Prediction of Doppler shift for securing GNSS

Nazmoon nahar

ID: 2013–2–60–043

Nazia Zerin

ID: 2013–2–60–059

Afsana Rahman

ID: 2014–2–60–020

A thesis submitted in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering

Department of Computer Science and Engineering
East West University
Dhaka-1212, Bangladesh

September, 2018

Declaration

We, hereby, declare that the work presented in this thesis is the outcome of the investigation performed by us under the supervision of Rashedul Amin Tuhin Senior Lecturer, Department of Computer Science and engineering, East West University. We also declare that no part of this thesis/project has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned

. . . .
Rashedul Amin Tuhin
Supervisor

Signature

. . . .
Nazmoon Nahar (ID: 2013-2-60-043)

Signature

. . . .
Nazia Zerin (ID: 2013-2-60-059)

Signature

. . . .
Afsana Rahman (ID: 2014-2-60-020)

Abstract

GNSS (Global Navigation Satellite System) is functioned extensively around the whole world for many distinct purposes. At first it was infrastructure for the intention of military function. Nowadays, it also has been used for civilian operations. In recent days it has been developed to its most efficient states and still being acquired further towards speck precision. Accompanying all the improvements, various vulnerabilities have been introduced by researchers and misused by the attackers. Several techniques have been and still being accomplished to secure the GNSS. Previous research exhibit that GNSS-based receivers are still exposed to a very primarily simple, yet operative, attack; known as the replay attack. The replay attack is specifically detrimental since the invader could make the receiver measure an inconsistent position, without even disrupting the encryption or without applying any sophisticated technique. The Doppler shift prediction is a useful and effective way to predict the replay attack. For predicting the Doppler shift at first we have to determine the position of the available satellites. Then through Doppler Shift method we will measure the Doppler shift frequency. Subsequently, identify the attacking signal by comparing the calculated Doppler shift frequency with the original given frequency. The attacker will always try to replay the signal by using the equivalent original given frequency. So, if the Doppler shifted frequency is equivalent to the original received frequency then it will consider as the authentic signal. Otherwise it will be considered as the inconclusive decision and then other test will be initiated. In this study, after the implementation of Doppler shift method, we will predict whether the signal is authentic or not. In this study, we have considered that the satellite has been moving along the straight directional path and the receiver is static. Here, we have used open source data which are available for educational purposes.

Acknowledgments

For the better understanding, a sample Acknowledgment is given below.

As it is true for everyone, we have also arrived at this point of achieving a goal in our life through various interactions with and help from other people. However, written words are often elusive and harbor diverse interpretations even in one's mother language. Therefore, we would not like to make efforts to find best words to express my thankfulness other than simply listing those people who have contributed to this thesis itself in an essential way. This work was carried out in the Department of Computer Science and Engineering at East West University, Bangladesh.

First of all, we would like to express my deepest gratitude to the almighty for His blessings on us. Next, our special thanks go to our supervisor, "Rashedul Amin Tuhin", who gave us this opportunity, initiated us into the field of "Prediction of Doppler shift for securing GNSS", and without whom this work would not have been possible. His encouragements, visionaries and thoughtful comments and suggestions, unforgettable support at every stage of our B.Sc study were simply appreciating and essential. His ability to muddle us enough to finally answer our own question correctly is something valuable what We have learned and We would try to emulate, if ever We get the opportunity.

We would like to thank "Nazmoon Nahar" for his excellent collaboration during performance evaluation studies; "Afsana Rahman" for his overall support; "Nazia Zerin" for her helpful suggestions in solving tricky technical problems. Last but not the least, We would like to thank our parents for their unending support, encouragement and prayers.

There are numerous other people too who have shown me their constant support and friendship in various ways, directly or indirectly related to my/our academic life. We will remember them in our heart and hope to find a more appropriate place to acknowledge them in the future.

Nazmoon Nahar

September, 2018

Nazia Zerin

September, 2018

Afsana Rahman

September, 2018

Table of Contents

Table of Contents

List of Figures

Chapter 1. INTRODUCTION

Earth is our home and it is sufficiently immense for us to explore. From the ancient time human constantly made a trip starting with one place then onto the next, out of their need and interest. It was quite difficult to Keep track of every place. Human dependably wanted to discover an effective and reliable path back home or to his destination. Maps helped voyagers for quite a while and still it's useful.
To find exactly a person's position is precisely incomprehensible with maps. Subsequently, "Navigation", the science of positioning was invented. Diverse countries created their own particular navigation system frameworks including the situation of stars, land points of interest, seas, woodlands et cetera.

Background

Since the coming of global positioning system, it had pushed us from numerous points of view to achieve our voyages. The most punctual type of Polynesian route was exclusively in view of encounters, as opposed to instruments and logical techniques [1]. Mechanical instruments what's more, logical techniques were presented and broadly utilized as a part of maritime positioning for decades.

Coordinated effort with Geodesy, the science that deals with the estimation and outline of the earth scaled the study of route towards a worldwide scope. A few organize frameworks were in activity in geodesy, most significant of them are the "World Geodetic Framework 1984" (WGS84) framework and the "Earth Focused, Earth Settled" (ECEF) framework.[3]

As in the cutting edge period, positioning system use the satellites around the earth, this is the reason, the present framework is by and large known as the global positioning system (GPS). A position decided with the assistance of GPS could be translated both in ECEF what's more, WGS84 framework as indicated by need with straightforward calculation.

GPS

GPS Stands for "Global Positioning System." GPS is a satellite navigation system wont to confirm the ground position of an object. GPS technology was 1st utilized by the U. S. military within the Nineteen Sixties and expanded into civilian use over the Nineteen Eighties.
GPS works in any weather, anyplace within the world, twenty four hours on a daily basis, with no subscription fees or charges. it's a world navigation satellite system that has geolocation and time data to a GPS receiver anyplace on or close to the earth wherever there's an unclogged line of sight to four or additional GPS satellites in **Figure 1** . Obstacles akin to mountains and buildings block the comparatively weak GPS signals. [1][2]

1

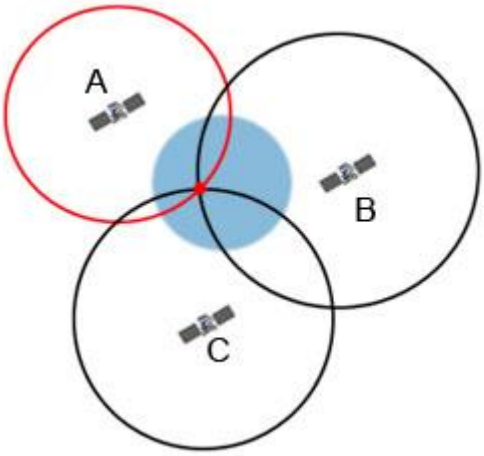


Figure 1. Position detecting

The GPS doesn't need the user to transmit any information, and it operates severally of any telecommunication or net reception, although these technologies will enhance the utility of the GPS positioning data. The GPS provides crucial positioning capabilities to military, civil, and industrial users round the world. The U. S. government created the system, maintains it, and makes it charge free and accessible to everyone with a GPS receiver.[3] The official U.S. Department of Defense (USDOD) name for GPS is NAVSTAR. A full constellation of twenty four satellites was achieved in 1994. [1][4]

Each satellite is constructed to last regarding ten years. Replacements are perpetually being designed and launched into orbit. A GPS satellite weighs just about 2,000 pounds and is regarding seventeen feet across with the solar panels extended. GPS satellites are supercharged by alternative energy like solar power, however they need backup batteries onboard, just in case of an eclipse. Transmitter power is merely fifty Watts or less.

Brief History of GPS

The GPS project was launched by the U.S. Department of Defense in 1973 to be used by the U. S. military and have become absolutely operational in 1995. The primary GPS satellite was launched in 1978[21].It was accessible for civilian use within the Eighties. Advances in technology and new demands on the prevailing system have currently diode to efforts to modernize the GPS and implement following generation of GPS Block IIIA.

Satellites and Next Generation Operational control system (OCX). Announcements from vice chairman V.P. and the White House in 1998 initiated these changes. In 2000, the U.S. Congress approved the modernization effort, GPS III. Throughout the Nineties, GPS quality was degraded by the u. s. government in a very program referred to as "Selective Availability", however, this can be not the case, and was discontinued in could 2000 by law signed by President Bill Clinton.[5][21]

[1] Figure1.[3]

New GPS receiver devices using the L5 frequency to start unharness in 2018 square measure expected to own a far higher accuracy and pinpoint a tool to among thirty centimeters or simply underneath one foot. The GPS system is provided by the U. S. government, which may by selection deny access to the system, as happened to the Indian military in 1999 throughout the Kargil War, or degrade the service at any time.

As a result, variety of states have developed or are within the method of putting in different international or regional navigation systems. The Russian international Navigation Satellite System (GLONASS) was developed contemporaneously with GPS, however suffered from incomplete coverage of the world till the mid-2000s. [12]

GLONASS is supplemental to GPS devices, creating a lot of satellites offered and enabling positions to be mounted a lot of quickly and accurately, to among 2 meters. China's BeiDou Navigation Satellite System is because of succeed international reach in 2020. There also are the European Union Galileo positioning system, and India's NAVIC. Japan's Quasi-Zenith Satellite System (scheduled to start in Nov 2018) are a GPS satellite-based augmentation system to increasing GPS's accuracy. [12]

Improving the security of GPS systems

Efforts to create military GPS satellites as immune against attack as potential begin at the supply. The USA military is presently operating to modernize its GPS system with the next-generation GPS III system. This program, convoy by the USA Air Force and Lockheed Martin, can deliver additional advanced capabilities, developing location, and navigation and timing services and give advanced anti-jam capabilities. This can build GPS III up to eight times additional secure; and additional correct and reliable than the present GPS system. [11]

A major a part of rising anti-jam capabilities and developing security is that the development of a replacement military signal referred to as M-Code. Whereas transmitted within the same frequencies as the present system, M-Code is broadcast from a high-gain direction antenna and a large angle antenna, lending a high-powered signal that refuse jamming and interference. M-Code is additionally designed to be autonomous, which can enable users to measure their position using the M-Code signal solely. [11]

In the modern-day theater of combat, the necessity to be ready to strike at targets that are on the other facet of the world has powerfully given itself. One solution to world threats is GPS guided missiles. exploitation the exceptional navigational and measuring talents of GPS, guided missiles, when being launched, may deliver an explosive to any a part of the world via the interface of the aboard pc within the missile with the GPS satellite system. The benefits of those missiles over alternative forms of guided missiles are that they're solely restricted by their fuel bladder.

Cases of Attack on GPS-based Systems

The drone hijacking incident by Iran in December 2011 is the most noteworthy example of jamming and spoofing attack. In June 2012, a group of researchers demonstrated the successful hijacking of a civilian drone by GPS spoofing. In June 2013, a research team from the University of Texas, Austin misdirected a luxury yacht named "White Rose", by overpowering the actual GPS signals with spoofing equipment. [12]

Problem definition

GPS target-hunting weapons don't seem to be affected with harsh climatic conditions or surrounded by a wire, nor do them leave the gunner vulnerable for attack. GPS target-hunting weapons, with their technological develop over previous, are the superior weapon of selection in modern-day warfare. As technology continues to developed, the face of warfare can still amendment. In time there'll be a superior system to interchange GPS target-hunting weapons.

an assault on a security convention utilizing replay of messages from an alternate setting into the proposed (or unique and expected) setting, accordingly tricking the genuine participant(s) into supposing they have effectively finished the convention run. In our paper the security convention means a GPS signal receiver and alternative setting means an adversary or attacker. When a satellite transmitted a signal and an adversary capture that signal before GPS receiver and also jammed GPS network that it could not receive an original signal. Than the adversary hold the signal for few moment than replay that signal to the actual receiver and GPS receiver didn't have knowledge about this is call replay attack signal . Because of that replay attack GPS receiver thing that it get an original signal and calculate the position but as the signal is being replayed the calculated position are not same as exact position that should be. If receiver want to determine a position it could not do it properly and it will calculate a false position. If we calculate a Doppler shift from that spoofed signal, it will not same if we count it from the original signal.

Objectives

When a satellite transmitted a signal and if an attacker spoofed the signal and delayed it, our objective is given bellow as sub-goal:

- Examining the positions calculated from the multiple combinations.
- Find each location of satellite and receiver correctly.
- Calculate the Doppler shift of received signal to check it is spoofed or not.
- Original signal Doppler shift is not same as spoofed signal's Doppler shift.
- Identifying the signals that are being spoofed.

Focus and Assumptions

This paper is focused on Global Positioning System (GPS) which is the most well-known Global Navigation Satellite System. For computational straightforwardness and constraints, this analysis is based on static receiver which is the limitation of this procedure. But, it has no effect on the theoretical concept. In case of moving objects there will be numerous amount of equations and the whole matter will be very complicated. In this less timing it is impossible for us to find and calculate those equations.

Chapter 2. KEY CONCEPT

GPS Concept [2]

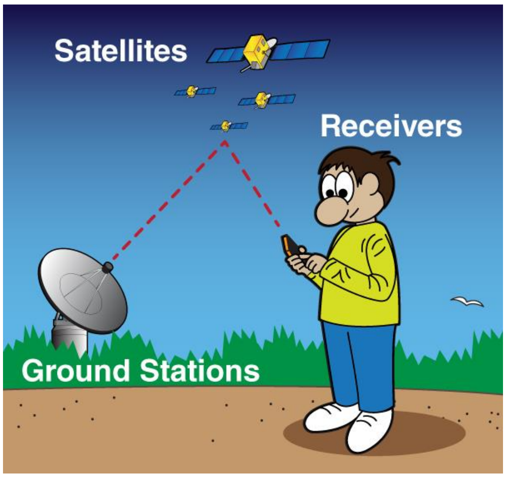


Figure 2. GPS system

How it works

The GPS system includes twenty four satellites deployed in area regarding 12,000 miles (19,300 kilometers) higher than the Earth's surface. They orbit the planet once each twelve hours at a particularly quick pace of roughly 7,000 miles per hour (11,200 kilometers per hour). The satellites are equally detached so four satellites are accessible via direct line-of-sight from anyplace on the world.[5]

Every GPS satellite broadcasts a message through signal that features the satellite's current location, orbit, and actual time. These signals, move at the speed of light, are intercepted by GPS receiver that calculates however far every satellite is predicated on however time it took for the messages to arrive.

