Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Comparative Study on GPS Navigation Systems: Attacks, Applications and Challenges for Security and Reliability

Cynthia J[1], Dr. S. Rathi[2]

[1]Research Scholar, Department of Computer Science and Engineering, Government College of Technology, India
[2]Professor, Department of Computer Science and Engineering, Government College of Technology, India
Email: cynthia.phd@gct.ac.in

GPS navigation devices are widely used for location and timing data but are vulnerable to attacks including spoofing, jamming and meaconing. This survey examines these attacks and explores enhancements such as differential GPS and multi-sensor integration. Challenges include security, authentication, encryption and the impact of multiple GNSS constellations. Applications that make use of many constellations and different GPS are highlighted in the paper. Future directions require consistent research and development to increase security and reliability. The paper enhance novel approaches for GPS system safety and dependability and provides a roadmap for future research. This survey acts as an outline for scholars and researchers interested in GPS navigation security.

Keywords: GPS navigation attacks, spoofing, jamming, meaconing, multi-sensor integration, security, authentication, encryption, GNSS constellations, reliability, safety.

1. Introduction

The NAVSTAR Global Positioning System (GPS), as described by Bradford et al. [1] is one of the military projects that gave rise to GPS navigation systems and has a long history. From its inception as a tool for the military, GPS has become a globally recognised technology for civilian use [2]. Global Navigation Satellite Systems (GNSS) such as GPS, GLONASS, Galileo, and BeiDou are currently in service, demonstrating the advancement of GPS technology over time [3]. From driving to aircraft, these technologies have revolutionised navigation in many domains.

According to Eric et al. [4], GPS receivers use trilateration to deduce location after receiving signals from orbiting satellites. But spoofing, jamming, and replay attacks are only a few of

the vulnerabilities that affect GPS systems [5][6]. Such vulnerabilities pose risks across numerous sectors necessitating a thorough exploration of attack types, advancements and challenges in GPS navigation security and reliability,

In this survey, our main objective is to:

1. Identify different attack types targeting GPS navigation systems.
2. Explore advancements and applications enhancing GPS navigation.
3. Address challenges to bolster GPS navigation security and reliability.

We can develop effective approaches to protect and improve GPS by having an in-depth understanding of its environment.

2. Related Works:

Recent research has extensively explored the vulnerabilities and attacks targeting GPS navigation systems, as described in Table 1. Cui et al. [7] examine safety and security challenges confronting autonomous vehicles (AVs), identifying unresolved issues and future research directions. Chowdhury et al. [8] stress the importance of addressing security challenges in self-driving cars and intelligent transportation systems (ITS), proposing countermeasures and emphasizing the need for continuous security research. Khan et al. [9] provide a comprehensive review of GPS spoofing attacks, categorizing techniques and discussing experiments on GPS-reliant mobile platforms. Riahi et al. [10] discuss vulnerabilities and cyber-attacks on Unmanned Aerial Systems (UAS), highlighting detection techniques and stressing the importance of cybersecurity. Meng et al. [11] highlights the significance of anti-spoofing technology in satellite navigation systems proposing a new classification and assessing existing detection methods, challenges and adaptability. Jeong et al. [12] analyse technology and implementation patterns while analysing recent research on standardization initiatives, protocols, applications and security in smart transportation systems.

Table 1: Summary of Existing surveys related to GPS attacks.

Publisher	Summary	Scope
Chowdhury et al.,[8] 2020	This paper examines cyber-attacks on self-driving cars and provides guidance for future research.	Developing more effective intrusion detection and prevention systems, designing secure communication protocols, developing more secure and reliable software, investigating cyber-attacks on physical components and investigating legal and ethical implications.
Cui et al.,[7] 2019	AV safety and security must be addressed to avoid accidents, with available safety and security remedies.	Developing more effective intrusion detection and prevention systems, designing secure communication protocols, building more secure software, investigating cyber-attacks on physical components and analysing legal and ethical implications.
Cao et al.,[13] 2019	This paper examines the security risks of GPS signal attacks in road navigation, as well as the limitations of current GPS security measures.	Future work will focus on developing highly robust security solutions, identifying potential vulnerabilities, researching GPS signal attacks, exploring alternate positioning technologies and conducting real-world experiments.

