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
- Traditional approaches like analysing signal-to-noise may prove effective

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

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
- Traditional approaches like analysing signal-to-noise may prove effective

Countermeasures

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

Backwards-compatible countermeasures:

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
- Traditional approaches like analysing signal-to-noise may prove effective

Countermeasures

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

Backwards-compatible countermeasures:
- Multi-receiver data comparison

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
- Traditional approaches like analysing signal-to-noise may prove effective

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

Backwards-compatible countermeasures:
- Multi-receiver data comparison
- Timing analysis[2]

[2] Jedermann et. al. (2021) "*Orbit-based Authentication Using TDOA Signatures in Satellite Networks*"

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
- Traditional approaches like analysing signal-to-noise may prove effective

Countermeasures

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

Backwards-compatible countermeasures:
- Multi-receiver data comparison
- Timing analysis[2]
- Physical-layer fingerprinting[3]

[2] Jedermann et. al. (2021) *"Orbit-based Authentication Using TDOA Signatures in Satellite Networks"*
[3] Oligeri et. al. (2022) *"PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"*

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
- Traditional approaches like analysing signal-to-noise may prove effective

Spoofing Earth Observation Satellites through Radio Overshadowing

Countermeasures

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[2]
- Physical-layer fingerprinting[3]

Comparative analysis presented in the paper

[2] Jedermann et. al. (2021) *"Orbit-based Authentication Using TDOA Signatures in Satellite Networks"*
[3] Oligeri et. al. (2022) *"PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"*

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
- Traditional approaches like analysing signal-to-noise may prove effective