A GPS receiver collected the broadcasts from multiple satellites to measure its actual position employing a method referred to as triangulation (as well as speed, time, and direction). If the GPS receiver is barely able to get signals from three satellites, an individual will get his location, however it'll be less correct. [6]

The GPS receiver desires four satellites to figure out a person’s location in 3-dimensions. If solely three satellites are out there, the GPS receiver will get associate approximate position by creating the idea at sea level. If it’s very mean sea level, the position are going to be moderately correct. But if an individual are within the mountains, the 2-D fix may be hundreds of meters off.

[2] Figure2 [3]

Once your location has been detected, the GPS unit will calculate alternative info, such as: Speed, Bearing, Track, Trip distance, Distance to destination, Sunrise and sunset time, And etc.an advanced GPS receiver can usually track all of the out there satellites at the same time,

However solely a range of them are going to be accustomed calculate someone's location or location connected alternative info. In order for a GPS device to figure properly, it should 1st establish an affiliation to the desired range of satellites. This method will take anyplace from some seconds to some minutes, counting on the power of the receiver. As an instance, a car's GPS unit can usually establish a GPS affiliation quicker than the receiver during a watch or smartphone. Most GPS devices conjointly use some variety of location caching to hurry up GPS detection. By memorizing its previous position, a GPS device will quickly confirm what satellites are going to be out there ensuing time it scans for a GPS signal.[5][6]

GPS Navigation Message

The positioning data from GPS satellites in sent within the kind of continuation codes that locate the transmitting satellite, offer locations of the opposite satellites within the system, and provides the navigation information. The codes that kind the GPS signal structure are superimposed upon 2 carrier waves within the L-band, a frequency range put aside for satellite transmission. Each the carrier frequencies and also the signal frequencies are borrowed directly from the aboard atomic_clock_generator frequency of 10.23 MHz. [19]

The coded signals are continual frequently in epochs on the order of fifteen seconds.
The codes used are brought up as "pseudo-random codes", a name applied by early radio astronomers who were the primary to create wide use of such codes. The codes are compatible to decryption of a message embedded in noise signals which can be orders of magnitude greater than the signal itself. Such techniques were important in memorizing radar echoes off the moon and asteroids. Use of those codes facilitates the searching for of signals that arrive at the same time from many GPS satellites.

How A GPS Tracker Communicates?

A GPS hunter functions is sort of a cell phone: It calculates position, speed, and direction information using several GPS satellites, however it reports that information via a cellular network. Once a person uses the Brick House Security GPS observation platform, that person will be able to check on a tracker's position in real time, or generate alerts supported the tracker's activity. However lot of individuals don't understand that it takes a cellular signal to deliver that data. To understand however most trackers work, it is important to grasp the excellence between a lively and a passive GPS tracker. Passive trackers, conjointly called GPS loggers, take the data transmitted from GPS satellites and store it, with no means that to transmit the information. Active trackers, conjointly called real time trackers, contain GPS satellite receivers additionally to cellular transmitters that modify the device to require in location data and transmit it ad it happens. [6]

Contain GPS satellite receivers in addition to cellular transmitters which enable the device to take in location information and transmit it as it happens. When a GPS hunter receives location info from the worldwide Navigation Satellite System (GNSS), it's receiving microwave signals containing location, speed, time, and direction info. As of Gregorian calendar month 2016, there are thirty two satellites within the GPS constellation (though solely thirty one are in use). To report information accurately, the GPS system needs a minimum of 4 satellites transmittal info to a receiver (tracker).

At any given time, from any point on surface, there are regarding 9 satellites visible from the bottom providing a good quantity of redundancy in info. The receiver uses the data from multiple satellites to triangulate a location supported variances in time. Every GPS satellite carries a particularly stable atomic clock that it uses as a baseline to calculate these variances. Once that location info is received by the GPS tracker, the data is transmitted at set intervals using radio frequencies over the mobile network. Several of Brick House's real time trackers report once per minute; though several may be set to report less oftentimes so as to preserve battery life, or a lot of oftentimes to supply a lot of correct location info (though one minute updates are sometimes quite enough to pinpoint a tracker's mechanical phenomenon and current location).[7]

When a GPS tracker transmits info, the quantity of info it sends is relatively smallest. Very similar to the data received from the satellite, the cellular information contains location, speed, direction, and time. This information is transmitted to Brick House's GPS portal that interprets it and displays it as a map read of premeditated points. The platform is additionally able to generate text or email alerts within the event that a planned speed has been exceeded, a region has been entered or exited, motion has been detected, or a panic alert has been generated.

Applications

GPS incorporates a style of applications onto land, at sea and within the air. Basically, GPS is usable everyplace except wherever it's not possible to receive the signal within most buildings, in caves and different subterranean locations, and underwater. The foremost common mobile applications are for navigation by general aviation and business craft. At sea, GPS is additionally usually used for navigation by recreational boaters, business fishermen, and skilled mariners. Land-based applications are additional numerous. The scientific community uses GPS for its preciseness timing capability and positioninfo.

Surveyors use GPS for an enhancing portion of their work. GPS offers price savings by drastically reducing setup time at the survey website and providing unbelievable accuracy. Basic survey units, cost accounting thousands of bucks, offers accuracies right down to one meter. Several costly systems are obtainable which will give accuracies to at intervals a cm.[2]

Recreational uses of GPS are virtually as varied because the variety of recreational sports obtainable. GPS is well-liked among hikers, hunters, snowmobilers, mountain rockers, and cross-country skiers, simply to call a number of. Anyone who must keep track of wherever he or she is, to search out his or her way to a nominative location, or recognize what direction and the way quick he or she goes will utilize the advantages of the worldwide positioning system.

GPS is currently commonplace in cars additionally. Many basic systems are in place and supply emergency margin help at the push of a button (by transmittal someone's current position to a dispatch center). Additional refined systems that show your position on a street map are obtainable. Presently these systems permit a driver to stay track of wherever he or she is and counsel the simplest route to follow to achieve a chosen location. The Mapmy India MMI Rover 201 permits someone to track his vehicle in real time using his phone or browser and gets house number-level map information for location.[2][4]

Moreover, he will get info like engine standing, speeding, vehicle route and address. The waterproof tracker has internal Battery for backup and an immobilizer to chop engine power if the automobile is taken. He will set it to advise you for over rushing additionally as if vehicle deviates from its route. Most folks are in things wherever we are tend to unable to find keys, spectacles, wallets, flash drives and different objects p of daily desires within the house. Rather than looking throughout the house, a person will use a compact Bluetooth tag hunter. These trackers are sometimes small (as giant as a coin) and may be simply stuck or clipped on to most objects.

Coordinate System

The investigation of Geodesy manages the estimation of the earth and position of a point around the earth. Without geodesy, worldwide situating is incomprehensible. Complimenting each other, GNSS frameworks likewise add to the geodetic estimations. To characterize a point accurately on the surface of the earth, a geographic coordinate system is required which would empower the portrayal of any point on the earth.

Demonstrating the earth as an ellipsoid, an arrangement of number is utilized to present the three-dimensional position on the earth surface. By and large, in WGS84 framework, the earth is thought to be an ellipsoid, and a position is spoken to by latitude, longitude and altitude from the ocean level.[23]

Henceforth, it is additionally known as the as the Latitude-Longitude-Altitude (LLA) system. Latitude represents the angular distance of a point north or south of the world's equator. It is indicated with φ and normally communicated in degrees and minutes. By definition, the equator has the latitude 0°, the North Shaft has the latitude 90° and the South Post has the latitude - 90 °.

In **Figure 3.** Longitude alludes to the angular distance of point east or west of the Prime Meridian. The prime meridian is a created line that is thought to be the longitude 0° that interfaces the south and north poles and goes through the Regal Observatory in Greenwich, Britain. Longitude is indicated with λ and furthermore communicated in degrees and minutes. The angle made by a point living in the east of the prime meridian has a longitude between 0° to 180° (or 0° to - 180° westbound). Elevation is the stature of a point from the mean ocean level, communicated in meters or feet.

[3]

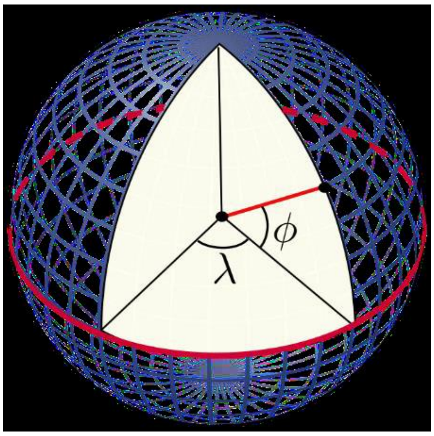


Figure 3. Definition of Latitude (φ) and Longitude (λ) on a sphere

Another coordinate system is called the "Earth-Centered, Earth-Fixed (ECEF)" coordinate system. The ECEF framework is a Cartesian arrange framework with the focused of the earth as the starting point. It is viewed as that the reference outline rotating with the earth so that a point settled on earth does not change its ECEF values. The z-axis does not speak to the earth's rotational axis because of the earth tendency; still it is conceivable to change over to and from ECEF to LLA with simple calculations. [23]

Carrier Frequency and Signal Codes

Every satellite intermittently transmit their characters, positions and other required environmental data in three distinctive transporter recurrence groups, e.g., in **Figure 4.** L1 (1575.42 MHz), L2 (1227.6 MHz) and L5 (1176.45 MHz). There are four kinds of GPS signals for regular citizen use in these recurrence groups: L1 C/A, L2C, L5 and L1C [25]. Alternate GPS signals are limited for military or other reason. The L1 bearer additionally contains the route message that is encoded to binary sequences for phase modulation. Figure 2 demonstrates the age of communicate message in GPS.

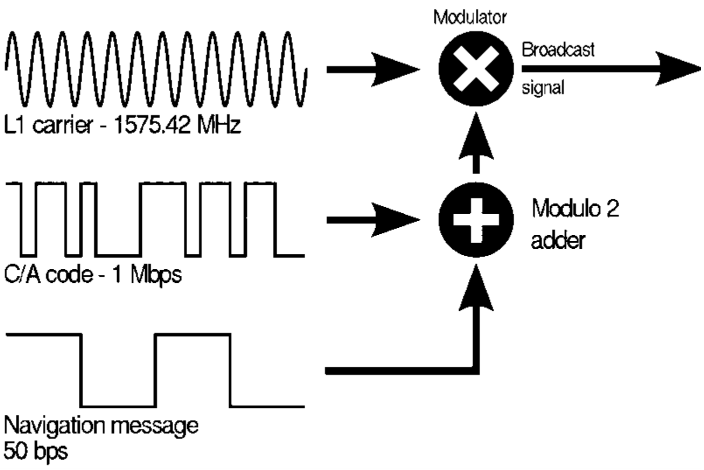


Figure 4. Signal frequency definition

[3] Figure3 [23]

The pseudoranges computed from C/A codes are called C1 write pseudoranges as C/A code utilize L1 bearer. Pseudoranges ascertained from P-code transmitted over L1 and L2 transporter are called P1 and P2 compose pseudoranges individually.

In this examination, the hypothesis of the point position calculation won't be talked about altogether. Or maybe, with the assistance of the Simple Suite [26] created by Kai Borre, the point situating issue would be tended to.

Pseudorange

The GPS receivers work with the assistance of no less than four satellites. For example, a GPS satellite transmits signs to the GPS receivers by means of predefined carriers and modulation methods. The receiver calculates the propagation time of the signals and determines individual distances from every one of the satellites. This separation is known as "Pseudorange", which is ascertained by multiplying the propagation time by the speed of signal propagation (speed of light, 3×108 m/s). Therefore, the receiver clock should be correctly synchronized with the exceedingly exact nuclear clock on the satellites. As the receiver are not outfitted with such exceptionally costly nuclear clock, the receiver clock bias must be included in pseudorange estimations. The signals are likewise influenced by tropospheric and ionospheric delays. These elements are thought about while ascertaining the position.

Necessity of the Fourth Satellite

Other than the three variable (x, y and z) for position, the receiver needs to remedy its clock bias and synchronize it with the nuclear clocks at the satellites. Henceforth, the receiver clock bias turns into the fourth variable. Explaining for four variable requires no less than four equations which are gotten from the signals from no less than four satellites [23].

The need of the fourth satellite is frequently better showed numerically. Let, Ts be the transmission time and Tr be the gathering time of a flag from satellite Si (where i=1, 2, 3… k), the receiver clock bias be ΔT. The Pseudorange ρ_i for Si is characterized by the equation given,

$$\rho i \;=\; (Tr \;-\; Ts \;-\; \Delta T) \;\times\; C \qquad \textbf{1}$$

Where c= speed of light, 3x108 m/s

If the receiver position is *x*, *y*, *z* and position of satellite *Si* is *xi*, *yi*, *zi* in ECEF coordinate system, then the true distance between the receiver and the satellite *Si* is:

$$\sqrt{}\,((xi \;-\; x)\;2 \;+\; (yi \;-\; y)\;2 \;+\; (zi \;-\; z)\;2\;) \qquad \textbf{2}$$

The true distance and the pseudo range ρ*i* could be related by the following equation:

$$\rho i = (Tr - Ts - \Delta T) \times c = \sqrt{((xi - x)^2 + (yi - y)^2 + (zi - z)^2)} \quad \mathbf{3}$$

In the past equation (3), the receiving time *Tr*, the transmitting time *Ts*, the light speed *c* and satellite coordinates *xi*, *yi*, *zi* are known variables. That leaves the receiver clock bias ΔT and the receiver's exact position *x*, *y*, *z* as the unknowns. So, for a system of *k* satellites, a total of *k* equations are found, with four variables, which turns the system into an overdetermined system. Such system of equations could be solved using well-defined mathematical methods (e.g. Gaussian Elimination, Least Squares Analysis).Equations for such systems with a total of *k* satellites are presented below:

$$\sqrt{((xi - x)^2 + (yi - y)^2 + (zi - z)^2)} = (Tr - Ts - \Delta T) \times c \qquad 4$$

Where, i = 1, 2…, k.

In eq. (4), all the unknowns except *x*, *y*, *z* and ΔT are known either from receiver calculation or transmitted by the GPS satellites. So, it is possible to calculate for *x*, *y*, *z* and ΔT for any $k \geq 4$.