Khan et al.,[9] 2021	The primary goal of this study is to increase awareness of GPS spoofing attacks and the significance of safe and reliable UAV operations.	UAVs need GPS receivers, multiple sensors, cryptographic techniques, machine learning and artificial intelligence, and regulatory frameworks.
Haider et al.,[14] 2016	This survey outlines methods to protect civilian GPS receivers from spoofing threats. It enhances the most effective countermeasures by examining combinations of strategies and analysing various alternatives. The study aims to increase public awareness about GPS vulnerabilities and the necessity for robust defences against spoofing attacks.	The paper suggests combining techniques to improve GPS receiver security, but does not specify future works.
Meng et al.,[11] 2022	Proposes a new classification standard for anti-spoofing technology and examines the difficulty, impact, and adaptability of current detection methods.	Provide a reference for future research and contribute to the field of navigation technology
Jeong et al.,[12] 2021	This paper provides an overview of the present state of research on safe and efficient driving in intelligent transportation systems with a focus on systems, protocols, applications and security, especially for autonomous vehicles. It emphasises the importance of international cooperation and standards in order to build smart transportation systems and protocols.	Secure communication protocols, improved road surface monitoring, autonomous driving systems, and cybersecurity measures to protect smart transportation systems from cyber-attacks.

3. Types of GPS Navigation System Attacks:

3.1 SPOOFING ATTACK:

GPS spoofing, a cyber-attack altering GPS signals to mislead receivers is a serious threat in aviation, transportation and military operations, Mohsen et al.,[15]. In Figure 1, the normal route follows accurate GPS signals, while the spoofed route deviates due to manipulated signals, potentially causing hazards. To counter this, researchers propose employing supervised machine learning like artificial neural networks for detecting spoofing signals.

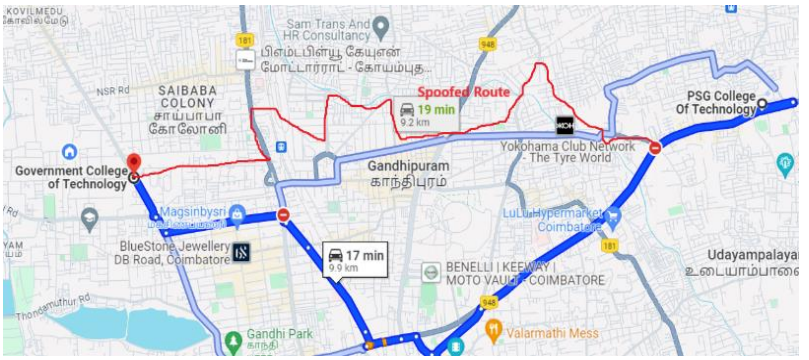

Fig 1: Navigation path of Normal and Spoofed routes

Current anti-spoofing methods include receiver-based techniques analyzing signal structure and behavior according to Shafiee et al.,[16]. Elements like early-late phase, delta and signal level are examined and machine learning algorithms such as K-NN and neural networks are utilized for detection. Simulation results show neural networks offer rapid detection and high accuracy.

As GPS spoofing grows more sophisticated, safeguarding against attacks becomes paramount. Alternative positioning technologies and enhanced cryptographic measures are being explored to fortify GPS security [17], [18]. Continuous research and innovation are vital to counter the evolving threat of GPS spoofing and ensure the integrity of critical infrastructure systems.

3.2 JAMMING ATTACK:

GPS jamming attacks disrupt GPS signals, causing loss of navigation, location, and timing data. Figure 2 represents the navigation path of a normal signal and a lost signal due to a jamming attack. Arjoune et al. [19] define them as high-power signals interfering with GPS receivers on the same frequency band as the network, hindering lawful transmission. These attacks range from simple handheld devices to sophisticated equipment making detection challenging [20]. Countermeasures include GPS signal filters and receivers with multiple antennas to detect and reject jamming signals. However, the evolution of techniques like frequency hopping presents future challenges in combatting GPS jamming. With GPS signals increasingly vital in critical infrastructure, continuous research is essential to address the escalating threat.

