4 The Growth and Expansion of Precise Navigation and Timing

Introduction

There are actually many terms that are used to characterize Global Navigation Satellite Services (GNSS) around the world. Some of these terms include: Precision Navigation and Timing (PNT), Sat Nav, and GPS (for Global Positioning Satellites). There are also a growing number of systems that provide this type of service. These include the Glosnass system operated by Russia, the Chinese Beidou and Compass systems, the Japanese Quasi-Zenith system, the Indian Regional Navigation Satellite system, and the European Galileo system. There are possibly others that might be initiated in the future, such as system deployed by the Republic of Korea and one operated by the United Kingdom if it is not able to negotiate continued participation in the Galileo system due to Brexit [1].

How GNSS Satellites Establish a User's Exact Location

A GNSS satellite is constantly sending out a timed signal, and as the signal radiates through space it creates an ever-expanding sphere. If at least three spheres from three different satellites intersect at the same instant in time it means it can only be one precise location above Earth's surface. The other possible intersection would be below Earth's surface. If four spheres from four satellites intersect at the exact same instant in time then there is only one possible location. If five spheres from five different locations intersect then there is even more precision as to the location. In short, the more signals from the overhead satellites that intersect at the same exact moment in time the better the accuracy of the location. Figure 4.1 illustrates the point – literally.

J. N. Pelton, *Space 2.0*, Astronautical Engineering,
https://doi.org/10.1007/978-3-030-15281-9_4

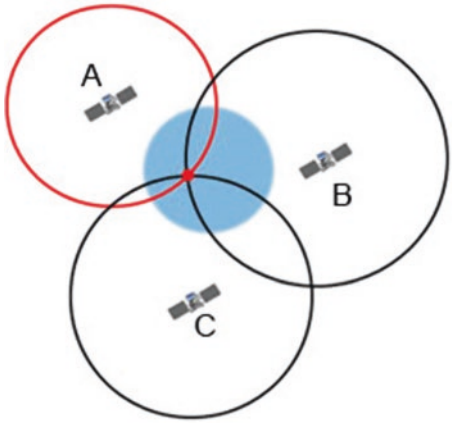

Fig. 4.1 The intersecting circles represent the radiated spheres from GNSS satellites

Innovations in GNSS Systems

These various navigation systems vary in their coverage and capabilities. All depend on the precision of timing provided by on-board atomic clocks. All but the Japanese system operate in high medium Earth orbits of about 12 hours in duration.

It is also possible to supplement the accuracy of these systems via land-based equipment to meet specialized needs. In the United States, the Federal Aviation Administration (FAA) has been responsible for the development of a satellite-based augmentation system (SBAS) known as the Wide Area Augmentation Service (WAAS). WAAS relies on ground stations located very precisely on very accurately surveyed locations distributed around the United States. It then constantly beams out locations via two different geosynchronous satellites, which are located at 107 degrees West and 133 degrees West.

The purpose of WAAS is to allow the combined GPS and WAAS navigation systems to assist with the takeoff, landing and all phases of aircraft operations in the United States. The stated goal of the WAAS operation is to improve the "accuracy, integrity and availability" of the GPS system as an aid to aviation and aviation safety [2].

There is also what is known as the Continuously Operating Reference Stations (CORS), which is run by the National Geodetic Survey (NGS). This unit is a part of the U. S. National Oceanic and Atmospheric Administration. CORS provides the NAVSTAR GPS network data consisting of carrier phase and code range measurements in support of three-dimensional positioning, meteorology, space weather, and geophysical applications throughout the United States, its territories, and also several other countries as well.

The CORS network is relied on by many surveyors and Global Information System (GIS) users, as well as a number of engineers, scientists and the public at large who are dependent on highly accurate positioning data, particularly those requiring three-dimensional locational data with exact precision within a very few centimeters – both horizontally and vertically.