In practice, at any given time and location on the earth, more than 4 GPS satellites are visible, and the receiver location is measured numerically by the Least Squares method
[23]

Triangulation and Triangulation

As GPS satellites announced their position and time, trilateration count distances to pinpoint their actual location on Earth. While surveyors use triangulation to count distant points, GPS positioning doesn't involve any angles any. So, Trilateration involves activity distances on the opposite hand Triangulation Measures Angles

What does Triangulation mean?

In wireless mobile communication system the largely used method to search out the situation of a telephone user is Triangulation. It will verify the precise location of a sender. Triangulation in mobile communication is often wont to pinpoint the precise geographical position of a user. This may be done exploitation numerous techniques comparable to through radial distance, direction or receiving a signal from 2 3|to 3|to a few} totally different points then assessing the precise position by overlapping of the three radial distances.

How it works:

Triangulation is employed in cruise navigation, radar systems, GPS systems in vehicles and different such cellular devices. It plays a vital role in emergencies and large setups like 911 are supported triangulation strategy of locating the situation in question.

A triangulation mechanism will be tormented by the presence of steel structures, water towers, communication posts and signal jammers. Victimization 2 or more points to work out the situation of transmitter or cellular phone user offer far more reliable results than counting on only one. In triangulation method one satellite will establish range, locating the detector on a sphere. 2 satellites will find the detector on the intersection of 2 spheres.

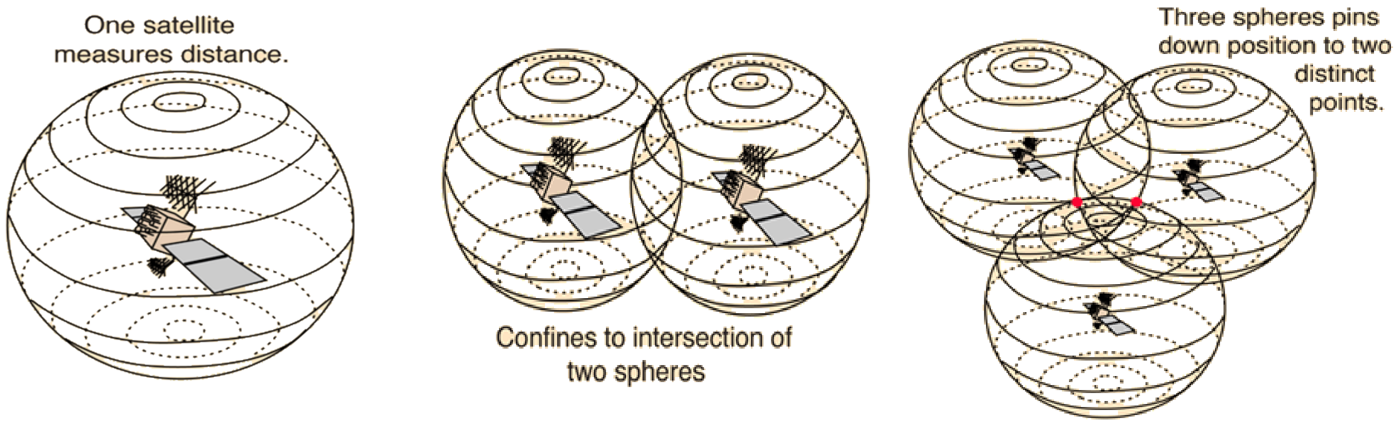


Figure 5. Three satellite define a position on earth

Adding a 3rd as within the GPS system locates it at one in every of 2 distinct points wherever the 3 spheres meet. The proper one is definitely chosen to urge a particular location. The twenty four GPS satellites carry atomic clocks to grant them the accuracy needed for position mensuration.

In the given **Figure 5 & Figure 6** shown by the highest drawing, the gap to the cellular phone is set by mensuration the relative time delays within the signal from the phone set to 3 totally different base stations. Within the situation shown by bottom drawing, directional antennas at 2 base stations will be wont to pinpoint the situation of the cellular phone.[7]

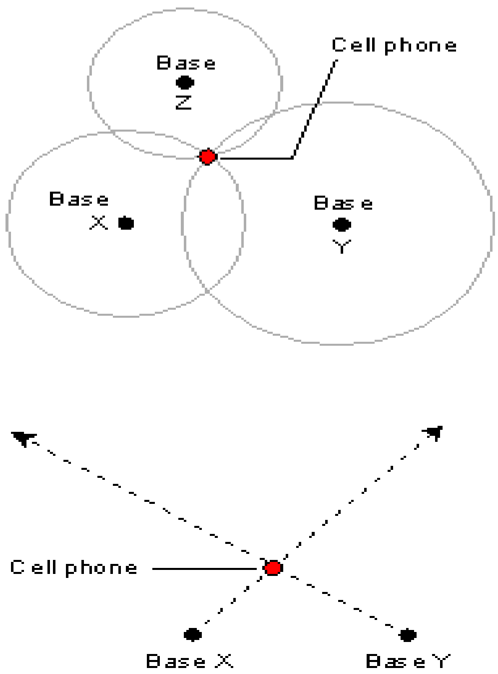


Figure 6. Detecting cell phone position

Triangulation is tough to hold out unless the person using the cellular phone desires to be located. This could be the case, as an example, in an emergency state of affairs. Triangulation is that the methodology by that the so-called 911 mobile phones work. Triangulation equipment may be confused by the reflection of signals from objects resembling massive steel-frame buildings, water towers, communications towers, and alternative obstructions. For this reason, a minimum of 2 freelance triangulation determinations ought to be created to verify the position of a cellular phone or alternative transmitter. A additional refined sort of triangulation is used by the global Positioning System (GPS).Also see mobile phone and GPS. [9]

Triangulation Measures Angles, Not Distance

On the opposite hand, surveyors use triangulation to count unknown distances. They are doing this by creating a baseline length. From every purpose, surveyor's count angles of distant points use equipment akin to theodolites. Once we determine the lengths and angles, triangulation evaluate the distances by forming triangles, as shown within the **Figure 7**.For example, surveyors gathered some 26,000 stations from Maede's Ranch in Kansas to make the North American Datum of 1927 (NAD27). However the world Positioning System uses the globe geodesic Survey (WGS84) to reference positions. [8]

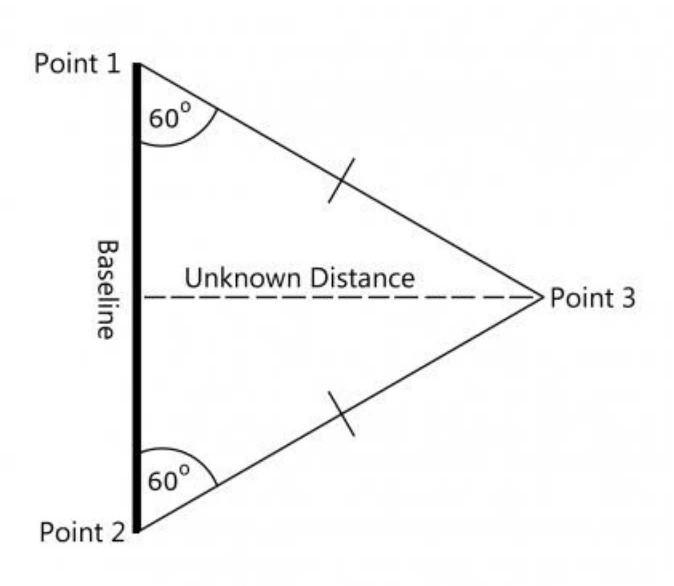


Figure 7. Working method of triangulation

Trilateration Measures Distance, Not Angles

Using a easy two-dimensional example we are able to describe however the GPS system pinpoint a position using trilateration, let's imagine we've 3 GPS satellites every with a identified position in space. Really, all that satellites do is broadcast a signal for your GPS receiver to choose up with a selected time and distance.
For example, the primary satellite broadcasts a signal that eventually hits your GPS receiver. We have a tendency to don't recognize the angle, however we have a tendency to do recognize the distance. That's why this distance forms a circle equal in all directions.

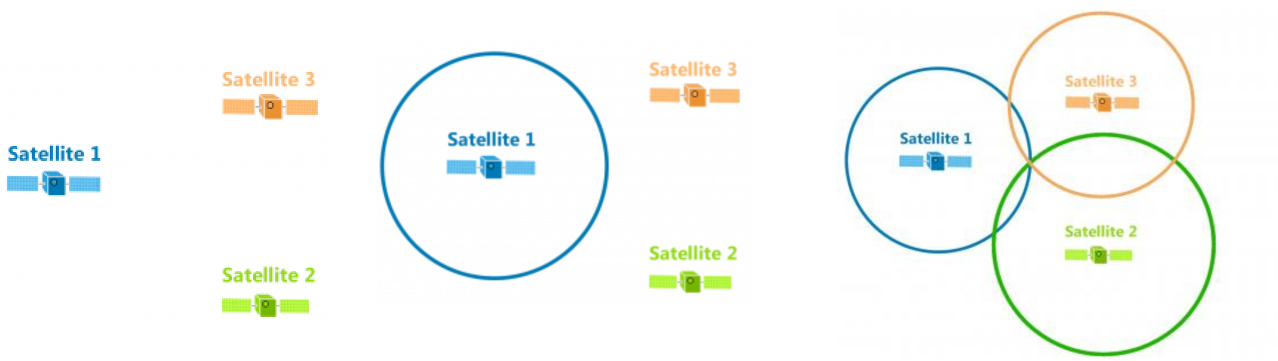


Figure 8. Use of 3 satellite for accuracy.

In **Figure 8 & figure 9**, all that satellites do is broadcast a signal for your GPS receiver to choose up with a selected time and distance. For example, the primary satellite broadcasts a signal that eventually hits your GPS receiver. We have a tendency to don’t recognize the angle, however we have a tendency to do recognize the distance. That’s why this distance forms a circle equal in all directions. This means that your GPS position may be anyplace on this circle at this specific radius.[9]

Again, this distance is equally broadcasted all told directions till it hits your GPS receiver. This implies that the distance may be anyplace thereon circle. But this point, we've 2 identified distances from 2 satellites. With 2 signals, the precise location may be any of the 2 points wherever the circles encounter. Because we've a 3rd satellite, it reveals your true position wherever all 3 circles encounter.

Figure 9. Satellite detect a position on earth.

Using 3 distances, trilateration will pinpoint an exact location. Every satellite is at the middle of a sphere and wherever all of them encounter is that the position of the GPS receiver. As the position of the GPS receiver moves, the radius of every circle (distance) also will amendment.

But the fact is in our three-dimensional world that GPS satellites broadcast signals as a sphere. Each satellite is at the middle of a sphere. Where all spheres encounter determines the position of the GPS receiver.

Doppler Shift

The Doppler impact (or the Doppler move) is the adjustment in recurrence or wavelength of a wave in relation to spectator who is moving with respect to the wave source. The explanation behind the Doppler impact is that when the source of the waves is moving towards the eyewitness, each progressive wave peak is radiated from a position nearer to the onlooker than the past wave. Along these lines, each wave sets aside marginally less opportunity to achieve the spectator than the past wave. Henceforth, the time between the arrivals of progressive wave peaks at the observer is lessened, causing an expansion in the recurrence.[15]

While they are voyaging, the separation between progressive wave fronts is diminished, so the waves "bundle together". On the other hand, if the source of waves is moving far from the observer, each wave is discharged from a position more remote from the eyewitness than the past wave, so the entry time between progressive waves is expanded, decreasing the recurrence. The separation between progressive wave fronts is then expanded, so the waves "spread out".

Chapter 3. The Adversary Model

GPS Guided System

The Global Positioning System (GPS) is a satellite navigation system that provides location and time information in all weather conditions and at any position where there is a line of sight to 4 or more GPS satellites. Such a system supports critical applications for military, civil and commercial users worldwide, having the US government as its main sponsor. It shows itself accessible to any operator by using a single GPS receiver.

Currently, a series of applications are developed and supported primarily by this “tool”, becoming highly dependent of it. They are called GPS-dependent systems, which include different tracking, encryption and navigation systems. GPS applications, such as transfer time, traffic signal timing and synchronization of cell phone base stations use the cheap and highly-accurate GPS infrastructure. However, although being essentially dependent on the GPS signals, just a few of them present some kind of countermeasure to electromagnetic attacks (jamming), becoming highly vulnerable to them.[11]

Replay Attack

A replay attack is a class of system assault in which an assailant recognizes an information transmission and falsely has it postponed or rehashed. In **Figure 10** The deferral or rehash of the information transmission is done by the sender or by the pernicious substance, who blocks the data and retransmits it. At the end of the day, a replay assault is an assault on the security convention utilizing replays of information transmission from an alternate sender into the proposed into receiving system, in this way tricking the members into trusting they have effectively finished the information transmission. Replay assaults assist assailants with gaining access to a network, pick up data which would not have been effectively available or finish a copy exchange. A replay assault is otherwise called a playback assault.[10][12]

GPS Spoofing

A GPS caricaturing assault endeavors to mislead a GPS collector by communicating off base GPS signals, organized to look like an arrangement of typical GPS signals, or by rebroadcasting honest to goodness signals caught somewhere else or at an alternate time. These mock signs might be adjusted so as to make the collector evaluate its situation to be some place other than where it really is, or to be found where it is yet at an alternate time, as dictated by the aggressor. One regular type of a GPS caricaturing assault, generally named a cart away assault, starts by communicating signals synchronized with the honest to goodness signals saw by the objective beneficiary.[10]

The intensity of the fake signs is then progressively expanded and drawn far from the certified signs. It has been recommended that the catch of a Lockheed RQ-170 automaton airplane in northeastern Iran in December, 2011 was the consequence of such an attack.[10] GPS ridiculing assaults had been anticipated and talked about in the GPS people group already, yet no known case of a malignant satirizing assault has yet been confirmed. A "proof-of-idea" assault was effectively performed in June, 2013, when the extravagance yacht White Rose was misled with caricature GPS signals from Monaco to the island of Rhodes by a gathering of advanced plane design understudies from the Cockrell School of Building at the College of Texas in Austin. The understudies were on board the yacht, enabling their caricaturing gear to bit by bit overwhelm the flag qualities of the genuine GPS star grouping satellites, adjusting the course of the yacht.