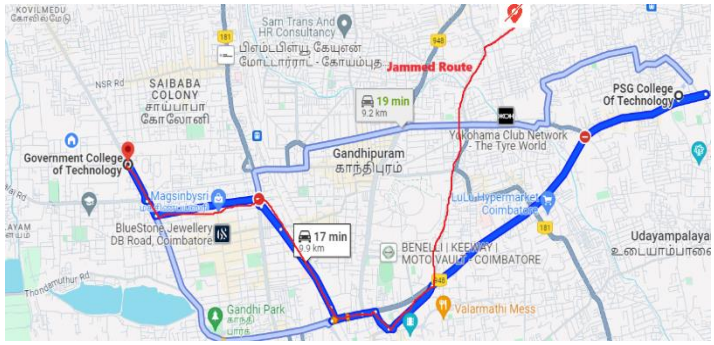

Fig 2: Navigation path of Normal and Lost signal due to jamming attack

3.3 MEACONING ATTACK:

GPS meaconing involves intercepting and rebroadcasting GPS signals to deceive receivers into believing they are genuine. Figure 3 illustrates the navigation path of normal and replayed signals due to a meaconing attack. Khan et al. [9] explain how hackers manipulate GPS receivers with fake signals. Sriramya et al. [21] propose a GPS time authentication algorithm to detect such attacks using static receiver networks. Techniques like signal processing and cryptographic methods as suggested by Michel et al., [22] prevent meaconing by canceling spoofed signals and adding digital signatures. Detection software and advanced security protocols are deployed to combat meaconing, with military and government agencies taking proactive measures.

Fig 3: Navigation path of Normal and Replay signals due to Meaconing attack

Future challenges lie in securing critical infrastructure and countering evolving attack methods, necessitating international collaboration and standardization of security protocols, as proposed by Jeong et al. [12].

4. Countermeasures Against GPS Attacks:

Countermeasures against GPS attacks like spoofing attack, jamming attack and meaconing attack is essential to be mitigated to ensure the accuracy and reliability of GPS based navigation system as depicted in Figure 4.

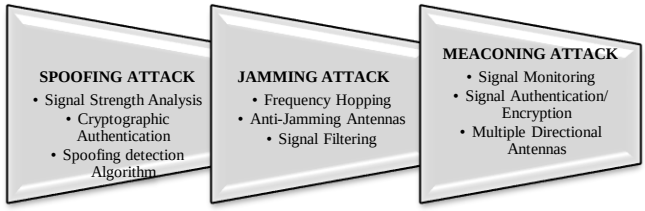

Fig 4: Countermeasures on Various GPS Attacks

4.1. Countermeasure for GPS Spoofing Attack:

Countermeasures against GPS spoofing encompass signal strength analysis, cryptographic authentication and spoofing detection algorithms. Quan et al. [23] propose a machine learning approach analyzing received signal strength to detect spoofing attacks. Cryptographic techniques, as described by Mukhtar et al. [24], provide secure solutions against spoofing, along with advanced signal processing and multi-antenna arrays. Ghorbani et al. [25] advocate for one-way encryption chains to validate GPS data, offering improved security compared to traditional methods. Spoofing detection algorithms, such as Wang et al.[26] Long Short-Term Memory model and Meng et al.[27] Drone Sensor Spoofing Detection utilize statistical analysis and machine learning to identify and reject spoofed GPS signals. These countermeasures enhance GPS security by analyzing signal characteristics and detecting anomalous patterns, safeguarding against potential spoofing attacks.

4.2. Countermeasure for GPS Jamming Attack:

Countermeasures against GPS jamming encompass frequency hopping, anti-jamming antennas, and signal filtering techniques. Zeng et al. [28] explain frequency hopping as rapidly changing a signal's carrier frequency, making it challenging for attackers to interfere. Kasturi et al. [29] propose a technique based on machine learning for detecting jamming attacks, even amidst frequency hopping. According to Chehemi et al.[30], Anti-jamming antennas reduces the jamming signals while enhancing GPS signals with various antenna array configurations to optimize performance. Signal filtering as suggested by Wang et al. [31], employs techniques like adaptive extended Kalman filtering to improve the connected vehicles safety and security by removing jamming signals. These countermeasures enhance GPS resilience against jamming attacks by dynamically adjusting frequencies, optimizing antenna configurations and filtering out interference.

