Chapter 3

Global Navigation Satellite Systems for Logistics

Cybersecurity Issues and Challenges

Noor Zaman Jhanjhi, Loveleen Gaur, Navid Ali Khan

Book Editor(s):Imdad Ali Shah, Noor Zaman Jhanjhi

First published: 28 June 2024
https://doi.org/10.1002/9781394204472.ch3

Summary

The availability of accurate location, navigation, and timing data made possible by Global Navigation Satellite Systems (GNSS) technology has had a profound impact on the logistics industry. They are now crucial to the logistics industry's supply chain management, route optimization, asset protection, and overall operational efficiency. Positioning, navigation, and timing services are made available to customers all around the world thanks to the GNSS networks of satellites. Most people are familiar with the United States Global Positioning System (GPS), the most widely used GNSS. GNSS receivers on the ground may be able to pick up signals that a network of satellites in Earth's orbit sends out. The receivers use the signals to determine their position, velocity, and time, allowing for more precise navigation and timing measures. Transportation, mapping, surveying, and time synchronization are just a few of the many fields where GNSS has become indispensable. The military, police, and emergency services rely on it for navigation and communication as well. Like any other technology dependent on communication and computer systems, GNSS is susceptible to cyberattacks. Navigation, timing, and synchronization are just a few of the many uses for Global Navigation Satellite Systems, including GPS, GLONASS, Galileo, and BeiDou. However, their reliance on wireless signals and computer systems makes them vulnerable to cyberattacks. GNSS system operators have implemented various security measures to address these cybersecurity threats, including encryption of signals, redundancy in the system design, and monitoring for signal anomalies. It is essential to continue improving cybersecurity measures to ensure the reliability and accuracy of GNSS systems. The primary object of this chapter is to measure cybersecurity for Global Navigation Satellite Systems in emerging technologies and provide recommendations to the practitioners, and this study opens doors for new researchers.

Hill , J. 2020 . Maxar Stock Surges on Strong 2Q, Executives Update Legion, Telesat LEO Outlook . *Via Satellite* . Accessed July 2021. **https://www.satellitetoday.com/business/2020/08/06/**

Google Scholar

Huang , W. , B. Männel , A. Brack , and H. Schuh . 2020 . Two Methods to Determine Scale-independent GPS PCOs and GNSS-based Terrestrial Scale: Comparison and Cross-check . *GPS Solutions* **25** (1). doi: 10.1007/s10291-020-01035-5 .

Web of Science® **Google Scholar**

Jewett , R. 2020 . FCC Grants OneWeb Market Access for 2,000-Satellite Constellation . *Via Satellite* . Accessed 10 July 2021. **https://www.satellitetoday.com/broadband/2020/08/26/fcc-grants-oneweb-market-access-for-2000-satellite-constellation/**

Google Scholar

Shah , I. A. , Jhanjhi , N. Z. , Humayun , M. , & Ghosh , U. (2022). Health Care Digital Revolution during COVID-19 . In *How COVID-19 Is Accelerating the Digital Revolution* (pp. 17 - 30). Springer , Cham .

Google Scholar

Manulis , M. , Bridges , C. P. , Harrison , R. , Sekar , V. , & Davis , A. (2021). Cyber security in new space: analysis of threats, key enabling technologies and challenges . *International Journal of Information Security* , **20** , 287 - 311 .

Web of Science® **Google Scholar**

Ujjan , R. M. A. , Taj , I. , & Brohi , S. N. (2022). E-Government Cybersecurity Modeling in the Context of Software-Defined Networks . In *Cybersecurity Measures for E-Government Frameworks* (pp. 1 - 21). IGI Global .

Google Scholar

Manesh , M. R. , & Kaabouch , N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions . *Computers & Security* , **85** , 386 - 401 .

Web of Science® **Google Scholar**

Global .

Google Scholar

Khalil , M. I. , Jhanjhi , N. Z. , Humayun , M. , Sivanesan , S. , Masud , M. , & Hossain , M. S. (2021). Hybrid smart grid with sustainable energy efficient resources for smart cities . *Sustainable Energy Technologies and Assessments* , **46** , 101211 .

Web of Science® Google Scholar

Ujjan , R. M. A. , Pervez , Z. , Dahal , K. , Bashir , A. K. , Mumtaz , R. , & González , J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN . *Future Generation Computer Systems* , **111** , 763 - 779 .

Web of Science® Google Scholar

Kbidy , G. , G. Adamski , and N. May . 2018 . Design Concepts and Challenges for the Iridium NEXT Command and Control System . In *2018 Space Operations Conference* , 2708. Marseille, France , May 28–June 1.

Google Scholar

Li , B. , H. Ge , M. Ge , L. Nie , Y. Shen , and H. Schuh . 2019 . LEO Enhanced Global Navigation Satellite System (Legnss) for Real-time Precise Positioning Services . *Advances in Space Research* **63** (1): 73 - 93 . doi: 10.1016/j.asr.2018.08.017 .

Web of Science® Google Scholar

Li , B. , L. Nie , H. Ge , M. Ge , and L. Yang . 2017 . Precise Orbit Determination of Combined GNSS and LEO Constellations with Regional Ground Stations . In *Proceedings of ION GNSS+ 2017* , 2137 – 2147 . Portland, Oregon , September 25–29.

Google Scholar

Dawson , M. , & Walker , D. (2022). Argument for Improved Security in Local Governments within the Economic Community of West African States . *Cybersecurity Measures for E-Government Frameworks* , 96 - 106 .

Li , X. , F. Ma , X. Li , H. Lv , L. Bian , Z. Jiang , and X. Zhang . 2019b . LEO Constellation-augmented multi-GNSS for Rapid PPP Convergence . *Journal of Geodesy* **93** (5): 749 - 764 . doi: 10.1007/s00190-018-1195-2 .

Web of Science® | Google Scholar

Li , X. , J. Wu , K. Zhang , X. Li , Y. Xiong , and Q. Zhang . 2019c . Real-Time Kinematic Precise Orbit Determination for LEO Satellites Using Zero-differenced Ambiguity Resolution . *Remote Sensing* **11** (23): 2815 . doi: 10.3390/rs11232815 .

Web of Science® | Google Scholar

Lu , J. , G. Zhang , G. Chen , W. Gao , and C. Su . 2020 . Development Status and Prospect of Satellite Navigation System . *Spacecraft Engineering* **04** : 1 - 10 .

Google Scholar

Gaur , L. , Ujjan , R. M. A. , & Hussain , M. (2022). The Influence of Deep Learning in Detecting Cyber Attacks on E-Government Applications . In *Cybersecurity Measures for E-Government Frameworks* (pp. 107 - 122). IGI Global .

Google Scholar

Ma , F. , X. Zhang , X. Li , J. Cheng , F. Guo , J. Hu , and L. Pan . 2020 . Hybrid Constellation Design Using a Genetic Algorithm for a LEO-based Navigation Augmentation System . *GPS Solutions* **24** (2): 1 - 14 . doi: 10.1007/s10291-020-00977-0

Web of Science® | Google Scholar

Su , X. 2017 . Theory and Method Research for Global Real-time Centi-meter Level Navigation System Based on High, Medium and Low Orbit Satellites . PhD diss., Wuhan University .

Google Scholar

Wang , K. , and Ahmed EI-Mowafy . 2021 . LEO Satellite Clock Analysis and Prediction for Positioning Applications . *Geo-spatial Information Science* : 1 - 20 . doi: 10.1080/10095020.2021.1917310 .

A. Almusaylim , Z., Jhanjhi , N. Z. , & Alhumam , A. (2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP . *Sensors* , **20** (21), 5997 .

Web of Science® | Google Scholar

Wang , L. , D. Li , R. Chen , W. Fu , X. Shen , and H. Jiang . 2020 . Low Earth Orbiter (LEO) Navigation Augmentation: Opportunities and Challenges . *Chinese Journal of Engineering Science* **22** : 144 . doi: 10.15302/j-sscae2020.02.018 .