GPS Jammer

Simply, "jammers" — which are likewise regularly called signal blockers, GPS jammers, phone jammers, content blockers, and so forth — are unlawful radio frequency transmitters that are designed to block, jam, or generally meddle with approved radio communication. Jamming technology generally does not separate amongst alluring and unfortunate interchanges.[18] A jammer can hinder every radio correspondence on any gadget that works on radio frequencies inside its range (i.e., inside a specific span of the jammer) by producing radio frequency waves that keep the focused on gadget from setting up or keeping up an association. For instance, jammers can:

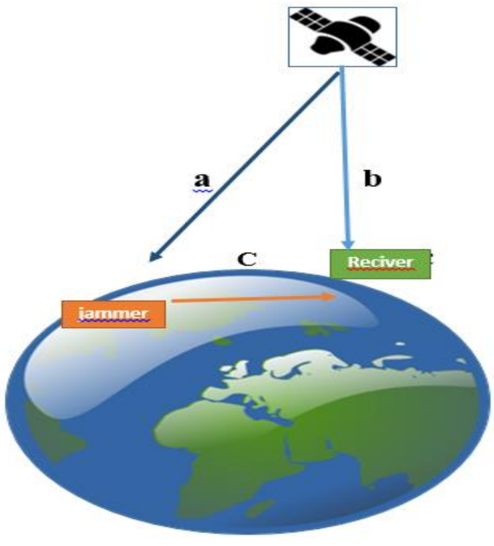


Figure 10. Jamming signal

- Keep your phone from making or accepting calls, instant messages, and emails;
- Keep your Wi-Fi empowered gadget from interfacing with the Web;
- Keep your GPS unit from accepting right positioning signals; and
- Keep a person on call from finding you in a crisis.

Obviously, losing a signal does not really imply that somebody adjacent is utilizing a jammer.

Attack Models

Jamming is outlined as "the emission of radio frequency with enough power and with the required options to avoid, in an exceedingly given space, the receivers to trace GPS signals". The low power of GPS signals (around −160 dBm on the Earth's surface) allows the jammer to be effective even at low power levels, creating comparatively easy and low-cost to be completed. Numerous economical jammers are on the market and price regarding $ 1000, being capable of generating a hundred W of power. This power is comfortable to produce a high operation distance, as are going to be seen next.[23]

Meaconing refers to the method of interception and retransmission of a signal. Considering GPS signals, a tool receives the signal, amplifying and retransmitting it. The target receiver receives the initial signal and also the retransmitted one shown in **Figure 11**. Once the malignant signal arrives with higher power, the target processes this signal as it is the true one, thereby providing data of positioning, navigation and time adore the knowledge of the malicious transmitter.

4

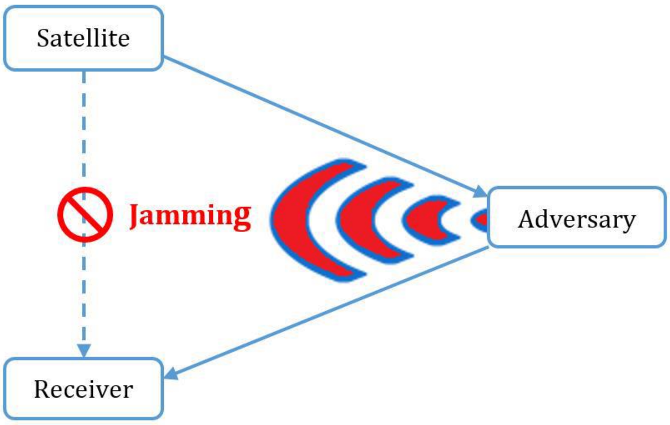


Figure 11. The adversary model.

Finally, the spoofing happens once a false PNT data is inserted into the target receiver that is unable to spot the attack. Though this method is a lot more complicated, it constitutes an original threat t to recent military and civil operations. [10][18]

The Friis' Transmission Equation offers the facility received by associate antenna, beneath idealized conditions, given another antenna a ways away and transmission a better-known amount of power. It is a decent approximation for estimating signal levels through free area,

[4] Figure11 [23]

considering the most factors that influence the propagation. It is thought-about simply a simplified equation as it doesn't think about the atmospheric attenuation (or the path loss) and ultimate influences of clouds and rain. It is written as:

$$P_r = \frac{P_t A_{ef}}{4\pi (R)^2} = \frac{P_t \lambda^2}{(4\pi R)^2} = G_t G_r \frac{\lambda^2}{(4\pi R)^2} \quad (1)$$

Or, in dB:

$$P_r = P_t + G_t + G_r + 20\log_{10}\frac{\lambda}{4\pi R} \quad (2)$$

Here : G_t Associate in Nursing G_r are the gains (with reference to an isotropic radiator) of the transmitting and receiving antennas, respectively; P_t is the transmitted power; A_{ef} is the effective area of the receiving antenna; R is the distance between antennas; λ is wavelength of the carrier.[23]

Thus, supported equation 1, it are often seen that, not considering path loss, the power density that reaches the GPS receiver is reciprocally proportional to the square of the gap (R) of the transmitter(jammer) antenna to the GPS antenna. If a lot more advanced and complicated propagation equation should be thought-about, Eq. 2 becomes:

$$P_r = P_t + G_t(\theta_t, \phi_t) + G_r(\theta_r, \phi_r) + \left(\frac{\lambda}{4\pi R}\right)^2 \ldots$$
$$\ldots \left(1 - |\Gamma_t|^2\right)\left(1 - |\Gamma_r|^2\right)\left|a_t . a_r^*\right|^2 e^{-\alpha R} \quad (3)$$

Here: $\mathbf{G_t(\theta_t,\phi_t)}$ is the gain of the transmitting antenna in the direction $\mathbf{(\theta_t,\phi_t)}$;
$\mathbf{G_r(\theta_r,\phi_r)}$ is the gain of the receiving antenna in the direction $\mathbf{(\theta_r,\phi_r)}$;
$\mathbf{\Gamma_t}$ and $\mathbf{\Gamma_r}$ are the reflection coefficients of the transmitting and receiving antennas;
$\mathbf{a_t}$ and $\mathbf{a_r}$ are the polarization vectors of the transmitting and receiving antennas;
$\boldsymbol{\alpha}$ is the absorption coefficient of the intervening medium.

Chapter 4. Modelling Tools

In this section, an abrupt preface on the modeling and simulation platform, MATLAB has been briefly described. The details of the entire process of finding Doppler shift has been compiled in MATLAB. Afterwards, the details of about RINEX have been discussed.

MATLAB

What is MATLAB?

MATLAB (matrix laboratory) is a multi-paradigm analytical computing ambiance and proprietary programming language refined via Math Works. MATLAB grant matrix guidance and controls, plotting of operations and statistics, application of algorithms, preface of user articulation, and combining with applications written in other languages, which includes C, C++, C#, Java, Fortran and Python.
Despite MATLAB is principally proposed on the whole for numerical computing, a non-compulsory toolbox makes the use of the MuPAD which is a symbolic engine, granting approaching to symbolic computing capabilities. An extra assortment, Simulink, adds graphical multi-realm simulation and version-primarily based design for dynamic and ingrained framework.

Why MATLAB?

For our mechanism, the fundamental compulsion to handle the factor of positioning contrivance after then evolve and administer the miscellaneous assortment of satellites and clarification test. On the contrary unlike other programming languages, MATLAB does not demand any significant libraries for the function. Alternately accommodate with a GPS receiver and then gathering and encoding the information to the convenient layout. In these mechanism formatted raw data of RINEX have been used. For 3-dimensional visualization, which was a key element in this inspection, applying the 3-D visualization and 3-D scatter plot operations, MATLAB made the process effortless in comparison with others.

Working Procedure of MATLAB

In our mechanism MATLAB have used for finding out the position of the victim. In our mechanism this has been used as a tool where we compile required fields for later calculations, observation and navigation position, observed velocity, received velocity, and ultimately Doppler shifted frequency. The window of MATLAB will look like **Figure 12**. The required calculation has been done using different types of formulas.

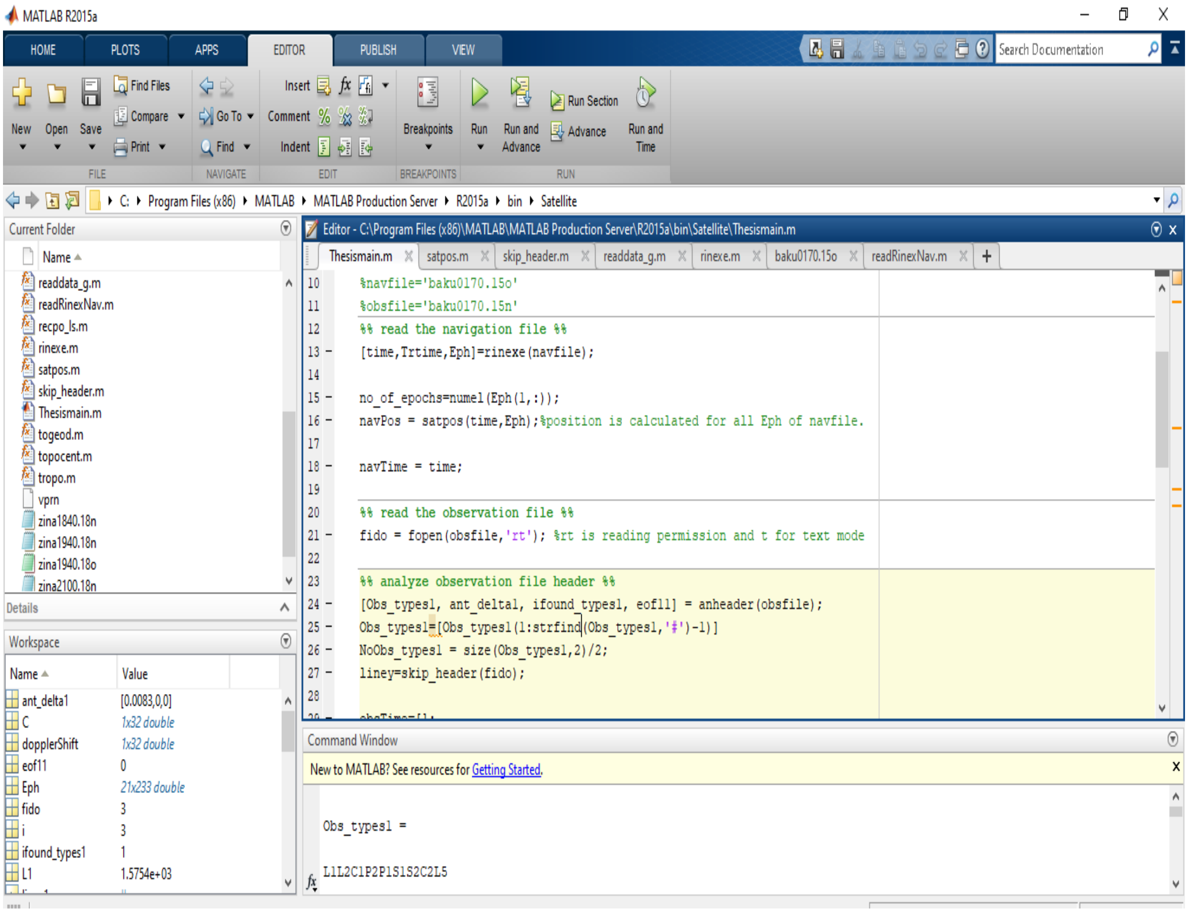


Figure 12. Screenshot of MATLAB 2015a.

RINEX

History of RINEX:

RINEX is a cipher for "Receiver independent change" layout. It is far the typical layout, evolved by Werner Gurtner from the Astronomical Institute, University of Berne, Switzerland. RINEX is the maximum broadly used format for raw satellite navigation data.

The navigation messages broadcasted from the satellites and the receiver observations have to be in RINEX 2.10 and 2.11 layout. The contemporary model of RINEX is 3.03 which is the latest version, but most of the satellite supervised stations and devices even now use RINEX version 2.11.[13]

The RINEX formatted navigation documents and observation files are originated with a "Header" segment, after then observed with the aid of a data section. Each of the fields of the RINEX formatted files are properly defined via the RINEX format documentation [21].

Despite the fact that not some portion of the RINEX organize, the Hatanaka compression scheme is regularly used to decreased the span of RINEX records, bringing about an ASCII-based Compact RINEX arrange. It utilizes higher-arrange time contrasts to diminish the quantity of characters expected to store time information.

Ultimately the output of a navigation receiver is generally its position, speed or other related physical quantities. However, the computation of these quantities are hinge on a series of calculations from one or more satellite constellations. Although receivers computes positions in real time, in many cases it is intriguing to store intermediate measures for later utilization.

RINEX is the standard format that permits the administration and transfer of the measures produced by the recipient, and their disconnection handled by a huge number of utilizations, whatever the producer of both the recipient and the computer application.

General Format description:

Currently according to 2.11 format it consists of seven ASCII file types:
1. Observation Data File
2. Navigation Message File
3. Meteorological Data File
4. GLONASS Navigation Message File
5. GEO Navigation Message File
6. Satellite and Receiver Clock Date File
7. SBAS Broadcast Data File

Each record type comprises of a header area and an information segment. The header area contains global data for the whole record and is set toward the start of the document. The header area contains header labels in segments 61-80 for each line contained in the header segment. These names are compulsory. [17]

The format has been advanced for minimum space prerequisites autonomous from the quantity of various observation sorts of a particular receiver by showing in the header the kinds of observations to be sorted. In the system of computer permitting variable record lengths the observation records may then be kept as short as could reasonably be expected. The most extreme record length is 80 bytes for each record.

Every observation record and each Meteorological Information document fundamentally contain the information from one site and one session. RINEX version 2 likewise permits to incorporate observation information from more than one site consequently possessed by a wandering receiver in fast static or kinematic applications.

In the event that information from more than single receiver it would not be cost-effective to incorporate the indistinguishable satellite messages gathered by the distinct receivers for few times. Subsequently the navigation Message Document from one receiver might be interchanged or a composite navigation Message file made containing non-superfluous data from a few recipients with a specific end goal to make the most complete record.