4.3. Countermeasure for GPS Meaconing Attack:

Countermeasures against GPS jamming attacks include signal monitoring, authentication/encryption and multiple directional antennas. Jeong et al. [32] focus on real-time monitoring of GNSS signals to enhance spoofing detection and lower false alarms. Signal authentication as proposed by Chu et al. [33], verifies GPS signal integrity using cryptographic techniques like Chameleon Hash Keychain and HMAC that prevents attackers from creating false signals[39] and securing against meaconing attacks. Multiple directional antennas promoted by Bhamidipati et al. [34] analyze signal data to detect irregularities indicating a meaconing attack. These countermeasures bolster GPS security by monitoring signals, authenticating data, and enhancing detection capabilities against spoofing and meaconing threats.

Table 2: Survey on types of attack, Countermeasures, technology used and Detection rate

Publisher	Attack Type	Countermeasure type	Methodology	Detection Accuracy
Youness et al.,[19] 2020	Jamming Attack	Anti-jamming algorithm using signal strength analysis	Machine Learning technique like RF,SVM and NN	99%
Quan et al., [23] 2021	Spoofing Attack	Signal Strength Analysis	An OSVM classifier for identifying cross-technology communication (CTC) spoofing attacks is built by modelling the RSS data of legitimate ZigBee device	Accuracy and Detection rate are both above 90%.
Bada et al.,[35] 2021	Spoofing attack	Signal strength analysis using absolute power and carrier to noise ratio	Signal strength analysis and trust model like beta and weilbull distribution.	High Accuracy rate
Ghorbani et al., [25] 2020	Spoofing Attack	Cryptographic Authentication	Based on Navigation Message Authentication (NMA), Timed Efficient Stream Loss-tolerant Authentication (TESLA). The TESLA algorithm receives the extracted	Examines the security and efficacy of the proposed approach in comparison to the Elliptic Curve Digital Signature Algorithm (ECDSA).

			navigation data from the GPS L1C/A.	
Jansen et al.,[36] 2018	Spoofing Attack	Cryptographic Authentication	Crowd-GPS-Sec	After 15 minutes of monitoring, it detects an attacker in less than 2 seconds and can pinpoint their location to within 150 metres.
Schmidt et al.,[37] 2020	Spoofing Attack	primarily makes use of the correlator tap output of the incoming signal and Signal Strength Analysis	Least Absolute Shrinkage and Selection Operator(LASSO) with Single Antenna Receiver	0.3% detection error rate in the signal-to-noise ratio (SNR)
Kim et al.,[34] 2019	Spoofing Attack	Spoofing detection Algorithm	Combination of Belief Propagation (BP) based Extended Kalman Filter with Distributed Multiple Directional Antenna (EKF)	Increased voltage stability by using evaluation metric called voltage stability index
Wang et al.,[26] 2020	Spoofing Attack	Spoofing Detection Algorithm	Machine Learning called LSTM(Long Short Term Memory)	GPS position accuracy when using the civil code (C/A code), which is neither encrypted nor authenticated. The precision of the C/A code pseudo-range is around 20 metres.
Meng et al.,[27] 2020	Spoofing Attack	Spoofing Detection Algorithm	SSDGOF is a GPS and optical flow fusion-based technique for detecting drone sensor mimicking.	Algorithm is more efficient than other methods
Yuchen et al.,[38] 2022	Jamming Attack	Anti-Jamming Algorithm	Detecting and classifying using OFDM receiver has 2 approaches Feature based model uses machine learning algorithm. Spectrogram based model uses CNN	Detection accuracy of Spectrogram based model is 99.79% and Feature based model is 92.20%
Kasturi et al.,[29] 2020	Jamming Attack	Frequency Hopping	When compared to other algorithms, such as Decision Tree, K-Nearest Neighbours (KNN), Support Vector Machine (SVM), and Artificial Neural Network (ANN), Random Forest performs better.	The ability to identify and categorise radio frequency jamming attacks is highly accurate.
Chehemi et al.,[30] 2020	Jamming Attack	Anti-Jamming Antennas	Using a database search, the first technique finds the configuration with the deepest null towards the jammer. Using the second procedure, the configuration with the	Work efficiently compared to other methods

