International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 1, Jan-Feb 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

GPS Security: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Global Positioning Security (GPS) focuses on vulnerabilities, real-world threats, and mitigation/protection strategies as GPS security is critical to modern economies, infrastructure, national defense, and personal systems as they rely on accurate positioning, navigation, and timing (PNT) provided by satellite systems like GPS. GPS is a part of a broader family of *Global Navigation Satellite Systems (GNSS)* which includes *GLONASS* (Russia), *Galileo* (EU), and *BeiDou* (China). All of these systems transmit timing and positioning data from satellites to receivers on earth to determine location and time. Apart from navigation, GPS also provides timing signals that underlie: financial transaction ordering, cell network synchronization, power grid stability, emergency response coordination, autonomous vehicles, and aviation and maritime navigation. The paper looks into the concept, pros, cons, and the usefulness of GPS Security to humanity.

KEYWORDS: *Global Positioning Security, GPS, Global Navigation Satellite Systems (GNSS), navigation, positioning, timing, GPS Jamming, GPS Spoofing, satellite navigation, cybersecurity, cyberattacks, timing attacks, artificial intelligence.*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "GPS Security: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-1, February 2026, pp.872-877, URL: www.ijtsrd.com/papers/ijtsrd100146.pdf

IJTSRD100146

INTRODUCTION

The Global Positioning System (GPS) is a satellite-based hyperbolic navigation system owned by the United States Space Force and operated by Mission Delta 31, as shown in Figure 1. The satellite constellation provides location, velocity, and time (PNT) data globally by the use of signals from orbiting satellites and ground receivers to calculate precise positioning via trilateration, essential for navigation in everything from smartphones to military systems, operating independently but enhanced by internet/cellular. The United States government created, controls, and maintains the GPS system, but this is freely accessible to anyone with GPS receiver. However, as at July 2023, 18 GPS satellites broadcast L5 signals, which are considered pre-operational prior to being broadcast by a full complement of 24 satellites in 2027 [1-5].

HISTORY

The GPS project was launched in 1973 in the United States to overcome the limitations of previous navigation systems [6], combining ideas from several predecessors, including classified engineering design studies from the 1960s. The US Department of Defense developed the system, which originally used 24 satellites, for use by the United States military, and became fully operational in 1993. Civilian use was allowed from the 1980s – due to the Cold War navigation mishap (e.g., Korean Air Lines Flight 007 in 1983). Credited for the invention were Roger L. Easton of the Naval Research Laboratory, Ivan A. Getting of The Aerospace Corporation, and Bradford Parkinson of the Applied Physics Laboratory [7]. The work of Gladys West on the creation of the mathematical geodetic earth model is credited as instrumental in the development of computational techniques for detecting satellite positions with the precision needed for GPS [8, 9], as shown in Figure 2.

The design of the GPS is based partly on similar ground-based radio-navigation systems, such as LORAN and the Decca Navigator System, developed in the early 1940s. Friedwardt Winterberg in 1955 proposed a test of general relativity – detecting time slowing in a strong gravitational field using accurate atomic clocks placed in orbit inside artificial satellites. Special and general relativity predicted that

the clocks on GPS satellites, as observed by those on earth, run 38 microseconds faster per day than those on the Earth. The design of GPS corrects for this difference [10, 11]; because without doing so, GPS calculated positions would accumulate errors of up to 10 kilometers per day (6 mi/d).

The Soviet Union launched its first artificial satellite (Sputnik 1) in 1957, with two American physicists, William Guier and George Weiffenbach, at Johns Hopkins University's Applied Physics Laboratory (APL) monitored its radio transmissions [12]. They realized that within some hours they could pinpoint where the satellite was along its orbit due to Doppler effect, and were given access to UNIVAC l computer by the Director of APL to perform the heavy calculations required. The following year, Frank McClure, the deputy director of the APL, asked Guier and Weiffenbach to investigate the inverse problem: pinpointing the user's location, as shown in Figure 3. (At the time, the Navy was developing the submarine-launched Polaris missile, which required them to know the submarine's location.) This led them and APL to develop the TRANSIT system [13]. In 1959, ARPA (renamed DARPA in 1972) also played a role in TRANSIT [14-16].

TRANSIT was first successfully tested in 1960. It was said that it used a constellation of five satellites and could provide a navigational fix approximately once per hour [17], as shown in Figure 4. The US Navy in 1967 developed the Timation satellite, which proved the feasibility of placing accurate clocks in space, a technology required for GPS [18]. During the Cold War arms race, the nuclear threat to the existence of the United States was the one need that did justify the cost in the view of the United States Congress. This deterrent effect is why GPS was funded [19-21] and was the reason for the ultra-secrecy at the time.