Definition of the Observables

GPS observables incorporate three key quantities that should be characterized: Time, Stage, and Range:

Time:

The time of the estimation is the receiver time of the acquired signals which has been received. It is indistinguishable for the phase and range estimation and is same for all satellites identified at that epoch. It is exhibited in GPS time (not Universal Time).

Pseudo range:

The pseudo-range (PR) is the distance from the receiver antenna to the satellite antenna including receiver and satellite clock offsets,

PR = distance + (receiver clock offset - satellite clock offset) * c

So that the pseudo-range reflects the actual behavior of the receiver and satellite clocks. The pseudo-range is stored in units of meters.

The pseudo-range (PR) is the space from the receiver antenna to the antenna of satellite which includes receiver and satellite clock offsets (and different biases, atmospheric delays is one of the examples):

PR = distance + c * (receiver clock offset - satellite clock offset +other biases)

So that the pseudo-range displays the actual behavior of the receiver and satellite clocks. The pseudo-range is saved in units of meters.[20]

Phase:

The phase is the provider-segment measured in entire cycles at both L1 and L2. The half-cycles deliberated by squaring-type receivers should be transformed to whole cycles and flagged through the wavelength aspect in the header segment (Only GPS).
The phase modifications within the identical sense as like as the range (negative doppler). The phase observations among epochs have to be linked by inclusive of the integer number of cycles. The phase observations will now not incorporate any systematic drifts from intentional offsets of the reference oscillators

The observables are not amended for external effects like atmospheric refraction, satellite clock offsets, and many others. If the receiver or the converter software accommodate the assessment the usage of the real-time-derived receiver clock offsets dT(r), The consistency of the 3 quantities phase / pseudo-range / epoch ought to be sustained, i.e. the receiver clock correction ought to be carried out to all three observables:

Time(corr) = Time(r) - dT(r)
PR(corr) = PR(r) - dT(r)*c
phase(corr) = phase(r) - dT(r)*freq

Satellite Numbers:

Version 2 has been organized to incorporate with GLONASS or different satellite systems' perceptions. Therefore we have to capable enough to differentiate the satellites of the disparate systems. We anticipate the two-digit satellite number with a system denominator.

snn	s:	satellite tv for pc machine
	lank:	gadget as defined in header document
	G :	GPS
	R :	GLONASS
	T :	Transit
	nn:	PRN (GPS), channel variety (GLONASS) or 2-digit satellite number.

Note: G, R, and T are obligatory in mixed files

Order of the Header Records:

As the file descriptors in columns sixty one-80 are obligatory, the programs studying a RINEX version 2 header are able to decode the header records with codecs in line with the record descriptor, supplied the records have been first read into an inner buffer.

We consequently propose to allow free obtaining of the header information, with the exceptions that has been given below:
- The "RINEX VERSION / TYPE" record must be the primary document in a file.
- The default "WAVELENGTH fact L1/2" report (if present) need to anticipate all records describing wavelength factors for particular satellites
- The "NUMBER OF SATELLITES" file (if present) have to be without delay followed by means of the corresponding variety of "PRN / # OF OBS" facts. (Those statistics may be on hand for documentary purposes. However, after all they may by oneself be constituted after having read the complete raw data report which we define them to be optionally available.[21]

Missing Items, Duration of the Validity of Values

Objects that are not recognized at the report creation time can be set to 0 or blank or the corresponding document can be absolutely neglected. Therefore items of missing header data may be set to 0 or blank by way of the program reading RINEX files. Each appraisal remains legitimate until changed by an additional header record. [22]

Event Flag Records

The "quantity of satellites" also coincide to the number of information of the equal number of epoch observed. Therefore it can be used to skip the precise quantity of records if certain event flags are not to be assess in component.

Receiver Clock Offset

A big wide variety of users requested to optionally encompass a receiver-derived clock offset into the RINEX layout. For us to prevent abashment and repetition, the receiver clock offset (if present) must file the appraisal that has been used to legitimate the observables as stated in the formulae beneath item 1. It would then be feasible to reassemble the unique observations if vital. Because the output layout for the receiver-derived clock offset is restricted to nanoseconds the offset ought to be rounded to the adjacent nanosecond before it is used to precise the observables to be able to guarantee accurate alteration.[22]

The Exchange of RINEX Files:

We recommend using the following naming convention for RINEX files:

```
ssssdddf.yyt   ssss:  4-character station name designator
                ddd:  day of the year of first record
                  f:  file sequence number within day
                 yy:  two digit year
                  t:  file type:  O: Observation file

                                  N: GPS Navigation file
                                  M: Meteorological data file
                                  G: GLONASS Navigation file
                                  L: Future Galileo Navigation file
                                  H: Geostationary GPS payload nav mess file
                                  B: Geo SBAS broadcast data file
                                    (Separate documentation)
                                  C: Clock file (separate documentation)
                                  S: Summary file (used e.g., by IGS, not a
                                     Standard)
```

To interchange RINEX files on magnetic tapes we propose using the following
Tape pattern:

- Non-label; ASCII; constant almanac dimension: eighty characters; block length: 8000
- First record on tape consists list of which use the above-noted naming conventions

While information transference instances or storage volumes are analytical we advise compressing the files precedent to repository or transmittal the use of the UNIX "compress" und "uncompress" programs. Consistent pattern are available on VAX/VMS and PC/DOS systems, as properly.

RINEX Observation Files for GEO Satellites

A recent satellite system qualifier has been described for the geostationary GPS signal payloads: "S", for use within the RINEX version / type header line and within the satellite modifier 'snn', nn being the GEO PRN range minus hundred.

e.g.: PRN = a hundred and twenty --> 'snn' = "S20"

In combined dual frequency GPS satellite / single frequency GEO payload commentary files the fields for the second frequency observations of GEO satellites remain blank, are set to 0 values or (if last inside the document) can be abbreviated.
The time system modifier of GEO satellites producing GPS signals defaults to GPS time.[22]

RINEX Navigation Message Files for GEO Satellites

As the GEO broadcast orbit layout varies from the GPS message a special GEO navigation message document format has been described which is sort of same with the GLONASS nav mess file format. The header segment carries facts about the propagating program, comments, and the distinction between the system time of GEO and UTC.

The primary data document carries the epoch and satellite clock information, the subsequent information comprise the satellite position, velocity and acceleration and auxiliary data such as health, age of the information, etc. The time tags in the GEO navigation documents are given in the GPS time frame, i.e. not UTC.
The amendment of the satellite time to UTC are given below:

GEO : Tutc = Tsv - aGf0 - aGf1 *(Tsv-Toe) - W0 - leap_sec
W0 being the amendment to alter the GEO system time to UTC. Toe, aGf0, aGf1 see under inside the layout definition tables.

The "Transmission Time of Message" (PRN / EPOCH / SV CLK header file) is disclosed in GPS seconds of the week. It symbolizes the inception of the message conveyance. It has to assign to the same GPS week as like as the "Epoch of Ephemerides".[21][22] It has to be accustom via - or + 604800 seconds, if vital (which might make it decreases than zero or greater than 604800, respectively). It is far a redefinition of the version 2.10 "Message frame time". "Health" will be explained as given below:

- Bits zero to three same to Health in Message type 17 (MT17)
- Bit four is set to at least one if MT17 health is unavailable
- Bit five is set to at least one if the URA index is same to fifteen

In the SBAS message explanations bit three of the health is presently marked as ‘reserved’.
In case of bit four set to one, it is acclaimed to set bits zero, one, two, three to at least one, too.

"User Range Accuracy" (URA):

The same delegation for transforming the URA index to meters is used as with GPS. Set URA = 32767 meters if URA index = 15.
"IODN" (Issue of Data Navigation):
The IODN is explained as the eight first bits after the message type 9, known as IODN in RTCA DO229, Annex A and Annex B and called "spare" in Annex C.
The "CORR TO device" TIME header record has been recovered by the way of the extra general file "D-UTC A0, A1, T, W, S, and U" in version 2.11.

Chapter 5. Methodology

In this section, the technique of the inspection have been represented in detail. It would encompass the method of the point positioning, software of hostile impact, mechanism of finding Doppler shift, detecting replay attack with the aid of difference in Doppler shift value.

General Methodology

- The main aim of our analysis is to find out the spoofed signal from among the available signal of satellites with the help of Doppler shift.
- At first we have to find out the position, time to get knowledge about the available satellites.
- After that we have been determined the Doppler shift of those available satellites with the help of navigation and observation file.
- From the navigation file we know the frequency of those distinct satellites.
- After the determination of the apparent frequency using Doppler shift method, we will compare both the frequency and find out the Doppler shift.
- The attacker will always try to replay the signal by keeping the frequency as same as the frequency of the navigation file.
- As we know there will be a shift in frequency and also we know the value of the shifted frequency so we can easily find out the replay signal or false signal.

Doppler Shift

The Doppler Effect (or the Doppler shift) is the transition in frequency or wavelength of a wave in terms of observer who is moving relative to the wave source. It is called after the Austrian physicist Christian Doppler, who described the phenomenon in 1842.

An ordinary instance of Doppler shift is the exchange of pitch heard when a car sounding a horn techniques and recedes from an observer. As compared to the emitted frequency, the acquired frequency is better at some stage in the approach, same on the on the spot of passing by, and lower at some stage in the recession.[15]

Redshifted and Blue shifted Doppler Shift

We can deduce the motion of a source by seeing whether the emission or absorption lines in its spectrum are shifted in wavelength relative to what we would expect their wavelengths to be if the source were at rest. The Doppler formula relates the amount of shift to the velocity of the source. When the velocity is small, the formula is simple:

$$\frac{\text{source velocity}}{\text{speed of light}} = \frac{\text{change in wavelength}}{\text{rest wavelength}}$$

Whilst the origin is transferring closer to us, the wavelengths are shifted to shorter wavelengths, that is, closer to the **blue**. While the source is transferring far away from us, the wavelengths are shifted to longer wavelengths, that is, towards the red.

The spectrum on the pinnacle shows the Hydrogen Balmer lines at their motionlessness wavelengths. Therefore, this origin is nearly at relaxation with respect to us. Within the bottom spectrum, all the boundary are shifted towards longer wavelengths. We are saying the spectrum is **redshifted** and we infer that the source is moving far from us.[16]

If the origin is moving at an immense velocities, i.e. near the speed of light, we require to implore a slightly extra convoluted equation to describe the diversity of wavelength to the origin velocity, primarily based at the identical perception. It is known as the relativistic Doppler formula. The beneath **Figure 13** expressed about the wavelength in Angstroms.

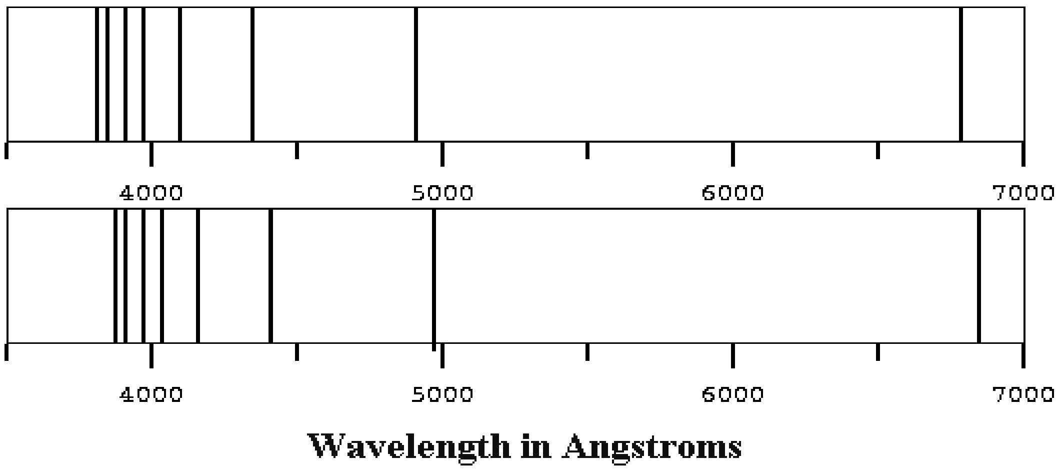


Figure 13. Wavelength in angstrom

Have you ever observed that after an emergency automobile with its siren blaring passes you that the tone that you listen changes in pitch? That is an example of the Doppler shift, and it is an effect that is associated with any wave phenomena (consisting of sound waves or light). Take into account a case where the firetruck is at rest within the hearth station driveway await for the firemen to board, as proven within the image underneath. If the siren is on, a listener far away to the right will apprehend the siren at the equal frequency at which it is far emitted. In fact, another stationary individual on the left side of the truck could pay attention the similar tone additionally. The **Figure 14** demonstrate the above descriptions.

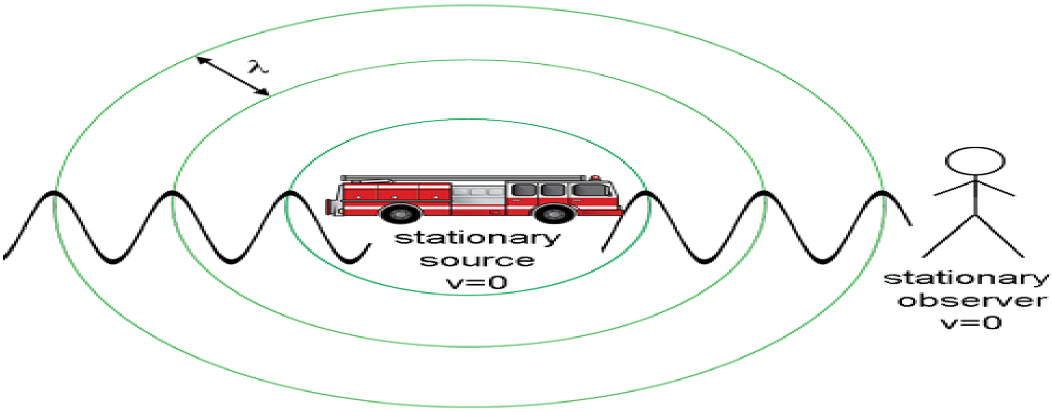


Figure 14. Change in frequency of static source and object

The static listener at the right listen the equal 400 Hz tone emanate with the aid of the fire truck. The circles constitute the wave fronts from the siren's sound waves.[15] Now recollect how this case modifies while the truck is transferring closer to the stagnant observer with a steady velocity, v, as pictured as **Figure 15**.