			largest maximum to null ratio is identified. Because it performed better than the Deepest Null searching method, the Max-to-Null Ratio searching strategy was specifically employed for the simulations.	
Wang et al., [31] 2020	Jamming Atack	Signal Filtering	Combines an adaptive extended Kalman filter (AEKF) with a trained One Class Support Vector Machine (OCSVM) model for anomaly identification to locate anomalies in the sensor data.	Better Accuracy
Jeong et al.,[32] 2020	Meaconing Attack	Signal Monitoring	Different kinds of spoofing detection techniques used for monitoring the signals of global positioning systems (GNSS)	Improve spoofing detection performance and lower the false alarm rate.
Zhu et al.,[39] 2022	Meaconing Attack	Detection Algorithm	Enhanced radio in conjunction with C/No-MV, or carrier noise moving variation	98%
Manesh et al., [15] 2019	Meaconing Attack	Signal Monitoring	Artificial neural network-based supervised machine learning with features like Doppler shift, pseudo range and signal to noise ratio (SNR)	ROC Curve metric shows the proposed method outperforms all signal processing techniques
Chu et al., [33] 2022	Meaconing Attack	Signal Authentication/ Encryption	By generating a Chameleon Hash Keychain and creating a new hash key every 30 seconds, GPS navigational message verification makes it more difficult for attackers to fake GPS signals.	Attackers will find it more difficult to interfere with navigational signals if GPS message subframes are protected with a distinctive hash key.
Bhamidipati et al., [34] 2019	Meaconing Attack	Multiple Directional Antennas	In power distribution systems, timing problems resulting from GPS spoofing were found and fixed using the Extended Kalman Filter (EKF) technique.	The BP-EKF algorithm complies with IEEE-C37.118 standards by accurately estimating GPS timing and detecting meaconing attacks.

5. Future Direction and Conclusion

The evolution of GPS technology is poised to tackle emerging challenges and fortify against threats. Quantum Positioning Systems (QPS) [40] represent a promising frontier, offering unparalleled precision and security through the integration of quantum optics and

cryptography. Multi-constellation systems [41] leverage redundant satellite signals to enhance accuracy and resilience against disruptions. Augmentation systems [42]bolster precision and defense against attacks, though they require robust security measures to safeguard against vulnerabilities.

In conclusion, GPS navigation systems face diverse threats, including spoofing, jamming, and meaconing attacks, with potentially severe consequences. Countermeasures such as anti-jamming systems, differential GPS, and signal authentication techniques have been developed to enhance GPS reliability and security. However, challenges persist, necessitating stronger security protocols, improved authentication methods, and greater collaboration among GPS providers to ensure signal integrity. Research and development efforts must prioritize the creation of more resilient and secure GPS systems capable of withstanding various forms of attacks and natural disasters. By implementing advanced anti-jamming systems, authentication protocols, and encryption techniques, GPS vulnerabilities can be mitigated, bolstering system resilience. Public awareness campaigns are crucial to emphasise the value of GPS security and the necessity for protective measures.

DECLARATION:

Competing Interests:

This paper has been approved by co-author. The authors have disclosed no competing interests regarding the content of this article

Author's Contributions:

All authors contributed equally to the writing of this paper. Cynthia J is a Research Scholar who developed the research question and hypothesis, conducted the literature review, designed the study protocol, collected the data, analyzed and interpreted the results and wrote the main manuscript text. Dr. S. Rathi is a Professor who provided guidance and mentorship throughout the work, assisted with data collection by providing access and helping to develop data collection tools and aided in data analysis by providing feedback on the analysis plan and helping to interpret the results.

Funding:

This work was not supported by any external funding.

Availability of data:

The data and material used in this study are not publicly available but are available upon request from the corresponding author. Interested researcher can contact cynthia.phd@gct.ac.in for access to the data.

References

1. T. H. E. Ieee, "NAVSTAR : Global Positioning System-Ten," vol. 71, no. 10, pp. 1177–1186, 1983.
2. B. Parkinson, K. Gromov, T. Stansell, and R. Beard, "History of Satellite Navigation," Proc. Annu. Meet. - Inst. Navig., pp. 17–65, 1995.
3. N. Bonnor, "A brief history of global navigation satellite systems," J. Navig., vol. 65, no. 1, pp.

