

# Spoofing Earth Observation Satellites through Radio Overshadowing

Edd Salkield<sup>1</sup> Joshua Smalles<sup>1</sup> Sebastian Köhler<sup>1</sup> Simon Benbach<sup>1</sup>  
Richard Baker<sup>1</sup> Martin Strohmeier<sup>2</sup> Ivan Martinovic<sup>1</sup>

<sup>1</sup>Systems Security Lab, University of Oxford

<sup>2</sup>Cyber-Defence Campus, e-Research Science & Technology

Although satellite data is increasingly relied upon, many satellites don't have authenticated down-links, which opens the door for spoofing attacks. My name's Edd Salkield, and I'm from the Systems Security Lab at the University of Oxford. I'm presenting Firefly, an analysis of the vulnerability and effects of spoofing attacks against current Earth observation satellite systems. In particular, we'll consider the effects of a motivated, modern adversary against NASA's real-time forest fire API. The current situation in space is that...

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

- └ Case Study: FIRMS

- └ Attack overview

- └ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>

---

<sup>1</sup><https://satsearch.mnhp.noaa.gov/firms/>

All the tools used in our attack will be published alongside our paper

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Case Study: FIRMS

└ Attack overview

└ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>

---

<sup>1</sup><https://satellite.mnsgo.noaa.gov/firms/>

<sup>2</sup><https://bluetooth-hack-club.github.io/2017/01/academic-account/>

All the tools used in our attack will be published alongside our paper

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Case Study: FIRMS

### └ Attack overview

### └ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks

<sup>1</sup><https://satellite.mnsgo.noaa.gov/firms/>

<sup>2</sup><https://www.researchgate.net/publication/351111111>

All the tools used in our attack will be published alongside our paper

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Case Study: FIRMS

### └ Attack overview

### └ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed

<sup>1</sup><https://satbaa.ndbc.noaa.gov/firms/>

<sup>2</sup><https://www.researchgate.net/publication/311111111>

All the tools used in our attack will be published alongside our paper

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Case Study: FIRMS

### └ Attack overview

### └ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create malicious packet structure

<sup>1</sup><https://satellite.mnsgis.com/arcgis/rest/services/>

<sup>2</sup><https://blatantreaders.com/gifs/news/gifs/with-an-academic-account>

All the tools used in our attack will be published alongside our paper

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Case Study: FIRMS

└ Attack overview

└ Attack overview

Attack overview  
Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create malicious packet structure
  - Process archived data to add/remove artifacts

<sup>1</sup><https://satellite.mngeo.mn.gov/firms/>

<sup>2</sup><https://blatantreaders.gitlab.io/sat-gps/#/01-an-academic-attack>

All the tools used in our attack will be published alongside our paper

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Case Study: FIRMS

### └ Attack overview

#### └ Attack overview

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create malicious packet structure
  - Process archived data to add/remove artifacts
  - Construct payload packet to trigger vulnerability chain

<sup>1</sup>[https://satbaas.nasa.gov/data/data\\_gov/details/](https://satbaas.nasa.gov/data/data_gov/details/)

<sup>2</sup><https://www.researchgate.net/publication/344444444>

All the tools used in our attack will be published alongside our paper



# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Countermeasures

└ Countermeasures

## **We discuss the countermeasures in context**

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Countermeasures

└ Countermeasures

## We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Countermeasures

## └ Countermeasures

## **We discuss the countermeasures in context**

### Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

### Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

### Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Countermeasures

### └ Countermeasures

Cryptography should be required in future satellites  
But existing satellites can't be upgraded

Backwards-compatible countermeasures:

- Multi-receiver data comparison

## **We discuss the countermeasures in context**

### Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

### Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

### Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Countermeasures

## └ Countermeasures

Cryptography should be required in future satellites  
But existing satellites can't be upgraded

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>

<sup>2</sup>Willems et al. (2017) "Data-based Authentication Using TDOA Signatures in Satellite Networks"

## We discuss the countermeasures in context

### Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

### Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

### Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Countermeasures

## └ Countermeasures

Cryptography should be required in future satellites  
But existing satellites can't be upgraded

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>
- Physical-layer fingerprinting<sup>3</sup>

<sup>2</sup>Estemourel et al. (2021) "Data-based Authentication Using TDOA Signatures in Satellite Networks"  
<sup>3</sup>Chen et al. (2022) "Physical Layer Authentication of Satellite Transmitters via Deep Learning"

## We discuss the countermeasures in context

### Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

### Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

### Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

# Spoofing Earth Observation Satellites through Radio Overshadowing

## └ Countermeasures

## └ Countermeasures

Cryptography should be required in future satellites  
But existing satellites can't be upgraded

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>
- Physical-layer fingerprinting<sup>3</sup>

Existing countermeasures are effective, but aren't viable in all scenarios

<sup>2</sup>Estemouret et al. (2017) "Data-based Authentication Using TDOA Signatures in Satellite Networks"  
<sup>3</sup>Chen et al. (2022) "Physical Layer Authentication of Satellite Transmitters via Deep Learning"

## We discuss the countermeasures in context

### Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

### Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

### Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Future work

└ Future research directions

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems



2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Future work

└ Future research directions

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Future research is required to:

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Future work

└ Future research directions

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Future research is required to:

- Validate this work against real-world receiver hardware

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Future work

└ Future research directions

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Future research is required to:

- Validate this work against real-world receiver hardware
- Comprehensively review other vulnerable satellites

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

2023-02-27

# Spoofing Earth Observation Satellites through Radio Overshadowing

└ Future work

└ Future research directions

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Future research is required to:

- Validate this work against real-world receiver hardware
- Comprehensively review other vulnerable satellites
- Analyze the effectiveness of proposed overshadowing countermeasures

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems