© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722902

GNSS Spoofing and Jamming Detection and Mitigation in Smart City Architecture

ZULAIHAT MUKHTAR[1], JENNIFER NANKO SAMBO[2], REKIYA SULE[3], BULUS KEFAS[4], SAEED BABA AHMAD[5], AISHA YAKUBU[6]
[1, 2, 3, 4, 5, 6]*National Space Research and Development Agency (NASRDA)*

Abstract- ***Global Navigation Satellite Systems (GNSS) have become an invisible utility underpinning nearly every subsystem of the modern smart city, from adaptive traffic control and autonomous vehicles to smart-grid timing, 5G/6G synchronization, and emergency dispatch. Because civil GNSS signals are transmitted at very low power over publicly documented formats, they are structurally vulnerable to jamming, which denies service through radio-frequency noise, and spoofing, which deceives receivers with counterfeit signals that appear authentic.***
This paper examines the role of GNSS within smart city architecture, surveys the jamming and spoofing threat landscape, and reviews current detection techniques spanning signal-level monitoring, cryptographic authentication, spatial antenna-array processing, and data-driven machine learning approaches. It then reviews mitigation strategies, including controlled reception pattern antennas, navigation message authentication, sensor fusion, and crowdsourced interference monitoring, before proposing a six-layer secure detection and mitigation architecture tailored to the distributed, multi-stakeholder nature of smart cities.

The paper concludes by identifying open research gaps, including adversarial machine learning, urban-canyon testing deficits, cross-jurisdictional governance, and the cost of hardened receiver hardware at municipal scale.

Keywords: GNSS, GPS spoofing, jamming, smart city, positioning navigation and timing, cybersecurity, critical infrastructure

I. INTRODUCTION

Global Navigation Satellite Systems (GNSS)—including GPS, Galileo, GLONASS, and BeiDou—supply the positioning, navigation, and timing (PNT) information on which modern urban infrastructure silently depends. In a smart city, GNSS synchronizes traffic signals, times financial transactions, guides autonomous vehicles and delivery drones, and disciplines the clocks that keep power grids and telecommunication networks in step (Septentrio, 2026; GPS World, 2026). This ubiquity has made GNSS a foundational, largely unquestioned layer of urban digital infrastructure.

That dependence is also a liability. Civil GNSS signals arrive at ground receivers at extremely low power and follow publicly documented interface specifications, making them easy to overpower with noise (jamming) or imitate with counterfeit signals (spoofing) (Lu et al., 2024; Zidan et al., 2020). Unlike many cybersecurity threats that require network access or software exploitation, GNSS attacks can be mounted from a moving vehicle or rooftop using commodity software-defined radios costing only a few hundred dollars (Radoš et al., 2024; Ghanbarzadeh et al., 2025). As the barrier to attack falls, the number of interconnected, GNSS-dependent systems within a city rises, so a single jamming or spoofing event no longer threatens one device but can cascade across transportation, utility, and public-safety systems simultaneously.

This paper addresses that intersection of vulnerability and interdependence. It first situates GNSS within smart city architecture, mapping the subsystems that rely on accurate PNT. It then characterizes the jamming and spoofing threat landscape, drawing on documented incidents and experimental studies, and surveys detection techniques across four families—signal/receiver-level monitoring, cryptographic authentication, spatial/antenna-array processing, and data-driven machine learning—before reviewing mitigation strategies at the hardware, network, and policy levels. Building on this review, the paper proposes a layered secure detection and mitigation architecture suited to the distributed governance and heterogeneous hardware typical of smart cities, and closes by identifying the research gaps that must be closed before such an architecture can be deployed with confidence at municipal scale.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722902

II. GNSS IN SMART CITY ARCHITECTURE

A smart city integrates sensors, communication networks, and data analytics to manage urban services such as mobility, energy, water, and public safety in a coordinated, data-driven way. GNSS contributes two distinct products to this integration: position and precise time, a common clock reference that lets distributed systems agree on the order and timing of events. Both products are consumed across nearly every domain of city operations, as illustrated in Figure 1.