Google Scholar

Wang , L. , R. Chen , B. Xu , X. Zhang , T. Li , and C. Wu . 2019 . " The Challenges of LEO Based Navigation Augmentation System – Lessons Learned from Luojia-1A Satellite ." In *Proceeding: China Satellite Navigation Conference (CSNC) 2019 Proceedings* , 298 - 310 . Beijing, China : Springer Singapore .

Google Scholar

Wang , L. , R. Chen , D. Li , B. Yu , and C. Wu . 2018 . Quality Assessment of the LEO Navigation Augmentation Signals from Luojia-1A Satellite . *Geomatics and Information Science of Wuhan University* **43** : 2191 - 2196 .

Google Scholar

Wu , C. , Y. Shu , G. Wang , and S. Li . 2020 . Design and Performance Evaluation of Tianxiang-1 Navigation Enhancement Signal . *Radio Engineering* **9** : 748 - 753 .

Google Scholar

Jhanjhi , N. Z. , Ahmad , M. , Khan , M. A. , & Hussain , M. (2022). The Impact of Cyber Attacks on E-Governance during the COVID-19 Pandemic . In *Cybersecurity Measures for E-Government Frameworks* (pp. 123 - 140). IGI Global .

Google Scholar

Zhang , C. , J. Jin , L. Kuang , and J. Yan . 2018 . LEO Constellation Design Methodology for Observing Multi-targets . *Astrodynamics* **2** (2): 121 - 131 . doi: 10.1007/s42064-017-0015-4 .

Novatel **https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss** [7] Chen , P. , Y. Yao , Q. Li , and W. Yao . 2017 . " Modeling the Plasmasphere Based on LEO Satellites Onboard GPS Measurements ." *Journal of Geophysical Research: Space Physics* **122** (1): 1221 – 1233 .

Google Scholar

Lu , Y. *Brief Introduction to the GPS and BeiDou Satellite Navigation Systems* . Springer , Singapore , 2021 , pp. 37 - 72 . doi: 10.1007/978-981-16-1075-2_2 .

Google Scholar

Zidan , J. , E. I. Adegoke , E. Kampert , S. A. Birrell , C. R. Ford , and M. D. Higgins . GNSS Vulnerabilities and Existing Solutions: A Review of the Literature . *IEEE Access* , pp. 1 – 1 , Feb. 2020 , doi: 10.1109/access.2020.2973759 .

Web of Science® **Google Scholar**

O'Hanlon , B. W. , M. L. Psiaki , T. E. Humphreys , and J. A. Bhatti . Real-Time Spoofing Detection Using Correlation Between Two Civil GPS Receiver . pp. 3584 - 3590 , Sep. 21, 2012 . **http://www.ion.org/publications/abstract.cfm?jp=p&articleID=10533** . Accessed: Jun. 15, 2021.

Google Scholar

O'Hanlon , B. W. , M. L. Psiaki , T. E. Humphreys , and J. A. Bhatti . Real-Time Spoofing Detection in a Narrow-Band Civil GPS Receiver . pp. 2211 - 2220 , Sep. 24, 2010 . **http://www.ion.org/publications/abstract.cfm?jp=p&articleID=9335** . Accessed: Jun. 15, 2021.

Google Scholar

Shah , I. A. , Sial , Q. , Jhanjhi , N. Z. , & Gaur , L. (2023). Use Cases for Digital Twin . In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 102 - 118). IGI Global .

Google Scholar

Yang , J. , Y. J. Chen , W. Trappe , and J. Cheng . Detection and localization of multiple spoofing attackers in wireless networks . *IEEE Transactions on Parallel and Distributed Systems* , vol. **24** , no. 1 , pp. 44 - 58 , 2013 , doi: 10.1109/TPDS.2012.104 .

Daneshmand , S. , A. Jafarnia-Jahromi , A. Broumandon , and G. Lachapelle . A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array . pp. 1233 - 1243 .

