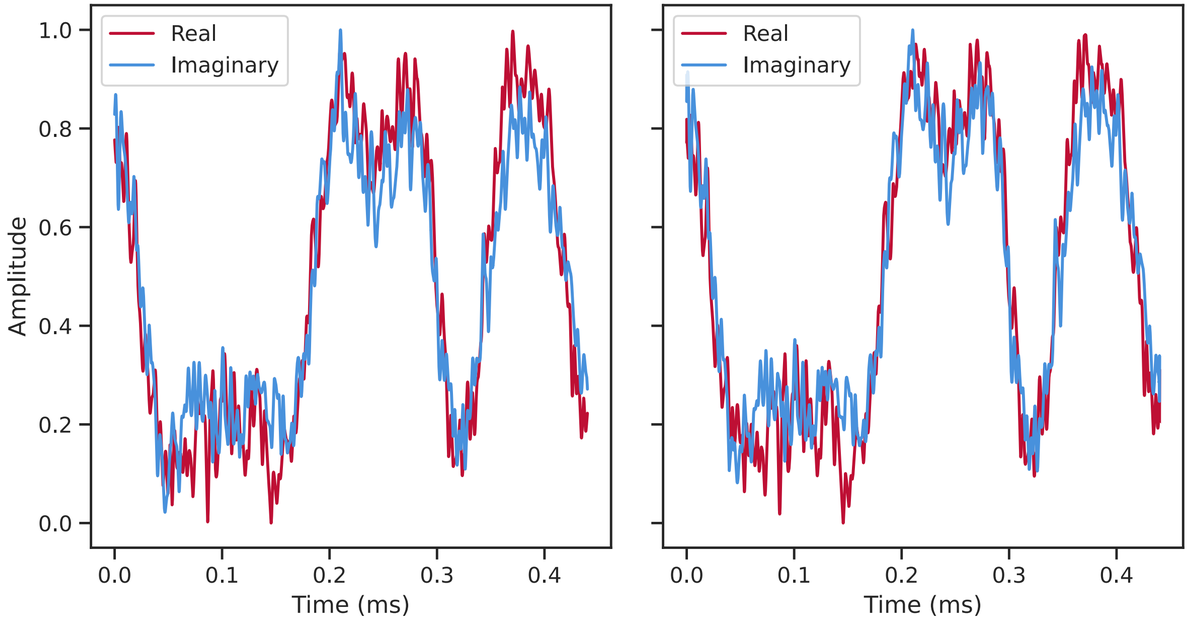
Quantised In-Orbit Fingerprinting for Uplink Authentication

CyberCUBE Experiment Proposal

Joshua Smailes, Simon Birnbach, Sebastian Köhler, Ivan Martinovic
Systems Security Lab, University of Oxford