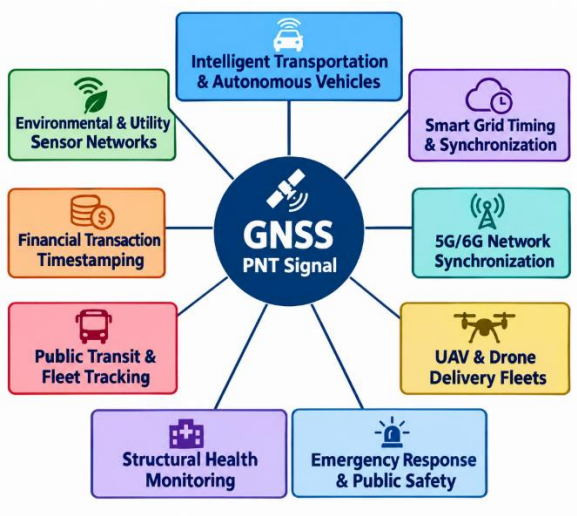

Figure 1. GNSS-dependent subsystems within a smart city architecture.

Intelligent transportation systems and autonomous or semi-autonomous vehicles use GNSS position fixes, often fused with inertial and vision sensors, for lane-level navigation, adaptive signal timing, and fleet routing (Deng et al., 2021). Transit authorities rely on the same signals to track buses and trains in real time (Septentrio, 2026). Electrical utilities use GNSS timing to synchronize phasor measurement units across the grid, a function that grows more sensitive as renewable generation increases the need for tight, wide-area synchronization (Laverty et al., 2021). Telecommunication operators similarly depend on GNSS-derived timing to synchronize base stations for 5G and emerging 6G networks (GPS World, 2026; Data Center Dynamics [DCD], 2024).

Beyond transportation and infrastructure timing, GNSS supports structural health monitoring of bridges and tunnels, environmental and utility sensor networks that geotag distributed readings, unmanned aerial vehicle (UAV) delivery and inspection fleets, and the timestamping of financial and emergency-dispatch transactions where accountability depends on an authoritative time source. Continuously Operating Reference Station (CORS) networks, often jointly operated by municipal, academic, and private actors, form a further layer of shared GNSS infrastructure that many of these applications draw on for augmentation and accuracy improvement (Septentrio, 2026).

The concentration of so many safety- and time-critical functions onto a single, physically undefended signal source is what distinguishes the smart city threat surface from that of any individual GNSS user. A jamming or spoofing event that would be a localized nuisance for one vehicle can, in a smart city, simultaneously degrade traffic control, delay emergency response, and desynchronize telecommunication or grid infrastructure sharing the same airspace (Lu et al., 2024). This shared dependency motivates treating GNSS resilience as a cross-cutting concern of smart city architecture rather than a problem for individual application owners to solve in isolation.

III. GNSS JAMMING AND SPOOFING THREATS

Jamming and spoofing are distinct attack classes. Jamming denies service by overwhelming the receiver's front end with radio-frequency noise or a competing signal, so the receiver loses lock and stops producing a position or time solution (Windward, 2026). Because GNSS signals arrive at roughly -130 dBm at the Earth's surface, even a low-power, inexpensive jammer can raise the local noise floor enough to blind receivers within tens to hundreds of meters (Ghanbarzadeh et al., 2025). Jamming waveforms vary from simple continuous-wave and narrowband tones to frequency-swept "chirp" signals that sweep across the entire GNSS band (Ghanbarzadeh et al., 2025).

Spoofing is more insidious: rather than denying service, it deceives the receiver into computing a false position, velocity, or time while continuing to report a solution with apparently normal confidence. Spoofing is broadly divided into relay-based (meaconing), which rebroadcasts intercepted genuine signals with an induced delay, and generative spoofing, in which

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722902

an attacker synthesizes counterfeit signals that mimic the code phase, carrier frequency, and navigation message of authentic satellites (Lu et al., 2024). Generative attacks are further graded by sophistication: primary attacks broadcast unsynchronized fake signals that are comparatively easy to detect; intermediate attacks estimate and match the genuine signal's parameters before gradually walking the receiver's tracking loop away from the true position; and advanced multi-antenna attacks coordinate several spoofing sources to control both position and arrival angle, defeating many single-antenna countermeasures (Lu et al., 2024).