Google Scholar

Hussain , M. , Talpur , M. S. H. , & Humayun , M. (2022). The Consequences of Integrity Attacks on E-Governance: Privacy and Security Violation . In *Cybersecurity Measures for E-Government Frameworks* (pp. 141 - 156). IGI Global .

Google Scholar

Tanıl , C. , P. M. Jimenez , M. Raveloharison , B. Kujur , S. Khanafseh , and B. Pervan . Experimental validation of INS monitor against GNSS spoofing . In *Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation* , ION GNSS+ 2018, Sep. 2018 , pp. 2923 - 2937 . doi: 10.33012/2018.15902 .

Google Scholar

Balakrishnan , S. , Ruskhan , B. , Zhen , L. W. , Huang , T. S. , Soong , W. T. Y. , & Shah , I. A. (2023). Down2Park: Finding New Ways to Park . *Journal of Survey in Fisheries Sciences* , 322 - 338 .

Google Scholar

Tanil , C. , S. Khanafseh , and B. Pervan . An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches . In *29th International Technical Meeting of the Satellite Division of the Institute of Navigation* , ION GNSS 2016, Sep. 2016 , vol. **4** , pp. 2981 - 2990 . doi: 10.33012/2016.14779 .

Google Scholar

Sun , M. , Y. Qin , J. Bao , and X. Yu . GPS Spoofing Detection Based on Decision Fusion with a K-out-of-N Rule . *International Journal of Network Security* , vol. **19** , no. 5 , pp. 670 - 674 , 2017 , doi: 10.6633/IJNS.201709.19(5).03 .

Google Scholar

Chhajed , G. J. , & Garg , B. R. (2022). Applying Decision Tree for Hiding Data in Binary Images for Secure and Secret Information Flow . In *Cybersecurity Measures for E-Government Frameworks* (pp. 175 -

Panice , G. , S. Luongo , G. Gigante , D. Pascarella , C. Di Benedetto , A. Vozella , and A. Pescapè . A SVM-based detection approach for GPS spoofing attacks to UAV . In *2017 23rd International Conference on Automation and Computing (ICAC)* , IEEE , pp. 1 - 11 , IEEE, 2017 . doi: 10.23919/IConAC.2017.8081999 .

Google Scholar

Shah , I. A. , Sial , Q. , Jhanjhi , N. Z. , & Gaur , L. (2023). The Role of the IoT and Digital Twin in the Healthcare Digitalization Process: IoT and Digital Twin in the Healthcare Digitalization Process . In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 20 - 34). IGI Global .

Google Scholar

Borh Borhani-Darian , P. , H. Li , P. Wu , and P., Closas , P. Deep Neural Network Approach to Detect GNSS Spoofing Attacks . In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation* (ION GNSS+ 2020), pp. 3241 - 3252 , 2020 .

Google Scholar

Shafiee , E. , M. R. Mosavi , and M. Moazedi . Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers . *Journal of Navigation* , vol. **71** , no. 1 , pp. 169 - 188 , Jan. 2018 , doi: 10.1017/S0373463317000558 .

Web of Science® **Google Scholar**

Neish , S. Lo , Y. H. Chen , and P. Enge . Uncoupled accelerometer based GNSS spoof detection for automobiles using statistic and wavelet based tests . In *Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation* , ION GNSS+ 2018, Sep. 2018 , pp. 2938 - 2962 . doi: 10.33012/2018.15903.

Google Scholar

Jhanjhi , N. Z. , Brohi , S. N. , Malik , N. A. , & Humayun , M. (2020 , October). Proposing a hybrid rpl protocol for rank and wormhole attack mitigation using machine learning . In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1 - 6). IEEE .

Google Scholar

Applications (pp. 49 - 64). IGI Global .

Google Scholar

Manickam , S. , and K. O'Keefe . Using Tactical and MEMS Grade INS to Protect Against GNSS Spoofing in Automotive Applications . Proceedings of ION GNSS+2016, 2016 .