1–14, 2012, doi: 10.1017/S0373463311000506.
4. E. Abbott and D. Powell, "Land-vehicle navigation using GPS," Proc. IEEE, vol. 87, no. 1, pp. 145–162, 1999, doi: 10.1109/5.736347.
5. T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," Proc. ACM Conf. Comput. Commun. Secur., pp. 450–461, 2012, doi: 10.1145/2382196.2382245.
6. A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global Positioning System," IEEE Trans. Ind. Electron., vol. 65, no. 8, pp. 6425–6435, 2018, doi: 10.1109/TIE.2017.2787581.
7. J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," Ad Hoc Networks, vol. 90, 2019, doi: 10.1016/j.adhoc.2018.12.006.
8. A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," IEEE Access, vol. 8, pp. 207308–207342, 2020, doi: 10.1109/ACCESS.2020.3037705.
9. S. Z. Khan, M. Mohsin, and W. Iqbal, "On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions," PeerJ Comput. Sci., vol. 7, pp. 1–35, 2021, doi: 10.7717/PEERJ-CS.507.
10. M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," Comput. Secur., vol. 85, pp. 386–401, 2019, doi: 10.1016/j.cose.2019.05.003.
11. L. Meng, L. Yang, W. Yang, and L. Zhang, "A Survey of GNSS Spoofing and Anti-Spoofing Technology," Remote Sens., vol. 14, no. 19, pp. 1–24, 2022, doi: 10.3390/rs14194826.
12. H. (Harrison) Jeong, Y. (Chris) Shen, J. (Paul) Jeong, and T. (Tom) Oh, "A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications," Veh. Commun., vol. 31, p. 100349, 2021, doi: 10.1016/j.vehcom.2021.100349.
13. Y. Cao, Q. Luo, and J. Liu, "Road Navigation System Attacks: A Case on GPS Navigation Map," IEEE Int. Conf. Commun., vol. 2019-May, pp. 1–5, 2019, doi: 10.1109/ICC.2019.8761439.
14. Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," 2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016, vol. 7, no. 4, pp. 573–577, 2017, doi: 10.1109/INTECH.2016.7845038.
15. M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," 2019 16th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2019, no. July 2020, 2019, doi: 10.1109/CCNC.2019.8651804.
16. E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," J. Navig., vol. 71, no. 1, pp. 169–188, 2018, doi: 10.1017/S0373463317000558.
17. E. Ranyal and K. Jain, "Unmanned Aerial Vehicle's Vulnerability to GPS Spoofing a Review," J. Indian Soc. Remote Sens., vol. 49, no. 3, pp. 585–591, 2021, doi: 10.1007/s12524-020-01225-1.
18. Y. Tian, N. Zheng, X. Chen, and L. Gao, "Wasserstein Metric-Based Location Spoofing Attack Detection in WiFi Positioning Systems," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/8817569.
19. Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," Int. Conf. Inf. Netw., vol. 2020-Janua, pp. 459–464, 2020, doi: 10.1109/ICOIN48656.2020.9016462.
20. R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms," Wirel. Pers. Commun., vol. 115, no. 4, pp. 2705–2727, 2020, doi: 10.1007/s11277-020-07212-6.