The practical consequences have been repeatedly demonstrated. Researchers at the University of Texas showed as early as 2012 that a civilian drone, and later an $80 million yacht, could be non-cooperatively redirected using a briefcase-sized spoofer (Lu et al., 2024). Studies of autonomous vehicles have shown that a spoofed fix can cause a vehicle's planner to believe it is exiting a highway when it is not (Zeng et al., 2017), while multi-sensor fusion pipelines used in high-level autonomous driving have themselves been shown to be exploitable when spoofing is combined with knowledge of the fusion algorithm (Shen et al., 2020). UAVs are especially exposed: experimental takeover attacks against commercial autopilots have hijacked flight paths (Sathaye et al., 2022), and coordinated spoofing against drone swarms has been shown to induce collision or formation collapse, directly relevant to the growing use of drone fleets for delivery and infrastructure inspection in cities (Sathaye et al., 2022).

Jamming, meanwhile, has moved from a theoretical risk to a routine operational hazard. Aviation and maritime industries now track jamming and spoofing hot spots through crowdsourced reporting because the volume of incidents, many associated with conflict zones, has grown substantially in recent years (Windward, 2026). For a smart city, the operative risk is less a single dramatic hijacking than the steady background probability that some GNSS-dependent subsystem—an ambulance router, a construction-zone traffic controller, a grid-synchronizing relay—will encounter degraded or falsified PNT data during ordinary operation, with consequences that scale with how many downstream systems trust that data without independent verification.

IV. DETECTION TECHNIQUES

Detecting GNSS interference is a prerequisite for any mitigation response, and the literature has converged on four broad families of technique, summarized in Figure 2: signal/receiver-level monitoring, cryptographic authentication, spatial/antenna-array processing, and data-driven approaches that increasingly rely on machine learning.

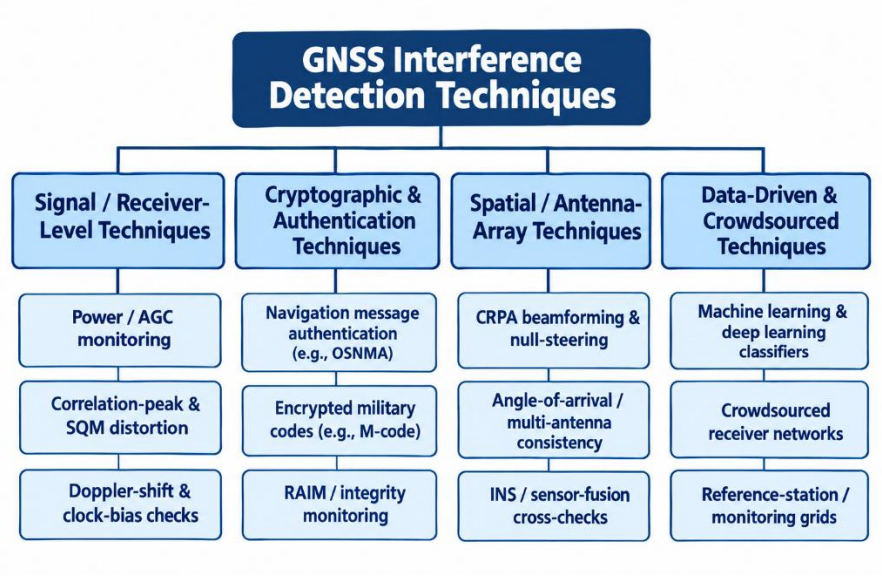

Figure 2. Taxonomy of GNSS jamming and spoofing detection techniques.