Satellite Fingerprinting

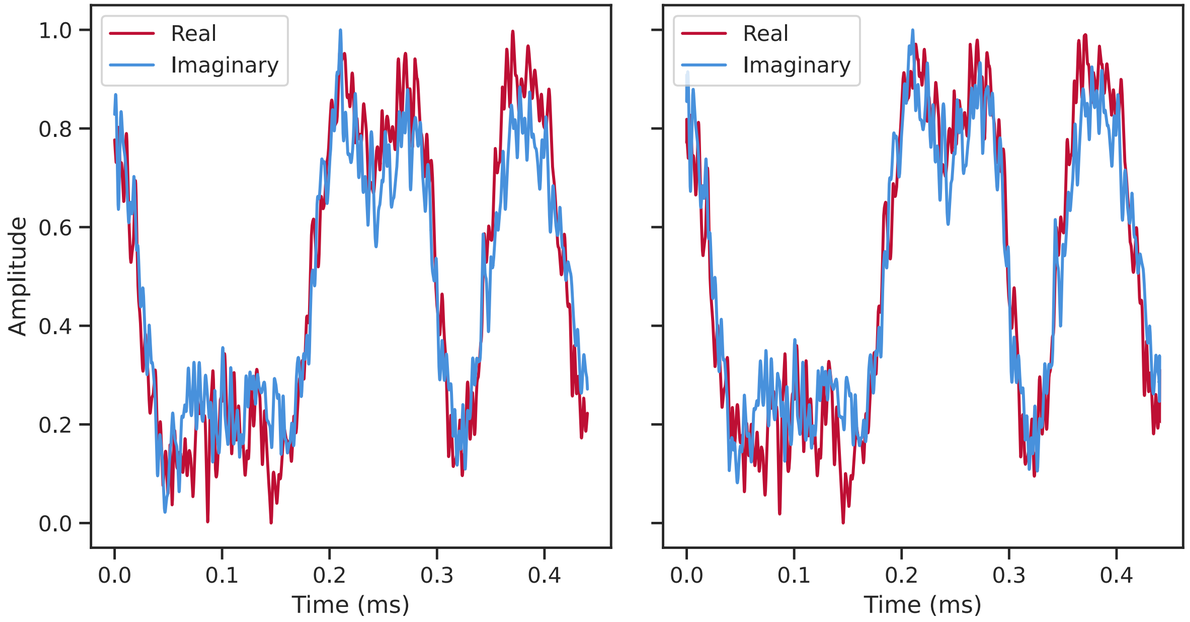
A brief introduction



- Transmitters have unique hardware differences

Satellite Fingerprinting

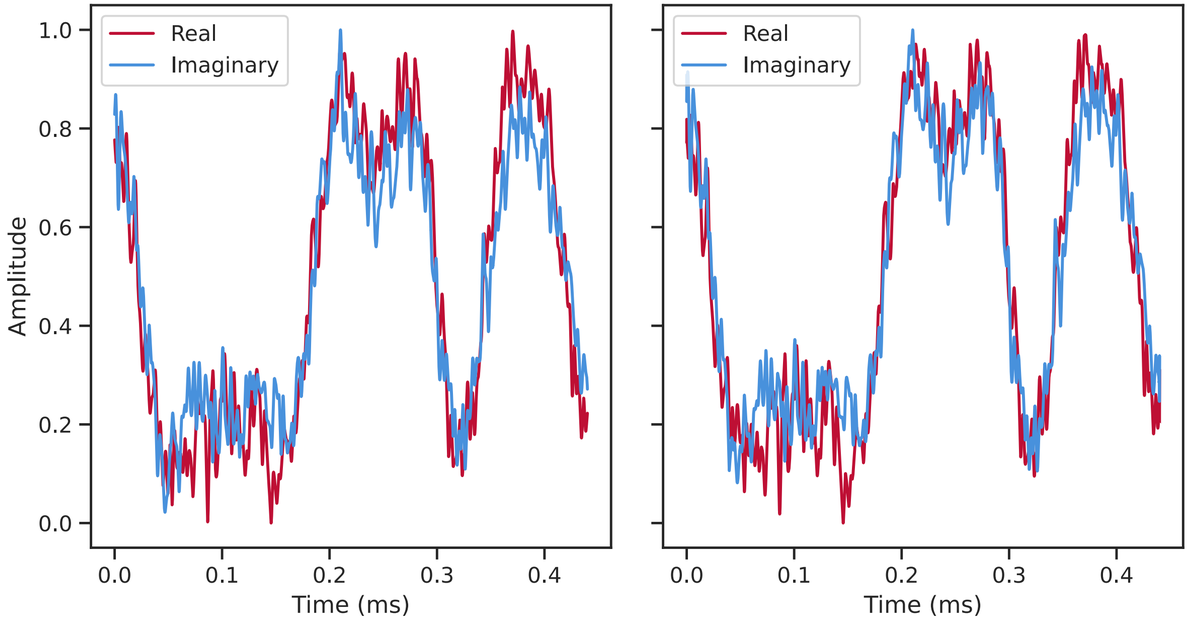
A brief introduction



- Transmitters have unique hardware differences
- These can be used to authenticate transmitters