The CORS network is a cooperative endeavor. Thus it involves many partners that include a number of governmental agencies plus academic, private and commercial participants. With the CORS network, the sites are independently owned and operated. There are over 2,000 stations in the network and over 200 different partner organizations [3].

There have been various efforts around the world to improve the accuracy of NGSS networks around the world via such means as ever more accurate atomic clocks and ground-based systems where exact locations are known, such as the WAAS and the CORS network. Improvements and augmentation systems that have been developed by other countries within their GNSS systems can be found in the article written by Dr. Sergio Camacho-Lara and referenced from the Second Edition of the *Handbook of Satellite Applications* by this author. Some of these systems are seeking to achieve even millimeter precision to support geodetic scientific purposes and other applications [4].

There have also been efforts to improve the resilience of GNSS systems and ensure their continuous availability and to protect them against possible cyber-attacks and hacking of their operating control systems.

One of the top concerns has been with an ongoing effort to upgrade the performance of GNSS satellites to make them less vulnerable to jamming and to guard against any hostile attacks that might be undertaken by a hostile government, a terrorist organization or even some form of criminal attack by hacker adversaries.

The velocity of the various GNSS satellites as they move in orbit relative to the speed of light is sufficient that the effects of Einstein's relativity of motion must be taken into account in order to achieve the proper calculation of a specific location with exact precision. Some of the most advanced systems now in operation include the Russian Glonass M series, the U. S. Navstar GPS Block IIIA satellites and the Chinese Beidou 3 satellites. (These three types of GNSS satellites are shown respectively in Figs. 4.2, 4.3 and 4.4.)

The specifications for the Chinese Beidou 3 satellites, for instance, include ultra-exact atomic clocks that are specified to have an accuracy of only being off by one second in every 300 years. Such accuracy, when coupled with high-performance ground systems, could produce location accuracies to within millimeters on Earth's surface [5].

If there is interest in the technical details about GNSS orbits, reference systems, carrier frequencies, time kinematic systems, GNSS Augmentation systems or other technical details, it recommended that one consults the article by Rogerio Enriquez-Caldera in the *Handbook of Satellite Applications* (Second Edition) [6].

In recent years the greatest areas of advancement have not come in the form of important technical upgrades to the satellites, No, the main advances are coming with the many important applications and new uses that continue to be developed for precise navigation and timing satellites. Today GNSS satellites provide vital services for the routing of ships at sea, cars, trucks, buses and other vehicles. These satellites assist with the takeoff, landings and routing of aircraft. They also provide vital timing services for countries around the world. The operational uses of these highly precise satellites also include time-stamping as

Fig. 4.2 The Glonass M Series as deployed by the Russian Federation. (Image courtesy of the Russian Academy of Science.)

part of the security system used for banking transactions and other secure financial transactions.

A market analysis of GNSS applications came up with the following figures. Location-based services represented 53% of the market, road-based services represented 38%. Other applications, such as surveying and mapmaking, rail, agriculture, fishing, maritime, timing synchronization, and security and aviation filled out the remaining 9%. The percentage of use, however, is not necessarily an accurate indication of the importance of the usage. The usage for aeronautical and time synchronization purposes only represents a little over 1% of the total, but these applications are vital to aircraft safety and operation of the Internet [7].

And going forward, opportunities remain even more diverse. GNSS systems will for instance not only be for aircraft routing and landing but will also be key to the operation of autonomous vehicles, autonomous freight operations, and even robotic freighters in the skies, flying above commercial airspace. This will not only potentially make automobile and trucking vehicular operations much safer, but all forms of freight operations on land and sea much more cost effective. There are many automated operations tied to GNSS networks that will likely allow significant productivity increases. Yet all of these vital operations come with additional concerns as to the reliable and continuous operation of these satellites. Thus there are significant privacy,

Fig. 4.3 The GPS Block IIIA Satellite Series. (Image courtesy of Lockheed Martin.)

cyber-security and vital infrastructure concerns attached to the safe and secure operation of these networks.