Google Scholar

Ramanishka , V. , Y.-T. Chen , T. Misu , and K. Saenko . Toward Driving Scene Understanding: A Dataset for Learning Driver Behavior and Causal Reasoning . *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* , pp. 7699 – 7707 , Nov. 2018 .

Google Scholar

Ujjan , R. M. A. , Taj , I. , & Brohi , S. N. (2022). E-Government Cybersecurity Modeling in the Context of Software-Defined Networks . In *Cybersecurity Measures for E-Government Frameworks* (pp. 1 - 21). IGI Global .

Google Scholar

Ujjan , R. M. A. , Khan , N. A. , & Gaur , L. (2022). E-Government Privacy and Security Challenges in the Context of Internet of Things . In *Cybersecurity Measures for E-Government Frameworks* (pp. 22 - 42). IGI Global .

Google Scholar

Muzafar , S. , Humayun , M. , & Hussain , S. J. (2022). Emerging Cybersecurity Threats in the Eye of E-Governance in the Current Era . In *Cybersecurity Measures for E-Government Frameworks* (pp. 43 - 60). IGI Global .

Google Scholar

Shah , I. A. , Wassan , S. , & Usmani , M. H. (2022). E-Government Security and Privacy Issues: Challenges and Preventive Approaches . In *Cybersecurity Measures for E-Government Frameworks* (pp. 61 - 76). IGI Global .

Google Scholar

- 122). IGI Global .

Google Scholar

Jhanjhi , N. Z. , Ahmad , M. , Khan , M. A. , & Hussain , M. (2022). The Impact of Cyber Attacks on E-Governance during the COVID-19 Pandemic . In *Cybersecurity Measures for E-Government Frameworks* (pp. 123 - 140). IGI Global .

Google Scholar

Hussain , M. , Talpur , M. S. H. , & Humayun , M. (2022). The Consequences of Integrity Attacks on E-Governance: Privacy and Security Violation . In *Cybersecurity Measures for E-Government Frameworks* (pp. 141 - 156). IGI Global .

Google Scholar

Ujjan , R. M. A. , Khan , N. A. , & Gaur , L. (2022). E-Government Privacy and Security Challenges in the Context of Internet of Things . In *Cybersecurity Measures for E-Government Frameworks* (pp. 22 - 42). IGI Global .

Google Scholar

Chhajed , G. J. , & Garg , B. R. (2022). Applying Decision Tree for Hiding Data in Binary Images for Secure and Secret Information Flow . In *Cybersecurity Measures for E-Government Frameworks* (pp. 175 - 186). IGI Global .

Google Scholar

Kok , S. H. , Abdullah , A. , & Jhanjhi , N. Z. (2022). Early detection of crypto-ransomware using pre-encryption detection algorithm . *Journal of King Saud University - Computer and Information Sciences* , **34** (5), 1984 - 1999 .

Web of Science® Google Scholar

Berrueta , E. , Morato , D. , Magaña , E. , & Izal , M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic . *Expert Systems with Applications* , **209** , 118299 .

Singhal , V. , Jain , S. S. , Anand , D. , Singh , A. , Verma , S. , Rodrigues , J. J. , … & Iwendi , C. (2020). Artificial intelligence enabled road vehicle-train collision risk assessment framework for unmanned railway level crossings . *IEEE Access* , **8** , 113790 - 113806 .

Web of Science® | Google Scholar

Lim , M. , Abdullah , A. , Jhanjhi , N. Z. , Khan , M. K. , & Supramaniam , M. (2019). Link prediction in time-evolving criminal network with deep reinforcement learning technique . *IEEE Access* , **7** , 184797 - 184807 .

Web of Science® | Google Scholar

Jhanjhi , N. Z. , Brohi , S. N. , Malik , N. A. , & Humayun , M. (2020 , October). Proposing a hybrid rpl protocol for rank and wormhole attack mitigation using machine learning . In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1 - 6). IEEE .

Google Scholar

Wiley Press Room