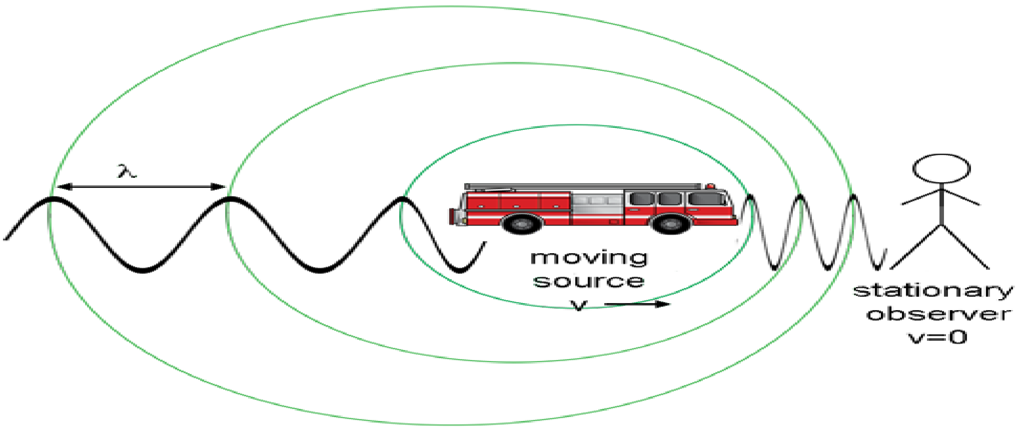


Figure 15. Change in frequency of moving source and stationary object

The static listener on the right does now not listen the same 400 Hz tone emitted via the fireplace truck in motion. The circles epitomize the sound waves fronts transmits from the siren. This has been explained using the **Figure 15.**

The frequency of the siren of engine as perceived with the aid of a person at the firetruck has not modified. Despite, the waves in the path of the truck's movement bunch up as the fire truck has been caught up to its very endemic sound waves. The strain fluctuations, which are illustrated via the sine waves, encroach upon the eardrum of the static observer at an expanded frequency. The static observer to the right consequently recognize a greater tone than the one in reality vented from the fire truck.

Consider that the waves at the back of the fire truck (on the left aspect of the diagram) are unfold out due to the fact that the siren is transferring far from its inherent sound. This will motive a static observer to the left of the truck to identify a decrease inside the frequency of the siren. [16]

For a supply shifting to the right, a static observer to the right would recognize a higher tone and one to the left could identify a decrease tone. The non-relativistic Doppler shifted frequency of an object moving with speed v with respect to a stationary observer, is:

$$f' = f_0 \left(\frac{1}{1 + \frac{v}{c_0}} \right)$$ ……………………………………………………………………………….*Equation 3*

And the Doppler shifted wavelength can be represented as:

$$\lambda' = \lambda_0 \left(1 + \frac{v}{c_0} \right)$$ ……………………………………………………………………………….*Equation 4*

In those equation 1 and equation 2, c_0 is the speed of the wave in a static medium (the agility of sound in this example), and the velocity is the radial intrinsic of the velocity (the part in a undistorted line from the observer). Both of the above formulas are contrary resemblance which can be real as long as the velocity of the moving object is a lot less than the speed of light.

"As a covenant, the velocity is authentic if the origin is shifting away from us and negative if the origin is moving closer to the observer."

Accordingly:

- If the supply is shifting away (actual velocity) the ascertained frequency is lower and the ascertained wavelength is greater (redshifted).
- If the supply is transferring towards (adverse velocity) the determined frequency is higher and the wavelength is shorter (blue shifted)

Formulas of Doppler shift with description:

This perceivable exchange in the frequency of sound due to relative movement among the source and the observer is the Doppler Effect. The figure 16 demonstrate that there is change in frequency if the source is at rest or if the source is at motion.

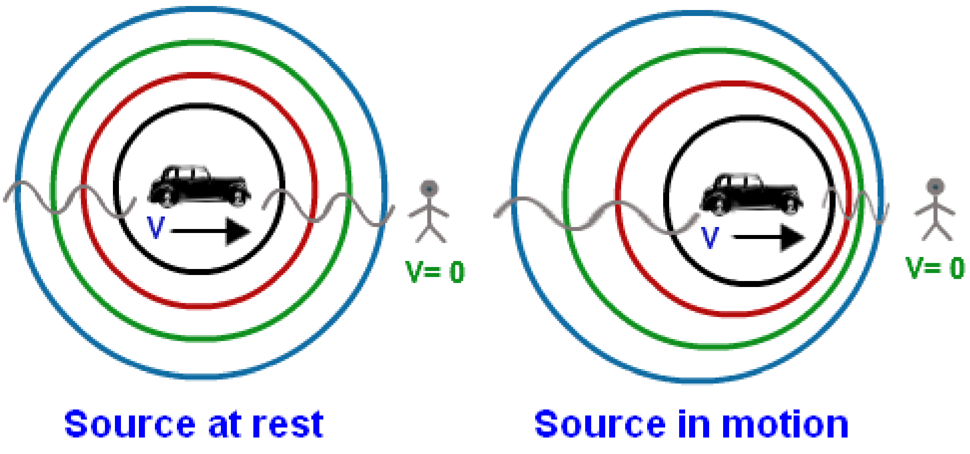


Figure 16. Source between rest and motion

There are eight **Doppler Effect Formulas** for frequency depending on cases:

(i)The equation 7 expressed when the source is propelling with respect to the stationary observer

$$f' = \frac{v}{v - v_s} f$$ ……………………………………………….Equation5

(ii) The equation 8 expressed when the source is propelling against the stationary observer

$$f' = \frac{v}{v + v_s} f$$ ……………………………………………………………….Equation 6

(iii) The equation 9 expressed when the observer is propelling with respect to the source at rest

$$f' = \frac{(v + v_o)}{v} f$$ ………………………………………………………………Equation 7

(iv) The equation 10 expressed when the observer moving against a source at rest

$$f' = \frac{(v - v_o)}{v} f$$ ………………………………………………………………Equation 8

(v) The equation 11 expressed when both Source and observer propels with respect to each other

$$f' = \frac{(v + v_o)}{(v - v_s)} f$$ ……………………………………………*Equation 9*

(vi) The equation 12 expressed when both Source and observer propels against each other

$$f' = \frac{(v - v_o)}{(v + v_s)} f$$ ……………………………………………………………………….*Equation10*

(vii) The equation 13 expressed when the Source is propelling towards the observer at rest and the observer is propelling against it

$$f' = \frac{(v - v_o)}{(v - v_s)} f$$ ………………………………………………………………………….*Equation 11*

(viii) The equation 14 expressed when the Observer is propelling the towards the source at rest and the source is propelling against it

$$f' = \frac{(v + v_o)}{(v + v_s)} f$$

……………………………………………………………………..*Equation12*

Where, v_s = Velocity of the Source,
v_o = Velocity of the Observer,
v = Velocity of sound or light in medium,
f = Real frequency,
f' = Apparent frequency.

Doppler shift formula is used to locate the ascertainable frequency and wavelength for the source transmitting toward the observer and away from the observer or observer shifting closer to the source or far away from the source. For our analysis we require the last four formulae. [14][16]

Algorithm of the predictable Analysis

- At first, read the observation file for reading the header like L1, L2, C1, P1 etc.
- Then skip the header of observation file.
- Calculate time of received.
- Extract the required field to calculate position using Fortran method of description as the RINEX file has been written using Fortran.

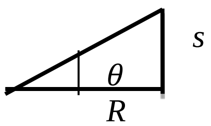
- Then, calculate the position x, y, and z from observation file which is referred as observation position.
- After finding the position from observation file, now, read the navigation file.
- Extract the required fields to calculate position from navigation file using Fortran.
- Then, calculate the position x1, y1, and z1 from navigation file which is referred as navigation position.
- The observation positions and navigation position are used to scatter the plot and observe that which satellites are available.
- Then both of them have been used to find out the Doppler shift of the available satellites.
- Formula of Doppler Shift has been shown in equation 11 to get the Doppler shifted frquency

$$\text{f} = \left(\frac{c+v_r}{c-v_s}\right) f_0 \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textit{Equation 13}$$

Where,

f = Doppler shifted frequency
*c = 2.99*10^8*
v_r= *Velocity of receiver*
v_s= *Velocity of satellites*
f_0= *Apparent frequency*
$\boldsymbol{\rho}$= *Distance from receiver to satellite*

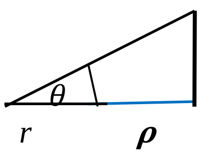
- To find Doppler shift at first find out the value of v_r, which has been shown in equation 12



$$\frac{s}{t} = \frac{r\theta}{t}$$

or, v_r = rω……………………………………………………………….................*Equation 14*

- Then calculate the value of v_s, which has been shown in equation 13



$$\frac{s}{t} = \frac{R\theta}{t}\;,\; R=\boldsymbol{\rho}+r$$

or, v_s = Rω……………………………………………………………….*Equation 15*

- For v_s, we have to measure the value of rho, which has been shown in equation 14

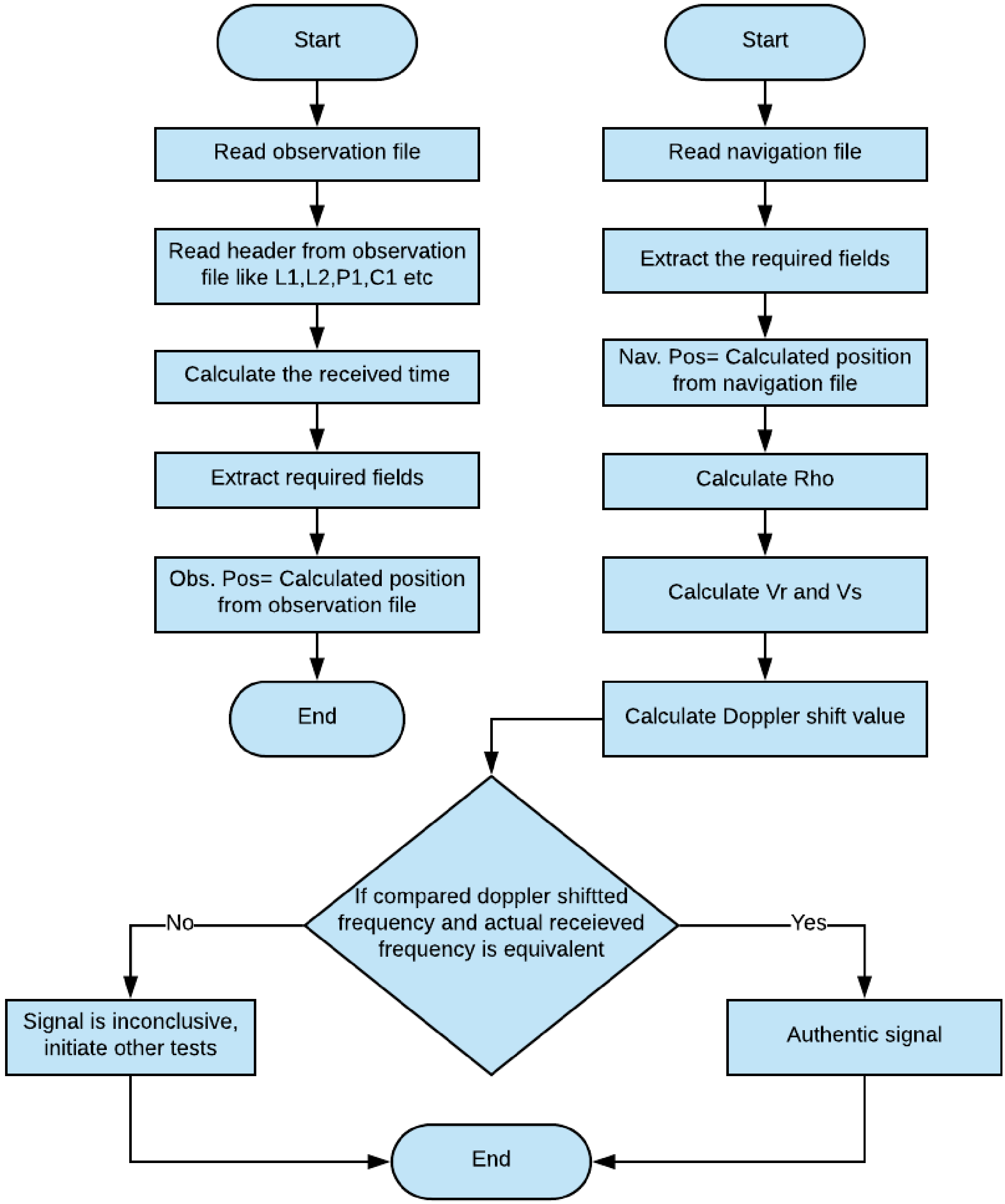
Nav. Pos. *Obs. Pos.*

(x, y, z) *(x1,y1,z1)*

$$\boldsymbol{\rho} = \sqrt{(x-x1)^2 + (y-y1)^2 + (z-z1)^2} \quad \text{……….…………} \textit{Equation 16}$$

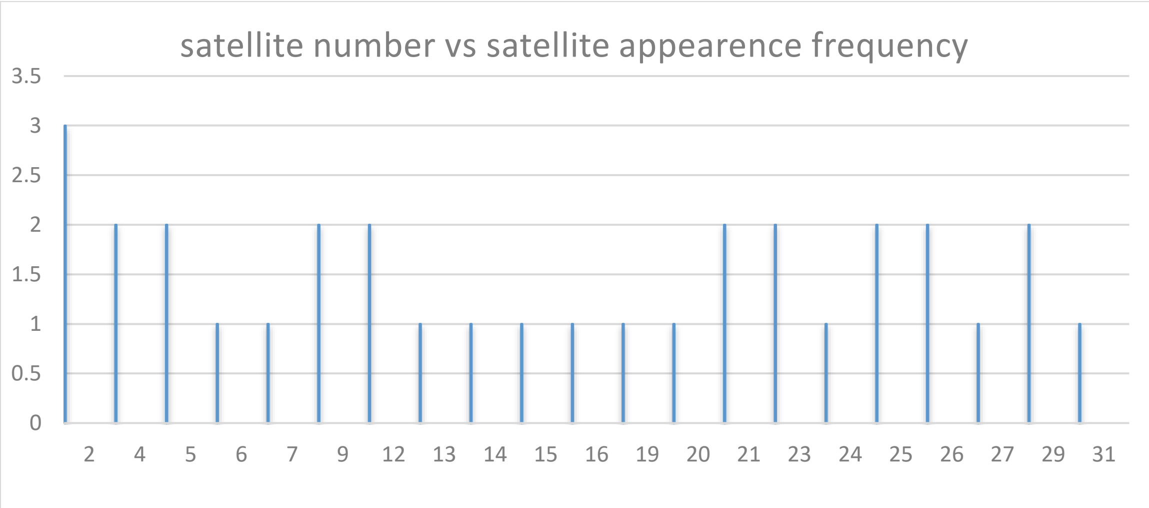
- ❖ Now, using the above measurement calculate Doppler shift and show them using a chart and a graph.
- ❖ Then compare the calculated Doppler shifted frequency with the original received frequency and observe the difference.
- ❖ If the compared value is not same then it would be considered as the authentic signal.
- ❖ If the compared value is same then it would be considered as inconclusive signal and after that initiate other four tests which are power test, inertia test, altitude test and MCSS test.