Key Issues and Concerns

The space-based precision navigation and timing services are now only second to satellite communications services in terms of market size. There are now billions of PNT units in operation around the world. Every smart phone in the world has a GPS unit installed inside, and thus there are truly billions of them operational worldwide. Just the manufacture and sales of GNSS units globally represents many billions of dollars in sales. The Satellite Industry Association's State of the Industry Reports for 2015 and 2016 put the totals for GNSS tracking units to be in excess of $30 billion per annum [8].

The applications have gone well beyond navigation, and the uses now include tracking of stolen vehicles and goods, security for tracking financial operations, support for detection

Fig. 4.4 Beidou 3 GNSS satellite with super accurate atomic clock. (Graphic courtesy of the China Academy of Sciences.)

systems for tsunamis, geodesic and seismic monitoring, and tracking of operational spacecraft and high altitude platform systems. In the future there might even be tracking of items such as orbital space debris or mobile robotic devices.

In the age of the Internet of Things, RFID systems, GNSS-based tracking and time-related services will be raised to a whole new level, with automated computer-based tracking of essentially anything that moves. The opportunities for GNSS-related services remain almost endless. Security systems of all different types can require someone to be precisely personally identified and also to be at an exact location to allow execution of various transactions. Commercial operations involved in transportation, shipping, retailing, farming, fishing and more can keep track of all of their assets in real time. Governments can use these systems for law enforcement, drug trafficking, pollution and environment policing and for a wide variety of national defense and military activities from surveillance to missile targeting to drone operations.

The concern is not whether we will find hundreds if not thousands of applications for GNSS networks. No, the concern is what is the backup plan if a vital GNSS system should fail or even be temporarily interrupted via jamming or other difficulty.

Should there be an interruption in the service of these vital networks, the

security of nations and vital economic systems could be put at risk. Just one example of this criticality is the fact that for most countries of the world the synchronization of the global Internet relies on GPS, and thus if this system were to fail then the global Internet could be put at risk.

These new applications have significant opportunities for new commercial products and services, but there must also be serious concerns for the various issues that can arise.

Personal Surveillance, Privacy and Freedom

Today GPS-enabled cell phones not only allow efficient navigation from one location to another but it also allows precise tracking of where a person is located. Today in China, residents are assigned a Social Index Score that combines information about not only financial transactions and the prompt payment of bills but also data about crime convictions, traffic infractions, who one's friends are and political activities. This combined score indicates not only one's financial and legal status but also an overall assessment of whether one is a 'good citizen' or of questionable character. Instead of pressure to avoid 'bad' behavior, this scoring system creates a series of incentives to engage in "good behavior with good friends." [9]

And this is not a phenomenon that is unique to China. In the United States there is not only the FICO credit score, but a number of secret scores are also available. There is the Northpointe's COMPAS scoring system that is used to predict the recidivism rate for those going to jail and to assist in setting bail. In addition one can be judged by the Acxion consumer score. There is the Johns Hopkins Frailty Score, the SMR Research Charitable Donor Score, and the HiQ Labs Keeper Score that tracks the likelihood that employees might be recruited away by competitors. And this is far from a complete list. In the age of the Internet and GNSS systems it is possible to use computers to cross reference many different sources to track where one goes, what one does, how one spends money, and who they associate with. And this tracking capability will only increase with the spread of hundreds of billions of Internet of Things enabled units [10].

The growth of GNSS network usage is but one aspect of the digital privacy issue, but anyone who is carrying a smart phone with a GPS chip should be on notice that his or her whereabouts is constantly able to be tracked. In older movies and television shows the detectives were always asking for the whereabouts of suspects and checking out alibis. In today's world, one only has to have the smart phone's GNSS chip monitored. This should give pause to anyone who loans their cell phone to someone else or agrees to change the Subscriber Identity Module from one phone to another.