Satellite Fingerprinting

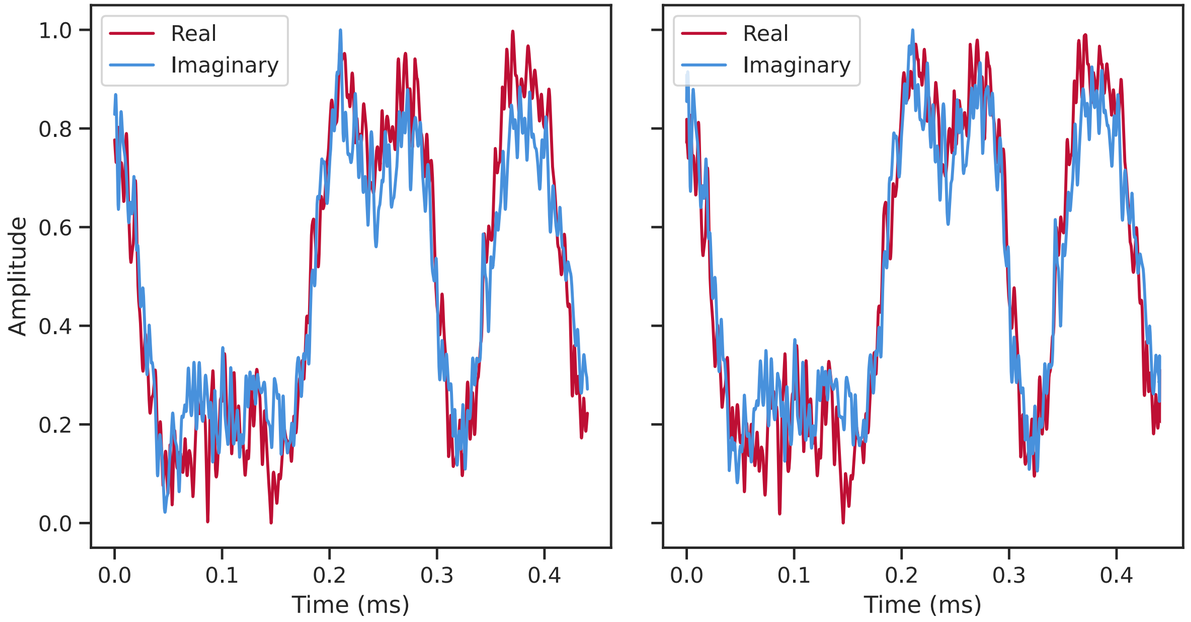
A brief introduction



- Transmitters have unique hardware differences
- These can be used to authenticate transmitters
- Difficult to fake

Satellite Fingerprinting

A brief introduction



- Transmitters have unique hardware differences
- These can be used to authenticate transmitters
- Difficult to fake
- No transmitter modifications required

Satellite Fingerprinting

Past Contributions

SatIQ system:[1,2]

- High sample rate (25MS/s, 1000x oversampling)
- Works in the presence of atmospheric attenuation/distortion
- Treats fingerprints as a biometric: extensible, less vulnerable to adversarial perturbations
- Resilient against replay attacks
- Extensible to new transmitters

Largest dataset of its kind, over 10 million messages from 3 locations

Transferable between satellite constellations [3]

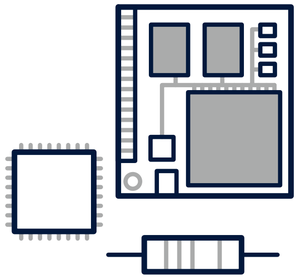
[1] Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, Ivan Martinovic. "Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting". ACM CCS 2023.

[2] Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, Ivan Martinovic. "SatIQ: Extensible and Stable Satellite Authentication using Hardware Fingerprinting". ACM TOPS, 2025.

[3] Cédric Solenthaler, Joshua Smailes, Martin Strohmeier. "OrbID: Identifying Orbcomm Satellite RF Fingerprints". SpaceSec 2025.

