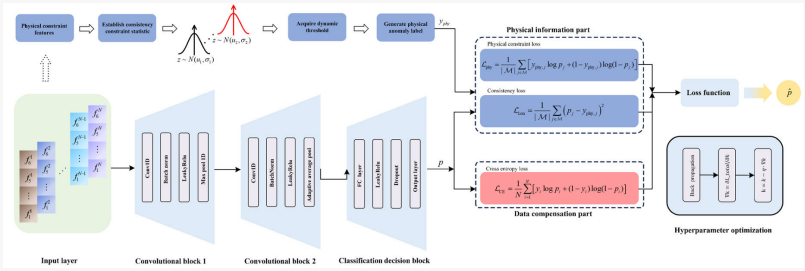
Teaching AI the laws of navigation: New physics guided detector catches GNSS spoofing even in never before seen attacks



Architecture of the proposed PCNNs framework.

GA, UNITED STATES, July 10, 2026 /EINPresswire.com/ -- Global Navigation Satellite System (GNSS) spoofing—the transmission of counterfeit signals that trick receivers into reporting false positions or times—poses a growing threat to aviation, maritime shipping, power grids and autonomous systems. While machine learning has improved detection, most models fail when confronted with attack scenarios they have never seen before, because they learn data patterns rather than the underlying physics of real signals. A new approach embeds a fundamental physical law directly into the neural network's training process, enabling the model to detect spoofing with over 92% accuracy—even in completely unfamiliar attack environments.

Conventional spoofing detectors rely on statistical rules or data‐hungry deep learning models that perform well on the scenarios they are trained on but collapse when the attack changes—for example, when a receiver moves from static to dynamic conditions or when the spoofing power profile shifts. Machine learning models learn the statistical quirks of their training datasets, not the invariant physical relationships that define authentic Global Navigation Satellite System (GNSS) signals. As a result, accuracy can plummet to around 50% in unseen scenarios—essentially random guessing. These challenges demand an approach that moves beyond pattern matching to capture the fundamental signal properties that spoofing cannot fully replicate.

Now, researchers from the National University of Defense Technology in Changsha, China, have developed Code‐Carrier Consistency Physics‐Constrained Neural Networks (CCC‐PCNNs), a detection framework that integrates physical laws into the learning process. The work, published (DOI: 10.1186/s43020-026-00199-8) June 26, 2026 in the journal Satellite Navigation, demonstrates that embedding the inherent consistency between code phase and carrier phase—a relationship that authentic GNSS signals obey but spoofing signals systematically violate—as a constraint in the loss function dramatically improves both accuracy and generalization.

The team designed a one‑dimensional convolutional neural network with a parallel “physics pathway” that computes real‑time consistency metrics from raw signal measurements. Rather than simply feeding physics‑derived features as extra inputs—a common but limited strategy—the researchers reformulated the loss function to penalize predictions that violate the code‑carrier relationship. This hybrid objective forces the model to learn representations that are both data‑driven and physically grounded. On benchmark datasets—collectively spanning static and dynamic receiver platforms, power advantages from 0.4 to 10 dB, and both time‑manipulation and position‑manipulation attacks—CCC‑PCNNs achieved average detection accuracy exceeding 98% under within‑scenario evaluation. More importantly, when tested on ten completely unseen scenarios, the model maintained Accuracy Retention Rates above 92.7%, outperforming standard one‑dimensional convolutional neural networks by 23.5%, Long Short‑Term Memory networks by 18.4%, Transformers by 9.4%, Support Vector Machines by 28.8%, Residual Networks by 24.2%, Graph Attention Networks by 27.0%, and the traditional CCC‑Detector by 46.2%. The adaptive threshold parameter driving the physics constraint converged reliably regardless of initialization, with standard deviations below 0.04. Inference latency remained at 0.353 milliseconds—only 32% slower than a bare one‑dimensional convolutional neural network, yet substantially faster than Residual Network and Transformer models.

“What makes this work different is that we are not just feeding physics‑derived numbers into a neural network and hoping it figures things out,” the authors said. “We are making the network respect a physical law during training—if its prediction violates code‑carrier consistency, it gets penalized. That forces the model to learn what a real signal must look like, not just what the training data happened to look like. The result is a detector that doesn’t panic when it encounters a new kind of attack—it just checks the physics and knows.”

The implications extend well beyond navigation. Any system that relies on time‑synchronized signals—power grid synchronization, telecommunications networks, financial trading platforms, and autonomous vehicle fleets—faces similar spoofing risks. For example, financial networks depend on GNSS for precise transaction timestamps, and 5G base stations require phase‑synchronized clocks; both are equally vulnerable to spoofing. CCC‑PCNNs offers a blueprint for building AI‑based security systems that are not brittle to distribution shifts, because they anchor decisions in physical invariants rather than statistical coincidences. The framework is computationally light enough for real‑time deployment on resource‑constrained receivers, requiring only 0.353 milliseconds per inference. Future work will address cold‑start scenarios—where a receiver powers on under active attack—by exploring pre‑loaded calibration baselines and cross‑satellite consistency checks, moving toward a new generation of physically intelligent navigation security.

References

DOI
10.1186/s43020-026-00199-8

Original Source URL
https://doi.org/10.1186/s43020-026-00199-8

About Satellite Navigation
Satellite Navigation (ISSN: 2662-1363; ISSN: 2662-9291) Satellite Navigation is the official journal of the Aerospace Information Research Institute. The aims to report innovative ideas, new results or progress on the theoretical techniques and applications of satellite navigation. The journal welcomes original articles, reviews and commentaries.

Lucy Wang
BioDesign Research
email us here