STARSentinel

A Multi-Vector Toolkit for Threat Detection in Space Systems Cybersecurity

29.04.2025

Submitted By:

UPASANA MANOJ SOLANKI

SOHAM SHRIKHANT GHAWARE

Cybersecurity Internship 2025

Digisuraksha Parhari Foundation & Infinisec Technologies Pvt. Ltd.

Abstract

With the increasing reliance on satellite systems for global navigation, communication, and space traffic control, the security of space systems has become a critical concern. STARSentinel is a multi-functional toolkit designed to simulate, detect, and analyze vulnerabilities in satellite-based systems. This research focuses on three high-risk areas: GNSS spoofing, satellite communication protocol security, and orbital spoofing threats.

The GNSS module parses GPS logs to identify sudden spatial or temporal jumps, which may indicate signal spoofing. The SatCom scanner simulates network-based scans and configuration checks to highlight insecure access points in satellite infrastructure. The Space Traffic Simulator uses real TLE data to model spoofed orbital positions and potential collisions.

STARSentinel provides researchers and students with a practical platform for space cybersecurity analysis and ethical red-teaming. The toolkit is designed using Python and open-source packages and emphasizes modular design, ethical usage, and real-world relevance.

Problem Statement & Objective

Modern space systems such as GNSS (Global Navigation Satellite Systems), satellite communication networks, and orbital traffic control systems are increasingly exposed to cybersecurity threats. GNSS signals are weak and unauthenticated, making them vulnerable to spoofing. SatCom networks often rely on insecure protocols or default configurations. Meanwhile, space traffic control lacks robust mechanisms for verifying satellite position integrity.

The objective of this research is to design and implement STARSentinel, a modular toolkit to simulate, detect, and demonstrate these vulnerabilities in a controlled environment. It is aimed at raising awareness, improving security analysis training, and aiding research in space systems cybersecurity.

Literature Review

- GNSS spoofing incidents have been documented in real-world cases such as the 2013 spoofing of the White Rose yacht and multiple maritime incidents near Russia and Iran.

- DEFCON and BlackHat presentations have revealed vulnerabilities in satellite uplinks, unencrypted telemetry data, and default web interfaces on SatCom systems.

- ESA and NASA have raised concerns over the growing risk of satellite collisions and emphasized the need for secure space situational awareness (SSA).

- Studies on cyber-physical systems (CPS) demonstrate how software-based attacks can have physical consequences in aerospace systems.

Research Methodology

This toolkit was implemented using Python. Key open-source libraries used include:

- pynmea2: For parsing GNSS NMEA logs

- python-nmap: For simulated port scanning

- skyfield & matplotlib: For satellite position calculation and 3D visualization

The project follows a modular structure:

1. GNSS Spoofing Detector: Detects positional jumps in GPS data.

2. SatCom Scanner: Emulates scanning insecure satellite devices and config flags.

3. Space Traffic Simulator: Uses TLE data to simulate spoofed satellites and measure collision distance.

Each module was tested independently with sample data and validated through visual and printed outputs.

Tool Implementation

- GNSS Spoofing Detector: Processes GPS logs to find sudden jumps in distance (>500m) or time (>10s), flagging them as potential spoofing.

- SatCom Scanner: Simulates port scanning on mock SatCom IPs, TLE integrity checks, and configuration audits (e.g., default password detection).

- Space Traffic Simulator: Loads real TLE data and injects a fake satellite with similar orbit; if distance <50 km, the system flags a potential collision.

Scripts are executed independently using command line or Python IDLE. Results are printed and optionally visualized (in 3D for orbits).

Results & Observations

- The GNSS spoofing module successfully flagged simulated GPS data anomalies, demonstrating the feasibility of spoof detection through signal analysis.

- The SatCom scanner identified insecure configurations (default passwords, open ports), showing how attackers could exploit exposed SatCom devices.

- The space traffic simulation showed that a fake satellite injected with a close orbit (within 17 km of the ISS) could trigger a potential collision alert.

All modules executed efficiently on a standard system (Windows 11, Python 3.11).

Ethical Impacts & Market Relevance

STARSentinel was built solely for ethical research and educational purposes. It does not interfere with real satellite systems or live signals.

Space cybersecurity is rapidly becoming a national security issue. This toolkit can support:

- Cybersecurity training programs (ethical hacking, CPS security)

- Academic research in aerospace cybersecurity

- Public sector efforts toward secure space systems (ISRO, DRDO, NASA, ESA)

By providing hands-on simulation, STARSentinel bridges the gap between theory and practical awareness.

Future Scope

- Adding real-time GPS spoof detection using SDR (software-defined radio) input

- Integration with public SatCom telemetry APIs for live monitoring

- Web dashboard with visual analytics

- AI/ML-based detection of orbital spoofing patterns

- Educational game mode for interactive cybersecurity training

References

1. Humphreys, T. E. (2012). "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer."

2. DEFCON 27 Talk: “Satellite Hacking: Breaking the Final Frontier”

3. ESA SSA Programme Reports (2023)

4. NIST Cybersecurity Framework for Space Systems

5. GPS World: "The Future of GNSS Security" (2022)

6. BlackHat 2020: “Hacking SatCom Terminals”

7. GNSS-SDR Open Source Framework

8. NASA TLE Database (Celestrak.org)

9. Skyfield Python Library Documentation

10. Cyber Physical Systems Security – MITRE White Paper (2021)