Selective Availability and Anti-Spoofing (1990s-2000s)

- Selective Availability Anti-Spoofing Module (SAASM)

In order to protect military PPS signals and enable secure decryption, SAASM technology was introduced for military receivers. This helped to facilitate encrypted signal access and secure key management [22].

- End of SA (selective availability) for civilians (2000)

As a result of the growing global reliance on GPS for civil and commercial uses, President Bill Clinton ordered SA turned off on May 1, 2000, vastly improving civilian accuracy and solidifying GPS as a global utility rather than a primary military system [23].

- Post-2000 modernization is also focused on anti-spoofing, to make it harder for adversaries to generate fake signals that can mislead receivers [24].

Recognizing GPS Vulnerabilities (2000s-Present)

Signal weakness – GPS signals are extremely weak by the time they reach the earth's surface, making them inherently vulnerable to jamming (blocking signals) and spoofing (broadcasting false signals). Jamming overwhelms GPS receivers with strong interference, stopping normal navigation. GNSS jamming is now widely documented, including in civil aviation and conflict zones [25, 26]. Spoofing is the transmission of counterfeit GPS signals to deceive receivers into computing incorrect locations or times, which is very dangerous as receivers may not detect it reliably [25]. Hence the need for both civilian and military GPS receivers to have enhanced signal authentication and spoof protection mechanism, and as well as advanced receiver designs and cryptographic techniques for secure signal verification [27], as shown in Figure 5.

Modern GPS Security

- The use of modern GPS lll program which started around 2018 introduces signals with better anti-jam capabilities, higher power, and improved security features. These include authenticated military codes like M-code, which is a newer encrypted military signal designed to – improve anti-jamming resistance, allow standalone acquisition (no need to rely on civilian codes), and increase secure cryptographic flexibility and key management [28, 29].
- Development of civil signal authentication technologies to detect spoofing [24].
- In order to combat GPS signal threats, modern navigation solutions are integrating inertial navigation systems (INS), multiple GNSS systems (using GPS + Galileo + GLONASS + BeiDou), advanced detection methods, and frequencies to increase resilience, such that if one signal is jammed or spoofed, others may still be valid [25, 30, 31], as shown in figure 6.

Emerging Threats: Jamming and Spoofing (2010s-today)

As GPS became essential to civilian infrastructure (aviation, telecom, shipping), security threats are expanding beyond military concerns:

Jamming

- Intentional interference can block or degrade GPS reception.

- Simple jamming can overpower the weak GPS signals received on Earth, making navigation impossible [32].

Spoofing

- Spoofing is the broadcasting of counterfeit GPS signals to deceive receivers into computing incorrect locations/times.
- Vulnerabilities became widely recognized after real-world incidents – including the 2011 capture of a U. S. drone by Iran by spoofing its GPS navigation [33].
- GPS jamming and spoofing are now part of electronic warfare strategies in conflict zones, used to disrupt both military and civilian operations (e.g., aviation over Eastern Europe) [34].

Due to the fact that civilian GPS lacks intrinsic authentication (unlike encrypted military signals), there is much focus on detecting spoofing and building countermeasures such as:

- Signal authentication by adding cryptographic authentication to detect fake signals [27].
- Receiver-side defenses – techniques like power-distortion monitoring and machine learning aimed to distinguish real satellite signals from spoofed ones [35].

Signal Weakness

GPS signals are weak and vulnerable to interference.

Lack of Authentication

Civilian GPS signals lack authentication, thereby making them susceptible to spoofing.

Complexity of Systems

The integration with other systems increases the vulnerability to cyber threats [36-40].

SOLUTIONS TO GPS SECURITY CHALLENGES

Some of the solutions to GPS security would include [36-40]:

- Anti-jamming techniques: This is by the use of antennas and receivers that filter or nullify jamming signals.
- Signal authentication: Implement cryptographic checks (e.g., military P(Y) code) to verify signal authenticity. Use of techniques such as RAIM (Receiver Autonomous Integrity Monitoring) to detect anomalies.
- Spoofing detection: Monitor signal anomalies and use multi-constellation GNSS (e.g., GPS + Galileo + GLONASS) for cross-validation and to improve resilience.
- Encryption: Modernized GPS signals (e.g., L1C, L2C, L5) use encryption to prevent spoofing.
- Multi-sensor integration: Combine GPS with inertial navigation or other sensors for redundancy.