Signal and receiver-level techniques exploit the fact that interference perturbs measurable receiver quantities even when it does not fully deny service. Power and automatic-gain-control (AGC) monitoring flags the sudden rise in received power that accompanies most jamming and many spoofing attacks (Lu et al., 2024). Correlation-peak and signal-quality-monitoring (SQM) techniques examine the shape of the receiver's early-late correlator outputs, which become distorted when a spoofed signal is superimposed on the genuine one; the power-distortion detector proposed by Wesson et al. (2017) combines power and correlator-shape observations to separate spoofing from ordinary multipath. Doppler-shift and clock-bias monitoring detect the anomalous frequency and timing behavior that arises when a spoofed signal's dynamics do not match the physical motion of a genuine satellite (Tanıl et al., 2017; Psiaki & Humphreys, 2016).

Cryptographic and authentication techniques address spoofing at its root by making it computationally infeasible to forge a signal a receiver will accept as genuine. Galileo's Open Service Navigation Message Authentication (OSNMA), operational since July 2025, appends a cryptographic signature to the navigation message so enabled receivers can verify a signal genuinely originates from Galileo and reject replayed or forged messages (European Commission, 2025; International Association of Marine Aids to Navigation and Lighthouse Authorities [IALA], 2025). The GPS program is pursuing an analogous capability, Chimera, while military-grade GPS already relies on the encrypted M-code signal, unforgeable without the classified key but unavailable to civil users (Taoglas, 2025). Receiver Autonomous Integrity Monitoring (RAIM) complements these approaches by using redundant pseudorange measurements to identify and exclude a measurement statistically inconsistent with the rest of the solution (Taoglas, 2025).

Spatial and antenna-array techniques exploit the physical geometry of legitimate satellite signals, which arrive from many different directions in the sky, in contrast to most spoofing sources, which broadcast from a single ground-based location. Controlled Reception Pattern Antenna (CRPA) arrays use multiple antenna elements to estimate the direction of arrival of each incoming signal and electronically steer nulls toward interference sources while preserving gain toward genuine satellites (Keysight, 2024). Angle-of-arrival consistency checks and multi-antenna carrier-phase comparisons provide a related, often lower-cost, detection signal even without full adaptive nulling (Lu et al., 2024). Inertial navigation system (INS) and sensor-fusion cross-checks compare the GNSS-derived trajectory against an independent dead-reckoning estimate, flagging divergence as a possible spoofing indicator, though such pipelines must be designed carefully since naïve fusion can itself be manipulated by an attacker aware of the algorithm (Shen et al., 2020; Tanıl et al., 2017).

Data-driven approaches have grown rapidly as public datasets and computing resources have become available. Supervised classifiers, including support vector machines, gradient-boosted trees, and neural networks, have been trained to distinguish spoofed from authentic signals using features such as carrier-to-noise ratio, pseudorange residuals, and Doppler shift (Bose, 2021; Nayfeh et al., 2023; Shafique et al., 2021). Deep-ensemble and image-based approaches that convert raw in-phase/quadrature samples into spectrograms have achieved jamming-classification accuracies approaching 99% across six interference classes (Ghanbarzadeh et al., 2025; Swinney & Woods, 2021), while tree-based ensembles have reported comparable performance for UAV-oriented spoofing detection (Dang et al., 2022; Wei et al., 2022). Machine-learning classifiers have likewise been applied to jammer-type identification in GNSS bands (Morales Ferre et al., 2019), and broader surveys confirm that no single family of method dominates across all attack types and operating conditions (Mohanty & Gao, 2024). Finally, crowdsourced and reference-network approaches aggregate observations from many receivers—smartphones, vehicle telematics units, or dedicated CORS stations—to detect and geolocate a jamming or spoofing source through triangulation, extending detection coverage well beyond what any single receiver could achieve alone (Scott, 2011; Strizic et al., 2018).

