction.** Recall the basic concept behind the requirement of three satellites for accurately determining 2-dimensional positions. Differential correction is similar in that it uses the known distances between two or more receivers to enhance GPS readings.

Positioning is the ability to accurately and precisely determine one's location and orientation two-dimensionally or sometimes three-dimensionally. It is referenced to a standard geodetic system such as World Geodetic System 1984 (WGS84) or the International Terrestrial Reference Frame (ITRF).

Navigation is the ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from sub-surface to surface and from surface to space.

Timing is the ability to acquire and maintain accurate and precise time from a standard Coordinated Universal Time (UTC) anywhere in the world and within user-defined parameters. Timing also includes time transfer.

In all it is therefore offers two types of service; Standard Positioning Service (SPS) which uses the coarse acquisition (C/A) code on the L1 frequency, and Precise Positioning Service (PPS) which uses the P(Y) code on both the L1 and L2 frequencies.

GPS Signal

A GPS signal contains 3 different bits of information - a pseudorandom code, ephemeris data and almanac data. The pseudorandom code is simply an I.D. code that identifies which satellite is transmitting information. You can view this number on your Garmin GPS unit's satellite page, as it identifies which satellites it's receiving.

Ephemeris data, which is constantly transmitted by each satellite, contains important information about the status of the satellite (healthy or unhealthy), current date and time. This part of the signal is essential for determining a position.

The almanac data tells the GPS receiver where each GPS satellite should be at any time throughout the day. Each satellite transmits almanac data showing the orbital information for that satellite and for every other satellite in the system.

Dilution of Precision

The arrangement of satellites in the sky also affects the accuracy of GPS positioning. The ideal arrangement (of the minimum four satellites) is one satellite directly overhead, three others equally spaced nearer the horizon (but above the mask angle). Imagine a vast umbrella that encompasses most of the sky, where the satellites form the tip and the ends of the umbrella spines.

GPS coordinates calculated when satellites are clustered close together in the sky suffer from **dilution of precision** (DOP), a factor that multiplies the uncertainty associated with

User Equivalent Range Errors (UERE - errors associated with satellite and receiver clocks, the atmosphere, satellite orbits, and the environmental conditions that lead to multipath errors). The calculation of DOP results in values that range from 1 (the best case, which does not magnify UERE) to more than 20 (in which case, there is so much error the data should not be used). According to Van Sickle (2001), the lowest DOP encountered in practice is about 2, which doubles the uncertainty associated with UERE.

GPS receivers report several components of DOP, including Horizontal Dilution of Precision (HDOP) and Vertical Dilution of Precision (VDOP). The combination of these two components of the three-dimensional position is called PDOP - position dilution of precision. A key element of GPS mission planning is to identify the time of day when PDOP is minimized. Since satellite orbits are known, PDOP can be predicted for a given time and location. Professional surveyors use a variety of software products to determine the best conditions for GPS work.

Sources of GPS signal errors

1. **Satellite clock**: GPS position calculations depend on measuring signal transmission time from satellite to receiver; this, in turn, depends on knowing the time on both ends. NAVSTAR satellites use atomic clocks, which are very accurate but can drift up to a millisecond (enough to make an accuracy difference). These errors are minimized by calculating clock corrections (at monitoring stations) and transmitting the corrections along with the GPS signal to appropriately outfitted GPS receivers.Ideal satellite geometry exists when the satellites are located at wide angles relative to each other. Poor geometry results when the satellites are located in a line or in a tight grouping.
2. **Upper atmosphere (ionosphere)**: As GPS signals pass through the upper atmosphere (the ionosphere 50-1000km above the surface), signals are delayed and deflected. The ionosphere density varies; thus, signals are delayed more in some places than others. The delay also depends on how close the satellite is to being overhead (where distance that the signal travels through the ionosphere is least). Buildings, terrain, electronic interference, or sometimes even dense foliage can block signal reception, causing position errors or possibly no position reading at all. GPS units typically will not work indoors, underwater or underground. This increases the travel time of the signal, thereby causing errors. By modeling ionosphere characteristics, GPS monitoring stations can calculate and transmit corrections to the satellites, which in turn pass these corrections along to receivers. Only about three-quarters of the bias can be removed, however, leaving the ionosphere as the second largest contributor to the GPS error budget.
3. **Receiver clock**: GPS receivers are equipped with quartz crystal clocks that are less stable than the atomic clocks used in NAVSTAR satellites. Receiver clock error can be eliminated, however, by comparing times of arrival of signals from two satellites (whose transmission times are known exactly). A receiver's built-in clock is not as

accurate as the atomic clocks onboard the GPS satellites. Therefore, it may have very slight timing errors.

4. **Satellite orbit**: GPS receivers calculate coordinates relative to the known locations of satellites in space, a complex task that involves knowing the shapes of satellite orbits as well as their velocities, neither of which is constant. The GPS Control Segment monitors satellite locations at all times, calculates orbit eccentricities, and compiles these deviations in documents called ephemerides. An ephemeris is compiled for each satellite and broadcast with the satellite signal. GPS receivers that are able to process ephemerides can compensate for some orbital errors.
5. **Lower atmosphere**: The three lower layers of atmosphere (troposphere, tropopause, and stratosphere) extend from the Earth’s surface to an altitude of about 50 km. The lower atmosphere delays GPS signals, adding slightly to the calculated distances between satellites and receivers. Signals from satellites close to the horizon are delayed the most, since they pass through the most atmosphere.
6. **Multipath**: Ideally, GPS signals travel from satellites through the atmosphere directly to GPS receivers. In reality, GPS receivers must discriminate between signals received directly from satellites and other signals that have been reflected from surrounding objects, such as buildings, trees, and even the ground. Antennas are designed to minimize interference from signals reflected from below, but signals reflected from above are more difficult to eliminate. One technique for minimizing multipath errors is to track only those satellites that are at least 15° above the horizon, a threshold called the "mask angle."