CONCLUSION

GPS security is critical for protecting navigation, timing, and critical infrastructure. Some of the key challenges include jamming, spoofing, and signal vulnerability due to weak, open, and unencrypted civilian signals. These vulnerabilities can lead to serious consequences, including navigation errors, service disruptions, and risks to safety and national security. There is therefore need for improving GPS security via stronger signal protection, anti-jamming techniques, signal authentication, system integration, and multi-constellation to enhance reliable, secure operation and to help mitigate risks. More information on GPS Security can be obtained from the books in [41-45] and the following related journals:

- Journal of the Institute of Navigation
- IEEE Transactions on Aerospace and Electronic Systems
- Sensors/IEEE Sensors Journal
- ISPRS Journal of Photogrammetry and Remote Sensing
- GIScience & Remote Sensing
- Remote Sensing (MDPI)
- Journal of Reliable and Secure Computing
- Cybersecurity/Communications Journals

REFERENCES

[1] United States Department of Defense (September 2008), "Global Positioning System Standard Positioning Service Performance Standard," (PDF) (4th ed.). Retrieved April 21, 2017.

[2] "GPS-NASA," Retrieved January 5, 2025.

[3] K. Raza (October 16, 2020), *Computational intelligence methods in COVID-19: Surveillance, prevention, prediction and diagnosis,* Springer Nature, p. 114.

[4] National Coordination Office for Space-Based Positioning, Navigation, and Timing (February 22, 2021), "What is GPS?" Retrieved May 5, 2021.

[5] "Global Positioning System," Wikipedia, the free encyclopedia, https://en.wikipedia.org/global- positioning-system

[6] *The global positioning system: a shared national asset: recommendations for technical improvements and enhancements,* National Academies Press, p. 16. Retrieved August 16, 2013.

[7] A. Darrin & B. L. O'Leary (June 26, 2009), *Handbook of space engineering, archaeology, and heritage,* CRC Press, pp. 239-240. Retrieved July 28, 2021.

[8] A. Butterly (May 20, 2018), "100 women: Gladys West – the 'hidden figure' of GPS," BBC News. Retrieved January 17, 2019.

[9] A. Mohdin (November 19, 2020), "Gladys West: the hidden figure who helped invent GPS," The Guardian. Retrieved November 29, 2023.

[10] "Inside the box: GPS and relativity – GPS World," October 9, 2023. Retrieved 12, 2025.

[11] "The satellite clock l GEOG 862: GPS and GNSS for Geospatial Professionals," www.e-education.psu.edu. Retrieved December 10, 2025.

[12] W. H. Guier & G. C. Weiffenbach (1997), "Genesis of satellite navigation," (PDF), Johns Hopkins APL Technical Digest, vol. 19, no.1, pp. 178-181. Retrieved April 9, 2012.

[13] S. Johnson (2010), Where good ideas come from, the natural history of innovation, New York. Riverhead Books.

[14] H. E. Worth & M. Warren (2009), *Transit to tomorrow – Fifty years of space research at the Johns Hopkins University Applied Physics Laboratory*, (PDF). Retrieved March 3, 2013.

[15] C. Alexandrow (April 2008), "The story of GPS."

[16] *DARPA: 50 years of bridging the gap* (April 2008).

[17] E. Howell, "Navstar: GPS satellite network." SPACE.com. Retrieved February 14, 2013.

[18] "NRL launched first time-based navigation satellite in 1967," *U.S. Naval Research Laboratory*. Retrieved January 5, 2025.

[19] "Arms Race and Cold War – UPSC Notes >> LotusArise." Retrieved December 10, 2025.

[20] "Arms Race: Definition, Cold War & Nuclear Arms*," History.com*. Retrieved December 10, 2025.

[21] "U.S. Nuclear Weapons: Changes in policy and force structure," www.everycrsreport.com. Retrieved December 10, 2025.

[22] "Selective availability anti-spoofing module," Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/selective-availability-anti-spoofing-module

[23] "Selective Availability," https://www.gps.gov/selective-availability

[24] B. Parkinson (August 25, 2009), "Signal authentication – Inside GNSS – Global Navigation Satellite," https://www.insidegnss.com/signal-authentication

[25] S. Cole (November 30, 2015), "Securing military GPS from spoofing and jamming vulnerabilities," https://www.militaryembedded.com

[26] "GNSS jamming," Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/GNSS-jamming

[27] K. Wesson, M. Rothlisberger and T. Humphreys, "Practical cryptographic civil GPS signal authentication," nma.pdf, *The Journal of the Institute of Navigation*, February 2012.

[28] "Global positioning system," https://www.grokipedia.com/page/Global-positioning-system

[29] B. C. Baker et al., "Overview of the GPS M Code signal – Mitre."

[30] K. Koril & V. Kumare, "Cyber security in satellite navigation system," *International Journal for Research Trends and Innovation* (IJRTI), vol. 10, no. 3, March 2025.

