Robust Adversarial Attack Detection

Tech ID: 34748 / UC Case 2026-587-0

BACKGROUND

The transition to 5G and 6G networks has led to a widespread adoption of machine learning (ML) for critical functions like modulation classification, channel estimation, resource management, and spectrum sensing. While ML has enhanced operational efficiency, it has simultaneously expanded the attack surface for adversarial ML at the Physical Layer (PHY), for example, from Generative Adversarial Networks (GANs). While techniques like radio frequency (RF) fingerprinting have emerged as a PHY-level authentication method based on hardware-induced signal traits (such as in-phase/quadrature (I/Q) imbalance and error vector magnitude), GANs can synthesize RF signals to mimic legitimate hardware-induced features up to 95% similarity. This is close enough to evade most detection schemes. Existing defenses to GANs based on convolutional neural networks, deep neural networks, supervised retraining, and/or heuristics do not generalize well across different modulations, protocols, channel conditions, or unseen attack types. Autoencoder and reconstruction-based approaches are often limited to clean reference signals, which are not always available in dynamic wireless environments. While GANs are excellent at mimicking low-order statistics (mean/variance), they fail to replicate complex signal structures.

TECHNOLOGY DESCRIPTION

To help address these challenges in security against adversarial attacks (e.g., GANs), researchers at UC Santa Cruz (UCSC) have developed a new approach to detection using higher-order moments, especially third-order and fourth-order statistics. Recognizing that GANs are typically optimized to minimize divergence in low-order properties, the UCSC methods extract features of order three (skewness) or higher (kurtosis) from baseband I/Q signal samples, rather than relying primarily on raw I/Q samples or low-order statistics. In turn, this enables a broader statistical signature than conventional approaches, by pulling features from multiple domains, including time, frequency (via Short-Time Fourier Transform), and/or bispectrum. The UCSC technology leverages such multi-branch neural networks (or other lightweight threshold-based) to intelligently fuse these multi-domain features. This enables protocol-agnostic and model-agnostic detection without requiring prior knowledge of the specific attack type or modulation scheme.

APPLICATIONS

- 5G/6G network infrastructure
- IoT device systems/software
- autonomous vehicle communication / V2X

FEATURES/BENEFITS

- Improved fingerprint reliability by exploiting the inherent mathematical inability of GANs to preserve third and fourth-order moments.
- Computationally efficient for edge devices by employing lightweight statistical calculations and training-free detection.
- Potential for fast deployment through deviation-based (anomaly detection) approach; lowers data needs for zero-day attacks.

RELATED MATERIALS

CONTACT

Marc Oettinger
marc.oettinger@ucsc.edu
tel: 831-502-0253.

INVENTORS

- Obraczka, Katia
- Rezki, Zouheir
- Xue, Li

OTHER INFORMATION

KEYWORDS

machine learning, Generative Adversarial Networks, GAN, PHY, adversarial attack, wireless security, wireless, moments, physical layer, signal processing, higher-order moments, detection, channel, RF fingerprinting, PHY-layer, physical-layer, adversarial, attack surface, zero-day, spoofing, evasion, adversarial machine learning, adversarial ML

CATEGORIZED AS

- **Communications**
  - Internet
  - Networking
  - Wireless
- **Computer**
  - Security
  - Software
- **Security and Defense**
  - Cyber security

RELATED CASES

2026-587-0

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Decoder-Only Transformer Methods for Indoor Localization
- A Novel Iot Protocol Architecture; Efficiency Through Data And Functionality Sharing Across Layers
- Patient Pressure Injury Prevention Methods and Software
- Platooning System and Methods
- Cross-Layer Device Fingerprinting System and Methods
- Smart Deployment of Nodes in a Network

University of California, Santa Cruz
Industry Alliances & Technology Commercialization
Kerr 413 / IATC,
Santa Cruz,CA 95064

Tel: 831.459.5415
innovation@ucsc.edu
https://officeofresearch.ucsc.edu/
Fax: 831.459.1658