V. MITIGATION STRATEGIES

Detection alone does not restore service; mitigation strategies determine how a system continues to operate safely once interference is identified. At the hardware

level, CRPA and adaptive beamforming antennas remain the most effective countermeasure against jamming and many spoofing geometries, since they suppress an interfering signal spatially rather than relying on statistical inference alone, though cost and size have historically limited them to aviation, defense, and high-value infrastructure rather than commodity municipal sensors (Keysight, 2024). Multi-frequency, multi-constellation receivers provide a complementary and increasingly affordable mitigation, since an attacker able to spoof one constellation's civil signal is far less likely to simultaneously spoof GPS, Galileo, GLONASS, and BeiDou across all frequency bands (Mohanty & Gao, 2024).

Cryptographic mitigation is advancing quickly on the Galileo side: because OSNMA lets a receiver reject unauthenticated navigation data outright, city systems that adopt OSNMA-capable receivers gain a free, standards-based defense against forged Galileo messages, though OSNMA still requires a stable signal to complete authentication and does not, by itself, protect against jamming or against spoofing of unauthenticated constellations (European Commission, 2025; IALA, 2025). Continued investment in encrypted military-grade signals such as M-code, and in the pending GPS Chimera service, will extend similar protection to other constellations over time (Taoglas, 2025).

Because no purely GNSS-based defense can guarantee availability during a sustained attack, resilient timing strategies that reduce reliance on GNSS altogether have become a priority for critical infrastructure operators. GNSS-independent time distribution—using terrestrial fiber links, chip-scale atomic clocks, or eLoran-style radio timing—lets telecommunication and grid operators maintain synchronization through a GNSS outage without the cost of an entirely redundant satellite system (DCD, 2024; GPS World, 2026). At the vehicle or platform level, sensor fusion with inertial navigation and dead reckoning allows continued operation for a bounded period after GNSS is lost or judged untrustworthy, buying time for a human operator or automated fallback to intervene (Tanıl et al., 2017).

At the network level, interference-monitoring networks—whether dedicated ground stations, reference receiver networks, or crowdsourced telemetry—allow a city to detect and geolocate a jamming or spoofing source and coordinate a response rather than relying on each affected device to defend itself independently (Windward, 2026; Scott, 2011). Historical vulnerability assessments of GPS-dependent transportation infrastructure argued for this kind of coordinated, system-level response well before smart city architectures existed, underscoring that the underlying problem is not new even though its urban scale is growing (Carroll, 2003). Finally, regulatory measures—mandatory interference reporting, spectrum enforcement against illegal jammers, and contingency procedures specifying which subsystems must degrade gracefully during a confirmed outage—remain necessary complements to technical mitigation, since no antenna or algorithm can substitute for institutional readiness to respond once an attack is confirmed.

VI. PROPOSED SECURE GNSS DETECTION AND MITIGATION ARCHITECTURE

No single technique reviewed above is sufficient alone: signal-level monitoring is cheap but evadable; cryptographic authentication is strong but limited to Galileo and vulnerable to jamming; antenna arrays are effective but costly; and machine-learning classifiers depend on training data that may not generalize to novel attacks (Lu et al., 2024; Ghanbarzadeh et al., 2025). Smart cities are therefore better served by a defense-in-depth architecture layering complementary techniques. Figure 3 proposes such an architecture, organized into six layers mapping onto a city’s governance structure, from the raw signal environment up to municipal decision-making.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722902

Figure 3. Proposed layered secure GNSS detection and mitigation architecture for smart cities.

Layer 0 represents the shared GNSS signal environment: constellations in view, ambient RF interference, and any adversarial jammers or spoofers present. Layer 1, receiver and antenna hardening, is implemented at each GNSS-dependent asset: multi-constellation, multi-frequency receivers, CRPA antennas where cost permits, OSNMA authentication where available, RAIM checks, and INS/dead-reckoning fallback (Keysight, 2024; European Commission, 2025; Tanıl et al., 2017). Layer 2 introduces distributed sensing that supplements individual receivers with fixed CORS stations, dedicated interference sensors, and crowdsourced telemetry, extending detection coverage across the city (Septentrio, 2026; Strizic et al., 2018).

Layer 3 aggregates this sensing at the edge and in the cloud, applying machine-learning classifiers to distinguish jamming, spoofing, and benign anomalies, and anchoring integrity assessments in a blockchain or other tamper-evident ledger so downstream consumers can verify that a position or timestamp was not silently altered (Islam et al., 2025; Ghanbarzadeh et al., 2025). Layer 4 exposes this intelligence to operators through a decision dashboard, ideally integrated with a digital twin, so traffic, grid, and emergency systems receive automated alerts while a human retains override authority. Layer 5, governance, closes the loop through incident reporting, cross-jurisdictional coordination, and continuity policy specifying acceptable degradation per service class.

The value of this architecture lies in the redundancy created by combining layers: an attack sophisticated enough to defeat Layer 1 hardening still tends to produce an anomaly visible to Layer 2–3 monitoring and fusion, while a jamming event too widespread for one reference station becomes tractable once city-wide observations are fused. Because the layers map to distinct organizational owners—vendors, network operators, city IT, and regulators—the architecture also clarifies accountability, otherwise difficult to establish when GNSS resilience is treated as a purely technical problem.

VII. CHALLENGES AND RESEARCH GAPS

Several obstacles stand between the architecture proposed above and practical deployment. Cost remains a genuine barrier: CRPA arrays and multi-frequency receivers standard in aviation and defense are still expensive relative to typical municipal IoT budgets, raising the question of how much hardening is justifiable for a traffic sensor compared with a grid synchronization unit (Keysight, 2024). Machine-learning detectors also face an adversarial and generalization problem: most classifiers are trained on a limited number of public datasets collected under relatively controlled conditions, and their performance on novel attack types or dense urban multipath remains uncertain, while an attacker aware of a deployed detector's features can in principle craft signals designed to evade it (Ghanbarzadeh et al., 2025; Swinney & Woods, 2021).

Cryptographic authentication is currently uneven across constellations: OSNMA protects Galileo's Open Service but does not defend against jamming, requires a stable signal to complete authentication, and offers no protection until receivers fleet-wide are upgraded to support it, while comparable authentication for GPS civil signals remains in earlier stages of development (European Commission, 2025; IALA, 2025). Most experimental evidence, moreover, has been gathered in open-sky or idealized conditions, with comparatively little published research on performance in dense urban canyons or under multiple simultaneous attack types (Lu et al., 2024). The crowdsourced monitoring central to Layer 2 of the proposed architecture also raises privacy questions, since the location data needed to detect interference sources is itself sensitive personal information (Strizic et al., 2018).

Finally, governance and regulatory fragmentation across municipal, national, and international authorities complicates the Layer 5 response: a jamming source near a city border, or a spoofing campaign linked to a foreign conflict, may exceed any single municipal regulator's jurisdiction, echoing concerns raised more than two decades ago about GPS-dependent transportation infrastructure facing threats no single operator could unilaterally resolve (Carroll, 2003). Closing these gaps will require coordinated investment in realistic urban testbeds, cross-constellation authentication, privacy-preserving crowdsourcing protocols, and clearer multi-jurisdictional incident-response frameworks.

VIII. CONCLUSION

GNSS has become a foundational, largely invisible utility for smart cities, supplying the position and timing information that transportation, energy, telecommunications, and public-safety systems depend on. That same ubiquity, combined with the structural weakness of low-power, publicly documented civil signals, makes jamming and spoofing a credible and growing threat, as demonstrated by more than a decade of experimental hijackings, UAV takeovers, and documented interference incidents. No single technique reviewed here—signal monitoring, cryptographic authentication, antenna-array processing, or machine learning—is sufficient in isolation. The six-layer architecture proposed instead argues for defense-in-depth, combining hardened receivers, distributed sensing, AI-based fusion anchored in tamper-evident ledgers, city-level decision support, and formal governance, so the compromise of any single layer does not translate into an undetected, city-wide failure. Realizing it will require sustained research into adversarial robustness, urban-environment testing, cross-constellation authentication, and cross-jurisdictional coordination—but treating GNSS resilience as someone else's problem is no longer viable for infrastructure that now touches nearly every function of the modern city.

REFERENCES

[1] Altaweel, A., Mukkath, H., & Kamel, I. (2023). GPS spoofing attacks in FANETs: A systematic literature review. IEEE Access, 11, 55233–55280. https://doi.org/10.1109/ACCESS.2023.3281731

[2] Bose, S. C. (2021). GPS spoofing detection by neural network machine learning. IEEE Aerospace and Electronic Systems Magazine, 37(6), 18–31.

[3] Carroll, J. V. (2003). Vulnerability assessment of the U.S. transportation infrastructure that relies on the Global Positioning System. Journal of Navigation, 56(2), 185–193. https://doi.org/10.1017/S0373463303002273

[4] Dang, Y., Benzaïd, C., Yang, B., Taleb, T., & Shen, Y. (2022). Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs. IEEE Internet of Things Journal, 9(24), 25068–25085.

[5] Data Center Dynamics. (2024, April 30). Why GNSS-independent time sync is crucial for critical national services. https://www.datacenterdynamics.com/en/opinions/why-gnss-independent-time-sync-is-crucial-for-critical-national-services/

[6] Deng, Y., Zhang, T., Lou, G., Zheng, X., Jin, J., & Han, Q.-L. (2021). Deep learning-based autonomous driving systems: A survey of attacks and defenses. IEEE Transactions on Industrial Informatics, 17(12), 7897–7912. https://doi.org/10.1109/TII.2021.3071405

[7] European Commission, Directorate-General for Defence Industry and Space. (2025, September 8). Observer: How Galileo OSNMA helps counter GNSS spoofing. https://defence-industry-space.ec.europa.eu/observer-how-galileo-osnma-helps-counter-gnss-spoofing-2025-09-08_en

[8] Ghanbarzadeh, A., Soleimani, M., & Soleimani, H. (2025). GNSS/GPS spoofing and jamming identification using machine learning and deep learning. arXiv. https://arxiv.org/abs/2501.02352

[9] GPS World. (2026, June 22). Timing matters: The critical role of GNSS-resilient systems in modern infrastructure. https://www.gpsworld.com/timing-matters-the-critical-role-of-gnss-resilient-systems-in-modern-infrastructure/

[10] Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. IEEE Transactions on Aerospace and Electronic Systems, 49(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400

[11] International Association of Marine Aids to Navigation and Lighthouse Authorities. (2025, December 17). Open Service Navigation Message Authentication (OSNMA). https://www.iala.int/e-bulletin/open-service-navigation-message-authentication-osnma/

[12] Islam, R., Bose, R., Roy, S., Khan, A. A., et al. (2025). Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model. Scientific Reports, 15, Article 06405. https://doi.org/10.1038/s41598-025-06405-y

[13] Keysight Technologies. (2024, November 29). The best anti-jam solutions for GPS/GNSS resilience. https://www.keysight.com/blogs/en/tech/positioning-navigation-and-timing/crpa-antennas-explained-choosing-and-testing-the-best-anti-jam-solutions-for-gps-gnss-resilience

[14] Lu, C., Lu, Z., Liu, Z., Huang, L., & Chen, F. (2024). Overview of satellite navigation spoofing and anti-spoofing techniques. Frontiers in Physics, 12, Article 1428544. https://doi.org/10.3389/fphy.2024.1428544

[15] Mohanty, A., & Gao, G. (2024). A survey of machine learning techniques for improving Global Navigation Satellite Systems. EURASIP Journal on Advances in Signal Processing, 2024, Article 73. https://doi.org/10.1186/s13634-024-01167-7

[16] Morales Ferre, R., de la Fuente, A., & Lohan, E. S. (2019). Jammer classification in GNSS bands via machine learning algorithms. Sensors, 19(22), Article 4841. https://doi.org/10.3390/s19224841

[17] Nayfeh, M., Li, Y., Al Shamaileh, K., Devabhaktuni, V., & Kaabouch, N. (2023). Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Computers & Security, 126, Article 103085.

[18] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. Proceedings of the IEEE, 104(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

[19] Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. Sensors, 24(13), Article 4210. https://doi.org/10.3390/s24134210

[20] Sathaye, H., LaMountain, G., Closas, P., & Ranganathan, A. (2022). SemperFi: Anti-spoofing GPS receiver for UAVs. In Proceedings

of the 2022 Network and Distributed System Security Symposium. Internet Society.

[21] Sathaye, H., Strohmeier, M., Lenders, V., & Ranganathan, A. (2022). An experimental study of GPS spoofing and takeover attacks on UAVs. In Proceedings of the 31st USENIX Security Symposium (pp. 3345–3362). USENIX Association.

[22] Scott, L. (2011). J911: The case for fast jammer detection and location using crowdsourcing approaches. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011) (pp. 1931–1940). Institute of Navigation.

[23] Septentrio. (2026). How GNSS receivers empower smart cities. https://www.septentrio.com/en/learn-more/insights/how-gnss-receivers-empower-smart-cities

[24] Shafique, A., Mehmood, A., & Elhadef, M. (2021). Detecting signal spoofing attack in UAVs using machine learning models. IEEE Access, 9, 93803–93815. https://doi.org/10.1109/ACCESS.2021.3089847

[25] Shen, J., Won, J. Y., Chen, Z., & Chen, Q. A. (2020). Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing. In Proceedings of the 29th USENIX Security Symposium (pp. 931–948). USENIX Association.

[26] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J., & Kim, Y. (2015). Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Security Symposium (pp. 881–896). USENIX Association.

[27] Strizic, L., Akos, D. M., & Lo, S. (2018). Crowdsourcing GNSS jamming detection and localization. In Proceedings of the 2018 International Technical Meeting of the Institute of Navigation (pp. 626–641). Institute of Navigation.

[28] Swinney, C. J., & Woods, J. C. (2021). Raw IQ dataset for GNSS GPS jamming signal classification [Data set]. Zenodo. https://doi.org/10.5281/zenodo.4610850

[29] Tanıl, Ç., Khanafseh, S., Joerger, M., & Pervan, B. (2017). An INS monitor to detect GNSS spoofers capable of tracking vehicle position. IEEE Transactions on Aerospace and Electronic Systems, 54(1), 131–143. https://doi.org/10.1109/TAES.2017.2739924

[30] Taoglas. (2025, October 30). Countering GNSS jamming and spoofing for aerospace and defense applications. https://www.taoglas.com/blogs/countering-gnss-jamming-and-spoofing-for-aerospace-and-defense-applications/

[31] Wei, X., Wang, Y., & Sun, C. (2022). PerDet: Machine-learning-based UAV GPS spoofing detection using perception data. Remote Sensing, 14(19), Article 4925. https://doi.org/10.3390/rs14194925

[32] Wesson, K. D., Evans, B. L., & Humphreys, T. E. (2013). A combined symmetric difference and power monitoring GNSS anti-spoofing technique. In 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP) (pp. 217–220). IEEE. https://doi.org/10.1109/GlobalSIP.2013.6736863

[33] Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2017). GNSS signal authentication via power and distortion monitoring. IEEE Transactions on Aerospace and Electronic Systems, 54(2), 739–754. https://doi.org/10.1109/TAES.2017.2735618

[34] Windward. (2026, June 25). What is GPS jamming? https://windward.ai/glossary/what-is-gps-jamming/

[35] Zeng, K. C., Shu, Y., Liu, S., Dou, Y., & Yang, Y. (2017). A practical GPS location spoofing attack in road navigation scenario. In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications (pp. 85–90). ACM. https://doi.org/10.1145/3032970.3032983

[36] Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2020). GNSS vulnerabilities and existing solutions: A review of the literature. IEEE Access, 9, 153960–

153976.
https://doi.org/10.1109/ACCESS.2020.3010353