[31] S. Maria Simsky, "Why secure GPS receivers are crucial for GNSS/INS systems?" https://journals.cices.org/ces/

[32] U.S. Government Accountability Office (GOA) (January 19, 2021), "GPS Modernization: DOD continuing to develop new jam-resistant capability, but widespread use remains years away." https://www.gao.gov/products/gsp-modernization

[33] M. L. Psiaki & T. E. Humphreys (29 July 2016), "Protecting GPS from spoofers is critical to the future of navigation – IEEE Spectrum," https://www.spectrum.ieee.org/protecting-gps

[34] C. Davenport (December 31, 2025), "GPS is key to the global economy. It's also surprisingly easy to attack," https://www.washingtonpost.com

[35] K. D. Wesson et al. (27 March 2020), "GNSS signal authentication via power and distortion

monitoring," (PDF), https://www.arxiv.org/abs/gnss-signal-authentication

[36] "Memorandum on Space Policy Directive 7," January 15, 2021 https://www.gps.gov

[37] A. Altaweel, H. Mukkath and I. Kamel, "GPS spoofing attacks in FANERTs: A systematic literature review," in IEEE Access, vol. 11, pp. 55233-55280, 2023, https://www.ieeexplore.ieee.org

[38] "NIST finalizes cybersecurity guidance for Positioning, Navigation and Timing Systems," https://www.nist.gov/nist-finalizes-cybersecurity-guidance-for-positioning-navigation-and-timing-systems

[39] L. He, W Li, C. Guo and R. Niu, "Civilian unmanned aerial vehicle vulnerability to GPS spoofing attacks," *2014 Seventh International Symposium on Computational Intelligence and design*, Hangzhou, China, 2014, pp. 212-215.

[40] "Category: GPS modernization," https://www.space.commerce.gov/category-gps-modernization

[41] L. Scott (January 2003), "Anti-spoofing & authenticated signal architectures for civil navigation systems," (PDF), Conference: ION GPS/GNSS 2003, 9-12 September 2003, Portland, Oregon.

[42] E. D. Kaplan & C. Hegarty, "*Understanding GPS/GNSS: Principles and applications*." 3rd Edition – NavtechGPS.

[43] J. G. Teunissen & O. Montenbruck (eds.), "*Springer Handbook of Global Navigation Satellite Systems l springer Nature Link.*"

[44] Y. T. Jade Morton et al. (eds.), "*Position, Navigation, and Timing Technologies in the 21st Century*."

[45] G. P. Petropoulos and P. K. Srivastava (eds.), "*GPS and GNSS Technology in Geosciences*."

Figure 1. Global Positioning System
Source:https://en.wikipedia.org/wiki/Global_Positioning_System

Figure 2. Geopositioning
Source:
https://en.wikipedia.org/wiki/Geopositioning

Figure 3. GPS tracking unit
Source:
https://en.wikipedia.org/wiki/GPS_tracking_unit

Figure 4. Satellite navigation device
Source:
https://en.wikipedia.org/wiki/Satellite_navigation_device

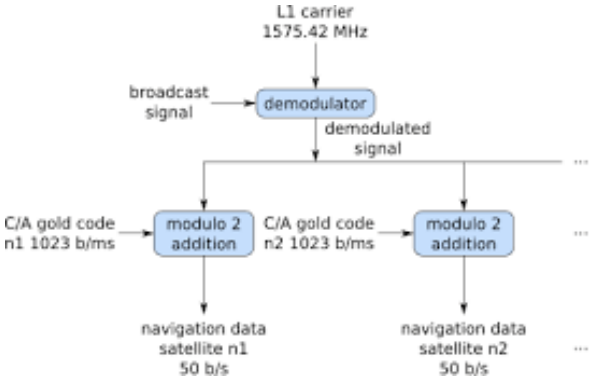

Figure 5. GPS signals

Source: https://en.wikipedia.org/wiki/GPS_signals

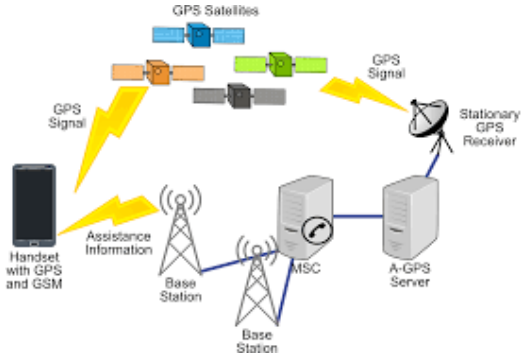

Figure 6. Assisted GNSS

Source:

https://en.wikipedia.org/wiki/Assisted_GNSS