21. S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," 2018 IEEE/ION Position, Locat. Navig. Symp. PLANS 2018 - Proc., pp. 1485–1491, 2018, doi: 10.1109/PLANS.2018.8373542.
22. J. Jetto, R. Gandhiraj, G.A.Shanmugha Sundaram and K. P. Soman, "Software Defined Radio-Based GPS Spoofing Attack Model on Road Navigation System," pp. 339–350, 2022, doi: 10.1007/978-981-16-1249-7_32.
23. Q. Sun, X. Miao, Z. Guan, J. Wang, and D. Gao, "Spoofing Attack Detection Using Machine Learning in Cross-Technology Communication," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/3314595.
24. M. Ahmad, M. A. Farid, and S. Ahmed, "Countermeasures against Spoofing," 2019 2nd Int. Conf. Comput. Math. Eng. Technol., no. February, pp. 1–8, 2019.
25. K. Ghorbani, N. Orouji, and M. R. Mosavi, "Navigation Message Authentication Based on One-Way Hash Chain to Mitigate Spoofing Attacks for GPS L1," Wirel. Pers. Commun., vol. 113, no. 4, pp. 1743–1754, 2020, doi: 10.1007/s11277-020-07289-z.
26. S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent detection algorithm against Uavs' GPS spoofing attack," Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS, vol. 2020-Decem, pp. 382–389, 2020, doi: 10.1109/ICPADS51040.2020.00058.
27. L. Meng, S. Ren, G. Tang, C. Yang, and W. Yang, "UAV sensor spoofing detection algorithm based on GPS and optical flow fusion," ACM Int. Conf. Proceeding Ser., pp. 146–151, 2020, doi: 10.1145/3377644.3377670.
28. H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," IEEE Commun. Surv. Tutorials, vol. 24, no. 2, pp. 767–809, 2022, doi: 10.1109/COMST.2022.3159185.
29. G. S. Kasturi, A. Jain, and J. Singh, "Detection and classification of radio frequency Jamming attacks using machine learning," J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl., vol. 11, no. 4, pp. 49–62, 2020, doi: 10.22667/JOWUA.2020.12.31.049.
30. M. Chehimi, E. Yaacoub, A. Chehab, and M. Al-Husseini, "Physical Layer Anti-jamming Technique Using Massive Planar Antenna Arrays," 2020 Int. Wirel. Commun. Mob. Comput. IWCMC 2020, pp. 1740–1745, 2020, doi: 10.1109/IWCMC48107.2020.9148405.
31. Y. Wang, N. Masoud, and A. Khojandi, "Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1411–1421, 2021, doi: 10.1109/TITS.2020.2970295.
32. S. Jeong and J. Lee, "Synthesis Algorithm for Effective Detection of GNSS Spoofing Attacks," Int. J. Aeronaut. Sp. Sci., vol. 21, no. 1, pp. 251–264, 2020, doi: 10.1007/s42405-019-00197-y.
33. P. Xv, "Signal Authentication Using a Chameleon Hash Keychain . In : Critical Infrastructure There may be differences between this version and the published version . You are Deposited on : 18 January 2022 Enlighten – Research publications by members of the Unive," vol. 9783030935, no. January, pp. 209–226, 2022, doi: 10.1007/978-3-030-93511-5.
34. S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "GPS Spoofing Detection and Mitigation in PMUs using Distributed Multiple Directional Antennas," IEEE Int. Conf. Commun., vol. 2019-May, 2019, doi: 10.1109/ICC.2019.8761208.
35. M. Bada, D. E. Boubiche, N. Lagraa, C. A. Kerrache, M. Imran, and M. Shoaib, "A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs," Transp. Res. Part A Policy Pract., vol. 149, no. May, pp. 300–318, 2021, doi: 10.1016/j.tra.2021.04.022.
36. K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks," Proc. - IEEE Symp. Secur. Priv., vol. 2018-May, pp. 1018–1031, 2018, doi: 10.1109/SP.2018.00012.
37. E. Schmidt, N. Gatsis, and D. Akopian, "A GPS Spoofing Detection and Classification Correlator-Based Technique Using the LASSO," IEEE Trans. Aerosp. Electron. Syst., vol. 56, no. 6, pp. 4224–4237, 2020, doi: 10.1109/TAES.2020.2990149.

38. Y. Li et al., "Jamming Detection and Classification in OFDM-Based UAVs via Feature- and Spectrogram-Tailored Machine Learning," IEEE Access, vol. 10, pp. 16859–16870, 2022, doi: 10.1109/ACCESS.2022.3150020.
39. X. Zhu, Z. Lu, T. Hua, F. Yang, G. Tu, and X. Chen, "A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance," Electron., vol. 11, no. 5, 2022, doi: 10.3390/electronics11050738.
40. S. Duan, S. Cong, and Y. Song, "A survey on quantum positioning system," Int. J. Model. Simul., vol. 41, no. 4, pp. 265–283, 2021, doi: 10.1080/02286203.2020.1738035.
41. D. Medina, K. Gibson, R. Ziebold, and P. Closas, "Determination of pseudorange error models and multipath characterization under signal-degraded scenarios," Proc. 31st Int. Tech. Meet. Satell. Div. Inst. Navig. ION GNSS+ 2018, pp. 3446–3456, 2018, doi: 10.33012/2018.16094.
42. V. Dissanayake, "A review of Cyber security risks in an Augmented reality world," Https://Virajdissanayake.Blogspot.Com/2019/02/a-Review-of-Cyber-Security-Risks-in.Html?M=1, no. March, p. 8, 2020, [Online]. Available: https://www.researchgate.net/publication/339941469_A_review_of_Cyber_security_risks_in_an_Augmented_reality_world