Flowcharts of the predicted Analysis



Chapter 6. Result and Analysis

We get the information of how many times a satellite has appeared from navigation file. Analyzing the following **Figure 17**, **satellite number vs satellite appearance frequency** graph we get that there are 21 satellites among them satellite 2 has appeared 3-times which is the highest appearance, satellite 4,5,9,12,21,3,25,26 and 27 have appeared 2-times and the other satellite 6,7,13,14,15,16,19,20,24,27,31 have no repetition of appearance in the respective navigation file.



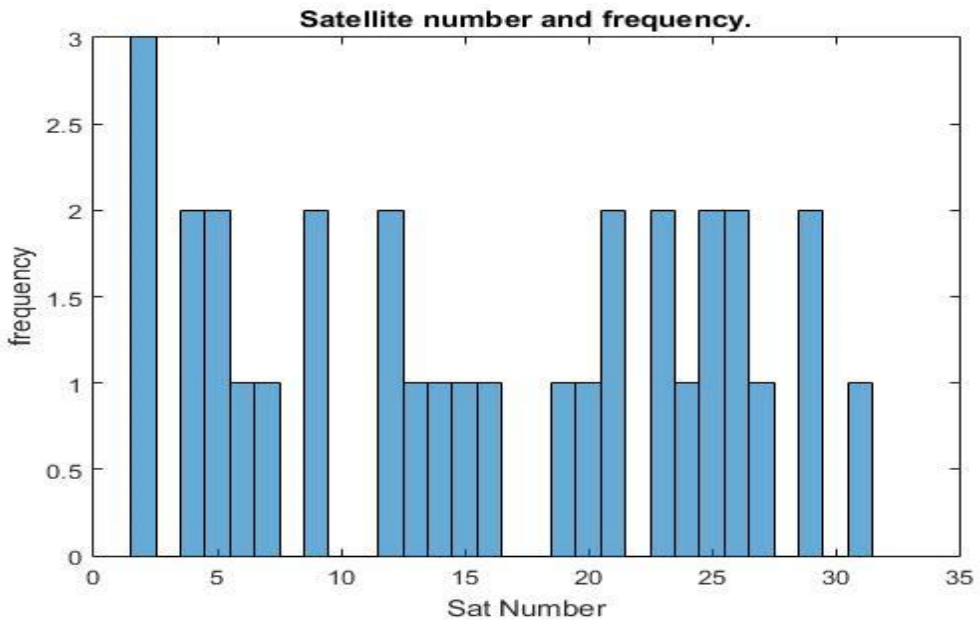


Figure 17. Satellite number vs appearing frequency of satellite.

From **Figure 18 and figure 19 of** the graph satellite number vs Doppler shift. In **Figure 18** we see that with the repetition of satellite the Doppler shift of the respective satellite has changed. This phenomena happens for the satellites those have appeared more than once in the navigation file. In Figure 19 the graph represents the Doppler shift of each satellite with respect to the carrier frequency of the satellite. Here, L1 is denoting the carrier frequency.

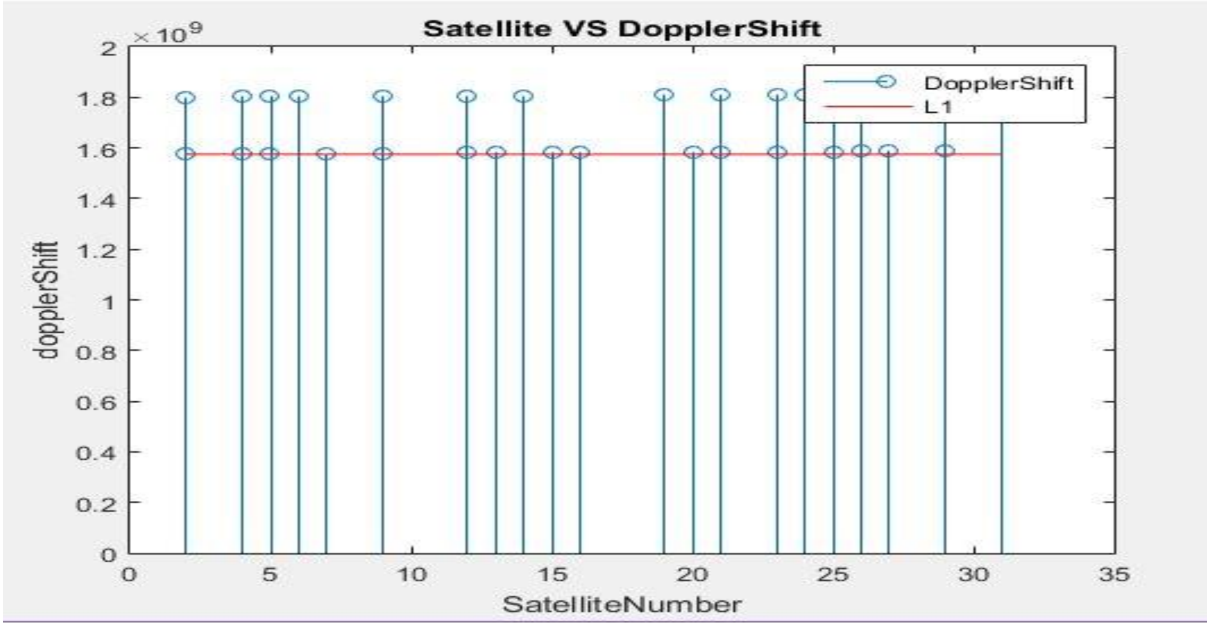


Figure 18. Satellite number vs Doppler shift

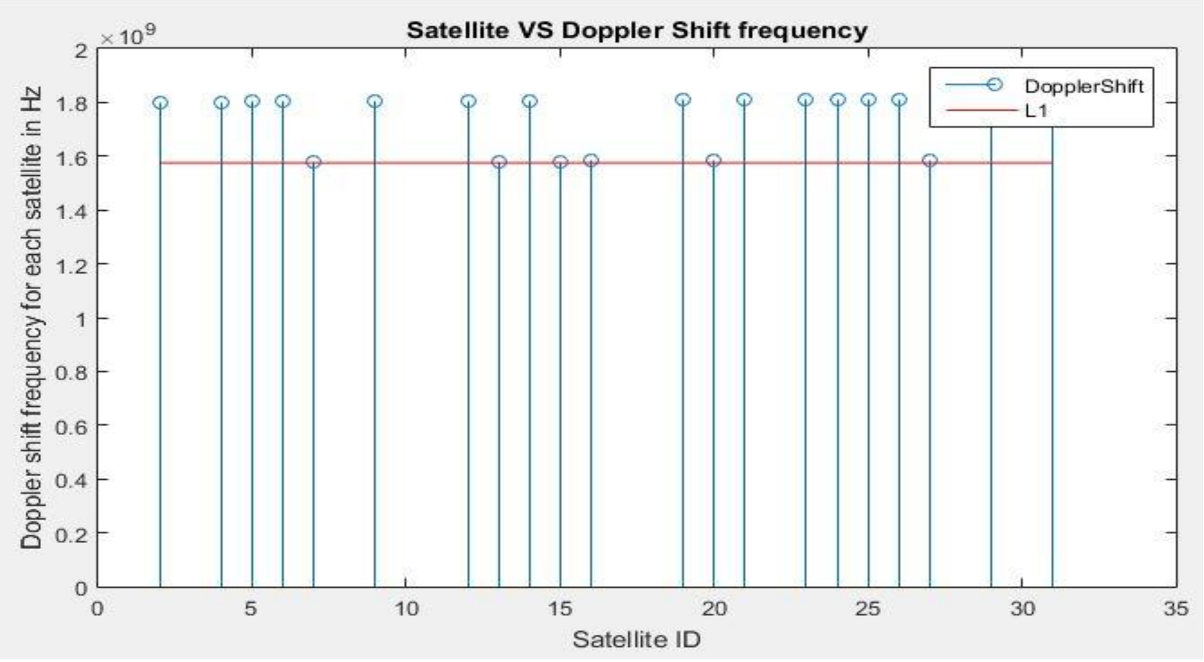


Figure 19. Satellite number VS Doppler shift for each satellite.

Satellite vs Doppler shift difference graph in **Figure 20** shows that the difference between the frequencies of Doppler shift of each satellite and carrier frequency L1. Here, the difference of frequencies is downward. Satellite 7, 3, 15, 16 and 20 have the minimum difference between the actual and shifted frequency which is 1581588575.99018 Hz.

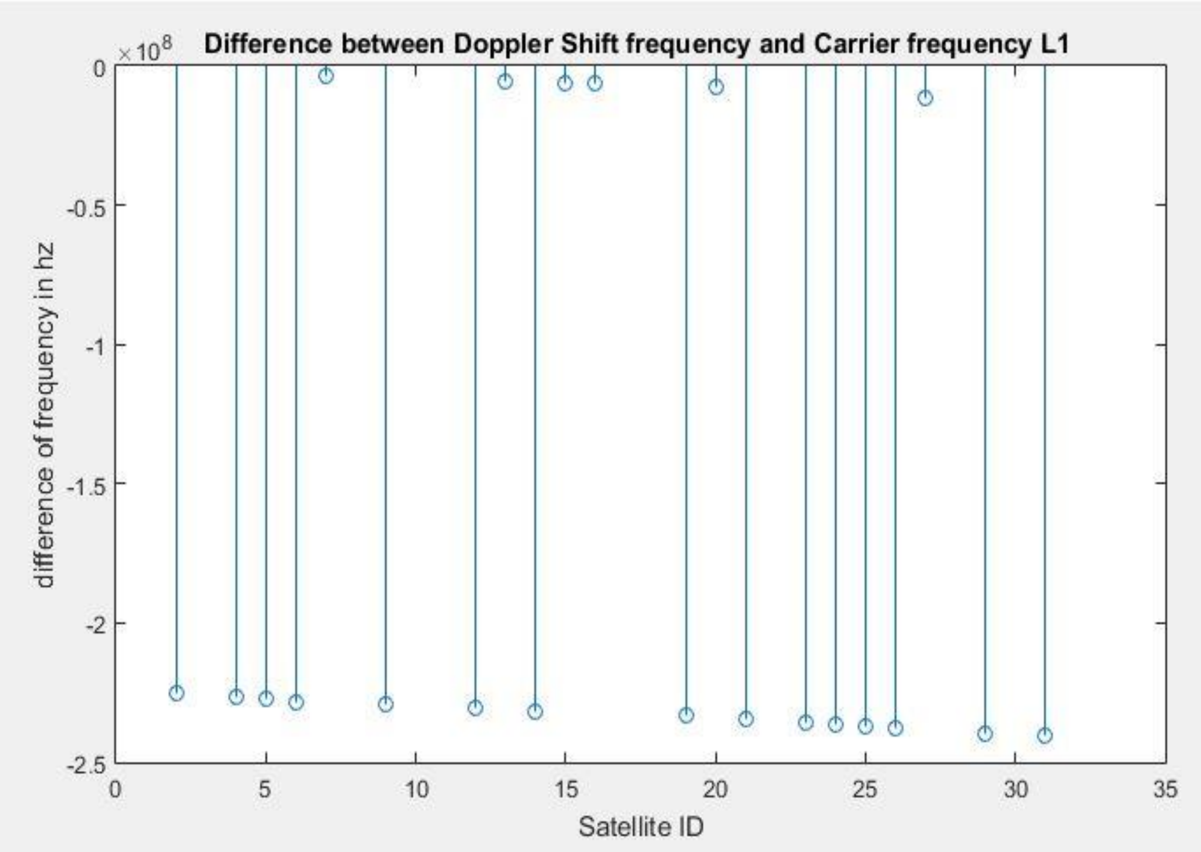


Figure 20. Satellite vs Doppler shift difference.

Satellite ID	Doppler shift frequency (Hz)	Difference between Doppler shift frequency and carrier frequency L1 (Hz)
2	1800.347403924184 ×10^6	-0.224927403924184
4	1801.834596653156 ×10^6	-0.226414596653156
5	1802.829616119982 ×10^6	-0.227409616119982
6	1803.827575265756 ×10^6	-0.228407575265756
7	1579.151888188046 ×10^6	-0.003731888188046
9	1804.828506900625 ×10^6	-0.229408506900625
12	1805.832454796528 ×10^6	-0.230412454796528
13	1580.767023947481 ×10^6	-0.005347023947480
14	1807.344164258745 ×10^6	-0.231924164258745
15	1581.588575990176 ×10^6	-0.006168575990176
16	1581.999244413522 ×10^6	-0.006579244413522
19	1808.862957104573 ×10^6	-0.233442957104573
20	1582.820364794632 ×10^6	-0.007400364794632
21	1809.879469539945 ×10^6	-0.234459469539945
23	1810.899220975923 ×10^6	-0.235479220975923
24	1811.922236245324 ×10^6	-0.236502236245324
25	1812.434980867159 ×10^6	-0.237014980867159
26	1813.462924981407 ×10^6	-0.238042924981407
27	1586.921589901269 ×10^6	-0.011501589901269
29	1815.011044999290 ×10^6	-0.239591044999290
31	1816.047263380434 ×10^6	-0.240627263380434

Figure 21. Satellite Id, Doppler shift of each satellite and Doppler shift difference.