Cyber-Security and Hacking of Computerized Systems with GNSS-Enabled Devices

The other large and potentially even more significant concern about GNSS-enabled tracking systems is the possibility that they might be hacked by techno-terrorists, with catastrophic results. There are concerns that GNSS

location results might be hacked in order to give airline pilots and autopilot systems false readings that could lead to fatal airline crashes. One of the James Bond movies *Tomorrow Never Dies* has the fantastical plot line with Johnathan Pryce playing a megalomaniac news executive, serving to distort GNSS readings so as to start a war between China and the West. This rather absurd plot line seems to suggest that he could make enormous amounts of money by reporting on the war that he rather singlehandedly has served to engineer.

Cyber-security is a difficult subject because there are so many potential areas of vulnerability. There are many types of malware in the form of viruses, Trojans, spyware and ransomware such as Wannacry. There are also so many possible modes of attacks through so many different types of devices such desktop computers, laptops, notebooks, cell phones and even data stored on the cloud, that users forget that there are even more potential areas of cyber-attack. The truth is that there are always more and new ways to possibly be attacked. There are now true concerns about Internet of Things-enabled devices from smart appliances such as refrigerators to washing machines to even more unlikely areas of vulnerability such as 'smart' doorbells, aquariums, or even baby monitors. There are certainly ways whereby GNSS systems can be jammed or potentially manipulated. And no one should forget that there is always some form of inside attack that can be made by code-protected infrastructure or highly secure systems.

And just as there are increasingly sophisticated ways that distributed denial of services (DDS) can overload websites, they could also certainly be used to disable vital GNSS navigational or timing services. A higher powered simulated but bogus GNSS signal could be used to steer an unsuspecting user into a dangerous or even a fatal activity. Consumers have become so accustomed to relying on the accuracy and reliability of GNSS signals and navigational instructions that they are in no way prepared for a potential criminal or terrorist attack that might be undertaken by either the jamming of a GNSS signal or a counterfeit signal that simulates signals from a GNSS network [11].

The latest GPS Block III satellites, for instance, have been designed to not only be more resistant to jamming and fake bogus signals but to be invulnerable to potential cyber-attack. The challenge is to have tools that aid the automatic detection of signal interference, jamming or spurious GNSS signals.

Vulnerability of Automated Systems That Depend on GNSS Systems and Backup Options

There are several concerns about the ongoing reliability and continuity of service of the various GNSS systems that are now deployed in space. At the most basic level there is the possibility that the battery that is supporting a mobile GNSS device, perhaps in a cell phone, loses power or a chip set might fail.

Then there is the special case of an autonomous vehicle that perhaps comes to a complicated construction site where flag men are diverting traffic into a confusing system defined by cones or a temporary alleyway.

Alternatively there could be a situation with a long tunnel where an

autonomous vehicle has lost contact with the GNSS network and needs backup support. In such cases there could be a need for the autonomous vehicle to signal a problem. A possible solution could be provided by a remote 'phantom driver' to respond to such an alarm. The remote human driver equipped with cameras and GNSS systems could then take over control of the automobile, truck or bus to provide temporary navigation through the obstacles until the complication to the autonomous control is resolved. The case of an overlong tunnel excursion or traffic jam in a tunnel could potentially defeat this remote phantom driver's rescue solution unless all tunnels were to be equipped with broadband video mobile telecommunications capabilities. A company known as Phantom Auto is actually testing various telecommunications-based capabilities to allow a backup human driver to assume control of stranded autonomous vehicles that find themselves in a confused or unsafe situation where the onboard computer system shuts down the autonomous controls [12].

The more serious problems would be with the GNSS satellite system itself. There are several catastrophic events that could have a calamitous effect on the half dozen GNSS networks now in operation. One major concern would be a coronal mass ejection (CME) on a particularly violent scale that moves in the direction of Earth, perhaps similar in size to the Carrington event of 1859. Or there could be an atomic blast detonated near Earth that creates a strong electromagnetic pulse (EMP) that would also destroy the electronic control systems on GNSS satellites. In both cases the effects would be similar. Yet another possibility would be a particularly strong solar radiation flare that would be of sufficient magnitude to harm the satellites' electronic control systems.