Satellite Fingerprinting

Uplink Limitations



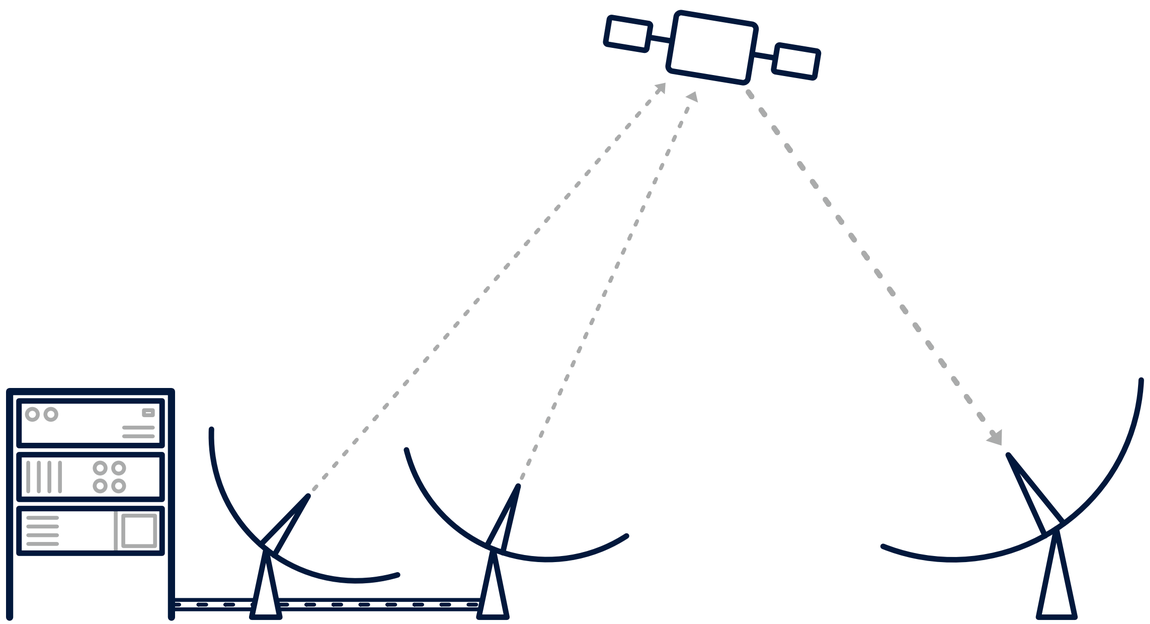
Limited Computational Capacity

Lack of Onboard SDRs

Limited Access to Research Satellites

Existing research has therefore remained limited to the downlink.

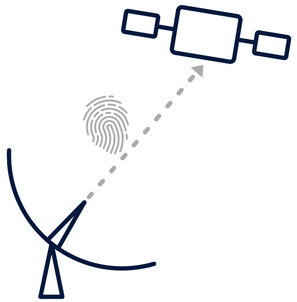
Goal



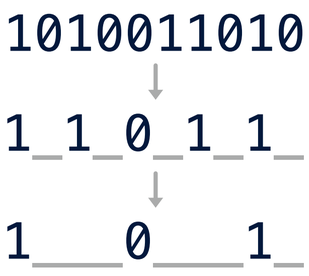
- Adapt terrestrial fingerprinting to work on the uplink, using CyberCUBE as a proof of concept
- Onboard data collection using the telecommand link
- Send captured data back to Earth for training/analysis
- Run trained models on the satellite for eventual end-to-end inference

Model Training

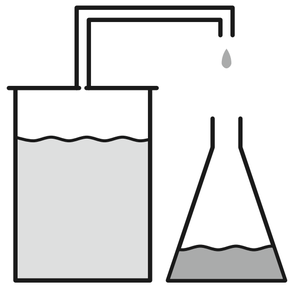
Alongside training models from scratch, we will test the following for more lightweight training/inference:



Finetuning



Quantisation



Distillation

Outcome

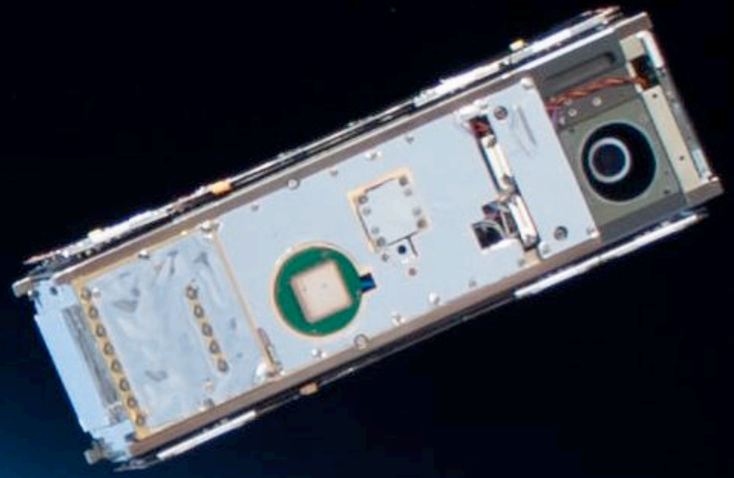
Uplink fingerprinting can provide a number of distinct benefits:

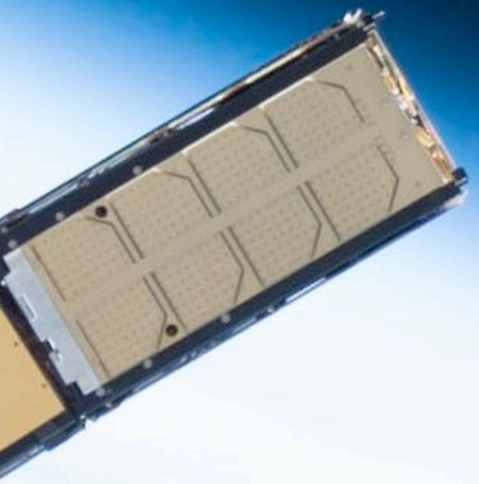
- Bolster telecommand by detecting spoofing and replay attacks
- Understand when attacks are occurring to more quickly deploy countermeasures
- Potential for user device segmentation for analytical purposes

Future work:

- Combine with GSaaS to form a larger dataset
- Bidirectional fingerprinting, looking at the uplink and downlink simultaneously

Thank you!





Any questions?

Image: NASA