In the **Figure 22** we have shown about satellite's and receiver's position for the respected available satellite. In **Figure 23** we have seen that the corrupted signal graph shows a straight line. Because corrupted signal shows exact frequency but due to Doppler shift there will be an obvious difference in frequency. So signal frequency can't not be same like L1 band frequency. If it show that both frequency are same than we can say that the signal frequency is not accurate on original.

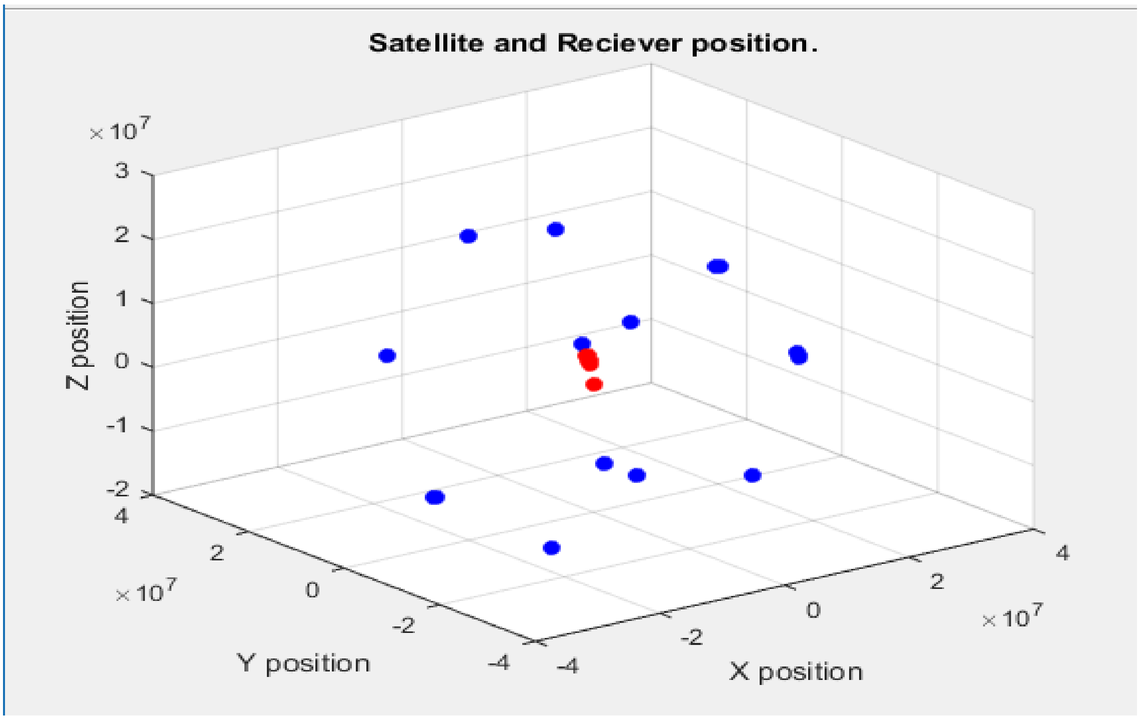


Figure 22. Satellite and receiver's position

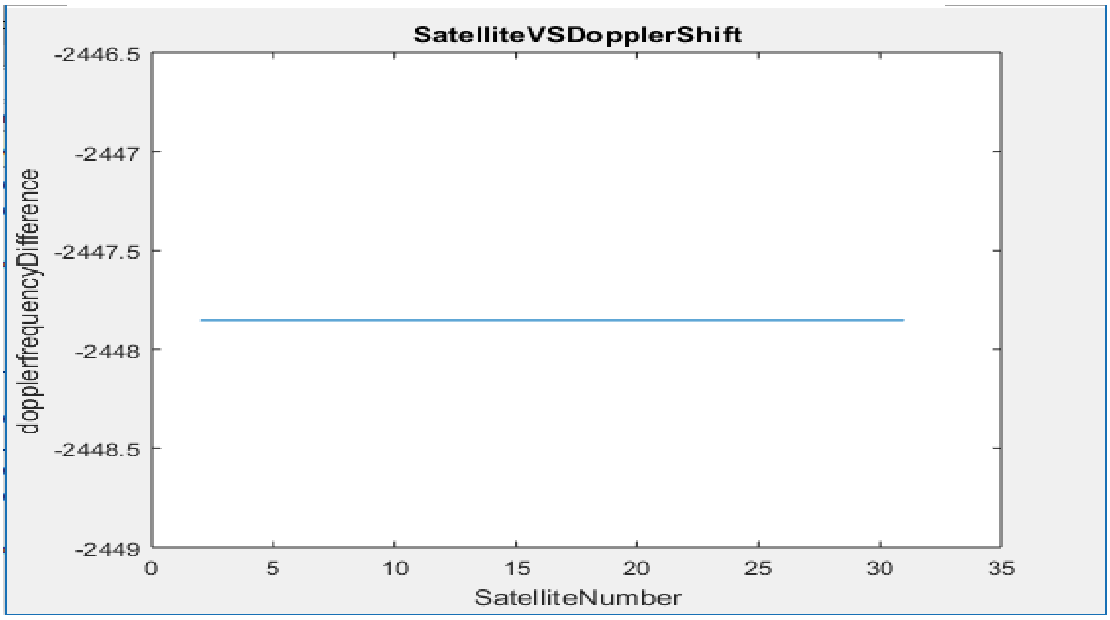


Figure 23. Corrupted signal's Doppler shift

Chapter 7. Conclusion

Summary:

As different types of countermeasures are being taken, the GNSS systems could still be hacked. Various vulnerabilities have been and still being explored, and steps are being proposed to secure the GNSS. Jamming is one of the heinous attacks against GNSS and methods had been implemented to ensure the authenticity of the GNSS signals. However, the replay attack is still an effective one, since it increases the pseudo range calculated by the receiver with an apparent increase in the signal propagation time.

In this report, based on previous study we have detected satellite's and receiver's position. This position helps us to detect about the available satellite. Then we have been used Doppler shift for detecting the replay attack. To detect whether the signal is coming from Jammer or the available satellite we have derived an algorithm. In the algorithm we have been calculated Doppler shift frequency of the available satellites. Then compare the calculated Doppler shift value with the apparent given frequency. If the difference is large the signal is coming from Jammer else the signal is coming from the original available satellite.

To detect the signal we implemented this mechanism. As satellite moving in curve path and the time clock is atomic so the signal is not perfectly arrived at the signal frequency which is expected. That's why Doppler shift will change and arrived at the frequency that we have calculated. If a sophisticated adversary can mimic the signal then it will create a negative effect on this algorithm but it is near impossible.

One of the reason is, normally the signal data which we have used and at least 7 satellite that we have considered for our calculation is totally unknown to a random adversary as there are 32 satellite's information is available and we have been chosen those 7 satellites randomly from that. So it is not possible for an adversary to predict the information of the calculated data of satellites.

Also in a very short time it will not possible to hack each and every satellite's data and change their information and also predict our considered satellite's and receiver's velocity if it is in a moving state and then calculated the Doppler shift. So our tool is near impossible to hack by the Jammer.

Limitations:

This tool work works on GPS data available open source for educational purposes. Currently, this tool works on static receiver but if we modified the Doppler shift equation by adding the velocity of the receiver then it will also accurately work on mobile receiver. We consider that the satellite is moving around the earth in a direction straight path but in real life the satellite follow the devious path.

Future works:

- In future our tool will be optimized more to implement this tool on real GPS devices.
- Now, this tool works on open source data which is available for educational purposes. In future it can be modified to work on real time data extracting from satellites.
- In future this algorithm can be make more accurate using other conditions like frequency’s power test, amplitude test, location inertia test, motion test etc.
- In future it will consider satellite’s devious path where we have used satellite’s straight directional path.
- We work using static receiver, in future it will consider mobile receiver.
- In future work this algorithm can be modified a little to work on GLONASS.

Bibliography

[1]D. Lee, "Garmin | What is GPS?", *Www8.garmin.com*, 2018. [Online]. Available: https://www8.garmin.com/aboutGPS/. [Accessed: 31- Aug- 2018].

[2]"GPS (Global Positioning System) Definition", *Techterms.com*, 2018. [Online]. Available: https://techterms.com/definition/gps. [Accessed: 31- Aug- 2018].

[3]"How does GPS work?| Explore | physics.org", *Physics.org*, 2018. [Online]. Available: http://www.physics.org/article-questions.asp?id=55. [Accessed: 31- Aug- 2018].

[4]"How GPS Works", *Maptoaster.com*, 2018. [Online]. Available: https://www.maptoaster.com/maptoaster-topo-nz/articles/how-gps-works/how-gps-works.html. [Accessed: 31- Aug- 2018].

[5]"How Does a Global Positioning System (GPS) Tracking System Works?", *ElProCus - Electronic Projects for Engineering Students*, 2018. [Online]. Available: https://www.elprocus.com/how-gps-system-works/. [Accessed: 31- Aug- 2018].

[6]"Learn How GPS Communication Works In GPS Tracking Devices", *Brickhousesecurity.com*, 2018. [Online]. Available: https://www.brickhousesecurity.com/gps-trackers/gps-communication/. [Accessed: 31- Aug- 2018].

[7]"What is triangulation? - Definition from WhatIs.com", *SearchNetworking*, 2018. [Online]. Available: https://searchnetworking.techtarget.com/definition/triangulation. [Accessed: 31- Aug- 2018].

[8]"What is Triangulation? - Definition from Techopedia", *Techopedia.com*, 2018. [Online]. Available: https://www.techopedia.com/definition/14856/triangulation. [Accessed: 31- Aug- 2018].

[9]"Trilateration vs Triangulation - How GPS Receivers Work - GIS Geography", *GIS Geography*, 2018. [Online]. Available: https://gisgeography.com/trilateration-triangulation-gps/. [Accessed: 31- Aug- 2018].

[10]"Spoofing and jamming: tackling threats to GPS-guided systems - Airforce Technology", *Airforce Technology*, 2018. [Online]. Available: https://www.airforce-technology.com/features/featurespoofing-and-jamming-tackling-threats-to-gps-guided-systems-5649119/. [Accessed: 31- Aug- 2018].

[11]J. Gould, "Guided-Bomb Makers Anticipate GPS Jammers", *Defense News*, 2018. [Online]. Available: https://www.defensenews.com/air/2015/05/31/guided-bomb-makers-anticipate-gps-jammers/. [Accessed: 31- Aug- 2018].

[12]Y. Lappin, "Missile defense expert warns of growing strategic threat", *The Jerusalem Post | JPost.com*, 2018. [Online]. Available: https://www.jpost.com/Defense/Precision-

guided-rockets-missiles-becoming-strategic-threat-architect-of-missile-defense-system-warns-338299. [Accessed: 31- Aug- 2018].

[13]"RINEX-FORMAT | Global Positioning System | File Format", *Scribd*, 2018. [Online]. Available: https://es.scribd.com/document/52630304/RINEX-FORMAT. [Accessed: 31- Aug- 2018].

[14]"Doppler Shift", *Imagine.gsfc.nasa.gov*, 2018. [Online]. Available: https://imagine.gsfc.nasa.gov/features/yba/M31_velocity/spectrum/doppler_more.html. [Accessed: 31- Aug- 2018].

[15]"Doppler Shift", *Astrosun2.astro.cornell.edu*, 2018. [Online]. Available: http://astrosun2.astro.cornell.edu/academics/courses/astro201/doppler.htm. [Accessed: 31- Aug- 2018].

[16]2018. [Online]. Available: https://formulas.tutorvista.com/physics/doppler-effect formula.html. [Accessed: 31- Aug- 2018].

[17]"IGS Formats", *IGS*, 2018. [Online]. Available: https://kb.igs.org/hc/en-us/articles/201096516-IGS-Formats. [Accessed: 31- Aug- 2018].

[18]"A Solution For The GPS Jammer Threat", *Strategypage.com*, 2018. [Online]. Available: https://www.strategypage.com/dls/articles/A-Solution-For-The-GPS-Jammer-Threat-11-21-2013.asp. [Accessed: 31- Aug- 2018].

[19]2018. [Online]. Available: https://www.coursehero.com/file/p4fdagv/The-time-tags-in-the-GLONASS-navigation-files-are-given-in-UTC-ie-not-Moscow/. [Accessed: 31- Aug- 2018].

[20]2018. [Online]. Available: https://www.coursehero.com/file/pplkmm/Gurtner-W-G-Mader-1990a-The-RINEX-Format-Current-Status-Future-Developments/. [Accessed: 31- Aug- 2018].

[21]"Handbook of Space Engineering, Archaeology, and Heritage", *CRC Press*, 2018. [Online]. Available: https://www.crcpress.com/Handbook-of-Space-Engineering-Archaeology-and-Heritage/Darrin-OLeary/p/book/9781420084313. [Accessed: 31- Aug- 2018].

[22]*Colorado.edu*, 2018. [Online]. Available: https://www.colorado.edu/engineering/ASEN/asen6090/rinex.format. [Accessed: 02- Sep- 2018].

[23]R. Tuhin, "Securing GNSS Receivers with a Density-based Clustering Algorithm", *DIVA*, 2018. [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=diva2:903430. [Accessed: 02- Sep- 2018].

Appendix A

List of Acronym

RINEX- Receiver independent change

3D-Three Dimensional Space

AWS-Amazon Web Services

VM-Virtual Machine

GNSS – Global Navigation Satellite Systems

GPS – Global Positioning System

MCSS – Multiple Combinations of Satellites and Solutions

WGS84 – World Geodetic System 1987

LLA – Latitude, Longitude, Altitude

ECEF – Earth Centered, Earth Fixed

GLONASS - Globalnaya Navigatsionnaya Sputnikovaya Sistema

ESA – European Space Agency

C/A – Coarse/Acquisition

SAASM - Selective Availability Anti-Spoofing Module

OPTICS - Ordering Points To Identify the Cluster Structure

EM – Expectation Minimization

mS, µS, nS – millisecond, microsecond, nanosecond

MATLAB – Matrix Laboratory

ELKI - Environment for Developing KDD-Applications Supported by Index-Structures

SV – Satellite Vehicle

PRN – Pseudo Random Noise

UNAVCO – University NAVSTAR Consortium

FTP – File Transfer Protocol

Appendix B

List of Notation

λ	This is Lambda
μ	This is mu
δ	This is Delta