The problem today is that the GNSS networks now in operation around our planet have become such critical infrastructure that the loss of these systems could have a catastrophic effect on the economy and transportation safety. These systems now provide truly vital services such as synchronization of the Internet and the use of these systems for the takeoff and landing of aircraft. They are also used for time stamping of banking operations and a wide variety of security activities. Perhaps in the next few years these GNSS networks will also become keys to autonomous vehicular self-driving cars and trucks. There are now various short videos available on You Tube with titles such as "Cosmic Hazards" and "If there were a day without satellites" that provide dramatic examples about how vital these networks have become to the entire global economy. They explore the consequences if the GNSS systems were to be disabled by solar storms, a manmade EMP or perhaps via a cyber-attack.

Care must therefore be taken as we move forward to design more redundancy into the GNSS networks and ground units to ensure with greater certainly their longer-term sustainability. This means user units and especially smart phones must be able to access more than one of these satellite networks if for some reason there should be a failure in one of these networks.

The Global Proliferation of GNSS Systems

The advent of more and more GNSS systems has continued to move forward. At one point there was just the GPS and

the Glonass systems. These systems were deployed for military reasons to support the precise tracking and guidance of ballistic missiles. The military purpose of these networks as well as the provision in these satellites for "selected availability" to obscure the exact positioning and navigation abilities of the GPS network led other countries to design and deploy alternative GNSS networks around the world.

Thus there are now six GNSS networks operating in orbit or now being implemented. These are the U. S. Navstar Global Positioning Satellite network, the Russian Glonass network, the Chinese Beidou network, the Japanese quazi-zenith network, the Indian Regional Navigation Satellite network, and the European Galileo network, which is currently being deployed. The United Kingdom has indicated that it may feel compelled to design and implement its own network if a cooperative agreement is not reached to allow its full participation in the Galileo GNSS network.

And this is not the only possibility for additional new GNSS networks. The Republic of Korea has indicated that it has plans to design, build and launch a new regional GNSS system. It will be phased in over time and is currently projected to be fully operational as of 2034. The South Korean Ministry of Science and Information and Communications Technology (ICT) has announced that it will take the lead in creating the Korean Positioning System (KPS).

The current lengthy schedule is to develop a ground test of the system components in 2021, design the core elements of the satellite navigation technology in 2022 and begin the production of the KPS satellites as of 2024. The current proposed design of the system (that might ultimately be different) would be to launch and operate a total of seven navigation satellites for the regional system, with three of the satellites being deployed in geostationary orbit above the Korean Peninsula. The effective navigation, timing and positioning system coverage area is to be up to a 1,000 miles around the perimeter of South Korea. The current navigational requirements are to utilize the U. S. GPS system, but the problem is that North Korea has frequently jammed the signals from it [13].

The question thus arises as to how many GNSS networks make technical, operational, and economic sense in our modern world? Does it make sense to have quite so many of these systems, especially since they essentially undertake the same function?

Other satellite applications such as satellite communications, satellite broadcasting, remote sensing, etc., provide unique services with increasing value to their users by relaying individualized messages or capturing images of particular sites. Additional spacecraft to provide more communications or remote sensing thus adds additional value, but satellite navigation systems are redundant and only add value in the event of spacecraft failure of the other systems. One could thus argue that adding more and more GNSS systems only increases the potential hazard of creating new orbital space debris and represents needless investment. In short, adding a fifth, sixth, seventh and eighth new GNSS system does not reasonably represent what can be described as true value once a reasonable level of redundancy and

backup is achieved. Super redundant systems do not allow new applications or uses, does not improve accuracy or efficiency of operation and uses up more RF frequencies, orbital space. In time it could also lead to additional orbital debris.

Conclusions

There have been a number of efforts to use space systems to create exact navigational systems from early in the space age. The first such systems used techniques such as Doppler shift that occurred as a satellite flew overhead in a precisely known orbit. The latest system that uses propagation times associated with transmission from satellites with ultra-exact atomic clocks on board is by far the most exact. With the latest atomic clock technology and calculation capabilities with the most exact chip sets in ground GNSS units, the level of precision has dropped from meters accuracy to even centimeters or even millimeters. This level of precision is sufficiently sophisticated to support targeting of missiles, the most exact surveys, or scientific geodetics work.

The current progress in the field of GNSS satellite navigation and precise timing is thus focused on essentially three areas. One area of concern is to work around and prevent the ill effects of jamming of GNSS signals coming from orbiting satellites. The second and closely related concern is to provide for the security of GNSS operations in order to prevent hacking. These cyber-security efforts seek to defeat attempts to hack into navigational or timing systems in either space or on the ground as well as in the military or commercial air space below outer space.

There are new cyber-security systems being developed to limit or prevent any and all adverse effects that might occur by virtue of interference with transmissions from GNSS networks. There is a particular effort to avoid distorting the accuracy of military tracking and targeting systems, and all types of automated systems that rely on GNSS systems such as aircraft avionics or autonomous vehicle navigation and control.

The third area for development with regard to GNSS operations is on the other side of the coin. These are research and development efforts in new applications, services and uses that depend on the effective use of GNSS systems. These efforts also include programs to coordinate cooperative use of all of the space-based systems. This activity would include efforts to create global standards, allocation of frequencies and new regulations with regard to anti-jamming measures, or other measures that would benefit all potential users all over the world. These new applications for GNSS networks can be of enormous value to new areas such as space traffic management, space situational awareness, etc. It might prove useful to the future safe utilization of the protozone, which is above commercial airspace. These new applications might include such activities as safe hypersonic transportation by means of space planes, the secure operation of high altitude platform systems, navigational support for robotic freighters operating above commercial air space and even the operation of dark sky stations.

References

1. Pelton, J.N., Camacho-Lara, S.: Introduction to satellite navigation systems. In: Pelton, J.N., Madry, S., Lara, S.C. (eds.) Handbook of Satellite Applications, 2nd edn, pp. 723–734. Springer Press, Cham (2017)
2. Camacho-Lara, S.: Current and future GNSS and their augmentation systems. In: Pelton, J.N., Madry, S., Lara, S.C. (eds.) Handbook of Satellite Applications, 2nd edn, pp. 781–790. Springer Press, Cham (2017)
3. Continuously Operating Reference Station. https://geodesy.noaa.gov/CORS/. Last Accessed 19 June 2018
4. Op cit, Sergio Camacho-Lara, pp. 781–804
5. Lin, J.: China's future satellite navigation will be millimeter-accurate. Popular Science, Nov. 7, 2017. https://www.popsci.com/china-beidou-3-satellite-navigation-system
6. Enriquez-Caldera, R.: Global navigation satellite systems: orbital parameters, time and space reference systems and signal structure. In: Pelton, J.N., Madry, S., Camacho-Lara, S. (eds.) Handbook of Satellite Applications, 2nd edn, pp. 735–762. Springer Press, Cham (2017)
7. GNSS: Market Report (2015) http://www.navipedia.net/index.php/GNSS_Market_Report
8. Satellite Industry Association-Tauri Group: State of the Industry Report. Washington, D.C. (2016)
9. Hvistendahl, M.: You are a number. Wired Magazine, January 2018. pp. 48–55
10. Myers, B: Secret scores. Wired Magazine, January 2018. p. 56
11. Pelton, J., Singh, I.: Digital Defense: A Cyber Security Primer. Springer Press, Cham (2015)
12. Burke, K: A designated driver for the driverless car: Phantom Auto tests remote-control system Feb. 17, 2018. http://www.autonews.com/article/20180217/MOBILITY/180219775/phantom-auto-tests-remote%20control%20for%20driverless%20cars
13. Korea will launch its own satellite positioning system, GPS World, February 5, 2018. http://gpsworld.com/korea-will-launch-its-own-satellite-positioning-system/